COURSE GUIDE

CSS 810
CYBERCRIME AND FORENSIC INVESTIGATION

Course Team Dr. Macpherson UchennaNnam, (Course Writer/Developer)-AE-FUNAI
Course Co-cordinator
Course Editor
Programme Leader

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16, Ahmadu Bello Way
Victoria Island, Lagos

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published By:
National Open University of Nigeria

First Printed 2021

ISBN: 978-978-058-313-2

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher

CONTENTS **PAGE**

INTRODUCTION

Welcome to CSS 810: Cybercrime and Forensic Investigation

CSS 810 is a 3-Credit Unit course that provides you the needed insights into the various topics and perspectives on cybercrime and forensic investigation. It is specifically prepared for students pursuing a Master Degree Programme in Criminology and Security Studies at the National Open University of Nigeria (NOUN).

Cybercrime is a complex social problem that requires sufficient state-of-the-art scientific and technology-assisted preventive and control tools and techniques, as well as acknowledged experts in digital forensic investigations, to combat. This course material is a basic guide on cybercrime and forensic investigation. It provides you with step by step but simple explanations and understanding of the role of forensic investigators and analysts in processing digital evidence and prosecution of cybercrime suspects.

In this course, cybercrime management techniques, analysis and critical thinking, as well as the role of science and technology in criminal justice are explored. Ethical issues and special topics and controversies surrounding the application of forensic investigation reports and digital evidence are presented. To have a comprehensive understanding of this course, and its various Units, you are required to develop critical thinking and intensive reading culture. You need to develop analytical skills to understand and apply forensic investigative procedures to address the aetiology and epidemiology of cybercrime, as well as support legal arguments, perspectives and decisions.

Cybercrime activities leave a trail of incriminating evidence, so you will focus on learning the tools, techniques, and procedures for detecting cybercrime and analysing collected data/evidence related to past and ongoing cyber offences. The focus will be on forensic approaches that preserve the evidential value of the collected evidence to make them admissible in a court of law. Another area of interest is to expose students to the steps or stages of computer forensic investigation, beginning from policy and procedure development through to the documenting and reporting phase. This entails ethical and lawful gathering and evaluation, assessment of information that concerns cybercrimes, with specific attention on the fundamentals of forensic examination, the organisation and management of the investigative processes, and the knowledge and skills necessary for conducting the investigation.

AIMS AND OBJECTIVES

In this course, aims and objectives will be explained. The module provides some useful information on the reading pattern, the role in using the Course Guide or Material, the structure of the module, and guidance for assessment.

AIMS

a) To provide step by step explanations to the roles of forensic investigation and evidence in criminal justice administration;
b) To examine the various forensic tools, approaches and procedures that preserve the legal value of collected physical and digital evidence samples;
c) To demonstrate in-depth understanding of digital forensic investigations: practices, procedures or protocols;
d) To apply digital forensic investigation approaches in addressing the aetiology and epidemiology of cybercrime and related crimes with a view to supporting legal arguments, perspectives and decisions; and
e) To critically evaluate and demonstrate the ability to communicate students programme through a combination of written papers and oral presentations on different subjects or areas in cybercrime and forensic investigation studies.

OBJECTIVES

i. To identify and expose you to the basic concepts, topics and perspectives on cybercrime;
ii. To present ethical issues in handling digital and physical evidence samples in relation to (computer and criminological) forensic investigation best practices;
iii. To analyse the controversies surrounding forensic investigations and evidence;
iv. To equip you with tools, techniques, and procedures for detecting cybercrime, evidence, and analyses collected data and information related to past and ongoing cyber offences;
v. To introduce you to the lawful gathering and evaluation of information that concerns cyber-dependent crimes and cyber-enabled crimes to make for a successful investigation;
vi. To recapture your attention on the fundamentals of investigation, organisation and management of investigative processes, and the knowledge and skills necessary for conducting the investigation.

WORKING THROUGH THIS COURSE

To complete this course, you are advised to check the Study Units, read the recommended books and other related, relevant Course Materials provided by the National Open University of Nigeria (NOUN). Each Module contains Self-Assessment Exercise (SAE) and Tutor-Marked Assignments (TMAs) for assessment purposes. There will be a written examination at the end of the course. The course should take students about 18 months to complete. You will find all the components of the course listed below. You need to allocate time to each Unit to finish the course successfully.

COURSE MATERIALS

For this course, you will require the following materials:

1) The Course Guide;
2) Study Units which are fifteen (15) in all;
3) Textbooks recommended at the end of the Units;
4) Assignment file where all the Unit assignments are kept; and
5) Presentation schedule.

STUDY UNITS

There are 15 Study Units in this course, broken into three Modules of five Units each.

They are as follows:

Module 1

Unit 1 Introduction and General Background to Cyberspace.
Unit 2 Types/Forms of Cybercrime.
Unit 3 Trends in Cybercrime.
Unit 4 Effects of Cybercrime
Unit 5 Prevention and Control of Cybercrime.
Unit 6 Obstacles to the Prevention and Control of Cybercrime.

Module 2

Unit 1 Introduction and General Background to Forensic Science/Investigation.
Unit 2 Scope/Units/Branches of Forensic Science/Investigation.
Unit 3 Role of Forensic Investigation and Evidence in the Criminal Justice System.
Unit 4 Basic Features of Cybersecurity Strategies.

Unit 5 Challenges of Forensic Investigation and Prosecution of Cybercrimes.

Module 3

Unit 1 Tools Used for Computer Forensics.
Unit 2 Ethical Issues in Cybercrime and Computer Forensic Investigations.
Unit 3 Digital Forensic Investigations: Practices, Procedures or Protocols.
Unit 4 Controversies Surrounding Forensic Investigations and Evidence in Court.

Each Unit contains some exercises on the topic covered, and you will be required to attempt the exercises. These will enable you evaluate your progress as well as reinforce what you have learnt so far. The exercise, together with the Tutor-Marked Assignments, will assist you in achieving the stated learning outcomes of the individual Units and the course.

TEXT BOOKS AND REFERENCES

You may wish to consult the references and other books suggested at the end of each Unit to enrich your knowledge of the course. This will enhance your understanding of the Course Material.

ASSESSMENT

Assessment for this course is in two parts, such as the Tutor-Marked Assignments, and a written examination. You will be required to apply the information and knowledge gained from this course in completing your assignments. You must submit the assignments to your tutor in line with submission deadlines stated in the assignment file. The work that you submit to your Tutor-Marked Assignment for assessment will count for 30% of your total score.

TUTOR-MARKED ASSIGNMENTS (TMAS)

In this course, you will be required to study 15 Units, and complete Tutor-Marked Assignments provided at the end of each Unit. The assignments carry 10% marks each. The best four of your assignments will constitute 30% of your final mark. At the end of the course, you will be required to write a final examination, which counts for 70% of your final mark.

The assignments for each Unit in this course are contained in your assignment file. You may wish to consult other related materials, apart from your Course Material, to complete your assignments. When you complete each assignment, send it together with a Tutor-Marked Assignment form to your tutor. Ensure that each assignment reaches your tutor before the deadline stipulated in the assignment file. If, for any reason you are unable to complete your assignment on time, contact your tutor before the due date to discuss the possibility of an extension. Note that extensions will not be granted after the due date for submission unless under exceptional circumstances.

FINAL EXAMINATION AND GRADING

The final examination for this course will be for three hours and count for 70% of your total mark. The examination will consist of questions, which reflect the information in your Course Material, exercise, and Tutor-Marked Assignments. All aspects of the course will be examined. Use the time between the completion of the last Unit and examination rate to revise the entire course. You may also find it useful to review your Tutor-Marked Assignments before the examination.

COURSE MARKING SCHEME

ASSESSMENT	**MARKS**
Assignments	Four assignments, best three marks of four count at 30% of course marks
Final Examination	70% of total course mark
Total	**100% of course marks**

COURSE OVERVIEW

Module 1	**Title of Work**	**Weeks Activity**	**Assessment (End of Unit)**
Unit 1	Introduction and GeneralBackground to Cyberspace	Week 1	
2	Types/Forms of Cybercrime	Week 2	
3	Trends in Cybercrime	Week 3	Assignment 1
4	Effects of Cybercrime	Week 4	
5	Prevention and Control of Cybercrime	Week 5	
6	Obstacle to the Prevention and Control of Cybercrime	Week 6	
Module 2			
Unit 1	Introduction and General Background to Forensic Science/Investigation	Week 7	Assignment 2

2	Scope/Units/Branches of Forensic Science/Investigation	Week 8	
3	Roles of Forensic Investigation and Evidence in Criminal Justice	Week 9	
4	Basic Features of Cybersecurity Strategies	Week 10	
5	Challenges of Forensic Investigation and Prosecution of Cybercrimes	Week 11	
Module 3			
Unit 1	Tools Used for Computer Forensics	Week 12	Assignment 3
2	Ethical Issues in Cybercrime and Forensic Investigations	Week 13	
3	Digital Forensic Investigations: Practices, Procedures or Protocols	Week 14	
4	Controversies Surrounding Forensic Investigation and Evidence in Court	Week 15	Assignment 2
	Revision	Week 16	
	Examinations	Week 17	
	Total	18 Weeks	

HOW TO GET THE MOST FROM THIS COURSE

In distance learning, your course material replaces the lecturer, but by no means, all-inclusive.

The Course Material has been designed in such a way that you can study on your own with little or no assistance. This allows you to work, and study at your pace, and at a time and place that best suits you. Think of reading your Course Material in the same way as listening to the lecturer. However, you are advised to study your Course Material in the same way a lecturer might give you some readings to do. The Study Units give you information on what to read, and these form your text materials. You are provided with exercise to do at appropriate points, like a lecturer might give you an in-class exercise.

Each of the Study Units follows a common format. The first item is an introduction to the Unit, and how a particular Unit is integrated with other Units and the course as a whole. Next to this is a set of learning

objectives and outcomes. These objectives inform you about what you are required to know by the time you have completed the Unit; they are meant to guide your study. The moment a Unit is finished, you must go back and check whether you have achieved the objectives. If you make this a habit, it will improve your chances of passing the course significantly.

The main body of the Unit guides you through the required reading from other sources. This will usually be either from the reference books or from a reading section. The following is a practical strategy for working through the course. If you run into difficulties, telephone your tutor. Remember that your tutor's job is to help you when you need assistance, so do not hesitate to call and ask your tutor for help or visit yourstudy centre.

Reading this Course Guide thoroughly is your first assignment

1) Organise a study schedule, design a 'Course Overview' to guide you through the course. Note the time you are expected to spend on each Unit and how the assignments relate to this Unit. You need to gather all the information into one place, such as your diary or a wall calendar. Whatever method you choose to use, you should decide and write in your own dates and schedule of work for each Unit.
2) Once you have created your own study schedule, do everything to be faithfully to it. The major reason students fail is that they get behind with their course work. If you get into difficulties with your schedule, please let your tutor know before it is too late for help.
3) Turn to Unit 1, and read the introduction and the objectives for the Unit.
4) Assemble the study materials. You will need the reference books in the Unit you are studying at any point in time.
5) Work through the Unit. As you work through the Unit, you will know what sources to consult for further information.
6) Before the relevant due dates (about 4 weeks before due dates), access the assignment file. Keep in mind that you will learn a lot by doing the assignment carefully, they have been designed to help you meet the objectives of the course and pass the examination. Submit all assignments not later than the due date.
7) Review the objectives for each Study Unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study materials or consult your tutor.
8) When you are confident that you have achieved a Unit's objectives, you can start on the next Unit. Proceed Unit by Unit

through the course and try to pace your study so that you keep yourself on schedule.

9) When you have submitted an assignment to your tutor for marking, do not wait for marking before starting on the next Unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the Tutor-Marked Assignment form and also the written comments on the ordinary assignments.

10) After completing the last Unit, review the course and prepare yourself for the final examination. Check to see that you have achieved the Unit objectives (listed at the beginning of each Unit) and the course objectives (listed in the Course Guide)

TUTORS AND TUTORIALS

There are 15 hours of tutorials provided to support this course. Tutorials are for problem solving and they are optional. You need to get in touch with your tutor to arrange date and time for tutorials if needed. Your tutor will mark and comment on your assignments, keep a close watch on your progress and any difficulties you might encounter and provide assistance to you during the course. You must submit your Tutor-Marked Assignments to your tutor well before the due date (at least two work days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, email, or discussion board. The following might be circumstances in which you will find necessary to contact your tutor if:

1. You do not understand any part of the Study Units or the designed readings.
2. You have difficulties with the exercises.
3. You have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

To gain maximum benefits from this course tutorials, prepare a question list before attending to them. You will learn quite a lot from participating in the discussions.

SUMMARY

The course guide has introduced you to what to expect in cybercrime and forensic investigations. It examined the general background of cybercrime and forensics, types/forms and prevention/control of

cybercrime, scope of forensic science, challenges of forensic investigations and prosecution of cybercrimes, roles of forensic investigations and evidence in criminal justice, and digital forensic investigation: Practices, procedures or protocols.

The course also discussed tools used in computer forensic, ethical issues in cybercrime and forensic investigations, and controversies surrounding forensic investigations and evidence in court. Upon completion, you should be equipped with the foundation for analysing and researching cybercrime and forensic investigation issues.

We wish you success with the course and hope you will find it both engaging and practical.

REFERENCES/FURTHER READING

Abdulkareem, H. (2018, July 30). How *Boko Haram* is Funded – UN. ThisDay, p. 51.

Abdullahi, A. & Saleh, M. (2017). Online identity theft in Nigeria: Risk factors and control. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 241-250). Zaria: Ahmadu Bello University Press.

Adegoke, N. & Aderoju, M. A. (2017). Cyber crime and technology misuse in Nigeria: Trends. issues and challenges. In Iwarimie-Jaja, D. & Agwanwo, D. E. (Eds.), *Contemporary criminality in Nigeria: Challenges and options* (pp. 301-319). Ibadan: Stirling-Horden Publishers.

Adejoh, S. O.; Alabi, T. A.; Adisa, W. B.; & Emezie, N. M. (2019). "Yahoo boys" phenomenon in Lagos metropolis: A qualitative investigation. *International Journal of Cyber Criminology*, *13* (1), 1-20.

Ajetunmobi, R. A. (2009). *Cyber crime – a case for computer forensic guidelines in Nigeria* (M. Sc. Dissertation). Department of Information Security and Computer Forensics, University of East London, London, United Kingdom.

Alemika, E. E. O. (2017). Foreword. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. ix-x). Zaria: Ahmadu Bello University Press.

Anon. (2016). *The science of forensic criminology*. Retrieved from http://www.forensiccriminologist.com/Forensic_Criminology.html. Accessed 19 March 2016.

Antwi-Boasiako, A. & Venter, H. (2017). A model for digital evidence admissibility. In Peterson, G. & Shenoi, S. (Eds.), *Advances in Digital Forensics* (pp. 23-38). Carolina: Carolina Academic Press.

Arshad, H.; Jantan, A. B.; & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems, 4*(2), pp. 346-376.

Ashcroft, J.; Daniels, D. J.; & Hart, S. V. (1999). *Forensic examination of digital evidence: A guide for law enforcement*. Washington, DC: US Department of Justice, Office of Justice Programme.

Behr, I. V.; Reding, A.; Edwards, C.; & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. Santa Monica, CA: RAND Corporation.

Beirne, P. & Messerschmidt, J. W. (2015). *Criminology: A sociological approach* (6th ed.). New York: Oxford University Press.

Bello, K. (2017). Information community technology and cybercrime. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 169-184). Zaria: Ahmadu Bello University Press.

Brantingham, P. & Brantingham, P. J. (2008). Crime pattern theory. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 78-93). Willan: Portland.

Brantingham, P. L. & Brantingham, P. J. (1993). *Environment, routine, and situation: Towards a pattern theory of crime*. New York: Crime Prevention Studies.

Burke, R. H. (2019). *An introduction to criminological theories* (5th ed.). New York: Routledge.

Casey, E. (2011). *Digital evidence and computer: Forensic science, computer and the internet* (3rd). Academic Press.

Chang, L. Y. C. & Grabosky, P. (2014). Cybercrime and establishing a secure cyber world. In M. Gill (Ed), *Handbook of Security* (pp. 321.339). New York: Palgrave.

Chavan, A. & Ahire, S. (2015). Perspectives of cybercrime with prevention, detection, and prosecution. *International Journal of*

Scientific Engineering and Technology Research, 4(18), 3391-3396.

Chisum, W. & Turvey, B. (2007). *Crime reconstruction*. Boston: Elsevier Science.

Clark, R. B. & Cornish, D. B. (1986). *The reasoning criminal: Rational choice perspective in offending*. New York: Springer-Verlag.

CloudFlare. (2018). *What is a DDoS attack*? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Accessed 10 January 2020.

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Cornish, D. B. & Clarke, R. V. (2008). The rational choice perspective. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 21-47). Willan: Portland.

Conlan, K.; Baggili, I. & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, *18*, 66- 75.

Dougherty, D. (n. d.). *Forensic sociology and criminology*. Retrieved from http://www.rosemont.edu/academics/graduate/forensic-sociology-criminology/. Accessed 19 March 2016.

Ebenezer, A. J. (2014). Cyber fraud, global trade and youth crime burden: Nigerian experience. *Afro Asian Journal of Social Sciences*, *5*(4)1-13.

Etuk, G. R. & Nnam, M. U. (2018). Predictors and risk factors of armed robbery victimisation in Nigeria: An integrated theoretical perspective. *European Scientific Journal, 14*(29),1-15.

Europol. (2018). *The internet organised crime threat assessment* 2018. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised- crime-threat-assessment-iocta-2018. Accessed 2 February 2020.

George, D.; Rawlings, R.; Williams, W.; Phillips, M.; Fong, G.; Kerich, M.; Momenam, R.; Umhau, J. & Hommer, D. (2004). A select group of perpetrators of domestic violence: Evidence of decreased metabolism in the right hypothalamus and reduced relationships between cortical/subcortical brain structures in

positron emission tomography. *Psychiatry Research: Neuroimaging*, *130*, 11-5.

Giddens, A. & Sutton, P. W. (2013). *Sociology* (7th ed.). Hoboken, NJ: John Wiley & Sons.

Goodman, M. D. & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Felson, M. (1998). *Crime and everyday life* (2nd ed.). Thousand Oaks, CA: Pine Forge.

Felson, M. & Boba, R. (2010). *Crime and everyday life* (4th ed.). Thousand Oaks, CA: Sage.

Frank, I. & Odunayo, E. (2013). Approach to cyber-security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science, Engineering and Education*. Retrieved from http://ijcrsee.com/index.php/ijcrsee/article/view/11/114. Accessed 10 December 2019.

Gordon, S. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, *2*(1), 13-20. DOI: 10.1007/s11416-006-0015-z.

Gudjonsson, G. H. & Haward, L. R. C. (1998). *Forensic psychology: A guide to practice*. London: Routledge.

Haralambos, M.; Holborn, M. & Heald, R. (2008). *Sociology: Themes and perspectives* (7th ed.). London: HarperCollins.

Hern, A. (2017, May 31). Hackers publish private photos from cosmetic surgery clinic. *Guardian*. Retrieved from https://www.theguardian.com/technology/2017/may/31/ hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments. Retrieved from 10 January 2020.

Holt, T. J.; Bossler, A. M. & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensic* (2nd). Routledge.

Hussien, M. D.; Sarki, Z. M. & Lalu, A. U. (2017). Forensic science, electronic evidence and cybercrime prosecution in Nigeria. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology assisted crime and control: A reader* (pp. 367-382). Zaria: Ahmadu Bello University Press.

Ibrahim, B. & Mukhtar, J. I. (2017). Emerging cyber-terrorism threats in Nigeria. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 415-428). Zaria: Ahmadu Bello University Press.

Iwarimie-Jaja, D. (2003). *Criminology: The study of crime* (2nd ed.). Owerri: Springfield Publishers.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of CyberCriminology, 1*(2), 7-9.

Jaishankar, K. (2008). Space transition theory of cybercrimes. In Schmallager, F. & Pittaro, M. (Eds.), *Crimes of the internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2017) (Ed.). *Cyber criminology: Exploring internet crimes and criminal behaviour*. India: CRC Press.

Kaufman, R. (2017, February 10). Forensic science controversies. *CQ researcher*, *27*, 121-144.

Lazarus, S. & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the economic and financial crimes commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

Lewis, L. (n. d.). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Retrieved from http://csis.org/files/media/csis/pubs/021101risks_of_cyberterror.pdf. Accessed 10 February 2020.

Lissitzyn, C. B. (2008). *Forensic evidence in court: A case study approach*. Durham, NC: Carolina Academic Press.

Madaki. M. & Sarki, U. U. (2017). Digital piracy and active internet users in Nigeria. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 287-296). Zaria: Ahmadu Bello University Press.

Manu, Y. A. (2017). Globalisation, cyber-terrorism and Nigeria's national security. In P.

N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp.395-411). Zaria: Ahmadu Bello University Press.

Maras, M. (2014). *Computer forensics: Cybercriminals, laws, and evidence*. Retrieved from

https://www.unodc.org/e4j/data/_university_uni_/computer_forensic_ criminals_laws_and_evidence.html? Accessed 4 February 2020.

Maras, M. (2016). *Cyber criminology*. Oxford: Oxford University Press.

Melvin, A. O. & Ayotunde, T. (2011). Spirituality in cyber crime ("yahoo yahoo") activities among youths in south west Nigeria. In Dunkels, E.; Franberg, G. & Hallgren, C. (Eds.), *Youth culture and net culture*: *Online social practices* (pp. 357-376). Hershey, PA: IGI Global.

Moffit, T.; Pannatia, C.; Prosenbeck, B.; Scott, E. & Siverson, D. (2012). *The HRE online experience – technology misuse and cyber crime*. Retrieved from https://sites.google.com.site/tommoffittportfolio/the-hre-online-experience/ technology-misuse-and-cyber-crime. Accessed 10 November, 2013.

Moore, R. (2005). *Cybercrime: Investigating high-technology computer crime*. Cleveland, Mississippi: Anderson Publishing.

Nasi, M.; Oksanen, A.; Keipi, A. & Rasanen, P. (2013). Cybercrime victimisation among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210.

National Crime Prevention Council. (2011). *Cybercrimes*. Retrieved from www.ncpc.otg. Accessed 22 January 2020.

Ndubueze, P. N. (2017a). Cyber criminology: Contexts, concerns and directions. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 1-28). Zaria: Ahmadu Bello University Press.

Ndubueze, P. N. (2017b). Cyber criminology: Context, concerns and directions. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 1-28). Zaria: Ahmadu Bello University Press.

Nnam, M. U.; Ajah, B. O.; Arua, C. C.; Okechukwu, G. & Okorie, C. O. (2019). The war must be sustained: An integrated theoretical perspective of the cyberspace- *boko haram* terrorism nexus in Nigeria. *International Journal of Cyber Criminology*, 13(2), 379-395.

National Security Council. (n. d.). *Transnational organised crime: A growing threat to national and international security*. Retrieved from http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat. Accessed 26 April 2020.

Nigeria Police Annual Report. (2010). *The Nigeria Police annual report*. Ikeja, Lagos: "F" Department and Nigeria Police Printing Press, FHQ annex.

Norden, S. (2013). *How the internet has changed the face of crime* (M. Sc. Dissertation). Florida Gulf Coast University, Florida, United States.

Norwich University Online. (2017). *5 steps for conducting forensic investigations*. Retrieved from https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations. Accessed 12 January 2020.

Nwokeoma, B. N.; Ndubueze, P. N. & Igbo, E. U. M. (2017). Precursor of online advance fee fraud in south east Nigeria. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 195-218). Zaria: Ahmadu Bello University Press.

Olumoye, M. Y. (2013). Cyber crime and technology misuse: Overview, impact and preventive measures. *European Journal of Computer Science and Information, 1*(3), 10-20.

Okoh, J. & Chukwueke, E. D. (2016). *The Nigerian cybercrime act 2015 and its implications for financial institutions and service providers*. Retrieved from https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its implications-for-financial-institutions-and-service-providers#.XqaZEBIod_k.Accessed 27 April 2020.

Osayi, K. K. (2017). Cyber-stalking, cyber-bulling and cyber-squatting: A conceptual analysis. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 29-46). Zaria: Ahmadu Bello University Press.

Otu, S. E. (2003). Armed robbery in the southeastern states of contemporary Nigeria: A criminological analysis. A Doctoral Thesis Submitted to the Department of Criminology, University of South Africa, Pretoria, South Africa.

Otu, S. E. (2010). Decision-making practices in armed robbery among armed robbers in Nigeria. *International Journal of Research in Arts and Social Sciences, 2*, 371-391.

Palmer, G. (2001). DFRWS technical report: A road map for digital forensic research. *Digital Forensic Research Workshop*. Utica, New York.

Parkin, S. (2017, September 8). *Keyboard warrior: The British hacker fighting for his life*. Retrieved from https://www.theguardian.com.news/2017/sep/08/lauri-love-british-hacker-anonymous-extradiction.us. Accessed 10 January 2020.

Raine, A.; Buchsbaum, M. & LaCasse, L. (1997). Brain abnormalities in murderers indicated by positron emission tomography. *Biological Psychiatry, 42*, 495-508.

Robinson, A.; Marchment, Z. & Gill, P. (2019). Domestic extremist criminal damage events: Behaving like criminals or extremists. *Security Journal, 32*, 153-167.

Roshier, B. (1989). *Controlling crime*. Chicago: Lyceum Books.

Saferstein, R. (2007). *Criminalistics: An introduction to forensic science* (9th ed.). New Jersey: Prentice Hall.

Samuel, K. O.; Osman, W. S.; Al-Khasawneh, Y. & Duhaim, S. (2014). Cyber terrorism attack of the contemporary information technology age: Issues, consequences and panacea. *International Journal of Computer Science and Mobile Computing, 3*(5), 1082-1090.

Scriven, M. & Paul, R. (1996). Defining critical thinking: a draft statement for the national council for excellence in critical thinking. Retrieved from http://www.criticalthinking.org/University/univlibrary/library.nclk. Accessed 19 March 2016.

Sharma, V. (2015). Information technology and cyber crime. *Journal of Institution of Information Technology and Management, 1*(1), 75-78.

Siegel, L. J. & McCormick, C. (2006). *Criminology in Canada: Theories, patterns and typologies* (3rd ed.). Toronto, ON: Thompson, Nelson.

Siegel, L. J. (2007). *Criminology: Theories, patterns, and typologies* (9th ed.). Belmont, California: Thomas Higher Education.

Siegel, L. J. (2008). *Criminology: The core* (3rd ed.). Belmont, California: Thomas Higher Education.

Silva, J. A.; Leong, G. B. & Ferrari, M. M. (2004). A neuropsychiatric developmental model of serial homicidal Behaviour. *Behavioural Science and the Law, 22,* 787- 799.

Smith, R.; Grabosky, P. & Urbas, G. (2004). *Cybercriminals on trial*. Cambridge: Cambridge University Press.

Sovern, J. (2004). Stopping identity theft. *The Journal of Consumer Affairs, 38*(2), 233- 242.

Stibli, E. (2010). Terrorism in the context of globalisation. *AARMS, 9*(1), 1-7.

Sutherland, E. H. & Cressey, R. D. (1974). *Criminology*. (9th ed.). Philadelphia: J.B. Lippincott.

Sykes, G. (1978). *Criminology*. New York: Harcourt Brace Jovanovich.

Tafoya, W. L. (2011). Cyber terror. *FBI law enforcement bulletin* (FBI.gov), November. Retrieved from https://leb.fbi.gov/articles/featured-articles/cyber-terror. Accessed 10 February 2020.

Tancredi, L. (2004). *Hardwired behaviour: What neuroscience reveals about morality*. London: Cambridge University Press.

The Nigerian Cybercrimes Act 2015. (2015).*Cybercrimes (prohibition, prevention, etc) Act, 2015*. Retrieved from https://www.the+cybercrimes+%28prohibition%2C+ prevention%2C+etc%29+act+2015. Accessed 26 April 2020.

United Nations Office on Drugs and Crime. (2013). *(Draft) Comprehensive Study on Cybercrime.* Retrieved from https://www.unodc.org/documents/organised-crime/unodc_ccpcj-eg.4_2013/cybercrime_study_210213.pdf. Accessed 20 February 2020.

United Nations Office on Drugs and Crime. (2017). *The drug problem and organised crime, illicit financial flows, corruption and terrorism* (Part 5). Vienna: The Author.

United Nations Office on Drugs and Crime. (2019). *E4J university module series: Cybercrime*. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/basics-of-computing.html. Accessed 20 December, 2019.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Ward, J. T. (2013). What is forensic psychology? Retrieved from http://www.apa.org/ed/precollege/psn/2013/09/forensic-psychology.aspx. Accessed 19 March 2016.

Wilson, C. (2008). *Botnet, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for progress*.

Wilson, S. M. & Peterson, L. C. (2002). The anthropology of online communication. *Annual Review Anthropology, 31*, 449-467. DOI: 10.1146/annurev.anthro.31.040402.085436.

Valacich, J. & Schneider, C. (2010). *Information systems today – managing in the digital world* (4th ed.). New Jersey: Pearson.

MAIN COURSE

CONTENTS **PAGE**

MODULE 1

Unit 1 Introduction and General Background to Cybercrime and Cyber Criminology.
Unit 2 Types/Forms of Cybercrime.
Unit 3 Trends in Cybercrime.
Unit 4 Effects of Cybercrime
Unit 5 Prevention and Control of Cybercrime.
Unit 6 Obstacle to the Prevention and Control of Cybercrime.

CONTENTS

1.0 INTRODUCTION

A way of understanding any subject is to know its meaning/definition, trends, purpose and scope. To understand cybercrime, we must define what it is and the definition should be in such a way as to make meaning clear to all the end-users.

2.0 OBJECTIVES

By the end of the unit, you will be able to:

- define and explain cybercrime,
- distinguish between cyber-dependent crimes and cyber-enabled crimes.

3.0 MAIN CONTENT

3.1 Introduction and General Background to Cyberspace

The term, 'cyber,' simply refers to the development of a new digital space existing and flourishing with the help of breakthrough in Information and Communication Technology (ICT) in recent times. The "breakthrough in digital technology involves the movement of social interaction, which has hitherto existed in the physical space, to a virtual domain that has come to be known across the globe as the cyber space" (Osayi, 2017, p. 29). Although some of the ICTs and/or Internet facilities are tangible and installed in the social-cum-physical space or environment, the vast majority of them are not. Nonetheless, they are mainly utilised or made super-functional in the cyberspace to aid human activities, whether pro-social or anti-social (Nnam, Ajah, Arua, Okechukwu, & Okorie, 2019).

Although cybercrime predates cyber criminology, the former is currently a subject of the latter. Cyber criminology is a new sub-field of criminology designed and introduced to specifically address the problem of crime and criminality committed in or linked to the cyberspace and other virtual environments. That is, cyber criminology is devoted to tackle cyber-dependent crimes and cyber-enabled crimes in the social and physical space. It is an emerging area of specialisation in the broad field of general criminology, established by an Indian criminologist, Prof. Karuppannan Jaishankar, in 2007.

The Nigerian cyberspace has been ever more vulnerable to crime of different typologies, yet not much improvement have been made by computer scientists, criminologists and law enforcement agents in Nigeria to understand the pathways and trajectories of the offending behaviour going on the virtual arena. It is against this backdrop that the current Course Material is designed to uniquely contribute to the relatively few existing texts on cybercrime and cyber criminology in relation to forensic investigations, though borrowing extensively from scholarly works of experts from the Western world.

According to Nnam *et al.* (2019), the sub-area of cyber criminology generally and cybercrime in particular, is critically under-researched in

Nigeria. Although the problem has received adequate scholarly attention in the Western world, as evidenced by a large volume of literature on the topic, it has received comparatively far less attention in Nigeria and thereby making the war on terrorism an effort in futility while the terrorists are having a field day in their daily atrocious operations. This is further explained thus:

> Since the establishment of cyber criminology in 2007 by an Indian Criminologist, Professor Karuppannan Jaishankar, the new sub-discipline seems to have been suppressed by the mainstream criminology and the various research efforts that relate to it are largely Western. Although Nigerian cyberspace is increasingly vulnerable to deviance, crime and terror, it is noted that not so many advances have been achieved by criminologists in Nigeria in form of understanding the dynamics of these critical developments. There seems to be a shortage of dedicated cyber criminologists and a dearth of cyber criminology textbooks in Nigeria, even if for reference purposes (Ndubueze, 2017a, p. xiv).

Although other factors (such as 'globalisation, mediatisation/digitisation, growth of virtual communities, etc') exist, the Internet revolution strongly influenced the development of cyber criminology. The discovery of the Internet and its intersection with ICT is a springboard for the emergence of cyber criminology. The abuse of the Internet, particularly its frequent use in committing crimes, spurred criminologists to explore this new area of specialisation in criminology and security studies. However, it is important to note that early literature generally conceived the Internet as revolutionary in relation to its technical innovation, social and political impacts (see Wilson & Peterson, 2002). This conception indeed negates the fact that the Internet has serious implications for criminology and criminal justice: People now exploit the vast (perhaps unintended) opportunities offered by the Internet to perpetrate crimes. Hence, the dire need to establish a specially designed area of cognate expertise, discipline to holistically address the cybercrime problem.

The Internet revolution has significantly reduced and accelerated the 'free' flow of communication and movement of goods and services. However, it also has both intended (pro-social, acceptable or approved)

and unintended (anti-social, unacceptable or disapproved) functions and benefits. According to the United Nations Office on Drugs and Crime (UNODC), although the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organisations and to transmit information on, as well as material support for, planned acts of terrorism, all of which require specific technical knowledge for the effective investigation of this offence (UNODC, 2012).

A recent research (see Nnam, *et al*., 2019) on cybercrime in Nigeria reveals that virtual environments, cyberspace is arguably characterised by both intended and unintended establishment goals. The former attempts to explain the original and main aim of creating the cyberspace: To catch up with globalisation trends in runaway society. Examples include improved and flourishing global economy, legal system, polity, security, crime prevention and control efforts, and such other structures of society. The latter, on the other hand, simply refers to the manipulation of the cyberspace. It explains a situation whereby the original conception of cyberspace is circumvented, subverted, or perhaps supplanted by individual offenders and terrorist groups to perfect in their criminal enterprise (Nnam, *et al*., 2019).

From the above source, again, the rapid advancement in modern science and technology, coupled with the near-recent advancement in social media networking, has permanently left the door of cyberspace ajar and unmanned. The situation has been exacerbated by such vulnerabilities obviously peculiar to the Internet and computer systems as hyper-speed in data retrieval, processing and transfer. Others include convenience, temporality of information, anonymity among users, and lack or total absence of clearly delineated cyber borders. Users, both criminals and non-criminals, currently use it with little or no restriction. There is high level criminogenic infiltration in the cyberspace, which has led to its contamination and abuse by most users. It is now a springboard for patterning and reshaping the modus operandi of many traditional crime perpetrators and criminal groups. Offenders now carry out research on the types of crime to indulge in, methods of attack and operation devise, and how to evade arrest, trial and conviction (Nnam, *et al*., 2019).

The information and communication technology is one of the strategic factors driving the increasing use of the Internet by terrorist organisations and their supporters for a wide range of purposes: Recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes (UNODC, 2012). Similar research findings show that “the so-called information revolution, with the unexpected rise of the Internet since the 1990s, has clearly been of growing societal

significance. The Internet offers terrorists and extremists the same opportunity and capability that it does for the rest of society: To communicate, collaborate and convince. There are already significant quantities of radical materials available online, and this volume is growing daily" (Behr, Reding, Edwards, & Gribbon, 2013, p. 3). This was explained in detail by Alemika (2017, p. ix), who "in his foreword to the first and only comprehensive text on cybercrime and cyber criminology in Nigeria (as at the time of this research) entitled *Cyber Criminology and Technology-Assisted Crime Control: A Reader*" (see Nnam, *et al*., 2019, p. 382), put it thus:

> Revolution in Information and Communication Technology (ICT) has brought tremendous benefits to humanity and society. It has advanced development in virtually all areas of human endeavour and enhanced the quality of goods and services offered by clients on global markets. ICT is most often deployed through the cyber space, largely invisible paths through which data and information are transmitted at very fast speed. However, the abuse of ICT has also brought misery to human beings. It has facilitated the ease with which serious crimes such as terrorism, transnational economic and financial crimes as well as political and economic espionages are perpetrated within and across countries. Crimes over cyberspace constitute serious threat to national security, economic development, political stability and fundamental rights. Paradoxically, it provides tremendous capacity for monitoring, preventing and combating these crimes and threats. ICT therefore provides opportunities and threats.

The popular belief is that the Internet has turned the world into a 'global village'. Establishing the veracity of this claim and/or otherwise repudiating it is problematic and contentious. But one thing is certain and universal about the Internet: It has altered, whether for good or bad, the entire social institutions and human behaviour. On the aspect of its advantageous position, the Internet has gone a long way to improve the flow of information, communication, world market and economy, art of governance, movement of goods and services, health and education, as well as integration of countries and criminal justice systems. Granted

that the Internet has immense benefits, but it is prone to abuse and presents both criminogenic and victimogenic opportunities for criminals to explore and exploit. Olumoye (2013) contended that the rapid expression of large-scale computer networks with the ability to access many systems through regular telecommunication lines increases the vulnerability of these systems and the opportunity for criminal activities.

Associated with the Internet is the phenomenon of globalisation; both phenomena intertwine with each other to give rise to the establishment of cyber criminology, and they are facilitated by information and communication technologies. Giddens and Sutton (2013) narrated that globalisation and its processes overlap with the development of information and communication technologies, which has facilitated the scope and speed of interaction among people globally. Others see it as a global process whereby individuals, peoples, economies and nation-states are becoming increasingly interconnected and interdependent to and with one another (Beirne & Messerschmidt, 2015).

Indeed, the globalisation trends received strong enhancement from the Internet revolution, and the innovation seems to have peaked in the 21st century, “when the digital divide began closing-up with relatively easy access to broadband across the world and particularly in developing countries, including Nigeria” (Ndubueze, 2017b, p. 2). The author further argued that “this development has deep-seated consequences for modern societies: While [as] businesses and leisure interactions have increased dramatically across the world, so have deviance, crime and terror” (p. 2). This, coupled with other social forces, interact to spur some criminologists to develop cyber-criminological thoughts. Notable among these early cybercrime researchers, as it were, is Holt (2003) who conducted a comparative investigation of the transnational nature of cybercrime in eight countries of the world. Yet, the actual development or emergence of cyber criminology is not attributed to him.

3.1.1 Definition of Cybercrime

Cybercrime poses many definitional problems. Currently, the crime has no one putative definition despite its relatively old history. This is as a result of the crime’s complex nature, multiple dimensions, proliferation of computers, and anonymity and transient status of the Internet connectivity and technology usage. Its definition is also affected and influenced by a country’s legal framework and political dynamics. Research also supports the fact that the idea of cybercrime is not new, yet there is significant confusion amongst academics, computer security experts and users as to the extent of real cybercrime (Gordon, 2006).

Interestingly, efforts have been made by the international community, policymakers, law enforcement agents, researchers and scholars to advance lucid and suitable conception of the term and crime. A comprehensive definition of cybercrime is founded on three basic elements: Firstly, its perpetration via electronic networks; secondly, technology's role; and thirdly, the various applicable laws (Nhan & Bachmann, 2015 cited in Ndubueze, 2017b). Hence, cybercrime is defined as an activity where computers or networks are a tool, a target or a place of criminality (Chavan & Ahire, 2015).

Various studies on cybercrime have been conducted. These studies have examined and defined cybercrime through the lens of psychology, sociology, and criminology, as well as other academic disciplines (see Jaishankar, 2011; Maras, 2016; Holt, Bossler, & Seigfried-Spellar, 2018). Contextually, cybercrime is defined as an act or omission to act which violates the law without cogent excuse or justification and is usually committed or omitted with the aid of Information and Communication Technology (ITC), or ITC being attacked while committing or omitting the crime. It is a computer-assisted or Internet-based criminal behaviour, but can be committed or omitted in the cyberspace or physical environment with the help of a computer or Internet facilities.

Cybercrime began with disgruntled employees causing physical damage to the computers they work with, the intention is to get back at their supervisors or employers. Nevertheless, as the ability to have personal computer at home becomes more accessible and popular, cybercriminals began to focus their efforts on home users (Matanmi, Ogunlere, Ayinde, & Adekunle, 2013 cited in Adegoke & Aderoju, 2017). Cybercrime is an unlawful act wherein computer is either a tool or target or both. The term 'computer' is contextualised beyond the conventional desktop or laptop to include cell phones, Personal Digital Assistance (PDA), and sophisticated watches, cars, among others (Sharma, 2015). According to Article 1 of the African Union Convention on Cyber Security and Personal Data Protection (AUCCSPDP) of 2014, a computer or computer system is "an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and including any data storage facility or communications facility related to or operating in conjunction with such device or devices" (AUCCSPDP, 2014, Article 1).

Maintaining similar position, UNODC (2019) reiterated that there is no generally accepted definition of cybercrime. However, some credible definitions have been offered by authorities in cybercrime. Cybercrime is an act that violates the law, which is perpetrated using ICT to either

target networks, systems, data, websites and/or technology or facilitate a crime (for detail, see Goodman & Brenner, 2002; Wall, 2007; Wilson, 2008; International Telecommunication Union [ITU], 2012; Maras, 2014; Maras, 2016). It can be perpetrated by individuals, groups, businesses, and nation-states. While these actors may use similar tactics (e.g., using malicious software) and attack similar targets (e.g., a computer system), they have different motives and intent for committing cybercrimes (Wall, 2007).

Cybercrime is said to know no boundaries; it can be committed in the cyberspace/virtual world or physical environment, suggests that computer could be the target of crime or assists in crime commission. For a better understanding of cybercrime, a distinction needs to be made between cyber-dependent crimes and cyber-enabled crimes. The former refers to those offences (e.g. hacking, phishing, vishing, etc) that can only be perpetrated with the help of computers, Internet facilities and/or ICT-assisted gadgets, while the latter describes traditional crimes (e.g. kidnaping, armed robbery, cultism, rape, examination misconduct, and murder) which their substantial transaction may take place in the physical space, but sometimes, can be facilitated and accomplished using the Internet and technology-assisted equipment (for detail, see also Europol, 2018).

Cyberspace, on the other hand, "comprises three partially overlapping terrains: (1) The Internet, encompassing all interconnected computers; (2) the World Wide Web (WWW), consisting only of nodes accessible via a URL interface; and (3) a cyber 'archipelago', comprising all other computer systems that exist in theoretical exclusion [i.e. not connected to the Internet or the web]" (Kello, 2013, p. 17 cited in Nnam, *et al*., 2019, p. 380). Nnam and his colleagues added that cyberspace is likened to ICT, comprising the Internet and other sophisticated computer-assisted communications. Although some of the ICTs and/or Internet facilities are tangible and installed in the social-cum-physical space or environment, the vast majority of them are not. Nonetheless, they are mainly utilised or made super-functional in the cyberspace to aid human activities, whether pro-social or anti-social (Nnam, *et al*., 2019).

3.1.2 Theories of Cyber Criminology and Cybercrime

At present, only one theory specifically on cyber criminology/cybercrime exists in the criminology literature. This theory is known as Space Transition Theory, suggesting the urgency and necessity to develop more theories or apply existing crime and victimisation theories either in their individual form or by deconstruction (integration) in explaining the prevalence of cybercrime in society. Nnam, *et al*. (2019) argued that theory integration is both a practical way of expanding the narrow horizons on theoretical

knowledge about cyber criminology and a means of setting the pace for (additional) theory building and theory deconstruction for thorough understanding of the nuances of cyberterrorism and other cybercrimes.

Space Transition Theory (Karuppannan Jaishankar, 2007)

Cyber criminology is relatively a new area of specialisation in the broad field of criminology. As a result, specific theories on cyber criminology and cybercrime is grossly lacking; as earlier indicated, only one theory exists to provide a direct and specific framework for cyber-criminological thoughts and theorising. According to Jaishankar (2007, 2008), since criminologists have started viewing the emergence of cyberspace as a new locus of criminal activity, a new theory is needed to explain why cybercrimes occurs. Spurred by this, Karuppannan Jaishankar propounded Space Transition Theory (STT) in 2007 to account for the new crime trend (Jaishankar, 2008). Below are basic assumptions of STT:

1. Persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position;
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime;
3. Criminal behaviour of offenders in cyberspace is likely to be imported to physical space which, in physical space, may be exported to cyberspace as well;
4. Intermittent ventures of offenders in the cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escape;
5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space. (b) Associates of physical space are likely to unite to commit crime in cyberspace;
6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society; and
7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes (Jaishankar, 2007, p. 7).

The theory of space transition explains the fast growing crime-switch among cybercriminals in both cyberspace and physical space that is linked to the Internet. The crime commission is also simplified and expedited by globalisation, which Stibli (2010) claimed that is linked to sophisticated technologies such as computerisation, miniaturisation, digitalisation, satellite communication, fibre optic and the Internet.

Linking these to crime, Federal Bureau of Investigation (FBI) asserted that the co-ordinated attacks by various terrorist organisations across the globe is connected to high-technology that encourages the proliferation of ICT which is now used by terrorists for destruction of lives and property and to cause public panic (FBI, 1999 cited in Manu, 2017). To illustrate the point further, Nnam, *et al*. (2019, p. 387) stated that:

> A case in point is the obvious social transitions, processes that occur in the cyberspace, wherein terrorists acquire criminogenic knowledge about crime of terror to improve upon and prolong their violent extremism with ease and success. And this is facilitated by the highlighted innovations in ICT and other transition space-based technologies, where several different terrorist groups experience interchange of ideas, intelligence, skills, and logistics. The cyber is a suitable space for crime-switch, shifting from the intended purposes—for advancement in information and communication technology—to the use of same for unintended objectives, such as to facilitate and co-ordinate terrorist activities.

Because theories of cyber criminology and cybercrime are hard to come by, researchers are beginning to integrate conventional victimology, sociology and criminology theorists, constructs, variables, perspectives and paradigms to explain the various classifications and forms of cybercrime. For instance, Ndubueze (2017b) fused Ankers' (1985) social learning and Cohen and Felson's (1979) routine activities theories with space transition theory of Jaishankar (2008) to address the contexts, concerns and directions of cyber criminology and cybercrime. Nnam, *et al*. (2019) systematically deconstructed such theories as routine activities (Cohen & Felson, 1979), social learning, rational choice (Clark & Cornish, 1986), and crime pattern (Brantingham & Brantingham, 1993) to establish a nexus between cyberspace and Boko Haram terrorism in Nigeria. Others integrated fraud triangle and routine activities theories to examine online advance fee fraud (Nwokeoma, Ndubueze, & Igbo, 2017). Thus, incorporating these conventional criminological/victimological/sociological theories into cyber criminology is an attempt to bridge the gap in both empirical and theoretical knowledge in the new subfield (Nnam, *et al*., 2019). Hence, some of these theories are reviewed below, noting their basic assumptions and unique application to the study of cybercrimes and cybercriminals.

Rational Choice Theory (Cesare Beccaria, 1739–1794)

The origin of rational choice theory can be traced to the classical school of criminology developed by an Italian social thinker, Cesare Beccaria, whose utilitarian approach strongly influenced the criminal justice system and was widely accepted throughout Europe and United States (Roshier, 1989; Siegel, 2008). The theory became powerful for more than 100 years before its popularity began to decline by the end of the 19th century, following the development of new theories that could best explain emergence of several different and more complex social problems. Interestingly, beginning in the 1960s, criminologists once again began to embrace classical approach to crime. That is, it has enjoyed resurgent popularity, as a number of criminologists have used it to explain the rising crime wave in modern society (Siegel, 2007, 2008).

Central to the predictions of rational theory is the notion that the perpetration of cybercrimes is a thought-out plan and action. Criminals of all types, including cybercriminals, voluntarily decide and choose whether or not to commit a particular crime (such as cyber-terrorism, hacking, piracy, cyber fraud, and so on) based on calculative, rational and conscientious weighing of the cost and benefits of each of the alternative choices of action (see Otu, 2003, 2010). Robinson, Marchment and Gill (2019) opined that the rational choice perspective on offending in volume crimes (like cybercrimes) is long established, with research consistently demonstrating that offenders are rational actors. Criminals (including, for instance, 'Yahoo-Yahoo Boys') make evaluations and judgments about a given situation that informed their decision to commit a crime ('Yahoo-Yahoo') at a given point in time. Decision-making is strongly influenced by the situational factors encountered in the immediate environment at the point of crime, as well as a consideration of past experiences and existing behaviour repertoires (Cornish & Clarke, 2008; Felson & Boba, 2010; Robinson, *et al*., 2019).

Yahoo-Yahoo [YY] is a popular cybercrime common among young male population in Nigeria. It involves the use of computers and phones connected to Internet facilities to manipulate and falsify information and data belonging to another with the motive and intent to defraud them. Most victims of Yahoo-Yahoo are people living outside Nigeria. Men are usually offenders, while women are often victims of this fast growing cybercrime. On the other hand, 'Yahoo-Yahoo Boys' [YYB] (also known as 'G-Boys') simply refers to or describes people, mainly boys or male population, who perpetrate Yahoo-Yahoo crimes. News making the rounds and confessional statements extracted from arrested YYB by the police and during mob actions are that the perpetration of or perfection in YY crimes is facilitated by applying magical and diabolical

powers and means. The term 'Yahoo-Yahoo' was coined in relation to the medium (e.g. yahoo email or Gmail) through which the crime is mainly committed. Lazarus & Okolorie (2019) agreed that *yahoo yahoo* originated from the fact that the use of Yahoo e-mails and Yahoo instant messenger was a dominant medium of communication between perpetrators and victims.

Still relating its basic tenets to the study of cybercrimes, rational choice theory maintains that some people take to cybercrimes such as cyberterrorism after considering certain factors, such as the need to pursue revolutionary, economic, political and religious goals. Other rational factors include how well a target and crime location are protected, and the efficiency and strengths of law enforcement agents. In other words, the cyberspace is transitional and anonymity, with vast and *difficulty-to-patrol* borders. Now, the 'rational cybercriminal' evaluates the cost-benefit before deciding to embark on any chosen cybercrime. The assessment includes risk of apprehension, seriousness of the expected punishment, the potential value of the act and target, and offender's immediate gratifications. Siegel (2008, p. 73) corroborated the assertion that terrorism (for instance), be it cyberterrorism or conventional terrorism, is the outcome of careful thought and planning, a rational act. Terrorists embark on suicide missions or decide to attack targets "after considering both personal—money, revenge, thrills, entertainment—and situational factors, such as target availability, security measures, and police presence".

The underlying principles of rational choice theory stress that offenders always pattern and structure their criminal activities and also take precautionary measures before, during and after carrying out their operations. This is done to conceal their identity, confuse law enforcement personnel, and easily target and gain access to their victims. The implication, however, is that situational factors such as perceived level of (capably) guardianship at a (potential) site may act as a control mechanism to discourage crime, terrorism (Brantingham & Brantingham, 2008). It has been argued that threats of terrorism "will be avoided if the potential targets are carefully guarded, if the means to commit crime are controlled, if potential offenders are carefully monitored, and if opportunities for crime are reduced" (Siegel & McCormick, 2006, p. 135). This particular idea now links the discussion to routine activities theory.

Routine Activities Theory (Lawrence Cohen and Marcus Felson, 1979)

Routine Activities Theory (RAT) was advanced by Lawrence Cohen and Marcus Felson in 1979. To some extent, routine activities theory is a

development and subdivision of rational choice theory. The central tenet of this theory is that three variables or elements connect and/or disconnect to either encourage or discourage the occurrence of cybercrime. These variables are motivated offender (cybercriminal) who encountered a suitable target (information, data, images, pictures, or human being) in a time and location (the Internet, cyberspace) where there is no capable guardian or guardianship (unsecured computers without strong antivirus, susceptible and/or greedy computer users, unsuspecting victims, etc). This victimisation patterns are in accordance with the position of Felson (1998) who argued that, for a personal or property crime to occur, there must be at the same time and place a perpetrator, a victim and/or an object of property.

What seems to be a balanced explanation and summary of routine activities theory has been offered by Burke (2019, p. 72): Crime is bound to occur "if there are other persons or circumstances in the locality that encourage it to happen but, on the other hand, the offence can be prevented if the potential victim or another person is present who can take action to deter it". The theory is suitable for understanding cybercrimes of Advanced Fee Fraud (AFF), cyberterrorism, identity theft, among others. Nonetheless, some researchers established that the principles of routine activities theory are not generally applied to all forms of cybercrime; its assumptions are more relevant to some cybercrimes than the other (see Leukfeldt & Yar, 2016 cited in Ndubueze, 2017b).

RAT presents a clear explanation of crimes that are more precipitated by lifestyle-routine activities of people in some depth than crimes not linked to people's lifestyles exposure. For instance, people who reveal much of their identifying information or expose their itineraries (routine activities) on Facebook, Twitter, YouTube, WhatsApp, and other social media platforms stand the high risk of cyberfraud and attacks. Likewise, young girls who dress indecently on social media are more prone to sexual abuse and violence than those who dress decently. Rational activities theory underscored "the importance of physical proximity to motivated offenders, exposure to high risk environments, target attractiveness, and absence of guardianship as necessary conditions for predatory crimes" (Meier & Miethe, 1993, p. 475 cited in Etuk & Nnam, 2018, p. 4).

Particularly, RAT provides a simple and direct insight into advanced fee fraud in that it usually occurs under false pretence using online transactions. In Nigeria, AFF is popularly known as 419, a name derived from the Section of the Nigerian Criminal Code that captures the crime. Victims of this crime are deceived, manipulated, blackmailed or forced to make advance payment for goods and services that do not actually

exist in the real world. The evolution of information and communication technology has its own latent, unintended function. There are changes in routine activities of people such as school, work, business and social interactions, which are much more facilitated with the Internet. This has also increased their vulnerability as suitable targets of crime and fraud in the cyberspace. Unlike the physical environment, cyberspace where most cybercrimes take place is a location that most time lacks capable guardianship partly because it almost always contains anonymous information/data and partly because Internet users are somewhat a hidden population with their dealings transitory and clandestine.

The basic assumption of routine activities also applies to the analysis of cyber terorrism. The borders in the cyber is weak and unsecured and, on this note, human daily activities taken place in the virtual environment lack capable guardians (effective policing) to provide adequate protection of information and Internet users. The motivated offenders, terrorists and their sponsors, are regularly manipulated the web to obtain digital information and clues that could help them to successfully commit the crime of terror. The modus operandi of some organised criminal groups are found on the Internet. The acts of kidnapping, armed robbery and terrorism are sometimes researched online and afterwards translate into use in the physical environment. Ajayi (2012) and Shola (2015) acknowledged that there are connections between terrorist groups which facilitate activities between Boko Haram in Nigeria and Al-Qaeda in the Maghreb, Hezbolla in Lebanon, Al-Shabab in Somalia, and the Islamic State of Iraq and Syria.

Social Learning Theory [Differential Association Theory] (Edwin H Sutherland, 1939)

Differential Association Theory (DAT) as a spinoff of social learning theory was developed by Edwin Sutherland in 1939. Owing to certain limitations observed in the early phase of DAT, a revision was made in the theory in 1947 to explain that anti-social behaviour is bound to occur when people acquire sufficient information and knowledge in favour of law violation to outweigh their association with prosocial conducts. For a better understanding, Sutherland summarised the underlying principles of his theory as follows:

1. Criminal Behaviour is learned and not inherited.
2. Criminal behaviour is learned in interaction with other persons in a process of communication.
3. That the principal part of the learning of criminal behaviour occurs within intimate personal groups (negatively meaning that impersonal agencies of communication such as movies,

newspaper play a relatively unimportant part in the genesis of criminal behaviour).

4. That learning includes (i) Techniques of committing the crime, which sometimes is very complicated, and at other times very simple, (ii) The specific direction of the motives, drives rationalisation and attitudes.
5. The specific direction of motives is learned from the definitions of the legal code as favourable or unfavourable. In some societies, an individual is either surrounded by persons who invariably define the legal codes as rule to be observed or by person whose definitions are favourable to the violation of the legal codes. The modern societies are characterised by both mixtures.
6. A person becomes criminal because of an excess of definitions favourable to law violation over definitions unfavourable to law violation. This is certainly the crux of differential association theory. When persons become criminal, they do so because of contacts with criminal patterns and also because of isolation from anti-criminal patterns.
7. Differential association may vary in frequency, duration, priority and intensity. Priority is assumed here to be important in the sense that the lawful behaviour developed in early childhood may persist throughout life while delinquent behaviour developed in the same vein may persist.
8. The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all the mechanisms that are involved in any other learning. This negatively implies that learning of criminal behaviour is not restricted to the process of imitation.
9. While criminal behaviour is an expression of general needs and values, these general needs and values do not explain it since non-criminal behaviour is an expression of the same needs and values. Thieves generally steal to obtain money and likewise honest labourers who work in order to secure money (Sutherland & Cressey, 1974, pp. 75-76)

From the assumptions of DAT, it can be argued that virtually all cybercrimes are learned the same or similar ways noncriminal tendencies are learnt. Sutherland applied the theory to the study of white-collar crime (otherwise known as crime of the powerful), which in modern times has strong ties with computer applications and Internet facilities. Currently, perpetrators of white-crime are using computers connected to the Internet to accomplish their criminal enterprise by learning the techniques and how to conceal traces. At the same time, people are beginning to leverage the Internet and carry out traditional crimes such as trafficking in illicit drugs and illegal sex trafficking.

Criminal networks exist with online black markets where trade occurs and criminals are able to take on specialised roles (National Security Council, n. d.). Even such interpersonal offending behaviours as bullying and stalking which were hitherto committed outside the cyberspace are now learnt and perpetrated using electronic media and the Internet.

The above reviewed theories are, by no means, exhaustive. Depending on the type or form of cybercrime and topic under investigation, these and/or other relevant theories of crime and victimisation can be used as analytical framework. Examples include situational crime prevention theory, frustration aggression theory, low self-control theory, general strain theory, among others.

3.1.3 Classification of Cybercrime

Another problematic area or aspect of cybercrime lies in its classification. Notwithstanding, acceptable frameworks for the categorisation of cybercrime have been provided by acknowledged experts. For instance, Brenner (2001) advanced four legal-based classifications:

1. Prohibited conduct (*actusreus*);
2. Culpable mental state (*mens rea*);
3. Attendant circumstance; and
4. Forbidden result or harm

The above categorisation, though too legalistic, is acceptable. But Nasi, Oksanen, Keipi and Rasanen's (2013) two-level cybercrime taxonomy appears more criminological, and they include institutional and individual levels. The institutional level, which consists of large-scale cyber-attacks that target governments, institutions and multinational corporations, is often carried out by hackers or cyber terrorists. The individual level refers to victimisation by known offenders or where the victims is particularly targeted. Related to this is the three grouping earlier put forward by Smith, Grabosky and Urbas (2004):

1. Offence that involves the use of digital technologies in its commission;
2. Targeted at computing and communication technologies; and
3. Incidental to the commission of other offences.

Above all, a frequently and widely quoted categorisation of cybercrime across disciplines is linked to Wall (2001):

1. Cyber-trespass (unauthorised crossing of online boundaries);

2. Cyber-deception or theft (fraudulent or illegal acquisition of information or resources online);
3. Cyber-pornography/obscenity (displaying of obscene or sexually expressive content online); and
4. Cyber-violence (dissemination of harmful content online).

3.1.4 The Nigerian Cybercrime Act 2015

There was no specific law on cybercrime prior to 2015. The increasing incidents of cybercrime led to the establishment of 'The Cybercrimes Act 2015' in Nigeria; the first legislation that deals specifically and directly with cybercrimes and cybersecurity. The Act was signed into law on the 15 May 2015, specifying the legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and other related offences. According to Okoh and Chukwueke (2016), The Act charges the offices of the National Security Advisor (NSA) and the Attorney-General of the Federation (AGF) with co-ordinating its enforcement and creates the multi-agency Cybercrime Advisory Council (the Council) and the National Cyber Security Fund (the Fund) to be overseen by the NSA.

Also, the Act guarantees the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programmes, and intellectual property and privacy rights. The Cybercrimes Act 2015 comprises 59 Sections, 8 Parts, and 2 Schedules, with 32 offences and penalties contained in Part III. Below are some of the offences and penalties that are prescribed for perpetrators of cybercrimes:

Part III Section 5 (Offence against any Critical National Information Infrastructure) stipulates that:

(1) Any person who with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to Section 3 of this Act, shall be liable on conviction to imprisonment for a term of not more than 10 years without an option of fine.

(2) Where the offence committed under Subsection (1) of this Section results in grievous bodily harm to any person, the offender shall be liable on conviction to imprisonment for a term of not more than 15 years without option of fine.

(3) Where the offence committed under Subsection (1) of this Section results in the death of person(s), the offender shall be liable on conviction to life imprisonment.

For clarity of purpose, "critical infrastructure means systems and assets which are so vital to the country that the destruction of such systems and asset would have an impact on the security, national economic security, national public health and safety of the country" (The Nigerian Cybercrimes Act, 2015, p. 38)

Part III Section 23 (Child Pornography and Related Offences) Stipulates that:

Any person who intentionally uses any computer system or network in or for:

(a) Producing child pornography;
(b) Offering or making available child pornography;
(c) Distributing or transmitting child pornography;
(d) Procuring child pornography for oneself or for another person; and
(e) Possessing child pornography in a computer system or on a computer-data storage medium: Commits an offence under this Act and shall be liable on conviction —

(i) In the case of paragraphs (a), (b) and (c), to imprisonment for a term of 10 years or a fine of not more than N20, 000,000.00 or to both fine and imprisonment; and
(ii) In the case of paragraphs (d) and (e) of this Subsection, to imprisonment for a term of not more than five years or a fine of not more than N10,000,000.00 or to both such fine and imprisonment.

(1) Any person who knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution shall be guilty of an offence and upon conviction shall be sentenced to One year imprisonment or a fine of Two Hundred and Fifty Thousand Naira or both.
(2) Any person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of:

(a) Engaging in sexual activities with the child;
(b) Engaging in sexual activities with the child where —

(i) Use is made of coercion, inducement, force or threats;

(ii) Abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or

(iii) Abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;

(c) Recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes; commits an offence under this Act and shall be liable on conviction —

(i) In the case of paragraphs (a), to imprisonment for a term of not more than 10 years and a fine of not more than N15,000,000.00; and

(ii) In the case of paragraphs(b) and(c) of this Subsection, to imprisonment for a term of not more than 15 years and a fine of not more than N25,000,000:00.

(3) For the purpose of Subsection (1) above, the term 'child pornography' shall include pornographic material that visually depicts —

(a) A minor engaged in sexually explicit conduct;

(b) A person appearing to be a minor engaged in sexually explicit conduct; and

(c) Realistic images representing a minor engaged in sexually explicit conduct.

(4) For the purpose of this Section, the term 'child' or 'minor' means a person below 18 years of age.

Part III Section 24 (Cyberstalking) Stipulates that:

(1) Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that —

(a) Is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) He knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent: Commits an offence under this Act and shall be liable on conviction to a fine of not more than N7, 000,000.00 or imprisonment for a term of not more than three years or to both such fine and imprisonment.

(2) Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network —

(a) To bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person;

(b) Containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; or

(c) Containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse theaddressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value: Commits an offence under this Act and shall be liable on conviction —

(i) In the case of paragraphs (a) and (b) of this Subsection, to imprisonment for a term of 10 years and/or a minimum fine of N25,000,000.00; and

(ii) In the case of paragraph (c) and (d) of this Subsection, to imprisonment for a term of five years and/or a minimum fine of N15, 000,000.00.

(3) A court sentencing or otherwise dealing with a person convicted of an offence under Subsections (1) and (2) may also make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which —

(a) Amounts to harassment; or

(b) Will cause fear of violence, death or bodily harm; prohibit the defendant from doing anything described/specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this Section, commits an offence and shall be liable on conviction to a fine of not more than N10,000,000.00 or imprisonment for a term of not more than three years or to both such fine and imprisonment.

(5) The order made under Subsection (3) of this Section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

(6) Notwithstanding the powers of the court under Subsections (3) and (5), the court may make an interim order for the protection of victim(s) from further exposure to the alleged offences.

Part III Section 25 (Cybersquatting) Stipulates that:

(1) Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the Internet or any other computer network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and shall be liable on conviction to imprisonment for a term of not more than two years or a fine of not more than N5,000,000.00 or to both fine and imprisonment.

(2) In awarding any penalty against an offender under this section, a court shall have regard to the following —

(a) A refusal by the offender to relinquish, upon formal request by the rightful owner of the name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria; or

(b) An attempt by the offender to obtain compensation in any form for the release to the rightful owner for use of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government of Nigeria.

(c) In addition to the penalty specified under this Section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

Part III Section 30 (Manipulation of Automated Teller Machine (ATM)/Point of Sales (POS) Terminals) Stipulates that:

(1) Any person who manipulates an ATM machines or POS terminals with the intention to defraud shall be guilty of an offence and upon conviction sentenced to five years imprisonment or N5, 000,000.00 fine or both.

(2) Any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using an ATM or Point of Sales device, shall be guilty of an offence and upon conviction sentenced to Seven years imprisonment without an option of fine.

3.2 Types/Forms of Cybercrime

The central focus of cybercrime and cybercriminals is both on material (data, networks, websites, or systems) and human (human beings or their reputations) resources, which makes the act a serious crime to watch. There are various forms of cybercrime. But, for the purpose of this course, only three broad types of cybercrime, with numerous subtypes, are discussed. And they are cyber theft, cyber vandalism, and cyberterrorism.

3.2.1 Cyber Theft

Cyber theft as a type/form of cybercrime is facilitated by computer networks. Cyber thieves use the cyberspace to distribute illegal goods and services for economic gain and to initiate and facilitate traditional crimes. Identity theft, computer fraud, denial of service attack, distribution of illegal sexual material, and e-tailing fraud are common forms of cyber theft.

Identity Theft

Identity theft is the appropriation of someone else's identity to commit theft or fraud (Sovern, 2004). The Canadian Internet Policy and Policy Interest Clinic (CIPPIC) broadly defined online identity theft as "the combination of unauthorised collection and fraudulent use of activities, including collection of personal information, creation of false identity documents, and fraudulent use of the personal information through electronic devices" (CIPPIC, 2007 cited in Abdullahi & Saleh, 2017).

Another working definition presents identity theft as:

> The assumption of another person's financial identity through the use of the victim's identifying information. This information includes a person's name, address, date of birth, social security number, credit card numbers, and checking account information. With this information, a thief is capable of charging merchandise to the victim's account and changing the billing address for the account so that the unauthorised purchase remain undetected (Elbirt, 2005 cited in Abdullahi & Saleh, 2017, p. 244).

Cyber theft is an unlawful use of the Internet to obtain a person's information with the aim of manipulating the victim's bank account

details and/or impersonate the victim to obtain a new credit card or bank statement of account for financial transactions there from. Identity thieves can steal someone's identity by hacking into their emails, computers, mobile phones, and school or workplace database. They may call the victim under the pretext of bankers who are on routine activity or check with their customer or send Short Message System/Service (SMS) requesting for certain personal data. To illustrate the operational techniques of identity theft, Ebenezer (2014) established that perpetrators create websites that seems to be legitimate but, in reality, are sham designed to defraud or obtain information that can be used to commit further economic crimes.

Computer Fraud

Any fraud scheme which involves the use of one or more components of the Internet to present fraudulent information to victims so as to conduct fraudulent transactions and obtain illegal benefit is computer fraud (Bello, 2017). To execute such a crime, this author further stated, very less expertise or (professional) knowledge is required, and is not an uncommon form of theft executed by certain employees of any organisation or company by hanging the data before making entries or even making false entries. A detailed and characteristic-like definition of computer fraud has been offered by the United States (US) Computer Fraud and Abuse Act of 1986; specifically 18 USC Section 1030(a)(1) addressed the problem as:

> Having knowingly accessed a computer without authorisation or exceeding authorised access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to the Executive Order or Statute to require protection against unauthorised disclosure for reasons of national defence or foreign relations, or any restricted data, as defined in paragraph Y. of Section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

Below are some examples of computer fraud (theft of information or hacking, Salimi Slice, Software Theft, Manipulation of Accounts or Banking Systems, and Corporate Espionage):

1. Theft of Information (hacking): The cybercrime of hacking refers to an unauthorised access to systems, networks, and data, which may be committed solely to gain access to a target or to gain and/or maintain such access beyond authorisation (UNODC, 2019). It is an unlawful act of obtaining information and data from a computer, such as software that is copied for profit. Moffit, Pannatia, Prosenbeck, Scott and Siverson (2012) defined hacking as the unauthorised access into or interference in a computer system or any access in order to corrupt, alert, stall or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft, and loss of electronic data message or electronic document.

   Research shows that hackers could also seek unauthorised access to systems to cause damage or other harm to the target. In 2014, for instance, Lauri Love, a British hacker, defaced websites, gained unauthorised access to United States' Government systems, and stole sensitive information from these systems (Parkin, 2017). In a similar development, hackers gained unauthorised access to the system of a Lithuanian plastic surgeon and obtained sensitive information about patients from different parts of the world, procedures they undertook, naked photos of the patients, medical data, among other forms of information. The cybercriminals then threatened each patient with the release of this information if the ransom was not paid. The amount of the ransom varied based on the quantity and quality of information about the patient that was stolen (Hern, 2017);

2. The 'Salami Slice': This is a situation where fraudsters carefully skims small amount of money from the balances of a large number of accounts in order to bypass internal controls and escape detection and arrest. Valacich and Schneider (2010) explained that Salami Slice involves stealing small amount of money from a large number of financial accounts. Adegoke and Aderoju (2017) mentioned the act of deducting small amount of funds from several (bank) accounts in the hope that such an insignificant amount would be unnoticed as the commonest example of Salami Slice;

3. Software Theft: This represents a comparative case of making copies of computer software which leads to a huge illegal market, depriving authors of significant revenues (e.g. includes lecturers or students duplicating the intellectual property (books, articles, etc) of another without due referencing or acknowledgement for economic and intellectual gains). Adegoke and Aderoju (2017, p. 308) called software theft software piracy and described it as "the use of or duplication of an intellectual or creative work of an author without permission or compensation (including referencing work) to the author. For them, "it is an act of infringement on the ownership rights and, if anyone is caught, he or she may be sued civilly for damages, be criminally prosecuted, or both";
4. Manipulation of Accounts/Banking Systems: This is similar to salami slice; however, the fraud is committed on a much larger and usually more complex scale. This sometimes, goes with cybercrimes of carding and phishing/spoofing. Valacich and Schneider (2010) described carding as the stealing of credit card information for one's own use or to sell it, while Adegoke and Aderoju (2017) stated is a fraudulent process of or attempt to obtain sensitive information, such as usernames, passwords, and credit cards. Another perspective of manipulation of account/banking systems is 'Shoulder Surfing' or Piggy Backing', which Adegoke and Aderoju (2017) described as an act looking over a person's shoulder while he or she is using an Automatic Teller Machine (ATM), a cell phone or other devices in order to steal or gain access to their information; and
5. Corporate Espionage: Here, some members of staff in a formal organisation/country pry into and steal trade secrets of their competitors in another firm/country. The aim is to outsmart one's competitor(s) so as to take the lead in the highly competitive and complex global marketplace.

Denial of Service Attack

First and foremost, it is necessary to note that Denial of Service Attack (DoS attack) is a typical example or representation of 'system interference'. Article 5 of the Council of Europe Cybercrime Convention also prohibits system interference, which is defined as the "intentional…serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (UNODC, 2019). A DoS attack is also proscribed under Article 29(1)(d) of the African Union Convention on Cyber Security and Personal Data Protection of 2014 (UNODC, 2019). The attack is usually severe because it "interferes with systems by overwhelming servers and/or intermediaries

(such as routers) with requests to prevent legitimate traffic from accessing a site and/or using a system" (Maras, 2016, p. 270).

Denial of service attack occurs when someone exerts undue pressure and influence on legitimate internet users and consequently threaten to prevent them from accessing the service. This could be an empty threat but is usually presented in such a manner that would frightened network consumers to pay extortion (the demanded sum of money), thinking that they paid to the rightful network provider or agency. Imagine a student who has been surfing the web to make sure he/she obtains relevant materials to complete his/her Continuous Assessment and Research Project facing denial of service attack. Failure to pay will attract continuous interception and interference by the attackers until the internet user (student) becomes frustrated and either exits the site or forced to pay the demanded amount of money.

Akin to DoS attack is Distributed Denial of Service Attack (DDoS attack)—"the use of multiple computers and other digital technologies to conduct co-ordinated attacks with the intention of overwhelming servers and/or intermediaries to prevent legitimate users' access" (Maras, 2016, pp. 270-271). The workings of a single form of DDoS attack is typified thus, according to CloudFlare (2018) and UNODC (2019), imagine many computers trying to connect to a single computer (the server) all at the same time. The single computer has a limited amount of processing power and network bandwidth. Also cited from these sources is the illustration: If too many computers try to connect at the same time, the server cannot respond to each connection quickly enough. The result is that the server may not be able to respond to *real* users because it is too busy with *fake* requests (CloudFlare, 2018).

These attacks (i.e. DDoS attacks) may be carried out "by an individual, group, or State; States can target critical infrastructure that are considered indispensable to the functioning of society. For example, Country A experienced a series of DDoS attacks perpetrated by Country B on its financial sector. As a result of these cyberattacks, citizens of Country A were unable to access online banking, and ATMs within this country were intermittently working" (UNODC, 2019, p. 22). "DDoS attacks are made possible by utilising digital devices that have been infected with malicious software (or *malware*) to enable the remote control of these devices and use them to launch cyberattacks" (p. 22).

Illegal Copyright Infringement

Illegal copyright infringement, otherwise known as warez, explains a situation whereby organised groups illegally acquire software, crack/rip (alter) its copyright protection and then post or upload it on the Internet

for members to access and use as well as sell to other users. In most cases, members of the warez community (illegal copyright infringers) make the illegitimate, pirated products available online before the legitimate commodity is introduced into the market. A good example of illegal copyright infringement is file sharing—programme that gives Internet users access to download music and other copyright materials illegally which results in nonpayment of royalties to the originators or owners. Digital piracy is an aspect of illegal copyright infringement. According to Madaki and Sarki (2017, p. 290), "although pirates' use different ways of committing and promoting piracy through the exploitation of certain devices and machines, software, videogames, books, photos, and periodicals tend to be common in many countries of the world, including Nigeria".

Distribution of Illegal Sexual Material

The globalisation trend is felt much on information and communication technology. Consequently, there is increasing distribution of illicit sexual contents, among which, pornography is taking the lead. The number of visits to sites displaying materials of an erotic nature speaks volumes about how revolution in ICT has facilitated the proliferation of porn industries for commercial purposes. Visitors to pornographic websites are first, given open access (free) to smaller sites that feature sexual materials, and later, lured into large firms with assorted nude photos, videos and live sexual entertainments, where they are tricked to pay high subscription service charge before they could be allowed access.

E-tailing Fraud

This involves the use of the Internet for both illegal buying and selling of goods and services. E-tailing fraud thrives in the eBay, that is, online auction sites or Internet sites for auction sales. It has assumed different dimensions, such as replacement of fairly used or cheaper merchandise purchased over the Net for higher quality purchases by someone—it could be a seller sending or buyer returning such goods. Imagine a situation whereby a student purchased a high quality and expensive HP laptop on eBay and received a similar-looking but inexpensive and lesser-valued product of the same model and brand. E-tailing fraud can be outright failure by a seller to supply to a buyer on promised items bought online.

3.2.2 Cyber Vandalism

Cyber vandalism is a type of cybercrime that is characterised by malicious intent to or outright damage of someone's property and/or reputation; cyber vandals are motivated more by malice than greed. They target computers and networks (1) to avenge on perceived injustices, (2) to prove to the world how susceptible, porous, anonymous and transient computer security systems can be, (3) to demonstrate their special expertise, experience and supremacy; and (4) the belief that information and programmes in the cyber space should be made available and free for people to access (see also Siegel, 2008). Cyber vandalism takes different forms, and these are: Logic bomb, spam, virus, web defacement, worm, cyber stalking, cyber bullying, cyber spying, and cyber espionage. Below are some highlights of the different forms of cyber vandalism as presented by Maras (2014, 2016) and supported by UNODC (2019):

1. **Worm:** Standalone malicious software that spreads without the need for user activity;
2. **Virus:** Malware that requires user activity to spread (e.g. an executable file with virus spreads when opened by the user);
3. **Trojan horse:** Malware designed to look like legitimate software in order to trick the user into downloading the programme, which infects the users' system to spy, steal and/or cause harm;
4. **Spyware:** Malware designed to surreptitiously monitor infected systems, and collect and relay information back to the creator and/or user of the spyware.
5. **Ransomware**: Malware designed to take users' system, files, and/or data hostage and relinquish control back to the user only after ransom is paid;
6. **Cryptoransomware:** Cryptoransomware (a form of ransomware) is malware that infects a user's digital device, encrypts the user's documents, and threatens to delete files and data if the victim does not pay the ransom;
7. **Doxware:** This is a form cryptoransomware that perpetrators use against victims that releases the user's data (i.e., makes it public) if ransom is not paid to decrypt the files and data;
8. **Cyber-stalking:** The use of information and communication technology (ICT) to commit a series of acts over a period of time designed to harass, annoy, attack, threaten, frighten, and/or verbally abuse an individual;
9. **Cyber-harassment:** The use of ICT to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse an individual (or individuals); and

10. **Cyber-bullying:** The use of ICT by children to annoy, humiliate, insult, offend, harass, alarm, stalk, abuse or otherwise attack another child or other children.

3.2.3 Cyber-terrorism

The term, 'cyber-terrorism,' received its coinage in 1982 from Barry Collin, who described the act as transcendence from the physical to the virtual realm and the intersection and the convergence of these worlds (see Lewis, (n. d.); Tafoya, 2011; Nnam, *et al*., 2019). Cyber-terrorism is a violent act that is commonly politically motivated, committed against population through the use of or facilitated by computer technology (National Crime Prevention Council, 2011). The act is conceived as the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information (Tafoya, 2011).

According to the Centre for Strategic and International Studies (CSIS), cyberterrorism is the use of computer network tools to shut down critical national infrastructure (such as transportation, energy, and government operations) or to coerce or intimidate a government or civilian population (Lewis, n. d.). This suggests that a cyberterrorist is someone who threatens, coerces or even intimidate a governmental organisation in order to promote and advance his or her own personal political and social objectives by launching computer based attacks which are aimed at the vital information stored in the computer and network (Bello, 2017).

There is a paradigm shift in the Modus Operandi (MOs) of terrorists across the globe. Virtually all the terrorist groups exploit the vulnerabilities of cyberspace, computers and networks to recruit members, source for funds, receive and spread information, and acquire weapons. As earlier stated, for instance, the 2012 UNODC report reveals that information and communication technology is one of the strategic factors driving the increasing use of the Internet by terrorist organisations and their supporters for a wide range of purposes: Recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes (UNODC, 2012). The speed, transient, convenience and anonymity of the cyberspace facilitate the spread ofterrorism. Unlike the physical or traditional terrorism, cyberterrorism is more

effective and easy in terms of perpetration. It poses less risk and lead; trace can be erased or destroyed within a twinkle of an eye.

3.3 Trends in Cybercrime

There is no one globally acceptable measure to calculate or determine the trends and patterns of cybercrime. This is partly because the validity and reliability of the indices used to ascertain cybercrime trends is relative: It varies from organisation to organisation, time to time, and depends on a country or an agency's cybersecurity investigation tools, culture and legal framework. Cyber theft, cyber vandalism, cyber terrorism, ransomware, and several different forms of cyber-enabled and cyber-dependent criminal behaviour have been described as cybercrime trends due to their pervasiveness and harm caused. However, rapid and sophisticated innovations in ICT and other space-based technologies will make identification of cybercrime trends simple, easy and possible. For instance, as the Europol's 2017 Internet Organised Crime Threat Assessment (EIOCTA) revealed that "law enforcement and security measures impact cybercrime and the tactics, tools and targets of cybercriminals, (so) these measures influence and impact future cybercrime trends.

In 2017, EIOCTA identified and classified ransomware as cybercrime trend, and was supported by TrendMicro in 2018. Ransomware is a virus or malicious programme design to infect computer systems, causing the data within the programmes and/or networks to be unavailable and inaccessible to legitimate Internet owners or users until they pay extortion, ransom to the cybercriminal. There is a direction of interest and modifications in the MOs of violators of this particular cybercrime; their targets now go beyond individuals to include private and public establishments (e.g. hospitals, schools, financial institutions, and the like), with 'ransom' demanded and received.

The Internet Crime Complaint Centre (ICCC), in collaboration with the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre (ANWCCC), revealed that Nigeria is now ranked third on the list of top ten sources of cybercrime in the world, with 8% behind the United States [US] (65%) and the United Kingdom [UK] (9.9%). Nigeria ranked third in four consecutive years: 2006, 2007, 2008 and 2009 as a country where cybercrime goes on uncontrolled in the world. Currently, the country ranked first in the perpetration of cyber-dependent and cyber-enabled crimes in West Africa.

SELF-ASSESSMENT EXERCISE (SAE) 1

Kidnapping is a 'physical space crime', but it can be facilitated in the cyberspace using the Internet. Discuss.

3.4 Effects of Cybercrime

Cybercrime poses many challenges for individuals, groups, organisations, and national and international governments. The social, psychological, political and economic lives of these populations are adversely affected by all forms of cybercrime. At all levels, cybercrime involves financial loss and waste of other resources, both material and human. It can lead to (1) destruction of lives through cyberterrorism and (2) loss of important documents and manipulation of personal and national database or repositories through cyber vandalism and cyber theft. The Symantec report of 2012 revealed that more than 1.5 million people fall victim to some sort of cybercrime every day. This ranges from password theft to extensive monetary swindles, with an average loss of $197 per victim; this is in addition to more than $110 billion dollars lost to cybercrime across the globe annually.

Cybercrime goes beyond loss of personal property to include 'cybermurder;' any cybercrime, particularly cyberterrorism, which results in fatality or has fatal impact. A typical example of cybermurder is the hacking into a Liverpool hospital in 1994 by a British hacker who changed the medical prescription that has been made by the nurse to the patient (Samuel, Osman, Al-Khasawneh, & Duhaim, 2014). In the US, a case of cybermurder has also been recorded. Frank and Odunayo (2013) made reference to the commission of this crime in 2006 when an underworld don was admitted in hospital to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse and this led to the death of the patient (see also Ibrahim & Mukhtar, 2017).

Even Nigeria is not immune to cybermurder as Boko Haram terrorists and their sympathisers are using the Internet to pose threats and violence on both security personnel and civilians. The Movement for the Emancipation of Niger Delta (MEND) also used the Internet to advance its violent movement (Ibrahim & Mukhtar, 2017). Beyond the use of the Internet to perpetrate physical-world terrorism, the authors further observed, is the tendency of organised cyberterrorists to use cyberspace as a tool for threatening information, people and organisations. Similarly, the Analytical Support and Sanctions Monitoring Team (ASSMT) submitted the report of the United Nations on Boko Haram terrorism in Nigeria. In the report, smuggling, extortion, remittances,

kidnapping, and charitable donations were major means through which this terror group receive funds (Abdulkareem, 2018).

Because of the vulnerabilities of computer systems, programmes and Internet connectivity, many banks, businesses, agencies and institutions, both private and public-owned, spend heavily to safeguard the cyberspace of their business. This is evidenced by the obvious increasing rate on budget allocation to security and defence across societies and institutions in recent times. The aim is to protect their Internet facilities and other ICT networks from cyber-attacks and cybercriminals.

3.5 Prevention and Control of Cybercrime

Owing to the pervasive influence of cybercrime and the challenge it presents for law enforcement agencies, many jurisdictions are intensifying actions to curtail the phenomenon. Indeed, laws are increasingly enacted both at the national level and in the international climes to drive policy and action. The international criminal justice system, particularly such international law enforcement agencies as Interpol, has entered into several treaties, bilateral agreements and partnerships between and among countries of the world. Even at the continental and regional levels, organisations such as the African Union, Organisation of American States and Europol are known for the provision of tips for cybersecurity.

For instance, the Council of Europe Convention on Cybercrime (CECC) is described as the most important international framework for combating cybercrime. The Council in 2001 provided a-three-path solution to cybercrime: (1) the reduction of frictions among national legislations, (2) the introduction of new investigative powers, and (3) the facilitation of international co-operation. As at September 2016, 52 countries had ratified, accessed or signed this legal instrument.

Other preventive and control measures are rooted in the 2002 Commonwealth Model Law on Computer and Computer-related Crime (CMLCCC) and the African Union Convention on Cyber Security and Personal Data Protection (AUCCSPDP) established in June 2014. In order to properly and effectively address the problem of cybercrimes, China, Kazakhstan, the Kyrgyz Republic, Russia, Tajikistan and Uzbekistan have formed a synergy with one another to build a robust anti-cybercrime agency called Shanghai Co-operation Organisation (SCO). What is more, Malaysia and China signed a Memorandum of Understanding (MoU) in August 2012 to combat trans-border crimes, with focus on cybercrime. This idea was informed by the dire need to go into a joint cybersecurity co-operation for a practical outcome. That is,

to achieve a successful war on crime by involving syndicates within and outside the two countries with regional and global networks.
In a bid to curtail the increasing rate of cybercrime and insecurity in the cyberspace, the government of Nigeria established the Nigerian Cybercrime Working Group (NCW) in 2004. This comprised representatives from government agencies and private sectors, and the aim was to develop legal framework on cybercrime and cybersecurity. The NCW was reinforced in 2007 through the establishment of the Directorate for Cyber Security (DCS), charged with responding to security issues regarding the rising usage of the Internet and other ICT in Nigeria. Besides, there exists extant laws and general rules which lent support to the above agencies/initiatives, though they were not specifically and directly linked to cybercrime. Examples of these laws include (1) The Nigeria Criminal Code (1990), (2) Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and (3) the Advance Fee Fraud and other Related Offences Act 2006. Generally, these laws and/or Acts were enforced to prevent and control crimes and criminality, including cybercrimes.

Despite the above prevailing legislations and punishment thereof, Nigeria is still experiencing ever-increasing rate of cybercrime, with no significant arrest and prosecution made. This was partly because of lack of specific legal framework on the offence and offenders and partly because of lack of cybercrime and forensic investigative resources, both human and material. The persistent problem then called for a strong and practical legislation to direct policy approach for a better result in the fight against cybercrimes. In response to this, a bill was put forward by the Nigerian government in September 2008 and was signed and passed into law in May 2015, hence 'The Nigerian Cybercrime (Prohibition, Prevention, Etc) Act 2015'. Under part III (see Offences and Penalties) Section 8, for instance, the Act prescribed the following punishment for cyber-terrorism offenders:

1. Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.
2. For the purpose of this Section, 'terrorism' shall have the same meaning under the Terrorism (Prevention) Act 2011 (As Amended).

3.5.1 The Nigerian Cybercrime Act 2015 and Cybercrime Prevention and Control

The Nigerian Cybercrime Act 2015 charged financial institutions and service providers with the duties and responsibilities of taking proactive measures aimed at preventing and controlling cybercrimes. These are contained in Part IV of the Act as highlighted by Okoh and Chukwueke (2016):

- Section 37(1) places a duty to verify the identity of customers carrying out electronic financial transactions, requiring the customers to present documents bearing their names, addresses and other relevant information before issuing ATMs, credit or debit cards, and other related electronic devices. Failure to do so attracts a fine upon conviction;
- Section 38 requires service providers to keep all traffic data and subscription for a period of at least two years. Further, service providers are required to turn over such information to law enforcement agencies and failure to comply with either attracts a fine of N7, 000000:000;
- Section 39 requires service providers, upon a court order, to assist competent authorities with the collection or recording of content and/or traffic data associated with specified communications. Under Section 40, they are required to provide assistance to law enforcement agencies in identifying offenders, tracing proceeds of offences and the cancellation of services used to commit offences; and
- Section 21 creates a responsibility to report to the National Computer Emergency Response Team (CERT) any attacks, intrusions or other disruptions liable to hinder the functioning of another system or network. The section further empowers CERT to propose isolation of affected systems and networks. Additionally, failure to report any such incident within seven days is an offence rendering the offender liable to be denied internet services and a mandatory fine.

3.5.2 The Nigeria Police and Cybercrime Prevention and Control

Although other police Departments can assist in the fight against cybercrime, personnel in the Criminal Investigation Department (CID) have been foremost respondents and investigators of this crime. This Department houses many Units or Sections, such as Administration: D1; Exhibits: D2; General Investigation: D3; Homicide: D4; Anti-Fraud Section: D5; among others. In all, only the D5 is singled out for

discussion based on its direct connection to combating cybercrimes and related matters.

D5: Anti-Fraud Section: Its Administrative/Investigative Procedures

As the name implies, the Anti-Fraud Section handles cases of fraud and fraud-related matters. If under the State Command, for instance, the Officer In-Charge (O/C) receives complaints through petitions, which the Commission of Police (CP) must minute to the Deputy Commission of Police (DCP) in-charge of Criminal Intelligence and Investigations Department (CIID), who would in turn minute to the O/C D5 for investigations.

Administrative/Investigative Procedures I: A Case of Fraud Involving the Use of Bank Transactions

When a petition is received against someone, the procedure taken is to write to the Branch Manager of the name/affected bankwhere the suspect and complainant are banking, with a Court Order (stamped and signed by a Magistrate or Judge) mandating the bank to submit to the police within a specified time the suspect's details: (i) Statement of Account (ii) Account Creation Detail File (iii) Bank Verification Number (BVN) (iv) Post No Debit (PND) on the account and (v) an order to arrest any person that may come to the bank to make transaction with the account. When these pieces of information are sent to the police, investigation will commence in earnest. The statement of account will reveal all the transactions that has been taken place with the named account. The account creation detail will enable the police to have access to the account holder's personal data. The BVN will help to unravel other accounts linked to the named account number.

In a case of fraud committed using Automated Teller Machine (ATM), the police will request for the statement of account and a record of the webcam obtained from the ATM Central Storage. The portion of the record to be requested will depend largely on the statement of account, which reveals when and how the transaction was made. The webcam will help to reveal the identity ofthe person who made the withdrawal by displaying the face of the suspect in the video record. With this information at hand, the suspect is then invited for interview and/or interrogation, as the case may be.

A Case of Fraud Suspects who Jumped Police Bail in Ebonyi State Police Command and ran to Owerri in Imo State

In this case, a Police Investigation Activities (PIA) will be issued to D5 Section to go in search of the suspect in his/her residence in Imo State. PIA is used to write to a State Police Command in another State where a

person to be arrested is currently residing. That is, it is used in interstate police investigation and arrests, different from the jurisdiction of the Command writing the letter. The appointed detectives at the Ebonyi State Criminal Investigation Department (SCID) will book and leave for Imo State Police Command Headquarters, Owerri. On arrival, they are expected to report to the CP and state their purpose with the PIA, which include the passport photographs of the detectives showing originality. In some cases, the receiving CP may signal/radio Nigeria Police Headquarters, Ebonyi State Command (NPHESC). Thereafter, he will direct the Divisional Police Officer (DPO), Owerri Urban Police Division and Area Commander to provide them (the detectives from PHESC) with necessary support and logistics that will lead to the arrest of the suspect and assist in his/her deportation to Ebonyi.

If a complaint is received orally, not documented in PIA (which is very rare), it must be recorded by the Charge Room Officer (CRO) on duty into a crime diary. It is from this crime diary (Form A1) that an Investigating Police Officer (IPO) makes his/her extract from. When investigating a case, any action taken must be written down, starting from the inside front cover of the case file to the inside back cover of the case file. Where there is no other space to write, a plain sheet may be used to continue recording the actions taken by the IPO. PIA is different from Police Invitation Letter (PIL), which is a letter written to a government official or a respectable person in society through his office or community head to release a named person to appear at a stated Police Station for interview.

3.6 Obstacle to the Prevention and Control of Cybercrime

Cybercrime poses serious challenges to the traditional criminal justice system, particularly law enforcement and legal subsystems. Some of these challenges overlap with those encounters by forensic investigators, prosecutors and presiding officers in assessing forensic evidence. These obstacles include, but by no means, exhaustive:

1. The growing trends in ICT frustrate the efforts made by personnel in the criminal justice and forensic technicians to combat cybercrime. This is because, unlike the physical space, the cyberspace is not only complex and operates on a highly accelerated pace, but also has features that are quite strange to the conventional criminal justice administrators. Most of them are not trained and certified computer, digital forensic analysts, so and this constitutes a major impediment to cybercrime prevention and control.
2. The Internet and other information and communication technologies are rapidly evolving and ever-present; a development that has given rise to an upsurge in the intensity,

seriousness and prevalence of cybercrime activities. Because of the ubiquity of Internet connectivity, perpetrators can commit the crime at their own convenient time and location with minimal risk of detection and apprehension.

3. The Internet borders are not clearly delineated and, as a result, are prone to attacks. It moves at a rapid pace and often keeps users anonymous and consequently provides a thriving criminogenic and victimogenic environments for cybercrime and cybervictimisation to beat security personnel and network.
4. Most information and data that are linked to cybercrime are digitalised or digital-based, thereby making them impermanent and easily altered or deleted to pervert the course of investigation and justice.
5. Cybercrimes occur more in the cyberspace than in the physical world. Many incidents often take place in different locations that may fall under the jurisdiction of different States. This situation could lead to investigation error and clashes in criminal justice system procedurals.

SELF-ASSESSMENT EXERCISE

i. Cyber theft covers other forms of cybercrime, such as:
   a. Denial of service attack
   b. Distribution of illegal sexual material
   c. Options a and b
   d. None of the above

ii. Which country is ranked first in the perpetration of cybercrime in West Africa?
   a. Mali
   b. Ghana
   c. Nigeria
   d. Gambia

iii. In 2012, ---------- and --------- signed a Memorandum of Understanding (MoU) to combat trans-border cybercrime.
   a. United States and Nigeria
   b. United Kingdom and United States
   c. China and Nigeria
   d. None of the above

Iv Below are examples of computer fraud:
   a. Corporate espionage
   b. Identity theft
   c. Cyber terrorism
   d. Denial of service attack

v. In which year was the term ‘cyber terrorism’ coined?

a. 1991
b. 1981
c. 1992
d. 1982

vi In 2001, the Council of Europe Convention on Cybercrime provides a3-path solution to cybercrime:
a. The reduction of frictions among national legislations
b. The introduction of new investigative power
c. The facilitation of international co-operation
d. All of the above

Vii Hacking simply means ----------
a. Manipulation
b. Theft of information
c. Cyber vandalism
d. Piracy

Viii In 2012, ------- report reveals that more than 1.5 million people fall victim to some sort of cybercrime every day.
a. The UNODC
b. The Symantec
c. The Europol
d. The African Charter

ix In which year was the Union Convention on Cyber Security and i Personal Data Protection established?
a. June 2014
b. July 2014
c. August 2014
d. September 2014

x -------- is a country with the highest rate of cybercrime in the world.
a. Nigeria
b. United Kingdom
c. United States
d. South Africa

4.0 CONCLUSION

In this Unit, the term ‘cybercrime’ has been conceptualised with different meanings and definitions provided for broad-based understanding and application. Various forms of cybercrime were elucidated and its trends, effects and prevention and control discussed in some depth. A brief review of national and international legislations on cybercrime and cybersecurity was also conducted.

5.0 SUMMARY

This Unit revealed the nature and extent of cybercrime. It was traced to be a global problem, with harmful effects on both national and international governments—be it developed or developing. It was realised that proper understanding of cybercrime can lead to its effective prevention and control through bilateral treaties, international cybersecurity collaboration, and national legislations.

6.0 TUTOR-MARKED ASSIGNMENT

1. With relevant examples, delineate between cyber-enabled crime and cyber-dependable crime.
2. Why did the Nigerian Cybercrime Working Group and Directorate of Cyber Security failed to curtail cybercrime.
3. How could cybercrime be effectively prevented and controlled?

7.0 REFERENCE/FURTHER READING

Abdulkareem, H. (2018, July 30). How Boko Haram is funded – UN. *ThisDay*, p 51.

Abdullahi, A. & Saleh, M. (2017). Online identity theft in Nigeria: Risk factors and control. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 241-250). Zaria: Ahmadu Bello University Press.

Adegoke, N. & Aderoju, M. A. (2017). Cyber crime and technology misuse in Nigeria: Trends, issues and challenges. In Iwarimie-Jaja, D., & Agwanwo, D. E. (Eds.), *Contemporary criminality in Nigeria: Challenges and options* (pp. 301-319). Ibadan: Stirling-Horden Publishers.

Alemika, E. E. O. (2017). Foreword. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. ix-x). Zaria: Ahmadu Bello University Press.

Behr, I. V., Reding, A.; Edwards, C. & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. Santa Monica, CA: RAND Corporation.

Beirne, P. & Messerschmidt, J. W. (2015). *Criminology: A sociological approach* (6th ed.). New York: Oxford University Press.

Bello, K. (2017). Information community technology and cybercrime. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 169-184). Zaria: Ahmadu Bello University Press.

Brantingham, P. L. & Brantingham, P. J. (1993). *Environment, routine, and situation: Towards a pattern theory of crime*. New York: Crime Prevention Studies.

Brantingham, P. & Brantingham, P. (2008). Crime pattern theory. In R. Wortley, & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 78-93). Willan: Portland.

Burke, R. H. (2019). *An introduction to criminological theories* (5th ed.). New York: Routledge.

Chavan, A. & Ahire, S. (2015). Perspectives of cybercrime with prevention, detection, and prosecution. *International Journal of Scientific Engineering and Technology Research, 4*(18), 3391-3396.

Clark, R. B. & Cornish, D. B. (1986). *The reasoning criminal: Rational choice perspective in offending*. New York: Springer-Verlag.

CloudFlare. (2018). *What is a DDoS attack*? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Accessed 10 January 2020.

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Cornish, D. B. & Clarke, R. V. (2008). The rational choice perspective. In R. Wortley, & L.Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 21-47). Willan: Portland.

Ebenezer, A. J. (2014). Cyber fraud, global trade and youth crime burden: Nigerian experience. *Afro Asian Journal of Social Sciences, 5*(4)1-13.

Etuk, G. R. & Nnam, M. U. (2018). Predictors and risk factors of armed robbery victimisation in Nigeria: An integrated theoretical perspective. *European Scientific Journal, 14*(29),1-15.

Europol. (2018). *The internet organised crime threat assessment* 2018. Retrieved from https://www.europol.europa.eu/activities-

services/main-reports/internet-organised- crime-threat-assessment-iocta-2018. Accessed 2 February 2020.

Giddens, A. & Sutton, P. W. (2013). *Sociology* (7th ed.). Hoboken, NJ: John Wiley & Sons.

Felson, M. (1998). *Crime and everyday life* (2nd ed.). Thousand Oaks, CA: Pine Forge.

Felson, M. & Boba, R. (2010). *Crime and everyday life* (4th ed.). Thousand Oaks, CA: Sage.

Frank, I. & Odunayo, E. (2013). Approach to cyber-security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science, Engineering and Education*. Retrieved from http://ijcrsee.com/index.php/ijcrsee/ article/ view/ 11/114. Accessed 10 December 2019.

Goodman, M. D. & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Gordon, S. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*,*2*(1), 13-20. DOI: 10.1007/s11416-006-0015-z.

Hern, A. (2017, May 31). Hackers publish private photos from cosmetic surgery clinic. *Guardian*. Retrieved from https://www.theguardian.com/technology/2017/may/31/ hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments. Retrieved from 10 January 2020.

Holt, T. J.; Bossler, A. M. & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensic* (2nd). Routledge.

Ibrahim, B. & Mukhtar, J. I. (2017). Emerging cyber-terrorism threats in Nigeria. In P.N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 415-428). Zaria: Ahmadu Bello University Press.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology*, *1*(2), 7-9.

Jaishankar, K. (2008). Space transition theory of cybercrimes. In Schmallager, F. & Pittaro, M. (Eds.), *Crimes of the internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (Ed.). (2017). *Cyber criminology: Exploring Internet crimes and criminal behaviour*. CRC Press.

Lazarus, S. & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40*, 14-26.

Lewis, L. (n. d.). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Retrieved from http://csis.org/files/media/csis/pubs/021101risks_of_cyberterror.pdf. Accessed 10 February 2020.

Madaki. M. & Sarki, U. U. (2017). Digital piracy and active internet users in Nigeria. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 287-296). Zaria: Ahmadu Bello University Press.

Manu, Y. A. (2017). Globalisation, cyber-terrorism and Nigeria's national security. In P.N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 395-411). Zaria: Ahmadu Bello University Press.

Maras, M. (2014). *Computer forensics: Cybercriminals, laws, and evidence*. Retrieved from https://www.unodc.org/e4j/data/_university_uni_/computer_forensic__criminals_laws_and_evidence.html? Accessed 4 February 2020.

Maras, M. (2016). *Cybercriminology*. Oxford: Oxford University Press.

Moffit, T.; Pannatia, C.; Prosenbeck, B.; Scott, E. & Siverson, D. (2012). *The HRE online experience – technology misuse and cyber crime*. Retrieved from https://sites.google.com.site/tommoffittportfolio/the-hre-online-experience/ technology-misuse-and-cyber-crime. Accessed 10 November, 2013.

Nasi, M.; Oksanen, A.; Keipi, A.; & Rasanen, P. (2013). Cybercrime victimisation among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210.

National Crime Prevention Council. (2011). *Cybercrimes*. Retrieved from www.ncpc.otg. Accessed 22 January 2020.

National Security Council. (n.d.). *Transnational organised crime: A growing threat to* national and international security. Retrieved from http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat. Accessed 26 April 2020.

Ndubueze, P. N. (2017a). Cyber criminology: Contexts, concerns and directions. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 1-28). Zaria: Ahmadu Bello University Press.

Ndubueze, P. N. (2017b) (Ed.). *Cyber criminology and technology-assisted crime control: A reader*. Zaria: Ahmadu Bello University Press.

Nnam, M. U.; Ajah, B. O.; Arua, C. C.; Okechukwu, G. & Okorie, C. O. (2019). The war must be sustained: An integrated theoretical perspective of the cyberspace-boko haram terrorism nexus in Nigeria. *International Journal of Cyber Criminology*, 13(2), 379-395.

Norden, S. (2013). How the internet has changed the face of crime (M. Sc. Dissertation). Florida Gulf Coast University, Florida, United States.

Nwokeoma, B. N.; Ndubueze, P. N. & Igbo, E. U. M. (2017). Precursor of online advance fee fraud in south east Nigeria. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 195-218). Zaria: Ahmadu Bello University Press.

Okoh, J. & Chukwueke, E. D. (2016). *The Nigerian cybercrime act 2015 and its implications for financial institutions and service providers*. Retrieved from https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its implications-for-financial-institutions-and-service-providers#.XqaZEBIod_k.Accessed 27 April 2020.

Olumoye, M. Y. (2013). Cyber crime and technology misuse: Overview, impact and preventive measures. *European Journal of Computer Science and Information, 1*(3), 10-20.

Osayi, K. K. (2017). Cyber-stalking, cyber-bulling and cyber-squatting: A conceptual analysis. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 29-46). Zaria: Ahmadu Bello University Press.

Otu, S. E. (2003). Armed robbery in the southeastern states of contemporary Nigeria: A criminological analysis. A Doctoral Thesis Submitted to the Department of Criminology, University of South Africa, Pretoria, South Africa.

Otu, S. E. (2010). Decision-Making practices in armed robbery among armed robbers in Nigeria. *International Journal of Research in Arts and Social Sciences, 2*, 371- 391.

Parkin, S. (2017, September 8). *Keyboard warrior: The British hacker fighting for his life*. Retrieved from https://www.theguardian.com.news/2017/sep/08/lauri-love-british-hacker-anonymous-extradiction.us. Accessed 10 January 2020.

Robinson, A., Marchment, Z. & Gill, P. (2019). Domestic extremist criminal damage events: Behaving like criminals or extremists. *Security Journal, 32*, 153-167.

Roshier, B. (1989). *Controlling crime*. Chicago: Lyceum Books.

Samuel, K. O.; Osman, W. S.; Al-Khasawneh, Y. & Duhaim, S. (2014). Cyber terrorism attack of the contemporary information technology age: Issues, consequences and panacea. *International Journal of Computer Science and Mobile Computing, 3*(5), 1082-1090.

Siegel, L. J. & McCormick, C. (2006). *Criminology in Canada: Theories, patterns, and typologies* (3rd ed.). Toronto, ON: Thompson, Nelson.

Siegel, L. J. (2007). *Criminology: Theories, patterns, and typologies* (9th ed.). Belmont, California: Thomas Higher Education.

Siegel, L. J. (2008). *Criminology: The core* (3rd ed.). Belmont, CA: Thomson Higher Education.

Sharma, V. (2015). Information technology and cyber crime. *Journal of Institution of Information Technology and Management, 1*(1), 75-78.

Smith, R., Grabosky, P. & Urbas, G. (2004). *Cybercriminals on trial*. Cambridge: Cambridge University Press.

Sovern, J. (2004). Stopping identity theft. *The Journal of Consumer Affairs, 38*(2), 233- 242.

Stibli, E. (2010). Terrorism in the context of globalisation. *AARMS, 9*(1), 1-7.

Sutherland, E. H. & Cressey, R. D. (1974). *Criminology*. (9th ed.). Philadelphia: J.B.: Lippincott.

Tafoya, W. L. (2011). Cyber terror. *FBI Law Enforcement Bulletin* (FBI.gov), November. Retrieved from https://leb.fbi.gov/articles/featured-articles/cyber-terror. Accessed 10 February 2020.

The Nigerian Cybercrimes Act 2015. (2015).*Cybercrimes (prohibition, prevention, etc) Act, 2015*. Retrieved from https://www.the+cybercrimes+%28prohibition%2C+ prevention%2C+etc%29+act+2015. Accessed 26 April 2020.

United Nations Office on Drugs and Crime. (2013). *(Draft) Comprehensive Study on Cybercrime*. Retrieved from https://www.unodc.org/documents/organised-crime/unodc_ccpcj-eg.4_2013/cybercrime_study_210213.pdf. Accessed 20 February 2020.

United Nations Office on Drugs and Crime. (2017). *The drug problem and organised crime, illicit financial flows, corruption and terrorism* (Part 5). Vienna: The Author.

United Nations Office on Drugs and Crime. (2019). *E4J university module series: Cybercrime*. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/basics-of-computing.html. Accessed 20 December, 2019.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Wilson, C. (2008). *Botnet, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for progress*.

Wilson, S. M. & Peterson, L. C. (2002). The anthropology of online communication. *Annual Review Anthropology, 31*, 449-467. DOI: 10.1146/annurev.anthro.31.040402.085436.

Valacich, J. & Schneider, C. (2010). *Information systems today – managing in the digital world* (4th ed.). New Jersey: Pearson.

MODULE 2

Unit 1 Introduction and General Background to Forensic Science/Investigation.
Unit 2 Scope of Forensic Science.
Unit 3 Roles of forensic Investigation and Evidence in Criminal Justice administration.
Unit 4 Basic Features of Cybersecurity Strategies.
Unit 5 Challenges of Forensic Investigation and Prosecution of Cybercrimes.

CONTENTS

1.0 INTRODUCTION

A way of understanding any subject is to know its meaning, definition and historical background. To understand forensic investigation and its components, we must define what it is and the definition should be in such a way as to make meaning clear to all.

2.0 OBJECTIVES

By the end of the Unit, you should be able to:

- explain the meaning of forensics and its etymology, as well as scope or branches;
- explain the meaning and types of digital evidence and forensic investigation;
- describe the basic knowledge in cybersecurity for a better analysis of the challenges facing forensic investigation and prosecution of cybercrime.

3.0 MAIN CONTENT

3.1 Definition and Origin of Forensic Science/Investigation

Etymologically, the term 'forensic' originates from the Latin word 'forensis', meaning 'public or pertaining to a forum'. Although a number of people erroneously believe that 'Criminalistics and Forensic Science' refers to a single course, discipline or subject, they are actually two separate areas of specialisation in the broad field of criminology. Simply put, forensics or forensic science is the application of science and technology for the purpose of criminal detection, investigation, litigation and sentencing. It is the application of scientific and technological procedures to law enforcement, legal and penological issues. Saferstein (2007, pp. 4-5) defined "forensic science as the application of science to law; it is the application of science to the criminal and civil laws that are enforced by police agencies in the criminal justice system"—police, courts, and prisons.

On the other hand, criminalistics is a branch or sub-field of forensic science under the discipline of criminology and security studies. The former prepares readers, learners, or students for the latter. Criminalistics is a foundation, preparatory course for grappling with the broad and complex subject matter of forensic science with ease. Critical to Criminalists is the identification, collection, collation, processing, examination, interpretation, and preservation of physical evidence pertaining to crime for the purpose of establishing victim-offender relationships. It helps to determine the motivation for crime commission, identifies victims and their offenders, and facilitates

unbiased judgment. However, the two disciplines are subsumed under forensic criminology and have remained inseparable as they complement each other in forensic investigation.

The art and science of forensic investigation is traced to ancient cultures and civilisations. In the circa 3000 BC, for instance, the ancient Egypt had already established a cultural and religious practice of mummification. Before the human body is mummified (embalmed), local forensic procedures are adopted in the removal and examination of human internal organs. History has it that postmortem study was carried out on Julius Caesar after he was stabbed to death in about 44 BC. The ancient Chinese also played important role in the development of forensic science. For instance, the first forensic study of human finger and palm prints is traced to Chinese civilisation of 650 AD. Nonetheless, forensic methods of investigating crime and criminals is said to have begun in 1883, when Alphonse Bertillon developed forensic investigative approaches called 'Portrait Parle' and 'anthropometry'—a scientific technique of recognising criminals by recording and analysing their physical characteristics and measurements. This was followed by the invention of fingerprints by Francis Galton (1833 – 1911) to assist in criminal investigation and legal proceedings.

Forensic investigation refers to the practices and methods of scientific enquiries into the aetiology and epidemiology of natural and social phenomena. The import is that forensic investigation is not limited to cybercrime (computer, digital, or electronic) forensic investigation. It cuts across different subject areas, such as medicine and paramedics, natural and physical sciences, social and behavioural sciences, management and actuarial sciences, engineering and technology, arts and humanities, and law. Nevertheless, of particular interest to end-users of this Course Material is forensic criminology which covers the certain courses in the broad field of Criminology and Security Studies Programme in Nigeria. These are: criminalistics, forensic science, criminal investigation, forensic science management, cybercrime and forensic investigation, forensic psychology, and so on. It is important to note that, in most cases, forensic criminological investigation requires the input of other disciplines to conduct a successful investigation with acceptable outcomes. Some of these include forensic medicine, biology, biochemistry, anatomy, chemistry, physics, geology, anthropology, psychology, sociology, geophysics, soil science, toxicology, and geophysics.

SELF-ASSESSMENT EXERCISE (SAE) 2

Give a comparative analysis of forensic science/investigation in ancient and modern cultures.

3.2 Scope/Units/Branches of Forensic Science/Investigation

Forensic science/investigation is encompassing; as earlier indicated, it is not limited to cybercrime or computer forensic science or investigation, but rather covers many subjects. Examples include forensic computer (digital or cyber forensic), forensic biology, forensic pathology, forensic anthropology, forensic odontology, forensic entomology, forensic toxicology, forensic psychology, forensic sociology, and forensic criminology. Discussions on these areas are necessary since they make significant contributions in the investigation of cybercrime.

3.2.1 Computer Forensic/Cyber/Digital Forensic

Computer forensic, otherwise known as cyber or digital forensic, refers to the analysis of information and data (evidence) either found in or generated with computers and technology-driven devices. Subsumed under digital forensic are scanner forensic, database forensic, network forensic, PDA (Personal Digital Assistant) forensic, disk forensic, multimedia forensic, mobile device forensic, printer forensic, and digital music device forensic. Generally, all this assists in cybercrime investigations by identifying, processing, retrieving, analysing, interpreting, presenting, and preserving digital evidence to direct investigation and justice. Through the use of digital information stored in or created with computer, cyber forensic experts can trace a suspect to a victim, offender and crime scene. Computer forensics is a specialised discipline that integrates legal knowledge with basic assumptions of computer science. Here, the methods of data collection and analyses go beyond the techniques apply in conventional policing, research by individuals, groups or institution to include specialised and widespread proficiency in the field of computer science and forensics.

Suffice it to say that gone are the days when computers were owned by a select few in society. At present, there is no formal organisation, not even security agency that does not make use of computers and the Internet. Sooner or later, whether in the developed or developing countries, every professional will be Information Communication Technology (ICT) compliant. We are currently in the Internet, cyber, or World Wide Web (WWW) age—a crucial stage in human advancement which Saferstein (2007) described as the ‘information superhighway’—is a medium for people to communicate and access millions of information from computers located anywhere on the globe. For him, no subject or profession remains untouched by the Internet; it brings together forensic scientists from all parts of the world, linking them into one common electronic community.

Based on this background information, computer criminalistics or computer forensic in is conceived as the application of information and data stored in or generated with computer in solving crime problem in society. The process begins from the crime scene, reaching crime laboratories and ends in the courtroom or correctional institutions. It is the methodical identification, collection, collation, analysis, interpretation and preservation of computer data for the purpose of legal consideration and adoption. With the results of computer analyses of both digital and physical evidence samples, victims and their offenders can be identify, balanced legal argument made, right decision taken and objective conclusion reached on a cybercriminal suit.

Many cybercrimes are committed using computers and Internet facilities. Not only that cybercrime and other Internet-based frauds are currently on the increase, such conventional crimes as kidnapping, murder, human trafficking, arson, armed robbery, drug trafficking, and terrorism are also becoming more complex and difficult to unravel. Indeed, countless conventional crime perpetrators carry out their offending behaviour with high criminogenic skills and artifice. They mutilate, alter or completely destroy crime scene and evidence to avoid detection and consequent apprehension. As a result, investigators are now searching and researching both cyber and physical environments for evidence and traces left by suspects of cybercrimes. Put in another way, conclusive evidential data can be obtained in a computer used in perpetrating, researching and rehearsing crime, as well as physical evidence samples (such as voiceprints, photographs, documents, prints, etc) can be analysed using computers.

Using homicide, arson and burglary as his reference point, Saferstein (2007) illustrated the uses of computer in forensic investigation: Criminal investigators frequently encounter computers and other digital devices in most cases. As homicide investigators sift for clues, they may enquire whether the method for a murder (cyberterrorism, cyberstalking, yahoo-yahoo, cyberattacks, etc) were researched on the Internet; whether signs of an extramarital affair can be found in email or remnants of instant messages, which might provide motive for a spouse killing or murder for hire (assassination); or whether threats were communicated to the victim prior to the murder by an obsessed stalker. Arson investigators would want to know whether financial records on a computer might provide a motive in an arson-for-profit-hire (Saferstein, 2007).

A burglary investigator would be certainly guided and assisted if law enforcement agents determined that the proceeds from a theft were being sold online, perhaps through the eBay or a similar online auction site (Saferstein, 2007). Included in the array of computer application to

forensic investigation, for instance, is that kidnapping and armed robbery investigators may check whether a victim or any of his relatives had recent reasonable financial transactions, especially if the bank notification (alert) of such transactions reflected on his computer or mobile phone. In a case of murder, a team of homicide investigators may investigate mobile phone numbers of the deceased and suspects/accused for digital examination.

3.2.2 Forensic Biology

Biology, in its narrowest and simplest definition, is the scientific study of living things. It is the scientific laws that control the life of living organisms, such as plants, human and animal. The biology of crime is conducted by certified biologists and biochemists. These professionals in the biological science unit of forensic science/criminalistics are responsible for the identification of such physical evidence samples as dried bloodstains and other body fluids found on computers or objects used in committing or omitting cybercrimes. The samples are collected by forensic biologist/biochemist and then subjected to Deoxyribonucleic acid (DNA) testing together with suspect profiling. The aim is to unravel cause of a particular cybercrime and its perpetrators or identify crime victims. Forensic biologists and biochemists may be called upon to conduct laboratory analyses of hairs and fibres deposited on computer keyboard and/or physical locations where cybercrime was initiated or completed. The results will assist policing institutions in their investigation and possibly facilitate successful prosecution of culprits.

3.2.3 Forensic Pathology

Forensic pathology is located in the medical science unit of forensic science. As a branch of medicine, forensic pathology applies both legal and criminological thoughts to determine the cause of a strange death by conducting a postmortem study/ autopsy. An autopsy or postmortem study is a medical examination which involves the dissection of a corpse to ascertain the real cause of death. Most pathologists are both coroners and medical examiners by virtue of their special training in forensics, criminalistics, or even law. Within this context, deaths are categorised into five: Natural, suicide, homicide, undetermined and accident. This classification is based on existing autopsy reports in forensic criminology literature. A forensic pathologist scientifically examines a corpse by collecting and analysing medical evidence, and then writes and submits admissible autopsy reports in the court of law.

Take for instance, ‘defensive wound’, ‘exit and entry wounds’, and ‘wound patterns’ found on a victim or dead body with gunshot can assist in establishing both the type of weapons used and the force applied in

inflicting the harm. A careful identification, collection and analysis of trace evidence will help to interpret the cause of death or source of injury/wound. From the explanation, how does forensic pathology relate to (cybercrime) cybercrime forensic investigation? Some cybercrimes are committed in a sub-cultural group context. The yahoo-yahoo crime in Nigeria is a case in point. This cybercrime is particularly organised and common among male students of tertiary institutions and young graduates. A conflict or fight may arise among them and, if not properly handled, may result in *kill-and-run*, which autopsy would be required to resolve.

The increasing efforts by policing agencies and public awareness on the workings of yahoo-yahoo has led to a shift in operational procedures, with perpetrators engaging in diabolical rituals in order to succeed in the criminal enterprise. Research findings revealed that a group of cybercriminals called 'yahoo plus' have introduced the use of 'magical and spiritual powers' (yahoo plus) to defraud unsuspecting victims with easy (see Melvin & Ayotunde, 2010; Adejoh, Alabi, Adisa, & Emezie, 2019). Conventional wisdom would reveal that this new approach to cybercrimes involves ritual killings and harvest of human organs to facilitate the crime. With this development, a deceased's relative or coroner's court may demand for or hold an inquest into unexplained demise uncovered by cybercrime investigators. It is forensic pathologists who will carry out the postmortem in partnership with cybercrime forensic investigators to determine the actual cause of death, link the killing to cybercrime, identify the probable perpetrator(s) and aid in the prosecution of the offender(s).

Sometimes, the cause of death may be self-evident, so obvious that it may not necessarily require autopsy. For instance, death resulted from violent crimes could be determined through eyewitness accounts or scientific observation of items related to the attack and interview or interrogations by professionals. Postmortem investigation only becomes necessary when the cause of death cannot be established using these methods. The processes involved in autopsy are complex, rigorous, money and time-consuming, as well as require special training and constant updating of pathologists with state-of-the-art forensics skills. Yet, an autopsy is necessary because the manner in which most deaths occur could be misleading or the crime scene where they occurred altered by the perpetrator(s) in order to divert the attention of investigators and thereby perverting the course of investigation and justice in the long-run. Saferstein (2007) reiterated that the cause of death may not always be what it seems at first glance. For instance, a deceased with a gunshot wound and a gun in his hand (or beside him) may appear to have committed suicide. However, an autopsy may reveal that the victim actually died of asphyxiation (suffocation) and the

gunshot wound occurred after death to cover up the commission of a crime.

With the aid of such electronic imaging as Positron Emission Tomography (PET), Superconducting Interference Device (SQUID), Magnetic Resonance Imaging (MRI), Brain Electrical Activity Mapping (BEAM), among others in the medical science unit of forensics, it has been known in the world of criminal justice system/administration that brain damage or malfunction could results in crime and delinquency. Siegel (2008) presented findings from some brain studies (see Raine, Buchsbaum, & LaCasse, 1997) which point to a particular area of the brain that is directly linked to criminal behaviour, including cybercrime. Using brain scanning techniques, empirical evidence reveals that substance abusers and violent offenders (who also contemplate cybercrimes) have impairment in these brain regions: Medial temporal lobe, superior parietal, prefrontal lobe, angular gyrus, and thalamus. Understanding these malfunctions in human brain may give much needed insights into the complexities of both conventional crimes and cybercrimes.

An attempt to caution a spouse, parent, guardian, sibling, colleague or student whose cybercriminal activities is known may be misinterpreted by the offender and thus finds expression in conflict. This is heightened if the person is into drug culture. Of course, psychoactive substance abuse is a common characteristic of cybercriminals, and illicit drug use has been responsible for impairments in some regions of the brain. Under the influence of drugs, poor cognition, dissonance, quarrel and violence are most likely to occur as an extension of cybercrime at home and school and in the workplace. . Research also shows that people who commit domestic violence have lower metabolism in the right hypothalamus and decreased connections between cortical and subcortical brain structures compared to the control group (George, Rawlings, Williams, Phillips, Fong, Kerich, Momenam, Umhau, & Hommer, 2004). The results of Positron Emission Tomography (PET) examinations carried out on known chronic violent offenders showed decreased cortical blood flow and hypometabolism in the subjects' non-dominant frontal and temporal lobes than the control group (Tancredi, 2005). Serial killers suffer a particular neurological disease named Asperger Disorder (AD), which is a severe brain damage that affects communication, social skills, behaviour and learning (Silva, Leong, & Ferrari, 2004).

On that score, conducting neurological examinations on people to determine their relationships with forensic investigation in relation to cybercrime is important. With forensic and legal medicine, investigators and prosecutors are better informed about the psycho-medical predictors

of cyber and conventional crimes. And marrying the outcomes with existing sociological and criminological causal explanations offers a strong analytical framework for advancing a better preventive and control measures. Forensic pathologists are required to scientifically determine why people indulge in cybercrime and therefore make recommendations to the criminal justice system for therapeutics. Offenders' treatment, correction, rehabilitation, aftercare services, and follow-up interventions are imperative for the management of all criminal cases. With those neurological findings known to police agencies, courts and prisons, processing of criminals and solving crime-problem will be somewhat an easy task. Indeed, neuroscience has complemented the traditional approach to cybercrime studies through forensic investigation.

3.2.4 Forensic Anthropology

Forensic anthropology is concerned with the study of ancient remains, especially human skeleton. This is done to identify decedents and then determined the cause of their death and thus link investigators and prosecutors to the possible murderer(s). Human skeletal remains, particularly the teeth, are the hardest part of the human body, which take scores of years or even centuries before they undergo a significant decomposition. The identification and scientific examination or dating of both the archaeological and anthropological evidence provide clues about the time a particular crime occurred.

Forensic anthropologists assist in cybercrime investigation. Their work appears to be a follow-up of forensic pathological investigation. A dead body that has undergone complete decomposition may give inconclusive result when subjected to autopsy. The services of forensic anthropologists are required under this circumstance to identify the deceased by approximating their age and sex as well as the nature and extent of injuries/wounds sustain during an attack (see forensic pathology section for details). By this means, a forensic or criminalistics anthropologist builds up a useful composite picture of the victim by engaging in crime scene reconstruction. A composite in this context is associated with reconstruction of all the facial features of a crime victim. In other words, a composite sketch or photograph covering pictures of each separate components of the victim's face are put together into one drawing, advertised in the media, and distributed to formal law enforcement agents/agencies for identification of crime victims and/or offenders.

3.2.5 Forensic Odontology

Odontology is the scientific study of the structure, health, growth and development of the teeth. It is a criminalistics/forensic science unit that

contributes to the location of (cyber) crime scene and identification of (cyber) crime victims as it relates to criminal investigation and prosecution. Hence, forensic odontology is the body of scientific knowledge that relates to the examination of the teeth in order to establish the identity of a dead person, especially a victim of crime whose body is found in an unrecognisable state.

The teeth are the most robust, durable parts of human skeletal remains; the last of them all to undergo complete decay, probably after some centuries. With the use of such (existing) dental records as X-rays, dental casts and even a photograph of the person's smile, Saferstein (2007) affirmed, a set of dental remains can be compared to a suspected victim. Another role of forensic odontology in criminal investigation is bite mark analysis. In some assaults or attacks, for instance, offenders leave bite marks on the body of their victims. During criminal investigation, a forensic odontologist is invited to empirically establish a link between the bite marks found on the victim's body and the dental structure of the suspect or accused.

3.2.6 Forensic Toxicology

Forensic toxicology is a branch of forensics or forensic science that deals with the examination of biological physical evidence samples, such as poisonous chemicals, drugs, alcohols and other related psychoactive substances, to ascertain the cause of automobile accident, poisoning, suicide, rape, sexual violent behaviour, and murder for ritual. A toxicology report by a certified forensic toxicologist is usually required to help crime investigators unravel the circumstances surrounding a mysterious death and for successful prosecution of offenders. Forensic toxicological results can reveal how a victim of cybermurder was killed, drugged or lured to fall prey to cybercrime by studying substances linked to the crime.

3.2.7 Forensic Entomology

Entomology is the scientific study of insects, while forensic/criminalistics entomology is the scientific study of insects found on or around a decomposing dead body for the purpose of criminal investigation and prosecution. Forensic entomologists develop keen interest in forensic investigation by paying special attention to murder or suicide, especially a victim whose body is found in the crime scene or dumpsites decomposing. When decomposition sets in after death, insects infect the corpse, eating the flesh and tissues of the deceased to an unrecognisable state. Common among these insects are blow-flies and other flies (e.g. houseflies) that lay eggs on meats or wounds. The maggots produced from the eggs of these flies consume

human remains and thereby making decomposition easier and faster. It is therefore, the duty of an investigating forensic entomologist to collect these dead body-consuming agents and subject them to forensic analysis. This will help to determine the developmental stages (the life cycles and habits) of such agents and the onset of their existence in a corpse. With this, experts can approximate and predict, with high degree of accuracy, the time a homicide or cyber-related homicide takes place and probably unravel the hidden circumstances surrounding the death.

3.2.8 Forensic Psychology

From the American Psychological Association (APA) perspective, forensic psychology is the application of clinical specialities to the legal arena. It involves the application of clinical psychology to the forensic setting; the application of research and experimentation in other areas of psychology such as cognitive psychology and social psychology to the legal field (Ward, 2013). Generally, psychologists believe that crime is a product of defective and abnormal traits developed in early childhood, and that criminals are usually sufferers of one or a combination of problem behaviours and psychological problems such as damaged self-concept and identity, depression, schizophrenia, and mood swings. Siegel (2007) argued that a part or branch of trait theories focuses on the psychological perspective of crime, including the associations between intelligence, personality, learning and criminal behaviour. This view has a long history, and psychologists, psychiatrists and other mental health professionals, have long played an active role in formulating forensic (criminological) theories. The same source further revealed that depression, 'bipolar disorder' (manic depression), and schizophrenia are characterised by extreme impairment of a person's ability to understand reality, think clearly, respond emotionally, communicate effectively, and behave appropriately.

Most perpetrators of cybercrime are more or less obsessed offenders, who nevertheless research and rehearse their criminality on the Internet. Cyberterrorism and child pornography are particularly connected to schizoid personality disorder, as evidenced by the manner in which perpetrators carry out their offending behaviour; they act under an abnormal psychological influence and projections. Since insanity is a legal excuse, the court engages a forensic psychiatrist to ascertain the mental capacity, reasoning and functionality of an accused standing trial in a court of law and then decide whether such a person should be exonerated or given lesser punishment. Saferstein (2007) asserted that forensic psychiatry is a specialised area in which the relationship between human behaviour and legal proceedings is examined. Experts in this aspect of forensic are trained for both civil and criminal litigations. For civil cases, Saferstein further illustrated, forensic psychiatrists

usually determine whether people are competent to make decisions about preparing wills, settling property or refusing medical treatment. For criminal cases, the author added, these experts evaluate the behavioural disorder and determine whether people are competent to stand trial. In fact, forensic psychiatrists examine behavioural patterns of criminals to guide them in the preparation of reliable and objective profiles of offenders in the criminal justice setting.

Forensic psychology involves many tasks in the criminal justice system. These include formal clinical consultations; informal interactions with clients (including criminal defendants) and their relatives; identification, investigation and assessment of cases; and constant psycho-legal research using state-of-the-art facilities. Also included in these tasks are: Provision of expert witness testimony in a court of law, design and implementation of psychotherapeutics, and other psycho-medical treatments to offenders with psychosocial disorder and drug-use problem. People who are likely to fall foul of the law or those whose behaviour ran counter to the legal rules and are being processed through the criminal justice system need the services of forensic psychologists. Although forensic psychologists are exposed to the basics of jurisprudence, an exceptional versatility in clinical skills is paramount and a precondition for practising forensic psychology.

In that regard, psychologists conduct both clinical and forensic examinations of individuals and their behaviour and personality traits, both prosocial and antisocial. They acquire and display requisite skills in interpersonal relations and technical interview and interrogation. This is in additional to their preparation and presentation of report writing during civil and criminal litigations. Dougherty (n. d.) explained that forensic psychologists perform such tasks as threat assessment for schools, child custody evaluations, competent evaluations of criminal defendants, counselling services to victims of crime, death notification procedures, screening and selection of law enforcement applicants, the assessment of Post-Traumatic Stress Disorder (PTSD), and delivery and evaluation of intervention and treatment programmes for juvenile and adult offenders.

Forensic psychology is also referred to as psychology of testimony and criminological psychology due to the fact that experts conduct crime witness, victim and suspect interviews and interrogations as well as provide expert testimony in courts during trial. In the criminal justices system, these roles are domiciled in police psychology and correctional psychology. Gudjonsson and Haward (1998) enumerated other roles of forensic psychologists in relation to criminal investigation to include consulting with attorneys, testifying in courts as expert witnesses, teaching in law schools and conducting research on various justice

related issues such as attitude of judges, eyewitness testimony, crime suspect confessions, police interrogation, police crime investigations, validity of lie-detector tests, death penalty and, above all, jury selection.

3.2.9 Forensic Sociology

Sociology is the mother of all social sciences, one of a number of social sciences which attempts to explain and understand human behaviour in society. Sociologists have studied a vast and diverse range of topics: Poverty, drug use, law, science, war, sports, health, death, colonialism, the body, ethnic conflict, sexuality, music, murder, mobile phones and humour. It is hard to think of any significant area of social life which has never been the subject of a sociological study (Haralambos *et al*., 2008). Traditionally, sociologists explore the causes and spread of crime and delinquency using socio-environmental factors or societal variables such as poverty and social exclusion, gender, neighbourhood conditions, educational attainment, power and authority, socio-economic status and other social and demographic backgrounds. This approach to crime and criminality is what "Adolphe Quetelet and Emile Durkheim referred to as sociological criminology, a perspective in the general field of sociology and an approach to criminology which focuses on the relationship between social factors and crime" (Siegel, 2007, p. 4).

In essence, sociologists align themselves with both sociological criminology and forensic criminology/investigation to explore crime and legal frameworks. As the rate of cybercrime is increasing globally and offenders applying more sophisticated techniques in their criminal enterprise, forensic sociologists strive to combat cybercrime using scientific tools and methods. They now adopt and apply forensic procedures in crime analysis and management as it relates to legal proceedings. A systematic combination of theoretical and practical specialist knowledge of science and law with a view to solving social and legal problems is the guiding compass for forensic sociologists.

Forensic sociologists influence reforms in the criminal justice system, so their professional advice and guidance are needed during a court hearing. Their expertise facilitates unbiased, swift, balanced and timely criminal investigation and prosecution. Forensic sociology qualifies as legal sociology with experts versed in the tradition of crime detection, investigation and paralegal procedurals. No wonder Dougherty (n. d.) defined forensic sociology as the application of theory, research, and practices to the legal, law enforcement, and correctional institutions and their impact through society. It focuses on micro and macro aspects of social forensics and crime patterns, as well as interventions. From this definition, it is established that the role of forensic sociologists in both criminal and civil cases can be seen in their research efforts and analyses

of crime victimisation data. They interpret local laws and profile social and demographic characteristics of crime perpetrators for a better law enforcement and adjudication.

3.2.10 Forensic Criminology

Criminology is not only a course of study, but also an area of specialisation in sociology. At present, some courses are naturally classified as forensic criminology: Forensics or forensic science, criminalistics, forensic psychology, forensic science management, criminal investigation, and the like. Criminology is often referred to as the sociological study of crime and delinquency. It looks into the pathways to criminal behaviour, including life-course and age of onset in criminal enterprise, and explores the ever-sweeping changes that are taking place in society, their motivations, and the processes involved in lawmaking, lawbreaking, and societal reactions to lawbreaking and lawbreakers. Iwarimie-Jaja (2003) simply defined criminology as the sociological study of adult crime. Another criminologist shared this view: Modern criminology is the study of social origin of criminal law, the administration of criminal justice, the causes of criminal behaviour, and prevention and control of crime, including individual rehabilitation and modification of the social environment (Sykes, 1978). Criminologists are involved in creating effective crime policies, developing methods of social control, and the correction and control of known criminal offenders (Siegel, 2016).

Criminologists assist lawmakers in altering the content of the criminal law in response to changing times and conditions. For instance, computer fraud, theft from ATMs, Internet scams, and illegal tapping of television cable lines are behaviours that did not exist when criminal law was originally conceived. The law must be constantly revised to reflect cultural, societal, and technological adaptations of criminal acts (Siegel, 2007). This perspective on general criminology centres on forensics and criminalistics, an important branch of criminology and criminal justice, which involves addressing legal questions and technicalities as they relate to the findings of laboratory analysis of crime and criminals. Chisum and Turvey (2007) contended that forensic criminology is a behavioural and forensic science, characterised by an integration of materials from many sub-disciplines, including forensic science, criminal investigation, criminalistics, forensic psychology, victimology, crime reconstruction (i.e. the interpretation of what happened in a crime scene), criminal event analysis, criminal profiling, and practical experience.

A popular and reliable criminology website (see Anon, 2016 in http://www.forensiccriminologist.com/Forensic_Criminology.html)

reported that the key distinguishing feature of a forensic criminologist, compared to other criminologists, is the expectation that his opinions and findings will be used in the context of an investigative format or submitted in a legal proceeding. A forensic criminologist has a particular examination to perform, or set of questions to answer. He is interested in theory and research, only so far as it can be applied to the analysis or interpretation of a particular case. As forensic experts, criminologists conduct a rigorous and critical analysis of the entire body of evidence that objectivity demands, and comprehensively comparing case facts and circumstances to each pieces of evidence (Anon, 2016 http://www.forensiccriminologist.com/Forensic_Criminology.html).
Quite naturally, forensic criminologists examine the criminal justice system from a sociological perspective. Like sociologists, criminologists are trained in criminalistics and forensic science to assess court systems, prison facilities, and law enforcement agencies (Dougherty, n .d.).

Virtually every social phenomenon is in the state of flux. Although some aspects of crime, law and science are still somewhat static, a greater part of them is relative, dynamic and socially constructed. As a result, forensic criminologists must possess highly developed cognition, critical thinking and reasoning skills to enable them grapple with the spatial dynamics and variations in cybercrimes, law and justice across cultures and professions. Critical thinking is of the essence in forensic studies, and this can be achieved by employing world-class research facilities, training and retraining of criminologists. A reasonable proficiency in evidence/facts evaluation and scale of justice balancing, practical experience, specialist knowledge and reliable information are also prerequisites for the development of critical thinking and reasoning for a successful forensic investigation. These garnered resources hold great promises for criminologists to understand the technicalities of forensic science and law and, in turn, achieve a resounding success in crime/criminal detection, investigation and prosecution. Scriven and Paul (1996) defined critical thinking as the intellectually disciplined process of actively and skillfully conceptualising, applying, analysing, synthesizing, and/or evaluating information gathered from, or generated by observation, experience, reflection, reasoning, or communication, as a guide to belief and action.

Given their practical experience, special training and wealth of knowledge, criminologists can provide an objective and accurate witness testimony, validate and corroborate forensic evidence or facts either for or against an accused in court. Also, they can be called upon during court hearing to demystify and clarify vague and confusing crime evidential data to ensure free and fair judgment. An earlier cited popular and reliable forensic criminology website (see Anon, 2016 in http://www.forensiccriminologist.com/Forensic_Criminology.html)

revealed that a forensic criminologist applies criminological analysis to a particular set of facts or circumstances using modern methodologies and generally accepted investigative practices and procedures. In the absence of specific policy and procedures, the investigating forensic criminologist applies global best practice standard. That is, the forensic criminologist employs theory in an applied manner, utilising case-based knowledge and experience, focusing on the practical as opposed to theoretical. Findings and opinions are based upon evidentiary analysis and case facts are amenable to objective scrutiny and systematic testing, consistent with understandable and easily explained scientific methods (see Anon, 2016).

3.2.11 Physical Evidence Samples and Forensic Investigation

Physical evidence cannot be explained and understood without first making reference to crime scene. Most physical evidence is found in the crime scene—a location where a criminal act was committed, or a place where victim-offender interaction took place. Nevertheless, crime can occur in more than one location and thereby leading to a multiple crime scenes, namely, primary, secondary, intermediate and dumpsite or disposal site. Physical evidence refers to all or any item/material or object that links crime investigators to victims and/or their offenders. The earlier postulation of Edmund Lucard several years back, that ‘every contact leaves a trace’, is indeed reverberating through the history of criminological thoughts. And this has been made possible through the advancement in science and technology and their application to criminal investigation and prosecution.

It is obligatory of the detective to identify and follow this trace evidence to logical conclusion. Trace/physical evidence could be directly or indirectly obtained from various crime scenes, victims, suspects, or witnesses. On arriving at the crime scene, investigators are expected to first cordon off or encase the area with bold inscription, warning people to keep off. Yellow ribbon with black inscriptions is used in this regard (e.g. CRIME SCENE DO NOT CROSS, etc). The first respondents (crime scene examiners who arrive the crime site) in their clothing/gadgets should carefully search the place without altering or contaminating the scene, identify physical evidence, use relevant equipment to collect samples, and properly preserve them for laboratory analysis and results consequently use in court.

There are two major types of physical evidence: questioned or unknown samples and controlled, known, standard, or reference samples. Questioned samples are of unknown origin; their origin is yet to be ascertained and samples are collected for identification and comparison purposes. On the other hand, the origin of controlled samples is known and samples are collected for the purpose of forensic examination and

comparison with unknown samples. Both samples are collected to provide investigators and presiding officers with fundamental clues about crime and criminals, or to establish victim-offender relationship. The meaning of crime scene, physical evidence as well as type, has been clearly delineated. Now, it is necessary to discuss the various physical evidence samples that aid forensic examiners and law enforcement agents in forensic investigation. These samples are hairs, fibres, bloodstains, paints, scrapings, weapons, polygraphs, voiceprints, photographs, prints and chemicals analyses.

Hairs Analysis

The hair is one of the human sense organs found in the outer layer of the skin, although its root is traced to an inner organ called 'hair follicle'. Hairs can grow in any part of the human skin, but much of them are found in the head. Like the teeth, the hair is hard and resistance to chemical decays as well as has the ability to keep structural properties for a lengthy period of time. Its unique colour, length and shape are good physical evidence samples for criminalistics/forensic examination. The follicular tag which is the hair's richest source of DNA is the characteristics that make the hair an important sample or evidence for placing a person at a crime scene. That is, the presence of DNA in the hair makes it amenable to forensic examination. Human hairs, especially the ones in the head and the eyelashes can fall out of the skin easily, providing avenue for three phases of hair growth called 'telogen phase' to take place. The implication is that hairs are usually found in crime scenes (including computer/laptop keyboard), whether there is a serious/violent crime transaction or not, between victims and their offenders.

Importantly, it should be noted that the hair in most cases cannot be seen with the naked eye. As a result, the aid of telescope, microscope, or other scientific devices is required to see, pick up and examine the morphology (colour, form and structure) of the hair. In order to link a suspect with criminal activities, experts are required to collect enough quantity of hairs (unknown sample) at the crime site using relevant apparatus and submit the unknown sample alongside with adequate known sample (collected from the suspect or victim) to the crime laboratory for forensic analysis, identification and comparison. This is done to identify whether the hair is of human or animal origin and also to ascertain whether the hair (unknown sample) collected at a crime site matches with a suspect's hair (known sample). The collection and preservation of hair for DNA examination must with approved tools, following scientific procedures. As a possessor of analytical skills, firstly, a forensic crime investigator collects hair from a crime scene or on an individual with forceps to avoid damaging or contaminating the

root tissue. Secondly, he or she should air-dry hair if it is mixed with suspected body fluids. Thirdly, the investigator should package each group of hair (known and unknown samples) separately in a clean paper or an envelope (not container or leather) with the corners properly sealed and labelled. Plastic containers should not be used in packaging the hair samples). Fourthly, the hair sample has to be refrigerated and submitted to the crime laboratory as soon as possible for further DNA examination and forensic analyses.

Furthermore, pubic and head hairs are mainly used for criminalistics, forensic hair examination and 'comparison' (i.e. cross-marching of known and unknown samples). For forensic examination, a minimum of 50 full-length head hairs and 24 full-length of pubic hairs are required for analysis, or constitute a representative sample. In the case of rape, which can occur in the course of committing cybercrime, a 'survivor' (victim of rape) should use a clean comb to carefully comb his or her pubic hairs to remove all fallen out or loose foreign hairs before the survivor is subjected to forensic examination. The comb with which the victim used in combing his or her pubic hairs should be sealed in a separate envelope and also submitted to the crime laboratory for forensic analysis.

Fibres Analysis

Fibre is a slender, fine filament; a thread-like natural or synthetic component/substance composed of spun glass, animal skin, and wood. Fibres are classified into two major groups: Natural and manufactured or artificial. The former could be obtained from plants or animals while the latter are obtained from both natural and synthetic polymers. Polymer is a substance that has a simple structure of large molecules; that is, a chemical compound which is composed of many atoms. Although different byproducts of plant fibres like cotton that is used in cloth-making are robust evidential sample, the majority of crime-scene evidence are human clothing made from animal fibres.

The animal fibres are essentially extracted from the hair coverings of goats, rabbits, sheep, and camels and then spun and turned into a variety of wool which is used to manufacture human clothing. The implication is that, during violent crime transaction which usually brings victims and their offenders or the weapon used into close physical or body contact, some fibres are inadvertently deposited at the crime scene. This makes fibres important physical evidence samples needed for a successful criminal detection and investigation. To avoid contamination and cross-contamination of fibre evidence, criminalists or any crime investigator should carefully identify, collect, preserve and package

'articles' (samples) in a separate envelope or any other paper bags with sealed corners.

During crime scene inspection, especially in such violent crimes as assault, automobile accident involving a 'hit-and-run' driver, murder, rape and other sexual violations, criminalists typically look out for fibres either at the scene of the incident or on the body of the 'objects' used in the physical or body contacts. For instance, a driver who hits a female pupil and ran away may not know that there is blood (see bloodstain analysis and develop self-critical thinking concerning bloodstain and fibre analyses), or that fibres or pieces of her school uniform is stuck to a particular area of the vehicle. Moreover, fibres or pieces of clothes belonging to a burglar (housebreaker) may be recovered from a broken window, door, or 'protector' (burglarproof). This evidence may provide experts with much needed clues about the origin of such fibres and ultimately assist them in placing or linking a suspect to a particular crime. To identify and compare the common origin of manufactured fibres which are commonly found in human clothing, a similar (not exact or the same) approach that is used in the case of hair analysis is sometimes applied.

Comparison microscope and other relevant electronic devices can be used in fibre identification and comparison. But, in some cases, the morphological features (colour, form/shape, structure, and even diameter) of fibres can also be examined using the naked eye. This is self-evident in the case of fibres or pieces of cloth that left a conspicuous trail or cut on the clothing of a suspect or victim, or even a whole fabric (shirt precisely) grabbed by a victim during crime transaction. For the naked eye fibre or a piece of fabric identification and comparison, a criminalist ought to be scrupulous in his or her processing (collection, packaging, preservation, analysis/examinations, and interpretation) of any evidence of forensic value. Here, the questioned/unknown samples (fibres or pieces of cloth) should be carefully inserted into the unknown/control/standard/reference samples (a torn shirt or trousers) and in that case an expert opinion can be formed with pinpoint accuracy.

Bloodstains Analysis

Blood is a complex physical evidence sample, and is of significance to forensic examiners. For this reason, no amount of crime-scene bloodstains should be ignored for whatsoever reasons. Rather, adequate care should be taken by investigators to spot a bloodstain at the crime scene. The identification of its specific location (presence), splatter, shape and appearance are also important in criminalistics examinations. Having achieved this, the first to do is to trace the origin of the bloodstains, whether it belongs to human or animal. However, most of

the crime-scene bloodstains are usually of human origin. Offenders often inflict injuries on the body of their victims or unknowingly get themselves injured in the course of committing a crime. This makes crime-scene bloodstains useful evidential sample for effective crime reconstruction and criminal investigations. The collection and preservation of human blood samples for criminalistics/forensic analysis requires series of processes, which Saferstein (2007, p. 624-625) stated thus:

Blood

1. Only qualified medical personnel should collect blood samples from a person.
2. Collect at least two 5-ml tubes of blood in purple-top tube with 'EDTA' as an anticoagulant for DNA analysis. Collect drug or drug-testing samples in grey-top tubes with 'NaF' (sodium fluoride).
3. Identify each tube with the date, time, subject's name, location, collector's name, case number, and evidence number.
4. Refrigerate, do not freeze blood samples.
5. Use cold packs, not dry ice, during shipping.
6. Pack liquid blood tubes individually in Styrofoam or cylindrical tubes with absorbent material surrounding the tubes.
7. Label the outer container KEEP IN A COOL DRY PLACE, REFRIGERATE ON ARRIVAL, and BIOHAZARD.
8. Submit to the laboratory as soon as possible.

Blood on a Person

1. Absorb suspected **liquid blood** onto a clean cotton cloth or swab. Leave a portion of the cloth or swab unstained as a control. Air-dry the cloth or swab and pack in a clean paper or an envelope with sealed corners. Do not use plastic containers.
2. Absorb suspected **dried blood** onto a clean cotton cloth or swab moistened with distilled water. Leave a portion of the cloth or swab unstained as a control. Air-dry the cloth or swab and pack in a clean paper or an envelope with sealed corners. Do not use plastic containers.

Blood on Surface or in Snow or Water

1. Absorb suspected **liquid blood or blood clots** onto a clean cotton cloth or swab. Leave a portion of the cloth or swab unstained as a control. Air-dry the cloth or swab and pack in a clean paper or an envelope with sealed corners. Do not use plastic containers.

2. Collect suspected **blood in snow or water** immediately to avoid further dilution. Eliminate as much snow as possible. Place in a clean airtight container. Freeze the evidence and submit as soon as possible to the laboratory.

Bloodstains

1. Air-dry **wet bloodstained garments**. Wrap **dried bloodstained garments** in a clean paper. Do not place wet or dried garments in plastic or airtight container. Place all debris or residues from the garments in a clean paper or an envelope with sealed corners.
2. Air-dry small suspected **wet bloodstained objects** and submit the objects to the laboratory. Preserve bloodstain patterns. Avoid creating additional stain patterns during drying and packaging. Pack to prevent stain removal by abrasive action during shipping. Pack in a clean paper. Do not use plastic containers.
3. When possible, cut a large sample of suspected **wet bloodstains from immovable objects** with a clean, sharp instrument. Collect an unstained control sample. Pack to prevent stain removal by abrasive action during shipping. Pack in a clean paper. Do not use plastic containers.
4. Absorb suspected **dried bloodstains on immovable objects** onto a clean cotton cloth or swab moistened with distilled water. Leave a portion of the cloth or swab unstained as a control. Air-dry the cloth or swab and pack in a clean paper or an envelope with sealed containers. Do not use plastic containers.

Blood Examination Request Letter

A blood examination request letter must contain the following information:

1. A brief statement of facts relating to the case.
2. Claims made by the suspect(s) regarding the source of the blood.
3. Whether animal blood is present.
4. Whether the stains were laundered or diluted with other body fluids.
5. Information regarding the victim(s)' and suspect(s)' health such as AIDS, hepatitis, or tuberculosis.

Paint Analysis

Generally, paints could be liquid or dried in nature. Paints are important trace evidence in criminal investigation and prosecution. Paint chips/particles from devices used in or during 'breaking and entering' can be found at a crime-scene. Some equipment, facilities, or certain

area of burgled house as well as garments belonging to a burglary suspect may have paints smeared and/or embedded in them during crime commission. Also, there is usually a cross-transfer of paints from one vehicle to another during collision, accident. With this, the establishment of common origin of paint evidence is possible. A critical comparison of questioned paint samples and control paint samples can be done with the naked eye and an acceptable result obtained and logic conclusion reached.

Nevertheless, the manual technique is sometimes, fraught with shortcomings. Based on the weaknesses of this particular method, crime investigators are not to limit their interest and logic to the naked eye examinations—laboratory analyses of such paints remain imperative for an 'end-doubt' result and conclusion. In a ‘hit-and-run’ (accident involving a driver whose identity is unknown) situation, for instance, forensic analysis will reveal the colour, make and model of a vehicle using a very small quantity of paint samples collected at an accident scene. This approach has made headway in identifying crime perpetrators.

For paint chips collection at the crime scene, experts are required to use a pair of tweezers in the collection, or pick up the sample with a clean and dry piece of paper. Tweezers is a small device that has two narrow pieces of metal fastened to one end, which is mainly used to pick up, move, or pull very small objects like paint chips. Upon collection, the samples should be preserved using plastic or glass phial (vial) and a very short, small envelope (similar to the ones used by patent medicine dealers, pharmacists in folding drugs). Do not remove or attempt to remove paint smear or stain embedded in objects or clothing. Rather, the entire garments or objects should be carefully collected, packaged and delivered to the crime laboratory for analysis.

Noteworthy is the fact that there is always a transfer of paints when a vehicle hits an object or collides with another. In a situation involving automobile collision, the method of paint sample collection is quite different. With the use of relevant tools, as earlier established, the unknown paint sample is collected either from the undamaged area of the car or scooped up from the ground if it can be seen at a ‘spotted and designated location’ (adjacent the crashed vehicle) where the accident occurred. A clean and unused ‘scalpel’ (a very sharp small knife that is used by medical doctors in some surgeries) makes excellent equipment for the collection of a standard/reference/known paint sample. Scalpel makes for a good and deep, sharp cut out of all the paint layers of a suspected vehicle.

Tools used to break and enter buildings or safes often contain traces of paints as well as other substances such as wood and safe insulation. Therefore, care must be taken not to lose these trace evidence. The crime scene investigator should not try to remove the paints; instead, he or she should package the samples and devices used in the collection for crime laboratory examination. Standard/reference paint should be collected from all surfaces suspected to have been in contact with the tool, and all layers of paints must be included in the sample. When the tool has left its impression on a surface, standard/reference pain sample is collected from an uncontaminated area nearest to the impression. No attempt should be made to collect the paint from the impression itself. If this is done, the impression may be permanently altered and its evidential value lost. Paint sample measuring 1/4 inch square is a standard, acceptable sample representation for crime laboratory analysis (Saferstein, 2007).

Weapon (Arms and Ammunition) Analysis

Weapons used in crime commission are of different types. Crime weapons are, among others, computers, 'pen', 'tongues', bludgeon (club), bayonet, dagger, broken bottles, axe, machete/cutlass, firearms (arms and ammunition), explosives, and the Internet. In keeping with the content of this course, only arms (guns) and ammunition (bullets) are discussed. Weapon analysis is a forensic/criminalistics study of firearms, including discharged bullets, pistol shells and cartridge casings. It is a laboratory examination of gunpowder residues and primer residues around bullet wounds, on a victim or suspect's clothing and other evidential objects. Weapon analysts also examine bullet holes, marks, or scrapings on human victims, walls and other objects to determine the possible distance and direction from where a shooter fired his or her target(s).

Firearms identification is necessary, given the increasing shooting incidents in society. This involves a paradigm shift from mere identification and comparison of ammunition of all types "to include knowledge of the operation of all types of weapons, restoration of obliterated serial number on guns, detection and characterisation of gunpowder residues on garments and around wounds, estimation of muzzle-to-target distances, and detection of powder (and primer) residues on hands" (Saferstein, 2007, p. 460). For avoidance of misconception, Saferstein (2007) brought to the fore the difference between firearms identification and ballistics: Firearms identification is a discipline mainly concerned with determining whether a bullet or cartridge was fired by a particular weapon. It is not to be confused with ballistics, which is the study of a projectile in motion.

The interior of firearms barrel is composed of five structures located in the internal portions of firearms barrel. These inner surfaces are: grooves, rifling, bore, lands, and calibre. Grooves are the cut, low-lying parts of a firearm barrel located between the lands in a riffle bore. Riffling is the spiral grooves produced in the bore of a gun barrel that causes a bullet to spin (not to tumble) while leaving the barrel. Bore is the inner surface of a gun barrel. Lands are the elevated part of a firearm barrel situated between the grooves in a riffle bore. Finally, calibre is the diameter of the inner surface of a firearm barrel. The calibre of a rifled firearm is calculated in hundredths of an inch or millimetres [mm] (e.g. **.**22 calibre or 9mm). The different chambers in the inner barrel of firearms make every projectile passing through it to exit, leaving unique/special marks on the bullet. The special marks are technically called 'striations' This provides criminalists with critical trace evidence that can link such arms and ammunition and the shooter to a crime.

Like fingerprints, no two firearm barrels have the same or matching 'striations' (special lines or markings in the interior portions of gun barrels). However, each weapon manufacturer uses identical and consistent number of grooves and lands in his or her firearms production. Even the width and direction of twist is approximately the same. For instance, all **.**32-calibre Colt revolvers have six lands and six grooves twisting to the left, while all **.**32-calibre Smith & Wesson revolvers are composed of five lands and five grooves twisting to the right. All these unique identification and comparison features—firearms class characteristics—enable experts to link guns and bullets used in perpetrating a crime to manufacturers, purchasers/owners, and a suspect's association with crime scene or criminal acts. The popular Avtomat Kalashnikov (AK-47) riffle has 7.62-calibre.

The pertinent question that requires critical thinking and answer is: What if a locally manufactured gun was used in committing a crime where those inner barrel structures may be missing? Such a gun, if recovered, should be submitted to experts for fingerprint and paint examinations. Crudely made guns retain much identifiable fingerprints compare to firearms manufactured using sophisticated scientific and technologies. Contained in the features of automatic guns are trigger guard and chequered part of the grip. These are two areas in a gun that do not keep particular and recognisable fingerprints. These components (particularly the chequered portion) are rarely built in the locally made guns. Even were they exist, a shooter can only hold the two portions to avoid fingerprint transfer, but cannot carry out a successful operation or fire targeted-shots without touching and holding greater parts of the gun.

Collection and Preservation of Firearms

The collection and preservation of firearms evidence is a difficult and risky task. First and foremost, investigators must consider every gun seen at a crime site or wherever firearms evidence is deposited or found to be loaded. With this in mind, precautionary measures should be taken to avoid 'accidental discharge' at the point of retrieving, in transit and upon submission. Therefore, experts are expected to unload such firearms to avoid recording casualties, but a detail profile of such gun must be made before disconnecting or unloading it. The positions of both the hammer and safety, and the location of every expended and unexpended projectile (bullets) must be accurately recorded before the unloading. The two categories of ammunition in the gun, fired/expended and unfired/unexpended, should be carefully retrieved and packaged in a separate envelopes with sealed corners and immediately be submitted to crime laboratory analysts for examination.

Identification tag must be attached to all types of firearms retrieved from the earth-surface crime location. The tag must contain the following information: The firearm's serial number, make and model, and the collector's initials. In a situation involving firearms evidence recovered from the water, do not dry or clean it; instead, submerge the evidence in a container full of water and convey to the crime laboratory. This is done to prevent rust and wearing and tearing from occurring in transit.

Collection and Preservation of Ammunition

Ammunition encompasses bullets of all types, including shells and cartridge casings, and they have class. Expended bullets have striation markings, which must be protected from scratching, damaging or obliteration that usually occurs during projectile-extraction from a victim's body or other targets. During bullet extraction, adequate caution is needed in order not to scratch a bullet in the course of extracting it from a target. Rather, fired ammunition must be removed by carefully cutting open the piercing surface area of the projectile. Clearly, encased in modern ammunition is **Gunpowder Residues**; a trace evidence sample usually exploited by forensic investigators during criminal investigation. It is a gaseous substance, smokeless powder that is discharged and found along with fired ammunition and cartridge cases on a victim or crime scene. Residues are difficult to remove from a contact or target.

With the presence of gunpowder residues on crime victims, garments, walls or other objects, gunshot distance determination is possible and

thereby leading to the tracking down of perpetrator(s) of a crime. Gunpowder residues always create 'bullet wipe' (a kind of dark ring formed around the entrance of a bullet hole created on a victim body, garment, or other objects) which is used in forensic investigation for distance determination between the shooter and his or her target(s). Again, this substance enables experts to separate a suicide situation from homicide, and murder from self-defence claims, by examining residues patterns using gunpowder microscope or infrared photographs. In test-firings, maximum scientific results and quick and easy-to-prove evidence are achieved using the suspect's firearms and ammunition (Saferstein, 2007).

Other strong trace evidence used by forensic scientists to track down perpetrators of crime is **Primer Residues**. Both gunpowder and primer residues are discharged in a 'forward-backward' direction when a shot is fired. That is, some of them follow the fired shot to (hit) the target while others are pulled back to the muzzle, barrel, and the shooter's hand. Most importantly, primer residues are mainly deposited in the phalanges (fingers), particularly the finger web of the shooter. With the aid of a microscope for primer residues detection, this trace evidence can even be clearly seen in the bullet wound encrusted with reddish-brown blood that is called tattooing. Without the use of a microscope, in some cases, cotton-hand-swabbing can be used in the collection of primer residues from a shooter's hand(s). But this is, sometimes, fraught with pitfalls, as primer residues can be easily removed from a suspect either by conscious or unconscious washing of hands.

The weaknesses associated with cotton-hand-swabs have necessitated the invention and application of automated gunshot particle search and identification systems, among which are, Scanning Electron Microscope (SEM) and Integrated Ballistic Identification System (IBIS). Modern gunpowder and primer detection requires the application of adhesive to a suspect's phalanges. Quite naturally, human hands are often contaminated, but the gunshot residue particles in the adhesive reveal distinctive shape and size. The most obvious chemical compositions that are presence in gunshot particles are barium, lead and antimony. These properties differentiate gunshot residues from other hand-contaminants, when exposed to SEM (Saferstein, 2007).

Recently, some automated firearms search systems have been introduced in the discipline of criminalistics, forensic science. Among these is the introduction and establishment of the National Integrated Ballistics Information Network (NIBIN) in 1999 through the collective efforts of Federal Bureau of Investigation (FBI) and Alcohol, Tobacco, Firearms and Explosives (ATF). NIBIN was developed under the Integrated Ballistic Identification System (IBIS). Agencies using the IBIS technology produce database files from bullets and cartridge casings

retrieved from crime scenes or test-fires from recovered firearms. More than 200 law enforcement agencies all over the world have embraced this technology (Saferstein, 2007). Also, IBIS "developed digital microscopic images of identifying features found on both expended bullets and cartridge casings by incorporating two software programmes: Bulletproof, a bullet-analysing module and Broadcaster, a cartridge-casing-analysing module" (Tontarski & Thompson, 1998 cited in Saferstein, 2007, p. 468).

Polygraph Analysis

Otherwise known as lie detector, polygraph helps forensic investigators to unravel the truth behind incidents, particularly crime. Here, crime suspects are subjected to polygraph testing by comparing the results with a subject's statement, victim's statement, or witnesses' statements. Polygraph is a scientific device that is used in detecting lies by measuring and recording certain physiological changes occurring and reoccurring in a subject's pulse, skin conductivity, blood pressure, and breathing. John Augustus Larson, a medical student at the University of California, Berkeley who was also police officer of the Berkeley Police Department in Berkeley, California, invented lie detector in 1921. Advocates of this criminal investigative tool maintained that untrue responses to a question will cause the said vital signs to react in certain ways and consequently produce physiological answers that are different from the supposing truthful responses.

Nevertheless, the validity and reliability of polygraphs has been in contention. Many professionals believed that the device is not completely scientific and thus results it produces can easily be manipulated either by the polygraph examiner (polygraphist) or the equipment itself, especially if is faulty or malfunctioned. At the same time, professional criminals may comport themselves during polygraph testing in order to manipulate, control and maintain a balanced blood pressure, respiration, and pulse rate—which are measuring rod and physiological determinants of deceptive and non-deceptive answers to a question—according to lie detector.

In 2001, for instance, Iacono (2001) argued that a significant fraction of the scientific community considered polygraph as a 'pseudoscience'. Specifically, the relevant-irrelevant questioning method used in polygraph examination has been challenged by many experts, including presiding officers during court hearing. This testing method is designed to determine subjects' responses to both crime questions and non-crime related questions. The relevant-irrelevant testing system is not ideal, as many innocent subjects (timid, naïve and gullible ones precisely) exert a heightened physiological reaction to crime relevant questions (Iacono, 2008).

Voiceprint Analysis

Voiceprint analysis covers virtually all aspects of electronic media, namely, telephone, television, radio, the Internet, and all tape-recorded communications. Simply put, voiceprint is the conversion of speech or oral communication into a visual display and performance. This can be achieved with the help of a special instrument called sound

spectrograph. The uniqueness of sound patterns in human speech under the control and manipulation of a sound spectrograph makes for easy and unbiased identification of different categories of individuals using their voices.

With spectrographic analysis of sound patterns produced in speech, forensic investigators can trace a kidnapper who, through telephone calls or messages, demands and negotiates ransom with a victim's relatives. This instrument can be used to establish the real identity of a student who used a strange telephone number to threaten or send threat messages to his or her lecturer(s). It can also be used to trace verbal communications between cybercriminals (yahoo-yahoo boys, cyber dates) and their victims.

Reporting the spectrographic findings of a Bell System Engineer, Lawrence Kresta, Saferstein (2007) contended that each voice has its own unique quality and character, arising out of individual variations in the vocal mechanism. On the other hand, a further review of Kresta's work by the same author showed that the probability that any two individuals have the same size of vocal cavities (throat, nasal, and two oral cavities formed by positioning the tongue) and co-ordinate their articulators (lips, teeth, tongue, soft palate, and jaw muscles) in a like manner is so small to make the human voice a unique personality. The Engineer reported that the voiceprint is simply a graphic display of the unique characteristics of the voice. Despite the wide purchasing and application of sound spectrographs by crime laboratories, criminalists and policing agencies, voiceprint (in some quarters) has not been generally accepted as scientific evidence in court and even in the general scientific community (Saferstein, 2007).

Photograph Analysis

A complete and clear photographic coverage of a crime-scene, victim and suspect is required for a successful criminal investigation. Fundamentally, all the physical evidence located at the crime scene must be accurately captured. The photograph should be taken using highly sophisticated cameras and such specialised image-capturing equipment as infrared, X-ray, digital imaging, and ultraviolent to make physical evidence visible to the naked eye. The photographing of a crime scene should be thoroughly done by a specially trained photographer. Only photographs in their original forms are admissible in courts; in other words, computer programmes must not be used to alter or improved photographs taken at the crime site, as this will be rejected during legal proceedings.

Using proper tools and guidelines, a crime-scene photographer is generally required to take as many photographs as possible in the field, with camera attached to tripod when necessary. In an indoors crime-scene, a crime investigator should be guided by the corners of the room as he or she takes overlapping shots. The interior portions of the house roof or ceiling, windows, floor, doors, and certain furniture and objects must be captured by an investigator. An outdoors crime-scene requires a systematic capturing and recording of the exterior views of a specific house where the scene is closer to: All adjacent buildings, road or street signs, trees, paths/roads, and addresses.

The photograph of each physical evidence must be taken separately and thereafter a collective shots taken, with each physical evidence in their original positions. Each crime-scene photographing must be accompanied by a brief description, clearly stating the date, time, film-roll and exposure number (for film cameras only) and file name and exposure number (for digital cameras only). Another point to note is shot distance on target, indicating whether the shots were taken with camera mounted on tripod or hand-camera-capturing method was used.

Fingerprint Analysis

The first systematic attempt at personal identification was developed by a French police expert, Alphonso Bertillon, in 1883. Prior to the discovery of fingerprint by Francis Galton (1833 – 1911), the Bertillon system relied on 'Portrait Parle' (a detail verbal description of a crime perpetrator or suspect's physical characteristics and clothing by a crime victim or an eyewitness) and 'Anthropometry' [a systematic combination of people's full-length and profile photographs with precise body measurements as a way of identification] (Saferstein, 2007).

The police and other law enforcement agents/agencies have tried on several occasions to track down criminals by looking for a dependable way of unique personal identifications. To this end, efforts were made to examine the finger ridge patterns or 'minutiae' (ridge characteristics such as bifurcations, ridge endings, enclosure, ridge island/ridge dot, and short ridge) which are unique features in human palms/fingers. It is important to note that no two persons all over the world—even identical twins with a similar DNA—have similar or the same fingerprints (i.e. finger ridge patterns). What is more, fingerprint is immutable and constant throughout a person's lifetime

Fingerprints are usually left behind at the crime site either by an offender/suspect or a victim. Based on this, it is important for crime investigators and laboratory analysts to gain in-depth knowledge and understanding of how fingerprints evidence are identified, collected and

analysed to avoid being rendered inadmissible in the court of law by presiding officers. According to Sheridan (2013), the location of a fingerprint often requires a vigilant and calculated search, but in circumstances where the print is visible to the naked eye, finding a fingerprint is relatively easy. The more intricate searches take place when the print is present on a surface but not visible. The type of fingerprint left behind usually determines the amount of time and effort investigators must spent in the course of locating and collecting the print. Lyle (2012), cited in Sheridan (2013), identified three types of fingerprints: Patent prints, plastic prints and latent prints.

1. **Patent prints** are easy to locate since they are visible to the naked eye. Patent prints occur when someone has a substance on their fingers, such as grease, paint, blood, or ink, which leaves a visible print on a surface.
2. **Plastic prints** are also easy to locate but are less common than patent prints since they occur when someone touches an object such as wax, butter, or soap and leaves a three-dimensional impression of the finger on the object.
3. **Latent prints** are the most common type of print but take the most effort to locate because they are invisible. Latent prints occur when someone touches any porous or nonporous surface. The natural oils and residue on fingers leave a deposit on surfaces which mirror the ridges and furrows that are present on the individual's finger.

The advancement in science and technology has necessitated the use of Automated Fingerprint Identification Systems (AFIS) for the purpose of criminal investigation. Now, fingerprints identification, classification, interpretation, retrieval and preservation are done with the support of computers. In 1999, according to Saferstein (2007), the FBI commenced full operation of the Integrated Automated Fingerprint Identification System (IAFIS), the largest AFIS in the United States that links State AFIS computers with the FBI database. AFIS computers are available from several different appliers. Each system scans fingerprint images and detects and records information about minutiae.

In Nigeria, AFIS computers are gradually gaining currency, as evidenced by the automated registration of mobile phone numbers by network service providers (such as MTN, GLO, AIRTEL, ETISALAT, and so on), the current issuance of driving licence by the Federal Road Safety Corps (FRSC), Independent Electoral Commission voters' card, Bank Verification Number (BVN), among others. Here, data linkage is necessary to build a robust and sustainable national fingerprints databases to facilitate forensic investigation and crime fighting.

Role of Forensic Investigation and Evidence in Criminal Justice Administration

Forensic investigation simply refers to the application of science and technology to unravel either the complexities of a phenomenon or behavioural pattern of human beings. Contextually, forensic investigation is an act of making thorough enquiry into the scientific and technology-based materials, information and data to determine the operational procedures and dynamics of a phenomenon, person or group of persons in relation to deviance, delinquency and crime. The outcome is to identify a lead and objectively follow it to establish outcomes for policy implication in the criminal justice administration.

3.3.1 Meaning and Types of Evidence

There is no straightjacket definition of evidence; it means different things to different professionals. But one thing is unique about evidence: it is uncovered in the course of investigation, and contextually is of paramount importance to law enforcement and legal proceedings. Therefore, investigation and evidence are indispensable in criminal litigation, since the determination of guilt and/or innocence by presiding officers rests on their validity, reliability and acceptability.

From the Nigerian legal point of view, evidence is divided into three: oral, documentary and real, though additional evidence called **electronic evidence, computer evidence or digital evidence** was incorporated into the legal system following the amendment of Nigerian Repealed Evidence Act 1954 in 2011. Thus, in all, there are four types of evidence in the country's judiciary. The latter, electronic evidence makes forensic investigation easier, faster and convenient, with outcomes acceptable in courts. **Oral Evidence:** This refers to verbal account or testimony given by a witness in a court of competent jurisdiction, which could assume the dimension of reexamination, examination-in-chief, or cross-examination. **Documentary Evidence:** Like data-type or instruments for data (evidence) collection in research, documentary evidence is divided into primary and secondary, suggesting that it may be sought and obtained through or using these two sources. Simply put, documentary evidence rely on contents and context of a document to prove or disprove (alleged) facts in court. **Real Evidence:** This is the production and presentation of material facts before the court for scrutiny. It can take the form of moveable and immoveable objects or phenomena. Generally, the three sets of evidence can only be admissible in the court of law if they are obtained through acceptable investigative procedures and by certified investigators.

3.3.2 Forensic Investigations and Evidence in Criminal Justice Administration

Any law enforcement agents can be charged with the collection of evidence, whether digital or physical, but only certified forensic scientists are involved in the analysis to establish the scientific and technological bases of such evidence and for it to be acceptable in the criminal justice system. Various forensic experts and forensic instruments are involved in the investigation of criminal activities. Hence, the roles of forensic investigation and evidence in criminal justice administration are summarised below:

1. Forensic professionals, particularly those in the physical science Unit, apply the knowledge garnered from geology, chemistry and physics to conduct laboratory analysis of chemicals, drugs, explosives, ammunition and shells, glasses, and soils to enable them achieve acceptable results for legal proceedings.
2. Forensic pathologists are trained to ascertain the cause of death through the performance of postmortem, autopsy. Postmortem study assists in determining the probable time, cause and manner of death by examining the body fluids and tissues, as well as pallor mortis, algor mortis, rigor mortis, and livor mortis.
3. Forensic biologists and biochemists collect hairs and plants from the scene of an incident and analyse the botanical and chemical properties to establish their origin or source and therefore facilitate successful prosecution of offenders. They also conduct DNA tests for law enforcement and legal purposes.
4. Experts in forensic science are skilled in analysing such physical evidence samples as blood, hairs and fingerprints collected from crime scene to identify suspects and as well present such evidence during court trial.
5. Forensic investigation reports and evidence are used to prove or disprove facts and determine guilt or innocence of the accused standing trial.
6. Forensic scientists use a special ‘image modification equipment’ to search for accused persons who jump bail or runaway-prisoners. With the aid of this equipment, experts can digitally reconstruct the age of the subjects and make a photograph of them to understand how they would look at aging.

3.4 Basic Features of Cybersecurity Strategies

3.4.1 Definition of Cybersecurity Strategies

Although the terms, ‘cybersecurity strategies’, ‘cybercrime strategies’ and/or ‘cybercrime prevention’ have been interchangeably used in some policy discourses and academic literature, they are separate approaches

to cybersecurity. Seger (2012) explained that, while cybersecurity strategies and cybercrime strategies complement each other and include some areas of overlap, they are not identical. For this author, cybercrime prevention strategies set out the efforts to directly and indirectly deal with cybercrime, such as law enforcement responses and the promotion of national and international co-operation between governments, businesses, academic institutions, organisations, and the public, in order to control and/or reduce cybercrime.

While, cybercrime strategies focus exclusively on crime prevention and criminal justice policies, programmes, and practices. On the other hand, UNODC (2019, p. 133) noted that "cybersecurity strategies provide guidance on cybersecurity matters (which can include cybercrime prevention), and map out objectives, action plans, measures, and the responsibilities of institutions in meeting these objectives. These strategies include legal, procedural, technical, and institutional measures designed to safeguard systems, networks, services, and data".

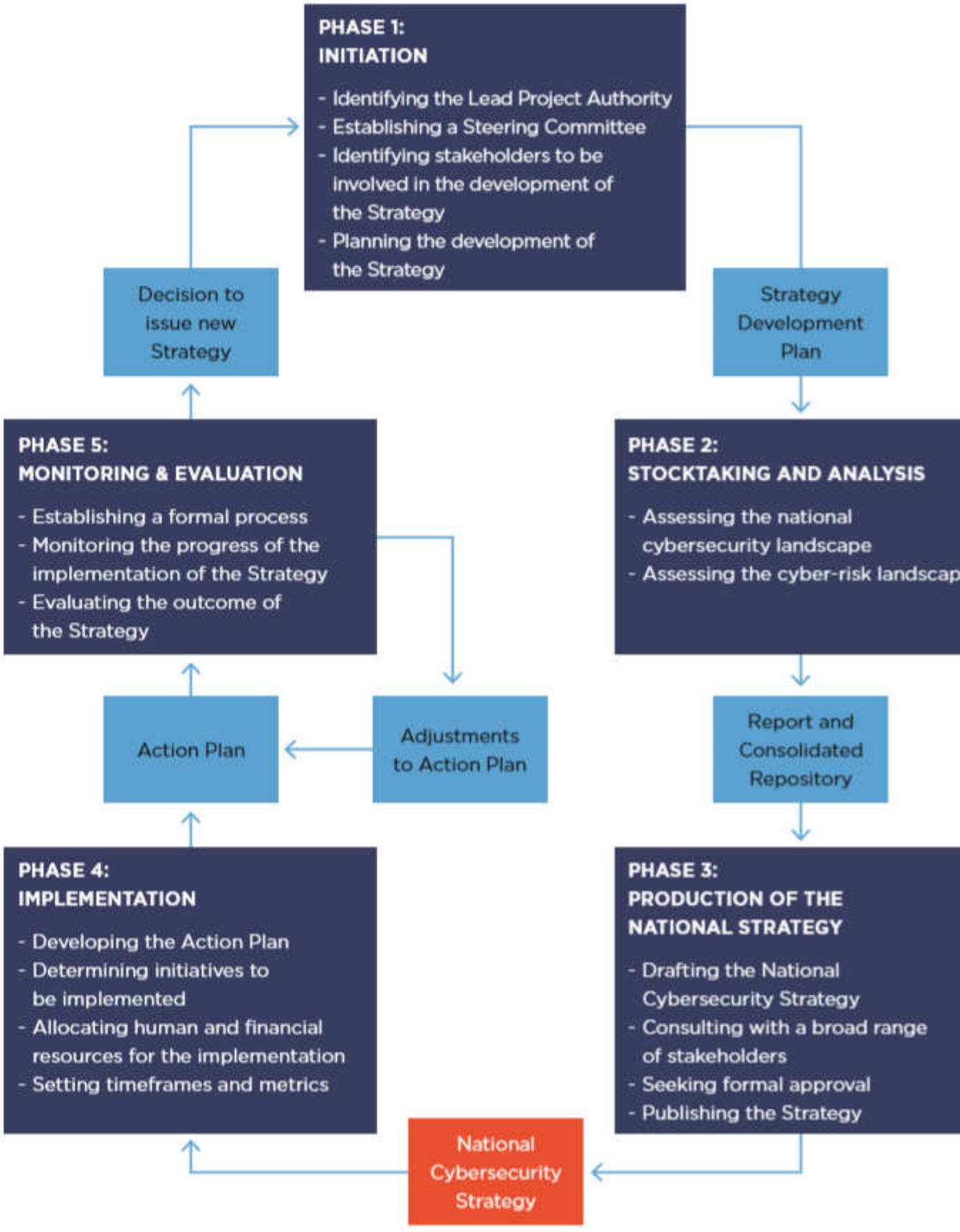
3.4.2 Cybersecurity Strategies

National cybersecurity strategies explain States' cybersecurity and cybercrime prevention objectives, both at the national and international climes. These objectives represent countries' aspirations, which could be national security-related or information and communication technology-based issues. In Sweden, for instance, its cybersecurity "strategy is based on the objectives for Sweden's security: Protecting the lives and health of the population, the functioning of society, and… [its] capacity to uphold fundamental values such as democracy, the rule of law and human rights and freedoms" (Swedish Ministry of Justice, 2017, p. 1 cited in UNODC, 2019, p. 134).

The national cybersecurity strategies "outline the principles on which the strategy is based, prescribe the interests that this strategy seeks to protect, identify the tools used to promote and protect these interests, identify cyber threats and the challenges these threats pose to national and economic security, delineate cybersecurity policy priorities, and allocate resources to these priorities" (Lindstrom & Luiijf, 2012, p. 44). National strategies "encourage…policymakers to identify strategic objectives ['ends'], to pinpoint the resources available to reach those objectives ['means'], and to provide a guide on how such resources are to be applied to reach stated objectives ['ways']" (Lindstrom & Luiijf, 2012, p. 46). These "strategies detail why the strategy is important and why it is needed (*context*), what it does (*objectives*), what it covers, and what and whom it impacts (*scope*)" (ITU, 2018, p. 30 cited in UNODC, 2019). The 2014 National Cybersecurity Strategies of Nigeria highlight the following objectives in Section 3.3.2:

1. A comprehensive cybercrime legislation and cyber-threat countermeasures that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace;
2. Provision of measures that protect critical information infrastructure, as well as reducing our national vulnerabilities through cybersecurity assurance framework;
3. To articulate an effective computer emergency response capability;
4. National mechanisms on capacity building, public awareness, and skills empowerment is necessary to help strengthen our capability so as to respond promptly and effectively to cyber-attacks and espionage;
5. A trusted mechanism for engaging national multi-stakeholder and international partners towards collectively addressing cyber threats;
6. To deter and protect government from all forms of cyber-attacks;
7. To co-ordinate cybersecurity initiatives at all levels of government in the country;
8. To build national capabilities against cyber threats with coherent co-operation through public-private sector partnership and multi-stakeholder engagement;
9. To promote national vision on cybersecurity through awareness, partnership through shared responsibilities and a trusted community of stakeholders; and
10. To promote co-ordination, co-operation and collaboration of regional and global stakeholders on cybersecurity (Cybersecurity Strategies of Nigeria, 2014, (n. p.).

3.4.3 Figure 1: Lifecycle of National Cybersecurity Strategy



Source: International Telecommunication Union. (2018). *A guide to developing a national cybersecurity strategy*, p. 17. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/d-str- cyb_guide.01-2018-pdf-e.pdf. Accessed 28 January 2020.

3.4.4 Challenges of Forensic Investigation and Prosecution of Cybercrimes

As earlier observed (see 3.5 in Module 2), the challenges of forensic investigations and prosecution of cybercrimes intersect well with that of cybercrime prevention and control in many aspect. This is because most forensic investigations involve the use of electronic resources and evidence. Notwithstanding, the three broad perspectives (training, operational standards, and international standardization) of Ajetunmobi (2009, p. 41) are considered germane and worthy of reiteration in this Section of the Course Material:

1. **Training:** Although there are many private organisations and educational institutions offering computer forensic seminars and classes internationally, there is need to have such facilities available in Nigeria, also. With the rate at which cybercrime is growing, computer forensic training is a worthwhile investment for private organisations and (State) law enforcement agencies. Since computer forensic evidence is very volatile, the preservation especially by law enforcement personnel requires specialised training for its handling. Network operators should also be trained, while lawyers should receive basic training towards understanding of computer evidence;
2. **Operational Standards in Computer Forensics:** Since cybercrime occurs mainly on international basis, basic guidelines for the planning and collection of evidence process, investigation and monitoring, analysis, reporting, and preservation of the evidence need to be established worldwide. This is because prosecution of suspects is often subject to location where the crime was perpetrated—if there is no standard procedure that is acceptable and admissible in any court of law anywhere in the world, then it renders presentation of the evidence fallible; and
3. **International Standardization of Computer Forensics:** Since different countries have their own computer forensic methods, standards, and laws (or none at all), what is an acceptable digital evidence in one country may not be in another country. This becomes a very serious problem when dealing with international crimes, as cybercrime often is. Because the Internet has no boundaries does not remove the fact that law enforcement agencies do. Investigations can be carried out but only with co-operation between law enforcement agencies of the countries involved—many borders may be crossed on the way with complications not only by evidence handling differences, but also by political and legal differences.

SELF-ASSESSMENT EXERCISE

i. The term, ‘circa’ contextually refers to ----------
   a. Cybercrime
   b. About
   c. Ultimate
   d. Security

ii. The height, gender, age, and facial morphology of a dead person can be established through ---------- examination.
   a. Forensic pathology
   b. Forensic biology
   c. Forensic odontology
   d. Forensic anthropology

iii. The first forensic study of human finger and palm prints is traced to --------- civilisation of 650AD.
   a. Egyptian
   b. Mesopotamia
   c. Chinese
   d. Roman

iv. --------- focused exclusively on crime prevention and criminal justice policies, programmes and practices.
   a. Cybersecurity strategies
   b. Cybercrime prevention
   c. Forensic investigation
   d. Cybercrime strategies

v. Portrait Parle and Anthropometry as aspects of forensics were invested by -------
   a. Alphonse Bertillon
   b. Francis Galton
   c. Michael Parle
   d. Silver Porta

vi. The device use by forensic scientists to search for a runaway accused or prisoner is called ---------
   a. Compass
   b. Image modification
   c. Imaging
   d. Atlantis

vii. Documentary evidence is classified into ------- and ---------
   a. Audio and visual
   b. Electronic and print
   c. Primary and secondary
   d. Soft and hard

viii. ------ is the production and presentation of material facts before the court for examination.
   a. Real evidence

b. Documentary evidence
c. Oral evidence
d. Digital evidence

ix. The branch of forensic science that deals with NDA test is --------
-
a. Cyber forensic
b. Forensic toxicology
c. Forensic odontology
d. Forensic biology

x. Who among these experts conducts postmortem study?
a. Forensic pathologist
b. Forensic mortician
c. Forensic anatomist
d. Forensic entomologist

4.0 CONCLUSION

In this Unit, the etymology of forensics has been traced, and the concepts of forensic investigations and digital evidence operationalised. Different types of computer evidence were identified and explained. Various scopes, units or branches of forensic science were discussed in some depth. We also discussed the roles of forensic investigations and evidence in the prosecution of cybercrimes and weaknesses of this technique of criminal investigation. Cybersecurity strategies and cybercrime have been clearly delineated to keep this course material in perspective. Several national cybersecurity strategies have been implemented to aid in combating cybercrimes through forensic investigations, with strong metrics to evaluate the effectiveness of these strategies.

5.0 SUMMARY

In this Unit, it is established that evidence, be it physical or electronic, is obtained through (forensic) investigation. It is used to prove or disprove facts and determines guilt or innocence of the accused in legal proceedings. Forensic investigation, when properly conducted by acknowledged experts, is more scientific, admissible, and ends-doubts in criminal litigation.

6.0 TUTOR-MARKED ASSIGNMENT

Critically study the challenges facing forensic investigation and prosecution of cybercrimes and proffer practical solutions to each of the identified weaknesses.

7.0 REFERENCE/FURTHER READING

Adejoh, S. O.; Alabi, T. A.; Adisa, W. B. & Emezie, N. M. (2019). "Yahoo yahoo boys" phenomenon in Lagos metropolis: A qualitative investigation. *International Journal of Cyber Criminology, 13*(1), 1-20.

Ajetunmobi, R. A. (2009). *Cyber crime – A case for computer forensic guidelines in Nigeria* (M. Sc. Dissertation). Department of Information Security and Computer Forensics, University of East London, London, United Kingdom.

Anon. (2016). *The science of forensic criminology*. Retrieved from http://www.forensiccriminologist.com/Forensic_Criminology.html. Accessed 19 March, 2016.

Chisum, W. & Turvey, B. (2007). *Crime reconstruction*. Boston: Elsevier Science.

Dougherty, D. (n. d.). *Forensic sociology and criminology*. Retrieved from http://www.rosemont.edu/academics/graduate/forensic-sociology-criminology/. Accessed 19 March, 2016.

George, D.; Rawlings, R.; Williams, W.; Phillips, M.; Fong, G.; Kerich, M.; Momenam, R.; Umhau, J. & Hommer, D. (2004). A select group of perpetrators of domestic violence: Evidence of decreased metabolism in the right hypothalamus and reduced relationships between cortical/subcortical brain structures in positron emission tomography. *Psychiatry Research: Neuroimaging, 130,* 11-5.

Gudjonsson, G. H. & Haward, L. R. C. (1998). *Forensic psychology: A guide to practice*. London: Routledge.

Haralambos, M.; Holborn, M. & Heald, R. (2008). *Sociology: Themes and perspectives* (7th ed.). London: HarperCollins.

Iwarimie-Jaja, D. (2003). *Criminology: The study of crime* (2nd ed.). Owerri: Springfield Publishers.

Melvin, A. O. & Ayotunde, T. (2011). Spirituality in cyber crime "yahoo yahoo" activities among youths in south west Nigeria. In Dunkels, E.; Franberg, G. & Hallgren, C. (Eds.), *Youth culture and net culture*: *Online social practices* (pp. 357-376). Hershey, PA: IGI Global.

Raine, A.; Buchsbaum, M. & LaCasse, L. (1997). Brain abnormalities in murderers indicated by positron emission tomography. *Biological Psychiatry, 42*, 495-508.

Saferstein, R. (2007). *Criminalistics: An introduction to forensic science* (9th ed.). New Jersey: Prentice Hall.

Scriven, M. & Paul, R. (1996). Defining critical thinking: a draft statement for the national council for excellence in critical thinking. Retrieved from http://www.criticalthinking.org/University/univlibrary/library.nclk. Accessed 19 March 2016.

Siegel, L. J. (2008). *Criminology: The core* (3rd ed.). Belmont, California: Thomas Higher Education.

Silva, J. A.; Leong, G. B. & Ferrari, M. M. (2004). A neuropsychiatric developmental model of serial homicidal Behaviour. *Behavioural Science and the Law, 22*, 787- 799.

Sykes, G. (1978). *Criminology*. New York: Harcourt Brace Jovanovich.

Tancredi, L. (2004). *Hardwired behaviour: What neuroscience reveals about morality*. London: Cambridge University Press.

International Telecommunication Union. (2018). *A guide to developing a national cybersecurity strategy*, p. 17. Retrieved from https://www.itu.int/dms_pub/itud/opb/str/d-str-cybguide.01-2018-pdf-e.pdf. Accessed 28 January, 2020.

United Nations Office on Drugs and Crime. (2019). *E4J university module series: Cybercrime*. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/basics-of-computing.html. Accessed 20 December, 2019.

Ward, J. T. (2013). What is forensic psychology? Retrieved from http://www.apa.org/ed/precollege/psn/2013/09/forensic-psychology.aspx. Accessed 19 March, 2016.

MODULE 3

Unit 1 Tools Used for Computer Forensics.
Unit 2 Ethical Issues in Cybercrime and Forensic Investigations.
Unit3 Digital Forensic Investigations: Practices, Procedures or Protocols.
Unit 4 Controversies Surrounding Forensic Investigations and Evidence in Court.

CONTENTS

1.0 INTRODUCTION

Although cybercrime is on the increase globally and intensified efforts have been made by the international community and criminal justice systems to combat the menace, it is necessary at this juncture to highlight some of the tools used for computer forensic and procedures to follow to make digital evidence admissible in the court of law.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- identify the tools and methods used for computer forensic examination, investigation.
- address ethical issues that could contradict electronic evidence and render it inadmissible in court if forensic protocols are not properly followed or observed.

- discuss digital forensic investigations, practices, procedures or protocols.
- assess the controversies surrounding forensic investigations and digital evidence in courts.

3.0 MAIN CONTENT

3.1 Tools Used for Computer Forensics Investigations

As highlighted in www.forensix.org, cited in Ajetunmobi (2009, pp. 35-37), below are tools used for computer forensic investigations:

1. **Access Data's Forensic Toolkit (also known as FTK):** This is a commercially used investigative tool used to examine relevant and compatible storage media image files. This tool has been used by private and government agencies worldwide and is considered to be one of the best of its kind in the market today;
2. **EnCase:** In most parts of the world, computer forensic investigators use the EnCase Software for the seizure, analysis and court presentation of computer evidence. This is due to the fact that EnCase is a widely accepted tool that is also commercially available. It has also been subjected to extensive reviews and testing which it withstood. The evidence acquired and processed using this tool have been successfully admitted into evidence in thousands of trials and preliminary hearing the world over, and defence lawyers using expert witnesses have not found it wanting in terms of its acceptability;
3. **Helix:** This is a customised version of the Knoppix live Linux CD used as an Incident Response and Forensic Tool. Its main function is to process live acquisitions of physical drives on a host machine. Logical drives such as CD/DVD ROM/Recordable Drives are not included as acquisition options in Helix;
4. **ILook:** Another computer forensic tool used and provided free of charge to qualifying law enforcement agencies throughout the world only is the ILook Investigator. This software was written by Elliot Spencer and is made available through the Electronic Crimes Programme of the Internal Revenue Service of the United States. ILook is a tool that can only be used by persons trained and skilled in the knowledge of forensic data recovery. Without a level of high expertise of knowledge and qualifications, findings produced from using ILook to examine digital evidence may be considered unreliable and cannot be subjected to verification;
5. **Paraben:** This is another respected name in the Computer Forensics Tools arena. In testing, the tool produces an ISO image but does not automatically verify that a good image has been produced (usually by MD5 Check Sum) like FTK imager and

other ISO imaging software tools such as NTI CD/DVD Maker version 6.7 and Nero Burning Rom v8.3.2.1;

6. **RootkitRevealer:** Created by Byce Cogswell and Mark Russinovich, RootkitRevealer is an advanced root kit detection utility that runs on Windows NT 4 and higher versions of Microsoft Windows with its output listing registry and file system API discrepancies which may indicate the presence of a user—or kernel—mode rootkit. This software successfully detects all persistent rootkits, but like ILook, can only be used by persons familiar with its working operations;
7. **SBMD5:** Created by Sanderson Forensics, it is used to calculate the MD5 checksum on the content of a SafeBack image held on tape. The hash/checksum generated is based on the information within the image and will compare it to a hash/checksum taken directly on the drive with a utility such as EnCase;
8. **Sector Inspector:** This is a tool created by Microsoft Corporation identified as SecInspect.exe as a command-line diagnostics tool which allows administrators to view the contents of master boot records, boot sectors, and IA64 GUID partition tables;
9. **SnapView HTML Viewer:** Created by Craig Wilson for Digital Detective, SnapView HTML is a quick and easy way to examine recovered HTML pages from unallocated space. This viewer is built using the same technology as the Internet Explorer. It can load up pages quickly and also toggle between page and source views using the F9 key. This viewer does not support HTML only; other formats are also supported by it. Some of these formats include JPEG, GIF, ICO, Flash Move, Adobe Acrobat, Microsoft Office documents such as MS Word, MS Excel, MS PowerPoint, Bitmap, etc;
10. **Stegdetect:** Created by Niels Provos, Stegdetect is an automated tool used for detection of steganographic contents in images. Its capability includes detection of several different steganographic methods used to embed hidden information in JPEG images. Its current detectable schemes include jsteg, jphide (UNIX and Windows), invisible secrets, and outguess 01.3b;
11. **Text2Hex:** Created by Craig Wilson for Digital Detective, this utility converts ASCII characters to hexadecimal values which are really useful when searching software that can accept hex values as search criteria. Its main usefulness is for designing hex search strings where the search strings uses unusual characters e.g. “{} [ ]? /.!%^*”. It also allows searching for Unicode characters, and the data can then be converted into pure hex values or a format usable by EnCase; and
12. **Wireshark (previously known as Ethereal):** Created by Combs *et al*., Wiresharkis a free network protocol analyser for UNIX and

> Windows. It allows one to examine data from a live network or from a capture file on disk. One can interactively browse the capture data, viewing summary and detail information for each packet received. Wireshark is known to have several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. Live data can also be read from Ethernet FDDI, PPP, Token-Ring, IEEE 802.11, and classical IP over ATM, and loopback interfaces (at least on some platforms supported by it). Operating systems on which it functions includes UNIX, Linux, and Windows.

As computer forensic investigators and analysts are developing tools for successful investigations, so cybercriminals are expanding the scope of anti-forensics to avoid detection, apprehension and prosecution. Anti-forensics are "tools and techniques to remove, alter, disrupt, or otherwise interfere with evidence of criminal activities on digital systems, similar to how criminals would remove evidence from crime scenes in the physical realm" (Conlan, Baggili, & Brietinger, 2016, p. 67).

3.1.1 Tutor-Marked Assignment

Examine the strengths and weaknesses of the tools used for computer forensic investigations.

3.2 Ethical Issues in Cybercrime and Forensic Investigations

Ethical issues in this context explain the standards and best practices guidelines for cybercrime and forensic investigations in relation to digital evidence handling and admissibility in the first two phases of the criminal justice system—police/law enforcement agencies and courts. The ethics or ethical code (of conduct) refers to the 'dos' (right) and 'don'ts' (wrong) of cybercrime and computer forensic investigators. It refers to the guidelines that clearly spelt out what these professionals should always do and what they should not do regardless of the situation. They are expected at all times to follow the due process of law as contain in their professional guide to handle (collect, collate, analyse, interpret and report findings) electronic evidence so as not to lose its validity, reliability and acceptability.

It is no wonder therefore, that the International Society of Forensic Computer Examiners (ISFCE) revealed the professional ethics for its members to imbibe in the course of discharging their duty. The aim is to make sure that standards are followed, achieved and guaranteed, so that the results of the forensic investigation become acceptable evidence by being accurate, dependable, conclusive and permissible. According to

ISFCE (n. d.)., the ethical considerations or standards, including the behaviours that computer forensic examiners, must abide by (such as 'abiding by legal orders and conducting a comprehensive examination of the evidence according to existing laws, standards, procedures, and guidelines') and outlawed behaviours (such as withholding evidence, engaging in biased analyses or reporting of evidence, and misrepresenting qualifications) they must detest.

Cybercrime law identifies standards of acceptable behaviour for information and communication technology users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates co-operation between countries on cybercrime matters (UNODC, 2013; UNODC, 2019). Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organisations. Others include rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organisations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law (UNODC, 2019).

From the foregoing, cybercrime code of ethic is relative; there is no unified standards to follow in forensic science generally, and digital forensic investigation. Each national and regional government have adopted different but acceptable practices in the validity and reliability of tools, methods and processes used in computer forensic examination. Examples are the 'European Network of Forensic Science Institutes' best practice manual for the forensic examination of digital technology', 'United States Working Group on Digital Evidence's best practices for computer forensic examination, digital evidence collection, and computer forensic acquisitions', Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine of 2017, African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (Draft African Union Convention) of 2012, and Nigerian Cybercrime Act 2015. A common idea which runs parallel to all global best practices for digital forensic studies is the emphasis on 'valid and reliable forensic investigation processes and outcomes". Accordingly, computer forensic ethics are summarised below:

1. Digital forensic evidence must be peer-reviewed and its validity and reliability maintained throughout the investigation processes.

2. Tools and methods used in digital forensic investigation must be 'scientifically valid', 'forensically sound', and 'legally admissible'.
3. Data, information or evidence processing must follow scientific and legal procedures (i.e. the exercise should not be conducted in a manner that establishes element of obscurity and/or mysticism).
4. Experts are bound to be neutral and objective in case management, assessment, and delivery.
5. Detailed and accurate documentation of digital forensic tools and techniques used in the investigation process is required.
6. Do not take sides or favour victims or offenders for whatsoever reason in the course of investigating case, cybercrime.
7. Do not manipulate, plant or destroy digital and physical evidence samples.
8. Always ensure that witness, victim and offender's rights are respected and protected.

3.2.1 Forensic Evidence Handling, Processes and Legal Admissibility

In the private sector, for instance, the Cyber Security Coalition (CSC) explained that the response/reaction to such cybersecurity incidents as 'denial of service attack, unauthorised access to systems, or data breach' requires a specific code of ethics that should be observed to contain the incident. From this source, there exists two major approaches for 'handling a cybersecurity incident: Recover quickly and gather evidence (CSC, 2015). The former is not concerned with the preservation and/or collection of data but the containment of the incident to minimise harm. Because of its primary focus on swift response and recovery, vital evidence could be lost. The latter monitors the cybersecurity incident and focuses on digital forensic applications in order to gather evidence of and information about the incident. Because of its primary focus on evidence collection, the recovery from the cybersecurity incident is delayed (CSC, 2015; UNODC, 2019).

In terms of electronic evidence admissibility, both legal and technical procedures are required, and must be followed to ensure the admissibility of such evidence in the court of law. For the legal requirements, the court examines the legal authorisation to conduct searches and seizures of information and communication technology and related data, and the relevance, authenticity, integrity and reliability of digital evidence. The technical requirements, on the other hand, requires that the court critically examines the digital forensic procedures and tools used to extract, preserve and analyse digital evidence; the digital laboratories whereby analyses are performed; the reports of digital forensic analysts; and the technical and academic qualifications of

digital forensic analysts and expert witnesses [if applicable] (Antwi-Boasiako & Venter, 2017).

Arising from the two variables, 'forensic evidence handling and legal admissibility', is the question of who handles or processes forensic evidence? "Forensic evidence processing involves two important groups of people. First, "the crime scene investigators on the scene are typically local police officers or members of a major crime unit of law enforcement officers who are trained to collect evidence and investigate crime" (Lissitzyn, 2008, p. 45). "The second group is composed of laboratory technicians. These technicians typically do not travel to crime scenes to gather evidence, but instead, test evidence (brought to them) in the laboratory" (p. 45). In all this, chain of custody must be maintained. By chain of custody, we mean "the process by which investigators preserve the crime (or incident) scene and evidence throughout the life cycle of a case. It includes information about who collected the evidence, where and how the evidence was collected, which individuals took possession of the evidence, and when they took possession of it" (Maras, 2014, p. 377). More importantly, forensic evidence handlers or processors argued that:

> Forensic evidence cannot be admitted in court unless the court is assured that it is genuine. It must also be introduced through the testimony of a witness who can personally identify it or who is in charge of a record-keeping process and can explain how the evidence was handled and safeguarded. Generally, this means that someone with custody or control over the evidence must show that the evidence was collected properly and that "chain of custody" remained unbroken. Otherwise, the evidence could have been tampered with, replaced, destroyed or substituted. From the moment the forensic evidence is removed from the scene until it is presented in court, it must be accounted for. Generally, this requires that anyone who removes or handles the evidence must sign the evidence log with the time and date the evidence was removed and replaced (Lissitzyn, 2008, p. 44).

3.3 Digital Forensic Investigations: Practices, Procedures or Protocols

The procedures of conducting digital forensic investigation are relative; it is dependent upon a country's legal framework and the nature of cybercrimes. Therefore, there is no single acceptable digital forensic practice across the globe. However, certain methodologies must be followed to drive research and development with regard to the conduct of digital forensic investigations. According to Maras (2014), for instance, the protocols should include search, acquisition, preservation, and maintenance of digital evidence; description; explanation and establishment of the origin of digital evidence and its significant. Other include the analysis of evidence and its validity, reliability, and relevance to the case; and the reporting of evidence pertaining to the case.

Another case in point is the effort of the Digital Forensic Research Workshop (DFRW). This body developed electronic forensic investigation model in 2001 in line with the United States Federal Bureau of Investigation's protocol for physical crime scene search. The model has seven stages: Identification, preservation, collection, examination, analysis, presentation, and decision (see Palmer, 2001). The seven phases are graphically presented below:

Figure 2: Electronic Forensic Investigation Model

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Source: Palmer, G. (2001). Digital forensic research workshop technical report: A road map for digital forensic research. *Digital Forensic Workshop*. Utica, New York.

The International Organisation for Standardisation (ISO), in conjunction with the International Electrotechnical Commission (IEC), published international standards for electronic evidence processing in 2012 (see ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence). The first phase is **identification:** This refers to the search for, identification, recognition and documentation of relevant digital evidence. When the evidence is identified and necessary protocols observed, a call or need for its collection is made. The **collection** stage entails the gathering of all digital materials or devices that are strongly believed after identification to contain data, information or traces of evidential value.

According to the UNODC (2019), the collected devices are conveyed from the crime scene or scene of the incident to a forensic laboratory or any other facility designated for this purpose for acquisition and investigation of the retrieved electronic evidence. This process is known as *static acquisition*. However, there are cases in which static acquisition is unfeasible. In such situations, *live acquisition* of data is conducted. Let us consider, for example, the systems of critical infrastructures (i.e., industrial control systems). These systems cannot be powered down as they provide critical services. For this reason, live acquisitions are conducted to collect volatile data and non-volatile data from live running systems (UNODC, 2019).

At the **Acquisition** stage, the electronic evidence is obtained without contaminating and/or compromising the validity and reliability of the sample. The United Kingdom National Police Chiefs Council (NPCC), formerly known as the United Kingdom Association of Chief Police Officers, emphasised this particular standard for digital forensics practice. For instance, Principle 1 states that “No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court” (UK Association of Chief Police Officers, 2012, p. 6). To achieve this, imaging is required; imaging involves producing a duplicate copy of digital device’s content without altering or compromising the integrity. This is accomplished using write blocker, a device designed to avoid the modification of records during the copying process.

The UNODC (2019) revealed that, to determine whether the duplicate is an exact copy of the original, hash value is employed; a hash value is calculated using mathematical computations. Here, a cryptographic hash function is used to produce a hash value. If the hash values for the original and copy match, then the contents of the duplicate are the exact same as the original. Understanding that there are certain “circumstances where a person finds it necessary to access original data [i.e. during live acquisitions],” the United Kingdom National Police Chiefs Council

noted that "the person [accessing this data] must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions" [Principle 2] (UK Association of Chief Police Officers, 2012, p. 6).

The **preservation** phase is concerned with the safeguarding, protection of both electronic devices and electronic evidence, which is best achieved through a 'chain of custody'. A systematic and confidential documentation is important at each of the digital forensics practice. Interestingly, subsequent ISO/IEC 27037 Guidelines include two additional essential phases, namely, analysis and reporting.

The **analysis** stage involves the application of appropriate digital forensic tools and approaches to examine and reveal the digital data, with the aim of determining its relevance and probable evidential value. Doing this is to ascertain whether the evidence of investigation is capable of making "the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence" (Rule 401, United States Federal Rules of Evidence). The period of **reporting** "includes a detailed description of the steps taken throughout the digital forensics process, the digital evidence uncovered, and the conclusions reached based on the results of the digital forensics process and the evidence revealed" (UNODC, 2019, p. 72).

3.3.1 Steps for Conducting Digital Forensic Investigations

There are several steps or stages of conducting digital forensic investigations. Till date, nevertheless, no universally acceptable steps exists. In 2017, the Norwich University Online (NUO) advanced five steps to follow in conducting digital forensic investigations, and they are: Policy and procedure development, evidence assessment, evidence acquisition, evidence examination, and documenting and reporting (NUO, 2017). They are adopted and explored in this Course Material for their informative and practical relevance to the Nigerian context.

Step 1: Policy and Procedure Development

Step one involves establishment of policies and procedures to guide experts in their forensic investigation. This will enable them understand the dos and don'ts of the profession, and to keep to legal rules and regulations pertaining to the collection, processing and preserving of digital evidence of forensic value and victim/offender handling. These guidelines include, among others, comprehensive instructions about when computer forensics investigators are authorised to recover potential digital evidence, how to properly prepare systems for evidence

retrieval, where to store any retrieved evidence, and how to document these activities to help ensure the authenticity of the data (Norwich University Online [NUO], 2017).

Certain policy and procedural rules must be carefully observed before the commencement of cyber or computer forensic investigation. Understanding and adhering to the ethics will not only equip investigators with additional knowledge and details of the case at hand, but also recognise all acceptable investigative tools and course of action concerning a case under investigation. To achieve this with huge success, the investigator is to meticulously read case briefs, understand the technicalities of cyber legislations, and seek and obtain authorisations (warrants) when necessary and applicable before investigating a case. At the same time, every law enforcement agencies has Information and Communication Technology Departments where these strict protocols and forensic rules of governance (policies and procedures) are developed and disseminated by acknowledged experts in cyber law, cybercrime, cyber forensics and cybersecurity. In the Nigeria police subsystem of the criminal justice system, for instance, the G Department is responsible for ICT matters in relation to digital policy development, with the following objectives:

- To develop an ICT policy for the Nigeria Police Force, in line with National ICT Policies, such as policies on procurement, use and maintenance of ICT equipment;
- To develop and empower the Nigeria Police personnel with ICT skills for operation efficiency and improved service delivery;
- To provide tools that will help accomplish efficient modern policing;
- To introduce ICT innovative solutions that are centred on strategic policing that will facilitate public participation in policing;
- To develop technological-driven Citizen and Law Enforcement Analysis and Reporting (CLEAR) programme that is designed within the context of police-community partnership for efficient and effective law enforcement;
- To provide and maintain a system for data collection, input analysis and necessary output;
- To provide and maintain security for all levels of access and privilege to information systems and technology in all Police Formations;
- To ensure that the Nigeria Police acquire the best ICT equipment that complies with global law enforcement standards;
- To evolve law enforcement technological solutions that will set pace for other security agencies globally; and

- To periodically conduct ICT related need assessment and advice the Force accordingly (Nigeria Police Annual Report, 2010).
-

Step 2: Evidence Assessment

Like policy and procedure development, evidence assessment is key to successful forensic investigation. As a forensic investigation process, evidence assessment requires investigators to critically and objectively evaluate potential cybercrime evidence. Proper classification and understanding of policies on cybercrimes gives investigators the latitude to process evidence, make them legally admissible, and even determine what works in the efforts to combat cybercrimes. This underscored the importance and symbiotic relationship between Steps One and Two, as it relates to prosecution of cybercrime suspects. The core element in Step One, strict guidelines and procedures, is raised with a view to determining whether the widely acceptable Antwi-Boasiako and Venter's (2017) Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) was properly followed. The HM-DEAA three-phase-model summerises the basic legal and technical guidelines that evidence assessment and acceptability to include 'digital evidence assessment, consideration, and determination'

The interest of the court is not only on what seasoned experts presented before it as evidence, but also concerned on how such evidence was processed and who were responsible for that exercise. In digital evidence assessment, the central concern of courts is to determine whether appropriate legal authorisations (such as search warrant, court order, or subpoena) were used to search and seize ICT and related data. Although these authorisations are relatively applied across jurisdictions due to peculiarities in national legal systems, search warrant remains a predominant legal order adopted by most jurisdictions to search and seize ICT and ICT-related data (UNODC, 2019).

At the digital evidence determination stage, the AIR (i.e. Authenticity, Integrity and Reliability) of digital and related evidence is thoroughly evaluated in relation to the results of the evaluation of the processes carried out in the evidence consideration phase. Examples include the application of forensically sound techniques and equipment to collect evidence and the testimony of expert witnesses and forensic analysts to substantiate the AIR of this evidence (see also US National Institute of Justice, 2004; Antwi-Boasiako & Venter, 2017; UNODC, 2019). In other words, strict adherence to the rule of validity, reliability and peer-review in technical and legal enquiries is a precondition for digital evidence admissibility or appropriateness.

At the digital evidence consideration level, a critical evaluation is undertaken to determine the integrity of digital evidence by scrutinising the forensic methods and devices employed in extracting the evidence, the competence and integrity of the forensic investigators who obtained, preserved, and analysed the digital evidence, and the forensic laboratories where the evidence was handled and examined (US National Institute of Justice, 2004; Maras, 2014; UNODC, 2019). This was further illustrated by the Norwich University Online (2017, n. p.) thus:

> …if an agency seeks to prove that an individual has committed crimes related to identity theft, computer forensic investigators use sophisticated methods to sift through hard drives, email accounts, social networking sites, and other digital archives to retrieve and assess any information that can serve as viable evidence of the crime. This is, of course, is true for other crimes, such as engaging in online criminal behaviour like posting fake products on eBay or Craigslist intended to lure victims into sharing credit card information. Prior to conducting an investigation, the investigator must define the types of evidence sought (including specific platforms and data formats) and have a clear understanding of how to preserve pertinent data. The investigator must then determine the source and integrity of such data before entering it into evidence.

Step 3: Evidence Acquisition

Connected to acquisition is the identification and collection of computer evidence. Identification involves the thorough search and research conducted in order to detect potential evidence that could guide digital forensic experts in their investigation. Following the recognition of electronic devices (i.e. evidence identification) this step contains or houses information of evidentiary value, such digital tools which are then collected (i.e. evidence collection). Upon identification, a process known as ‘static acquisition’ is conducted; this requires that the identified and collected devices be taken to the forensic laboratory or any relevant test centre, for evidence acquisition and analyses.

Not all computer devices are mobile or detachable; even when they are, the affected systems or digital tools could be linked to critical national

infrastructure and thus making 'static acquisition' of evidence difficult or impossible. Systems/computers or other electronic devices connected to critical infrastructure are so essential that any disconnection or interruption in their connectivity and functionality would have serious implications for national security, economy, and public health and safety. These systems provide vital goods and services and hence cannot be completely shutdown. Faced with this challenge, live acquisition of evidence becomes a necessary alternative. For instance, UNODC (2019) reported that industrial control computers as systems of critical infrastructure offer critical services and as such cannot be powered down, "and so live acquisitions are conducted that collect volatile data and nonvolatile from running. These live acquisitions, however, can interfere with the normal functions of the industrial control system" (p. 69).

Planning for digital evidence acquisition and processes involved are always in-depth and demanding. Such requires detailed records before, during, and after obtaining the evidence. For instance, comprehensive and firsthand information acquired must be documented and preserved; these including all hardware and software specifications, any systems used in the investigation process, and the systems being investigated (NUO, 2017). The policies and procedures developed in Step One becomes much more needed at this juncture to reinforce the general guidelines for evidence acquisition and preservation of its integrity. These guidelines include "the physical removal of storage devices, using controlled boot discs to retrieve sensitive data and ensure functionality, and taking appropriate steps to copy and transfer evidence to the investigator's system" (NUO, 2017, n. p.).Overall, evidence acquisition should be done in a 'deliberate and legal manner'. This is further explained to mean that the ability to document and validate the 'chain of evidence', like the chain of custody, is extremely important when following a court case, "and this is especially true for computer forensics given the complexity of most cybersecurity cases".

Step 4: Evidence Examination

Evidence examination also represents the analysis phase, which refers to the use of suitable digital forensic devices and procedures to discover and retrieve digital data. The reason for evidence examination or analysis is not farfetched: It is to determine the importance and possible worth of evidence. The purpose of this determination is to investigate whether the evidence of analysis "has the tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence" (Rule 401 United States Federal Rules of Evidence cited in UNODC, 2019, p.).

Therefore, there must be an established policies and procedures to follow and tools to use by forensic analysts when or in retrieving, copying, and storing evidence within appropriate databases. These methods make for the examination of evidence from chosen archives (files and records), and the use of several different techniques in interpreting and analysing data. For NUO (2017, n. p.), "these could include utilising analysis software to search massive archives of data for specific keywords or file types, as well as procedures for retrieving files that have been recently deleted. Data tagged with times and dates is particularly useful to investigators, as are suspicious files or programmes that have been encrypted or intentionally hidden". A detailed information on this has been further extracted from NUO (2017, n. p.):

> Analysing file names is also useful, as it can help determine when and where specific data was created, downloaded, or uploaded and can help investigators connect files on storage devices to online data transfers (such as cloud-based storage, email, or other Internet communications). This can also work in reverse order, as file names usually indicate the directory that houses them. Files located online or on other systems often point to the specific server and computer from which they were uploaded, providing investigators with clues as to where the system is located; matching online filenames to a directory on a suspect's hard drive is one way of verifying digital evidence. At this stage, computer forensic investigators work in close collaboration with criminal investigators, lawyers, and other qualified personnel to ensure a thorough understanding of the nuances of the case, permissible investigative actions, and what types of information can serve as evidence.

Step 5: Documenting and Reporting

Critical to digital forensic investigation, like any other investigations, is proper and detailed documentation and reporting of the processes involved or steps taken to accomplish a task. Of particular interest to computer forensic analysts is to keep accurate and complete records of information or data, such as software and hardware specifications. Evidence of accuracy in documentation and sample (potential evidence)

collection and related activities or processes involved in the investigation is also necessary. These include documenting and reporting the scientific techniques adopted in assessing "system functionality and retrieving, copying, and storing data, as well as all actions taken to acquire, examine and assess evidence. Not only does this demonstrates how the integrity of user data have been preserved, but also ensures that proper policies and procedures have been adhered to by all parties" (NUO, 2017, n. p.).

The documenting and reporting phase involves providing an in-depth account of the steps throughout the forensic investigation processes, taking into specific consideration the digital evidence recovered, how they were assessed, acquired and examined, and the conclusion reached based on the findings of the investigation and the scientific evidence uncovered. The whole essence of digital forensic is to acquire and analyse data and then reveal results, evidence that meet ethical and legal standards. This is why accurate and detailed documenting and reporting of actions connected to digital evidence/data and their handling and processing is paramount, for anything short of and contrary to these may possibly compromise the validity and reliability of both the evidence and the case under litigation. Recently, the use of Artificial Intelligence (AI)—"computational models of human behaviour and thought processes that are designed to operate rationally and intelligently" (Maras, 2017, p. 7) in producing results that are trustworthy is making headway in forensic science and/or investigation.

Conversely, the use of AI may not be successful in all the steps or stages involved in computer forensics. Take the analysis phase, and ultimately its presentation, for instance, the results produce by AI could be trustworthy but may pose serious analytical problem. Experts may find it particularly difficult to give accurate account of how the results were generated and conclusion reached, and this violates both technical and legal ethical requirements for digital forensic investigation. In view of that, since 'hindsight is always wiser than foresight', human intelligence/assistance is needed to complement artificial intelligence in digital forensic studies, beginning from the first phase through to the last.

Digital forensic experts must chronicle all the course of action pertaining to a particular event or case in a protected computerised format and stored in designated files and dockets. Doing this is to further guarantee the genuineness of any evidence, since the archived digital documents and records contain the 'why', 'when', 'where', and 'how' the computer evidence was uncovered. Also arising from this is the fact that cybersecurity and legal experts stand to verify the legality of any computer evidence presented in a court of law by comparing "the

investigator's digitally recorded documentation to dates and times when the data were accessed by potential suspects via external sources" (NUO, 2017, n. p.).

3.1 Controversies Surrounding Forensic Investigations and Evidence in Court

The criminal justice system depend upon the outcomes of forensic investigations and digital evidence to determine guilt or innocence, convict or acquit the accused standing trial in the court of law. Both physical evidence samples (e.g. hairs, fingerprints, DNA, fibres, arms and ammunition, footprint, and blood, saliva and other body fluids) and digital evidence (information and data obtained from computers and/or other electronic devices which can be processed, investigated forensically to establish a case) are used to prove or disprove cases, but they are not without controversies. They have caused a number of wrongful convictions or faulted and considered inadmissible for not being 'forensically sound' (lack legal validation, reliability and integrity) and upholding 'chain of custody' or other forensics principles and procedures not followed. Consider the cases below:

Case 1: Culled from Arshad, H.; Jantan, A. B. & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientificvalidation of digital evidence. *Journal of Information Processing Systems, 4*(2), 346-376.

> In a recent study of 100 random digital forensics lawsuits [in the United States, US], 10 of these cases claimed errors in data collection and analysis with only two of these cases reversed (Cole, Gupta, Gurugubelli, & Rogers, 2015). Incorrect output and a wrong timestamp were blamed on the forensic software being at fault. Furthermore, the contamination of evidence during examination was cited. Another 13 cases appealed for miscalculation in sentences and sentence enhancement, and from among these claims, six were proven to be valid in court. In this regard, the State of Florida v. Casey Anthony (2011), the murder trial of a 2-year-old girl, is an example where false forensic evidence was offered. The forensic software used to search for the term 'Chloroform' reported that the word was cited 84 times by the primary suspect while it was only once (Eckelberry, Dardick, Folkerts, Shipp, Sites, Stewart & Stuart, 2007) mentioned, with the erroneous data, proving to be a severe setback for the prosecution.

Case 2: Culled from Kaufman, R. (2017, February 10). Forensic science controversies. *CQ researcher*, *27*, 121-144. Retrieved from http://library.cqpress.com/. Accessed 8 February, 2020.

> Nearly 2,000 people have been exonerated in the past two decades according to the National Registry of Exonerations—a database of all known exonerations since 1989 run by the Newkirk Center for Science and Society at the University of California, Irvine, the University of Michigan Law School and Michigan State University College of Law. And in more than 400 of those cases, flawed or misleading forensic evidence had helped convict them (see The National Registry of Exonerations in http://tinyurl.com/7x2efzu). "Traditional forensics put these people in prison in the first place," says Brandon Garrett, a University of Virginia Law Professor and a member of the AdvisoryBoard of the National Registry of Exonerations who wrote *Convicting the Innocent: Where Criminal Prosecutions Go Wrong.* "People came in and said, 'The evidence absolutely matches the defendant; nobody else could have left that print.' A lot of the science was either exaggerated … or inaccurately presented."

Case 3: Culled from Kaufman, R. (2017, February 10). Forensic science controversies. *CQ researcher*, *27*, 121-144. Retrieved from http://library.cqpress.com/. Accessed 8 February, 2020.

> In 2004, the FBI erroneously matched the fingerprint of a U.S. citizen with prints found at the scene of a train bombing in Madrid, Spain, carried out by Islamic extremists (see FBI apologises to lawyer held in Madrid bombings, The Associated Press, NBC News, May 25, 2004, http://tinyurl.com/j49k8ed). A government review found that the FBI had allowed its examiners to know personal information about the suspect—that he was Muslim—and to switch back and forth between his print and the print found at the scene in a way that allowed examiners to minimise differences and magnify similarities (see A Review of the FBI's Handling of the Brandon Mayfield Case, Oversight and Review Division, Office of the Inspector General, March 2006, http://tinyurl.com/zz9q565).

Case 4: Culled from Kaufman, R. (2017, February 10). Forensic science controversies. *CQ researcher*, *27*, 121-144. Retrieved from http://library.cqpress.com/. Accessed 8 February, 2020.

In 2012, SantaeTribble of Washington, D.C., was exonerated for murder and armed robbery after 28 years in prison. He had been convicted after an FBI examiner said he had microscopically matched Tribble's hair to 13 strands found at the scene. Subsequent DNA testing revealed that none of the hairs were Tribble's and that one belonged to a dog (see Hsu, 2016).

> The Tribble case, along with that of Kirk Odom—another D.C. man, who was convicted of rape, sodomy, armed robbery and first-degree burglary, also on hair evidence—triggered a massive post-conviction review of 2,500 cases in which the FBI's lab had provided hair-matching evidence. So far, FBI examiners have been found to have provided flawed testimony in over 95 percent of 268 cases. Of these, 32 defendants had been sentenced to death, 14 of whom were executed or died in prison (Hsu, 2015).
>
> Forensic mistakes can have devastating effects on the lives of the wrongly convicted. Tribble was exonerated in 2012 at the age [of] 51 after spending more than 26 years in prison, where he contracted hepatitis C and HIV from heroin use (Tribble and his attorneys said he was clean when he entered the system). Prison, according to Tribble's lawyers, who sued the District of Columbia for restitution, "ruined his life, leaving him broken in body and spirit and, quite literally, dying" (Strengthening Forensic Science in the United States: A Path Forward, Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, August 2009, http://tinyurl.com/ykpscj8).
>
> In 2016, a D.C. Superior Court judge ordered the city to pay Tribble $13.2 million—one of the largest such awards the District of Columbia has been ordered to pay. Tribble's prognosis, however, is not good. Doctors say he may not live past 2019 (National District Attorneys Association Slams President's Council of Advisors on Science and Technology report, National District Attorneys Association, September 2, 2016, http://tinyurl.com/j7ppnh3).

Case 5: Culled from Kaufman, R. (2017). Forensic science controversies. *CQ researcher, 27,* 121-144. Retrieved from http://library.cqpress.com/. Accessed 8 February, 2020.

In 2013, David Camm of Georgetown, Indiana, was exonerated of murdering his wife and children after DNA found at the scene was linked to the real killer. Blood-spatter experts had disagreed on whether the blood found on Camm's shirt proved he was near his daughter when the gun went off, or were 'contact stains' produced when Camm tried to pull his son's body out of the car where he was found. A forensic biologist who testified for the defence said "people who are not scientists" had rendered most of the earlier opinions (Kircher, 2013).

In Nigeria, there also exists controversies surrounding the acceptability of forensic investigation reports and digital evidence. This is because the Repealed Evidence Act 1945 did not clearly and specifically authenticate the admissibility of digital evidence. A working example is in FRN vs Fani-Kayode, where the issue of electronically generated evidence was raise when the Federal High Court rejected a certified true copy of the computer-generated Statement of Account, but the Court of Appeal later overruled the decision. Another controversy occurred in Nuba Commercial Farms vs NAL Merchant Bank Ltd (2001), where it was held that a Statement of Account produced by a document obtained electronically by a computer is not admissible under the Evidence Act. The same decision was reached in UBA Plc vs Abacha Foundation for Peace and Unity (Danladi, 2014 cited in Hussien, Sarki, & Lalu, 2017).

However, following the enactment of Evidence Act 2011 and the Cybercrime Act 2015, all investigation reports and digital evidence that met legally approved standards are now admissible in all Nigerian courts. This development in our legal system will, to a large extent, address the controversies. For instance, Section 84(1) of the Evidence Act 2011 states, inter alia, "in any proceeding, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it (is shown) that the conditions in Section 2 are satisfied in relation to the statement and computer in question". These conditions (see pp. 28-29 of Evidence Act 2011) are:

1. That the document containing the statement was produced by the computer during a period over which the computer was used regularly to store a process information for the purpose of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual;
2. That over that period there was regularly supplied to the computer in the ordinary course of those activities information of

the kind in the statement or of the kind from which the information contained is derived;

3. That throughout the material part of that period if the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its content; and
4. That the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of the activities.

SELF-ASSESSMENT EXECISE

i. ------ is defined as the standards and best practice guidelines for cybercrime and forensic investigation in relation to digital evidence handling.
   a. Forensics
   b. Cyber forensic
   c. Ethical issues
   d. Legal proceedings

ii. The acronym 'ISFCE' stands for ------
   a. Information System Functional Computer Experts
   b. International Society of Forensic and Cybercrime Experts
   c. Indexing Standards for Forensic Computer Education
   d. None of the above

iii. Which of these tools is used for computer forensic investigation?
   a. Hardware
   b. Disc
   c. EnCase
   d. Drive

iv. ------- is a customised version of the Knoppix live Linux CD used as an Incident Response and Forensic Tool.
   a. Helix
   b. Ilook
   c. Parabeen
   d. Sector Inspector

v. Two major approaches for handling a cybersecurity incident are ---- and ------
   a. Retrieval and chain of custody
   b. Extraction and storage
   c. Incident and documentation
   d. Recover quickly and gather evidence

vi. Evidence admissibility requires ----- and -----
   a. Legal and technical procedures
   b. Investigation and legal procedures
   c. Ethical and legal procedures

d. Searches and seizures

vii. The process by which investigators preserve the crime or incident scene and evidence throughout the life cycle of a case is called ----

a. Preservation
b. Cybersecurity strategies
c. Chain of custody
d. Evidence retrieval

viii. ------- involves producing a duplication of copy of digital device's content without altering or compromising the integrity.

a. Duplication
b. Imaging
c. Recopying
d. Write blocker

ix. Wireshark was formerly known as ------

a. Ethereal
b. Text2Hex
c. SBMD5
d. RootkitRevealer

x. Who invested Stegdetect?

a. Craig Wilson
b. Sanderson Forensics
c. Byce Cogswell and Mark Russinovich
d. Niels Provos

4.0 CONCLUSION

This particular module discussed the tools used for computer forensic examination. It addressed ethical issues that could contradict electronic evidence and renders it inadmissible in court if not properly followed or observed. Different sets of digital evidence are handled or processed by cybercrime investigators and digital forensic professionals. Complete compliance, adherence to national policies and international best practice guidelines is imperative. On the other hand, any electronically generated evidence that does not conform or meet the stipulated technical and legal requirements is prone to cause controversies during legal proceedings and consequent wrongful conviction.

5.0 SUMMARY

The strengths and weaknesses of digital forensic investigations and evidence have been assessed. From the discussion, the latter (advantages) outweighs the latter (disadvantages); it is established that the act of forensic investigation generally is usefulness and necessary, as it helps to unravel complex crimes and criminality. With the right forensic tools and their proper application, victims and their offenders are identified for either treatment or punishment, which ordinarily would not have been possible without forensic science. The aim of applying science to law, forensics, is to guarantee proficiency in proving and/or disproving facts, identifying the right perpetrator of crime, and then determining guilt or innocence.

6.0 TUTOR-MARKED ASSIGNMENT

Critically review the five steps for conducting forensic investigations according to Norwich University Online.

7.0 REFERENCES/FURTHER READING

Antwi-Boasiako, A. & Venter, H. (2017). A model for digital evidence admissibility. In Peterson, G. & Shenoi, S. (Eds.), *Advances in Digital Forensics* (pp. 23-38). Carolina: Carolina Academic Press.

Arshad, H.; Jantan, A. B. & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientificvalidation of digital evidence. *Journal of Information Processing Systems, 4*(2), 346-376.

Conlan, K.; Baggili, I. & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, *18*, 66-75.

Hussien, M. D.; Sarki, Z. M. & Lalu, A. U. (2017). Forensic science, electronic evidence and cybercrime prosecution in Nigeria. In Ndubueze, P. N. (Ed.), *Cyber criminology and technology assisted crime and control: A reader* (pp. 367-382). Zaria: Ahmadu Bello University Press.

Kaufman, R. (2017, February 10). Forensic science controversies. *CQ researcher*, *27*, 121-144.

Lissitzyn, C. B. (2008). *Forensic evidence in court: A case study approach*. Durham, NC:

Maras, M. (2014). *Computer forensics: Cybercriminals, laws, and evidence*. Retrieved from https://www.unodc.org/e4j/data/_university_uni_/computer_forensic_criminals_laws_and_evidence.html? Accessed 4 February, 2020.

Nigeria Police Annual Report. (2010). *The Nigeria Police Annual Report*. Ikeja, Lagos: "F" Department and Nigeria Police Printing Press, FHQ annex.

Norwich University Online. (2017). *5 steps for conducting forensic investigations*. Retrieved from https://online.norwich.edu/academic- programs/ resources/5-steps-for-conducting-computer-forensics- investigations. Accessed 2 February 2020.

Palmer, G. (2001). DFRWS technical report: A road map for digital forensic research. *Digital Forensic Research Workshop*. Utica, New York.

United Nations Office on Drugs and Crime. (2019). *E4J university module series: Cybercrime*. Retrievedfrom https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/basics-of-computing.html. Accessed 20 December, 2019.