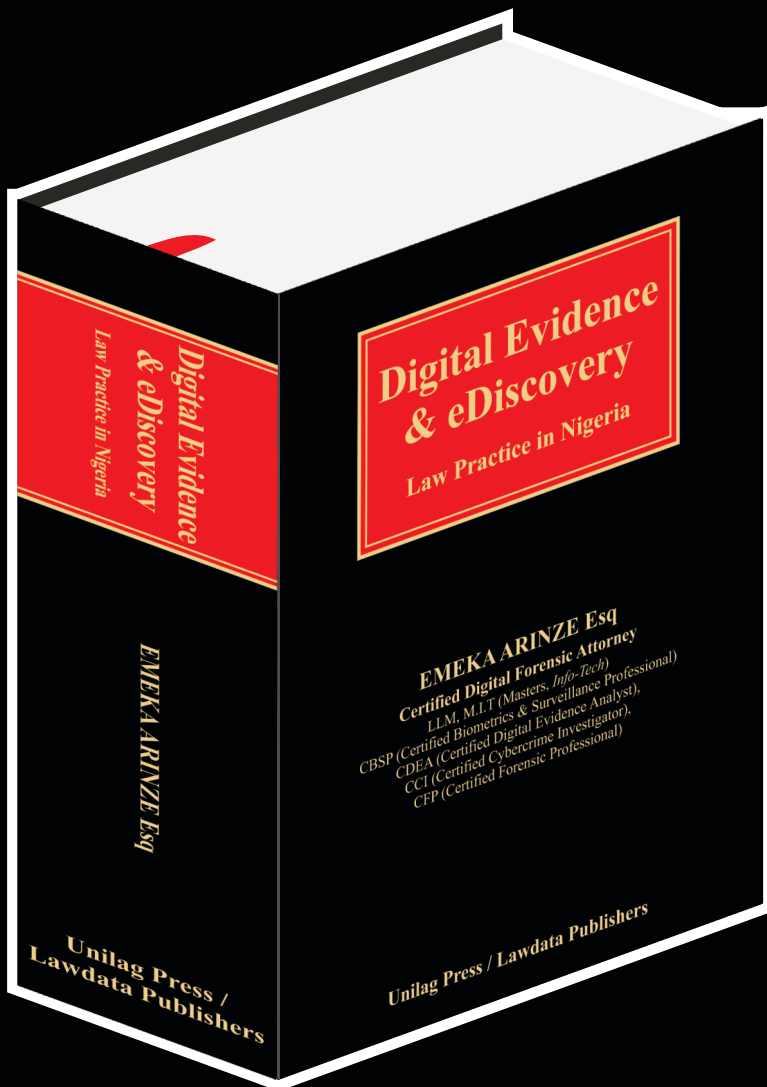


# DIGITAL EVIDENCE & EDISCOVERY LAW PRACTICE IN NIGERIA

Electronic Evidentiary Tool For the 21st Century Law Practice

## BROCHURE



Incorporating Online Training Portal in Digital Evidence & eDiscovery Law Practice for the bar and the bench in Nigeria

The book ePlatform is available online @ [www.godigital.ng](http://www.godigital.ng) on any web browser and also available as mobile app for Android in Google Play Store and iPhone in Apple Store.



The Access Code to the ePlatform as contained on the inside front cover of the book is shown below.

**THIS Book Access Code**  
Book Identification (ID)

**2265 5550 0021 9966**

Secures your Entry into the  
Book ePlatform

@  
[www.godigital.ng](http://www.godigital.ng)

Convended and Delivered by

**Digital Evidence &  
Cyber Forensic Institute,  
Nigeria**

# WELCOME

## Message from the Author

On behalf of all employees of WhiteHall Solicitors, Digital Evidence & Cyber Forensic Institute and Lawdata Communication Solutions Ltd I extend our warmest regard to you all as we bring on board the book titled **Digital Evidence & eDiscovery Law Practice in Nigeria**, through this brochure.

It is undeniable that technology in the last decade has disrupted the practice of law. Data involving smart phones, apps, iPads, cloud capabilities, e-discovery, litigation preparedness, advocacy, and even artificial intelligence are now regular features in our courts. No wonder in the review of the book, International Commentary on Evidence, Deirdre M. Dwyer, opined:

*“It is self-evident that as our society makes increasing use of electronic devices, such as computers and mobile phones, so the evidence that we rely on in litigation, both civil and criminal, will be increasingly electronic in nature. But central to this increasing use of electronic evidence are fundamental technical and legal questions about the quality of that evidence and the circumstances under which it can be obtained and then admitted into court.”*

This statement, anchored on the digital dynamics of the 21st Century, no doubt underpins the essence of this book. Its primary objective is geared towards developing analytical skills for the Bar and the Bench to meet the challenges of legal practice inherent in the new world legal order. Given the avalanche of electronic data that pervade the digital ecosystem, and their concomitant interest in litigation, no 21st century trial lawyer is likely to succeed without the knowledge of electronic evidence and eDiscovery methodology. The Bench also is not an exception.

This brochure introduces the salient points in the book with a view to helping lawyers and judges understand that they have to deal with DATA, (not just DOCUMENTS) in their native locations and forms in order to be effective in client representation and dispensation of justice.

The brochure brings into focus, in a summary form, the content and expectation of the book. That is, its general content; the foreword (written by the former Chief Justice of Nigeria, Justice Walter Onnoghen); and its most critical element - the use of the book as an electronic tool.

It is, therefore, with great pleasure that I welcome you all on board as we begin our journey into the world of digits and its versed terrain of essential evidentiary tools of the digital age.



**Emeka Arinze Esq.**  
WhiteHall Solicitors  
www.whitehallsolicitors.com  
arinze@whitehallsolicitors.com  
emekaarinze12@yahoo.com  
Tel. 08162907894, 08033050301



Editor-in-Chief  
**Mrs Anastasia Arinze**  
B.A. (Hons) (English)

Publisher  
**Lawdata Communication Solutions Ltd.**

Enquires to  
editor@lawdt.com

Visit us on



www.godigital.ng  
info@godigital.ng

Contact us

**Digital Evidence & Cyber Forensic Institute**

13b Gilbert Odior Street,  
Thomas Estate, Lekki-Epe  
Express Way, Ajah, Lagos.  
info@de-cfi.com  
www.de-cfi.com  
0903 434 8127

**Lawdata Communication Solutions Ltd.**

Flat 4 Block A No 1  
Kumasi Crescent, Wuse II  
Abuja (FCT) Nigeria  
info@lawdt.com  
www.lawdt.com  
0814 544 0567

## About The Author

Emeka Arinze Esq. LL..B (Hons), B.L, LL.M, M.I.T (Info-Tech), CBSP, DEA, CCI, CFP

Emeka Arinze Esq., is the first Nigerian lawyer to be dual qualified in Law and Forensic Technology. Called to Nigerian bar in 1983, he holds a Masters' degree (LL.M) in law of the University of Lagos, Nigeria and a Masters' degree in Information Technology (with emphasis on forensic technology) of the University of Lagos, Nigeria.

In 2006 Emeka Arinze attended a certificate course on Cyber Crime & National Security organised by NACETEM, Obafemi Awolowo University, Ile-Ife., and was awarded a certificate on Cyber Crime & National Security upon completion of the course.



In 2006, Emeka Arinze was trained by a Canadian based company; [Data & Scientific Systems Inc on Data Intrusion Detection & Prevention technique, featuring two-factor authentication process that incorporates eToken Authenticators, SafeWord Authenticators, SafeNet iKey USB Token & Smart Card.](#) These processes enable secure PKI implementation, secure access to the web, e-mail, digital credentials, encryption and decryption capabilities, as well as software authentication and single sign-on solutions.

In 2008, Emeka Arinze attended an international training conference in Digital Evidence in London. The training was accredited by the Law Society of England and the Bar standards. It was organised by MIS Training Institute, London in partnership with and under the guidance of Stephen Mason, a Visiting Research Fellow, Digital Evidence Research, British Institute of International & Comparative law. The area of coverage in the training include, [eDiscovery, electronic evidence integrity, trustworthiness, reliability and admissibility procedure, electronic signature, search & seizure of digital evidence in civil and criminal procedure, tendering & production of digital evidence, Biometric issues and evidence handling, video footage analyses, digital evidence practice in other jurisdictions etc.](#) He was awarded a Certificate in Digital Evidence upon successful completion of the program.

In furtherance of the understanding of the dynamics of the Internet Technology and its convergence with the law, in 2010, Emeka was admitted for a course on Internet & the Law at the University of Cape Town, South Africa. Upon a successful completion of the course, he was awarded a certificate by the University of Cape Town, South Africa on Internet and the Law.

Having acquired the basic academic and theoretical background in forensic Technology, the need for certifications in the various areas of Digital Forensic Technology becomes imperative. Consequently, he was trained for certification in [Biometrics & Surveillance, Digital Evidence analyses, cybercrime investigation and digital forensics at various institutions in India from 2010 through 2013.](#)

## ...About The Author

Emeka Arinze, after a successful completion of training on specific areas of Digital Forensics conducted by Asian School of Cyber Law, Mumbai, India and after successfully completing the examination administered by Asian School of Cyber Law and Data Techno Solutions Pvt, India and having obtained an aggregate score of 73% was duly certified in April 2013 as follows;

CFP (Certified Cyber Forensic Professional)

CCI (Certified Cyber Crime Investigator)

DEA (Certified Digital Evidence Analyst)

In addition to the above certifications, Emeka Arinze is also a [Certified Biometrics & Surveillance Professional, CBSP](#). He was trained and certified in Biometrics & Surveillance by an Indian Academy as a Biometric and Surveillance Professional. The training and certification have the support and approval of Indian Institute of Technology, Bombay, KIIT University, Bhubaneswar, India (formerly Kalinga Institute of Industrial Technology), The National Skill Development Corporation (NSDC) a Public Private Partnership (PPP) set up to facilitate the skill development in India and Larsen & Toubro Limited (L&T) Indian multinational conglomerate.

Consequent upon these certifications, Emeka Arinze was inducted as a member into the prestigious [Asian Network of Professionals and Association of Digital Forensic Investigators, India](#).

Over a decade, Emeka Arinze has been responsible for training of lawyers and judges at the Institute of Advanced Level Studies (NIALS), Lagos on Digital Forensic Advocacy and related fields.

Emeka Arinze has had the opportunity of providing forensic leads in cases bordering on election petition at various Election Petition Tribunal in Nigeria (from 2011 to 2015), such cases as led by Chief Wole Olanipeku SAN, Prof A A Utuama, Dr Alex Izinyon SAN, Chief Adebayo Adenipekun SAN, Chief E.L Akpofure SAN, Mr Ken Mozie SAN, Mr E. Ohwovoriole SAN, Mr Tayo Oyetibo SAN, Chief Kalu Umeh SAN (the Attorney General of Abia State, Nigeria), Dr. Livy Uzoukwu SAN, Chief Chris Uche SAN, Dr. Mike Ozekhome SAN, Chukwuma-Machukwu Umeh SAN, Dr. Mrs. V. J. O. Azinge SAN, Olalekon Ojo SAN, Emeka Okpoko SAN, Kabiru T. Turaki SAN, etc.

And most recently in 2018, [Emeka Arinze provided forensic expert opinion/report, demonstrating the possibility of Voice \(biometric\) Impersonation at the National Judicial Council Investigative Panel Against Justice Akon Ikpeme of the Cross River State Judiciary, sequel to the petition of the Civil Society Network Against Corruption and Senator Smart Adeyemi respectively. Emeka Arinze was led in evidence by Mr Mba Ukwani SAN, Mr Emeka Ofordile SAN, Mr Abdul Ibrahim SAN and Mr Tawo E Tawo SAN.](#)

Satisfied with the said forensic demonstration of voice impersonation by Emeka Arinze, the National Judicial Council Investigative Panel acquitted the said Justice Akon Ikpeme of all allegations as made out by the Civil Society Network Against Corruption and Senator Smart Adeyemi respectively.

# The Book Foreword

Written By  
**Hon. Mr. Justice Walter S. N. Onnoghen, GCON**  
**The Honourable Chief Justice of Nigeria**  
**November, 2018**

There is no-gainsaying that technology has ushered in a paradigm shift in the way we think and about how legal meanings are disseminated and construed. Even our most cherished existence and contacts with reality are now technologically mediated and constructed. Within a span of two decades, the practice of discovery of writings, recordings, photographs, and other non-testimonial evidence in both criminal and civil cases in our courts has transformed from one that was based almost entirely on the manual retrieval, review, and production of tangible documents by counsel to one that is almost entirely dependent on accessing, searching, reviewing, and producing digital or computer-generated information.

The "digital explosion" has required a more fundamental change on how counsel and judges must think about digital evidence and eDiscovery in legal proceedings. While the digital natives of the legal profession typically have greater knowledge and less phobia regarding what is needed to engage in what has come to be known as "e-discovery," there are many counsel and judges of our time who look at the digital process with concern, if not fear and loathing.

Part of the problem lies with not knowing where to begin to develop the knowledge and experience needed to survive in the daunting new world of digital evidence and e-discovery. Though their technical proficiency has not matched the pace of the increased role that technology plays in an interdisciplinary global environment, the bar and the bench cannot abdicate their responsibilities due to ignorance of the current technology as they impact on the modern law practice. The bar and the bench must remain accountable for rendering competent legal services to the client and the effective dispensation of justice respectively.

“*One of the compelling points of this book is that the author writes from the vantage point of law and forensics, having been dual qualified*”

The book, Digital Evidence & eDiscovery Law Practice in Nigeria is a timely intervention to address this challenge. The author has opined, "as lawyers and judges, we cannot walk away from the overwhelming majority of the evidence that may be lurking in the computer hard drives, networks and other devices. Not having digital discovery skills is a ticking time bomb in the 21st century law practice. A pervasive lack of knowledge about electronic data, coupled with experience grounded exclusively on paper discovery, makes it hard for lawyers and judges to meet the challenges of digital data discovery. We must, therefore, learn to master electronic discovery and at its extreme, exploit its powerful sub-discipline, digital forensics". I agree no less with this postulation. Counsel and the court must therefore stay abreast of changes in the law and its practice and understand the benefits and risks associated with relevant technology; and in addition to their legal expertise, must also have enough knowledge in different areas

“ *Emboldened by the quality of scholarship demonstrated, and the convergence of law and forensic technology brought into focus by the author, I commend this book as a critical resource to the bar and the bench respectively, as they confront eDiscovery and evidentiary issues posed by electronically stored data in the course of proceedings in our courts.* ”

of technology and forensics to enable them identify issues, understand concepts, contribute to teams and connect ideas across disciplines. Above all, every lawyer and the court need basic knowledge of how the Internet works; how computer systems, tools and storage functionality are preserved; how digital forensic investigations are conducted; understand forensic expert evidence and a host of other electronic dynamics relevant to the 21st century litigation.

One of the compelling points of this book is that the author writes from the vantage point of law and forensics, having been dual qualified. The book, written in a conversational style, while keeping the commentary broad and all inclusive, is divided into five parts, to wit: digital evidence; eDiscovery law practice; digital forensic investigation, prosecution and defence; expert witness and forensic evidence and finally, precedents and landmark cases from foreign jurisdictions. Sprinkled throughout the book are very helpful references to cases, secondary sources, and other materials fully automated, thereby giving the book depth beyond its relative brevity. A quick look at the table of contents reveals an impressive inventory of the most important digital evidence and e-discovery topics of the day. Like a well-designed website, it is informative, interesting and easy to navigate, providing up-to-date practical information that would impact on the lawyers' efficiency to effectively represent clients in a world meshed in digital technology, eDiscovery processes and the basic understanding of forensic expert evidence.

Emboldened by the quality of scholarship demonstrated, and the convergence of law and forensic technology brought into focus by the author, I commend this book as a critical resource to the bar and the bench respectively, as they confront eDiscovery and evidentiary issues posed by electronically stored data in the course of proceedings in our courts.



**Hon. Mr. Justice Walter S. N. Onnoghen, GCON**  
**The Honourable Chief Justice of Nigeria**  
**November, 2018**

## The Book - *Digital Evidence & eDiscovery Law Practice in Nigeria*

Evidentiary issues raise certain fundamental questions on the evolution of digital evidence. It is obvious that no matter how knowledgeable a digital forensic expert (not also trained as a lawyer) engaged as an expert in providing expertise on technical issues in court, he cannot conduct an examination-in-chief, cross-examine a witness or re-examine a document custodian or computer forensic expert on the other side. This is the province of the lawyer. For lawyers to engage in effective examination or cross examination of such expert witness in court, they must as a matter of necessity make effective effort towards understanding client's use of technology, electronic data dynamics, methods, policies and procedures inherent in managing electronically-stored information (ESI). The lawyer, at all-time material, should be prepared to defend his introduction of computer evidence against all objections and attack such digital evidence produced by opposing counsel where expedient. A working knowledge of the computer, the evidence it can generate, and the evidentiary questions raised, prove invaluable for the bar and the bench in today's rapidly changing and increasingly automated society.

“*The 21st century bar and bench must possess the “I” shaped and “T” shaped quality skills. The “I”-shaped professional is highly versed in a specific area of expertise, whilst the “T”-shaped professional has broader skills and knowledge and learns by linking up different perspectives from different specialties. Although the bench and the bar have deep legal expertise, they must also have the ability to collaborate across disciplines such as technology and forensics.*”

For the bar and the bench to fit into the emerging concept of digital evidence and eDiscovery and explore the potential knowledge inherent in digital data in streamlining the pre-trial and trial processes, they must in addition to their earlier legal training acquire skills across relevant disciplines. The ability to apply skills across disciplines comes handy anywhere problem solving is required. To be relevant in this dispensation, the bench and the bar must have basic knowledge of adjacent and connecting fields so as to readily adapt and address the novel and complex problems that often arise. Therefore, the 21st century bar and bench must possess the “I” shaped and “T” shaped quality skills. The “I”-shaped professional is highly versed in a specific area of expertise, whilst the “T”-shaped professional has broader skills and knowledge and learns by linking up different perspectives from different specialties. Although the bench and the bar have deep legal expertise, they must also have the ability to collaborate across disciplines such as technology and forensics.

This book (1300 pages) delves into these questions and provides a starting point for further consideration of law of evidence in the current dispensation. To achieve the understanding of the



## *...The Book - Digital Evidence & eDiscovery Law Practice in Nigeria*

technical issues in the convergence of law and technology, the book is divided into five parts, namely: Part A, Digital Evidence; Part B, eDiscovery Law Practice; Part C, Digital Forensic Investigation, Prosecution and Defence; Part D, Forensic Evidence and Expert Witness, and Part E, Precedents and Landmark Cases from Foreign Jurisdictions in Digital Evidence; eDiscovery; Digital Forensic Investigation and Forensic Expert Evidence.

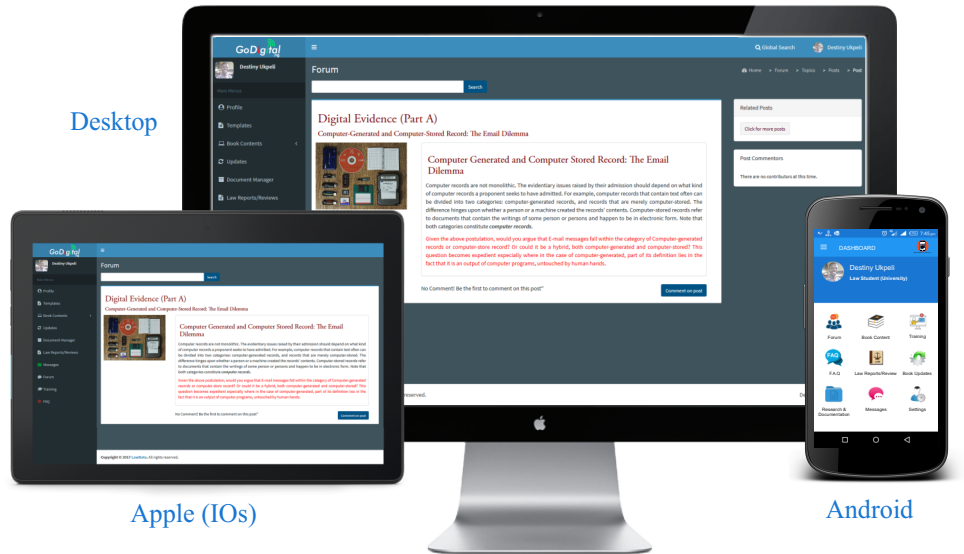
# The Book ePlatform

Technological development have contributed to information explosion and the way we communicate in the 21st century. There is no-gain saying that the world has shifted from manual to automated practices. Authoring books has followed suit, paving way for automated acquisition and dissemination making it readily available to potential users quickly and easily. The book conceived as an electronic tool has an electronic counterpart. Sequel thereto, the content of the book are individually marked and electronically serialized with a definite code item for access to the platform.

The book is automated with Indexing services as a solution to providing current and reliable information to users. The electronic index encompasses not only an index at the back of a book, but also Table of Cases, Statutes and syllabi.

Acquisition of the book gives the user (in compliance with terms of use) access to the ePlatform by implementing the use of the access code located at the inside front cover of the book along with a valid email address of the user. A replica of this is seen at the inside front cover of this brochure.

The ePlatform is available online @ [www.godigital.ng](http://www.godigital.ng) on any web browser and also available as mobile app for Android in Google Play Store and iPhone in Apple Store.



## How to Register & Access the ePlatform

To access the Apps you need to have a godigital.ng account. Having an account is simple. Obtain a copy of the Book, then use the book ID number located at the inside front cover of the book and your valid email address to register.

You can place an order for a book by calling +234 814 544 0567 or visit [www.godigital.ng](http://www.godigital.ng). See the back page for direction.

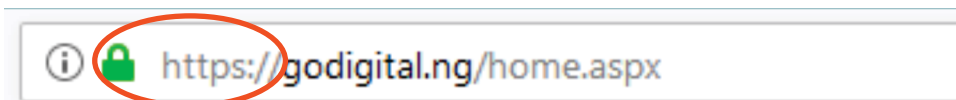
### **To register, having obtained the book, do the following:**

- ◉ Visit [godigital.ng](http://godigital.ng)
- ◉ Click the register menu
- ◉ Enter your book ID number and email address
- ◉ Click Get Started.

### **To register from the Mobile App:**

- ◉ Tap register from the start of the App
- ◉ Enter your book ID number and email address
- ◉ Tap Submit.

## Security of Information Supplied & Traversed on all ePlatforms



We implement a variety of security measures to maintain the safety of your personal information when you enter, submit, or access your personal information.

We implement a 256-bit Secure Socket Layer (SSL) encryption. 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files. What that means is that all supplied sensitive/credit information is transmitted via Secure Socket Layer (SSL) technology. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

## Library Multi-User Account - One-to-Many

The App implements a multi-user account - *One-to-Many System* called the Library Account that is designed for usage in the library of law firms, corporate entities, judicial departments, etc, when same is integrated into their libraries. *GoDigital.ng* only supports one user account per book ID number. However, a *GoDigital Library Account* supports one book ID for multiple user accounts for a minimal fee.

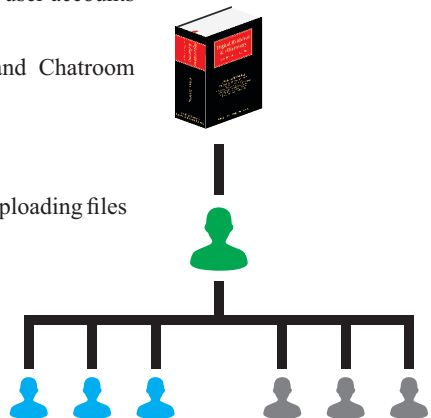
The Library account comes with the Dropbox and Chatroom features as described below for user interaction.

### ⦿ **Dropbox (File Sharing)**

All users connected to a library can share files by uploading files into the Dropbox.

### ⦿ **Chatroom**

Library account users can communicate with one another in real-time through chatting.



# The Book Table of Content

## INTRODUCTION

1. Virtual Environment and the Dilemma of the Judicial Tripod in the 21st Century
  - A. The Judges' Dilemma
  - B. The Lawyers' Dilemma
  - C. The Law Enforcement and Prosecuting Agencies' Dilemma
2. The 21st Century Lawyers and “T-Shaped” Quality Skills
3. Why This Book? Focus and Summary of Its Content
  - A. Part A: Digital Evidence
  - B. Part B: eDiscovery Law Practice
  - C. Part C: Digital Forensic Investigation, Prosecution and Defence
  - D. Part D: Expert Witness and Forensic Evidence
  - E. Part E: Precedents and Landmark Cases from Foreign Jurisdictions in Digital Evidence, eDiscovery, Digital Forensic Investigation and Forensic Expert Evidence

## PART A DIGITAL EVIDENCE

### CHAPTER 1 An Overview of the Law of Evidence: The Pre-Digital Age

1. Background
2. The Earlier Conversation
  - A. The Law of Evidence and Its Essence
  - B. Forms and Nature of Evidence
  - C. Evidence: All about Proof
  - D. The Concept of Document and “Original”
3. Witnesses and Hearsay Rule
  - A. Examination of Witnesses
4. The New Age Conversation

### CHAPTER 2 The Emergence of the Law of Evidence in the Contemporary World: Integrated Circuits and the Concept of Binary Digits

1. Evidence: Why Digital?
  - A. Computer as a Digital Machine
3. The Analog and Digital Phenomenon
  - A. Preference of Digital Technology Over Analog
  - B. Analog-to-Digital Conversion
  - C. Digital-to-Analog Converter (DAC)
4. Digital Evidence as a Product of Integrated Circuits and Binary Digits

## **...The Book Table of Content**

5. Binary Thinking: A Mind-Set of Evidence in the Digital Age

### **CHAPTER 3 Understanding Computer System Components, Functions and Their Evidentiary Values**

1. Hardware Components
  - A. Central Processing Unit (CPU) and Motherboard
  - B. Memory
  - C. Peripherals/Devices
2. Software Components
  - A. System Software
  - B. Applications Software
  - C. Proprietary or Open Software
3. How Computer Inputs, Processes, Outputs and or Stores Data
  - A. Starting the Computer: The Booting Process/Data Input
  - B. Data Processing and Storage
  - C. Data Output
4. The Evidentiary Value of Computer Components in Legal Proceeding

### **CHAPTER 4 Digital Evidence Sources and Their Evidentiary Values**

1. Hard Drives
  - A. Files Created by the Computer User
  - B. Files Protected by Computer User
  - C. Files created by the Computer
2. Networks and Servers
  - A. Home Directories
  - B. File Servers, Shared Drives or Group Shares
  - C. Email Servers
  - D. Internet-Based File Servers or Internet Storage Providers
3. Device Equipment
  - A. Photocopiers
  - B. Keylogger
  - C. Mobile Devices
  - D. Satellite Navigation Devices
  - E. Internet Service Providers (ISP) Records or Log Files
  - F. Backup Devices
  - G. Subscriber Identity Module (SIM)

## **...The Book Table of Content**

### **CHAPTER 5 Admissibility Foundation for Digital Evidence**

1. The Concept of Authenticity
  - A. Alteration of Computer Records
  - B. The Reliability of Computer Programs
  - C. Identifying the Author of Computer-Stored Records
2. The Concept of Relevancy
  - A. Structure of Argument about Relevance
3. Unfair Prejudice
4. The Hearsay Rule
  - A. Hearsay Rule and Computer-Generated Records
  - B. Hearsay Rule and Computer-Stored Records
  - C. Hearsay Rule and Voicemails
5. The Concept of “Original” and the Application of the Best Evidence Rule to Computer Records in the Admissibility Process
6. The Admissibility Foundation Check-list
7. Evidentiary Weight of Electronic Documents

### **CHAPTER 6 Electronic Document and Admissibility Foundation**

1. Introduction: Document Generally
2. Electronic Document
3. The Concept of Signature in Electronic Document
  - A. Electronic Signature: Proof of Electronic Communication under the Evidence Act
4. Computer-Stored and Computer-Generated Records as Documents
  - A. Computer-Stored Document/Records
  - B. Computer-Generated Records
5. Specific Electronic Documents Prone to Litigation and Their Admissibility Consideration
  - A. Electronic Mail (Email)
  - B. Text Messaging (Short Message Service)
  - C. Instant Messaging (Chat Room Discussions)
  - D. WhatsApp: An Online Messaging Service
  - E. Black Box in Legal Proceedings (Evidentiary and Admissibility Issues)
  - F. Digital Radiography (CT scan, MRI and other forms of X-ray documents) as Evidence in Legal Proceedings
  - G. Voice Biometrics and Forensic Evidence

### **CHAPTER 7 Digital Images as Evidence**

1. Introduction
2. Understanding Digital Image
  - A. Digital Image File Format
3. Digital Images and the Concept of “Original”
4. The Nature of Digital Image: Photograph and Video
  - A. Digital Photograph
  - B. Video as Digital Image

## **...The Book Table of Content**

5. Other Special Consideration for admissibility of Digital Image.
  - A. Early Disclosure; Avoidance of Trial by Ambush (Case of Video Data)
  - B. Policy Orientation
6. Objections to the Admissibility of Video and Photographic Images and their Audios
  - A. Objection to the use of video evidence at trial may take the following forms:
  - B. When objection to the use of video evidence is raised, response is usually expected. Response may take the following forms;
  - C. On foundational issues, both parties must bear in mind that at all time material that:
  - D. Parties must acquaint themselves with the materiality of witnesses and the fact they are expected to testify:
7. Useful Tips and Precautionary Steps as Guide when Relying on Video or Digital Photographs for use as Evidence in the Courtroom or to launch a Challenge to Digital Image Admissibility
8. Summary of Instances where Court Can Reject Video Evidence
9. Training of Law Enforcement Officers and Prosecutors in Video Imagery

### **CHAPTER 8 Cellphone Data and Cellular Networks as Evidence**

1. Introduction
2. Key Common Components in all Cellular Phones
  - A. Operating System
  - B. Software
  - C. SIM Card
  - D. SD Cards
  - E. Battery
  - F. Keypad
  - G. Bluetooth
  - H. Caller ID
  - I. Global Positioning System (GPS)
3. Cellular Phone Capabilities
4. Cellular Networks and Channel-Access Technologies
  - A. Global System for Mobile (GSM)
  - B. Code Division Multiple Access (CDMA)
5. Basic Components of Cellular/Mobile Networks
  - A. Base Transceiver Stations (BTS)
  - B. Mobile Station (MS)
  - C. Mobile Switching Centre (MSC)
  - D. Public Switched Telephone Network (PSTN)
6. Call Detail Record (CDR)
7. Cellular Location Evidence and Admissibility Issues
  - A. Placing the Defendant in the Crime Scene
  - B. The Hearsay Rule: Can Cell Phone Records, as kept by the Telecom Service Providers, be classified as Business Records for Purposes of Admissibility?
  - C. Relevance or Otherwise of Cell Site Location Information
  - D. Authentication of Cell Phone Records



## **...The Book Table of Content**

- E. Lay and Expert Testimony in Presentation of Call Detail Record and Cell Site Data in Court
- F. Should a Certificate be produced to Authenticate Cellphone Record for Admissibility?

### **CHAPTER 9 Social Networks and Digital Evidence**

1. Introduction
2. Classification of Social Media Network
  - A. Facebook
  - B. WhatsApp
  - C. Twitter
  - D. Google+
  - E. Wikipedia
  - F. LinkedIn
  - G. Reddit
  - H. Pinterest
  - I. Myspace
  - J. Instagram
3. Impact of the Content of Social Media Data on Criminal Investigation, eDiscovery and Tort Involving Insurance and Personal Injury Cases
  - A. Social Networks and Criminal Investigation
  - B. eDiscovery/Interrogatories
  - C. Tort involving Insurance and Personal Injury
  - D. Tort Involving Defamatory Publication
4. Admissibility Issues in Social Networks
  - A. Gathering and obtaining Evidence from Social Media Networks for Admissibility (Printouts and Screenshots)
  - B. Relevancy Issues
  - C. Authentication Issues
  - D. The Hearsay Rule
  - E. Unfair Prejudice
5. Tips for introducing Social Media Content into Evidence
  - A. Authentication Tips: Preliminary Questions
  - B. Authenticating the Exhibit
  - C. Authenticating Social Media Post
  - D. Tips on Authenticating Tweets

### **CHAPTER 10 Satellite Image (Data) as Digital Evidence**

1. Satellite and Its Constituents
  - A. Treaty on Principles governing Activities of States in Exploration and use of Outer Space, including the Moon, Artificial Earth Satellites and Remote Sensing of Earth from Outer Space by UN
  - B. Global Positioning System (GPS)
  - C. Google Earth Satellite Imagery
2. Privacy and Security Issues in Satellite Imagery (Data)

## **...The Book Table of Content**

3. Technical and Legal Challenges faced by Satellite Imagery as Legal Evidence
4. Foundation for Admissibility of Satellite Imagery/Data
  - A. System Functionality and Authentication
  - B. Chain of Custody
  - C. Manipulation and Reliability Issues
5. Use of Satellite Imagery as Evidence at the International Courts of Justice and other Organisations

### **CHAPTER 11 Electronic Banking and Evidentiary Challenges**

1. What is Electronic Banking?
2. The eBanking Service Delivery Channels
  - A. The Credit and Debit Card System
  - B. Automated Teller Machine (ATM)
  - C. Point-of-Sale Terminal
3. Evidentiary and Legal Challenges in eBanking
  - A. Enforceable Electronic Banking Transactions: Banks and Customer Relationship
  - B. Vulnerabilities of Online Banking System: Weaknesses in the Technology
4. Unauthorised Transfers and Bankers' Liability: The ATM Factor
  - A. The Foreseeability of Crime and the Duty to Exercise Ordinary Care
  - B. Unauthorised Transfers at ATMs Premises
5. Disputed Chip & Pin Transaction: Use of Forensic Evidence
  - A. Validating the Application Transaction Counter (ATC)
  - B. Validating the Cryptogram
  - C. Nature of Dispute and their Inherent Problems
6. Documentation of Electronic Funds Transactions
7. ePayment Dispute Resolution in Nigeria
  - A. Composition
  - B. Terms of Reference
  - C. Objectives of the Arbitration Framework
  - D. Coverage Area of ePayment Dispute Arbitration Framework
  - E. Criteria for admitting Complaints by the ePayment Dispute Arbitration Panel
  - F. ePayment Dispute: Eligibility for Submission to the Arbitration Panel
  - G. ePayment Dispute Liability
  - H. Documents required for ePayment Dispute Arbitration irrespective of Channels
  - I. Administration of the Arbitration Panel
  - J. The Structure of the Arbitration Panel
  - K. Ways for making all Parties Submissive to the Panel
  - L. Sanctions and Enforcement
  - M. Other Matters

### **CHAPTER 12 Legal Issues Specific to Deoxyribonucleic Acid (DNA) Forensic Evidence**

1. Deoxyribonucleic Acid (DNA): An Overview
2. DNA Profile and the Forensics Database

## **...The Book Table of Content**

3. The Creation of National DNA Database: A Case for Legislative Frame Work for Nigeria
4. DNA and Admissibility Issues
5. Foundation for Admissibility of DNA Evidence in Court
  - A. Reliability
  - B. Prejudice
  - C. Chain of Custody
  - D. Laboratory Standards and Best Practice Requirement for Compliance
6. DNA Report: A catalyst in the Hands of The Prosecutor and The Defence Counsel in Criminal Proceeding
8. Presentation of DNA Evidence in Court: Use of Experts

### **CHAPTER 13 Logs as Digital Evidence**

1. What are Log Files/Records?
2. Different Log Types and Their Evidentiary Values
3. Can Log Records be Manipulated?
4. Activities highlighting the Usefulness of Log Records in Litigation Process
  - A. Email Account Activity
  - B. Posting and Deleting Content on the Internet
  - C. Unique Identifiers
  - D. Interstate Commerce
5. Authenticating Log Data for Admissibility
  - A. Best Practices that ensure Admissibility of Log Data

### **CHAPTER 14 Cryptography and Blockchain: The Backbone of Digital Evidence Authentication**

1. Introduction
2. Cryptography
  - A. What is Cryptography?
  - B. Cryptography and Digital Signature
3. Blockchain Technology
  - A. Introduction
  - B. The Blockchain Concept

### **CHAPTER 15 Chain of Custody: It's Application to Digital Evidence**

1. Introduction
2. The Phrase, "Chain of Custody" and Its Documentation
3. Chain of Custody in the Digital Environment
  - A. Ensuring Integrity of Chain of Custody Log
  - B. Chain of Custody and Hardware Components
4. Chain of Custody in Certain eDocument and their Authentication Process
  - A. Audio and Video Files
  - B. Email
  - C. Webpage
5. Party Admitting and Party Objecting to Digital Chain of Custody: What to Watch Out For

## **...The Book Table of Content**

- A. The Admitting Party
- B. The Party Objecting

### **CHAPTER 16 Judicial Notice in the Digital Age**

1. What is Judicial Notice?
2. Technology and Judicial Notice
  - A. Can Courts Take Judicial Notice of The Fact That Computers and Scientific Instruments Work in an Efficient Manner until Proved Otherwise?
  - B. Digital Content that Courts may take Judicial Notice
3. Framework for the Application of Judicial Notice in the Digital Age
  - A. The Legal Framework
  - B. Reliability of the Source
  - C. Bias Consideration

### **CHAPTER 17 System Malfunction and Integrity Violation: A Case for Section 84 of the Evidence Act, 2011**

1. Mechanical Errors
  - A. Environmentally-Induced Errors
  - B. Hardware Failure
2. Software Failure
  - A. Instances of Software Failure in Recent Times
3. Operating System Upgrade
  - A. Insufficient Hardware
  - B. Driver Problems
  - C. Activation Error
4. The Human Error - Factor
  - A. Operating Mistakes
  - B. Input Errors
5. Technological Obsolescence
  - A. Risks Associated with Use of Obsolete Hardware and Software
6. Malware Infection
  - A. Computer Virus
  - B. Computer Worms
  - C. Trojan Horse
  - D. Spyware
  - E. Ransomware
  - F. Adware
  - G. Bot
  - H. Rootkits
7. Other Threats that can Compromise the Function of a Computer
  - A. Cookies
  - B. Bluetooth

## **...The Book Table of Content**

8. Evidentiary Issues in Malware implicated in Criminal Trial: The Case of Trojan, Bots and Adware Defence
  - A. Options available to Prosecution in Rebuttal to Malware Defence: The Case of Child pornography and related offences as Prohibited by Section 23 of the Nigeria Cybercrime Act 2015

### **CHAPTER 18 Evaluation of Section 84 of Nigeria Evidence Act 2011 and A Critique of the Supreme Court Decisions in Kubor v. Dickson and Kubor v. Sylva**

1. Introduction
  - A. Understanding the underlying Technology as a Precursor to Section 84 of the Evidence Act
2. Analysis and Evaluation of Section 84
  - A. Section 84 (1): Admissibility of Statement Contained in a Document Produced by a Computer
  - B. Section 84 (2): Regularly Conducted Activity, Trustworthiness and Reliability of the Computer
  - C. Section 84 (3): Activity Derived from a Networked Device
  - D. Section 84(4): Production of Certificate
  - E. Section 84 (5)
3. Does the Evidence Act Contemplate or Permit the Proof of Electronic Record by Oral Evidence if the Requirements under Section 84(4) of the Act are not complied with? A Critique of the Supreme Court Decision in Dickson v. Sylva
4. The Supreme Court Decision in Kubor v. Dickson with reference to Section 84 (2) and (4) of the Act: A Critique

## **PART B eDISCOVERY LAW PRACTICE**

### **CHAPTER 19 eDiscovery: An Overview**

1. Discovery as a Judicial Process
2. eDiscovery Explained
3. Electronically-Stored Information (ESI): The Subject of eDiscovery
  - A. Forms and Sources of ESI
  - B. Challenges posed by ESI
  - C. Unique Characteristics of ESI as Distinguished from Traditional Paper-based Files

### **CHAPTER 20 The Development of eDiscovery Guidelines, Reference Models/Legal Framework**

1. The Sedona Principles and eDiscovery
2. Electronic Discovery Reference Model (EDRM)
3. Electronic Discovery Best Practices (EDBP)
  - A. Litigation Readiness Activities.
  - B. Cooperation.
  - C. Review.

## **...The Book Table of Content**

- D. Productions.
- E. Evidence

### **CHAPTER 21 An Overview of eDiscovery Development and Application in Different Jurisdictions and Nigeria**

- 1. The United States of America
- A. The 2006 Amendment to the US Federal Rules of Civil Procedure
- 2. Canada
- 3. The United Kingdom
- 4. Australia
- 5. Singapore
- 6. Nigeria

### **CHAPTER 22 Litigation-Readiness Plan: Getting Ready for eDiscovery**

- 1. Early Engagement of an Expert
- 2. Counsels' Initial Appraisal of Clients' Corporate IT Infrastructure and Interview
  - A. Corporate IT Infrastructure: Data Map
  - B. Client Interview

### **CHAPTER 23 The Preservation of Evidence and Litigation Hold**

- 1. Introduction
- 2. The Duty to Preserve Evidence: When does it arise?
  - A. Before the Commencement of Litigation
  - B. After the Commencement of Litigation
- 3. Preserving Evidence through Demand Letter
  - A. Content of Letter of Preservation
- 4. Litigation Hold

### **CHAPTER 24 Pre-Trial Conference and Early Exchange of Computer System Information Pursuant to eDiscovery**

- 1. Introduction
- 2. Pre-Trial Conference/Hearing and eDiscovery
  - A. Meet and Confer
- 3. Early Exchange of Computer System Information

### **CHAPTER 25 Production of Electronically Stored Document**

- 1. Requests for Production of ESI
- 2. Production Formats in eDiscovery
  - A. The Native File Format
  - B. Near-Native Forms
  - C. Image (Near-Paper) Production
  - D. Searchable Text Files
  - E. Paper Production
- 3. Inadvertent Production of Privileged/Confidential Information
- 4. Possession, Custody or Control

## **...The Book Table of Content**

5. Responses and Objections
6. Search for Production ESI
  - A. Index Search
  - B. Concept Search
  - C. Boolean Search
  - D. Fuzzy Search
  - E. Phonic Search
  - F. Synonym Search
  - G. Stemming Search
  - H. Predictive Code/Search
  - I. Multimodal Approach
7. Are Keywords disclosable by Parties in Litigation?
8. Cost Shifting and Cost Sharing Agreements in Production

### **CHAPTER 26 Accessibility and Inaccessibility Issues in the Production of Electronically Stored Information**

1. Introduction
2. Accessible and Inaccessible Electronically Stored Information
  - A. Media-Based Factors
  - B. Data Complexity Factors
  - C. Guidelines to Parties on Accessible and Inaccessible ESI

### **CHAPTER 27 The Principle of Proportionality in Producing Electronically Stored Information in eDiscovery**

1. Introduction
2. The Emerging Concept of Proportionality
3. The Sedona Conference Principles of Proportionality
  - A. The Burden and Cost of Preserving Potentially Relevant Information should be weighed against the Potential Value and Uniqueness of the Information when determining the Appropriate Scope of Preservation
  - B. Discovery should generally be obtained from the Most Convenient, Least Burdensome and Least Expensive Sources
  - C. Undue Burden, Expense or Delay resulting from a Party's Action or Inaction should be weighed against that Party
  - D. Extrinsic Information and Sampling may assist in the Analysis of whether requested Discovery is Sufficiently Important to Warrant the Potential Burden or Expense of Its Production
  - E. Non-Monetary Factors should be considered when Evaluating the Burdens and Benefits of Discovery
  - F. Technologies to Reduce Cost and Burden should be considered in the Proportionality Analysis

### **CHAPTER 28 Spoliation and Sanctions**

1. Introduction
2. What is Spoliation?
3. Preventing Spoliation

## *...The Book Table of Content*

4. Sanctions for Spoliation
  - A. Consideration for Sanction
  - B. Safe Harbour Principles

### **CHAPTER 29 Subject-Specific Sources of Discoverable Electronic Stored Information in eDiscovery**

1. Introduction
2. Databases in eDiscovery
  - A. Structured and Unstructured Data
  - B. General Principles in Database Discovery
  - C. Databases and Their Relevance in Criminal eDiscovery: The Case of Alibi
  - D. Prosecutions Database: The Defence Access
3. eDiscovery and Audio Evidence
  - A. Nature and Sources of Audio Data in eDiscovery
  - B. Preservation, Production/Retrieval and Privileged Issues in Audio Data
  - C. Tools and Reviewing Mechanism of Audio Data
  - D. Strategies for Managing Voice Recordings
4. Matrimonial Dispute and eDiscovery
  - A. Discovery involving Family Computer
  - B. Limitations of Disclosure on Electronic Communications
  - C. Production of Computer Hard Drives and Cell Phone SIM Cards
5. eDiscovery and Financial Services: Banks and Other Related Institutions
  - A. Litigation Readiness Plan, Incorporating CBN Directives: A Case for Document Retention Policy
  - B. Compliance and Audit Procedures
6. eDiscovery in Mergers and Acquisitions (M&A)
  - A. Developing an eDiscovery Checklist for M&A
7. eDiscovery and Metadata
  - A. Preserving and Producing Metadata in eDiscovery
  - B. When to Demand Production of Metadata in eDiscovery
  - C. Production of Metadata and Privileged Information
  - D. Relevance of Metadata in eDiscovery
8. Cloud Computing and eDiscovery
  - A. What really is “Cloud” in this Context?
  - B. eDiscovery in the Cloud: The Potential Benefit
  - C. Cloud Data Storage for Litigators: Disadvantages
  - D. Implementation of eDiscovery Process in the Cloud
9. eDiscovery in Arbitration
  - A. Arbitral Bodies in Nigeria
  - B. Rules or Protocols of Arbitral Bodies Dealing with eDiscovery in Arbitration in Nigeria
  - C. The IBA Rules on the Taking of Evidence in International Commercial Arbitration
10. eDiscovery in Criminal Investigation, Prosecution and Defence
  - A. Background



## ...The Book Table of Content

- B. eDiscovery in Criminal Proceedings in Nigeria: Applicability of Existing Laws
- C. Common Challenges in eDiscovery in Criminal Cases
- D. Management of eDiscovery in Criminal Proceeding: Need for Expert Intervention
- E. The Right Against Self-Incrimination and eDiscovery
- F. eDiscovery of Emails and Text Messages in Criminal Proceeding
- G. When does a Duty to Preserve ESI or Electronic Data Relevant to Criminal Investigation Arises?
- H. Recommended Process for eDiscovery in Criminal Litigation

### **CHAPTER 30 Freedom of Information Act (FOIA) 2011: Access to Information in the Age of Electronic Record**

- 1. Introduction
- 2. Historical Development of Freedom of Information
- 3. Enactment of Nigeria's Freedom of Information Act (FOIA)
- 4. Freedom of Information Act (FOIA) 2011
  - A. The Objective of the Act
  - B. Institutions to which FOIA Applies
  - C. Files and Records subject to FOI Request and Production
  - D. Obligation of the Public Institution to Keep, Organise and Maintain Records
  - E. Right of any Person to Access, Request or Disclose Information
  - F. Information Exempted from Disclosure
  - G. Response to Access Request and Timeline
  - H. Consequences for Refusal to Respond to Request
  - I. Judicial Remedy for Denial of Access to Information
  - J. Implementation of the FOIA and Role of the Attorney-General of the Federation
  - K. Proactive Disclosure Requirements under the FOI Act
  - L. Categories of Records required to be Disclosed Proactively
  - M. Failure to Disclose Records Proactively under Section 2(3) of the FOI Act
- 5. Are States Obligated to Enforce the Freedom of Information Act (FOIA)?
- 6. The use of Technology in Access and Response to Request under the FOI Act with a view to managing its eDiscovery Process
  - A. Background
  - B. Creation and Maintenance of Public Records by Governments and Public Institutions
  - C. Format of Record Keeping and Maintenance
  - D. Access to Public Records in the Same Format Kept and Maintained by Governments and their Agencies
  - E. Where the Records Requested are in the Cloud
  - F. Is Private Email used by Officials of Government Agencies and Public Institutions subject to FOI Act?
  - G. Maintaining Authenticity and Trustworthiness of Electronic Records for Purposes of FOI Act
  - H. Application and Use of eDiscovery Process in the Management of Potentially Responsive ESI under FOI Act

## *...The Book Table of Content*

### **PART C DIGITAL FORENSIC INVESTIGATION, PROSECUTION AND DEFENCE**

#### **CHAPTER 31 The Basic Concepts and Locard Exchange Principle in Digital Forensic Investigations**

1. The Background Concepts
  - A. Forensics and Its Historical Emergence
  - B. Digital Forensics as a sub-division of Forensic Science
2. The Locard Exchange Principle otherwise known as Trace Evidence
  - A. Trace Evidence in Digital Activity Log
  - B. Trace Evidence and Fingerprint Identification
  - C. Trace Evidence in Deoxyribonucleic Acid (DNA) Marching

#### **CHAPTER 32 Investigators, Prosecutors and Defence Counsel Familiarity with Basic Computer Concepts and Resources**

1. Operating System
  - A. Operating System Feature
2. File System Concept
  - A. Inodes
  - B. Hard Links and Symbolic Links
  - C. File Operations
  - D. The Registry Structures
  - E. The Hierarchical Tree Structure
  - F. Variability of the Registry
  - G. How Registry Data is used
  - H. The Boot Process

#### **CHAPTER 33 Locating and Protecting Electronically-Stored Data in Digital Investigation**

1. Deleted Data
2. Hidden/Encrypted Data
3. Device Shielding
4. Renamed Files and Files with changed Extensions
5. Evidence Commonly found on Hard Drives
  - A. Files created by Computer Users
  - B. Files Protected by Computer Users
  - C. Global Position System (GPS)
  - D. Barriers and Signal Jamming

#### **CHAPTER 34 Digital Forensic Investigative Tools**

1. Disk Imaging Tool
  - A. The National Institute of Standards and Technology (NIST)
2. Software Authentication Tool
  - A. National Software Reference Library (NSRL)

## **...The Book Table of Content**

3. Decryption Tools
4. Audit Log File Tool
5. IP Address Tracker
6. Email Recovery Tool

### **CHAPTER 35 Search and Seizure in Digital Forensic Investigation**

1. Introduction
2. Search and Seizure Defined
3. Fundamental Issues for Consideration in Search and Seizure in the Digital Age
  - A. Privacy Issues and Search Warrants
  - B. The Computer and the Warrant Process
  - C. Nature of Search in the Technological Environment
4. Existing Rules on Search and Seizure in Nigeria
5. Applicable Rules on Search and Seizure of Computers and Their Devices in Digital Forensic Investigation in Nigeria
  - A. Explanatory Notes on Section 45 of the Act
6. Description of what to be Seized: Computer System Search
  - A. Laser Printers
  - B. Hard Disk Print Buffers
  - C. Print Spooler Device
  - D. Monitors
  - E. Scanners
7. Digital Property in the Cloud Subject to Search and Seizure
  - A. Drafting a Warrant for Cloud Search and Seizure
8. Affidavit in Support of Warrant for Search and Seizure of Computers
  - A. The Role of the Computer in the Offence
  - B. Description of Technical Information as contained in the Affidavit
  - C. Description of the Role of the Computer in the Offence, where the Computer is an Instrumentality of the Crime
  - D. Search Plan of the Computer used for the Illegal Purpose
9. Further Consideration of Relevant Sections of the Cybercrime Act in relation to Search and Seizure
  - A. Section 45(2)(e) Relating to Use or Cause to use a Computer or any Device to Search any Data contained in or available to any Computer System or Computer Network
  - B. Section 45(2)(f): Use of any Technology to Decode or Decrypt any Coded or Encrypted Data contained in a Computer into Readable Text or Comprehensible Format
10. Exceptions to the Warrant Requirement: Warrantless Searches
  - A. Exigent Circumstances
  - B. The Plain View Doctrine
  - C. Border Searches
  - D. Consent Searches
  - E. Privileged and Confidential Information: The Doctors, Lawyers and the Clergy
11. Offsite Search and Authorisation Request
12. Need for Engagement of Experts in Search and Seizure Operations

## **...The Book Table of Content**

13. Is there Any Permissible Time Period for Examining Seized Media, Imposed by the Nigeria Cybercrime Act, 2015?
14. Acquiring Data for Search and Seizure by Investigators
15. Jurisdiction of a Judge to issue Search Warrant on a Computer System Existing Outside its National Territory
  - A. Mutual Legal Assistance Treaty
16. Basic Tips for Government Agencies for Request for Assistance from the Authority of Foreign Jurisdictions in Investigation, sequel to Search and Seizure
17. Illegally-Obtained Evidence: Improper Search and Seizure
  - A. Effect of Sections 14 and 15 of the Evidence Act 2011 on Illegally or Improperly obtained Evidence

### **CHAPTER 36 Digital Forensic Investigative Methodology and Techniques**

1. The Goal of Digital Forensic Investigation
2. Investigative Framework: Methodology and Technique
  - A. The Technique and Methodology
  - B. Digital Forensics Investigation Framework: The FORZA (FORensics ZAchman) Framework
3. Applicable Principles, Guidelines and Best Practices in Digital Forensic Investigation Technique and Methodology
  - A. UK Association of Chief Police Officers (ACPO): Providing Guidance in Investigating Cyber Security Incidents and Crime
  - B. ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence
  - C. US National Institute of Justice: Electronic Crime Scene Investigation
4. Common Agreement on Methodology and Technique in Digital Forensic Investigation
  - A. Preliminary Issues for Consideration
  - B. Maintaining System/Data Integrity and Chain of Custody
  - C. The Common Areas of Agreement

### **CHAPTER 37 Application of Digital Forensic Investigative Technique: A Case of Money Laundry in Nigeria**

1. Introduction
2. Money Laundry: Its Techniques
3. Criminalising Money Laundry: FATF and Nigeria
4. Digital Forensic Investigation in Money Laundry
  - A. Information Sources in Money Laundry Investigation
  - B. The Application of Digital Forensic Technique in the Investigation
4. Money Laundering and Asset Recovery
  - A. Management of Seized Assets
5. Typical Case Scenario on Money Laundry, Applying Digital Forensic Investigative Techniques
  - A. Tracing and Recovery of Nigeria's illegally Acquired Assets from an individual Assisted

## **...The Book Table of Content**

by the United Kingdom

### **CHAPTER 38 Cybercrime: Evidentiary Issues in Prosecution and Defence in Consequence of Digital Forensic Investigation**

1. Cybercrime and Its Inherent Nature
2. Prosecution
  - A. Powers of Prosecution under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015
  - B. Managing Prosecution in the Digital Age
  - C. Preparing the Witness for Trial
  - D. Prosecution's Anticipation of Defence Reaction to the Charge as Proffered
3. Defence Counsel Obligation
  - A. Defence Cross-Examination of the Prosecution's Witnesses and Reaction to the Forensic Report if any
  - B. Defence Counsel Insistence on the Disclosure of Forensic Report by the Prosecution
  - C. Challenging Evidence as Elicited by the Prosecution: Defence Counsel Familiarity with Tools and Best Practices Used in the Investigative Process

## **PART D EXPERT WITNESS AND FORENSIC EVIDENCE**

### **CHAPTER 39 The Emergence of Expert Witness, the Concept of Expert Opinion and Common Knowledge**

1. Introduction
2. The Concept of Expert Opinion and Common Knowledge
  - A. Distinction between Facts and Opinion
  - B. Common Knowledge and Expert Opinion
  - C. The Constituent of Common Knowledge
3. The Expert Witness
  - A. The Essential Qualities of an Expert Witness
4. Instructing an Expert
  - A. Letter of Instruction
  - B. Jointly Appointed Experts
  - C. Can a Corporation be Instructed/Appointed Expert to Testify in Court?

### **CHAPTER 40 Duties and Responsibilities of Expert Witness**

1. Experts' Duty to the Court
2. Experts Duty to the Body of Knowledge He Professes
3. Experts' Duty to the Client

### **CHAPTER 41 Ethical Issues and Disqualification of Expert Witness**

1. Introduction
2. Conflict of Interest
  - A. Prior Relationship with the Opposing Side that resulted in Access to that Party's Confidential Information
  - B. Expert switching Sides during the Existence of the Dispute

## **...The Book Table of Content**

3. Cognitive Bias
- A. Instances of Bias by Contextual Factors where Forensic Decisions may have been influenced
  4. Engagement of an Expert as both Advisor and Independent Expert

### **CHAPTER 42 The Expert Witness Report**

1. Expert Report: How Defined?
2. Content/Format of Expert Witness Report
  - A. Introduction and Background
  - B. Qualifications
  - C. Description of Material Collection and Methodology
  - D. Description of Method of Analysis
  - E. Questions to be Addressed
  - F. Body of the Opinion
  - G. Copies of Exhibits, Appendices etc.
  - H. Review of the Report
  - I. The Expert's Declaration
3. The Role of Counsel in Preparing/Drafting Expert Report

### **CHAPTER 43 Admissibility of Forensic Expert Evidence in Court**

1. Admissibility Process of Forensic Expert Evidence in Court: The Need for Caution
  - A. Annie Dookhan: A Tragedy of a Kind
  - B. Exonerated by DNA Evidence: The Case of Santae Tribble
  - C. Contamination by Secondary Sources
2. The Gatekeeper Role for the Trial Judge
3. Developing and Evolving Standards of Admissibility of Scientific Evidence
  - A. The Frye "General Acceptance" Standard
  - B. The US Federal Rules of Evidence 702
4. The Standard and Criteria for Evaluating Scientific Evidence for Admissibility: The Daubert Trilogy
  - A. The Daubert Decision
  - B. General Electric v. Joiner
  - C. The Kumho Decision
5. Daubert Decision and Its Influence in other Foreign Jurisdiction
  - A. Canada

### **CHAPTER 44 Digital Forensic Expert Witness in Court**

1. Expert Testimony and the Ultimate Issue
2. Preparing the Expert to Testify
  - A. Counsel Involvement in Preparation of the Expert in Giving Evidence in Court: Any Ethical Issue?
  - B. Taking of Oath or Affirmation to tell the Truth, the Whole Truth and nothing but the Truth
3. Direct Examination (Examination-in-Chief) of Expert Witness
  - A. How to Proceed during Direct Examination
4. Cross-Examination of Expert Witness

## **...The Book Table of Content**

- A. Preparation for the Cross-Examination of Forensic Expert Witness
- B. Developing Questions in Aid of Cross-Examination
- C. Cross-Examination of Expert Witness: Consulting Expert to Assist Counsel
5. Reliability of the Expert Evidence in Court
  - A. Failure to Consider Relevant Data
6. Weight and Probative Value of Expert Evidence
  - A. Questions the Court may consider in evaluating Expert's Methodology with a view to what weight to be attached in favour of or against Admissibility
7. Is Forensic Expert Report/Evidence Binding on Court?
8. Attitude of Court towards the Report of a Team of Experts
9. Can Court Suo Moto call Expert Evidence?
10. Conflict arising in the Report of Experts: How Treated?

### **PART E      Precedents & Landmark Cases from Foreign Jurisdictions in Digital Evidence, eDiscovery, Digital Forensic Investigation & Forensic Expert Evidence**

#### **CHAPTER 45      Stare Decisis and Persuasive Authority: Resort to Foreign Decisions in Digital Evidence and eDiscovery Law Practice in Nigeria**

1. Introduction
2. The Concept of Persuasive Authority: Legal Argument When There Is No Binding Precedent
3. Recent Case Law Development in Digital Evidence and eDiscovery Law in the US, UK and Canada
4. Resort to Foreign Decisions in Digital Evidence and eDiscovery Law Practice

#### **CHAPTER 46      Digital Evidence: Landmark Cases**

1. Lorraine v. Markel American Insurance Company
2. State of Connecticut v. Alfred Swinton
3. United States of America, v. Robert N. Angleton, Defendant
4. State of Alaska, Petitioner, v. George L. Coon, Respondent

#### **CHAPTER 47      eDiscovery: Landmark Cases**

1. Zubulake v. UBS Warburg LLC
2. Williams v. Sprint/United Management Co.

#### **CHAPTER 48      Digital Forensic Investigation: Landmark Cases**

1. Thanh Long Vu v. The Queen

#### **CHAPTER 49      Forensic Expert Evidence: Landmark Cases**

1. Introduction
2. Frye v. United States
3. William Daubert v. Merrell Dow Pharmaceuticals, Inc
4. General Electric Co v. Joiner
5. Kumho Tire Co. V. Carmichael

*...The Book Table of Content*

<b>Appendix</b>	Accessible at <a href="http://www.godigital.ng">www.godigital.ng</a>
<b>Evidence Act, 2011</b>	Accessible at <a href="http://www.godigital.ng">www.godigital.ng</a>
<b>Index</b>	Accessible at <a href="http://www.godigital.ng">www.godigital.ng</a>



## Online Training:

*Convened & Delivered by Digital Evidence & Cyber Forensic Institute*

Aside the forum engagement, special technical training restricted to the technical content and use of the book is organized for specified group as listed: [Judges](#), [Magistrates](#), [State Counsels](#), and [Legal Practitioners in Corporate Practice](#), [Legal Practitioners in Private Practice](#), [Law Students in Nigeria Law School and Undergraduate Law Students in the Universities](#)). This training is specifically requested by organisation to which the respective disciplines belong. Special arrangement is made to acquire the books that would give access (in compliance with terms of use) to the training portal by implementing the use of the access code located at the inside front cover of the book along with a valid email address of the user. The training runs and spread over a period of 12 calendar months and taken at the leisure of participants.

TRAINING

Trainings

Online Trainings [Join Training](#)

Delta State Judiciary Training 2019/2020

Joined: 6/27/2019 11:37:11 AM

TRAINING

Trainings | Training

Delta State Judiciary Training 2019/2020

Introduction

Welcome to the Delta State Judiciary Training 2019/2020

**Delivery**

This training consists of 44 modules delivered over a period of 44 weeks starting on Monday, June 3, 2019 and ending on Sunday, June 9, 2020.

This training is divided into 44 modules. Weekly modules are opened to you on the dates stated in the training calendar.

## Digital Evidence & Cyber Forensic Institute

The Training, derived specifically from the content of the book is convened and delivered by [Digital Evidence & Cyber Forensic Institute, \(DECFI\) Nigeria](#). DECFI is the first Institute in Nigeria with global standards, approved by the Federal Government to chart the partway for Nigerian lawyers, Judges, Prosecutors & Legal Departments of Corporations in Forensic Technology, Digital Evidence and Electronic Discovery. DECFI is a centre for research, knowledge and innovation that delivers the necessary skills to the Nigerian bar and the bench in the development and acquisition of the technical knowledge in meeting the demand of the critical domain of emerging eDiscovery and digital evidence.

The Online Training Portal is characterized by its easy-learning approach modularly structured and designed to ensure maximum learning experience by all participants. For detailed information on the syllabus, visit [www.de-cfi.com](http://www.de-cfi.com)

## The Modular Structure

Every training program is divided into Modules, where each module consist of Notes & Videos, Tests, Assignments & Discussion Forums.

### ⦿ Notes & Videos

Notes contain the objective of each module and lesson guide. Along some of the notes are also lesson videos.

### ⦿ Assignments

Assignment is one way of evaluating a participant on each module. Assignments are expected to be completed on or before the closure of the module. A Text Editor is provided in the Training Portal where these assignments are done and submitted.

### ⦿ Tests

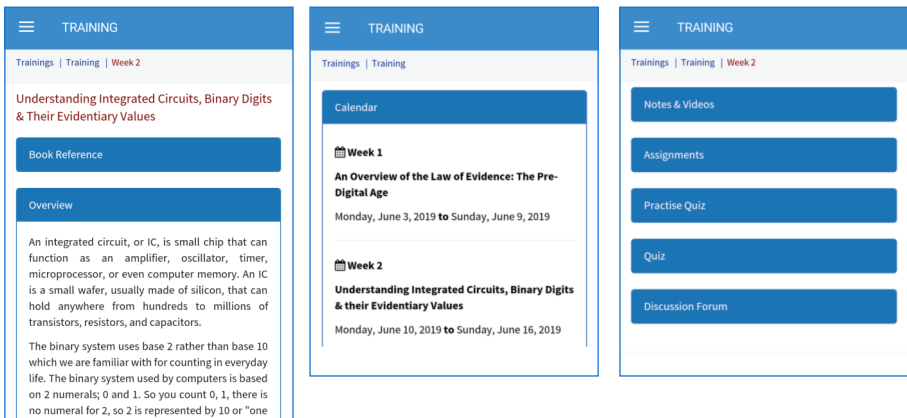
Module Test is another assessment method of the training. Test consist of Multiple-Choice questions, Fill-The-Gap and True or False questions. The Test can only be attempted ONCE, hence there is the Practise Test that helps participants get familiar with the Test Portal.

### ⦿ Discussion Forums

The Discussion Forum is the platform where participants discuss and share ideas relating to the module. Every module has its discussion forum that is related to the module lessons.

### ⦿ Assessments

The total score of each module is derived from the scores on the Tests, Assignments and participation in Discussions. These scores are collated and used to compute the total score of the participant for the module.



## Certificate of Proficiency in Digital Evidence & eDiscovery Law Practice

After completion of the entire exercise, a successful participant is awarded a Certificate of Proficiency in Digital Evidence & eDiscovery Law Practice

## Certificate of Compliance with Digital Evidence & eDiscovery Law Practice

This certificate is issued to a law firm whose in-house counsel participated successfully in the training as conducted by Digital Evidence & Cyber Forensic Institute.

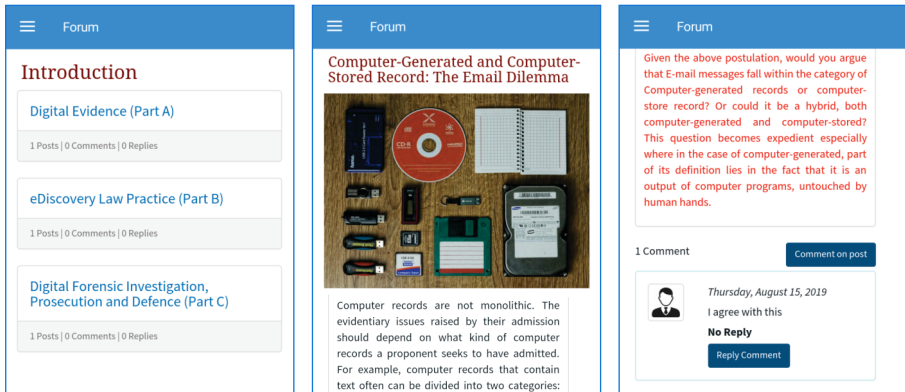
# The Features of the Book ePlatform

The Digital Evidence & eDiscovery Application is a digital tool that helps you make efficient use of the book (Digital Evidence & eDiscovery Law Practice in Nigeria). It is the electronic counterpart of the book.

**It is enriched with the following Features:**

## ⦿ Discussion Forum

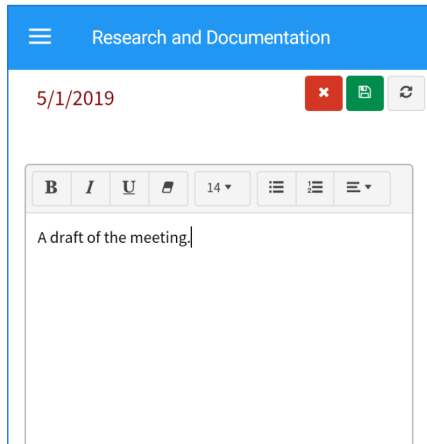
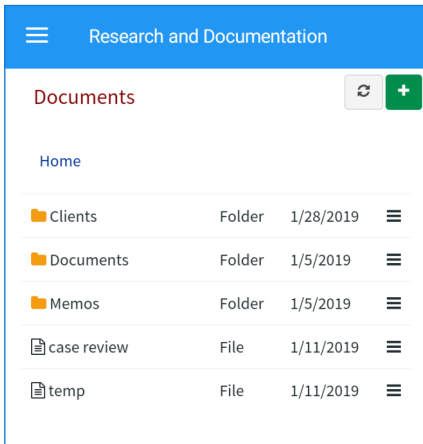
The Discussion Forum provides a platform where specific technical topics from the book are discussed. The Forum is classified into groups (Judges, Magistrates, State Counsels, Legal Practitioners in Corporate Practice, Legal Practitioners in Private Practice, Law Students in Law Schools & Law Students in Law Universities). Discussion posts are published to all groups but member participation (comments and replies) are only shared within each group. For example, a member in the law students group or any other group for that matter cannot see or in any way involved in discussions and contributions made by member of the judges group or any other group. Privacy of each group is protected and secured.



## ⦿ Research & Documentation

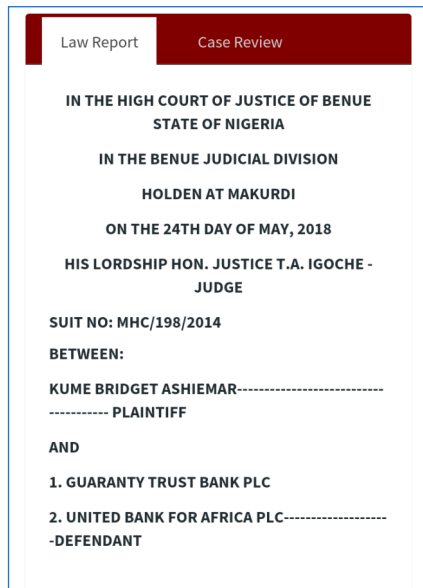
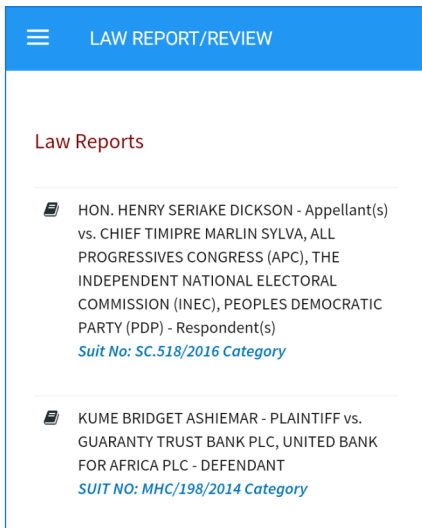
As a user, the electronic platform gives you easy access to and for use of templates for managing data output in real time. Access to the platform also provides a research area that is standardized for securing and keeping all user files organized in one place for effective and efficient management and search. This function is provided by the Document Manager as seen below.

## ...The Features of the Book ePlatform



### ⊙ Law Report/Case Review

Law Report/Case Review brings into focus law reports of cases specifically bordering on Digital Evidence & eDiscovery Law Practice in Nigeria and the technical content-review of such cases.

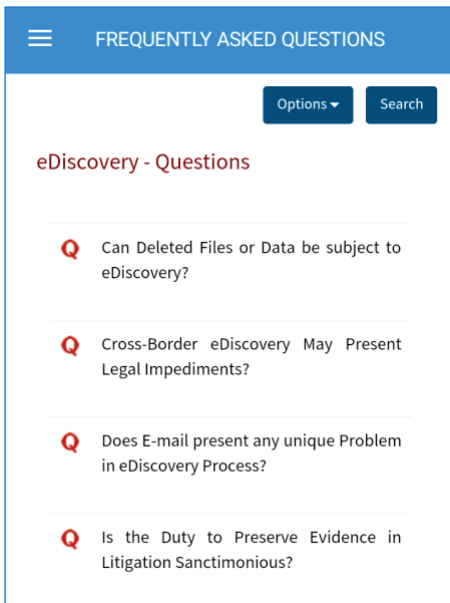


## ...The Features of the Book ePlatform

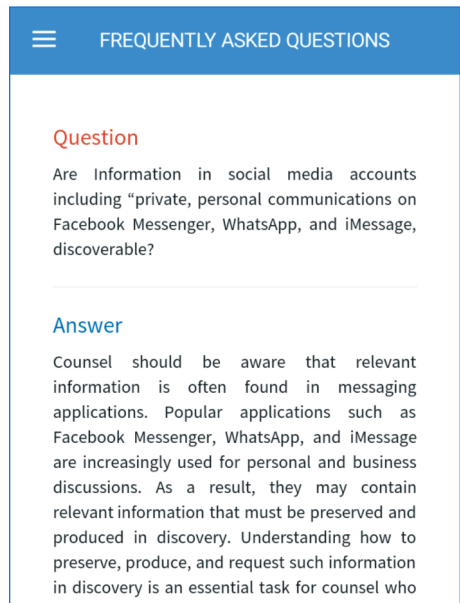
### ⦿ Frequently Asked Questions

Frequently Asked Questions (FAQ) is a facilitation ePlatform that incorporates commonly asked questions by counsel in some context and pertaining to a particular topic, with specific reference to concepts and admissibility of digitally derived evidence and the process of electronic discovery. Answers are typically tailored to incorporate trends in digital developments and its convergence with the laws and legal principles.

Frequently Asked Questions are helpful to both the Bench, in-house counsel in corporations and litigation lawyers because of its inherent ability of providing answers to questions raised in real-time. Users are therefore encouraged to submit any question, requiring immediate attention and be rest assured that answers are promptly provided in real-time.



The screenshot shows a mobile application interface for 'FREQUENTLY ASKED QUESTIONS'. At the top, there is a blue header with a hamburger menu icon and the text 'FREQUENTLY ASKED QUESTIONS'. Below the header, there are two buttons: 'Options' with a dropdown arrow and 'Search'. The main content area is titled 'eDiscovery - Questions' in red. Below this title, there is a list of four questions, each preceded by a red 'Q' icon. The questions are: 'Can Deleted Files or Data be subject to eDiscovery?', 'Cross-Border eDiscovery May Present Legal Impediments?', 'Does E-mail present any unique Problem in eDiscovery Process?', and 'Is the Duty to Preserve Evidence in Litigation Sanctimonious?'.

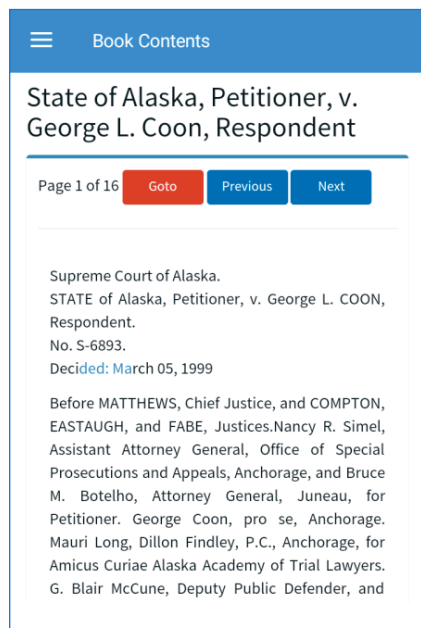


The screenshot shows a mobile application interface for 'FREQUENTLY ASKED QUESTIONS'. At the top, there is a blue header with a hamburger menu icon and the text 'FREQUENTLY ASKED QUESTIONS'. Below the header, there is a red 'Question' section with the text: 'Are Information in social media accounts including "private, personal communications on Facebook Messenger, WhatsApp, and iMessage, discoverable?'. Below the question, there is a blue 'Answer' section with the text: 'Counsel should be aware that relevant information is often found in messaging applications. Popular applications such as Facebook Messenger, WhatsApp, and iMessage are increasingly used for personal and business discussions. As a result, they may contain relevant information that must be preserved and produced in discovery. Understanding how to preserve, produce, and request such information in discovery is an essential task for counsel who'.

## ...The Features of the Book ePlatform

### Ⓞ The Index of Subject Matter

The index of cited cases, table of statutes, and table of practice direction created and incorporated in the printed version of the book are fully automated, electronically searchable and can be reached at [www.godigital.ng](http://www.godigital.ng). Also automated are the Appendix incorporating eDiscoveryCheck List/Questionnaire; Sample Interrogatories; Letter Sent to Client with Interrogatories; Legal Holds and Preservation Letters Template; letter to the Client and Opponent; Preservation Letter for Web Host/Provider/ISP,



## ...The Features of the Book ePlatform

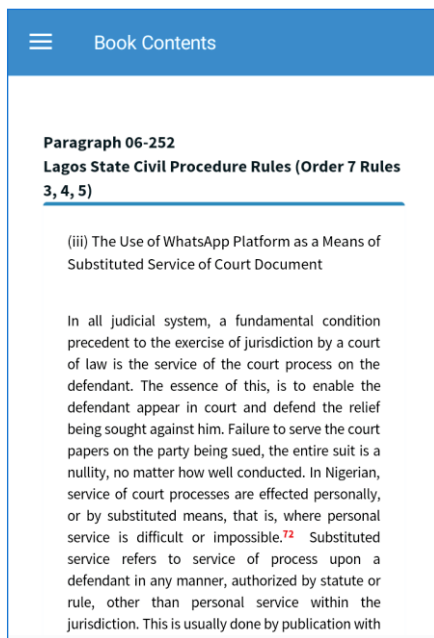
Application (Request) and Affidavit For Search Warrant; Grant Of Warrant To Search; Search Warrant; Officer's Return; Certificate of Authenticity Submitted in Response to a Subpoena, The Evidence Act, 2011; CBN Guidelines on Electronic Banking in Nigeria April, 2016, the Glossary etc.

Designed with an e-book in mind, *hyperlinks* were used instead of *page numbers* and particularly paragraphed for ease of reference, while in court. Hyperlinks bring the user to the exact location of the relevant text, the index of subject matter, the index of cited cases, table of statutes, table of practice direction with readers utilizing tablets and smartphones, for precision linking.



The screenshot shows a mobile application interface for 'Book Contents'. It features a blue header with a hamburger menu icon and the text 'Book Contents'. Below the header, there is a list of legal topics, each with a corresponding page number in a blue box:

- Lagos State Civil Procedure Rules (Order 7 Rules 3, 4, 5) 06-252
- US Federal Rule of Civil Procedure (Rule 26(b)(2)) 23-19
- Lagos State Civil Procedure Rules (Order 26 Rule 8) 09-13
- Lagos State Civil Procedure Rules (Order 26 Rules 8) 25-23
- Civil Procedure Rules (CPR) England and Wales 39-70
- Lagos State Civil Procedure Rules (Order 26 Rule 8) 20-01
- US Federal Rule of Civil Procedure (Rule 37) 28-22



The screenshot shows a mobile application interface for 'Book Contents'. It features a blue header with a hamburger menu icon and the text 'Book Contents'. Below the header, there is a detailed view of a specific paragraph:

**Paragraph 06-252**  
**Lagos State Civil Procedure Rules (Order 7 Rules 3, 4, 5)**

(iii) The Use of WhatsApp Platform as a Means of Substituted Service of Court Document

In all judicial system, a fundamental condition precedent to the exercise of jurisdiction by a court of law is the service of the court process on the defendant. The essence of this, is to enable the defendant appear in court and defend the relief being sought against him. Failure to serve the court papers on the party being sued, the entire suit is a nullity, no matter how well conducted. In Nigerian, service of court processes are effected personally, or by substituted means, that is, where personal service is difficult or impossible.<sup>72</sup> Substituted service refers to service of process upon a defendant in any manner, authorized by statute or rule, other than personal service within the jurisdiction. This is usually done by publication with



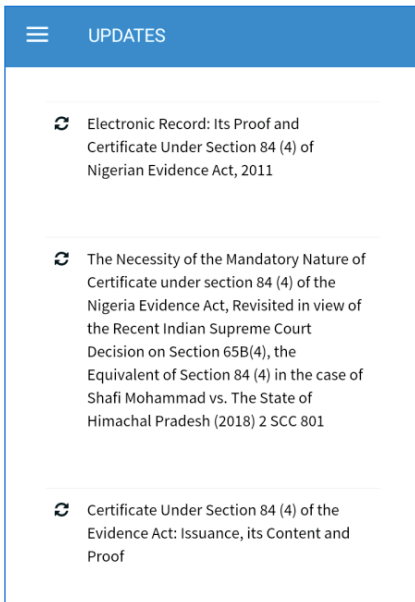
## ...The Features of the Book ePlatform

### ⦿ Updates

Access to Continues Research and Development on Digital Evidence & eDiscovery Law Practice in Nigeria by Digital Evidence and Cyber Forensic Institute, Nigeria.

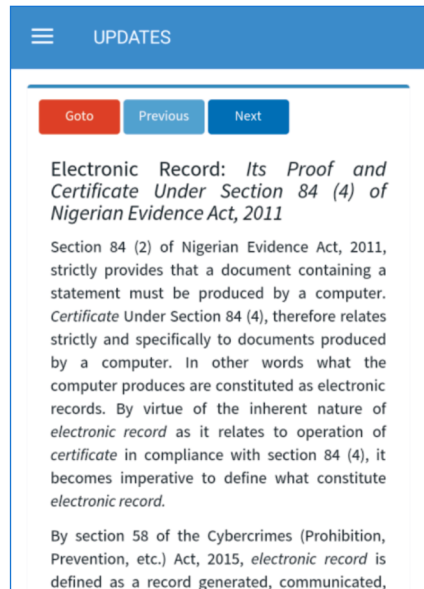
Obsolescence is the state of being which occurs when an object, service or practice is no longer wanted even though it may still be in good working order. It refers to something that is already disused, discarded or antiquated.

Electronic books such as Digital Evidence & eDiscovery Law Practice in Nigeria would also in course time attain the same status of obsolescence. Mindful of this expectation, I have developed a working relationship with Digital Evidence and Cyber Forensic Institute, Nigeria for continued research and development in Digital Evidence & eDiscovery. Attention is focused on all courts relevant judgments in digital evidence and eDiscovery issues within and outside Nigeria, with a view to effective updates, critique and review. All users and subscribers to this book are beneficiaries of the research outcomes, subject to our terms of use and policy.



The screenshot shows a blue header with a hamburger menu icon and the word 'UPDATES'. Below the header is a list of three articles, each preceded by a circular refresh icon. The articles are:

- Electronic Record: Its Proof and Certificate Under Section 84 (4) of Nigerian Evidence Act, 2011
- The Necessity of the Mandatory Nature of Certificate under section 84 (4) of the Nigeria Evidence Act, Revisited in view of the Recent Indian Supreme Court Decision on Section 65B(4), the Equivalent of Section 84 (4) in the case of Shafi Mohammad vs. The State of Himachal Pradesh (2018) 2 SCC 801
- Certificate Under Section 84 (4) of the Evidence Act: Issuance, its Content and Proof





The screenshot shows a blue header with a hamburger menu icon and the word 'UPDATES'. Below the header are three buttons: 'Goto' (red), 'Previous' (blue), and 'Next' (blue). The main content area displays the title of an article: *Electronic Record: Its Proof and Certificate Under Section 84 (4) of Nigerian Evidence Act, 2011*. Below the title is the text of the article, which discusses Section 84 (2) of the Nigerian Evidence Act, 2011, and the nature of electronic records. The text concludes with a reference to Section 58 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, defining an electronic record.

## Subscription

The initial registration entitles users free access to the Digital Evidence & eDiscovery App available on web browser (Godigital.ng), Google Play for Android and Apple Store IOs for a period of 12 calendar months incorporating the training. The Users thereafter may continue usage by way of annual subscription on a minimal fee to be determined by Lawdata Communication Solutions Ltd. Users may cancel their subscription at any time.

## Visit Us On







 [www.godigital.ng](http://www.godigital.ng)  
 [info@godigital.ng](mailto:info@godigital.ng)

## Contact Us



 13b Gilbert Odior Street, Thomas Estate,  
Lekki-Epe Express Way, Ajah, Lagos.  
 [info@de-cfi.com](mailto:info@de-cfi.com)  
 [www.de-cfi.com](http://www.de-cfi.com)  
 0903 434 8127



 Flat 4 Block A No 1 Kumasi Crescent,  
Wuse II Abuja (FCT) Nigeria  
 [info@lawdt.com](mailto:info@lawdt.com)  
 [www.lawdt.com](http://www.lawdt.com)  
 0814 544 0567

**LawData**


LawData Communication Solutions Ltd


Lawdata Communication Solutions Ltd, is a specific- purpose built technology company with the sole aim of delivering e-Solutions to law firms in Nigeria. Founded in 2004, by a veteran Nigeria lawyer and a technologist with specific bent in digital forensic technology, Lawdata evolved over the years as the pioneer of one-stop shop for e-Solutions to lawyers and law firms in Nigeria.


Our service offering encompasses:

- Electronic Law Book Publishers
- Case Management Software - Lawbreiff
- Legal Document Scanning & Imaging-DocXpress
- Law Firm Web Design/Hosting Service
- Attorney Blog Design & Support
- Law Firm Web Mastering & Maintenance
- Virtual Onsite Support
- Social Media & Networking
- Search Engine Optimisation
- Network Design & Installation
- Courtroom Technology

Visit us on

 [www.lawdt.com](http://www.lawdt.com)

 [info@lawdt.com](mailto:info@lawdt.com)

 0814 544 0567

To place order for **DIGITAL EVIDENCE & eDISCOVERY LAW PRACTICE IN NIGERIA**, please visit [www.godigital.ng](http://www.godigital.ng) and complete the form on the Place Order Page as shown below and we will get back to you within 24 hours.



[About Us](#) [Contact Us](#) [Register](#) [Sign In](#) [Book Verification](#) [Place Order](#)

## Place an order

To place order for DIGITAL EVIDENCE & eDISCOVERY LAW PRACTICE IN NIGERIA, please complete this form and we will get back to you within 24 hours.

Fields marked \* are required.

First Name\*

Street\*

Last Name\*

City\*

Email Address\*

State\*

Phone Number\*

Country\*

Number of Books\*

Enter the code below

**4 4 3 5 4**

Submit

For more information please call  
0814 544 0567