

Digital Forensics and Cybercrime Investigation in Nigeria

COURSE OVERVIEW

With the rise in digital crimes, Nigerian law enforcement agencies increasingly rely on computer, mobile, and network forensics to trace criminal activities and gather digital evidence admissible in court. This course explores the legal, regulatory and technological frameworks that shape cybercrime investigation, with a strong focus on evidence collection, preservation, analysis, and presentation in court. It further integrates practical case studies from Nigeria's evolving cyber landscape, enabling participants to connect theory with actual challenges and solutions in combating cyber enabled offenses. Participants will be equipped generally with a solid foundation in the principles, tools and methodologies of investigating digital crimes within the Nigerian context.

WHO SHOULD ATTEND?

This course is suitable for law enforcement officers, cybersecurity professionals, investigators, prosecutors, IT auditors, compliance officers and regulatory personnel involved in crime detection and prosecution. It also benefits legal practitioners, corporate security managers, and policymakers seeking to enhance their knowledge of digital forensics, cybercrime trends, and the practical application of Nigeria's cyber laws.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Explain the fundamentals and scope of digital forensics and cybercrime investigation.
- Identify and apply relevant Nigerian laws and regulations governing cybercrime and digital evidence.
- Demonstrate skills in acquiring, preserving, and analyzing digital evidence from various devices.
- Use digital forensic tools to conduct investigations on computers, networks, mobiles, and storage media.
- Evaluate cybercrime incidents and develop strategies for effective response and mitigation.
- Prepare comprehensive forensic reports and testify effectively in legal proceedings.
- Stay updated on emerging cybercrime trends and implement best practices for digital security and investigation.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- Fundamentals of digital forensics and cybercrime concepts in Nigeria.
- Procedures for collecting, preserving, and examining electronic evidence.
- Application of forensic tools for analyzing data from computers, networks, and mobile devices.
- Legal frameworks and regulations governing cybercrime and digital evidence.
- Methods for conducting cybercrime investigations and assessing digital threats.
- Preparation of forensic reports and effective testimony in legal proceedings.
- Emerging challenges and best practices in digital forensics and cybercrime investigation.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.

1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded