Training Course Outline

ITU and Digital Bridge Institute (DBI)

Title	Cyber Forensics and IT Risk Management
Modality	Online instructor led
Dates	March 14 – 25, 2022
Duration	2 Weeks
Registration deadline	March 11, 2022
Training fees	150 USD
Description	This course presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation. This course will also present different IT risk and its management as well as risk management policy development.
Code	22OI27997AFR-E

1.LEARNING OBJECTIVES

Objectives of the training course include the following:

1. Understand cyber forensics
2. Understand chain of custody, digital evidence gathering, preservation and presentation
3. Use different tools for cyber forensics
4. Understand anti – forensic tools and methods
5. Write good report
6. Understand IT risk and management
7. Develop risk management policy

2. LEARNING OUTCOMES

It is expected that upon completion of the training session, participants will be able to:

1. Understand cyber forensics
2. Understand chain of custody
3. Apply and use different tools to acquire, preserve and analyze evidence
4. Perform different forensics ranging from Windows to Linux, network, and email forensics
5. Understand different anti –forensics techniques and uncover it
6. Write acceptable technical report about an incidence
7. Understand IT risk analysis and management
8. Develop IT risk management strategy

9. Apply IT risk management best practices

3.TARGET POPULATION

This training is targeted at the police and other law enforcement personnel, defense and military personnel, security professionals, system administrators, legal practitioners, government agencies and IT managers

4.ENTRY REQUIREMENTS

Participants Requirement

- Basic digital literacy skill
- Basic understanding of internet
- Basic understanding of cybersecurity

Laptop Requirement

- Minimum of 8Gb RAM
- Core i5 system processor
- ITB Hard disk

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	**Contact details**
Ms. Oloyede Olajumoke Elizabeth	Email: ooloyede@dbi.edu.ng Telephone: +2348060146414
Mr. Nelson Afundu	Email: nafundu@dbi.edu.ng
Mr. Ayodeji Idris	Email: aidris@dbi.edu.ng

6.TRAINING COURSE CONTENTS

Computer Forensics in Today's World

- Forensic science
- Evolution of computer forensics
- Objective of computer forensics
- Need for computer forensics
- Forensics readiness
- Cybercrime
- Cybercrime investigation

Computer Forensics Investigation Process

- Investigating computer crime
- Computer forensics methodology
- Obtain search warrant
- Evaluate and secure the scene
- Process of data collection
- Understanding Hard Disks and File Systems
- Hard Disk Drive Overview
- Disk Drive Overview
- Hard Disk Drive

- Solid-State Drive (SSD)
- Types of Hard Disk Interfaces
- Hard Disk Interfaces
- Understanding file system

Data Acquisition and Duplication

- Data acquisition and duplication concepts
- Data acquisition types
- Data acquisition tool requirements
- Acquisition best practices
- Data acquisition software tools

Windows Forensics

- Collecting volatile information
- Collecting Non volatile information
- Windows memory analysis
- Windows registry analysis
- Cache, cookie and history analysis
- Windows file analysis
- Metadata investigation
- Forensics tools

Linux Forensics

- Collecting volatile information
- Collecting Nonvolatile information
- Linux memory analysis
- Forensics tools

Network Forensics

- Network forensics
- Network forensics analysis mechanism
- OSI model
- TCP/IP model
- IDS, Firewall, and honeypots
- Network attack
- Investigating network traffics
- Traffic capturing and analysis tools

Investigating Email Crimes

- Email terminology
- Email clients and servers
- Email crimes
- Email headers
- Steps to investigate email
- Email forensics tools

Mobile Forensics

- Android Operating System
- Mobile forensic tools

Investigative Reports

- Computer forensics report
- Features of a good report
- Computer forensics report template

- Investigative report writing

IT risks and governance

- Risk and governance definition
- Steps to risk management
- Risk management strategies
- Standards, frameworks, and best practices for IT risk management
- Risk identification
- Loss, threat, and vulnerability
- Threat sources
- Risk calculation
- Vulnerability assessment
- Inherent, current, and residual risk
- Risk register

Risk response

- Risk response terms
- Parameters for risk selection
- Risk response plan
- Effective risk reporting plan

7.TRAINING COURSE SCHEDULE

Week / Session	Topic	Exercises and interactions
Week 1	**Computer Forensics in Today's World** • Forensic science • Evolution of computer forensics • Objective of computer forensics • Need for computer forensics • Forensics readiness • Cybercrime • Cybercrime investigation • Computer Forensics Investigation Process • Investigating computer crime • Computer forensics methodology • Obtain search warrant • Evaluate and secure the scene • Process of data collection • Understanding Hard Disks and File Systems • Hard Disk Drive Overview • Disk Drive Overview • Hard Disk Drive • Solid-State Drive (SSD) • Types of Hard Disk Interfaces • Hard Disk Interfaces • Understanding file system **Data Acquisition and Duplication**	• Read course materials • Participate in online classes • Take quiz • Participate in forum discussion • Write learning journal

	• Data acquisition and duplication concepts • Data acquisition types • Data acquisition tool requirements • Acquisition best practices • Data acquisition software tools **Windows Forensics** • Collecting volatile information • Collecting Non volatile information • Windows memory analysis • Windows registry analysis • Cache, cookie and history analysis • Windows file analysis • Metadata investigation • Forensics tools **Linux Forensics** • Collecting volatile information • Collecting Nonvolatile information • Linux memory analysis • Forensics tools	
Week 2	**Network Forensics** • Network forensics • Network forensics analysis mechanism • OSI model • TCP/IP model • IDS, Firewall, and honeypots • Network attack • Investigating network traffics • Traffic capturing and analysis tools **Investigating Email Crimes** • Email terminology • Email clients and servers • Email crimes • Email headers • Steps to investigate email • Email forensics tools **Mobile Forensics** • Android Operating System • Mobile forensic tools **Investigative Reports** • Computer forensics report • Features of a good report • Computer forensics report template • Investigative report writing **IT risks and governance** • Risk and governance definition • Steps to risk management	• Read course materials • Participate in online classes • Take quiz • Participate in forum discussion • Write learning journal • Submit assignment

	- Risk management strategies - Standards, frameworks, and best practices for IT risk management **Risk identification** - Loss, threat, and vulnerability - Threat sources - Risk calculation - Vulnerability assessment - Inherent, current, and residual risk - Risk register **Risk response** - Risk response terms - Parameters for risk selection - Risk response plan - Effective risk reporting plan	

8.METHODOLOGY (Didactic approach)

This course shall be delivered fully online. There will be instructor led sessions, case studies, forum discussions, weekly assignments, weekly learning journals and quizzes. All participants must do all the assignments and quizzes and pass to be issued the ITU certificate. The instructor will have question and answer session once a week via ZOOM or Google Meet from 09.00hours to 12.00hours. Pre-recorded video will be made available on the ITU dashboard

9.EVALUATION AND GRADING

Evaluation of participants at this course will be based on the following:

- Class Attendance - 20% (10% per week)
- Quizzes - 20% (10% per week)
- Assignment - 20%
- Forum participation - 30% (15% per week)
- Learning journal – 10% (5% per week)

Only participants who have successfully completed all assessments with a pass mark of 60% shall be awarded the ITU Certificate.

10.TRAINING COURSE COORDINATION

Course Coordinator: Name: **Mr. Paulinus O. UGWOKE** Head, Research, Education and Training Department, Digital Bridge Institute, Abuja, NIGERIA Tel. No: +234 803 360 7540 Email address: pougwoke@dbi.edu.ng	**ITU Coordinator:** Name: **Mr. Emmanuel NIYIKORA** Programme Officer, ITU Area Office for West Africa, DAKAR Tel. No : +250 788312939 Email address: emmanuel.niyikora@itu.int