



**ITU Centres of Excellence Network for Africa**

**Digital Bridge Institute (DBI), Abuja, Nigeria**

**Online Training Course on**

**Emerging Cybercrime Trends: Cybercrime Investigation & Mobile Forensics**

**November 22 – December 3, 2021**

**TRAINING COURSE OUTLINE**

**COURSE DESCRIPTION**

Title	<b>Emerging Cybercrime Trends: Cybercrime Investigation &amp; Mobile Forensics</b>
Objectives	Objectives of the training course include the following: <ul style="list-style-type: none"><li>• Understand cybercrime</li><li>• Understand motives for cybercrime</li><li>• Understand different threats and threat actors</li><li>• Understand information technology trends</li><li>• Understand different IT trends and associated crimes</li><li>• Perform malware analysis</li><li>• Understand mobile forensics</li><li>• Perform mobile forensics</li><li>• Identify anti – forensics technique</li><li>• Apply zero trust framework</li></ul>
Dates	November 22 – December 3, 2021
Duration	2 Weeks
Registration deadline	November 19, 2021
Training fees	100USD
Course code	21OI27764AFR-E

## DESCRIPTION OF THE TRAINING COURSE

---

This course presents a detailed methodological approach to understanding trends in cybercrimes and how cybercrimes can be investigated. It is a comprehensive course covering major forensic investigation scenarios that enable students to acquire hands-on experience on various cybercrime investigation techniques and standard tools necessary to successfully carry-out a mobile forensic investigation. This course will also teach participants how to gather electronic artifacts from mobile devices.

## LEARNING OUTCOMES

---

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

1. Discuss emerging cybercrime trends and other threats
2. Mitigate against cybercrimes
3. Carryout malware analysis
4. Carryout mobile forensics
5. Identify anti-forensics techniques
6. Apply zero trust framework

## TARGET POPULATION

---

This training is targeted at private investigators, intelligence analysts and law enforcement agents

## TUTORS/INSTRUCTORS

---

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Ms. Olajumoke OLOYEDE	Email: <a href="mailto:ooloyede@dbi.edu.ng">ooloyede@dbi.edu.ng</a> Tel: +234 806 014 6414

## EVALUATION

---

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 - 40% (20% per week)

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

## TRAINING COURSE CONTENTS

---

### Introduction to Cybercrime

- Introduction to cyberspace and cybercrime
- Types of cybercrimes
- Types of cybercriminals
- Motives of cybercriminals
- Understanding cyber attack
- Notable data breaches

### Threats and Vulnerabilities

- Introduction to threat
- Types of threat

- Global threat landscape
- Introduction to vulnerability
- Types of vulnerability
- Vulnerability lifecycle management

### **Information Technology Trends**

- IT evolution
  - The past: e.g mainframe, floppy disk, static website, infrared etc
  - The present: smart devices and cloud
  - The future: Internet of things, virtual reality, 5G
- Emerging trends
  - Cloud computing
  - IoT
  - Blockchain

### **Emerging Cybercrime**

- Business Email Compromise
- Cryptocurrency scams
- Cloud base attacks
- IoT- focused attack
- Hacking as a service
- Ransomware as a service
- Insider attack

### **Malware Analysis**

- Mobile forensic tools
- Anti – forensic techniques

### **Mobile Forensics**

- Android Operating System
- Mobile forensic tools
- Anti – forensic techniques

### **Other trends**

- Zero Trust Framework
- Cyber insurance

### **Practicals and tools**

- Forensic tools
- Anti – forensic tools
- Malware analysis tools
- Wallets and Explorers
- Blockchain analytics tools

## **METHODOLOGY**

---

This course shall be delivered fully online. There will be instructor led sessions, case studies, forum discussions and weekly assignments, and quizzes. All participants must do all the assignments and quizzes and pass to be issued the ITU certificate. The instructor will deliver live lectures daily via ZOOM or Google Meet from 09.00hours to 12.00hours.

## TRAINING COURSE SCHEDULE

Week	Topic	Exercises and Interactions
<b>Week 1</b>	<p><b>Introduction to Cybercrime</b></p> <ul style="list-style-type: none"> <li>• Introduction to cyberspace and cybercrime</li> <li>• Types of cybercrimes</li> <li>• Types of cybercriminals</li> <li>• Motives of cybercriminals</li> <li>• Understanding cyber attack</li> <li>• Notable data breaches</li> </ul> <p><b>Threats and Vulnerabilities</b></p> <ul style="list-style-type: none"> <li>• Introduction to threat</li> <li>• Types of threat</li> <li>• Global threat landscape</li> <li>• Introduction to vulnerability</li> <li>• Types of vulnerability</li> <li>• Vulnerability lifecycle management</li> </ul> <p><b>Information Technology Trends</b></p> <ul style="list-style-type: none"> <li>• IT evolution               <ul style="list-style-type: none"> <li>○ The past: e.g mainframe, floppy disk, static website, infrared etc</li> <li>○ The present: smart devices and cloud</li> <li>○ The future: Internet of things, virtual reality, 5G</li> </ul> </li> <li>• Emerging trends               <ul style="list-style-type: none"> <li>○ Cloud computing</li> <li>○ IoT</li> <li>○ Blockchain</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Read course materials</li> <li>• Participate in online classes</li> <li>• Take quiz</li> <li>• Participate in forum discussion</li> </ul>
<b>Week 2</b>	<p><b>Emerging Cybercrime</b></p> <ul style="list-style-type: none"> <li>• Business Email Compromise</li> <li>• Cryptocurrency scams</li> <li>• Cloud base attacks</li> <li>• IoT- focused attack</li> <li>• Hacking as a service</li> <li>• Ransomware as a service</li> <li>• Insider attack</li> </ul> <p><b>Malware Analysis</b></p> <ul style="list-style-type: none"> <li>• Mobile forensic tools</li> <li>• Anti – forensic techniques</li> </ul> <p><b>Mobile Forensics</b></p>	<ul style="list-style-type: none"> <li>• Read course materials</li> <li>• Participate in online classes</li> <li>• Take quiz</li> <li>• Participate in forum discussion</li> <li>• Submit assignment</li> </ul>

	<ul style="list-style-type: none"> <li>• Android Operating System</li> <li>• Mobile forensic tools</li> <li>• Anti – forensic techniques</li> </ul> <p><b>Other trends</b></p> <ul style="list-style-type: none"> <li>• Zero Trust Framework</li> <li>• Cyber insurance</li> </ul>	
--	--	--

## TRAINING COORDINATION

<p><b>Course Coordinator:</b></p> <p>Name : <b>Mr. Paulinus O. UGWOKE</b>  Head, Research, Education and Training  Département, Digital Bridge Institute, Abuja,  NIGERIA  Tel. No : +234 803 360 7540  Email address : <a href="mailto:pougwoke@dbi.edu.ng">pougwoke@dbi.edu.ng</a></p>	<p><b>ITU Coordinator:</b></p> <p>Name : <b>Mr. Emmanuel NIYIKORA</b>  Programme Officer,  ITU Area Office for West Africa, DAKAR  Tel. No : +250 788312939  Email address: <a href="mailto:emmanuel.niyikora@itu.int">emmanuel.niyikora@itu.int</a></p>
--	--

## REGISTRATION AND PAYMENT

### ITU Academy portal account

Registration and payment should be made online at the ITU Academy portal.

To be able to register for the course you MUST first create an account in the ITU Academy portal at the following address:

<https://academy.itu.int/user/register>

### Course registration

When you have an existing account or created a new account, you can register for the course online at the following link: <https://academy.itu.int/training-courses/full-catalogue/emerging-cybercrime-trends-cybercrime-investigation-mobile-forensics>

You can also register by finding your desired course in our training catalogue

<https://academy.itu.int/training-courses/full-catalogue>

### Payment

#### 1. On-line Payment

A training fee of USD 100 per participant is applied for this training. Payment should be made via the online system using the link mentioned above for training registration at: <https://academy.itu.int/training-courses/full-catalogue/emerging-cybercrime-trends-cybercrime-investigation-mobile-forensics>

#### 2. Payment by Bank Transfer

Where it is not possible to make payment via the online system, select the option for offline payment to generate an invoice. Use the invoice to make a bank transfer to the ITU Bank account shown below. Then send the proof of payment and the copy of invoice to [Hcbmail@itu.int](mailto:Hcbmail@itu.int) and copy the course coordinator. **All bank transaction fees must be borne by the payer.**

**Failure to submit the above documents may result in the applicant not being registered for the training.**

#### 3. Group Payment

Should you wish to pay for more than one participant using bank transfer and need one invoice for all of them, create an account as **Institutional Contact**. **Institutional Contacts** are users that represent

an organization. Any student can request to be an institutional contact or to belong to any existing organization.

To do this, head to your profile page by clicking on the “**My account**” button in the user menu. At the bottom of this page you should see two buttons:

- a. If you want to **become an institutional contact**, click on the “**Apply to be an Institutional Contact**” button. This will redirect you to a small form that will ask for the organization name. After you fill the name of the organization you want to represent, click on “**continue**” and a request will be created. An ITU Academy manager will manually review this request and accept or deny it accordingly.
- b. If you want to **belong to an existing organization**, click on the “**Request to belong to an Institutional Contact**” button. This will redirect you to a small form that will ask you to select the organization you want to join from an organization list. After you select the correct organization, click on “**continue**”, a request will then be created. The Institutional Contact that represents that organization will manually accept or deny your request to join the organization.

#### ITU BANK ACCOUNT DETAILS:

Name and Address of Bank:	UBS Switzerland AG Case postal 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 100
Payment Reference:	CoE-AFR 27764 - P.40590.1.02

#### 4. Other method of payment

If due to national regulations, there are restrictions that do not allow for payment to be made using options 1 & 2 above, please contact the ITU Coordinator for further assistance.