



ITU Centres of Excellence Network for Africa

Digital Bridge Institute (DBI), Abuja, Nigeria

Online Training Course on

Cyber Forensics and IT Risk Management

October 11 – 22, 2021

TRAINING COURSE OUTLINE

COURSE DESCRIPTION

| | |
|-----------------------|--|
| Title | Cyber Forensics and IT Risk Management |
| Objectives | Objectives of the training course include the following: <ul style="list-style-type: none">• Understand cyber forensics• Understand chain of custody, digital evidence gathering, preservation and presentation• Understand how to use different tools for cyber forensics• Understand anti – forensic tools and methods• Understand how to write good report• Understand IT risk and management• Understand how to develop risk management policy |
| Dates | October 11 – 22, 2021 |
| Duration | 2 Weeks |
| Registration deadline | October 8, 2021 |
| Training fees | 100USD |
| Course code | 21OI26520AFR-E |

DESCRIPTION OF THE TRAINING COURSE

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.

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, 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

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

TUTORS/INSTRUCTORS

| NAME OF TUTOR(S)/INSTRUCTOR(S) | CONTACT DETAILS |
|--------------------------------|---|
| Ms. Olajumoke OLOYEDE | Email: ooloyede@dbi.edu.ng Tel: +234 806 014 6414 |

EVALUATION

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

- Class Attendance
- Quizzes
- Assignments
- Forum participation

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

TRAINING COURSE CONTENTS

Introduction to Cyber Forensics

- What is Cyber Forensics?
- Image integrity and its tools
- Performing image integrity using the forensic tools

Steganography

- Performing steganography and steganalysis using appropriate tools
- Performing windows registry analysis and forensics using taught tools
- Data acquisition

Network traffic analysis

- Performing network traffic analysis using taught tools
- Identifying components of email headers, recover deleted email, and using other instructor specified tools to perform email forensics

Report writing

- Writing good reports
- Features of good reports
- ISO 31000

Risk Management

- What is Risk Management ?
- How to develop risk management plan
- Features of a risk management plan

METHODOLOGY

Course Materials: The relevant course material will be made available on the ITU Academy portal at the beginning of the course.

Online Discussion Forums: Participants are expected to participate actively in discussion forums on selected topics throughout the week.

Chat Sessions: Online chat sessions with the tutors will take place on Thursdays of each week. All participants are expected to join the chat sessions as they will be graded.

Quizzes: Two mandatory online quiz will be held at the end of each week.

Assignment: There will be a mandatory assignment for the course.

TRAINING COURSE SCHEDULE

| Week | Topic | Exercises and Interactions |
|--------|---|---|
| Week 1 | Introduction to Cyber Forensics <ul style="list-style-type: none">• What is Cyber Forensics?• Image integrity and its tools• Performing image integrity using the forensic tools Steganography <ul style="list-style-type: none">• Performing steganography and steganalysis using appropriate tools• Performing windows registry analysis and forensics using taught tools• Data acquisition | <ul style="list-style-type: none">• Read week 1 material• Participate in online class• Submit week 1 assignment• Take week 1 quiz• Participate in forum discussion for week 1 |
| Week 2 | Network traffic analysis <ul style="list-style-type: none">• Performing network traffic analysis using taught tools• Identifying componenst of email headers, recover deleted email, and using other instructor specified tool to perform email forensics Report writing <ul style="list-style-type: none">• Writing good reports• Features of good reports• ISO 31000 Risk Management <ul style="list-style-type: none">• What is Risk Management ?• How to develop risk management plan• Features of a risk management plan | <ul style="list-style-type: none">• Read week 2 material• Participate in online class• Submit week 2 assignment• Take week 2 quiz• Participate in forum discussion for week 2 |

TRAINING COORDINATION

| | |
|---|---|
| Course Coordinator: Name : Mr. Paulinus O. UGWOKÉ 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 |
|---|---|

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/index.php/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/cyber-forensics-and-it-risk-management-online>

You can also register by finding your desired course in our training catalogue
<https://academy.itu.int/index.php/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/cyber-forensics-and-it-risk-management-online>

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 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:

- 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 26520 - 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.