Training course outline

ITU and National Computer Board / Computer Emergency Response Team of Mauritius

Title	**Digital Forensic Essentials – An investigative approach**
Modality	Online
Dates	13 – 15 April 2022
Duration	3 days
Registration deadline	8 April 2022
Training fees	Free
Description	The proliferation of technology in the modern-day workplace presents a world of opportunity for fraudsters and pose complexity for the investigators and examiners. Desktops, laptops, smartphones, digital cameras, even watches and GPS devices can all be used to abet a fraud. They also all leave behind a digital trail. Gathering and preserving electronic evidence requires a special set of considerations. Without a thorough understanding of digital forensics, your next move could compromise evidence or cause your findings to be inadmissible in court.
Code	22OI28038AFR-E

1.LEARNING OBJECTIVES

The main objective of this training course is to allow participants to acquire essential knowledge to collect electronic evidence and use it for investigation. Other objectives include:

- Learning to properly handle digital evidence
- Learning to categorize types of digital storage devices
- Learning to seize, secure and analyze digital evidence
- Learning to apply methods of seizing digital evidence and recognizing the legal implications
- Understanding the forensic examiners role and the dos and don’ts of handling digital evidence

2. LEARNING OUTCOMES

This three-day instructor-led course will introduce you to the essential knowledge you need to acquire in order to investigate on electronic evidence. Participants will also learn about best practices for evidence collection, chain of custody and analysis. This course will also aid participants in the understanding of incident response using forensic tools.

3.TARGET POPULATION

The target audience for this course is as follows:

- Current and future CSIRT/CIRT/CERT managers and team members
- C-level managers such as CIOs, CSOs, CROs, CISOs
- Cybersecurity professionals such as information security analysts, security engineers, incident handlers, network security administrators, malware analysts, IT professionals from ISPs, RENs, IXPs, SOCs, NOCs, TLDs, amongst others
- Legal professionals and law enforcement personnel

4.ENTRY REQUIREMENTS

Foundation in Cybersecurity

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Kaleem Usmani	kusmani@cert.ncb.mu
Manish Lobin	mlobin@cert.ncb.mu

6.TRAINING COURSE CONTENTS

Topics to be covered in this course are as follows:

- Principles of Digital Forensics & Examination Process
    - Basic elements in Digital Forensics investigation
    - Terminology and equipment used
    - Gathering & reviewing digital evidence
    - How forensic examination is planned
    - Phases of examination

- Evidence Seizure & Security – Which tools to use?
    - Digital search & seizure
    - Industry Best practices

- Overt vs Covert methods
- Evidence collection & storage
- Chain of custody considerations
- Tools traditionally used and why

- Putting it all Together: Preparing your case for the next step
  - Assurance that evidence was obtained and handled in the most appropriate manner possible
  - Report on analysis of the evidence

7.TRAINING COURSE SCHEDULE

Week / Session	Topic	Exercises and interactions
Day 1 **13 April 2022** **11am – 2pm** **(Geneva Time)**	Principles of Digital Forensics & Examination Process	Presentations Discussion Group work Case studies
Day 2 **14 April 2022** **11am – 2pm** **(Geneva Time)**	Evidence Seizure & Security – Which tools to use?	Presentations Discussion Group work Case studies
Day 3 **15 April 2022** **11am – 2pm** **(Geneva Time)**	Putting it all Together: Preparing your case for the next step	Presentations Discussion Group work Case studies

8.METHODOLOGY (Didactic approach)

The training will be carried out online through the ITU Academy Platform. It will include presentations, discussion, group work, case studies and an exam.

9.EVALUATION AND GRADING

An exam will be conducted at the end of the course. Participants are required to get 60% of the marks in order to pass the exam. It is also to be noted that Presentations, Discussions, Group works, and Case studies will not be graded.

10.TRAINING COURSE COORDINATION

Course coordinator: Name: Manish Lobin Email address: mlobin@cert.ncb.mu	ITU coordinator: Name: Mr. Emmanuel NIYIKORA Programme Officer, ITU Area Office for West Africa, DAKAR Tel : +250 788312939 Email address: emmanuel.niyikora@itu.int