MINISTRY OF DIGITAL

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

DIGITAL FORENSICS ESSENTIAL

Level: Fundamental | **Duration:** 2 days

This course is intended for managers, government officers or researcher/educators who are interested to understand high level information about digital forensic. Participants are encouraged to participate in decision making to manage evidence, forensics team, tools and resources.

Objectives

1. Identify the methodology of conducting forensic on digital evidence
2. Understand ways to preserve and analyze evidence and to present result to stakeholders
3. Learn to setup a forensic laboratory, to manage evidence and resources

Target Participants

1. Managers
2. Government officers involve in incident response
3. Researchers/Educators
4. Individual interested in digital forensics

Modules

1. Digital Forensics in Malaysia Landscape

Digital forensics consists of several major digital areas, namely mobile phone forensics and video forensics. Each area introduce new terms to the world of digital forensics, which will be covered in this topic. The case studies, technologies, issues and challenges faced by the First Responder will be discussed in this topic. The topics covered include:

- Forensic Science: An Introduction
- Digital Forensic: An Introduction
- Digital Evidence
- People & Roles
- Case Study
- Challenges

2. Digital Forensics Methodology & Terminology

To be involved in digital crime investigation, one must first know and understand the methodology of the digital forensics. Basically, there are 5 main processes in conducting forensics examination and analysis. All of these processes will be taught in details during the course. Participants will also learn about the Best Practice for seizing and acquiring evidence at crime scene. The topics covered include:

- Digital Forensics Methodology
- Terminology
- Conclusion

3. Digital Evidence: What Data Can You Retrieved?

What types of data can be extracted from computer or mobile phone or CCTV? What challenges do they present? In this topic, participants will be exposed with types of data that can be collected from different kind of digital media, as well as the challenges in getting all the potential evidentiary data. The topics covered include:

- Computer Analysis
- Mobile Device Analysis
- Internet/Email Analysis
- Video Analysis
- Image Analysis
- Audio Analysis
- Conclusion

Modules

4. First Responder Standard Operating Procedure

First Responder is the first person that is responsible to react towards an incident. To be a First Responder, one must know the steps taken to preserve the evidence as best as one could. The first responder should be prepared and his actions should be planned. Deliberate, rush or hurried actions could damage potential evidence. He/she should have a first responder toolkit and a predetermined incident response plan to follow regardless of the type of data being collected. The topics covered include:

- Who is First Responder?
- What are the Roles?
- When First Responder Comes In?
- How to Perform the Tasks?

5. Introduction to Data Imaging

Digital evidence can be collected from many sources; namely hard drives, memory devices, and web pages. Special care must be taken when handling computer evidence. Digital information can be easily tampered, and once tampered it is usually impossible to detect that a change has taken place (or to revert the data back to its original state) unless other measures have been taken. This topic will teach the participants on how to forensically acquire and preserve data. The topics covered include:

- Introduction
- Live Imaging
- Dead Imaging
- Hardware Based Tool
- Software Based Tool
- CSI: What to Expect?
- Conclusion

6. Image with FTK Imager

7. Autopsy

The next step after acquisition process is to analyze what has been acquired. In this topic, participants will be exposed with the analysis on digital evidence and writing a forensic report.

8. Quality Management for Digital Forensics

To produce high quality evidence and to ensure that it is admissible into the court, certain measures need to be taken by the laboratory and the analyst. This topic shall discuss in details the elements need to be considered when dealing with digital evidence. The topics covered include:

- Introduction
- ISO/IEC 17025
- Importance of Quality Management
- Management Requirements
- Technical Requirements
- Conclusion

9. Building a Digital Forensics Laboratory

How many staff should I employ? What are the tools that I need to purchase? What are the conditions that a storage room should have? How to ensure that the evidence is secured? All these questions will be answered in this topic.

For additional information, please visit www.cyberguru.my. You can also contact us at training@cybersecurity.my or call at 03 8800 7999

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my