COMPUTER FORENSIC

Course Syllabus

Cyber Security Professional Program

Subject Code: FOR0040a / Version: 1.0

Updated on 29/09/2021

Official content of **idCARE.UI**
Indonesia Cyber Awareness and Resilience Center

Supported by **JICA**
Japan International Cooperation Agency

Course Syllabus

As of 29 Sept 2021

Course Title	**COMPUTER FORENSICS**
Course goals	1. Build an in-house forensic capability using a variety of free, open-source, and commercial tools. Identify and handle digital artefact/evidence to answer critical questions, including application execution, file access, data theft, external device usage, file download, anti-forensics, and detailed system usage and Implement triage, live system analysis, and alternative acquisition techniques. 2. Compile reports and presents the findings during the digital forensics examination to the entity which was impacted by the cyberattack, or to the court for public investigation
Course Objective	1. Module 1: ● Able to recognize the origins of forensic science, the difference between scientific conclusions and legal decision-making. ● Able to explain the process of digital forensic workflow. ● Able to explain and make use of basic forensic tools. 2. Module2: ● Able to carry out the process to handle cases of digital forensic starting from acquiring, preserving, analyzing until reporting on data concerning a crime or incident. ● Able to analyze file imaging in windows. 3. Module 3: ● Able to perform live forensic analysis with automatic and manual tools. ● Able to identify sources of evidentiary value in various evidence sources including various computer files/logs, volatile data, and through disk forensics. 4. Module 4: Able to perform mac/ios extraction and analysis in terms of mac systems.
Participants	1. Information security professionals: Who want to learn in-depth concepts of digital forensics investigations 2. Incident response team members: Who regularly respond to complex cyber security incidents. 3. Law enforcement officers/agents: Who want to become a subject-matter expert on digital forensics. 4. Forensics investigators: Who works with law enforcement agencies, as well as private firms, to retrieve information from computers and other digital devices in relation to cyber incident or cybercrime.
Prerequisites	In this course, the handling of digital artifacts will be learned by analyzing cyber incidents and crimes involving computers so that basic knowledge about computer systems and digital storage media is needed.

Course contents and schedule

<u>40 sessions</u>

(1session = 50min)

Pretest

1. Module 1: Digital Forensics Essentials

Digital forensics essential focuses on the core principles: what is digital forensics and how to utilize digital investigations and digital evidence. This serves to teach users and potential users of digital forensics investigators, so they better understand what needs to be done and how their services can be better utilized. This not only serves as a basis for aspiring digital forensic practitioners, but also fills gaps in the fundamental understanding of existing digital forensic practitioners who want to take their abilities to a more advanced level.

This material will begin with theories about the definition, principles and processes of digital forensics, accompanied by case studies and complete practice of digital forensic processes starting from gathering evidence to reporting.

1.1. Introduction to digital forensics

1.2. Digital forensics definition, principles and evolution
- Forensic science
- Digital forensics
- Digital evidence

1.3. Digital forensics process
- Identification
- Acquisition & collection
- Examination
- Analysis

1.4. Digital forensics documentation, report and presentation
- How to write a report
- Report structure
- Findings

1.5. Digital forensics readiness
- Frameworks, standard and methodologies
- Legal/law aspects
- People
- Policy, procedure, guideline
- Technology, tools, infrastructures

Module 1 Practice:
- Digital evidence acquisition
  - Write blocker – with software & hardware tools
  - Forensic Imaging – imaging disk to file with FTK imager
  - Cloning With Clonezilla
- Digital evidence examination
  - Open file imaging with FTK imager
  - Open file imaging with autopsy
- Digital evidence documenting and reporting
  - reporting with autopsy

Module 1 Practical Test

Module 1 Test

2. Module 2: Computer and Windows Forensic Analysis

Computer and Windows forensic analysis focuses on developing basic computer forensics and in-depth digital forensic knowledge about the Microsoft Windows operating system. Participants will learn how to recover, analyze, and authenticate forensic data on computer systems and Windows systems, track the activities of certain users on the network, and organize findings for use in internal investigations, and civil/criminal litigation.

This topic discusses the handling of digital evidence on computers in general and in more depth with the Windows operating system, with more practice on how to acquire digital evidence from a computer, analyze files, windows registry, internet activities, etc.

2.1. Computer forensics
- Computer architecture
- File system and structure

2.2. Windows digital forensics and advanced data triage
- Need forensics software
- Types of computer forensics tools
- Tasks Performed by computer forensics tools
- UNIX/Linux command-line forensic tools
- GUI forensic tools
- Validating and testing forensic software
- Computer forensics examination protocol
- Acquisition
- Computer forensic analysis

2.3. Windows registry forensics and analysis
- Windows registry

2.4. Windows email, and event logs
- E-mail investigations in cyber crime
- Exploring the email architectures
- Term in mail server
- Protocol email
- Work flow of mail server
- Example spoofing email
- Example phishing
- Investigating email crimes and violations
- Examining email messages
- Viewing email headers
- Examining email headers
- Examining additional email files
- Tracing an email message
- Using network email logs
- Understanding email servers
- Examining linux email server logs
- Examining microsoft email server logs
- Using specialized email forensics tools
- Using a hex editor to carve email messages
- Recovery outlook files

2.5. Windows web browser forensics
- Browser forensics
- History web browser
- Cache web browser

- Cookie web browser
- Mozilla firefox
- Google chrome
- Open appdata
- Browsing history view
- Mozilla cache view

Module 2 Test

Module 2 Practice:

- Analysis Basic
- Recovery Data
- Analyze Digital Evidence With Autopsy
- File Signature Analysis
- Triage Acquisition
- Bypass Password Windows
- Email analysis

Module 2 Practical Test

3. Module 3: Live Forensics

When examining a computer or device that is turned on; a live forensics examination, the examiner has to collect volatile data. Volatile data includes information on what the device is currently up to. It also gives the examiner the opportunity to examine the memory and network activities and any other active data transaction. The ultimate goal of a live investigation is to preserve as much volatile data as possible and ensure that data resting on hard drives is available for later analysis.
Live forensics provides the essential skills needed for a digital forensic examiner to successfully triage system memory and network directly and analyze captured memory images and network traffic. Use the most effective freeware and open-source tools and provide an in-depth understanding of how these tools work, understand the structure of memory as it is to understand the structure of the disk and the registry. Having in-depth knowledge of memory and network allows the examiner to access specific target data for the needs of a case.

This topic will discuss the handling of digital evidence on live computer equipment (live computers), beginning with a discussion of theories about memory and networking with the direct practice of handling forensic data live from memory and network.

3.1. Live forensic

3.2. Memory forensics

- Memory forensics
- Data obtained from memory
- Virtual memory (swap space)
- Acquisition methods
- Memory forensics tools
- Memory acquisition tools
- Memory acquisition with ftk imager
- Volatility
- Memory analysis

3.3. Network forensics

- Internet protocols
- Network basics
- OSI & TCP/IP
- Network forensics overview
- Network logs
- Examining the honeynet project
- Simple network forensics
- Approach to network forensics
- Constraints
- Typical scenario
- Information available
- Analysis
- Reviewing network logs
- Using packet sniffers
- Tools
- Network analysis
- Summary

Module 3 Test

Module 3 Practice:

- Practice Network Forensic Analysis
  - Capture Network
  - Packet Data Protocol Filtering
- Memory Forensics Analysis
  - Capture Memory Data with FTK imager
  - Analysis Memory (Memory Forensics with Volatility)

Comprehensive Case Study

- Acquisition - Analysis - Report

Module 3 Practical Test

4. Module 4: Mac Forensic Analysis

Mac forensic analysis aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac, focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies.

This topic will discuss the handling of digital evidence on Mac/Apple-based computers, starting with understanding the file system, configuration, logs, user activities, etc. accompanied by direct practice of how to collect, handle and analyze the evidence.

4.1. Introduction to Mac System

- Apple and Mac history
- Mac OS version
- Mac hardware transition
- Mac OS architecture
- Mac forensic analysis tools
- OS X file system domains

	● OS X file system artifacts 4.2 Mac data acquisition ● Disk and partitions ● Acquisition tools ● Memory acquisition ● Volatile data ● Mounting disk image ● Disk eject & unmount 4.3 Application data Analysis ● Timestamp Formats ● SQLite Database ● SQLite Manager and Browser ● Property List Files 4.4 Mac Forensic Investigation ● System Information ● Active Network Connection ● Active Network Connection by Process ● Network Configuration ● User Logged on ● Running Process ***Module 4 Practice***: ● Collecting Artifacts ● Apple FSEvents Forensics ● MacOS forensic on Virtual Machine ***Module 4 Test*** ***Post test***
Scheme of Instructions	Lecture 40% hands-on training 60%
Keywords	Digital forensics, Windows forensics, Mac forensics, memory forensics, forensics investigation,
Tools and software required for hands-on training	1. Write blocker Tableau Hardware or Write blocker software (https://github.com/digitalsleuth/Registry-Write-Block) 2. FTK (https://accessdata.com/product-download/ftk-imager-version-4-2-0) 3. Clonezilla (https://clonezilla.org/) 4. Lazesoft (https://www.lazesoft.com/) 5. Exiftools (https://exiftool.org/) 6. Hex editor (ttps://mh-nexus.de/en/hxd/) 7. Steghide (http://steghide.sourceforge.net/) 8. Volatility (https://www.volatilityfoundation.org/) 9. Win-Ufo (https://www.caine-live.net/page2/page2.html) 10. Nirsoft Live forensic (https://www.nirsoft.net/)

	11. HirenbootCD (https://www.hirensbootcd.org/) 12. Kali linux (https://www.kali.org/) 13. SIFT (https://digital-forensics.sans.org/community/downloads)
Reference books	1. “Digital Forensics with Open Source Tools”, Cory Altheide and Harlan Carvey 2. “Computer Forensics and Cyber Crime: An Introduction”, Marjie T. Britz 3. “The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters