# IRH Advance Digital Forensics Investigation Techniques and Incident Response

## Course Introduction

Currently there are many attacks to corporate network. Securing corporate network and system is the proactive steps to protect corporate assets but there might be an attack that successfully gets into corporate system. Incident respond and computer forensics are reactive steps to handle and control the loss of corporate damages. A well incident respond can control the further loss of corporate assets and may lead to an investigation of an attack. IT professional should be ready for such an incident.

We will discuss on how to do forensic over various platforms such as Windows, Linux and MAC OSX. The techniques for evidence acquisition on both volatile and non-volatile data as well as data and file system analysis are covered in the course.

Participants will gain skills on collecting evidence and data analysis on well-known platforms by using professional forensics tools and can leverage the knowledge from this course for the other areas of forensics.

## Course Objectives

- To understand attacking methods and tools
- To learn where the evidences of attacks can be collected
- To learn how to interpret the evidences that attackers leave
- To experience a hands-on exercise of incident respond

## Course Highlights

- Windows and Linux Forensic tools provided
- Forensic Workstation Software
- Real World experience penetration testing from Instructor
- Free membership for ACIS Alumni
    - Access to the latest information related to the course subjects
    - A life-time class re-sit

## Learning Level

- Expert

## Course Duration

- 5 Days (30 Hours)

## Target Group

- IT Security Officer
- Digital Forensic Investigator

- Cyber Cop/Law Enforcement

## Course Outline

### Module 1: Introduction to Digital Forensics

- Real-World Incidents
- Introduction to the Incident Response Process
- What Is a Computer Security Incident?
- What Are the Goals of Incident Response?
- Incident Response Methodology
- Forensics LAB
    - Prepare for Forensic Workstation using Open Source Tools
        - SIFT (SANS Investigative Forensic Toolkit)
        - Helix
        - DEFT
- LAB: Installation Forensic Toolkit Live DVD

### Module 2: File system essentials

- File system layer (Physical and logical disks)
- Master Boot Record (MBR) and partition table
- Windows disk signature
- Allocated, unallocated, and slack space
- Metadata layer fundamentals
- File name layer fundamentals
- Introduction Linux File System
    - Ext file system

### Module 3: Windows File systems in-depth

- FAT12/16/32
    - File Allocation Table (FAT) structure
    - Root directory
    - Cluster chains
- NTFS
    - NTFS overview
    - Master File Table (MFT)
    - NTFS system files
    - NTFS metadata attributes ($Standard_Information, $Filename, $Data)

- NTFS timestamps
- Alternate data streams
- What happens when data is deleted from a NTFS file system?

**Module 4: Live Data Collection from Windows Systems**

- Important of Disk Duplication
- Obtaining Volatile Data
- Collecting Volatile Data
- Scripting Your Initial Response
- Performing an In-Depth Live Response
- Collecting the Most Volatile Data
- Collecting Live Response Data
- LAB: Data Collection using COFEE

**Module 5: Forensic Duplication**

- Forensic Duplication
- Forensic Duplicates As Admissible Evidence
- What Is a Forensic Duplicate?
- What Is a Qualified Forensic Duplicate?
- Forensic Duplication Tools
- LAB: Duplicating with dd and dcfldd

**Module 6: Data Analysis Techniques**

- Mounting raw and .E01 images
- Mounting physical and logical drive images
- Mounting split images
- Timeline analysis process
- MACB meaning by file system (NTFS vs. FAT)
- Rules of Windows timestamps for $STDINFO and $Filename
- Extract unallocated and slack space
- File carving using file headers/footers
- Extracting data using Inode/MFT/FAT directory entry
- File name pointers
- Recover deleted from file system
- LAB: Using Sleuth Kit ,Autopsy ,PTK to analyze disk image
- LAB: File Carving using Foremost

**Module 7: Memory Analysis**

- Memory analysis techniques
- Identify rogue processes
- Analyze process DLLs and handles
- Review network artifacts
- Look for evidence of code injection
- Memory Timelining
- Memory registry examinations
- LAB: Memory analysis using Volatility Framework
- LAB: Memory analysis using MANDIANT

**Module 8: Advance Forensics Analysis Techniques**

- Investigating the APT, organized crime hackers, and hackivists
- Memory analysis
- File system timeline analysis
- Recovering key windows files
- Finding malware
- Metadata Analysis
- Malware Analysis
    - Executable file Analysis
    - Document Analysis
        - Microsoft Office analysis (Macro)
        - PDF Analysis
- Social Network Forensics
- LAB: Metadata Analysis Tools
- LAB: Social network Forensic Tools
- LAB: PDF and Document Forensic Tools

**Module 9: Investigating Microsoft windows**

- Investigating Windows File system
- Investigating Registry
- Investigating Internet Activity
- Extract Content(File Carving)
- LAB: Analyze Registry
- LAB: Analyze Internet Activity

**Module 10: Image Files Forensic**

- Introduction to image files
- Recognize image files
- Locate and recover image files
- Analyze image file headers
- Analyze Geo-Location from Image files
- LAB: Analyze Image file
- LAB: Geo-Location Analysis

**Module 11: Network Evidence Extraction**

- Gather evidence from network devices
- Generate Packet Dump Metadata
- Create Network Event timeline
- Type of Packets
- Extract Traffic Content(File Carving)
- Reconstruct Web histories and cached Web content

**Module 12: Network Forensics Tools**

- Demonstrate Network Forensic tools
    - Wireshark
    - Ngrep and TCPExtract
    - Network Miner
    - Xplico
    - Commercial Tools
        - CACE Pilot
- LAB: Using Network Forensic Tools
- LAB: Network Forensic from Scenarios

**Module 13: Mobile Forensics**

- Introduction to Mobile network
- Introduction to Mobile forensics
- SIM Cards Forensics
- Smartphone Imaging tools
- How to Forensic smartphone from backup files
    - Extract Data from Backup files
- Smartphone forensics with Commercial tools

**สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)**

คุณธนภัทร ไชยพิมล
Mr. Tanapat Chaipimol
Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776
Mobile: (66) 86-330-8532
Email: tanapat.ch@acisonline.net

คุณกิตมณี นิยมญาติ
Ms. Kitmanee Niyomyat
Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776
Mobile: (66) 86-325-7129
Email: kitmanee.ni@acisonline.net

**ACIS Professional Center Co.Ltd.**

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330
Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: registration@acisonline.net
Website: www.acisonline.net