PROFESSIONAL TRAINING COURSE

3 Days Course on

Introduction to Digital Forensic First Responder (DF)

TWO SIGMA TECHNOLOGIES

Two Sigma Technologies
Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel : 018-3651369/Fax :03-61880602
zurina@2-sigma.com
www.2-sigma.com

Introduction to Digital Forensic First Responder (DF)

This course will provide a foundation in the field of Computer Forensics. The student will learn how to obtain and analyse digital information for possible use as evidence in civil, criminal or administrative cases. Topics include applications of hardware and software to computer forensics, computer forensics law, volume and file system analysis, computer forensics investigations, and computer forensics in the laboratory. Hands-on exercises guide discussions and reinforce the subject matter.

This course is designed as an introductory course in computer forensics. Students will first understand the need for computer forensics. Students will learn best practices for general incidence response. The course will then focus on the tools and techniques to perform a full computer forensic investigation.

Course Settings

Date	Refer to Training Calendar
Venue	Refer to Training Calendar
Fees	Contact Us at sales@2-sigma.com
Timings	0900-1700 (3 Days)
Inclusive	Certificates and notes
Audience	The course has been designed for IT personnel, administrators, computer support staffs and an end-user who are aware the importance of data in their storage. No previous repair or data recovery experience necessary.

Data Recovery -Schedule

Day 1	
09.00am – 10.00am	**Introduction to Computer Forensics** • Course overview • Understanding the need for computer forensics • Defining computer forensics
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	**Computer Hardware** • Understanding the computer components • Digital Media • Hard disk basics **Computer Forensic Incidents** • Introduction • The Legal System • Criminal Incidents • Civil Incidents • Computer Fraud • Internal Threats • External Threats • Investigative Challenges
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	**Digital Incident Response** • Digital Incident Assessment • Initial Assessment · Type of Incident · Parties Involved • Incident / Equipment Location • Available Response Resources • Securing Digital Evidence • Chain of Custody • Potential Digital Evidence **OS / Disk Storage Concepts** • OS / Disk Storage Concepts • Disk Based Operating Systems • OS / File Storage Concepts • Disk Storage Concepts 1 • Demo - Creating a file and writing it to FAT/NTFS • Disk Storage Concepts 2 • Slack Space • File Management · File Formats •

Day 2	
09.00am – 10.00am	**Digital Acquisition & Analysis Tools** • Digital Acquisition & Analysis Tools • Digital Acquisition • Terms Defined • Demo - Generic Hash Demo / Crypto Demo • Demo - Hashing a File • Digital Acquisition Procedures 1 • Demo -Winhex Software • FTK Explorer / OsForensic • Demo - Osforensic Acquisition • Digital Acquisition Procedures 2 • Digital Forensic Analysis Tools • Demo - Autopsy
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	**The Forensic Toolkit** • Forensic hardware • Hardware write/blockers • Hard drive acquisitions • Processing the scene • Lab 1: Hard drive acquisition **E-mail Analysis** • Viewing e-mail • Webmail • POP • IMAP
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	**File Signature Analysis** • File signatures • File extensions • Differences between • Identifying differences • Reading: Instructor Handouts **Forensic Examination Protocols** • Forensic Examination Protocols • Demo - Create Disk Images • Demo - Data Recovery Exercise • “The 20 Basic Steps”

	• Demo - File Carving Exercise
Day 3	
09.00am – 10.00am	**Other Windows Artifacts** • Common windows artifacts • Recycle bin • My Documents • Recent files • Installed programs • Lab 8: Basic Computer Forensics Lab
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	**Image Restoration** • Live Acquisition • Recovery and Searching • Password Cracking and Encryption **Data Carving** • Data recovery: identifying hidden data, Encryption/Decryption, • Steganography, • Recovering deleted files. • Digital evidence controls: uncovering attacks that evade detection by Event Viewer, Task Manager. • Windows GUI tools, data acquisition, disk imaging, recovering swap files, temporary &cache files
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	**Anti-Forensics** • Traditional methods ○ Overwriting Data and Metadata ○ Cryptography, Steganography, and other Data Hiding Approaches ○ Decrypting EFS • Non-traditional methods ○ Targeting forensic tool blind spots ○ Targeting forensic tool vulnerabilities ○ Targeting generic tool/lib vulnerabilities **Digital Evidence Presentation** • Processing a complete forensic case • Preparing a forensic report • Digital Evidence Presentation • The Best Evidence Rule conclusion

More Information

Two Sigma Technologies
19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel: 018-3651369/Fax: 03-61880602

To register, please email to zurina@2-sigma.com or fax the registration form to 03-61880602, we will contact you for further action.