Forensic Techniques for End user Raids

A two day practical training course for investigators who are required to deal with live computers during onsite raids. The course has an emphasis on investigators who conduct end user raids but is suitable for anyone who needs to extract data from a live computer in an evidentially sound manner The course will provide the candidate with an understanding of computer forensics principles and techniques regularly employed by computer forensic investigators. The candidate will work through a series of exercises and train how to deal with live computers and conduct a focused investigation using a range of forensic tools. A certificate of completion will be provided on successful completion of the course.

Aim of the Course:

The aim of the course is to provide the candidate with an understanding of:

- Computer forensic principles and techniques.
- How to conduct a focused investigation.
- How to manually extract data from the live computer.
- How to extract data from a live computer in an evidentially sound manner using a range of forensic tools.

Course Level:

The course is aimed at investigators who are required to deal with live computers during onsite raids. Laptops will be provided for each course candidates.

Course Location:

Siam Computer and Language school, Victory Monument branch

471/19 Ratchawithi Road, Ratchathewi, Bangkok, 10400

Course Date:

09:00 to 16:00, 6th – 7th June 2013

Course Cost:

1000 USD

Orion Investigation Co. Ltd
Unit 2001-2002, 20th Floor, BBC Building, 29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110, Tel 02 714 3801, Fax 02 714 3804

Course content:

What is Digital Forensics?	Sources of Evidence
The Four Principles of Computer Based Evidence	Preparing for Onsite Raids
Types of Data	Exporting FTK Imager to USB Pen Drive
The Four Levels of Computer Data	OSForensics
Physical Acquisitions	Installing OSForensics
Hash Values	Investigation Scenario
Evidence Handling and Chain of Custody	Identifying Installed Software
Investigation Fundamentals	Examination of the Application Event Log
FTK Imager	Extracting Serial Numbers/Product Keys
Installing FTK Imager	Extracting Microsoft Windows/Office Product keys
Creating a Forensic Image	Extracting Details of User Created Files
Forensic Previews	Registry Examination
Mounting a Forensic Image	System Files
Time & Date Stamps	Analysis of the Prefetch Files
Data Storage	Forensic Approach
The Unallocated Space	Creating Custom Content Forensic Image
Traditional Approach to Digital Forensics	Creating a File Listing
Scenario 1	Recovery of Deleted Files
Live Forensics	Master File Table (MFT)
Capturing Volatile Data	Analysis of the RegBack Folder
Focused Approach to Digital Forensics	Analysis of the Registry Backup File
Software Piracy	Reporting
Identifying Sources of Evidence	Summary

Further Information

For further information and booking form, please contact Orion Investigations. Email: forensics@orionforensics.com

Orion Investigation Co. Ltd
Unit 2001-2002, 20th Floor, BBC Building, 29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110, Tel 02 714 3801, Fax 02 714 3804