Digital Forensics Foundation Training

A 4 day practical training course for people who are responsible for digital forensic investigations or are wishing to become a digital forensic investigator. The course will provide a solid foundation in the understanding of digital forensics principles and techniques. Each subject is covered in depth and supported by practical scenario based exercises to reinforce the learning points. The candidate will use a range of free and open source forensic tools. This allows the candidate the opportunity to practice what they have learnt on the course without the need to invest in expensive forensic software / hardware. The course has been designed by experienced forensic investigators with many years' experience ensuring the course content is both relevant and practical.

Course Level:

The course is aimed at people who are responsible for digital forensic investigations or are wishing to become digital forensic investigators, including: IT security professionals and law enforcement officers.

Course Location:

Siam Computer and Language school, Victory Monument branch

471/19 Ratchawithi Road, Ratchathewi, Bangkok, 10400

Course Date:

TO Be Confirmed

Course Cost:

39,800 Baht

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:

1 – Introduction to Digital Forensics • Define Digital Forensics • Define the types of Forensic Investigations • Legal Considerations	**7 - File Systems & Data Storage** • Introduction to File Systems • Data Storage • File System Metadata • Live, Deleted and Unallocated Data • File Slack and Ram Slack • NTFS Compression and Encryption
2 - Investigation Fundamentals • Best Practice Guidelines • The Four Principles of Computer Based Evidence • The basics of information gathering	**8 – File Information** • Date and Time Stamps • File Metadata
3 - Identification and seizure of digital equipment • Evidence Handling & Chain of Custody • Identifying Electronic Sources of Evidence • Seizure of Electronic Devices	**9 - Forensic Analysis Techniques** • Analysis Environments • Case Preparation • Folder / File Recovery • File Signatures and Data Carving • Data Reduction and Hash Analysis • Keyword Searching • Evidence Corroboration
4 - Forensic Acquisitions • Forensic Acquisitions • Forensic Image • Forensic Clone • Forensic Image vs. Forensic Clone • FTK Imager • Hash Values	**10 – Windows OS Artefacts** • The Windows Registry • Internet History • Link Files • Previously connected USB Devices • Log Files • Prefetch Files
5 - Understanding Digital Data • Binary Digits • Binary Conversion • Storage Devices • Understanding Electronic Data	**11 – Forensic Challenges** • SSD Drives • Encryption and Passwords • Cloud Forensics
6 - Understanding Hard Drive Terminology • Physical Drives • Understanding Hard Drive Terminology • Unified Extensible Firmware Interface (UEFI) • GUID Partition Table (GPT)	**12 – Reporting** • Purpose and layout of Report • Content of Report

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