Digital Forensics Foundation Training

หลักสูตรการฝึกอบรม 4 วันเป็นหลักสูตรที่เหมาะสำหรับบุคคลทั่วไปที่สนใจด้านการพิสูจน์หลักฐานทางดิจิทัล (digital forensics) หลักสูตรนี้จะช่วยสร้างความเข้าใจขั้นพื้นฐานอย่างลึกซึ้งในการพิสูจน์หลักฐานทางดิจิทัล รวมถึงทางด้านเทคนิคต่างๆ โดยจะครอบคลุมเนื้อหาเชิงลึกและฝึกปฏิบัติตามวัตถุประสงค์การเรียนรู้ในแต่ละขั้น ผู้ฝึกอบรมจะได้ทดลองใช้เครื่องมือที่เป็น open source ซึ่งจะได้เรียนรู้และทดลองปฏิบัติตามหลักสูตรโดยไม่ต้องเสียค่าใช้จ่ายเพิ่มเติมในการใช้ซอฟต์แวร์และฮาร์ดแวร์

หลักสูตรนี้ทั้งภาคทฤษฎีและปฏิบัติได้รับการออกแบบโดยผู้เชี่ยวชาญและมีประสบการณ์อย่างสูงทางด้านการพิสูจน์หลักฐานทางดิจิทัล (digital Evidence) ซึ่งผู้เชี่ยวชาญเคยเป็นอดีตตำรวจจากประเทศอังกฤษ มีประสบการณ์ตรง ด้าน Digital Forensics และมีประสบการณ์ในการเป็นวิทยากรจัดอบรมให้กับหน่วยงานต่างๆ ทั้งภาครัฐ เช่นสำนักงานตำรวจแห่งชาติ และเอกชน ทั้งในอังกฤษ ยุโรป และประเทศไทยเป็นเวลากว่า 15 ปี

ครอบคลุมเนื้อหาดังนี้ :

- ความสำคัญกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
- ประเด็นทางกฎหมายในการได้มาซึ่งพยานหลักฐานดิจิทัล
- กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ถูกต้องตามหลักมาตรฐานสากล (Forensics Procedures) และเครื่องมือ (Forensics Tools) สำหรับการเก็บรักษาพยานหลักฐานดิจิทัล
- การวิเคราะห์ข้อมูลทางอิเล็กทรอนิกส์
- การนำเสนอรายงานพยานหลักฐานดิจิทัล (Forensics Report) ในกระบวนการทางกฎหมาย
- หลักสูตรนี้ใช้มาตรฐานเดียวกันกับ The Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic (UK) (ACPO) และเนื้อหาในหลักสูตรบางส่วนสอนในระดับปริญาโทในประเทศอังกฤษ

เหมาะสำหรับใคร:

หลักสูตรนี้เหมาะสำหรับบุคคลทั่วไปที่สนใจด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล และช่วยสร้างความเข้าใจแนวทางเก็บข้อมูลหลักฐานดิจิทัล รวมถึงเทคนิคต่างๆ โดยจะครอบคลุมเนื้อหาเชิงลึกและฝึกปฏิบัติตามวัตถประสงค์การเรียนรู้ในแต่ละขั้น ผู้ฝึกอบรมจะได้ทดลองใช้เครื่องมือที่เป็น Open Source ซึ่งจะได้เรียนรู้และทดลองปฏิบัติตามหลักสูตรโดยไม่ต้องเสียค่าใช้จ่ายเพิ่มเติมในการใช้ซอฟแวร์และฮาร์ดแวร์ และผู้เข้าอบรมต้องมีพื้นฐาน it

วัตถุประสงค์:

หลักสูตรจะมุ่งเน้นบุคคลที่มีหน้าที่รับผิดชอบในการตรวจสอบพิสูจน์หลักฐานทางดิจิทัลหรือกำลังคิดที่จะเป็นผู้ตรวจสอบหรือผู้เชี่ยวชาญพิสูจน์หลักฐานทางดิจิทัล รวมถึงเจ้าหน้าที่ IT ,It Security ,เจ้าหน้าที่ทางกฎหมาย

Orion Investigations Co Ltd
16th, 20th,25th Floor, Unit 1601,2001-2002,2501 BBC Building, 29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110 Thailand.
Tel : +66-2-7143801 to 3 Fax : +66 (0) 2 714 3804

Course Location:

Orion Investigations Co Ltd 20th Flr, ,Bangkok Business Building (BBC),29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110 Thailand.

Course Date:

To be advised

Course Cost:

42,586 THB(Included Vat)

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

Orion Investigations Co Ltd
16th, 20th,25th Floor, Unit 1601,2001-2002,2501 BBC Building, 29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110 Thailand.
Tel : +66-2-7143801 to 3 Fax : +66 (0) 2 714 3804

Further Information

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

In-House Training please contact sales directly

Orion Investigations Co Ltd
16th, 20th,25th Floor, Unit 1601,2001-2002,2501 BBC Building, 29 Sukhumvit 63 North Kong Tan, Wattana, Bangkok 10110 Thailand.
Tel : +66-2-7143801 to 3 Fax : +66 (0) 2 714 3804