



CFAIRT # 4 Computer Forensics Awareness



Incident Response training For IT Staff -One Day Course-

หลักสูตรฝึกอบรมความสำคัญของการทำ Computer forensics และการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

รายละเอียดของหลักสูตร
และใบจอง

สอบถามและสำรองที่นั่ง...
โทรศัพท์ 02-714-3801-3
แฟกซ์ 02-714-3804
forensics@orionforensics.com
www.orionforensics.com

1

เหมาะสำหรับใคร

หลักสูตรอบรมในการทำความเข้าใจในหลักฐานทางดิจิทัล ระยะเวลา 1 วัน สำหรับพนักงาน IT ในการจัดการกับภัยคุกคามด้านความปลอดภัยในโลกไซเบอร์ โดยหลักสูตรจะอธิบายความหมายของ Computer Forensics และเทคนิคเบื้องต้นสำหรับผู้ที่เกี่ยวข้องกับการทำ Computer Forensics ผู้เข้ารับการฝึกอบรมจะได้เรียนรู้วิธีการเบื้องต้นต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์และวิธีการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ โดยใช้เครื่องมือและวิธีการทางด้าน Computer Forensics

2

วัตถุประสงค์

เพื่ออธิบายความหมายของ Computer Forensics, การได้มาซึ่งหลักฐานทางคอมพิวเตอร์และเทคนิคการทำ Computer forensic ตามแบบที่ผู้เชี่ยวชาญปฏิบัติ เพื่อให้ผู้เข้าอบรมได้รับความรู้เพื่อจะได้วางแผนเตรียมรับมือกับเหตุการณ์ที่อาจจะเป็นภัยคุกคามจากโลกไซเบอร์ และอบรมการใช้เทคนิคการทำ Computer Forensics เพื่อให้สามารถเก็บรักษาข้อมูลได้อย่างถูกต้อง

3

ระดับของหลักสูตร

พนักงาน IT ขององค์กรต่างๆที่ยังไม่มีความรู้เกี่ยวกับการทำ Computer Forensics และเทคนิคการทำ Computer Forensics เบื้องต้น

เนื้อหาในการฝึกอบรม

- Introduction แนะนำหลักสูตร
- About the Course เกี่ยวกับหลักสูตรHigh lights from the 2011 Global Economic Crime Survey ตัวอย่างเหตุการณ์ที่เกิดขึ้น
- What is Computer Forensics? Computer Forensics คืออะไร
- Sources of Evidence แหล่งที่มาของหลักฐาน
- Why is Computer Forensics Important to your Organization? ทำไมการทำ Computer Forensics จึงมีความสำคัญต่อองค์กรของคุณ
- The Four Principles of Computer Based
- หลักการในการหาหลักฐาน ทาง Computer
- The Forensic Image การคัดลอกข้อมูล
- Cloned Drives การโคลนนิ่งฮาร์ดดิสก์
- The Four Levels of Computer Data ระดับของข้อมูล
- The Unallocated Spaceพื้นที่ว่างในฮาร์ดดิสก์
- Types of Data ชนิดของข้อมูล
- Hash Valuesการทำลายนิ้วมือให้กับข้อมูล
- Dates and Timesวันและเวลา
- Previewing Computer verses Forensic Image
- การเปรียบเทียบระหว่างการข้อมูลแบบปกติกับแบบ Computer Forensics
- FTK Imager โปรแกรม FTK Imager
- Installing FTK Imager การติดตั้ง โปรแกรม FTK Imager
- Exercise – Previewing Hard Drive ฝึกปฏิบัติการดูข้อมูล
- Exercise – Creating Forensic Image ฝึกปฏิบัติการทำ Forensic Image
- Exercise – Creating Custom Content Forensic Image ฝึกปฏิบัติการทำ Forensic Image แบบเลือกเฉพาะส่วนที่สนใจ
- Mounting a Forensic Image การดูข้อมูล Forensic Image ในรูปแบบเสมือนจริง
- Exercise - Mounting a forensic Image ฝึกปฏิบัติการดูข้อมูล Forensic Image ในรูปแบบเสมือนจริง
- Memory Capture การเก็บข้อมูลจาก Ram หรือหน่วยความจำ
- Exercise 5.0 – Capturing RAM Memory ฝึกปฏิบัติการเก็บข้อมูลจาก Ram หรือหน่วยความจำ
- Analyzing Memory Files วิเคราะห์หน่วยความจำ
- Exercise 6.0 – Analyzing Memory File ฝึกปฏิบัติการวิเคราะห์หน่วยความจำ
- Incident Response การรับมือกับเหตุการณ์ที่ไม่คาดคิด
- Responding to Incidents การปฏิบัติเมื่อเกิดเหตุ
- Incident Response Plan แผนการรับมือกับเหตุการณ์ที่ไม่คาดคิด
- Demonstration of the functionality of AccessData forensic software, FTK การสาธิตการใช้งานโปรแกรม FTK

ค่าลงทะเบียน
-9,950บาท/คน
*อาหารม Coffee Break 2 เวลา
*อาหารกลางวัน

สถานที่
-โรงเรียนสยามคอมพิวเตอร์และภาษา
สาขานุสาวรีย์ชัย (ฝั่งถนนดินแดง) กทม

วันและเวลา
-วันที่ 06 กันยายน 2556
-เวลา 09.00-16.00 น.

www.orionforensics.com
www.orioninv.co.th

English Course Details ...Click

Computer Forensics คืออะไร...คลิก

