TTDF03 : Windows Forensics Analysis Course

Description :

หลักสูตรสำหรับผู้ที่ผ่านการอบรมหลักสูตร Computer Forensics Awareness and Incident Response Training มาก่อน และมีความรู้พื้นฐานด้านเทคนิคเกี่ยวกับระบบปฏิบัติการวินโดวส์ เน้นเจาะลึกในการใช้เครื่องมือทางนิติวิทยาศาสตร์ต่างๆ เพื่อตรวจสอบและวิเคราะห์หลักฐานดิจิทัลในระบบ Windows

Instructor :

avatar
Image not found or type unknown

อาจารย์สมิทธ์ ณ นคร
Hi-Tech Leader, Orion Investigations

Training Date : **20-21 October 2026**
fee : **10,000 ฿** (ราคายังไม่รวม Vat 7%)
Days & Duration : **2 Day(s) | 12 Hour(s)**
Time : **09:00:00 - 16:00:00**
Language : **Thai**
Venue : **Training Room 3rd floor, Software Park Building Chaengwattana Road, Nonthaburi**
Type : **Classroom**
Category : **Digital Forensics**

Objectives :

- เพื่อให้ผู้เรียนได้เรียนรู้วิธีการใช้เครื่องมือทางนิติวิทยาศาสตร์ต่างๆ เพื่อตรวจสอบและวิเคราะห์หลักฐานดิจิทัลในระบบ Windows
- เพื่อให้ผู้เรียนมีการพัฒนาทักษะการปฏิบัติ เพื่อระบุหลักฐานดิจิทัลที่เกี่ยวข้องจากระบบ Windows
- เพื่อให้ผู้เรียนสามารถใช้เครื่องมือสำหรับการวิเคราะห์ การตีความ และรายงานผลการค้นพบ ในลักษณะที่สามารถอธิบายหลักฐานดิจิทัลได้

Target Group :

- System Admin, IT Admin
- IT Staff, IT Support, Helpdesk
- Incident Response Team (IR)
- Cyber Team, Security Team, IT Team
- ทีม Digital Forensics Analyst ที่ต้องการเรียนรู้เทคนิค และวิธีการใช้เครื่องมือทางนิติวิทยาศาสตร์ต่างๆ
- ผู้จัดการ, หัวหน้างาน หรือบุคลากรทางไอที ที่ต้องการเรียนรู้การสืบสวนทางนิติวิทยาศาสตร์ของ Windows (Windows Forensics Analysis)
- ผู้เรียนต้องผ่านการอบรมหลักสูตร Computer Forensics Awareness and Incident Response Training มาก่อน และมีความรู้พื้นฐานด้านเทคนิคเกี่ยวกับระบบปฏิบัติการวินโดวส์

Benefits :

หลังจบหลักสูตรนี้ ผู้เข้าอบรมจะ...

- มีความรู้และความเข้าใจ มีทักษะและเทคนิค สำหรับการสืบสวนทางนิติวิทยาศาสตร์ของ Windows (Windows Forensics Analysis)
- สามารถใช้เครื่องมือ Open Source สำหรับการวิเคราะห์หลักฐานดิจิทัล, การระบุตำแหน่งของหลักฐานเพื่อตอบคำถามที่สำคัญ
- มีความเข้าใจเทคนิคทางนิติวิทยาศาสตร์ที่ใช้ในการตรวจสอบและวิเคราะห์สิ่งต่างๆ ที่เก็บไว้ในระบบปฏิบัติการ Microsoft Windows
- ได้ร่วมแลกเปลี่ยนประสบการณ์กับผู้เชี่ยวชาญ และสามารถนำความรู้ที่ได้รับไปประยุกต์ให้เกิดประโยชน์ต่อการปฏิบัติงานในองค์กรและต่อตนเอง

Course Outline :

Day 1: Windows Artifacts

Section 1 – Windows Artifacts

- Windows Registry
- USB Forensics
- Prefetch Files
- Link File Analysis
- Jump Lists
- Thumbcache
- Volume Shadow Copies
- Event Logs
- Recycle Bin
- NTFS Journaling
- Internet History

Day 2: Windows Analysis

Section 1 – Basic Concepts

- Types of Digital Evidence
- Dealing with Theft of Company Data

Section 2 – Case and Data Sources

- CASE AND DATA SOURCE

- PROCESSING & LAYOUT
- FILE SYSTEM VIEW
- OTHER VIEWS & RESULTS VIEW

Section 3 – Analyzing Data Sources

- KEYWORD SEARCH
- TIMELINE
- BOOKMARKS & TAGS

Section 4 – Reporting

- Reporting
- Exercise – Dealing with Theft of Company Data

Payment Condition :

Payment can be made by:

1. **Cash or Credit Card or Bank Cheque payable to**
   สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ or National Science and Technology Development Agency
   (a post-dated cheque is not accepted) on the first day of the service or within the last day of the service.

2. **Account transfer and send the proof of the payment** (the deposit slip) via email ttd@swpark.or.th

   - **ธนาคารกรุงเทพ** สาขาอุทยานวิทยาศาสตร์
     Saving Account Number: **080-0-00001-0**
     Account Name: **สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ**

   - **ธนาคารกรุงไทย** สาขาตลาดไท
     Saving Account Number: **152-1-32668-1**
     Account Name: **สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ**

Notes:

- Withholding tax (3%) is exempt.
- Should you need to withdraw, you must send the notice of the withdrawal in writing no later than 7 working days before the commencement date. The cancellation less than 7 days will be subject to a fine of 40% of the fee.
- Software Park Thailand reserves the rights to cancel courses due to unforeseen circumstances.

Contact Person :

For more information, contact our course coordinator on:

เสกสรรค์ สังสุข (อิฐ)
Mr. Seksun Sungsook
: +662 583 9992 Ext. **81421**
: +6681 913 1828
: seksun.sun@nstda.or.th

You are encouraged to use the course schedule as a guide to plan your training. The schedule is accessible at www.swpark.or.th for more information.

LINE เพิ่มเพื่อน