TTDF01 : Digital Forensics - Unlocking the Secrets

Description :

เมื่อ Cyber Threats คุกคาม และ Cyber Awareness อาจไม่เพียงพออีกต่อไป **Digital Forensics (นิติวิทยาศาสตร์ทางดิจิทัล)** จึงเป็นอีกหนึ่งทักษะความรู้ที่ทุกคนควรทราบ เพื่อให้เข้าใจเทคนิคและแนวทางปฏิบัติในการสืบสวนเพื่อหาหลักฐานนิติวิทยาศาสตร์ทางดิจิทัล ตลอดจนสามารถเข้าใจ จัดการ และจัดเก็บหลักฐานทางดิจิทัล (Digital Evidence) ที่สำคัญและมีความสมบูรณ์เพื่อให้สามารถนำไปใช้ในกระบวนการกฎหมายต่อไป

Instructor :

avatar
Image not found or type unknown

อาจารย์สมิทธ์ ณ นคร

Hi-Tech Leader, Orion Investigations

Training Date : **20 August 2026**

fee : **5,000 ฿** (ราคายังไม่รวม Vat 7%)

Days & Duration : **1 Day(s) | 6 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 :

ปัจจุบันการทำงานและการดำเนินชีวิตของทุกๆ คน จะเกี่ยวข้องกับโลกออนไลน์ซึ่งสามารถเข้าถึงและใช้งานได้สะดวก มีการให้ความรู้เพื่อสร้างความตระหนักด้าน IT Security Awareness แก่บุคลากร รวมถึงทางหน่วยงานได้จัดเตรียมระบบความปลอดภัยเพื่อรักษาและสร้างความมั่งคงปลอดภัยต่อข้อมูลแต่ในขณะเดียวกันภัยคุกคามทางไซเบอร์ (Cyber Threats) และการหลอกลวงทางโลกออนไลน์ก็มีการพัฒนารูปแบบที่หลากหลายและทำให้เกิดการหลงกลได้โดยง่ายมากขึ้น จนก่อให้เกิดการถูกหลอกลวง/ละเมิด/คุกคามด้านข้อมูลและทรัพย์สิน สร้างความเสียหายเป็นจำนวนมากในแต่ละปี

ดังนั้น การให้ความตระหนักรู้ (Awareness) และการป้องกัน (Preventive Maintenance) อาจไม่เพียงพอแล้วสำหรับการทำงานและการดำเนินชีวิตในปัจจุบัน จึงขอเรียนเชิญทุกท่านเข้าร่วมเรียนรู้และสร้างความเข้าใจเรื่อง Digital Forensics (นิติวิทยาศาสตร์ทางดิจิทัล) คืออะไร มีเทคนิคและวิธีการอย่างไร ตลอดจนสามารถเข้าใจ จัดการ และจัดเก็บหลักฐานทางดิจิทัล (Digital Evidence) ที่สำคัญ และมีความสมบูรณ์อย่างทันท่วงที เพื่อประโยชน์ต่อการใช้ในกระบวนการกฎหมายต่อไป

วัตถุประสงค์:

- เพื่อให้ผู้เรียนได้รับรู้และเข้าใจถึง Cyber Threats หรือ ภัยคุกคามทางไซเบอร์
- เพื่อให้ผู้เรียนมีความรู้ความเข้าใจ Digital Forensics (นิติวิทยาศาสตร์ทางดิจิทัล) คืออะไร มีเทคนิค วิธีการ และแนวทางปฏิบัติในการสืบสวนเพื่อหาหลักฐานนิติวิทยาศาสตร์ทางดิจิทัลได้อย่างไร (Digital Forensics)
- เพื่อให้ผู้เรียนเข้าใจว่าอะไรคือหลักฐานทางดิจิทัล (Digital Evidence) ประเภทของหลักฐานทางดิจิทัล และแนวทางการรวบรวมหลักฐานดิจิทัลที่ถูกต้องและสมบูรณ์เพื่อให้สามารถนำไปใช้ในกระบวนการกฎหมายต่อไป

Target Group :

- บุคคลทั่วไป (ทุกท่านที่สามารถใช้งานโปรแกรมหรือ Application ในระบบออนไลน์ได้) และต้องการเรียนรู้และมีความเข้าใจในนิติวิทยาศาสตร์ทางดิจิทัล (Digital Forensics)
- บุคลากรในสายไอที/ดิจิทัล
- บุคลากรในอุตสาหกรรมประกันภัย สถาบันทางการเงิน และอื่นๆ
- เจ้าหน้าที่กฎหมายหรือทนาย เจ้าหน้าที่ Audit

Benefits :

หลังจบหลักสูตรนี้ ผู้เข้าอบรมจะ...

- รับรู้และเข้าใจถึง Cyber Threats หรือ ภัยคุกคามทางไซเบอร์
- มีความรู้ความเข้าใจถึง Digital Forensics (นิติวิทยาศาสตร์ทางดิจิทัล) ว่าคืออะไร มีเทคนิค วิธีการ และแนวทางปฏิบัติในการสืบสวนเพื่อหาหลักฐานนิติวิทยาศาสตร์ทางดิจิทัลได้อย่างไร
- เพื่อให้ผู้เรียนเข้าใจว่าอะไรคือหลักฐานทางดิจิทัล (Digital Evidence) ประเภทของหลักฐานทางดิจิทัล และแนวทางการรวบรวมหลักฐานดิจิทัลที่ถูกต้องและสมบูรณ์เพื่อให้สามารถนำไปใช้ในกระบวนการกฎหมายต่อไป
- เข้าใจคำศัพท์ทางเทคนิคที่ใช้โดยนักนิติวิทยาศาสตร์ การตระหนักถึงปัญหาที่อาจเกิดขึ้นจากหลักฐานดิจิทัล สามารถประเมินความถูกต้องและความสมบูรณ์ของหลักฐานดิจิทัล
- ได้ร่วมแลกเปลี่ยนประสบการณ์กับผู้เชี่ยวชาญ และสามารถนำความรู้ที่ได้รับไปประยุกต์ให้เกิดประโยชน์ต่อการปฏิบัติงานในองค์กรและต่อตนเอง

Course Outline :

1. **Cyber Threats**
2. **Introduction to Digital Forensics**
    a. Define Digital Forensics
    b. Legal Considerations
    c. How Courts Assess the Integrity of Electronic Evidence
3. **Investigation Fundamentals**

a. Best Practice Guidelines
b. The Four Principles of Computer Based Evidence
c. Identifying Electronic Sources of Evidence
d. The Four Levels of Computer Data
e. Live / Deleted Data

4. **Forensic Techniques / Terms Explained Computer forensics**
   a. Forensic Image
   b. Forensic Clone
   c. Hash Values (digital fingerprint)
   d. Forensic Acquisition Reports
5. **Understanding Digital Evidence**
   a. Time and Date Stamps (what you need to know)
   b. File Metadata (the hidden information)
   c. Internet History
   d. Email Headers
6. **Types of Digital Evidence**
   a. Types of Digital Evidence
   b. Dealing with Theft of Company Data
   c. Dealing with Websites
7. **Preparing Digital Evidence for Court**
   a. How to Prepare a Forensic Report?
   b. How to Prepare Evidence for Court?
   c. Giving Evidence as an Expert Witness

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