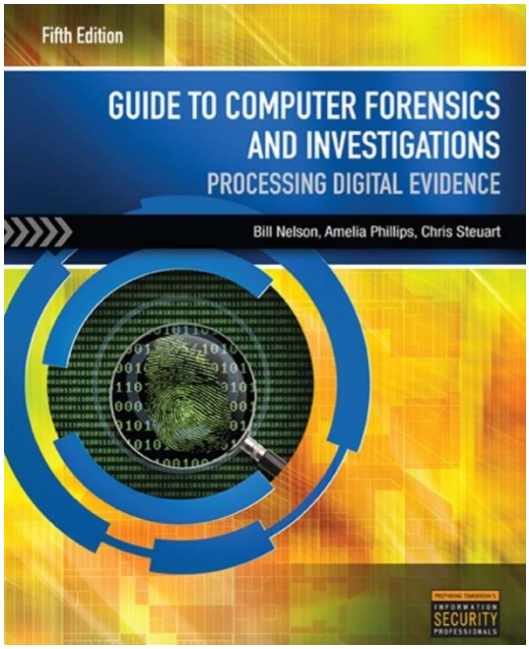
บทวิจารณ์หนังสือ

ประภาดา ตลึงจิตร
มหาวิทยาลัยวลัยลักษณ์

doi: 10.14456/jisb.2017.24



Title: Guide to computer forensics and investigations: processing digital evidence

Author: Bill Nelson, Amelia Phillips, Chris Steuart

Edition: 2015

Publisher: Cengage learning

Number of pages: 690

หนังสือ Guide to computer forensics and investigations เป็นหนังสือที่กล่าวกับความมั่นคงปลอดภัยและการวิเคราะห์สารสนเทศที่เป็นดิจิทัลที่จัดเก็บในคอมพิวเตอร์เพื่อใช้เป็นหลักฐานในการฟ้องร้องต่อไป หนังสือเล่มนี้จะมีเนื้อหาเกี่ยวกับขั้นตอนในการจัดทำ computer forensics หลักฐานและขั้นตอนในการจัดเก็บข้อมูลจาก E-mail and social media, Mobile device, Cloud computing และระบบปฏิบัติการต่างๆ รวมถึงการวิเคราะห์หลักฐานและการใช้เครื่องมือและโปรแกรมช่วยจัดเก็บและวิเคราะห์หลักฐานที่เป็นดิจิทัล ตัวอย่างหลักฐานที่ควรจัดเก็บจาก E-mail and social media, Mobile device, Cloud computing มีดังนี้

หลักฐานที่จัดเก็บ มีดังนี้

1. ตัวอย่างหลักฐานที่ควรจัดเก็บจาก E-mail
   - copy e-mail message เพื่อดู e-mail header, e-mail message, และ e-mail log จาก server
2. ตัวอย่างหลักฐานที่ควรจัดเก็บจาก Social media (เช่น facebook, twitter เป็นต้น)
   - วันและเวลาครั้งสุดท้ายที่บุคคล log on เข้าไปยัง social media
   - e-mail address ที่ใช้ในการ log on
   - การ configuration social media เช่น ให้ทุกคนสามารถดูข้อมูลใน facebook ได้ เป็นต้น
   - ข้อมูลที่ post ใน social media
   - ผู้ใดเข้ามาแอบดูข้อมูลใน social media เช่น facebook เป็นต้น
3. ตัวอย่างหลักฐานที่ควรจัดเก็บจาก Mobile device
   - เพื่อให้ข้อมูลที่จะเป็นหลักฐานใน RAM คงอยู่เมื่อได้ mobile มายังไม่ควรปิดเครื่อง
   - disconnect การ synchronize กับ user's laptop
   - laptop ที่มีการโอนข้อมูลจาก mobile ไม่ว่าจะเป็น picture หรือ video

- OTG ที่โอนข้อมูลจาก mobile
- ให้ mobile อยู่ใน airplane mode เพื่อไม่ให้เชื่อมต่อกับภายนอกได้ เนื่องจากอาจจะมาลบข้อมูลได้ หรืออาจจัดเก็บ mobile ใน faraday cage
- ข้อมูลเกี่ยวกับ mobile จาก network provider

4. ตัวอย่างหลักฐานที่ควรจัดเก็บจาก Cloud computing
   - จาก cloud service provider (CSP) ประกอบด้วย
     . ทีมงานที่ถูกฝึกมาให้จัดการกับภัยที่จะเกิดกับ cloud
     . SLA (service level agreement) ที่ทำกับลูกค้า ประกอบด้วย service hours, restriction applied to the customer, availability of the cloud, levels of support, response time for data transfers, limitation, contingency plan, business continuity and disaster recovery plan, fees, security measures และ terminology of the cloud's systems and applications โดย business continuity and disaster recovery plan จะทำให้สามารถได้ข้อมูลที่เก็บใน cloud กลับคืนมากรณีที่ข้อมูลหายได้
     . cloud topology, policies และ data storage methods และอุปกรณ์ต่างๆ เพื่อพิจารณาว่าสามารถจัดเก็บข้อมูลจาก cloud ได้หรือไม่ เช่น จาก remote cloud storage เป็นต้น
     . ในกรณีที่ cloud มีการ run snapshot ยิ่งถ้ามีการใช้ MD5 หรือ SHA1 จะทำให้ทราบได้ว่ารายละเอียดข้อมูลมีการเปลี่ยนแปลงหรือไม่ นอกจากนี้ยังสามารถทราบได้จากวันและเวลาของ file
     . ข้อมูลที่จัดเก็บใน disk (data at rest) ข้อมูลที่กำลังส่งไปในเครือข่าย (data in motion) และข้อมูลที่อยู่ใน RAM (data in use) มีการเข้ารหัสหรือไม่ ถ้ามีต้องขอคีย์ที่ใช้ในการถอดรหัสจากเจ้าของข้อมูลหรือ CSP ถ้าไม่ให้คีย์อาจต้องขอความร่วมมือจากทนายความ
   - จาก cloud customer ประกอบด้วย
     . data จากคอมพิวเตอร์หรือ mobile ของ customer
     . web browser's cache file
     . CSP's application ที่ถูกติดตั้งใน mobile ภายใต้ user application folder

   - ปัญหาด้านเทคนิคที่เกี่ยวกับ cloud มีดังนี้
     . Architecture การกำหนดสถานที่จัดเก็บข้อมูลเพื่อนำมาเป็นหลักฐานด้าน forensic ค่อนข้างมีปัญหาสำหรับ cloud เนื่องจาก CSP มักจะเก็บสถานที่ตั้งของคอมพิวเตอร์ที่ให้บริการ cloud ไว้เป็นความลับ
     . Analysis of cloud forensic data ต้องมั่นใจในว่า clock ของ server ได้รับการ synchronized อย่างถูกต้อง
     . Anti-forensics โดย hacker อาจใช้เทคนิคในการปรับเปลี่ยนหรือซ่อนข้อมูล เช่น ซ่อนข้อมูลด้วยการใช้ data-hiding utilities หรือปรับเปลี่ยน timestamp ทำให้ยากต่อการจัดทำ timeline ของเหตุการณ์ เป็นต้น นอกจากนี้ยังรวมถึงการใช้ hash value เพื่อเปรียบเทียบว่าแฟ้มข้อมูลถูกปรับเปลี่ยนหรือไม่
     . Incident first responders เป็นบุคคลที่ได้รับการฝึกฝนให้มีหน้าที่จัดการกับ network incidents อาจไม่ให้ความร่วมมือในการให้ข้อมูลได้เช่นกัน
     . Role management ในการค้นหาหลักฐานอาจจำเป็นต้องทราบ access controls ซึ่งอาจทำให้ระบุได้ว่าผู้ใดอาจได้รับผลกระทบเพิ่มเติมได้
     . Standards and Training ในการค้นหาหลักฐานควรทราบถึง common standard ที่ CSP นำมาใช้ด้วย โดย standard นี้จะให้ข้อมูล เช่น privacy agreements, security measures, questionnaires เป็นต้น