Email Investigation

พันตำรวจเอก สันติพัฒน์ พรหมะจุล
ผู้กำกับการฝ่ายอำนวยการ ๑ กองบังคับการอำนวยการ
ตำรวจภูธรภาค ๑

หัวข้อการบรรยาย

- การสืบค้นข้อมูลทางอินเทอร์เน็ต
- การสืบค้นข้อมูลจากอีเมล์
- การรวบรวมพยานหลักฐาน

การสืบค้นข้อมูลทางอินเทอร์เน็ต

- สิ่งสำคัญที่จะระบุตัวผู้ใช้งาน ก็คือ IP Address
- เมื่อได้ IP Address แล้ว จะต้องดู วัน - เวลา ประกอบ
- ระบุ Time Zone (ประเทศไทย?)
- ข้อมูลที่ระบุตัวผู้ใช้งาน จะต้องสอบถามจาก ผู้ให้บริการ (Internet Service Provider – ISP)
- รู้ได้อย่างไรว่า เป็นข้อมูลของ ISP ใด????

การสืบค้นข้อมูลทางอินเทอร์เน็ต

- สืบค้นจากเว็ปไซต์ที่ให้บริการ ได้แก่ whois.sc, domaintools.com, whatismyipaddress.com
- ข้อมูลที่ได้เป็นข้อมูลเบื้องต้นที่ระบุว่า IP Address เป้าหมาย อยู่ในความดูแลของ ISP ใด
- ข้อมูลมีทั้งที่เป็นการเชื่อมต่อแบบ Internet Broadband และ Mobile Network (2G, 3G, 4G)

การสืบค้นข้อมูลจากอีเมล์

- Email จะประกอบด้วย
  - Mail header
  - Body/contents
  - Attachments

- Email จะถูกส่งจาก Mail server ต้นทาง ไปยัง Mail server ปลายทาง โดยแต่ละ Server จะมีการบันทึก Time stamp ไว้ที่ Mail header

การสืบค้นข้อมูลจากอีเมล์

- ข้อมูลสืบค้นได้จาก Email คือ
  - IP Address ของ ต้นทาง/ปลายทาง
  - Time stamp
  - ผู้ส่ง/ผู้รับ
  - Contents/Attachment

การรวบรวมพยานหลักฐาน

- สิ่งที่ต้องคำนึงเมื่อเริ่มกระบวนการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ คือ
  - พยานหลักฐานประเภทนี้ ถูกทำลาย/เปลี่ยนแปลง/มีการปนเปื้อน ได้ง่าย ทั้งจากตัวเจ้าหน้าที่/คนร้าย
  - ต้องรู้ฐานความผิด เพื่อนำไปสู่การสืบค้นข้อมูลที่ถูกต้อง ตามความต้องการ/สนับสนุนการดำเนินคดี
  - มีการบันทึกขั้นตอนดำเนินการต่างๆ ไว้ชัดเจน สามารถนำไปอ้างอิงในการดำเนินคดีได้
  - ต้องเป็นไปตามที่กฎหมายให้อำนาจไว้

การรวบรวมพยานหลักฐาน

- พยานหลักฐานทางอิเล็กทรอนิกส์ มีอะไรบ้าง
  - ข้อมูลจราจรทางคอมพิวเตอร์
  - Contents ในเว็ปไซต์ต่างๆ/อีเมล์
  - Medias ต่างๆ
  - Storages
  - Mobile devices/Computer

พันตำรวจเอก สันติพัฒน์ พรหมะจุล

ตำรวจภูธรภาค ๑

Mobile: 09 7952 9887

e-mail: santipat@police.go.th