พยานหลักฐานทางอิเล็กทรอนิกส์

กลุ่มงานสนันสนุนคดีเทคโนโลยี บก.ปอท.

การรักษาความน่าเชื่อถือของพยานหลักฐาน

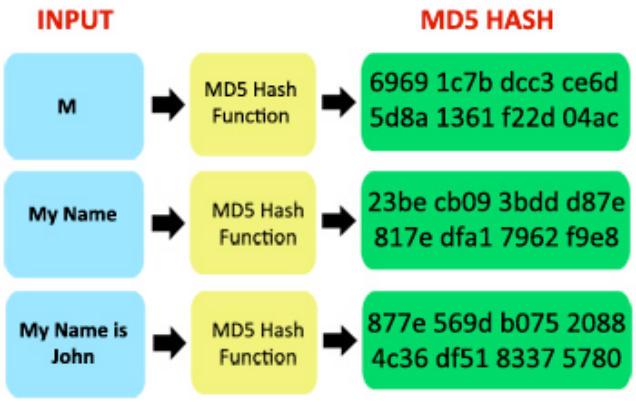
หลักการทั่วไปในการรักษาความน่าเชื่อถือของพยานหลักฐาน มีหลักสำคัญ ๓ ประการ

- การยืนยันว่า เป็นพยานหลักฐานที่แท้จริง (Authentication of Evidence)
- การรักษาห่วงโซ่ของพยานหลักฐาน (Chain of Custody)
- การยืนยันความถูกต้องของพยานหลักฐาน (Evidence Validation)

กฎในการรักษาความน่าเชื่อถือของพยานหลักฐานทางอิเล็กทรอนิกส์ 4 ประการ

- ต้องไม่กระทำให้เกิดการเปลี่ยนแปลงใดๆ
- กรณีมีความจำเป็นต้องเปลี่ยนแปลง หลีกเลี่ยงไม่ได้ ต้องอธิบายได้ ทำให้เปลี่ยนแปลงน้อยที่สุด และบันทึกไว้
- เครื่องมือที่ใช้ต้องได้ผลลัพธ์แบบเดียวกัน
- ปฏิบัติตามกฎหมาย

การยืนยันความถูกต้อง



ความเกี่ยวเนื่องในคดี

อาชญากรรมจะเกี่ยวเนื่องกับระบบคอมพิวเตอร์ใน 3 ลักษณะ

- ระบบคอมพิวเตอร์ตกเป็นเป้าหมายของอาชญากรรม(Hacker / Email Scam / ขโมย แก้ไข เปลี่ยนแปลงข้อมูล /โจมตีและทำลายระบบ)
- ใช้ระบบคอมพิวเตอร์ในการกระทำความผิด(Romance Scam /หลอกขายของ/ขายของผิดกฎหมาย /เว็บลามกอนาจาร/เว็บพนัน)
- ข้อมูลผิดกฎหมาย(การนำข้อมูลที่ผิดกฎหมายเข้าไปยังระบบคอมพิวเตอร์ โพสต ข้อความทำให้ประเทศเสียหาย)

คดีที่มีพยานหลักฐานทางอิเล็กทรอนิกส์เข้าไปเกี่ยวข้อง

- ฉ้อโกง
- แชร์ลูกโซ่
- ขโมยข้อมูลทางการค้า
- ฆาตกรรม
- หมิ่นประมาท
- ก่อการร้าย
- ฟอกเงิน
- ยาเสพติด
- ฯลฯ

องค์ประกอบของคอมพิวเตอร์ และข้อมูล

คอมพิวเตอร์ มีองค์ประกอบที่สำคัญ 3 หน่วย คือ

- หน่วยประมวลผล (Processor Unit)
- หน่วยความจำ (Memory)
- อุปกรณ์รับส่งข้อมูล (Input/Output Unit)

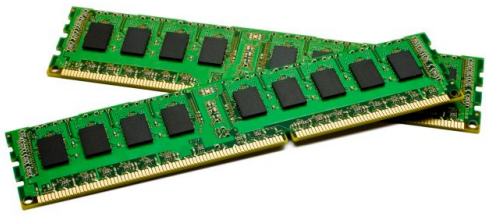
แหล่งบันทึกข้อมูลอิเล็กทรอนิกส์

แหล่งบันทึกข้อมูลอิเล็กทรอนิกส์ ในปัจจุบันมีอยู่ 3 ประเภท คือ

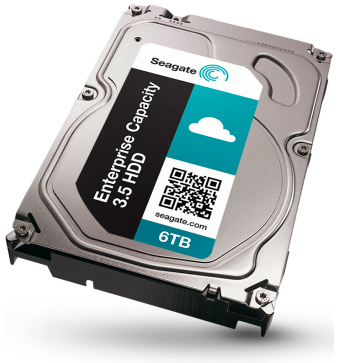
- สื่อบันทึกข้อมูลแบบประจำที่ (Fixed storage)
- สื่อบันทึกข้อมูลแบบพกพา (Removable media)
- Online/Cloud storage

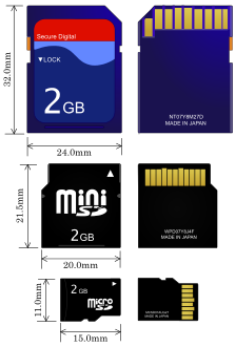
ชนิดข้อมูลทางคอมพิวเตอร์

Volatile data เป็นข้อมูลที่สูญหายไปทันทีที่ปิดเครื่องคอมพิวเตอร์ คือข้อมูลที่บันทึกใน (Memory) เช่น ข้อมูล Network connections, Running applications, Running processes, Open/listening network connections รวมถึงอาจพบพาสเวิร์ดสำหรับใช้งานโปรแกรม เปิดอ่านอีเมล หรือเข้าถึงพาร์ทิชันฮาร์ดดิสก์ที่ถูกเข้ารหัสไว้ เป็นต้น
ประโยชน์ของข้อมูล Volatile data อาจจะสามารถใช้กู้ password ที่คนร้ายอาจไม่ยอมบอก และสามารถใช้ในการตรวจการทำงานของมัลแวร์ได้



Non-volatile data เป็นข้อมูลที่ไม่สูญหายเมื่อปิดคอมพิวเตอร์ กล่าวคือข้อมูลที่อยู่ในสื่อบันทึกข้อมูลต่าง ๆ เช่น ฮาร์ดดิสก์ ซีดี ดีวีดี Thumb drive SSD SD-Card ฯลฯ





การตรวจยึดพยานหลักฐานทางอิเล็กทรอนิกส์

แนวทางทั่วไปในการตรวจยึด

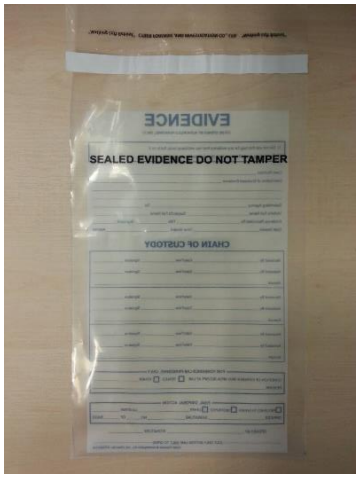
- การ รปภ. สถานที่เกิดเหตุ
- การ รปภ. ส่วนที่มีพยานหลักฐานทางอิเล็กทรอนิกส์
- การยึดอุปกรณ์คอมพิวเตอร์และสื่อบันทึกข้อมูล
- จัดเก็บ
- ส่งของกลางไปตรวจพิสูจน์

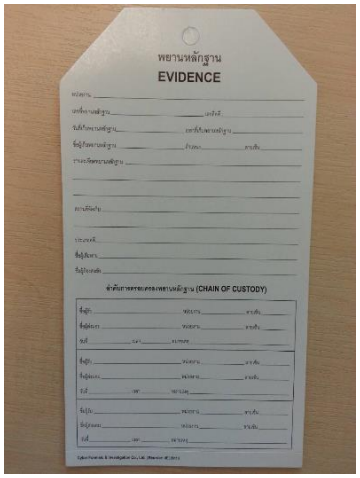
ขั้นตอนในการตรวจค้นและยึด

- รักษาสถานที่เกิดเหตุกันทุกคนออกจากคอมพิวเตอร์
- จดบันทึก วาดแผนที่ พร้อมถ่ายภาพโดยละเอียด
- ระบุจุดที่ตั้งคอมพิวเตอร์ทั้งหมด พร้อมกำหนดชื่อจุด เพื่ออ้างอิง

- ติดป้าย บรรจุ เพื่อเตรียมขนย้าย
- คอมพิวเตอร์ ปิด - ห้ามเปิด
- คอมพิวเตอร์ เปิด - ถ่ายภาพหน้าจอ
- กรณีมีพยานหลักฐานปรากฏบนหน้าจอ ให้ถ่ายภาพแล้วพิมพ์ออกมาให้ ผู้ต้องสงสัยลงชื่อรับรอง
- กรณีต้องการเก็บ Volatile memory/data ให้ผู้เชี่ยวชาญดำเนินการ เพราะต้องใช้ software พิเศษ
- ดึงสายไฟฟ้าจากคอมพิวเตอร์ กรณีเป็นคอมพิวเตอร์แบบพกพา ให้ถอดแบตเตอรี่ออก
- คอมพิวเตอร์แบบพกพารุ่นใหม่ จะไม่มีช่องให้ถอดแบตเตอรี่ ให้กดปุ่มปิด-เปิด ค้างไว้ คอมพิวเตอร์จะดับไปเอง
- ติดป้ายกำกับที่สายเชื่อมต่อกับช่องต่อต่างๆ ให้ตรงกัน ช่องที่ไม่ใช้งานให้ปิดทับไว้
- ถ่ายรูปจุดเชื่อมต่อทุกจุด และรอบคอมพิวเตอร์
- ดึงสายที่เชื่อมต่อออกทั้งหมด แล้วบรรจุคอมพิวเตอร์ในกล่องกันกระแทก ปิดคาดด้วยเทป แล้วให้ผู้ต้องสงสัยลงลายมือชื่อกำกับไว้ที่เทปคาด
- ถ่ายภาพและบันทึกทุกขั้นตอนโดยละเอียด
- การตรวจยึด Smart phone และ Tablet ถ้าใส่รหัสป้องกันไว้ ให้ถามจากเจ้าของอุปกรณ์
- ปรับให้เป็น Flight mode เพื่อป้องกันไม่ให้ติดต่อกับเครือข่าย
- บรรจุใน Faraday bag หากไม่มีให้ห่อด้วยกระดาษตะกั่ว หรือแผ่นฟอยล์
- ยึดสายสัญญาณ, ที่แปลงไฟฟ้าของเครื่องมาด้วย*

*** สวมถุงมือก่อนการปฏิบัติงานทุกครั้ง






พยานหลักฐ
VIDEN
3M

ปัญหาที่พบในการตรวจพิสูจน์

- การจัดลำดับความสำคัญของของกลางที่จะให้ตรวจ
- มือถือถูก Hard reset หรือ Factory reset ทำให้กู้ข้อมูลไม่ได้
- นำส่งอุปกรณ์ประกอบไม่ครบ เช่น adaptor*
- อุปกรณ์ที่ส่งให้ตรวจติดรหัสผ่าน
- กรณียึด CCTV ให้นำส่งอุปกรณ์บันทึกทั้งตัว ไม่ใช่แค่ Hard disc หรือเมมการ์ด(Memory)
- ต้องการสำเนาข้อมูล ให้เตรียมสื่อบันทึกมาด้วย
- ประเด็นคำถามตรวจพิสูจน์ไม่ชัดเจน
- ประเด็นคำถามตรวจพิสูจน์ที่พ่วงความเห็นทางกฎหมาย ทำให้ไม่สามารถตรวจพิสูจน์ได้

คดีฆ่า ผอ.ส่วนการศึกษา อบต. ในจังหวัดศรีสะเกษ

ส่งฟ้องศาลคดี ‘ผู้กองเหน่ง’ ฆ่า ผอ.อ้อย 11 ข้อหา-พ่อดีใจลูกไม่ตายฟรี หวังได้รับโทษสาสม

วันที่ 6 มกราคม 2561 - 02:39 น.

ตัวอย่างอุปกรณ์ตรวจพิสูจน์