**องค์ความรู้ด้านการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์**

**9**

**การตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ หรือการตรวจพิสูจน์พยานหลักฐานดิจิทัล**

เป็นการนำหลักนิติวิทยาศาสตร์มาประยุกต์ใช้กับพยานหลักฐานอิเล็กทรอนิกส์ ในประเด็นข้อทางกฎหมาย โดยเป็นการประยุกต์ใช้เทคโนโลยีคอมพิวเตอร์กับปัญหาทางกฎหมายในกรณีที่พยานหลักฐานประกอบด้วยสิ่งที่สร้างขึ้นโดยมนุษย์ และสิ่งที่สร้างขึ้นโดยเทคโนโลยีอันเป็นผลมาจากการมีปฏิสัมพันธ์กับมนุษย์

**คำนิยาม**

พยานหลักฐานทางอิเล็กทรอนิกส์ หมายถึง ข้อมูลใด ๆ ที่จัดเก็บหรือส่งต่อในรูปแบบดิจิทัลหรือแอนาล็อกที่เกี่ยวข้องกับการสืบสวนสอบสวน หรือการพิจารณาในชั้นศาล

พยานหลักฐานดิจิทัล มักใช้แทนกันได้กับคำว่าพยานหลักฐานทางอิเล็กทรอนิกส์ แต่จะใช้อ้างถึงเฉพาะข้อมูลที่จัดเก็บหรือส่งต่อ  
ในรูปแบบดิจิทัลที่เกี่ยวข้องกับการสืบสวนสอบสวน หรือการพิจารณาในชั้นศาล

**หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล** ประกอบด้วย

1. การเก็บรวบรวมพยานหลักฐาน (Collection)

* กระบวนการรวบรวมข้อมูลอิเล็กทรอนิกส์ตามความเป็นจริง เพื่อค้นหาข้อมูลที่มีคุณค่าพอที่จะเป็นหลักฐานในคดี  
  ในอุปกรณ์อิเล็กทรอนิกส์ เช่น เครื่องคอมพิวเตอร์ เครื่องมือสื่อสาร สื่อบันทึกข้อมูล ข้อมูลบนคลาวน์ จากสถานที่เกิดเหตุ ซึ่งรวมถึงกระบวนการสร้างห่วงโซ่การครอบครองวัตถุพยาน (Chain of custody) และการเก็บรักษาอย่างระมัดระวัง (Preservation) เพื่อลดความเสี่ยงต่อการเปลี่ยนแปลงหรือเสียหายต่อพยานหลักฐาน

1. การยืนยันความถูกต้องพยานหลักฐาน (Verification)

* กระบวนการทำสำเนาข้อมูลวัตถุพยาน (Forensic Imaging หรือ Acquisition) ที่มีการยืนยันความถูกต้องของข้อมูลจาก  
  ค่าความจำเพาะของข้อมูล (Hash Value) ในลักษณะการเข้ารหัสโดยใช้อัลกอริทึม เช่น MD5, SHA1, SHA256 เนื่องจากตามมาตรฐานสากล กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลนั้น จะไม่ดำเนินการกับวัตถุพยานโดยตรง จึงมีความจำเป็นต้องมีการตรวจสอบว่า พยานหลักฐานต้นฉบับกับสำเนาตรงกันหรือไม่จากค่าความจำเพาะของข้อมูล

1. การวิเคราะห์พยานหลักฐาน (Analysis)

* กระบวนการค้นหา และเก็บรวบรวมข้อมูลจากวัตถุพยานทั้งหมด โดยการวิเคราะห์ข้อมูลขึ้นอยู่กับลักษณะเฉพาะและพฤติการณ์แวดล้อมของแต่ละคดี เช่น คดีภาพลามกอนาจารเด็ก เป้าหมายของการตรวจสอบจะอยู่ที่การค้นหาไฟล์ข้อมูลทั้งที่เป็นไฟล์ภาพนิ่งและไฟล์ภาพเคลื่อนไหว เป็นต้น ทั้งนี้ ขึ้นอยู่กับวัตถุประสงค์ที่ต้องการส่งมาตรวจพิสูจน์

1. การนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน (Presentation)

* กระบวนการนำเสนอผลการตรวจพิสูจน์เป็นลายลักษณ์อักษร หรือรายงานการตรวจพิสูจน์พยานหลักฐาน ซึ่งควรมีการเขียนอย่างชัดเจน กระชับ และถูกต้อง โดยอธิบายว่ามีสิ่งใดบ้างที่ได้รับการตรวจสอบ กระบวนการทำสำเนาข้อมูล เครื่องมือและกระบวนการที่ใช้ และสิ่งที่พบในการตรวจพิสูจน์

**ประเภทของพยานหลักฐานดิจิทัล**

1. แบ่งตามการสร้างข้อมูล: ข้อมูลที่สร้างโดยระบบคอมพิวเตอร์ (System Created Data) และข้อมูลที่สร้างโดยผู้ใช้งาน (User Created Data)
2. แบ่งตามการเข้ารหัส: ข้อมูลเข้ารหัส (Encrypted Data) และข้อมูลไม่เข้ารหัส (Non-encrypted Data)
3. แบ่งตามชนิดอุปกรณ์: คอมพิวเตอร์ (คอมพิวเตอร์ตั้งโต๊ะ, คอมพิวเตอร์พกพา, เซิร์ฟเวอร์), อุปกรณ์สื่อสารเคลื่อนที่ (โทรศัพท์มือถือ, แท็บเล็ต), สื่อบันทึกข้อมูล (แฟลชไดร์ฟ, ฮาร์ดไดร์ฟ, ซีดี, ดีวีดี, การ์ดหน่วยความจำ), กล้องวงจรปิด (CCTV),   
   โดรน (Drone), IoT (Internet of Thing: นาฬิกาอัจฉริยะ, สมาร์ททีวี เป็นต้น)

**ประเภทของข้อมูลดิจิทัล**

1. Volatile Data คือ ข้อมูลที่เก็บไว้ชั่วคราวใน RAM ของคอมพิวเตอร์ในขณะที่ระบบกำลังทำงาน
2. Non-volatile Data คือ ข้อมูลดิจิทัลประเภทหนึ่งที่จัดเก็บถาวรในระบบไฟล์บนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์บางประเภท

**เครื่องมือที่ใช้ในการตรวจพิสูจน์**

- ฮาร์ดแวร์ที่สามารถทำสำเนาข้อมูลได้ เช่น เครื่อง TD3, เครื่อง TX1 เป็นต้น

- ซอฟต์แวร์ลิขสิทธิ์ทั้งแบบเสียค่าใช้จ่ายและแบบไม่มีค่าใช้จ่ายที่สามารถทำสำเนาข้อมูล และวิเคราะห์ข้อมูล เช่น FTK Imager, Encase, AXIOM, Cellebrite เป็นต้น โดยต้องมีการตรวจสอบความใช้ได้ของซอฟต์แวร์ก่อนการใช้งานเสมอ

**วิธีการตรวจพิสูจน์**

ตรวจพิสูจน์ตามหลักวิชาการและตามมาตรฐานสากลที่ประยุกต์ใช้

**อาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมทางไซเบอร์**

การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย และ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ อาทิ การโจมตีระบบคอมพิวเตอร์, การทำลาย-แก้ไข-ขโมยข้อมูล, การหลอกลวงให้เสียทรัพย์, การขโมยข้อมูลทางอินเตอร์เน็ตซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ, อาชญากรนำเอาระบบการสื่อสารมาปกปิดความผิดของตนเอง, การละเมิดสิทธิ์ปลอมแปลงรูปแบบเลียนแบบระบบซอฟต์แวร์โดยมิชอบ,   
ใช้คอมพิวเตอร์เผยแพร่สื่อลามกอนาจารและข้อมูลที่ไม่เหมาะสม, ใช้คอมพิวเตอร์ฟอกเงิน, อันธพาลทางคอมพิวเตอร์ที่ก่อกวน ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไป ระบบการจราจร, หลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม, แทรกแซงข้อมูลแล้วนำข้อมูลนั้นมาเป็นประโยชน์ต่อตนโดยมิชอบ, ใช้คอมพิวเตอร์แอบโอนเงินบัญชีผู้อื่นเข้าบัญชีตัวเอง เป็นต้น

**ประเภทคดีออนไลน์ยอดนิยมในปัจจุบัน**

1. หลอกลวงซื้อขายสินค้าหรือบริการ
2. หลอกให้โอนเงินเพื่อทำงาน
3. หลอกให้กู้เงิน
4. หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์
5. ข่มขู่ทางโทรศัพท์(Call center)