ข้อเสนอแนะมาตรฐาน
การจัดการอุปกรณ์ดิจิทัล ในงานตรวจพิสูจน์พยานหลักฐาน

คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล

ผู้ตรวจแก้ร่างข้อเสนอแนะ

นางสุรางคณา วายุภาพ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางสาวพิชญลักษณ์ คำทองสุก	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ที่ปรึกษา

พลตำรวจโท วิสนุ ปราสาททองโอสถ	สำนักงานตำรวจแห่งชาติ
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ประธาน

นายธงชัย แสงศิริ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงาน

พันตำรวจเอก นิเวศน์ อาภาวศิน	สำนักงานตำรวจแห่งชาติ
พันตำรวจโท หญิง จีรบูรณ์ บำเพ็ญนรกิจ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
พันตำรวจโท นันทวุฒิ รอดมณี	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
นายปกรณ์ ธรรมโรจน์	สำนักงานอัยการสูงสุด
นางสาวอมรรัตน์ เล็กวิชัย	สถาบันนิติวิทยาศาสตร์
นางสาวธนิสสรา ลิ้นสุวรรณ	สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
นายโสพส พานิชปรีชา	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายธันวา วาทหงษ์	บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส คอนซัลติ้ง (ประเทศไทย) จำกัด

เลขานุการ

นางสาวกรรณิกา ภัทรวิศิษฏ์สัณธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน
Version 1.0

จัดทำโดย คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล

ศูนย์ดิจิทัลฟอเรนสิกส์
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์ 0 2123 1234 โทรสาร 0 2123 1200
E-mail: dfc@thaicert.or.th
www.etda.or.th

คำนำ

ปัจจุบันโลกพัฒนาไปสู่ยุคดิจิทัลซึ่งไม่เพียงแต่การติดต่อสื่อสารหรือการทำงานที่เปลี่ยนแปลงรูปแบบไป แต่ข้อมูลหรือวัตถุต่างๆ ที่อาจเป็นเบาะแส หรือถูกนำมาใช้เป็นพยานหลักฐานก็เปลี่ยนแปลงตามไปด้วย เช่น การฉ้อโกงทางการเงินโดยใช้เทคโนโลยีและอุปกรณ์ดิจิทัลเป็นเครื่องมือ การติดตามหาตัวผู้กระทำความผิดจำเป็นต้องหาร่องรอยพยานหลักฐานดิจิทัลจากอุปกรณ์ดิจิทัล หรือข้อมูลและข้อมูลจราจรที่เกี่ยวข้อง

“พยานหลักฐานดิจิทัล” มีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่าย และการแก้ไขนั้นอาจไม่เหลือร่องรอยให้ตรวจสอบในภายหลัง ดังนั้น การดำเนินการกับพยานหลักฐานดิจิทัลจึงจำเป็นต้องมีกระบวนการจัดเก็บ ตรวจค้น วิเคราะห์ และรายงานผลที่ได้มาตรฐานเช่นเดียวกับการดำเนินการกับพยานหลักฐานประเภทอื่น ๆ ซึ่งต้องผ่านกระบวนการคัดเลือก การนำสืบ และการพิจารณาน้ำหนักหรือความน่าเชื่อถือของพยานหลักฐาน โดยเฉพาะอย่างยิ่งแนวปฏิบัติทางด้านเทคนิค เพื่อให้พยานหลักฐานดิจิทัลคงไว้ซึ่งความน่าเชื่อถือและสามารถรับฟังได้ตลอดสายกระบวนการยุติธรรม

แม้ในปัจจุบันศาลไทยให้การยอมรับและรับฟังพยานหลักฐานดิจิทัล แต่การพิสูจน์ อ้างอิง หรือการนำสืบก็ยังมีความท้าทายอย่างมากและในหลายครั้งเกิดเป็นข้อโต้แย้งเมื่อมีการอ้างอิง ตัวอย่างปัญหาที่พบเมื่อมีการอ้างอิงพยานหลักฐานดิจิทัล เช่น การอ้างข้อมูลคอมพิวเตอร์ซึ่งเป็นสิ่งไม่มีรูปร่างและไม่สามารถจับต้องได้โดยตรงทั้งยังสามารถถูกเปลี่ยนแปลงได้โดยง่ายมาเป็นพยานหลักฐานนั้น เราจะเชื่อได้อย่างไรว่าข้อมูลที่ได้มานั้นมีความครบถ้วนสมบูรณ์และมีความน่าเชื่อถือ ข้อโต้แย้งเรื่องข้อมูลพยานหลักฐานที่อยู่ในรูปดิจิทัลอาจถูกเปลี่ยนแปลงในระหว่างกระบวนการรวบรวมพยานหลักฐาน หรือข้อโต้แย้งเรื่องความน่าเชื่อถือของผลการวิเคราะห์และตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นต้น ดังนั้นจึงควรให้ความสำคัญกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลตั้งแต่ต้นทางที่ควรดำเนินการโดยผู้ที่มีความรู้ เข้าใจการทำงานของเครื่องมืออิเล็กทรอนิกส์ ใช้เครื่องมือและวิธีการที่เป็นมาตรฐานสากลเพื่อให้มีความน่าเชื่อถือ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA เป็นหน่วยงานที่จัดตั้งขึ้นตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ภายในกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เป็นหน่วยงานหลักที่ทำหน้าที่ดำเนินการพัฒนา ส่งเสริม และสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ สร้างโอกาส และความเท่าเทียมให้กับทุกคน ด้วยการเสริมสร้างความแข็งแกร่งให้กับฐานรากด้านไอซีทีของประเทศ อันได้แก่ การพัฒนากฎหมายเพื่ออำนวยความสะดวก การสร้างมาตรฐานที่ใช้ขับเคลื่อนระบบเศรษฐกิจ และการสร้างกลไกในการสร้างความเชื่อมั่นให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์

ETDA จึงได้จัดตั้งคณะทำงานขึ้นคณะหนึ่งอันประกอบไปด้วยผู้เชี่ยวชาญและทรงคุณวุฒิจาก สถาบันนิติวิทยาศาสตร์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานอัยการสูงสุด และ บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส คอนซัลติ้ง (ประเทศไทย) เพื่อร่วมกันจัดทำร่างข้อเสนอแนะเกี่ยวกับมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน โดยอ้างอิงพื้นฐานจากการศึกษาแนวปฏิบัติสากล ได้แก่ ACPO Good Practice Guide for Digital Evidence (Edition: March 2012); ISO/IEC 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence, First edition 2012-10-15 และ SWGDE Best Practices for Computer Forensics V3-1 ทั้งพิจารณาปรับปรุงเพื่อให้เหมาะสมกับรูปแบบการปฏิบัติงานในไทยและความพร้อมของหน่วยปฏิบัติ โดยมุ่งหวังให้เป็นแนวทางสำหรับการปฏิบัติงานที่มีความสอดคล้องกับมาตรฐานสากล และสามารถยกระดับให้เป็นมาตรฐานได้ในอนาคต

สารบัญ

ข้อเสนอแนะมาตรฐาน
การจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน

1. ขอบเขตข้อเสนอแนะ

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางสำหรับการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานที่มีความสอดคล้องกับมาตรฐานสากล สำหรับการปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการ ซึ่งครอบคลุมการจัดการคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิทัลแบบภายนอก ข้อมูลคอมพิวเตอร์ และเครื่องมือสื่อสารเคลื่อนที่ โดยมีหลักการสำคัญดังปรากฏในข้อ 3 ซึ่งเจ้าหน้าที่สามารถพิจารณาดำเนินการตามความเหมาะสมกับแต่ละสถานการณ์ ภายใต้หลักการดังกล่าว และภายใต้อำนาจหน้าที่ตามที่กฎหมายกำหนด

2. คำจำกัดความ

สำหรับข้อเสนอแนะฉบับนี้

2.1. พยานหลักฐาน หมายถึง หลักฐานที่ใช้ในการพิสูจน์ข้อเท็จจริง

2.2. พยานหลักฐานดิจิทัล ได้แก่ ข้อมูลที่ได้เก็บรักษาบนสื่อบันทึกข้อมูลหรืออยู่ระหว่างการส่ง รับ ด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งสามารถถูกใช้อ้างอิงเป็นพยานหลักฐาน

2.3. หลักฐานที่เป็นอุปกรณ์ดิจิทัล หมายถึง อุปกรณ์ที่ใช้สำหรับประมวลผลหรือจัดเก็บข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ ได้แก่ คอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิทัลแบบภายนอก และเครื่องมือสื่อสารเคลื่อนที่

2.4. คอมพิวเตอร์ ได้แก่ คอมพิวเตอร์พีซี เซิร์ฟเวอร์ และ แล็ปท็อป

2.5. เครื่องมือสื่อสารเคลื่อนที่ ได้แก่ โทรศัพท์เคลื่อนที่ และ แท็บเล็ต

2.6. Chain of custody หมายถึง กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บรวบรวม

2.7. สื่อบันทึกข้อมูลที่พร้อมใช้งาน หมายถึง สื่อบันทึกข้อมูลที่จัดเตรียมไว้สำหรับงานตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ซึ่งผ่านการลบข้อมูลเก่าด้วยวิธีเขียนทับ (Wiping) และสร้างระบบไฟล์สำหรับบันทึกข้อมูลขึ้นใหม่ (Format)

2.8. ฮาร์ดดิสก์แบบเชื่อมต่อภายใน (Internal hard disk) หมายถึง ฮาร์ดดิสก์แบบที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์

2.9. ฮาร์ดดิสก์แบบเชื่อมต่อภายนอก (External hard disk) ได้แก่ ฮาร์ดดิสก์แบบที่ไม่ได้ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์ สามารถเชื่อมต่อกับเครื่องคอมพิวเตอร์โดยใช้พอร์ต เช่น USB, FireWire, Thunderbolt หรือ eSATA เป็นต้น

2.10. การคัดกรองข้อมูลในหลักฐาน (Triage /Preview) หมายถึง การเปิดดู คัดแยก และจัดลำดับความสำคัญข้อมูลที่เกี่ยวข้องเพื่อเก็บรวบรวม และตรวจวิเคราะห์ในภายหลัง โดยให้เกิดการ

เปลี่ยนแปลงของข้อมูลน้อยที่สุด และการเปลี่ยนแปลงนั้นต้องไม่เกี่ยวข้องกับสาระสำคัญของพยานหลักฐานดิจิทัล

2.11. Volatile data หมายถึง ข้อมูลที่จะเปลี่ยนแปลงได้ง่าย หากมีความเปลี่ยนแปลงต่ออุปกรณ์ดิจิทัลที่เกี่ยวข้อง เช่น ข้อมูลที่อยู่ในหน่วยความจำหลัก (RAM) ที่จะสูญไปเมื่อไม่มีกระแสไฟฟ้าหล่อเลี้ยงคอมพิวเตอร์ หมายเลขไอพีของอุปกรณ์ดิจิทัลที่จะเปลี่ยนแปลงไปเมื่อถูกตัดการเชื่อมต่อ เป็นต้น

2.12. Write blocker หมายถึง ฮาร์ดแวร์หรือซอฟต์แวร์ที่มีความสามารถในการป้องกันการเขียนข้อมูลลงในสื่อบันทึกข้อมูล

2.13. นาฬิกาเทียบเวลา หมายถึง นาฬิกาที่ถูกตั้งเวลาตามเวลามาตรฐานที่สามารถอ้างอิงและน่าเชื่อถือ เช่น โทรศัพท์เคลื่อนที่ที่ตั้งค่าอ้างอิงเวลากับผู้ให้บริการอัตโนมัติ (ภาคผนวก ข. 1 การเทียบเวลา)

3. หลักการปฏิบัติงานเกี่ยวกับพยานหลักฐานดิจิทัล

พยานหลักฐาน เป็นสิ่งที่ใช้ในการพิสูจน์ข้อเท็จจริง ซึ่งรวมถึงแสดงความบริสุทธิ์หรือความผิดของบุคคล คุณค่าของพยานหลักฐานอยู่ที่คุณสมบัติในการพิสูจน์ข้อเท็จจริง การปฏิบัติหน้าที่จึงต้องคำนึงถึงการรักษาคุณค่าของพยานหลักฐาน และการแสดงความน่าเชื่อถือในกระบวนการที่เกี่ยวข้องกับการจัดการพยานหลักฐานอย่างสมเหตุผล

การนำพยานหลักฐานดิจิทัลไปใช้ในการพิสูจน์ข้อเท็จจริง มีแนวคิดและหลักการเช่นเดียวกับพยานหลักฐานอื่น แต่เนื่องจากพยานหลักฐานดิจิทัลมีความเปราะบางและซับซ้อน เทคโนโลยีของอุปกรณ์ดิจิทัลถูกพัฒนาอย่างรวดเร็ว และข้อมูลสามารถถูกเปลี่ยนแปลงได้ง่ายโดยที่ผู้ปฏิบัติงานตรวจพิสูจน์อาจรู้หรือไม่รู้ตัว ดังนั้น การปฏิบัติงานที่เกี่ยวข้องกับงานตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงควรให้ความสำคัญตามหลักการดังต่อไปนี้

(1) ควรดำเนินการโดยผู้ที่เคยผ่านการฝึกอบรมในเรื่องนั้น ๆ มาก่อน หรือปฏิบัติตามแนวทางในเอกสารฉบับนี้

(2) ควรรักษาสภาพพยานหลักฐานไม่ให้ถูกเปลี่ยนแปลง หรือถูกเปลี่ยนแปลงน้อยที่สุด โดยผู้ปฏิบัติงานต้องสามารถอธิบายและบันทึกสิ่งที่ดำเนินการ เหตุผลที่ทำให้พยานหลักฐานต้องเปลี่ยนแปลง และผลกระทบจากการดำเนินการนั้น ๆ ได้อย่างละเอียดเป็นลายลักษณ์อักษร

(3) ควรรักษาความต่อเนื่องของการครอบครองพยานหลักฐาน (Chain of Custody) โดยมีข้อมูลที่จำเป็นต้องบันทึก ได้แก่ ข้อมูลติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, ข้อมูลติดต่อและลายมือชื่อของผู้รับมอบพยานหลักฐาน, วันที่และเวลาในการรับ-ส่งมอบพยานหลักฐาน, เหตุผลในการรับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น โดยรูปแบบหนึ่งของการแสดง Chain of Custody เช่น การใช้แบบฟอร์ม

(4) มีการบันทึกขั้นตอนการปฏิบัติงาน การเก็บรวบรวมและการวิเคราะห์พยานหลักฐานโดยละเอียดเพียงพอให้ผู้ตรวจพิสูจน์รายอื่นที่มีความเชี่ยวชาญในสาขาเดียวกันสามารถเข้าใจได้ และหากทำซ้ำด้วยวิธีการเดิมและเครื่องมือที่มีลักษณะเดียวกันจะต้องได้ผลลัพธ์เหมือนกัน

(5) บุคคลที่เข้าถึงพยานหลักฐานต้องเป็นผู้ที่ได้รับมอบหมายหรือมีหน้าที่รับผิดชอบโดยตรง

(6) ผู้ปฏิบัติงานพึงตระหนักถึงหน้าที่และความรับผิดชอบในการปฏิบัติงาน รวมถึงการดำเนินการตามกฎหมายที่เกี่ยวข้อง เช่น กฎหมายเกี่ยวกับพยานหลักฐาน เป็นต้น

(7) เครื่องมือและอุปกรณ์ที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐาน จำเป็นต้อง

(7.1) มีสภาพพร้อมใช้งานและเหมาะสมกับกระบวนการตรวจพิสูจน์พยานหลักฐานแต่ละประเภท

(7.2) มีมาตรการในการป้องกันการเปลี่ยนแปลงและปนเปื้อนของพยานหลักฐาน (การปนเปื้อน หมายถึง การปะปนของข้อมูลอื่นกับพยานหลักฐาน เช่น การปะปนข้อมูลจากเคสเก่ากับเคสปัจจุบัน หรือ การปะปนข้อมูลในเคสกับข้อมูลที่มีอยู่ในเครื่องคอมพิวเตอร์ของผู้ปฏิบัติงาน ทำให้ผลการวิเคราะห์ข้อมูลผิดพลาด เป็นต้น)

(7.3) ได้รับการตรวจสอบความถูกต้องแม่นยำ (Validation) ของเครื่องมือก่อนใช้งานอย่างสม่ำเสมอ

(7.4) มีคู่มือการใช้งานหรือเอกสารคำอธิบายเพื่อใช้ประกอบการอ้างอิง

4. การปฏิบัติงานในสถานที่เกิดเหตุ

4.1. เครื่องมือ

ในการปฏิบัติงานตรวจพิสูจน์หลักฐานดิจิทัลควรจัดเตรียมเครื่องมือให้พร้อมสำหรับการปฏิบัติงาน ซึ่งมีรายการเบื้องต้นที่ควรจัดเตรียม ดังนี้

4.1.1. เครื่องมือทั่วไป

(1) อุปกรณ์ถ่ายภาพ

(2) ถุงมือ (ชนิดที่ไม่ทิ้งร่องรอยติดอุปกรณ์ดิจิทัล และใช้ครั้งเดียว)

(3) ป้ายหมายเลขกำกับหลักฐาน

(4) เครื่องสำรองไฟฟ้า (UPS)

(5) ชุดเครื่องมือ เช่น ไขควงแฉก ไขควงแบน ไขควงหกเหลี่ยม มีดคัตเตอร์ เป็นต้น

(6) ไฟฉาย

(7) บรรจุภัณฑ์สำหรับบรรจุหลักฐาน เช่น ถุงกระดาษ ถุงพลาสติก ถุงกันไฟฟ้าสถิต เป็นต้น เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นจากปัจจัยต่าง ๆ เช่น อุณหภูมิ ความชื้น และแรงกระแทก เป็นต้น

(8) เทปกาว

(9) เทปปิดผนึก สำหรับปิดผนึกบรรจุภัณฑ์ของหลักฐาน ซึ่งเมื่อปิดทับแล้ว หากมีการเปิดหรือดึงออกสามารถปรากฏร่องรอยการเปิดผนึกได้

(10) แบบฟอร์มเอกสาร เช่น แบบฟอร์มยินยอมให้เก็บหลักฐาน แบบฟอร์มการระบุ Chain of custody เป็นต้น

4.1.2. เครื่องมือตรวจพิสูจน์

(1) นาฬิกาเทียบเวลา

(2) คอมพิวเตอร์สำหรับงานตรวจพิสูจน์หลักฐานดิจิทัล

(3) เครื่องมือสำหรับเก็บ Volatile data

(4) เครื่องมือคัดกรองข้อมูลในหลักฐาน

(5) เครื่องมือทำสำเนาข้อมูล

(6) Write blocker

(7) สื่อบันทึกข้อมูลที่พร้อมใช้งานสำหรับเก็บสำเนาข้อมูลที่เป็นหลักฐานดิจิทัล เช่น ฮาร์ดดิสก์ หรือ USB flash drive เป็นต้น

(8) อุปกรณ์ป้องกันคลื่นสัญญาณ เช่น Faraday bag กล่องโลหะปิดสนิท อลูมิเนียมฟอยล์ หรืออุปกรณ์อื่นที่ผ่านการทดสอบแล้วว่าป้องกันคลื่นสัญญาณได้

4.2. การประเมินและวางแผนการเก็บรวบรวมหลักฐานดิจิทัลในสถานที่เกิดเหตุ

การประเมินและวางแผนการเก็บรวบรวมหลักฐานดิจิทัล ควรจะดำเนินการตามแนวทางดังนี้

4.2.1 ประเมินสถานที่เกิดเหตุในด้านต่าง ๆ เช่น สถานที่ การเดินทาง สภาพอากาศ ความปลอดภัย เวลา เป็นต้น ซึ่งอาจเป็นอุปสรรคหรือส่งผลต่อการปฏิบัติงาน

4.2.2 สอบถามหรือกำหนดประเด็นที่ต้องการตรวจพิสูจน์เพื่อประเมินและระบุรายการหลักฐานที่ต้องเก็บรวบรวม ลำดับและวิธีการจัดเก็บ เครื่องมือที่ต้องใช้ รวมถึงความจำเป็นในการทำสำเนาข้อมูลที่เป็นหลักฐานดิจิทัลในสถานที่เกิดเหตุ

หมายเหตุ ในกรณีที่เป็นการดำเนินการร่วมกับพนักงานเจ้าหน้าที่ ควรหารือกับเจ้าหน้าที่ผู้รับผิดชอบก่อนดำเนินการ

4.2.3 กำหนดหน้าที่และความรับผิดชอบของผู้ปฏิบัติงานในสถานที่เกิดเหตุ

4.2.4 ในกรณีที่จำเป็นต้องใช้กระบวนการตรวจพิสูจน์หลักฐานประเภทอื่นประกอบด้วย เช่น จัดเก็บ DNA หรือลายนิ้วมือแฝง ให้หารือกับเจ้าหน้าที่ผู้รับผิดชอบเกี่ยวกับลำดับการดำเนินการ

4.3 การเก็บรวบรวมหลักฐาน (Evidence collection)

4.3.1 หลักการทั่วไป

การเก็บรวบรวมหลักฐานควรดำเนินการตามแนวทางดังนี้

(1) ห้ามบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าไปในสถานที่เกิดเหตุ

(2) ควรสวมถุงมือระหว่างการปฏิบัติงานในสถานที่เกิดเหตุ

(3) กำหนดรูปแบบการตรวจค้นสถานที่เกิดเหตุ และดำเนินการตามที่กำหนดอย่างถี่ถ้วน

(4) กำหนดหมายเลขและวางป้ายหมายเลขกำกับหลักฐานแต่ละชิ้น

(5) ถ่ายภาพรายละเอียดต่อไปนี้

(5.1) หากพบคอมพิวเตอร์ หรือเครื่องมือสื่อสารเคลื่อนที่ ให้ถ่ายภาพทุกด้านและพื้นที่รอบ ๆ หลักฐานที่จะจัดเก็บ อุปกรณ์เชื่อมต่อภายนอกและจุดเชื่อมต่อ รวมทั้งสภาพโดยรวมให้เห็นว่าหลักฐานแต่ละชิ้นวางไว้ในตำแหน่งใด

(5.2) ข้อมูลเฉพาะของหลักฐาน เช่น หมายเลข Serial number ผู้ผลิต รุ่น ความเสียหายที่พบ เป็นต้น

(5.3) สิ่งอื่นที่อาจเป็นประโยชน์เพิ่มเติม เช่น สิ่งพิมพ์ กระดาษบันทึกข้อความ หรือหนังสือเกี่ยวกับความรู้ทางคอมพิวเตอร์เพื่อบ่งบอกถึงระดับความรู้ทางคอมพิวเตอร์ของผู้ต้องสงสัย

(6) จดบันทึกรายละเอียดต่อไปนี้

(6.1) สิ่งที่พบ สิ่งที่ได้ดำเนินการ รวมถึงสิ่งผิดปกติ เช่น ร่องรอยความเสียหายภายนอกของหลักฐาน

(6.2) สภาพและรายการอุปกรณ์ภายนอกที่เชื่อมต่อกับหลักฐาน

(6.3) สิ่งอื่นที่อาจเป็นประโยชน์เพิ่มเติม เช่น สิ่งพิมพ์ กระดาษบันทึกข้อความ หรือหนังสือเกี่ยวกับความรู้ทางคอมพิวเตอร์เพื่อบ่งบอกถึงระดับความรู้ทางคอมพิวเตอร์ของผู้ต้องสงสัย

(7) กรณีพบหลักฐานอยู่ภายนอกอาคาร และสภาพอากาศขณะนั้นอาจส่งผลต่อหลักฐาน ควรพิจารณาดำเนินการกับหลักฐานนั้นเป็นลำดับแรก

(8) รวบรวมข้อมูลที่เกี่ยวข้อง เช่น ชื่อผู้ใช้ รหัสผ่าน ข้อมูลในการเข้าใช้งานระบบปฏิบัติการ หรือระบบเครือข่าย การใช้เทคโนโลยีเฉพาะ เช่น การใช้ Active Directory การเข้ารหัสลับข้อมูล (Encryption) เป็นต้น

4.3.2 กรณีหลักฐานเป็นคอมพิวเตอร์

(1) ควรตรวจสอบและจดบันทึกรายละเอียดดังนี้

(1.1) สถานะของคอมพิวเตอร์ว่าปิด เปิด หรืออยู่ในโหมด stand by หากไม่แน่ใจให้ใช้วิธีสังเกตไฟสถานะที่เครื่อง ฟังเสียงการทำงานของพัดลม ขยับเม้าส์ หรือกดคีย์บอร์ดปุ่ม Shift

(1.2) สภาพและรายการอุปกรณ์ภายนอกที่เชื่อมต่อกับคอมพิวเตอร์

(1.3) ตรวจสอบในช่อง CD, DVD, Floppy, Card reader และพอร์ตเชื่อมต่อ USB ต่าง ๆ ว่ามีสื่อบันทึกข้อมูลใด ๆ ค้างอยู่หรือไม่ หากมีให้จดบันทึกไว้เป็นหลักฐานอีกชิ้นหนึ่ง โดยระบุว่าพบในคอมพิวเตอร์เครื่องใด หากเครื่องคอมพิวเตอร์เปิดทำงานอยู่ให้ปฏิบัติตามข้อ 4.3.2 (2) ก่อนถอดสื่อบันทึกข้อมูลออกมาจัดเก็บในบรรจุภัณฑ์

(2) หากพบคอมพิวเตอร์เปิดทำงานอยู่ให้ดำเนินการตามแนวทางดังนี้

(2.1) ถ่ายภาพรายละเอียดต่อไปนี้

ก. หน้าจอแสดงผลของโปรแกรมที่เปิดอยู่ทุกหน้า และทุกแท็บ

ข. หากพบข้อมูลแสดงวันเวลาของเครื่องปรากฏที่หน้าจอแสดงผล ให้ถ่ายภาพวันเวลาให้เห็นชัดเจนเทียบกับนาฬิกาเทียบเวลา

(2.2) ถ้าหน้าจอแสดงผลถูกล็อคและต้องใช้รหัสผ่านในการเข้าสู่ระบบปฏิบัติการ ให้สอบถามรหัสผ่านจากเจ้าของเครื่องเพื่อปลดล็อคเครื่อง หากไม่ทราบรหัสผ่านที่ถูกต้องให้ปิดเครื่องด้วยวิธีการตามข้อ 4.3.2 (2.13)

(2.3) หากสังเกตพบการใช้เทคนิคซ่อนหรือทำลายข้อมูลเพื่อไม่ให้สามารถตรวจพิสูจน์พยานหลักฐานได้หรือทำได้ลำบาก (Anti-forensics) เช่น การใช้ซอฟต์แวร์ลบข้อมูล ให้หยุดการทำงานของซอฟต์แวร์นั้นทันที แล้วจดบันทึกลักษณะการทำลายข้อมูลที่สังเกตได้ และวิธีการที่ใช้หยุดการทำงานของซอฟต์แวร์นั้น รวมทั้งผลลัพธ์ที่ปรากฏ

(2.4) จัดเก็บ Volatile data

(2.5) หากพบว่าโพรเซสที่ทำงานอยู่มีความเชื่อมโยงกับที่เก็บข้อมูลนอกสถานที่ (Off-site storage หรือ Cloud storage) ให้พิจารณาขอบเขตอำนาจหน้าที่ในการจัดเก็บ

หลักฐานดิจิทัล ในกรณีที่มีความจำเป็นต้องดำเนินการเกินขอบเขตอำนาจ ให้ขออำนาจทางกฎหมายเพิ่มเติม

(2.6) บันทึกไฟล์ที่พบว่าเปิดอยู่ลงในสื่อบันทึกข้อมูลที่พร้อมใช้งาน (Save As) บันทึกภาพหรือจดบันทึกชื่อไฟล์ ตำแหน่งที่ปรากฏ (Path) ในคอมพิวเตอร์ โดยระวังไม่ทำให้ไฟล์ในคอมพิวเตอร์ถูกเปลี่ยนแปลง

(2.7) หากพบ Virtual machine เปิดทำงานอยู่ ให้สั่ง Hibernate เครื่อง Virtual machine และจดบันทึกว่าเป็นการเก็บรวบรวมหลักฐานดิจิทัลจาก Virtual machine

(2.8) กรณีที่เกี่ยวข้องกับมัลแวร์ และคอมพิวเตอร์ติดตั้งโปรแกรมแอนตี้ไวรัสไว้ ให้เก็บข้อมูล Log ของโปรแกรมแอนตี้ไวรัส

(2.9) หากพบซอฟต์แวร์เข้ารหัสลับข้อมูล (Encryption) ติดตั้งอยู่ หรือสันนิษฐานว่าอาจมีการเข้ารหัสลับฮาร์ดดิสก์ ให้ทำสำเนาข้อมูลแบบ Logical ตามข้อ 5.3.1.4 (2) เนื่องจากสำเนาข้อมูลที่ได้จะไม่ถูกเข้ารหัสลับ ก่อนที่จะปิดเครื่องคอมพิวเตอร์ และให้สอบถามรหัสผ่านจากเจ้าของข้อมูล

(2.10) หากมีการใช้ฮาร์ดดิสก์แบบ RAID ให้ทำสำเนาข้อมูลแบบ Logical ตามข้อ 5.3.1.4 (2) จัดเก็บข้อมูลในทุกพาร์ทิชัน และสอบถามรวมทั้งจดบันทึกข้อมูล ดังต่อไปนี้

ก. เป็นแบบฮาร์ดแวร์ RAID หรือ ซอฟต์แวร์ RAID

ข. เป็น RAID แบบใด (เช่น 0, 1, 5, หรือ 10)

ค. ขนาดของ Stripe/Chunk (Stripe/Chunk size)

ง. กรณีเป็นฮาร์ดแวร์ RAID มีลำดับการเรียงฮาร์ดดิสก์และเชื่อมต่อพอร์ตอย่างไร

จ. กรณีเป็นซอฟต์แวร์ RAID ใช้ซอฟต์แวร์ใดในการบริหารจัดการ RAID

(2.11) กรณีที่ไม่สามารถทำสำเนาข้อมูลได้เองทั้งหมดและจำเป็นต้องได้รับความร่วมมือจากผู้ดูแลระบบ ควรคำนวณค่าแฮชยืนยันความถูกต้องของสำเนา และจัดให้มีรับรองโดยเจ้าของข้อมูลและผู้ทำสำเนาด้วย

(2.12) พิจารณาความเป็นไปได้ในการปิดเครื่องคอมพิวเตอร์ เพื่อจัดเก็บหลักฐานมาดำเนินการต่อในห้องปฏิบัติการ หากไม่สามารถปิดเครื่องได้ ให้ทำสำเนาข้อมูลขณะที่เครื่องเปิดด้วยวิธี Physical หรือ Logical

(2.13) กรณีสามารถปิดคอมพิวเตอร์ได้ ให้ดำเนินการด้วยวิธีการสำหรับ คอมพิวเตอร์พีซี แล็ปท็อป และเซิร์ฟเวอร์ ดังนี้

ก. คอมพิวเตอร์พีซี

ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวเครื่องคอมพิวเตอร์พีซีออก (ไม่ใช่ถอดจากแหล่งจ่ายไฟฟ้า)

ข. เซิร์ฟเวอร์

ข.1 ในกรณีเซิร์ฟเวอร์ดังกล่าวเป็นเครื่องให้บริการที่มีระบบฐานข้อมูล ควรปิดโปรแกรมฐานข้อมูลตามขั้นตอนที่กำหนดไว้ในคู่มือการใช้งาน ก่อนปิดเครื่อง

ข.2 ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวเครื่องเซิร์ฟเวอร์ออก

ข.3 เนื่องจากอาจมีข้อมูลที่สามารถใช้เป็นพยานหลักฐานดิจิทัลบันทึกไว้ในเทปสำรองข้อมูล จึงควรพิจารณาจัดเก็บเทปสำรองข้อมูลและเครื่องอ่านเทปที่เกี่ยวข้อง

ค. แล็ปท็อป

ค.1 ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวแล็ปท็อปออก

ค.2 ถอดแบตเตอรี่ออก

ค.3 หากไม่สามารถถอดแบตเตอรี่ออกได้ ให้กดปุ่มเปิดเครื่องค้างไว้จนกว่าเครื่องจะดับ

(3) หากพบคอมพิวเตอร์ปิดอยู่ให้ดำเนินการตามแนวทางดังนี้

(3.1) ถอดสายที่เชื่อมต่อกับเครือข่ายและอุปกรณ์ต่อพ่วงทั้งหมด และควรบันทึกการเชื่อมต่อสายต่าง ๆ ข้างต้นไว้ด้วย

(3.2) หากจำเป็นต้องทำสำเนาหลักฐานดิจิทัลในสถานที่เกิดเหตุ ให้ใช้วิธีการตามข้อ 5.3

(3.3) จัดเก็บคอมพิวเตอร์ และสายไฟฟ้าลงบรรจุภัณฑ์ โดยปฏิบัติตามข้อ 4.4

(3.4) กรณีที่เป็นเซิร์ฟเวอร์ ให้รวบรวมข้อมูลเกี่ยวกับ RAID ตามข้อ 4.3.2 (2.10) และพิจารณาจัดเก็บเทปสำรองข้อมูลและเครื่องอ่านเทปที่เกี่ยวข้อง

4.3.3 กรณีหลักฐานเป็นเครื่องมือสื่อสารเคลื่อนที่

(1) หากทำได้ ให้สอบถามรหัสผ่านเพื่อปลดล็อคเครื่องและซิมการ์ด และจดบันทึกโดยให้ระบุด้วยว่าเป็น PIN หรือ Pattern lock

(2) ในกรณีที่หลักฐานเปิดใช้งานอยู่ และสามารถเข้าใช้งานได้ ควรดำเนินการดังนี้

(2.1) ตรวจสอบรายละเอียดเกี่ยวกับหลักฐาน และตั้งค่าเครื่องมือสื่อสาร ดังนี้

ก. บันทึกภาพหลักฐานและเนื้อหาที่ปรากฏบนหน้าจอแสดงผล และจดบันทึกข้อมูลโดยละเอียด

ข. ตรวจสอบข้อมูลเฉพาะของหลักฐาน เช่น IMEI รุ่น ผู้ให้บริการ เป็นต้น

ค. เปิดการใช้งานโหมดเครื่องบิน (Airplane mode) เพื่อตัดการรับสัญญาณ

ง. ปิดการใช้งานสัญญาณไร้สาย (Wi-Fi) เพื่อตัดการสื่อสารผ่านระบบเน็ตเวิร์ก

จ. ปิดการใช้งานสัญญาณบลูทูธ (Bluetooth)

ฉ. ปิดการใช้รหัสผ่าน เพื่อให้สามารถเข้าถึงเครื่องได้ภายหลัง

ช. ปิดการล็อคหน้าจอแสดงผล (Disable screen lock)

(2.2) ดำเนินการบรรจุและเคลื่อนย้ายหลักฐาน

(3) กรณีที่ไม่สามารถเข้าใช้งานหลักฐานได้ เช่น ติดล็อครหัสผ่าน ให้บันทึกภาพหลักฐานและเนื้อหาที่ปรากฏบนหน้าจอแสดงผล และจดบันทึกโดยละเอียด หลังจากนั้นจึงดำเนินการบรรจุและเคลื่อนย้ายหลักฐาน

(4) กรณีที่หลักฐานอยู่ในสถานะปิดการใช้งาน ให้ดำเนินการบรรจุและเคลื่อนย้ายหลักฐาน

(5) ไม่ควรถอดแบตเตอรี่ออกจากตัวเครื่องเนื่องจากอาจทำให้สูญเสียข้อมูล เช่น ประวัติการโทร การตั้งค่าวันเวลาในหลักฐาน เป็นต้น เว้นแต่ในกรณีที่จำเป็นต้องเก็บเครื่องเป็นระยะเวลานาน ควรถอดแบตเตอรี่ออกเพื่อป้องกันแบตเตอรี่เสื่อมสภาพซึ่งอาจทำให้สารที่อยู่ในแบตเตอรี่รั่วซึมและก่อให้เกิดความเสียหายแก่หลักฐานนั้นได้

(6) เก็บอุปกรณ์เสริมทั้งหมด เช่น สายเคเบิลสำหรับชาร์จไฟ สายเคเบิลข้อมูลสำหรับต่อเชื่อม SD card ซิมการ์ด เป็นต้น รวมทั้งตรวจดูบริเวณรอบ ๆ ว่ามีการจดรหัสผ่านไว้หรือไม่ หากพบให้รวบรวมไว้

(7) หากพบเครื่องมือสื่อสารเคลื่อนที่อยู่ในน้ำ ให้รีบถอดแบตเตอรี่ออกทันที แล้วจัดเก็บอุปกรณ์ในสภาพที่มีน้ำในแหล่งที่พบหลักฐานอยู่ และนำกลับไปตรวจวิเคราะห์ในห้องปฏิบัติการโดยเร็ว

4.3.4 กรณีหลักฐานเป็นสื่อบันทึกข้อมูล

สื่อบันทึกข้อมูลในที่นี้หมายความรวมถึง สื่อบันทึกข้อมูลดิจิทัล ได้แก่ ฮาร์ดดิสก์แบบเชื่อมต่อภายนอก USB Flash drive, SD card, CD, DVD และ Blu-ray Disc เป็นต้น การเก็บสื่อบันทึกข้อมูลเหล่านี้ควรดำเนินการตามแนวทางดังนี้

(1) จัดเก็บลงในบรรจุภัณฑ์
(2) ในกรณีจำเป็นต้องทำสำเนาหลักฐานดิจิทัลในสถานที่เกิดเหตุ ให้ดำเนินการตามข้อ 5.3
(3) หากพบสื่อบันทึกข้อมูลอยู่ในน้ำ ให้จัดเก็บหลักฐานในสภาพที่มีน้ำในแหล่งที่พบหลักฐานอยู่และนำกลับไปตรวจวิเคราะห์ในห้องปฏิบัติการโดยเร็ว

4.3.5 การคัดกรองข้อมูลในหลักฐาน (Triage/Preview)

การคัดกรองข้อมูลในหลักฐาน เป็นกระบวนการ เพื่อเปิดดู คัดแยก และจัดลำดับความสำคัญข้อมูลที่เกี่ยวข้องสำหรับเก็บรวบรวมและตรวจวิเคราะห์ในภายหลัง โดยให้เกิดการเปลี่ยนแปลงของข้อมูลน้อยที่สุด และการเปลี่ยนแปลงนั้นต้องไม่เกี่ยวข้องกับสาระสำคัญของพยานหลักฐานดิจิทัล โดยการปฏิบัติกระบวนการนี้ขึ้นอยู่กับความเหมาะสม หรือความจำเป็น แล้วแต่กรณี เช่น เงื่อนไขความเร่งด่วนในการทราบผล

ในกรณีที่ต้องจัดให้มีการคัดกรองข้อมูลในหลักฐาน มีข้อพึงระวัง ดังนี้

(1) ผู้ดำเนินการต้องอธิบายสิ่งที่ได้ดำเนินการ ผลการดำเนินการ และการเปลี่ยนแปลงที่เกิดขึ้นกับข้อมูลภายในหลักฐานได้
(2) กระบวนการนี้เป็นเพียงขั้นตอนการตรวจสอบเบื้องต้น ซึ่งไม่สามารถทดแทนการตรวจพิสูจน์ที่ครบถ้วนได้ จึงมีความเป็นไปได้ที่จะไม่พบข้อมูลสำคัญที่ต้องการ
(3) ก่อนดำเนินการควรตรวจสอบให้แน่ใจว่าซอฟต์แวร์คัดกรองข้อมูลในหลักฐานที่เตรียมมาสามารถใช้กับหลักฐานนั้น ๆ ได้
(4) ผู้ดำเนินการต้องพยายามไม่ทำให้วันเวลาของข้อมูลที่บันทึกในหลักฐานเปลี่ยนแปลงไป

4.4 การบรรจุและการเคลื่อนย้าย (Packaging and Transportation)

4.4.1 กรณีหลักฐานเป็นเครื่องมือสื่อสารเคลื่อนที่ ซึ่งสถานะของเครื่องเปิดใช้งานและติดรหัสผ่าน ทำให้ไม่สามารถตั้งค่าอุปกรณ์เพื่อตัดสัญญาณได้ ให้บรรจุหลักฐานลงในอุปกรณ์ป้องกันคลื่นสัญญาณก่อน แล้วจึงดำเนินการในขั้นตอนต่อไป

4.4.2 จัดเก็บหลักฐานลงในบรรจุภัณฑ์ ใช้เทปปิดผนึกปิดผนึกหลักฐานให้เรียบร้อย ไม่ให้มีรอยชำรุดฉีกขาด ลงชื่อผู้ปฏิบัติงานและวันเวลาคร่อมทับเทปปิดผนึกกำกับไว้

4.4.3 ติดป้ายหมายเลขกำกับ (Label) หลักฐานลงบนบรรจุภัณฑ์ทุกชิ้น โดยห้ามติดบนหลักฐานโดยตรง

4.4.4 ในการดำเนินการควรระบุรายละเอียดใน Chain of custody โดยบันทึกข้อมูลให้ครบถ้วน

4.4.5 ควรขนย้ายหลักฐานมายังยานพาหนะเป็นลำดับสุดท้ายก่อนที่จะออกจากสถานที่เกิดเหตุ และขนย้ายหลักฐานไปเก็บในที่ปลอดภัยทันทีที่ถึงจุดหมายปลายทาง

4.4.6 เคลื่อนย้ายหลักฐานด้วยความระมัดระวังเป็นพิเศษ หลีกเลี่ยงการกระทบกระเทือน การวางหลักฐานซ้อนทับกัน บริเวณที่มีสนามแม่เหล็กไฟฟ้าหรือไฟฟ้าสถิต เช่น ใกล้ลำโพงและวิทยุสื่อสาร เป็นต้น บริเวณที่มีแสงแดดจัดหรือมีความชื้นและการเปลี่ยนแปลงของอุณหภูมิหรือความชื้นกะทันหัน

4.4.7 ในการรับและส่งมอบหลักฐาน ก่อนส่งมอบให้สังเกตสภาพบรรจุภัณฑ์ว่าชำรุดหรือไม่ เทปปิดผนึกฉีกขาดหรือไม่ และถ่ายภาพสภาพหลักฐานที่ได้รับมา

5. การปฏิบัติงานในห้องปฏิบัติการ

5.1 เครื่องมือ

5.1.1 เครื่องมือทั่วไป

(1) อุปกรณ์ถ่ายภาพ
(2) ถุงมือ (ชนิดที่ไม่ทิ้งร่องรอยติดหลักฐาน และใช้ครั้งเดียว)
(3) เครื่องสำรองไฟฟ้า (UPS)
(4) ชุดเครื่องมือ เช่น ไขควงแฉก ไขควงแบน ไขควงหกเหลี่ยม และ มีดคัตเตอร์ เป็นต้น
(5) บรรจุภัณฑ์สำหรับจัดเก็บหลักฐาน เช่น ถุงกระดาษ ถุงพลาสติก และถุงป้องกันไฟฟ้าสถิต เป็นต้น
(6) แบบฟอร์มที่เกี่ยวข้อง เช่น Chain of custody เป็นต้น

5.1.2 เครื่องมือตรวจพิสูจน์

ผู้ปฏิบัติงานควรเตรียมเครื่องมือตรวจพิสูจน์เบื้องต้น ดังนี้

(1) นาฬิกาเทียบเวลา
(2) คอมพิวเตอร์สำหรับงานตรวจพิสูจน์หลักฐานดิจิทัล
(3) ซอฟต์แวร์สำหรับตรวจพิสูจน์หลักฐาน
(4) เครื่องมือสำหรับตรวจพิสูจน์เครื่องมือสื่อสาร
(5) เครื่องมือคัดกรองข้อมูลในหลักฐาน
(6) เครื่องมือทำสำเนาข้อมูล
(7) Write blocker
(8) สื่อบันทึกข้อมูลที่พร้อมใช้งานสำหรับเก็บสำเนาหลักฐานดิจิทัล เช่น ฮาร์ดดิสก์ หรือ USB flash drive เป็นต้น
(9) อุปกรณ์ป้องกันคลื่นสัญญาณ เช่น Faraday bag, กล่องโลหะปิดสนิท, อลูมิเนียมฟอยล์ หรืออุปกรณ์อื่นที่ผ่านการทดสอบแล้วว่าป้องกันคลื่นสัญญาณได้

5.2 การประเมินและวางแผนการตรวจพิสูจน์ (Evaluation)

การประเมินและวางแผนการตรวจพิสูจน์ ควรดำเนินการตามแนวทางดังนี้

5.2.1 ประเมินความเป็นไปได้ในการตรวจพิสูจน์ โดยพิจารณาจากองค์ประกอบต่างๆ เช่น บุคลากร ความรู้ ความเชี่ยวชาญ เครื่องมือ และระยะเวลาดำเนินการ เป็นต้น

5.2.2 วางแผนการเกี่ยวกับ แนวทางในการตรวจพิสูจน์ ข้อมูลที่ต้องตรวจวิเคราะห์ วิธีการที่ใช้ และเครื่องมือที่ใช้

5.2.3 ในกรณีที่มีหลักฐานหลายชิ้น ควรจัดลำดับความสำคัญของหลักฐาน ให้คำนึงถึงข้อควรระวังตามข้อ 4.3.5

5.2.4 กรณีคดีที่มีจุดประสงค์ในการตรวจพิสูจน์เดียวกัน หากมีหลักฐานประเภทเดียวกันหลายชิ้น ควรเลือกใช้แนวทางและวิธีการตรวจพิสูจน์แบบเดียวกัน

5.3 การสำเนาข้อมูล (Acquisition)

การสำเนาข้อมูลควรดำเนินการตามแนวทางดังนี้

(1) การสำเนาข้อมูลต้องทำโดยผู้ที่ผ่านการฝึกอบรมมาแล้วเท่านั้น
(2) ผู้ปฏิบัติงานต้องศึกษาวิธีการใช้งานและข้อจำกัดของเครื่องมือที่นำมาใช้ทำสำเนาข้อมูลอย่างละเอียด
(3) ควรสวมถุงมือระหว่างการปฏิบัติงาน
(4) ควรระมัดระวังในการแกะบรรจุภัณฑ์
(5) ตรวจสอบและบันทึกสภาพทางกายภาพของหลักฐานทุกชิ้นก่อนนำมาตรวจพิสูจน์ เช่น ฝาปิดเคสคอมพิวเตอร์พีซีถูกปิดขันน็อตอย่างเรียบร้อยหรือไม่ ฝาหลังส่วนที่ปิดฮาร์ดดิสก์ของแล็ปท็อปถูกปิดขันน็อตอย่างเรียบร้อยหรือไม่ เป็นต้น
(6) สังเกตสภาพทางกายภาพของหลักฐาน และระมัดระวังหลักฐานที่อาจมีสิ่งปนเปื้อนที่เป็นพิษหรือมีอันตรายต่อชีวิตได้
(7) สำเนาข้อมูลในหลักฐาน
    (7.1) สำเนาข้อมูลในหลักฐานด้วยกระบวนการที่น่าเชื่อถือและสามารถตรวจสอบได้
    (7.2) สำเนาข้อมูลลงในสื่อบันทึกข้อมูลที่พร้อมใช้งาน
    (7.3) หากพบข้อผิดพลาดระหว่างการสำเนาข้อมูล ให้จดบันทึกรายละเอียดไว้
    (7.4) ยืนยันความครบถ้วนสมบูรณ์ของข้อมูลที่สำเนาได้ ด้วยการคำนวณและเปรียบเทียบค่าแฮช ของต้นฉบับและสำเนา เช่น MD5 SHA1 SHA256 เป็นต้น โดยดำเนินการอย่างน้อยสองรูปแบบ
(8) จัดเก็บสื่อบันทึกข้อมูลที่เก็บสำเนาข้อมูลไว้ในบรรจุภัณฑ์

5.3.1 การสำเนาข้อมูลจากคอมพิวเตอร์และสื่อบันทึกข้อมูล

การสำเนาข้อมูลจากคอมพิวเตอร์และสื่อบันทึกข้อมูล ให้ดำเนินการตามแนวทางดังนี้

5.3.1.1 ถอดฮาร์ดดิสก์แบบเชื่อมต่อภายในออกจากคอมพิวเตอร์อย่างระมัดระวัง บันทึกภาพสภาพและการเชื่อมต่อก่อนการถอด เพื่อให้สามารถประกอบฮาร์ดดิสก์กลับเข้าไปยังตำแหน่งเดิมได้อย่างถูกต้อง

5.3.1.2 หลังจากถอดฮาร์ดดิสก์แบบเชื่อมต่อภายในออกหมดทุกลูกแล้ว ให้ตรวจดูว่ามีสื่อบันทึกข้อมูลอื่นอยู่ในเครื่องหรือเชื่อมต่อที่พอร์ตใด ๆ หรือไม่ เช่น CD, DVD, USB flash drive หากพบให้นำออกจากเครื่องแล้วจดบันทึกไว้ กำหนดเป็นหลักฐานเพิ่มเติม

5.3.1.3 เชื่อมต่อคอมพิวเตอร์เข้ากับจอแสดงผล และเสียบปลั๊กไฟ แล้วบู๊ตเครื่องและเข้า BIOS เพื่อตรวจสอบค่าวันและเวลาของเครื่องเทียบกับวันและเวลาของนาฬิกาเทียบเวลา แล้วจดบันทึก

5.3.1.4 การสำเนาข้อมูล แบ่งเป็น 3 ประเภท ได้แก่ Physical, Logical, และ Volatile data การสำเนาข้อมูลด้วยวิธีการเหล่านี้ให้ดำเนินการตามแนวทางดังนี้

(1) Physical

ก. เป็นการสำเนาข้อมูลทั้งหมดในหลักฐานแบบบิตต่อบิต (bit-by-bit)

ข. ใช้ Write blocker เพื่อป้องกันการเปลี่ยนแปลงข้อมูลต้นฉบับ หากทำได้

ค. สามารถทำได้โดยใช้วิธีการใดวิธีการหนึ่งดังนี้

ค.1 Imaging (Disk-to-file) คือ การสำเนาฮาร์ดดิสก์ทั้งลูกเก็บในรูปแบบไฟล์

ค.2 Cloning (Disk-to-disk) คือ การสำเนาฮาร์ดดิสก์ทั้งลูกลงในฮาร์ดดิสก์อีกลูกหนึ่ง

(2) Logical

ก. เป็นการสำเนาข้อมูลเฉพาะส่วนจากหลักฐาน เช่น พาร์ทิชัน, ไดเร็กทอรี หรือ ไฟล์บางไฟล์ เป็นต้น

ข. ใช้ Write blocker เพื่อป้องกันการเปลี่ยนแปลงข้อมูลต้นฉบับ หากทำได้

ค. อาจเลือกใช้ในกรณีพบ RAID หรือกรณีที่คาดว่าฮาร์ดดิสก์หลักฐานถูกเข้ารหัสลับไว้

(3) Volatile data

ก. อย่างน้อยให้สำเนาข้อมูลจากหน่วยความจำหลัก (RAM) ของคอมพิวเตอร์ที่กำลังเปิดใช้งานอยู่ (Live) ซึ่งข้อมูลสามารถเปลี่ยนแปลงได้ตลอดเวลา

ข. รันซอฟต์แวร์สำหรับจัดเก็บ Volatile data จากสื่อบันทึกข้อมูล (เช่น USB flash drive) ที่เชื่อถือได้

ค. การรันคำสั่งซอฟต์แวร์สำหรับจัดเก็บข้อมูลต้องใช้สิทธิระดับสูงที่สุด (Administrator) เพื่อให้สามารถจัดเก็บข้อมูลได้ครบถ้วน

ง. ซอฟต์แวร์สำหรับจัดเก็บข้อมูลบางตัว จะบันทึกสำเนาข้อมูลลงในโฟลเดอร์เดียวกับโฟลเดอร์ที่ซอฟต์แวร์นั้นอยู่ ดังนั้นจึงต้องตรวจสอบพื้นที่ในสื่อบันทึกข้อมูลให้มีเพียงพอจัดเก็บก่อนเริ่มจัดเก็บข้อมูล

จ. ห้ามจัดเก็บ Volatile data ลงในหลักฐาน

5.3.1.5 หลังจากตรวจสอบค่าวันและเวลาของเครื่อง และสำเนาข้อมูลเสร็จแล้ว ประกอบฮาร์ดดิสก์กลับเข้าไปในคอมพิวเตอร์อย่างเดิม แล้วปิดฝา ขันน็อตให้เรียบร้อย (หากได้รับคอมพิวเตอร์มาในสภาพที่มีน็อตปิดฝา)

5.3.1.6 จัดเก็บหลักฐาน (Store) ตามวิธีการที่เหมาะสม

5.3.2 การสำเนาข้อมูลจากเครื่องมือสื่อสารเคลื่อนที่

5.3.2.1 กรณีเครื่องอยู่ในสถานะเปิดการใช้งาน

(1) ตรวจดูสถานะแบตเตอรี่ หากเหลือน้อยให้ชาร์จแบตเตอรี่ให้เต็ม แล้วจึงสำเนาข้อมูลจากตัวเครื่องด้วยวิธีที่เหมาะสม โดยศึกษาจากคู่มือการใช้งานของเครื่องมือที่ใช้ในการสำเนาข้อมูล เนื่องจากเครื่องมือสื่อสารเคลื่อนที่แต่ละรุ่นมีวิธีดำเนินการที่แตกต่างกัน

(2) หลังจากสำเนาข้อมูลจากตัวเครื่องเสร็จแล้วให้ปิดเครื่อง ถอดสื่อบันทึกข้อมูลอื่นที่พบออกมา เช่น ซิมการ์ด SD Card เป็นต้น แล้วสำเนาข้อมูล

(3) จดบันทึกข้อมูลเฉพาะของเครื่องมือสื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูลที่พบ เช่น ยี่ห้อ Model IMEI และ Serial number เป็นต้น

(4) หลังจากสำเนาข้อมูลจากตัวเครื่องและสื่อบันทึกข้อมูลอื่นที่พบเรียบร้อยแล้ว ให้นำสื่อบันทึกข้อมูลประกอบกลับเข้าไปในตำแหน่งเดิม

5.3.2.2 กรณีเครื่องอยู่ในสถานะปิดการใช้งาน

(1) ถอดสื่อบันทึกข้อมูลอื่นที่พบ เช่น ซิมการ์ด SD Card เป็นต้น แล้วนำสื่อบันทึกข้อมูลดังกล่าวไปสำเนาข้อมูล

(2) เปิดเครื่องมือสื่อสารเคลื่อนที่และตรวจดูสถานะแบตเตอรี่ หากเหลือน้อยให้ชาร์จแบตเตอรี่ให้เต็ม แล้วจึงสำเนาข้อมูลจากตัวเครื่องด้วยวิธีที่เหมาะสม โดยศึกษาจากคู่มือการใช้งานของเครื่องมือที่ใช้ในการสำเนาข้อมูล

(3) จดบันทึกข้อมูลเฉพาะของเครื่องมือสื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูลที่พบ เช่น ยี่ห้อ Model IMEI และ Serial number เป็นต้น

(4) หลังจากสำเนาข้อมูลจากตัวเครื่องและสื่อบันทึกข้อมูลอื่นที่พบเรียบร้อยแล้ว ให้นำสื่อบันทึกข้อมูลประกอบกลับเข้าไปในตำแหน่งเดิม

หมายเหตุ ในกรณีที่เครื่องมือไม่สามารถสำเนาข้อมูลจากตัวเครื่องได้ ให้กดดูข้อมูลจากอุปกรณ์โดยตรง เช่น ประวัติการโทรศัพท์ สมุดโทรศัพท์ SMS และ อีเมล เป็นต้น พร้อมทั้งบันทึกภาพถ่ายหรือวิดีโอ แสดงหน้าจอข้อมูลในแต่ละรายการ หรือหากมีอำนาจหน้าที่ทางกฎหมายและมีบุคลากรและเครื่องมือพร้อมอาจสกัดข้อมูลด้วยวิธี Chip-off

5.4 การวิเคราะห์ (Analysis)

5.4.1 ผู้ปฏิบัติงานต้องผ่านการฝึกอบรมและมีความเชี่ยวชาญในขอบข่ายที่ตรวจพิสูจน์

5.4.2 ห้ามวิเคราะห์หลักฐานดิจิทัลต้นฉบับโดยตรง ให้ดำเนินการจากสำเนาหลักฐานดิจิทัลเท่านั้น

5.4.3 ปฏิบัติตามมาตรการควบคุมและมาตรฐานที่สอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้อง

5.4.4 ตรวจสอบเวลาที่ตั้งค่าในหลักฐานดิจิทัลให้แน่ใจ เช่น การตั้งค่าวันและเวลาใน BIOS และค่า Time zone เพื่อให้สามารถตั้งค่าในซอฟต์แวร์ตรวจพิสูจน์หลักฐานดิจิทัลได้อย่างถูกต้อง

6. การบันทึก (Document) และรายงานผลการตรวจพิสูจน์ (Report)

6.1 การบันทึก

ในการดำเนินการทุกขั้นตอนต้องบันทึกข้อมูลและจัดทำเอกสารที่จำเป็น และเก็บรักษาเอกสารไว้ตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง โดยควรบันทึกข้อเท็จจริงที่เกี่ยวข้องกับการตรวจพิสูจน์ ให้มีรายละเอียดเพียงพอที่หากมีการเปลี่ยนแปลงผู้รับผิดชอบคดีแล้ว ผู้ที่มารับผิดชอบคนใหม่จะสามารถเข้าใจที่มาและสิ่งที่ได้ดำเนินการไปแล้วได้

การบันทึกควรมีรายละเอียดอย่างน้อย ดังนี้

(1) ชื่อผู้ปฏิบัติงาน

(2) วันและเวลาที่เริ่มดำเนินการ และวันและเวลาที่ดำเนินการแล้วเสร็จ

(3) รายละเอียดของการรวบรวมหลักฐาน เช่น รูปแบบและเวอร์ชันของเครื่องมือที่ใช้สำเนาข้อมูล เป็นต้น

(4) สภาพทางกายภาพ และข้อมูลเฉพาะของหลักฐาน เช่น คำอธิบายสภาพทางกายภาพ Serial number ผู้ผลิต และ รุ่น เป็นต้น

(5) คำอธิบายเกี่ยวกับหลักฐาน

(6) ค่าแฮชของหลักฐานดิจิทัลต้นฉบับและของสำเนาอย่างน้อยสองรูปแบบ
(7) ภาพถ่าย และ/หรือ แผนภาพ/แผนที่
(8) รายละเอียดเกี่ยวกับบรรจุภัณฑ์และสภาพของหลักฐานที่ได้รับเอกสาร Chain of custody
(9) ข้อมูลที่ได้รับจากการหารือหรือสอบถามผู้ที่เกี่ยวข้อง
(10) สำเนาเอกสารแสดงการอนุญาต หรือเอกสารตามกฎหมาย เช่น หมายศาล หนังสือยินยอมให้ตรวจสอบหรือจัดเก็บหลักฐาน เป็นต้น
(11) ข้อมูลเพิ่มเติมอื่น ๆ ตามที่กฎหมายกำหนด
(12) ประเด็นที่ตรวจพิสูจน์
(13) วิธีการวิเคราะห์ข้อมูลในหลักฐาน และผลการวิเคราะห์

6.2 การรายงานผลการตรวจพิสูจน์

ผลการตรวจพิสูจน์ต้องนำเสนอในรูปแบบที่เข้าใจได้ง่าย ถึงแม้ผู้อ่านไม่มีความรู้ด้านเทคนิค

6.2.1 ผู้ตรวจพิสูจน์ต้องสามารถอธิบายสิ่งที่ปรากฏในรายงานทั้งหมดได้
6.2.2 ระบุรายละเอียดการสำเนาข้อมูลในหลักฐาน และการจัดการกับหลักฐาน
6.2.3 ตอบประเด็นที่ต้องตรวจพิสูจน์ รวมถึงระบุข้อมูลที่สำคัญ ได้แก่
(1) ชื่อผู้ตรวจพิสูจน์
(2) วันที่ตรวจพิสูจน์
(3) วัตถุประสงค์และขอบเขตของการตรวจพิสูจน์
(4) ข้อจำกัดในการตรวจพิสูจน์ (หากมี)
(5) รายละเอียดของพยานหลักฐาน โดยระบุสภาพภายนอก วิธีการบรรจุและเคลื่อนย้าย รวมถึงความสมบูรณ์และความถูกต้องของหลักฐาน การปิดผนึกและการลงลายมือชื่อกำกับ
(6) รายละเอียดของเครื่องมือที่ใช้ในการตรวจพิสูจน์
(7) กระบวนการตรวจพิสูจน์ และรายละเอียดอื่น ๆ ที่เกี่ยวข้อง
(8) ผลการตรวจพิสูจน์และบทสรุป

7. คุณสมบัติของผู้ปฏิบัติงาน

7.1 ผู้ปฏิบัติงานในสถานที่เกิดเหตุ

ผู้ปฏิบัติงานในสถานที่เกิดเหตุ ควรผ่านการฝึกอบรม และมีความรู้ ดังนี้ เพื่อประโยชน์ในการเก็บรวบรวมหรือสำเนาพยานหลักฐานให้ถูกต้องครบถ้วน

(1) กฎหมาย หลักการ รูปแบบ และวิธีการ ที่เกี่ยวข้องกับการค้นสถานที่เกิดเหตุ
(2) ทักษะที่ต้องใช้ในสถานที่เกิดเหตุ เช่น การเข้าพื้นที่ การถ่ายภาพ การควบคุมผู้ต้องหา การสัมภาษณ์ผู้ที่เกี่ยวข้อง การจดบันทึก และข้อจำกัดต่าง ๆ ในการปฏิบัติงานในสถานที่เกิดเหตุ รวมทั้งผลลัพธ์ที่เกิดจากข้อจำกัดนั้น
(3) หลักการสำคัญเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐาน เช่น
- การคัดกรองข้อมูลในหลักฐาน
- การเก็บรวบรวมหลักฐาน
- การสำเนาหลักฐาน

- การรักษาสภาพของหลักฐาน
- การจัดเก็บหลักฐาน
- การทดสอบยืนยันการทำงานของซอฟต์แวร์/ฮาร์ดแวร์/เครื่องมือที่ใช้ (Validation)
- การบรรจุและเคลื่อนย้ายหลักฐาน ความเสี่ยง และผลลัพธ์ที่อาจเกิดขึ้นจากปัจจัยต่าง ๆ เช่น อุณหภูมิ ความชื้น และแรงกระแทก
- Chain of custody

(4) ความคุ้นเคยกับเทคโนโลยีและอุปกรณ์ดิจิทัลชนิดต่าง ๆ ที่อาจเป็นหลักฐานได้ เช่น

- การจัดเก็บข้อมูลแบบ RAID
- ระบบเครือข่าย
- อุปกรณ์ระบบเครือข่าย
- ข้อมูลรูปแบบต่าง ๆ เช่น ฐานข้อมูล ไฟล์เอกสาร และ ไฟล์รูปภาพ
- ระบบไฟล์ เช่น NTFS, FAT และ ext4
- ระบบปฏิบัติการ เช่น Microsoft Windows, UNIX (Linux) และ Mac OS

(5) ความเข้าใจถึงความสำคัญของข้อมูล เช่น ข้อมูล System log, Application configuration, Email server log, Web server log และ IP information

7.2 ผู้ปฏิบัติงานตรวจวิเคราะห์ข้อมูลในห้องปฏิบัติการ

ผู้ปฏิบัติงานตรวจวิเคราะห์ข้อมูลในห้องปฏิบัติการ ควรผ่านการฝึกอบรม และมีความรู้ ดังนี้ เพื่อความน่าเชื่อถือของผลการวิเคราะห์และตรวจพิสูจน์พยานหลักฐานดิจิทัล

(1) ทักษะที่ต้องใช้ในห้องปฏิบัติการ เช่น วิธีการและการใช้เครื่องมือในการประกอบข้อมูลที่ถูกจัดเก็บแบบ RAID การคัดกรองข้อมูลในหลักฐาน การทำสำเนาข้อมูล การจดบันทึก การเขียนรายงานสรุปผลการตรวจพิสูจน์ และข้อจำกัดต่าง ๆ ในการตรวจวิเคราะห์ข้อมูล รวมทั้งผลลัพธ์ที่เกิดจากข้อจำกัดนั้น

(2) หลักการสำคัญเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐาน เช่น

- การคัดกรองข้อมูลในหลักฐาน
- การเก็บรวบรวมหลักฐาน
- การสำเนาหลักฐาน
- การรักษาสภาพของหลักฐาน
- การจัดเก็บหลักฐาน
- การทดสอบยืนยันการทำงานของซอฟต์แวร์/ฮาร์ดแวร์/เครื่องมือที่ใช้ (Validation)
- การบรรจุและเคลื่อนย้ายหลักฐาน ความเสี่ยง และผลลัพธ์ที่อาจเกิดขึ้นจากปัจจัยต่าง ๆ เช่น อุณหภูมิ ความชื้น และแรงกระแทก
- Chain of custody

(3) ความคุ้นเคยกับเทคโนโลยีและอุปกรณ์ดิจิทัลชนิดต่าง ๆ ที่อาจเป็นหลักฐานได้ เช่น

- การจัดเก็บข้อมูลแบบ RAID
- ระบบเครือข่าย

- อุปกรณ์ระบบเครือข่าย
- ข้อมูลรูปแบบต่าง ๆ เช่น ฐานข้อมูล ไฟล์เอกสาร และ ไฟล์รูปภาพ
- ระบบไฟล์ เช่น NTFS, FAT และ ext4
- ระบบปฏิบัติการ เช่น Microsoft Windows, UNIX (Linux) และ Mac OS

(4) ความเข้าใจถึงความสำคัญของข้อมูล เช่น ข้อมูล System log, Application configuration, Email server log, Web server log และ IP information

(5) ความรู้ทางเทคนิคที่จำเป็นสำหรับการวิเคราะห์ข้อมูล เช่น

- File systems
- Operating Systems (OS)
- String search
- Data carve
- Email analysis
- Registry analysis
- Artifact analysis
- Log file analysis
- Web browser analysis
- Network analysis
- Memory forensics
- Malware analysis
- Cloud forensics

8. ข้อเสนอแนะเพิ่มเติม

8.1 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

8.1.1 ในการตรวจพิสูจน์หลักฐานดิจิทัล ควรสำเนาข้อมูลอย่างน้อย 2 ชุด แบ่งเป็น Master copy และ Working copy เพื่อลดความเสี่ยงที่อาจเกิดการเปลี่ยนแปลงและปนเปื้อนของพยานหลักฐาน ดังนี้

(1) Master copy เป็นสำเนาข้อมูลที่ทำจากหลักฐานดิจิทัล โดยสำเนานี้จะถูกเก็บรักษาไว้อย่างมั่นคงปลอดภัยเหมือนเป็นหลักฐานชิ้นหนึ่ง และไม่ถูกนำไปใช้ เว้นแต่มีความจำเป็นต้องกลับไปใช้ข้อมูลจากหลักฐานต้นฉบับ จะใช้ข้อมูลจากสำเนานี้แทน เพื่อลดความเสี่ยงที่อาจเกิดผลกระทบต่อข้อมูลในหลักฐาน

(2) Working copy เป็นสำเนาข้อมูลที่ทำจาก Master copy จะถูกใช้ในการตรวจวิเคราะห์ ทั้งนี้ ในการสำเนาข้อมูลทุกครั้งต้องตรวจเปรียบเทียบค่าแฮชของต้นฉบับข้อมูลและสำเนาข้อมูลทั้งสองชุดด้วย

8.1.2 มีการกำหนดชั้นความลับ และจำกัดสิทธิในการเข้าถึงข้อมูลโดยกำหนดบุคคลผู้มีสิทธิเข้าถึงข้อมูลและประเภทของข้อมูลเช่น

(1) หนังสือร้องขอให้ดำเนินการตรวจพิสูจน์ประเด็นต่าง ๆ
(2) สำเนาหลักฐานดิจิทัล
(3) บันทึกการตรวจค้น และการตรวจพิสูจน์
(4) ผลการตรวจพิสูจน์
(5) ไฟล์หรือข้อมูลที่คัดลอกออกมาจากหลักฐานดิจิทัล

8.1.3 เลือกใช้สื่อบันทึกข้อมูลที่จะนำมาใช้เก็บรักษาข้อมูลในระยะยาวที่เหมาะสม คำนึงถึงอายุของสื่อบันทึกข้อมูล และเครื่องมือที่ใช้ในการอ่านข้อมูล

8.2 แบบฟอร์มต่าง ๆ

ควรมีแบบฟอร์ม Checklist หรือ Template เพื่อความถูกต้อง ครบถ้วนของข้อมูล เช่น

(1) Checklist เครื่องมือที่ต้องนำไปในสถานที่เกิดเหตุ
(2) Checklist หรือ แบบฟอร์มรวบรวมรายชื่อเครื่องมือที่ใช้ ซึ่งมีข้อมูลยืนยันการทดสอบ (Validate) เครื่องมือแต่ละชิ้น หรือการอ้างอิงไปยังเอกสารอื่นที่เชื่อถือได้ เช่น ผลการทดสอบเครื่องมือจาก National Institute of Standards and Technology (NIST)
(3) Template การจดบันทึกข้อมูลในสถานที่เกิดเหตุ
(4) Template การจดบันทึกข้อมูลการตรวจพิสูจน์ในห้องปฏิบัติการ
(5) Template การเขียนรายงานผลการตรวจพิสูจน์
(6) แบบฟอร์ม Chain of custody โดยมีตัวอย่างในภาคผนวก ก
ข้อมูลที่ต้องระบุลงใน Chain of custody ได้แก่
(6.1) ข้อมูลการติดต่อและลายมือชื่อของผู้ส่งมอบหลักฐาน
(6.2) ข้อมูลการติดต่อและลายมือชื่อของผู้รับมอบหลักฐาน
(6.3) วันที่และเวลาในการรับและส่งมอบหลักฐาน
(6.4) เหตุผลในการรับและส่งมอบหลักฐาน
(6.5) วิธีการส่งมอบหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้อง หรือส่งมอบโดยพนักงานส่งของ เป็นต้น
(6.6) สถานที่จัดเก็บหลักฐาน
(6.7) รายละเอียดเกี่ยวกับหลักฐาน เช่น ประเภท ยี่ห้อ รุ่น สี Serial number และสภาพ เป็นต้น
(7) แบบฟอร์มในการรับคำร้องขอการตรวจพิสูจน์
(8) แบบฟอร์มบันทึกประวัติการฝึกอบรม และความเชี่ยวชาญของเจ้าหน้าที่แต่ละคน

8.3 เครื่องมือ

เครื่องมือสำหรับใช้ในการปฏิบัติงานมีหลากหลายประเภท ทั้งที่เป็นแบบ Commercial และแบบ Open source ซึ่งผู้ปฏิบัติงานควรศึกษาวิธีใช้เครื่องมืออย่างถูกต้องเพื่อให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ และควรเลือกใช้เครื่องมือที่ผ่านการทดสอบ (Validate) ยืนยันการทำงานมาแล้วเท่านั้น โดยผู้ปฏิบัติงานอาจทดสอบเอง หรือศึกษาจากแหล่งอ้างอิงที่เชื่อถือได้ เช่น NIST ก็ได้

เครื่องมือสามารถแบ่งตามประเภทการใช้งาน ได้แก่

(1) Forensic data acquisition tools
(2) Write blockers
(3) Triage/Preview tools
(4) Forensic examination tools

โดยมีตัวอย่างรายชื่อเครื่องมือปรากฏในภาคผนวก ค และผู้ที่สนใจสามารถหาข้อมูลเพิ่มเติมได้จาก http://forensicswiki.org/wiki/Tools

ภาคผนวก ก ตัวอย่างแบบฟอร์ม

Chain of Custody

หน่วยงานที่ร้องขอ:				
เลขที่หนังสือ:			**ลงวันที่:**	
ชื่อผู้ติดต่อ:			**โทรศัพท์:**	
ลำดับที่	**หมายเลขพยานหลักฐาน**	**ประเภท และ ลักษณะพยานหลักฐาน** (เช่น ฮาร์ดดิสก์, แฟลชไดร์ฟ ,ฯลฯ)	**คำอธิบาย** (เช่น ยี่ห้อ, รุ่น, Serial Number)	**วันที่ส่งพยานหลักฐานคืน**

ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	หลักฐานลำดับที่:	เหตุผล: ต้นทาง:	ปลายทาง:	วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	**รับรายงานผลการตรวจ**			วันที่: เวลา:
ลงชื่อ...ผู้ให้ (..)	ลงชื่อ...ผู้รับ (..)	**รับเอกสารประกอบรายงานผลการตรวจ**			วันที่: เวลา:

ภาคผนวก ข ข้อมูลเพิ่มเติมทางเทคนิค

ข.1 การเทียบเวลา

ระหว่างกระบวนการเก็บหรือสำเนาหลักฐานดิจิทัล ผู้ปฏิบัติงานจำเป็นต้องเทียบเวลาของหลักฐานดิจิทัล กับเวลามาตรฐาน และให้บันทึกความคลาดเคลื่อนจากเวลามาตรฐาน โดยให้บันทึกเป็นหน่วยของเวลาระดับที่ละเอียดที่สุดที่จะทำได้ ตัวอย่างของเวลามาตรฐาน ได้แก่ เวลาจากนาฬิกามาตรฐานของสถาบันมาตรวิทยาแห่งชาติ (รายละเอียดของนาฬิกาอ้างอิงสามารถดูเพิ่มเติมได้ที่ http://www.nimt.or.th/index.php?menu=time)

ข.2 การตรวจสอบข้อมูลที่สำคัญในเครื่องมือสื่อสารเคลื่อนที่

ตามหลักการแล้ว ผู้ปฏิบัติงานไม่ควรเปิดดูข้อมูลในเครื่องมือสื่อสารเคลื่อนที่โดยไม่จำเป็น เพราะจะทำให้ข้อมูลในหลักฐานเปลี่ยนแปลง แต่เพื่อประโยชน์ในการสืบสวน ก่อนที่จะสำเนาข้อมูลหรือส่งตรวจในห้องปฏิบัติการ ผู้รับผิดชอบคดีอาจพิจารณาตรวจดูเฉพาะข้อมูลที่สำคัญอย่างระมัดระวัง และทำให้ข้อมูลเปลี่ยนแปลงน้อยที่สุด โดยตรวจสอบข้อมูลดังนี้

(1) ตรวจสอบ IMEI โดยกด *#06#
(2) ตรวจสอบหมายเลขโทรศัพท์ โดย
    ก. สำหรับเครือข่าย AIS กด *545# แล้วกดโทรออก
    ข. สำหรับเครือข่าย DTAC กด *102# แล้วกดโทรออก
    ค. สำหรับเครือข่าย TRUE กด *933# แล้วกดโทรออก
(3) ตรวจสอบชื่อบัญชีของแอปพลิเคชันที่ใช้ติดต่อสื่อสาร เช่น อีเมล, LINE และ Facebook เป็นต้น

ภาคผนวก ค ตัวอย่างเครื่องมือในงานตรวจพิสูจน์หลักฐานดิจิทัล

ตัวอย่างเครื่องมือในงานตรวจพิสูจน์หลักฐานดิจิทัล มีดังนี้

(1) Forensic data acquisition tools

เป็นเครื่องมือที่ใช้ในการสำเนาข้อมูลจากหลักฐานดิจิทัล มีทั้งชนิดฮาร์ดแวร์ และ ซอฟต์แวร์

(1.1) ชนิดฮาร์ดแวร์

แต่ละรุ่นจะรองรับการเชื่อมต่อกับฮาร์ดดิสก์แบบต่าง ๆ เช่น IDE, SATA มีความสามารถป้องกันการเขียนทับข้อมูลต้นฉบับ (Write block), สามารถสำเนาข้อมูลหลายชุดพร้อมกันได้ และสามารถตั้งค่าให้คำนวณค่าแฮชแบบต่าง ๆ เช่น MD5, SHA1, SHA256 เพื่อยืนยันความถูกต้องครบถ้วนของข้อมูลหลังจากเสร็จสิ้นการสำเนาข้อมูลได้ ตัวอย่างเช่น Voom Hardcopy 3P/III, Logicube, Image MASSter และ Tableau TD3 เป็นต้น

(1.2) ชนิดซอฟต์แวร์

ต้องรันซอฟต์แวร์บนคอมพิวเตอร์ โดยเชื่อมต่อสื่อบันทึกข้อมูลต้นฉบับ และสื่อบันทึกข้อมูลที่พร้อมใช้งานที่นำมาบันทึกสำเนาข้อมูล เข้ากับเครื่องคอมพิวเตอร์ที่รันซอฟต์แวร์ ซอฟต์แวร์บางตัวมีความสามารถในการป้องกันการเขียนทับข้อมูลต้นฉบับ แต่สำหรับซอฟต์แวร์ที่ไม่สามารถป้องกันการเขียนได้ ต้องเชื่อมต่อสื่อบันทึกข้อมูลต้นฉบับเข้ากับเครื่องคอมพิวเตอร์ผ่านอุปกรณ์ Write blocker ด้วย ตัวอย่างเช่น FTK Imager, EnCase, F-Response, dd/dcfldd, MacQuisition, DumpIt (สำหรับเก็บ RAM) และ RamCapture (สำหรับเก็บ RAM) เป็นต้น

(2) Write blocker

เป็นอุปกรณ์ป้องกันการเขียนทับข้อมูลต้นฉบับ มีหลายแบบ (Interface) ขึ้นอยู่กับการเชื่อมต่อกับสื่อบันทึกข้อมูลต้นฉบับที่ต้องการสำเนา เช่น USB, SATA, IDE, SCSI, SAS ในการใช้งานจะเชื่อมต่อกับคอมพิวเตอร์ผ่านพอร์ตต่าง ๆ ได้ เช่น USB, FireWire, eSATA ตัวอย่างเช่น Tableau และ Digital Intelligence เป็นต้น

(3) Triage/Preview tools

เป็นเครื่องมือที่ใช้ในการคัดกรองข้อมูลที่คาดว่าเกี่ยวข้องกับคดีจากหลักฐาน เพื่อให้ได้ข้อมูลเบื้องต้นมาอย่างรวดเร็ว ไม่ต้องรอให้สำเนาข้อมูลเสร็จก่อน โดยเครื่องมือจะสามารถแสดงผลข้อมูลแบบแบ่งเป็นประเภทต่าง ๆ ได้ ทำให้สามารถวิเคราะห์ข้อมูลที่พบได้เร็วขึ้น โดยไม่ทำให้ข้อมูลในหลักฐานเปลี่ยนแปลง ตัวอย่างเช่น ADF Solution, DFF (Digital Forensics Framework) และ IEF (Internet Evidence Finder) เป็นต้น

(4) Forensic examination tools

เป็นเครื่องมือช่วยวิเคราะห์ข้อมูลในหลักฐาน โดยเครื่องมือจะแปลงข้อมูลที่ถูกเก็บในที่ต่าง ๆ ในรูปแบบต่าง ๆ ในคอมพิวเตอร์หรือเครื่องมือสื่อสารเคลื่อนที่ ให้ออกมาในรูปแบบที่คนสามารถอ่านได้ง่าย โดยเครื่องมือสามารถอำนวยความสะดวกแก่ผู้ปฏิบัติงาน เช่น สามารถกรองข้อมูลประเภทที่ต้องการ, จัดเรียงข้อมูล, ค้นหาคำ, กู้ข้อมูลที่ถูกลบไปแล้ว รวมทั้งบริหารจัดการข้อมูลของแต่ละคดีได้ เป็นต้น ตัวอย่างเช่น FTK, EnCase, X-Ways Forensics, IEF, BlackLight, The Sleuth Kit และ SIFT Workstation เป็นต้น

อภิธานศัพท์

ค่าแฮช (Hash Value) หมายถึง ค่าเฉพาะที่ได้จากการคำนวณเนื้อหาของข้อมูลด้วยฟังก์ชันทางคณิตศาสตร์ เป็นเสมือนลายนิ้วมือของข้อมูล ใช้ยืนยันความถูกต้องครบถ้วนของข้อมูล โดยค่านี้มักเป็นเลขฐาน 16 ความยาวแน่นอน ขึ้นอยู่กับฟังก์ชันที่ใช้ ที่นิยมได้แก่ MD5 ซึ่งมีขนาด 16 ไบต์ (128 บิต) ดังนั้นค่า MD5 ทั้งหมดที่จะมีได้คือ 2^128 ค่า และ SHA1 ซึ่งมีขนาด 20 ไบต์ เป็นต้น

System log หมายถึง ล็อกของระบบ หรือไฟล์ที่เก็บข้อมูลเกี่ยวกับการตั้งค่าการทำงาน ประวัติการใช้งาน รวมทั้งข้อผิดพลาดที่เกิดขึ้นในระบบ

Application configuration หมายถึง การตั้งค่าการทำงานของแอปพลิเคชัน

Email server log หมายถึง ล็อกของอีเมลเซิร์ฟเวอร์ หรือข้อมูลเกี่ยวกับประวัติการรับส่งอีเมลแต่ละฉบับของแต่ละบัญชีผู้ใช้ มีข้อมูล เช่น ผู้ส่ง ผู้รับ ผู้ที่ได้รับสำเนาอีเมล วันเวลาการรับส่งอีเมล เป็นต้น

Web server log หมายถึง ล็อกของเว็บเซิร์ฟเวอร์ ซึ่งอาจประกอบไปด้วยล็อกการเข้าใช้งาน (Access log) และล็อกข้อผิดพลาด (Error log)

Forensic data acquisition หมายถึง การสำเนาข้อมูลจากหลักฐานดิจิทัล โดยทั่วไปจะมีการคำนวณค่าแฮชยืนยันความถูกต้องครบถ้วนของสำเนาข้อมูลที่ได้

Virtual machine หมายถึง คอมพิวเตอร์เสมือนที่ถูกจำลองขึ้นมาด้วยโปรแกรมเฉพาะไว้ภายในเครื่องคอมพิวเตอร์ที่ใช้งานจริง และมีความสามารถในการทำงานเหมือนกับคอมพิวเตอร์จริง

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 21 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310

เว็ปไซต์ไทยเซิร์ต www.thaicert.or.th
เว็ปไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) www.etda.or.th
เว็ปไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th