ข้อกำหนดขั้นต่ำด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดีย

เอกสารสำหรับห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ที่จัดตั้งใหม่

หน่วยงานพันธมิตรเชิงกลยุทธ์ด้านนิติวิทยาศาสตร์ระหว่างประเทศ

(INTERNATIONAL FORENSIC STRATEGIC ALLIANCE: IFSA)

ฉบับที่ 1

IFSA

International Forensic Strategic Alliance

หน่วยงานพันธมิตรเชิงกลยุทธ์ด้านนิติวิทยาศาสตร์ระหว่างประเทศ

(INTERNATIONAL FORENSIC STRATEGIC ALLIANCE: IFSA)

ข้อกำหนดขั้นต่ำด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดีย

เอกสารสำหรับจัดต้องห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์

IFSA ข้อกำหนดขั้นต่ำ 4

IFSA

International Forensic Strategic Alliance

เอกสารฉบับนี้แปลจากเอกสารต้นฉบับภาษาอังกฤษ และจัดทำขึ้นเพื่ออำนวยความสะดวกในการเข้าถึงของห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ทั่วโลก ซึ่งไม่ใช่การแปลอย่างเป็นทางการ

©พฤศจิกายน 2566 (ค.ศ. 2023)

สารบัญ

บทนำ	3
คำนำ	4
1 ความสามารถของบุคลากร	6
2 เครื่องมือและวัสดุสิ้นเปลือง	9
3 การเก็บรวบรวมวัตถุพยาน การตรวจพิสูจน์ การแปลผล และการรายงานผลการตรวจพิสูจน์	12
4 ระเบียบปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และการตรวจสอบความใช้ได้	18
5 การบริหารจัดการด้านคุณภาพ	20
6 อภิธานศัพท์	22

บทนำ

หน่วยงานพันธมิตรเชิงกลยุทธ์ด้านนิติวิทยาศาสตร์ระหว่างประเทศ (INTERNATIONAL FORENSIC STRATEGIC ALLIANCE: IFSA) ได้พัฒนาเอกสารฉบับนี้ เพื่อเป็นข้อกำหนดขั้นต่ำที่ซึ่งจะช่วยให้ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ที่จัดตั้งใหม่ในประเทศกำลังพัฒนาสามารถให้บริการทางวิทยาศาสตร์แก่กระบวนการยุติธรรมได้

วัตถุประสงค์ของคู่มือมาตรฐานฉบับนี้ เพื่อเป็นพื้นฐานหรือจุดเริ่มต้นสำหรับห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ให้ปฏิบัติตาม เพื่อให้ผลการตรวจพิสูจน์มีความถูกต้อง แม่นยำ และน่าเชื่อถือ ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ควรมีความมุ่งมั่นในการปรับปรุงคุณภาพการให้บริการอย่างต่อเนื่อง

คู่มือมาตรฐานฉบับนี้ได้อธิบายข้อกำหนดขั้นต่ำด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดีย โดยระบุหัวข้อ ดังต่อไปนี้

1. ความสามารถของบุคลากร
2. เครื่องมือและวัสดุสิ้นเปลือง
3. การเก็บรวบรวมวัตถุพยาน การตรวจพิสูจน์ การแปลผล และการรายงานผลการตรวจพิสูจน์
4. ระเบียบปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และการทดสอบความใช้ได้
5. การบริหารจัดการด้านคุณภาพ

คำนำ

หน่วยงานพันธมิตรเชิงกลยุทธ์ด้านนิติวิทยาศาสตร์ระหว่างประเทศ (INTERNATIONAL FORENSIC STRATEGIC ALLIANCE: IFSA) เป็นความร่วมมือกันระหว่างเครือข่ายห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์จาก 6 ภูมิภาค ประกอบด้วย

- ห้องปฏิบัติการตรวจพิสูจน์ทางอาชญากรรมของสหรัฐอเมริกา (American Society of Crime Laboratory Directors: ASCLD)
- เครือข่ายนิติวิทยาศาสตร์แห่งยุโรป (European Network of Forensic Science Institutes: ENFSI)
- สถาบันนิติวิทยาศาสตร์แห่งชาติ ออสเตรเลีย นิวซีแลนด์ (National Institute of Forensic Science Australia New Zealand: NIFS ANZ)
- สถาบันอาชญวิทยาและนิติวิทยาศาสตร์ของ Iberoamericana (Academia Iberoamericana de Criminalística y Estudios Forenses: AICEF)
- เครือข่ายนิติวิทยาศาสตร์แห่งภูมิภาคเอเชีย (Asian Forensic Sciences Network: AFSN)
- เครือข่ายนิติวิทยาศาสตร์แห่งภูมิภาคแอฟริกาใต้ (Southern Africa Regional Forensic Science Network:SARFS)

IFSA ทำงานร่วมกับพันธมิตร 3 หน่วยงาน ได้แก่ ศูนย์วิจัย Leverhulme ด้านนิติวิทยาศาสตร์ (Leverhulme Research Centre for Forensic Science) สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) และองค์กรตำรวจสากล (INTERPOL)

IFSA ตระหนักถึงความสำคัญของการบริหารจัดการด้านคุณภาพของห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ ทั้งนี้ เพื่อให้ผลการตรวจพิสูจน์เป็นไปตามมาตรฐาน ไม่ว่าจะเป็นการปฏิบัติงานในภาคสนาม หรือภายในห้องปฏิบัติการ

ในเดือนกุมภาพันธ์ พ.ศ. 2555 ได้มีการจัดประชุมพิเศษของ IFSA ณ กรุงเวียนนา โดย UNODC เป็นเจ้าภาพ เพื่อหารือเกี่ยวกับสิ่งที่จำเป็นที่ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ที่จัดตั้งขึ้นใหม่ในประเทศกำลังพัฒนาควรมี จึงเห็นควรให้มีการจัดทำเอกสารข้อกำหนดขั้นต่ำ (MRD) เพื่อให้คำแนะนำแก่ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์เหล่านั้น

ในเดือนตุลาคม พ.ศ. 2557 ได้มีการจัดทำและทบทวนเอกสารในสาขาเฉพาะทาง 3 ชุดแรก ได้แก่ การพิสูจน์เอกลักษณ์ของยาเสพติด, การตรวจวิเคราะห์ดีเอ็นเอ และการตรวจสถานที่เกิดเหตุ เอกสารเหล่านี้มุ่งเน้นด้านคุณภาพที่สำคัญ โดยใช้ถ้อยคำอย่างง่าย และมีการยกตัวอย่างประกอบ เอกสารข้อกำหนดขั้นต่ำ (MRD) ทั้ง 3 ชุดดังกล่าว ได้มีการทำให้เป็นปัจจุบันและทบทวนเป็นเวอร์ชั่น 2 ซึ่งประกาศใช้เอกสารเหล่านี้ในเดือนธันวาคม พ.ศ. 2563 เอกสารข้อกำหนดขั้นต่ำ (MRD) ด้านการตรวจพิสูจน์พยานเอกสาร และด้านพิษวิทยา เอกสารทั้ง 2 ชุดนี้ได้มีการประกาศใช้ในปี พ.ศ. 2566 และในขณะนี้ เอกสารข้อกำหนดขั้นต่ำ (MRD) เพิ่มเติมในด้านการตรวจพิสูจน์มานุษวิทยา และการตรวจพิสูจน์ลายพิมพ์นิ้วมืออยู่ระหว่างการพัฒนา

เอกสารข้อกำหนดขั้นต่ำ (MRD) เหล่านี้ มีวัตถุประสงค์เพื่อเป็นคู่มือเริ่มต้นสำหรับห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ที่จัดตั้งขึ้นใหม่ เพื่อสร้างระบบการบริหารจัดการด้านคุณภาพ และความสามารถในการปฏิบัติงานในระยะเวลาอันสั้น ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ควรดำเนินการภายใต้ข้อกำหนดขั้นต่ำนี้ และควรพยายามปรับปรุงคุณภาพการบริการอย่างต่อเนื่อง โดยได้รับการรับรองมาตรฐานที่กำหนดไว้

ในการจัดทำร่างเอกสารเหล่านี้ คณะทำงานแลผู้เชี่ยวชาญจากเครือข่ายนิติวิทยาศาสตร์ระดับภูมิภาคทั้ง 6 แห่ง ตลอดจนพันธมิตรของ IFSA ได้มีส่วนสนับสนุนโดยประชุมหารือหลายครั้ง เอกสารข้อกำหนดขั้นต่ำ (MRD) ฉบับสมบูรณ์จะเกิดขึ้นไม่ได้ หากไม่มีส่วนร่วมของทุกภาคส่วนดังที่ได้กล่าวมา

IFSA หวังเป็นอย่างยิ่งว่าเอกสารเหล่านี้จะเป็นส่วนสำคัญสำหรับห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ในการสร้างการให้บริการทางด้านนิติวิทยาศาสตร์ที่มีคุณภาพ

คณะกรรมการ IFSA

พฤศจิกายน 2566 (ค.ศ. 2023)

1 ความสามารถของบุคลากร

เจ้าหน้าที่ห้องปฏิบัติการทุกคนต้องมีความเข้าใจในหน้าที่และความรับผิดชอบของตนเองอย่างชัดเจน และควรปฏิบัติหน้าที่และความรับผิดชอบเหล่านี้ตามจรรยาบรรณที่ใช้ในห้องปฏิบัติการ[1]

ในส่วนนี้เจ้าหน้าที่ห้องปฏิบัติการควรมีการศึกษาและการฝึกอบรมขั้นต่ำที่จำเป็นสำหรับการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดีย

1.1 การศึกษา

ความพิเศษทางนิติวิทยาศาสตร์ด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดียมักมีความซับซ้อน เนื่องจากพบว่าข้อกำหนดด้านการศึกษาด้านนี้ยังไม่ทันสมัย ความต้องการในการพัฒนาการตรวจพิสูจน์ การค้นหา การสกัด การนำเสนอ การตีความ และการเก็บรักษาพยานหลักฐานดิจิทัล เป็นตัวกำหนดความซับซ้อนและทักษะที่หลากหลาย ไม่เฉพาะด้านนิติวิทยาศาสตร์ดั้งเดิม แต่ยังมีด้านอื่นนอกจากกระบวนการยุติธรรมทางอาญา เช่น ด้านการธนาคาร ด้านมัลติมีเดีย ด้านโทรคมนาคม ด้านวิศวกรรมซอฟต์แวร์ และอื่น ๆ

สิ่งเหล่านี้มักทำให้การพัฒนาหลักสูตรการฝึกอบรมขั้นต่ำสำหรับเจ้าหน้าที่ที่ปฏิบัติงานด้านนิติวิทยาศาสตร์ที่รับผิดชอบในการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีความซับซ้อน ยกตัวอย่าง ผู้เชี่ยวชาญเฉพาะทางสามารถทำงานได้เทียบเท่าผู้เชี่ยวชาญด้านมัลติมีเดียในอุตสาหกรรมด้านบันเทิง และอยู่ในบริบทงานด้านนิติวิทยาศาสตร์

ถึงแม้ว่าข้อกำหนดด้านการศึกษาระดับสูงจะไม่เฉพาะเจาะจง แต่ควรขึ้นอยู่กับลักษณะและความซับซ้อนของงานที่ต้องดำเนินการ และเจ้าหน้าที่ที่ปฏิบัติงาน (ผู้ตรวจพิสูจน์/เจ้าหน้าที่ทางด้านเทคนิค) ควรมีวุฒิการศึกษาระดับมหาวิทยาลัย หรือคุณสมบัติที่เทียบเท่า (ตัวอย่างเช่น ประกาศนียบัตรที่เป็นการรับรองระบบเฉพาะด้านเครือข่าย, ด้านเสียง, ด้านภาพเคลื่อนไหว, ด้านโปรแกรมคอมพิวเตอร์ เป็นต้น หรือประกาศนียบัตรที่เน้นด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ได้รับจากผู้ให้การรับรอง) โดยเน้น

---

[1] ตัวอย่างจรรยาบรรณที่ใช้ในห้องปฏิบัติการโดยเครือข่ายห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์จาก 6 ภูมิภาค

- ห้องปฏิบัติการตรวจพิสูจน์ทางอาชญากรรมของสหรัฐอเมริกา (American Society of Crime Laboratory Directors: ASCLD) – www.ascld.org
- เครือข่ายนิติวิทยาศาสตร์แห่งยุโรป (European Network of Forensic Science Institutes: ENFSI) – www.enfsi.eu
- สถาบันนิติวิทยาศาสตร์แห่งชาติ ออสเตรเลีย นิวซีแลนด์ (National Institute of Forensic Science Australian New Zealand: NIFS ANZ) – www.anzfss.org
- สถาบันอาชญวิทยาและนิติวิทยาศาสตร์ของ Iberoamericana (Academia Iberoamericana de Criminalistica y Estudios Forenses: AICEF) – www.aicef.net
- เครือข่ายนิติวิทยาศาสตร์แห่งภูมิภาคเอเชีย (Asian Forensic Sciences Network: AFSN) – www.afsn.asia

ทางด้านเทคโนโลยีสารสนเทศเป็นอย่างมาก อย่างไรก็ตาม ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์ยังคงมีหน้าที่ให้การศึกษา ฝึกอบรม และประสบการณ์ในการตรวจพิสูจน์ที่ดำเนินการในห้องปฏิบัติการ

การธำรงรักษาและการพัฒนาชุดทักษะที่มีอยู่ของผู้ตรวจพิสูจน์ทางด้านดิจิทัลเป็นสิ่งสำคัญลำดับแรก เนื่องจากบริบททางวิชาการด้านนี้มีการพัฒนาสูง โอกาสในการศึกษาอย่างต่อเนื่อง (ตัวอย่างเช่น การเข้าร่วมประชุม, การสัมมนา, การทบทวนวรรณกรรมทางวิทยาศาสตร์ที่เกี่ยวข้อง) ต้องแสวงหาอย่างแข็งขัน รวมถึงการมีส่วนร่วมกับผู้ปฏิบัติงานที่มีลักษณะงานคล้ายกันผ่านเครือข่าย เช่น เครือข่ายความร่วมมือ IFSA และการประชุมทั้งแบบเป็นทางการและไม่เป็นทางการ

นอกจากทักษะทางวิชาการด้านการตรวจพิสูจน์ทางด้านดิจิทัลแล้ว เจ้าหน้าที่ที่ปฏิบัติงานควรได้รับการศึกษาที่เกี่ยวข้องตามหน้าที่ดังต่อไปนี้

- การบริหารจัดการในบริบทการสืบสวนที่ซับซ้อน
- การเก็บรักษาวัตถุพยาน และการบันทึกวัตถุพยาน
- ทักษะการถ่ายภาพนิ่งและภาพเคลื่อนไหวของวัตถุพยาน
- ระบบการบริหารจัดการคดี
- ทักษะการสื่อสารที่ดี (ทั้งการเขียนและการพูด) และความสามารถในการสื่อสารเรื่องที่ซับซ้อนให้เข้าใจได้ง่าย
- ความสามารถในการนำเสนอสิ่งที่ตรวจพบจากวัตถุพยานในกระบวนการยุติธรรมได้ (กระบวนการทางกฎหมาย)

1.2 การฝึกอบรม

ห้องปฏิบัติการควรมีเอกสารโปรแกรมการฝึกอบรมสำหรับเจ้าหน้าที่ที่ปฏิบัติงานทางด้านเทคนิค การฝึกอบรมควรดำเนินการโดยผู้ปฏิบัติงานที่มีสมรรถนะ ความสามารถ และประสบการณ์ และคำนึงถึงความก้าวหน้าของผู้ตรวจพิสูจน์จากพื้นฐานไปจนถึงเชี่ยวชาญในสาขาย่อย (สาขาย่อยมีมากมาย และรวมถึงการตรวจเสียง และการประมวลผลภาพ, การเข้ารหัส, ระบบควบคุมอุตสาหกรรม, การตรวจพิสูจน์โทรศัพท์ทางนิติวิทยาศาสตร์ขั้นสูง เป็นต้น) อย่างไรก็ตาม ก่อนที่ห้องปฏิบัติการทางด้านนิติวิทยาศาสตร์จะมีความเชี่ยวชาญ ควรพิจารณาจ้างการวิเคราะห์ที่ซับซ้อนจากหน่วยงานภายนอก และหาความร่วมมือระหว่างห้องปฏิบัติการ

ประเภทและระดับการฝึกอบรมควรพิจารณาจากรูปแบบการให้บริการสำหรับทีม DF ในแต่ละหน่วยงาน (ตัวอย่างเช่น เข้าร่วมแค่ภาคสนาม หรืออยู่ในห้องปฏิบัติการเท่านั้น)

การพิจารณาจัดจ้างหน่วยงานภายนอกมาดำเนินการฝึกอบรมทั้งหมดหรือบางส่วนสำหรับผู้ให้บริการทางด้านนิติวิทยาศาสตร์ที่ขาดทักษะและประสบการณ์ (ยกตัวอย่างเช่น การตรวจพิสูจน์ข้อมูลทางการเงิน, การตรวจพิสูจน์มัลติมีเดีย เป็นต้น) หรือในกรณีที่จำนวนผู้ตรวจพิสูจน์ที่ต้องได้รับการฝึกอบรมไม่แสดงถึงความพยายามและคงไว้ซึ่งทักษะที่จำเป็นในการพัฒนาและดำเนินการหลักสูตรภายใน อย่างไรก็ตาม แนวทางนี้พิจารณาเฉพาะกรณีที่ส่งผลต่อคุณสมบัติผู้ตรวจพิสูจน์ หากสิ่งที่ได้มาคือ ใบประกาศนียบัตรการเข้าร่วมฝึกอบรม จะไม่สามารถรับประกันได้ว่า ผู้ที่เข้าร่วมฝึกอบรมจะมีทักษะที่มากกว่าตอนก่อนเข้ารับการฝึกอบรม

ควรมีการประเมินประสิทธิผลของการฝึกอบรม โดยถือเป็นส่วนหนึ่งในระบบคุณภาพของห้องปฏิบัติการ

ทักษะทางเทคนิคที่ได้รับจากหลักสูตรการฝึกอบรมทั้งที่เป็นทางการและไม่เป็นทางการจากหน่วยงานภายใน, จากการจัดจ้างหน่วยงานภายนอก หรือหลักสูตรภายนอก ควรได้รับการจัดทำเป็นเอกสาร ควรให้ความสำคัญกับความถี่ของการฝึกอบรม โดยพิจารณาจากความก้าวหน้าอย่างต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ กรณีที่ห้องปฏิบัติการมีการใช้งานโปรแกรมเชิงพาณิชย์ที่เสียค่าใช้จ่าย หรือโปรแกรมภายใน ผู้ตรวจพิสูจน์ที่ได้รับการฝึกอบรมควรได้รับใบประกาศนียบัตรหลังการประเมิน โดยใบประกาศนียบัตรควรระบุขอบเขตของความสามารถและกรอบเวลาที่ความสามารถดังกล่าวนั้นหมดอายุ แม้ว่าหลักสูตรฝึกอบรมที่ไม่มีการประเมินจะเพียงพอสำหรับการพัฒนาผู้ตรวจพิสูจน์ แต่ไม่ควรใช้หลักสูตรที่ไม่มีการประเมินเหล่านี้เพียงอย่างเดียวในการพัฒนาผู้ปฏิบัติงานใหม่

ผู้ปฏิบัติงาน หรือวิธีการทดสอบควรได้รับการประเมินว่ามีความสามารถและมีความชำนาญก่อนปฏิบัติงานที่เกี่ยวกับคดี และได้ใบประกาศนียบัตรที่เกี่ยวข้องกับการทำงานอย่างต่อเนื่อง เพื่อทำให้มั่นใจว่าผ่านการประเมินและการทดสอบอย่างสม่ำเสมอ

ใบประกาศนียบัตรที่เกี่ยวข้องกับการทำงานและการพัฒนาในสาขาวิชาชีพอย่างต่อเนื่องถือเป็นสิ่งสำคัญ

โปรแกรมการฝึกอบรมควรมีวัตถุประสงค์เพื่อพัฒนาทักษะ ดังต่อไปนี้

- การชี้บ่ง การเก็บรักษา และการจัดการความปลอดภัยของแหล่งที่มาของพยานหลักฐานดิจิทัลทั่วไป
- การทำสำเนาข้อมูลทางนิติวิทยาศาสตร์ของข้อมูลดิจิทัลสำหรับการตรวจพิสูจน์
- ความคุ้นชินของเทคนิคการเข้ารหัสค่าความจำเพาะของข้อมูล เพื่อเปิดใช้งานการตรวจสอบความสมบูรณ์ของวัตถุพยานและความคุ้นชินกับอัลกอริธึมทั่วไป (MD5, SHA1, [2]SHA256)
- การตรวจสอบความสมบูรณ์ของไฟล์ และการคงไว้ซึ่งห่วงโซ่วัตถุพยานในทุกขั้นตอนของการตรวจพิสูจน์ (ผ่านการประยุกต์ใช้การเข้ารหัส โดยบุคคลที่เชื่อถือได้ และปลอดภัยแยกต่างหาก)
- การเก็บรักษาข้อมูลต้นฉบับในรูปแบบการเข้ารหัสสำเนาข้อมูล
- การตรวจพิสูจน์ และวิเคราะห์จากสำเนาวัตถุพยานในขอบข่ายของการตรวจ
- การทำเอกสารสิ่งที่ตรวจพบ และข้อมูลที่เกี่ยวข้อง เพื่อสามารถทำซ้ำได้
- การแปลผล และรายงานผลการตรวจพิสูจน์
- การตรวจพบความผิดปกติในผลการตรวจพิสูจน์ และสะท้อนกลับไปยังระบบคุณภาพ และ
- การนำเสนอในชั้นศาล

[2] แนะนำใช้ SHA256 มากกว่า MD5 หรือ SHA1

2 เครื่องมือและวัสดุสิ้นเปลือง

2.1 สิ่งอำนวยความสะดวก

หากเป็นไปได้ สิ่งอำนวยความสะดวกในการรับวัตถุพยาน, การจัดการวัตถุพยาน และการจัดเก็บวัตถุพยานควรแยกพื้นที่ออกจากบริเวณที่ใช้ในการตรวจพิสูจน์ (เพื่อป้องกันความสับสนและโอกาสที่วัตถุพยานสูญหาย เนื่องจากอุปกรณ์ดิจิทัลจำนวนมากมีลักษณะคล้ายกัน)

บริเวณที่ใช้ในการปฏิบัติงานทั้งการทำสำเนาข้อมูล และการตรวจวิเคราะห์พยานหลักฐานดิจิทัลควรเป็นพื้นที่ที่มีเครื่องสำรองไฟเพื่อลดความเสียหายของข้อมูลและการสูญเสียหลักฐาน ควรพิจารณาจำนวนจุดจ่ายไฟ แผ่นป้องกันไฟฟ้าสถิต แสงสว่าง การควบคุมอุณหภูมิและความชื้น และการควบคุมการเข้า-ออกพื้นที่ปฏิบัติงานร่วมด้วย

อาหาร เครื่องดื่ม และของเหลวที่ไม่อยู่ในบรรจุภัณฑ์ ควรแยกออกมาจากบริเวณที่ใช้ปฏิบัติงานของพยานหลักฐานทางอิเล็กทรอนิกส์

หากมีการตรวจพิสูจน์ทางเสียง ควรจัดห้องปฏิบัติการเฉพาะทางเสียงที่มีสภาพแวดล้อมสำหรับการแยกเสียง ซึ่งจะช่วยเพิ่มความสามารถของผู้ตรวจพิสูจน์ได้อย่างมาก ในลักษณะเดียวกัน ควรจัดห้องปฏิบัติการเฉพาะทางแสงที่มีแสงสว่างแบบพิเศษ หรือแผ่นบังแสง เพื่อช่วยตรวจสอบวัตถุที่เกี่ยวกับภาพเคลื่อนไหว

พื้นที่ทั้งหมดที่เกี่ยวข้องกับการจัดเก็บ การจัดการ และการวิเคราะห์ควรมีการรักษาความปลอดภัยและควบคุมการเข้าถึง โดยให้บุคคลที่ไม่ได้รับอนุญาตทั้งหมดถูกพาเข้าไปในสถานที่เสมอ บุคคลที่ไม่ได้รับอนุญาตดังกล่าวควรบันทึกการเข้า-ออกห้องปฏิบัติการเพื่อให้มีบันทึกเมื่ออยู่ในพื้นที่ควบคุม

ห้องตรวจพิสูจน์เฉพาะที่สามารถทำความสะอาดได้ง่าย มีประโยชน์และช่วยให้สามารถประมวลผลอุปกรณ์อิเล็กทรอนิกส์ได้พร้อมกัน (เช่น คอมพิวเตอร์แบบพกพา) สำหรับวัตถุพยานทางอิเล็กทรอนิกส์ และวัตถุพยานทางชีวมิติ (เช่น ลายนิ้วมือ, สารพันธุกรรม)

พื้นที่ในการจัดเก็บ และจัดการกับอุปกรณ์อิเล็กทรอนิกส์ ควรมีการป้องกันไฟฟ้าสถิต เพื่อป้องกันไม่ให้เกิดความเสียหายต่อวัตถุพยาน

2.2 เครื่องมือ

เครื่องมือที่ใช้ในการจัดการ การทำสำเนา และการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทอนิกส์มีหลากหลาย เครื่องมือที่มีความสำคัญต่อพยานหลักฐานทางอิเล็กทรอนิกส์ ได้แก่ (แต่ไม่จำกัดเพียง)

- โครงสร้างพื้นฐานด้านเครือข่าย และสถาปัตยกรรมทางเทคโนโลยีสารสนเทศ (การจัดเก็บและการสำรองสำเนาข้อมูล)
- กล้องถ่ายภาพ (ภาพนิ่งและภาพเคลื่อนไหว) สำหรับบันทึกที่เกิดเหตุ วัตถุพยาน และสิ่งที่ตรวจพบ
- คอมพิวเตอร์สำหรับการปฏิบัติงานภาคสนาม (คอมพิวเตอร์แบบพกพา) และคอมพิวเตอร์สำหรับการประมวลผลพยานหลักฐานทางอิเล็กทรอนิกส์ในห้องปฏิบัติการ

- เครื่องมือป้องกันการเขียนข้อมูลใหม่ (ฮาร์ดแวร์ และ/หรือซอฟต์แวร์) ที่อนุญาตให้เชื่อมต่อกับพยานหลักฐานทางอิเล็กทรอนิกส์เพื่อนำมาวิเคราะห์คอมพิวเตอร์ได้อย่างปลอดภัย
- ซอฟต์แวร์ (แบบเปิดเผยรหัส, แบบไม่มีค่าใช้จ่าย หรือแบบมีค่าใช้จ่าย) ที่อนุญาตให้ทำสำเนาข้อมูล
- สื่อที่สามารถบูตได้ และ/หรือฮาร์ดแวร์ที่จำเป็นอื่น ๆ ที่สามารถเชื่อมต่อและทำสำเนาข้อมูลจากวัตถุพยาน โดยไม่ได้ทำการวิเคราะห์คอมพิวเตอร์
- อัปเดตซอฟต์แวร์ให้เป็นปัจุบัน (แบบเปิดเผยรหัส, แบบไม่มีค่าใช้จ่าย หรือแบบมีค่าใช้จ่าย) เพื่อประมวลผลและตรวจพิสูจน์สำเนาวัตถุพยาน ซอฟต์แวร์ควรมีการจัดทำเป็นเอกสาร และสามารถทำซ้ำในกระบวนการที่ใช้ได้
- อุปกรณ์สกัดข้อมูลจากโทรศัพท์เคลื่อนที่ และ
- เครื่องมือที่ใช้เปิดพยานหลักฐานที่ใช้ในการพิจารณาในชั้นศาล (ยกตัวอย่างเช่น เครื่องอ่านเขียนดีวีดี)
- ฮาร์ดแวร์ที่เกี่ยวกับการทำสำเนาข้อมูล และสายเชื่อมต่อข้อมูลสำหรับอุปกรณ์ที่มีความแปลก

ผู้ตรวจพิสูจน์ควรรักษาและคงความคุ้นเคยกับระบบปฏิบัติการหลายระบบ (รวมถึงระบบปฏิบัติการวินโดวส์, ระบบปฏิบัติการ MacOS และระบบปฏิบัติการ Linux)

คอมพิวเตอร์แบบพกพา, เครื่องป้องกันการเขียนข้อมูลใหม่ และซอฟต์แวร์ทั้งหมดควรได้รับการประเมินความเหมาะสมกับงาน บันทึกการบำรุงรักษาและบันทึกการตรวจสอบเครื่องมือสำคัญที่มีผลต่อการตรวจพิสูจน์ทั้งหมดควรเก็บรักษาไว้เพื่อวัตถุประสงค์ด้านคุณภาพและการสอบกลับได้

เฉพาะผู้ที่ได้รับการฝึกอบรมเกี่ยวกับการใช้อุปกรณ์อย่างปลอดภัยเท่านั้น ที่สามารถเชื่อมต่อและดำเนินการกับวัตถุพยาน

2.3 วัสดุสิ้นเปลือง

วัสดุสิ้นเปลืองทั่วไปที่ใช้ในการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ได้แก่

- สื่อสำหรับจัดเก็บสำเนาวัตถุพยานและภาพถ่าย
    - สื่อบันทึกที่ใช้ในกล้องถ่ายภาพ และใช้ในเครื่องมือบันทึก
    - สื่อบันทึกข้อมูล เช่น แฟลชไดร์ฟ/USB/ดีวีดี/เทปสำหรับจัดเก็บและแสดงผลสำหรับชุดข้อมูลขนาดเล็กถึงชุดข้อมูลขนาดกลาง
    - สื่อบันทึกข้อมูลฮาร์ดไดร์ฟแบบพกพาสำหรับจัดเก็บชุดข้อมูลขนาดใหญ่
- ถุงมือแบบใช้แล้วทิ้ง เพื่อป้องกันผู้ตรวจพิสูจน์จากการปนเปื้อนของวัตถุอันตราย และเพื่อรักษาความสมบูรณ์ของพยานหลักฐานทางนิติวิทยาศาสตร์ด้านอื่น ๆ (โดยปกติเป็นทางด้านชีวมิติ) ในกรณีที่การตรวจพิสูจน์ทางดิจิทัลต้องทำการตรวจพิสูจน์ก่อน และ
- หน้ากากอนามัยแบบใช้แล้วทิ้ง เพื่อรักษาความสมบูรณ์ของพยานหลักฐานทางนิติวิทยาศาสตร์ด้านอื่น ๆ (โดยปกติเป็นทางด้านชีวมิติ)

เมื่อมีการนำสื่อบันทึกข้อมูลกลับมาใช้ใหม่ระหว่างการตรวจพิสูจน์และการทำคดี ควรมีนโยบายและระเบียบปฏิบัติงานเพื่อป้องกันการรั่วไหลของข้อมูลและการปนเปื้อนของสื่อบันทึกข้อมูลระหว่างคดี ยกตัวอย่างเช่น ควรมีการเก็บรักษาบันทึกการล้างข้อมูลดิสก์

และระเบียบปฏิบัติงานในการทวนสอบที่เกี่ยวข้องไว้ในแฟ้มคดี เมื่อมีการล้างข้อมูลดิสก์ ระเบียบปฏิบัติงานต้องให้มีการตรวจสอบความใช้ได้ก่อนใช้งาน เพื่อทำให้มั่นใจว่า ล้างข้อมูลดิสก์ได้อย่างถูกต้อง พร้อมตรวจสอบเพิ่มเติมเพื่อให้แน่ใจว่า ใช้งานได้กับดิสก์ข้อมูลที่มีขนาดความจุมากกว่า 4 เทราไบต์

3 การเก็บรวบรวมวัตถุพยาน การตรวจพิสูจน์ การแปลผล และการรายงานผลการตรวจพิสูจน์

การตรวจพิสูจน์นิติวิทยาศาสตร์ทางด้านดิจิทัลในปัจจุบันสามารถกำหนดขั้นตอนได้ ดังนี้

- การระบุ หรือชี้บ่ง
- การเก็บรักษา
- การทำสำเนา
- การตรวจพิสูจน์
- การวิเคราะห์ และ
- การจัดทำรายงานผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล

3.1 การเก็บรวบรวมวัตถุพยาน

การค้นหาจะดำเนินการเพื่อค้นหาและเลือกข้อมูลที่มีคุณค่าพอที่จะเป็นหลักฐานในคดี เครือข่ายท้องถิ่น เครือข่ายบริเวณกว้าง สภาพแวดล้อมคลาวด์ เครือข่ายส่วนตัวเสมือน และอุปกรณ์โทรคมนาคม เพื่อพิจารณาว่าควรรวมหรือยกเว้นอุปกรณ์หรือสภาพแวดล้อมเฉพาะตามการจัดแสดงที่เป็นไปได้หรือไม่ การตัดสินใจว่า วัตถุพยานชิ้นไหนเกี่ยวข้อง หรือไม่เกี่ยวข้อง วัตถุพยานชิ้นไหนตรวจยึด หรือไม่ตรวจยึด ควรมีการบันทึกการตัดสินใจดังกล่าวไว้ในแฟ้มคดี

พยานหลักฐานทางอิเล็กทรอนิกส์ประกอบด้วยข้อมูลที่สร้างขึ้นหรือข้อมูลที่บันทึกบนอุปกรณ์อิเล็กทรอนิกส์ในหลายวิธี ประเภทข้อมูลทั่วไปที่มักระบุระหว่างการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ประกอบด้วย

- ข้อมูลและเมทาเดตาที่ใช้งานอยู่ (เหล่านี้คือข้อมูลที่ผู้ใช้ปกติของระบบมองเห็นได้ เอกสารนี้เป็นตัวอย่างของ “ข้อมูลที่ใช้งานอยู่”)
- ข้อมูลเมทาเดตาของไฟล์ที่ฝังตัวและข้อมูลเมทาดาตาของไฟล์/ระบบปฏิบัติการ (รวมถึงข้อมูลเกี่ยวกับไฟล์ที่จัดเก็บโดยระบบ และอาจรวมถึงเวลา และวันที่, ตำแหน่ง และหมายเลขประจำเครื่องของฮาร์ดแวร์ และซอฟต์แวร์) เมทาดาตาบางประเภท เช่น DVR สามารถจัดเก็บในลักษณะที่ไม่ได้มาตรฐาน และสามารถเข้าถึงได้ผ่านซอฟต์แวร์ของผู้ผลิต หรือซอฟต์แวร์เฉพาะโดเมนเท่านั้น)
- การสำรองข้อมูล (รวมถึงข้อมูลจากการสำรองข้อมูลที่สำคัญขององค์กรอย่างเป็นทางการ, ข้อมูลโทรศัพท์เคลื่อนที่ หรือข้อมูลคลาวด์[3]

[3] ผู้ตรวจพิสูจน์ต้องมั่นใจว่า ไม่ผิดแนวทาง/กฎหมายของประเทศในการจัดการกับข้อมูลคลาวด์

- ข้อมูลที่ไม่ใช้งาน (ถูกลบ) (โดยทั่วไปรวมถึงข้อมูลที่ผู้ใช้ปกติของระบบมองไม่เห็น แต่สามารถกู้คืนได้โดยใช้ความรู้และเครื่องมือเฉพาะทาง ข้อมูลอาจถูกลบผ่านกิจกรรมของผู้ใช้ หรือโดยอัตโนมัติ (ระบบ)
- ข้อมูลระเหย (เป็นข้อมูลที่หายไป เมื่อปิดเครื่องคอมพิวเตอร์ ตัวอย่างที่พบบ่อยที่สุดของข้อมูลระเหย คือ ข้อมูลที่เก็บไว้ในหน่วยความจำระบบ) และ
- ข้อมูลโทรคมนาคม (รวมถึงข้อมูลจราจรของเครือข่ายที่ส่งและรับ ซึ่งเป็นส่วนหนึ่งของการเชื่อมต่อของระบบอินเตอร์เน็ตหรืออินทราเน็ต)

อุปกรณ์อิเล็กทรอนิกส์ทั่วไปที่สามารถเป็นพยานหลักฐานดิจิทัล ได้แก่ คอมพิวเตอร์, คอมพิวเตอร์แบบพกพา, โทรศัพท์เคลื่อนที่, ข้อมูลแอปพลิเคชันมือถือ, ข้อมูลคลาวด์, ข้อมูลเครือข่าย, ระบบองค์กร, ระบบกล้องวงจรปิด, ระบบยานพาหนะ, โดรน, ระบบนำทางทางทะเล เป็นต้น

การพิจารณาลักษณะของข้อมูลประเภทต่าง ๆ มีความสำคัญ เนื่องจากสิ่งเหล่านี้ก่อให้เกิดความท้าทายที่แตกต่างกันในแง่ของการแปลผลข้อมูล, การสกัดข้อมูล, บันทึกผลการตรวจพิสูจน์, การเตรียมการเพื่อนำเสนอคุณค่าของพยานหลักฐาน, การเก็บรักษาและการจัดเก็บวัตถุพยาน, การนำเสนอในชั้นศาล เป็นต้น นอกจากนี้ ควรมีการวางแผนอย่างรอบคอบ เพื่อทำให้แน่ใจว่า มีการจัดเก็บข้อมูลที่สามารถสูญหายได้ก่อนการปิดระบบ หรือการเชื่อมต่อกับระบบที่ใช้งานอยู่เพื่อเก็บรวบรวมข้อมูล (การแยกโทรคมนาคมแบบไร้สาย)

ในระหว่างการรวบรวมและประมวลผลอุปกรณ์อิเล็กทรอนิกส์ เป็นเรื่องปกติที่จะพบข้อมูลที่อาจได้รับการคุ้มครองหรือได้รับสิทธิ์พิเศษทางใดทางหนึ่ง (เช่น ภายใต้ สิทธิพิเศษของทนายความ, สิทธิพิเศษทางวิชาชีพตามกฎหมาย หรือเกี่ยวข้องกับรัฐสภา/รัฐบาล) สิ่งอำนวยความสะดวกควรมีกระบวนการเพื่อให้สามารถจัดการวัสดุดังกล่าวได้อย่างปลอดภัย รวมถึงจำกัดเฉพาะสมาชิกที่จำเป็นต้องรู้เท่านั้น

ผลกระทบทางการเงินของการจัดการพยานหลักฐานทางอิเล็กทรอนิกส์ สำหรับผู้ให้บริการทางนิติวิทยาศาสตร์และผู้รับบริการ (เช่น เหยื่อ, ผู้ต้องหา, บุคคลที่สาม เป็นต้น) เป็นข้อพิจารณาที่สำคัญ เนื่องจากอาจจำกัดคุณภาพ ขอบเขต และมูลค่าของวัตถุพยานต่อกระบวนการยุติธรรมทางอาญา

ฮาร์ดแวร์และซอฟต์แวร์ที่ออกแบบมาเพื่อจัดการกับข้อมูลที่ซับซ้อนที่พบในอุปกรณ์อิเล็กทรอนิกส์ และระบบขององค์กรเพิ่มขึ้น เนื่องจากเครื่องมือเหล่านี้มีวัตถุประสงค์เพื่อจัดการกับข้อมูลที่เพิ่มขึ้นอย่างทวีคูณ และจำเป็นอย่างยิ่งที่เครื่องมือที่ใช้จะต้องคำนึงถึงแง่มุมที่เป็นลักษณะเฉพาะของนิติวิทยาศาสตร์ เครื่องมือใดก็ตามที่นำมาใช้ ทั้งแบบที่ไม่เสียค่าใช้จ่ายและแบบที่เสียค่าใช้จ่ายควรได้รับการตรวจสอบก่อนนำมาใช้งาน เพื่อทำให้มั่นใจว่า เป็นไปตามข้อกำหนดทางนิติวิทยาศาสตร์ทั้งหมดที่กำหนดไว้ในห้องปฏิบัติการ

กระบวนการรวบรวมวัตถุพยานต้องได้รับการออกแบบเพื่อพิจารณาความท้าทายที่ต้องเผชิญกับเทคโนโลยีสารสนเทศ และควรพิจารณาประเด็น ดังต่อไปนี้

- ระบุสิ่งที่กำลังมองหา (ก่อนเริ่มการตรวจพิสูจน์)
- การตรวจยึดและการมีอยู่ของอุปกรณ์อิเล็กทรอนิกส์เป็นไปตามข้อกำหนดทางกฎหมาย (เช่น เงื่อนไขของหมายค้น)

- ลดการหยุดการดำเนินงาน โดยเฉพาะอย่างยิ่งกับบุคคลที่สามหรือสิ่งอำนวยความสะดวกในการจัดเก็บข้อมูล
- ลดผลกระทบทางการเงิน ซึ่งรวมถึงการระบุ และกำจัดแหล่งข้อมูลภายนอกในที่เกิดเหตุ เพื่อป้องกันการรวบรวมและจัดเก็บข้อมูลที่ไม่จำเป็น
- ใช้ระบบและเครือข่ายผู้ตรวจพิสูจน์ที่เชี่ยวชาญแยกต่างหากในการจัดเก็บและตรวจพิสูจน์วัตถุพยาน
- ปฏิบัติตามขั้นตอนการทำงานและกระบวนการที่จัดทำขึ้นโดยห้องปฏิบัติการ และ
- เก็บบันทึกการรวบรวมวัตถุพยาน ประมวลผล และการตัดสินใจที่สำคัญ

3.2 การตรวจพิสูจน์

เมื่อพิจารณาความเกี่ยวข้องและคุณค่าที่เป็นไปได้ของข้อมูลที่แสดงหรือจัดเก็บอยู่ในอุปกรณ์ หรือบริบทในการจัดเก็บ กระบวนการสกัดข้อมูลจะออกแบบให้สามารถเก็บข้อมูลจากวัตถุพยานมากที่สุด ควรพิจารณาข้อควรระวังเกี่ยวกับปริมาณข้อมูล, การเก็บรักษาข้อมูล, ความเสี่ยงที่ข้อมูลจะสูญหาย และ/หรือความเสี่ยงประเด็นคำถามที่อาจขึ้นกับทุกฝ่ายที่ได้รับผลกระทบจากการสกัดข้อมูล

3.3 การแปลผล

3.3.1 การจัดเรียงผลการตรวจพิสูจน์

ในการพิจารณาข้อกำหนดเฉพาะของการพิจารณาคดีในชั้นศาลที่เกี่ยวข้องกับขอบเขตอำนาจศาลที่ดำเนินการตรวจสอบรายงานผลการตรวจพิสูจน์, การรายงานสิ่งที่พบ เช่น ศาลต้องมีการวางแผนอย่างรอบคอบ เนื่องจากวิธีการรายงานแบบดั้งเดิมมักจะไม่สามารถทำได้ เมื่อมีการนำเสนอพยานหลักฐานทางอิเล็กทรอนิกส์

3.3.1.1 การจัดระเบียบ

ลักษณะของข้อมูลที่มีอยู่ในอุปกรณ์อิเล็กทรอนิกส์อาจดูเหมือนไม่มีการจัดระเบียบ เนื่องจากอัลกอริธึมในการจัดเก็บข้อมูลที่แตกต่างกัน เกือบทุกครั้งจะได้รับและวิเคราะห์ข้อมูลที่นำเสนอในชั้นศาลที่ต่างจากข้อมูลดิบ การจัดระเบียบข้อมูลดังกล่าว ควรสร้างข้อมูลที่ชัดเจนและรัดกุม โดยไม่เปลี่ยนแปลงลักษณะหรือผลกระทบต่อเมทาดาตา

3.3.1.2 การลดปริมาณข้อมูล และการกรองข้อมูล

ด้วยขนาดอุปกรณ์จัดเก็บข้อมูลที่เพิ่มขึ้น และจำนวนไฟล์ในระบบทั่วไป จึงเป็นไปไม่ได้ที่ผู้ตรวจพิสูจน์จะสามารถมองหาทุกสิ่งในอุปกรณ์ได้ ด้วยเหตุนี้ การใช้คำค้น, ข้อความค้นหา และลายเซ็นของไฟล์ (file signatures) จึงมีความสำคัญอย่างยิ่งในการลดปริมาณข้อมูลให้อยู่ในระดับที่สามารถบริหารจัดการได้ วิธีการลดข้อมูลดังกล่าวควรใช้โดยคำนึงถึงเป้าหมายของการสืบสวนสอบสวนเสมอ และควรบันทึกเป็นการตัดสินใจที่สำคัญ เพื่อให้บุคคลที่สามสามารถตรวจพิสูจน์ซ้ำในลักษณะเดียวกันได้ แม้จะได้วิธีการลดข้อมูล แต่คุณภาพของข้อมูลที่ได้รับจากระบบขององค์กรมักจะอยู่นอกเหนือความสามารถของผู้ให้บริการทางด้านนิติวิทยาศาสตร์ที่พัฒนามากที่สุด และต้องมีการพิจารณาและเปิดเผยเป็นพิเศษ

3.3.1.3 รูปแบบ

เมื่อมีการสร้างรายงานผลการตรวจพิสูจน์ ควรคำนึงถึงกลุ่มเป้าหมาย และด้วยเหตุนี้จึงควรนำเสนอข้อมูลในรูปแบบที่สามารถอ่านและทำความเข้าใจได้ง่าย หากไม่สามารถทำได้ อาจมีความเสี่ยงที่ข้อมูลสำคัญจะหายหรือตีความผิดพลาด เมื่อแปลงข้อมูลเพื่อเพิ่มความสามารถในการอ่าน ควรคงไว้ซึ่งลิงก์ไปยังแหล่งข้อมูลต้นฉบับที่ไม่ได้เปลี่ยนแปลงแหล่งที่มาของข้อมูล เพื่อสามารถสอบย้อนกลับได้

ตัวอย่างทั่วไปของสิ่งนี้ คือ “ประวัติเหตุการณ์” เมื่อนำเสนอข้อมูลโทรคมนาคม เช่น บันทึกการโทรที่พบในอุปกรณ์มือถือ หากไม่มีการนำเสนอหลักฐานตามลำดับเวลา อาจทำให้เกิดความสับสน

3.3.1.4 การทบทวน

การตรวจพิสูจน์ข้อมูลที่สกัดจากอุปกรณ์อิเล็กทรอนิกส์มักต้องมีการตรวจสอบข้อมูลดิบอย่างครอบคลุมร่วมกับเจ้าหน้าที่สืบสวนสอบสวน, ผู้รับบริการ, เจ้าหน้าที่ตามกฎหมาย ในระหว่างการประชุมก่อนการพิจารณาคดี เพื่อพิจารณาความเกี่ยวข้องและป้องกันการรวบรวมข้อมูลที่ไม่เกี่ยวข้อง และปล่อยประเภทข้อมูลที่ได้รับการคุ้มครอง การทบทวนรายงานผลการตรวจพิสูจน์โดยผู้รู้เสมอกันควรเป็นส่วนหนึ่งในกระบวนการตรวจพิสูจน์ ซึ่งควรนำเข้าระบบคุณภาพของห้องปฏิบัติการ และช่วยทำให้มั่นใจว่า รายงานผลการตรวจพิสูจน์มีข้อมูลที่เหมาะสม

3.3.2 การเก็บรักษาวัตถุพยาน

ผู้ตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์มีหน้าที่ในการรักษาวัตถุพยาน เพื่อป้องกันการสูญหาย และการทำลายข้อมูล และควรปฏิบัติหน้าที่ ดังนี้

- รักษาไว้ซึ่งห่วงโซ่วัตถุพยาน และควบคุมข้อมูลที่สกัดได้จากแหล่งที่มาของวัตถุพยาน
- มีสถานที่เฉพาะสำหรับเก็บรักษาพยานหลักฐานดิจิทัล รวมถึงรายละเอียดในการสำรองข้อมูล และการกู้คืนข้อมูลจากภัยพิบัติ
- จัดทำเอกสารที่เกี่ยวข้องกับการเก็บรักษาวัตถุพยาน
- ประเมินปัญหา ปริมาณข้อมูล และความจำเพาะ/ขอบข่ายที่ร้องขอ
- หากเป็นไปได้ ควรจำกัดการเก็บรวมรวมข้อมูลเฉพาะคำค้น, วันที่, ชื่อไฟล์ เป็นต้น
- สกัดข้อมูลลงในโฟลเดอร์ที่กำหนด และใช้ฟังก์ชันการเข้ารหัสค่าความจำเพาะของข้อมูล เพื่อทำให้มั่นใจว่าข้อมูลมีความสมบูรณ์ทุกครั้งที่มีการถ่ายโอนข้อมูล
- มีส่วนร่วมในการสืบสวนสอบสวน เพื่อทำให้มั่นใจว่าการร้องขอจะไม่ส่งผลให้เกิดการยึดวัตถุพยานที่มีข้อมูลปริมาณมากและยุ่งยาก

3.3.3 การแปลผลการตรวจพิสูจน์มัลติมีเดีย

ซอฟต์แวร์ประมวลผลสัญญาณสามารถนำมาประยุกต์ใช้เพื่อปรับปรุงวัตถุพยานประเภทเสียงและภาพเคลื่อนไหว ทั้งนี้เพื่อวัตถุประสงค์ในการสืบสวนสอบสวน โดยเฉพาะอย่างยิ่งวัตถุพยานประเภทเสียงและภาพเคลื่อนไหวที่มีการบันทึกภายใต้สภาพแวดล้อมที่ไม่เหมาะสม โดยปกติจะแนะนำให้ประมวลผลโดยการดึงข้อมูลจากวัตถุพยานต้นฉบับ เพื่อไม่ให้ข้อมูลใด ๆ สูญหาย กรณีที่ไม่สามารถทำได้ อาจยอมรับในการทำงานบนสื่อที่แปลงมาแล้ว หากกระบวนการแปลงนั้นสมเหตุสมผล และเปิดเผยทั้งหมด

การเลือกเทคนิคการประมวลผลสัญญาณ เช่น การกรอง ขึ้นอยู่กับการวิเคราะห์สัญญาณ สัญญาณรบกวน และลักษณะความผิดเพี้ยนของการบันทึกเสียงและภาพเคลื่อนไหว หากมีการนำเสนอวัตถุพยานที่มีการแปลงในชั้นศาล ผู้ตรวจพิสูจน์ต้องอธิบายวิธีการประมวลผลสัญญาณและข้อจำกัดของวิธีการนั้น โดยทั่วไปผู้ตรวจพิสูจน์ทางด้านมัลติมีเดียจะไม่แปลผลคำพูดหรือเนื้อหาในภาพเคลื่อนไหว เว้นแต่จะสามารถแสดงเห็นถึงความสามารถในการใช้วิธีการที่มีการตรวจสอบความใช้ได้ของวิธีที่เพียงพอสำหรับสถานการณ์เฉพาะกรณี และเข้าใจข้อจำกัด และสมมติฐานที่เกี่ยวข้องกับวิธีการนั้น

ในทำนองเดียวกัน การแปลผลเกี่ยวกับที่มาของการบันทึกเสียงหรือการบันทึกภาพเคลื่อนไหว หรือกิจกรรมที่เกี่ยวข้องกับการผลิตการบันทึก ควรนำเสนอเฉพาะในกรณีที่ผู้ตรวจพิสูจน์สามารถแสดงให้เห็นถึงความสามารถในการประยุกต์ใช้วิธีการที่เกี่ยวข้องและวิธีการตรวจสอบความใช้ได้ที่เพียงพอ

3.3.4 ความท้าทาย

ผู้ตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์อาจประสบกับความท้าทาย ดังต่อไปนี้

- การสุ่มตัวอย่างจากการเก็บรวบรวมข้อมูล ที่ห้ามไม่ให้เก็บรวบรวมข้อมูลทั้งหมด หรือเป็นไปไม่ได้ที่จะได้ข้อมูลทั้งหมด
- ความต้องการในการตามให้ทันแหล่งข้อมูลที่ซับซ้อนที่เพิ่มขึ้น
- การใช้งานแบบเข้ารหัสที่เพิ่มขึ้น
- ข้อผูกพันในการใช้ระบบการตรวจพิสูจน์ขององค์กรเพื่อดูข้อมูล
- ข้อผูกพันในการรวมระบบการตรวจพิสูจน์ขององค์กรเพื่อประมวลผลหลายระบบ
- การที่ผู้ตรวจพิสูจน์พยานหลักฐานดิจิทัลเปิดเผยการละเมิดข้อมูลและภาพดิจิทัล ตามที่ระบุโดยทั่วไปในการแสวงหาผลประโยชน์จากเด็ก และการสืบสวนสอบสวนด้านการต่อต้านการก่อการร้าย และ
- ความจำเป็นในการเข้าถึงวัตถุพยานประเภทคลาวด์ (อำนาจทางกฎหมายในการเข้าถึงข้อมูลระยะไกล)

3.4 การรายงานผลการตรวจพิสูจน์

ผู้จัดการห้องปฏิบัติการควรทำให้มั่นใจว่า รายงานหรือข้อความใด ๆ[4] ที่จัดทำโดยผู้ตรวจพิสูจน์ประกอบด้วยข้อมูลต่อไปนี้เป็นอย่างน้อย

- หมายเลขคดีหรือหมายเลขอ้างอิง
- ชื่อ-นามสกุลและตำแหน่งของผู้ตรวจพิสูจน์
- รายละเอียดของข้อมูลที่เกี่ยวข้อง และเอกสารอ้างอิงใด ๆ
- ข้อจำกัดใด ๆ ในการตรวจพิสูจน์ (ไม่ว่าจะกำหนดโดยผู้ตรวจพิสูจน์หรือเจ้าหน้าที่สืบสวนสอบสวน) และข้อสันนิษฐานใด ๆ ของผู้ตรวจพิสูจน์ที่ได้จากผลการตรวจพิสูจน์
- การกำหนดระเบียบปฏิบัติงานและการดำเนินการโดยผู้ตรวจพิสูจน์ รวมถึงสิ่งที่พบที่เกี่ยวข้อง

[4] ILAC G19:2014 S4.9

- การอธิบายและการระบุข้อเท็จจริงที่เกี่ยวกับวัตถุพยานที่ชัดเจน เมื่อเทียบกับวัตถุพยานที่แสดงความคิดเห็น ผู้ตรวจพิสูจน์ได้รับอนุญาตให้ทำได้
- อ้างถึงห่วงโซ่วัตถุพยานสำหรับวัตถุพยานใด ๆ ที่อ้างอิงในรายงานหรือข้อความ และ
- บันทึกกิจกรรมใด ๆ ที่เกี่ยวข้อง หรือวัตถุพยานต้นฉบับที่แนบมากับรายงานหรือข้อความ (ไม่ว่าจะอยู่ในรูปแบบกระดาษหรือดิจิทัล) ควรมีการระบุ หรือให้บริการตามความต้องการ

3.5 ฐานข้อมูล

เพื่อลดการเปิดดูเนื้อหาภาพที่ไม่เหมาะสม (ซึ่งอาจส่งผลทำให้เกิดความเครียด และส่งผลต่อสุขภาพจิต) แนะนำให้ใช้ฐานข้อมูลค่าความจำเพาะของข้อมูล

โดยฐานข้อมูลค่าความจำเพาะของข้อมูลนี้สามารถสร้างและคงไว้ซึ่งขอบเขตอำนาจของศาลและหน่วยงานแต่ละแห่ง อย่างไรก็ตาม ควรพิจารณาฐานข้อมูลที่มีอยู่ทั่วไป เช่น ฐานข้อมูลที่เผยแพร่โดย Interpol และ Project VIC

ฐานข้อมูลค่าความจำเพาะของข้อมูลไม่ควรใช้ในการระบุและประมวลผลไฟล์เพียงอย่างเดียว เนื่องจากความผิดพลาดของมนุษย์อาจส่งผลให้การจัดประเภทไม่ถูกต้อง หรือการจำแนกประเภทอาจแตกต่างกันระหว่างขอบเขตอำนาจของศาล

4 ระเบียบปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และการตรวจสอบความใช้ได้

4.1 ระเบียบปฏิบัติงาน และขั้นตอนการปฏิบัติงาน

การพัฒนาขั้นตอนการปฏิบัติงานโดยผู้ให้บริการทางด้านนิติวิทยาศาสตร์ที่รับผิดชอบงานด้านการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ควรมีจุดมุ่งหมายเพื่อให้มั่นใจว่า ขั้นตอนการปฏิบัติงานมีความเกี่ยวข้องและคำนึงถึงลักษณะการพัฒนาของเทคโนโลยีสารสนเทศที่มุ่งเป้าไปที่สิ่งเหล่านี้

- การสื่อสารที่เหมาะสมระหว่างผู้มีส่วนได้ส่วนเสียในการสืบสวนสอบสวน ซึ่งเป็นสิ่งสำคัญ และทำให้มั่นใจว่า
    - การชี้บ่งและการค้นพบแหล่งที่มาทั้งหมด
    - หลักฐานที่เก็บไว้มีความเกี่ยวข้อง และ
    - มีการสร้างหลักฐานที่เกี่ยวข้อง

ขั้นตอนการปฏิบัติงานด้านการสื่อสารอาจรวมถึงกระบวนการให้คำปรึกษาแก่ผู้ที่ทำหน้าที่ในการสืบสวนสอบสวน เพื่อช่วยกำหนดประเภทหรือระดับของความช่วยเหลือที่จำเป็น ซึ่งจะช่วยให้ผู้ตรวจพิสูจน์สามารถมุ่งเน้นไปที่ประเด็นที่เกี่ยวข้อง (วันที่/เวลา ประเภทของวัตถุพยาน) และสามารถระบุข้อพิจารณาฉพาะอื่น ๆ ที่อาจส่งผลกระทบต่อกระบวนการหรือวิธี (ยกตัวอย่างเช่น จำเป็นต้องเข้าถึงข้อมูลบนคลาวด์)

ขั้นตอนการปฏิบัติงานที่กำหนดและจัดทำเป็นเอกสารระเบียบปฏิบัติงาน จำเป็นต้องทำให้มั่นใจว่า

- ผู้ตรวจพิสูจน์ต้องเข้าใจและปฏิบัติตามขั้นตอนการปฏิบัติงานที่ใช้เป็นแนวทางในกระบวนการตรวจพิสูจน์
- ผู้ตรวจพิสูจน์ต้องเข้าใจโครงสร้างพื้นฐานที่สนับสนุนกระบวนการตรวจพิสูจน์
- ผู้ตรวจพิสูจน์ต้องเข้าใจและปฏิบัติตามขั้นตอนที่ระบุในระเบียบปฏิบัติงานที่เกี่ยวข้องกับการตรวจพิสูจน์ทั้งหมด
- ผู้ตรวจพิสูจน์ต้องเข้าใจและบันทึกข้อจำกัดของการตรวจพิสูจน์
- ควรพิจารณาความเสี่ยงที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ และระเบียบปฏิบัติงานทั้งหมด ควรคำนึงถึงผลกระทบทางด้านการเงิน การหยุดการทำงานอย่างกะทันหัน การเสื่อมสภาพของวัตถุพยาน อุปสรรคในกระบวนการยุติธรรม และการสูญเสียการควบคุม และกระจายวงกว้างอันเนื่องมาจากการออกคำสั่งการเข้าถึงแบบครอบคลุม ข้อพิจารณาโดยทั่วไป คือ
    - ระบุเอกสารที่เกี่ยวข้อง
    - แจ้งเจ้าของเอกสารหรือผู้ดูแล

- เห็นด้วยกับฝ่ายต่าง ๆ เกี่ยวกับระเบียบปฏิบัติงานด้านการตรวจพิสูจน์ โดยเฉพาะอย่างยิ่ง เมื่อจำเป็นต้องมีการตรวจพิสูจน์ระบบองค์กร
- เก็บรักษาเอกสารที่เกี่ยวข้อง
- กำกับติดตามการปฏิบัติตามการเก็บรักษา และ
- กระบวนการจัดทำเอกสาร

จำเป็นต้องมีขั้นตอนในการจัดการกับพยานหลักฐานทางอิเล็กทรอนิกส์ และส่วนใหญ่ประกอบด้วย

- การรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์
- การจัดเรียงและการจัดระเบียบชุดข้อมูล
- ทบทวนข้อมูลที่สกัดได้ เพื่อกำหนดความเกี่ยวข้อง และ
- สรุปผลการตรวจพิสูจน์และจัดทำรายงานผลการตรวจพิสูจน์

4.2 การตรวจสอบความใช้ได้

เครื่องมือ (แบบเปิดเผยรหัส, แบบไม่มีค่าใช้จ่าย หรือแบบมีค่าใช้จ่าย) ที่ใช้ในกระบวนการตรวจพิสูจน์พยานหลักฐานควรมีการอัปเดตเป็นประจำ เนื่องจากการอัปเดตมักจะมีการปรับปรุงวิธีการที่ใช้หรือลดความเสี่ยงที่เคยเกิดขึ้น หลังการอัปเดตในแต่ละครั้ง ควรมีการประเมินความเหมาะสมโดยการตรวจสอบความใช้ได้ของเครื่องมือ เพื่อทำให้มั่นใจว่าผลการตรวจพิสูจน์มีความน่าเชื่อถือ และข้อผิดพลาดของเครื่องมือที่ใช้ในการตรวจพิสูจน์เป็นที่ทราบและเข้าใจโดยทั่วกัน

เนื่องจากเครื่องมือเชิงพาณิชย์ไม่สามารถจัดการได้กับทุกสถานการณ์เสมอไป จึงเป็นเรื่องปกติที่ผู้ตรวจพิสูจน์ต้องคิดและพัฒนาซอฟต์แวร์แบบใช้ครั้งเดียว (ทั่วไปเรียกว่า “สคริปต์”) เพื่อช่วยในการตรวจพิสูจน์พยานหลักฐาน เครื่องมือดังกล่าวควรทดสอบกับชุดข้อมูลที่ทราบค่า (ถ้ามี) ภายใต้การเปลี่ยนแปลงของพารามิเตอร์ทั้งโดยนัยและชัดเจน ซึ่งกำหนดลักษณะของชุดข้อมูลเฉพาะ เพื่อทำให้มั่นใจว่า เครื่องมือเหล่านี้สามารถทำงานได้อย่างถูกต้อง และสามารถหาข้อมูลหรือหลักฐานใด ๆ ได้ และข้อผิดพลาดของเครื่องมือที่ใช้ในการตรวจพิสูจน์เป็นที่ทราบและเข้าใจโดยทั่วกัน ควรเก็บรักษาบันทึกการทดสอบ

เครื่องป้องกันการเขียนข้อมูลใหม่ แหล่งจ่ายไฟ และสายเคเบิ้ลข้อมูลที่ใช้ในการป้องกันแหล่งข้อมูลที่เป็นหลักฐาน ควรมีการตรวจสอบการใช้งานเป็นประจำ เพื่อให้สามารถทำงานอย่างเหมาะสม เพื่อทำให้มั่นใจว่า ผู้ตรวจพิสูจน์ไม่สามารถเปลี่ยนแปลงแหล่งที่มาของวัตถุพยานโดยไม่ได้ตั้งใจ เหล่านี้เป็นสิ่งสำคัญเมื่อใช้เครื่องป้องกันการเขียนข้อมูลใหม่ หรือเครื่องมือที่มีอยู่แล้ว ได้รับการอัพเกรด (ไม่ว่าจะเป็นอัพเกรดซอฟต์แวร์ หรืออัพเกรดเฟิร์มแวร์) บันทึกที่แสดงการทำงานที่ถูกต้องของเครื่องป้องกันการเขียนข้อมูลใหม่ควรเก็บรักษาไว้เผื่อกรณีจำเป็นต้องใช้ในชั้นศาล หรือใช้ในกระบวนการตรวจสอบ

5 การบริหารจัดการด้านคุณภาพ

การบริหารจัดการด้านคุณภาพเป็นกระบวนการที่ใช้ในการตรวจสอบความถูกต้องของผู้ตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ การบริหารจัดการด้านคุณภาพควรนำมาใช้ในแต่ละกระบวนการตรวจพิสูจน์ ไม่ควรตรวจสอบแค่กระบวนการสุดท้าย และกระบวนการทั้งหมดสามารถสะท้อนความพยายามในการปรับปรุงอย่างต่อเนื่อง

พยานหลักฐานทางอิเล็กทรอนิกส์มีความแตกต่างจากนิติวิทยาศาสตร์ดั้งเดิมตรงที่เขตอำนาจศาลและสิ่งอำนวยความสะดวกจำนวนมากไม่ได้แสวงหาหรือธำรงรักษาไว้ซึ่งการรับรองระบบคุณภาพ เช่น ระบบ ISO/IEC 17020 หรือระบบ ISO/IEC 17025 แม้ว่าจะไม่ได้รับการรับรองทั้งระบบ แต่ควรคำนึงถึงการนำมาตรฐานสากลมาประยุกต์ใช้บางส่วนที่สามารถช่วยปรับปรุงคุณภาพสำหรับงานในห้องปฏิบัติการ อย่างน้อยที่สุด สิ่งอำนวยความสะดวกควรปฏิบัติตาม ILAC G19:2014

ผู้ตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ควรมีรายการตรวจสอบการดำเนินการที่สำคัญเพื่อกำกับติดตาม (ยกตัวอย่างเช่น รายละเอียดวัตถุพยาน, เทคนิค/กระบวนการ, ซอฟต์แวร์/ฮาร์ดแวร์ที่ใช้) เป็นอย่างน้อย ขณะกำลังดำเนินการ ณ สถานที่เกิดเหตุ และการได้มาซึ่งวัตถุพยาน เพื่อช่วยคงไว้ซึ่งความสมบูรณ์ของวัตถุพยาน และการบริหารจัดการวัตถุพยาน (หรือห่วงโซ่วัตถุพยาน)

สิ่งอำนวยความสะดวกควรมีการธำรงรักษาและปฏิบัติตามระเบียบปฏิบัติงานที่เกี่ยวกับการเก็บรักษาเอกสารซึ่งระบุไว้เฉพาะดังรายการต่อไปนี้

- การทดสอบความชำนาญของห้องปฏิบัติการ
- ความสามารถของผู้ปฏิบัติงาน
- การตรวจสอบความใช้ได้ของผลการตรวจพิสูจน์โดยใช้ชุดข้อมูลที่ทราบค่า
- การรับตัวอย่าง และกรบันทึกการดำเนินงาน
- การเก็บรักษาข้อมูล
- การปฏิบัติการแก้ไข
- การตรวจติดตาม
- ประวัติการฝึกอบรม
- การพัฒนาวิชาชีพอย่างต่อเนื่อง และ
- การเป็นพยานศาล

โปรแกรมการบริหารจัดการด้านคุณภาพควรระบุและจัดทำเป็นเอกสารที่แสดงให้เห็นอำนาจ หน้าที่ ความรับผิดชอบ และความสัมพันธ์ของบุคลากรทั้งหมดในด้านการบริหาร การปฏิบัติ หรือการทวนสอบงานที่ส่งผลต่อความถูกต้องในการสืบสวนสอบสวนทางดิจิทัล

ควรพิจารณาใช้ชุดทดสอบความชำนาญที่ได้รับการรับรองเพื่อนำมาใช้ตรวจสอบความใช้ได้ของระเบียบปฏิบัติงาน ห้องปฏิบัติการและผู้ปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล ชุดทดสอบความชำนาญเหล่านี้ (ถ้ามี) ควรครอบคลุมหัวข้อต่าง ๆ ตั้งแต่ทักษะทั่วไปในการจัดการพยานหลักฐานดิจิทัลจนถึงทักษะเฉพาะในสาขาการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ควรทราบและรายงานข้อผิดพลาดในทุกขั้นตอนในกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

หากไม่มีชุดทดสอบความชำนาญที่ได้รับการรับรอง ควรมีการทำแบบทดสอบร่วมกันระหว่างห้องปฏิบัติการที่มีการทำงานในลักษณะเดียวกัน วัตถุประสงค์หลักของสิ่งเหล่านี้ เพื่อแสดงให้เห็นว่า กระบวนการตรวจพิสูจน์ของห้องปฏิบัติการมีความสม่ำเสมอและมีความถูกต้องในการดำเนินงานโดยใช้ข้อมูลจริงที่ทราบค่า เป็นการตรวจสอบวิธีตรวจพิสูจน์ของห้องปฏิบัติการ ไม่ได้เป็นการตรวจสอบผู้ปฏิบัติงานเป็นรายบุคคล

6 อภิธานศัพท์

อภิธานศัพท์ต่อไปนี้ ไม่ถือเป็นคำศัพท์เฉพาะทางด้านดิจิทัลและมัลติมีเดีย แต่เป็นคำศัพท์ที่ใช้กันอย่างแพร่หลายในสาขานิติวิทยาศาสตร์

DVD	แผ่นดิจิทัลอเนกประสงค์
USB	บัสอนุกรมแบบใช้ร่วม
พยานหลักฐานทางอิเล็กทรอนิกส์	ข้อมูลใด ๆ ที่จัดเก็บหรือส่งต่อในรูปแบบดิจิทัลหรือแอนาล็อกที่เกี่ยวข้องกับการสืบสวนสอบสวน หรือการพิจารณาในชั้นศาล
พยานหลักฐานดิจิทัล	พยานหลักฐานดิจิทัลมักใช้แทนกันได้กับคำว่าพยานหลักฐานทางอิเล็กทรอนิกส์ แต่จะใช้อ้างถึงเฉพาะข้อมูลที่จัดเก็บหรือส่งต่อในรูปแบบดิจิทัลที่เกี่ยวข้องกับการสืบสวนสอบสวนหรือการพิจารณาในชั้นศาล
พยานหลักฐานมัลติมีเดีย	พยานหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการบันทึกเสียง การบันทึกภาพเคลื่อนไหวและภาพนิ่ง

สมาชิก IFSA

พันธมิตรเชิงกลยุทธ์

ติดต่อ:

International Forensic Strategic Alliance: http://www.ifsa-forensics.org