ร่าง

คู่มือมาตรฐานการตรวจพิสูจน์ พยานหลักฐานดิจิทัลและมัลติมีเดีย

ตามแนวทางของ IFSA

เสนอโดย: กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์

กองตรวจพิสูจน์ทางวิทยาศาสตร์ สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม

กุมภาพันธ์ 2565

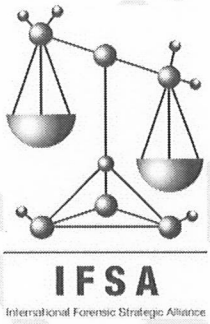
ข้อกำหนดขั้นต่ำสำหรับหลักฐานดิจิทัลและมัลติมีเดีย

INTERNATIONAL FORENSIC STRATEGIC ALLIANCE

MINIMUM REQUIREMENTS FOR DIGITAL AND MULTIMEDIA EVIDENCE

A document for emerging laboratories

IFSA MRD 4



สารบัญ

คำแนะนำ	4
คำนำ	5
1 ความสามารถของบุคลากร	7
2 อุปกรณ์และวัสดุสิ้นเปลือง	10
3 การรวบรวม การวิเคราะห์ การตีความ และการรายงาน	12
4 ขั้นตอน โปรโตคอล และการตรวจสอบ	19
5 การจัดการคุณภาพ	21
6 อภิธานศัพท์	22

การแนะนำ

International Forensic Strategic Alliance (IFSA) ได้พัฒนาเอกสารนี้เป็นข้อกำหนดขั้นต่ำซึ่งจะช่วยให้ผู้ให้บริการด้านนิติวิทยาศาสตร์ที่เกิดขึ้นใหม่ในประเทศกำลังพัฒนาสามารถให้บริการทางวิทยาศาสตร์แก่ระบบยุติธรรมทางอาญาได้

วัตถุประสงค์ของเอกสารนี้คือเพื่อสร้างพื้นฐานหรือจุดเริ่มต้นที่ต้องปฏิบัติตามเพื่อให้ได้ผลลัพธ์ที่เชื่อถือได้ ผู้ให้บริการด้านนิติวิทยาศาสตร์ควรสร้างบนพื้นฐานนี้และพยายามปรับปรุงคุณภาพของบริการที่มีให้อย่างต่อเนื่อง

เอกสารนี้อธิบายข้อกำหนดขั้นต่ำสำหรับการสืบสวนที่เกิดเหตุ มันกล่าวถึงกรอบการทำงานต่อไปนี้:

1. ความสามารถของบุคลากร
2. อุปกรณ์และวัสดุสิ้นเปลือง
3. การรวบรวม การวิเคราะห์ การตีความ การรายงาน
4. ขั้นตอน โปรโตคอล การตรวจสอบ
5. การจัดการคุณภาพ

คำนำ

International Forensic Strategic Alliance (IFSA) เป็นความร่วมมือพหุภาคีระหว่างเครือข่ายห้องปฏิบัติการทางนิติวิทยาศาสตร์ระดับภูมิภาคทั้งหกเครือข่าย:

- ผู้อำนวยการห้องปฏิบัติการอาชญากรรมแห่งอเมริกา (ASCLD)
- เครือข่ายสถาบันนิติวิทยาศาสตร์แห่งยุโรป (ENFSI)
- สถาบันนิติวิทยาศาสตร์แห่งชาติออสเตรเลีย นิวซีแลนด์ (NIFS ANZ)
- la Academia Iberoamericana de Criminalística และ Estudios Forenses (AICEF)
- เครือข่ายนิติวิทยาศาสตร์แห่งเอเชีย (AFSN)
- เครือข่ายนิติวิทยาศาสตร์ภูมิภาคแอฟริกาใต้ (SARFS)

IFSA ทำงานอย่างใกล้ชิดกับพันธมิตรเชิงกลยุทธ์ทั้งสามราย ได้แก่ Leverhulme Research Center for Forensic Science, สำนักงานยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (UNODC) และ INTERPOL

IFSA ตระหนักถึงความสำคัญของกรอบการจัดการคุณภาพในห้องปฏิบัติการนิติวิทยาศาสตร์เพื่อให้มีคุณภาพและผลลัพธ์ที่ได้มาตรฐาน ไม่ว่าจะเป็นขั้นตอนการปฏิบัติงานในภาคสนามหรือในห้องปฏิบัติการ

ในเดือนกุมภาพันธ์ 2555 ในการประชุมพิเศษของ IFSA ซึ่งจัดโดย UNODC และได้ประชุมกันในกรุงเวียนนาเพื่อหารือเกี่ยวกับความต้องการของห้องปฏิบัติการนิติวิทยาศาสตร์ที่เกิดขึ้นใหม่ในประเทศกำลังพัฒนา ได้มีการตัดสินใจสร้างชุดเอกสารข้อกำหนดขั้นต่ำ (MRD) เติมช่องว่างในคำแนะนำที่มีอยู่ สำหรับการจัดการปัจจุบันของห้องปฏิบัติการเหล่านี้

ในเดือนตุลาคม 2014 มีการสร้างเอกสารชุดแรกสามชุดเกี่ยวกับการระบุตัวยาที่ถูกยึด การวิเคราะห์ดีเอ็นเอ และการสืบสวนที่เกิดเหตุ เอกสารเหล่านี้ได้เน้นที่ด้านคุณภาพที่สำคัญ โดยใช้คำศัพท์และภาพประกอบที่เรียบง่าย ขณะนี้ MRD ทั้งสามได้รับการอัปเดตและตรวจสอบเพิ่มเติมด้วยเวอร์ชัน 2 ของเอกสารเหล่านี้ที่เผยแพร่ในเดือนธันวาคม 2020 ในขณะที่เขียน MRD เพิ่มเติมอีกสามรายการในพื้นที่ของ ขณะนี้อยู่ระหว่างการพัฒนาหลักฐานทางดิจิทัลและสื่อ การตรวจสอบเอกสาร และการวิเคราะห์ลายนิ้วมือแฝง มีการสร้างเอกสารอภิธานศัพท์แยกต่างหากเพื่อแนะนำผู้ใช้ผ่านแนวคิดที่สำคัญของเอกสารนี้

MRDs เหล่านี้มีขึ้นเพื่อใช้เป็นแนวทางในการเริ่มต้นสำหรับห้องปฏิบัติการนิติวิทยาศาสตร์ที่เกิดขึ้นใหม่ เพื่อสร้างระบบการจัดการคุณภาพและความสามารถทางวิทยาศาสตร์/ทางเทคนิคอย่างรวดเร็ว เมื่อทำได้สำเร็จแล้ว ห้องปฏิบัติการควรสร้างต่อไปบนพื้นฐานนี้และพยายามปรับปรุงคุณภาพการบริการอย่างต่อเนื่องโดยได้รับการรับรองตามมาตรฐานที่กำหนดไว้

ในการร่างเอกสารเหล่านี้ คณะทำงานด้านวิทยาศาสตร์และผู้เชี่ยวชาญจากเครือข่ายนิติวิทยาศาสตร์ระดับภูมิภาคทั้งหกแห่ง ตลอดจนพันธมิตรเชิงกลยุทธ์ของ IFSA ได้มีส่วนสนับสนุนอันมีค่าในระหว่างการปรึกษาหารือรอบต่างๆ MRDs สุดท้ายที่นำเสนอในชุดนี้จะเป็นไปไม่ได้หากไม่มีการมีส่วนร่วมของทุกคน

เป็นความหวังของ IFSA ที่เอกสารเหล่านี้จะมีบทบาทสำคัญในการก้าวไปสู่การสร้างบริการด้านนิติวิทยาศาสตร์ที่มีคุณภาพ

คณะกรรมการ IFSA

กันยายน 2564

1. ความสามารถของบุคลากร

เจ้าหน้าที่ห้องปฏิบัติการทุกคนต้องมีความเข้าใจที่ชัดเจนเกี่ยวกับหน้าที่และความรับผิดชอบของพวกเขา และควรปฏิบัติตามสิ่งเหล่านี้ตลอดเวลาตามหลักจรรยาบรรณ (ดูตัวอย่างในเชิงอรรถด้านล่าง) ที่ห้องปฏิบัติการนำมาใช้

ส่วนนี้แนะนำการศึกษาขั้นต่ำและการฝึกอบรมที่จำเป็นสำหรับเจ้าหน้าที่ห้องปฏิบัติการเพื่อทำการวิเคราะห์หลักฐานดิจิทัลและมัลติมีเดีย

1.1 การศึกษา

ความเชี่ยวชาญพิเศษทางนิติวิทยาศาสตร์นี้มักจะซับซ้อนเนื่องจากข้อกำหนดด้านการศึกษาไม่ใช่แบบดั้งเดิมและไม่มีการพัฒนาหลักสูตรการฝึกอบรมที่ชัดเจน ความต้องการที่พัฒนาขึ้นสำหรับการตรวจสอบ การแยก การตีความ และการเก็บรักษาหลักฐานดิจิทัล กำหนดทักษะที่ซับซ้อนและหลากหลายอย่างมาก ไม่เพียงแต่ในนิติวิทยาศาสตร์แบบดั้งเดิมเท่านั้น แต่ยังพบได้ทั่วไปในอุตสาหกรรมอื่นๆ นอกระบบยุติธรรมทางอาญา เช่น การธนาคาร มัลติมีเดีย โทรคมนาคม ฯลฯ

ซึ่งมักจะทำให้การพัฒนาหลักสูตรการฝึกอบรมขั้นต่ำเป็นเอกพจน์สำหรับผู้ประกอบวิชาชีพนิติวิทยาศาสตร์ที่รับผิดชอบในการตรวจสอบหลักฐานทางดิจิทัลมีความซับซ้อน ผู้เชี่ยวชาญสามารถทำงานได้อย่างสะดวกสบายเท่าเทียมกัน (เช่น) ในฐานะผู้เชี่ยวชาญด้านมัลติมีเดียที่ทำงานในอุตสาหกรรมบันเทิงตลอดจนในสภาพแวดล้อมทางนิติวิทยาศาสตร์

ข้อกำหนดด้านการศึกษาระดับอุดมศึกษาแม้ว่าจะไม่เฉพาะเจาะจงควรขึ้นอยู่กับลักษณะและความซับซ้อนของงานที่ต้องทำ และผู้ปฏิบัติงาน (ผู้ตรวจสอบ / ช่างเทคนิค) ควรสำเร็จการศึกษาระดับมหาวิทยาลัยหรือวุฒิการศึกษาทางเลือกที่เทียบเท่า (เช่น การรับรองระบบที่เป็นกรรมสิทธิ์ในเครือข่าย วิดีโอเสียง การเขียนโปรแกรม ฯลฯ หรือการรับรองที่เน้นหนักไปที่นิติดิจิทัลจากผู้ให้บริการที่ได้รับการรับรอง) โดยเน้นหนักในด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตาม มันยังคงเป็นหน้าที่ของผู้ให้บริการด้านนิติวิทยาศาสตร์ในการแสดงการศึกษาในห้องปฏิบัติการ การฝึกอบรม และประสบการณ์ที่เทียบเท่ากับการตรวจที่ดำเนินการในห้องปฏิบัติการ

ในกรณีที่ไม่มีโปรแกรมการฝึกอบรมอย่างเป็นทางการ การดูแลรักษาและพัฒนาชุดทักษะของผู้ตรวจสอบนิติดิจิทัลที่มีอยู่ถือเป็นสิ่งสำคัญอันดับแรก โอกาสในการศึกษาต่อ (เช่น การเข้าร่วมประชุม การสัมมนาผ่านเว็บ และการทบทวนวรรณกรรมทางวิทยาศาสตร์ที่เกี่ยวข้อง) จะต้องได้รับการแสวงหาอย่างแข็งขันและควรรวมถึงการมีส่วนร่วมกับผู้ปฏิบัติงานที่มีความคิดคล้ายคลึงกันผ่านฟอรัมที่เป็นทางการและไม่เป็นทางการ

ควรพิจารณาใช้การทดสอบความสามารถเชิงพาณิชย์ที่ผ่านการรับรองสำหรับการตรวจสอบความถูกต้องของขั้นตอน ห้องปฏิบัติการ และบุคคลที่ทำการตรวจสอบหลักฐานดิจิทัล การทดสอบความชำนาญเหล่านี้ครอบคลุมหัวข้อต่างๆ ตั้งแต่ทักษะการจัดการหลักฐานดิจิทัลทั่วไปไปจนถึงสาขาย่อยที่เชี่ยวชาญเป็นพิเศษ

นอกเหนือจากทักษะทางเทคนิคที่เกี่ยวข้องกับนิติดิจิทัลแล้ว ผู้ปฏิบัติงานที่ประสบความสำเร็จควรมีการศึกษาเกี่ยวกับ:

• การจัดการสภาพแวดล้อมการสืบสวนที่ซับซ้อน

• การเก็บรักษาและการบันทึกหลักฐาน;

• ทักษะการถ่ายภาพและวีดิทัศน์;

• ระบบการจัดการเคส;

• ทักษะการสื่อสารที่แข็งแกร่ง (ทั้งการเขียนและปากเปล่า) และความสามารถในการถ่ายทอดหัวข้อที่ซับซ้อนด้วยคำศัพท์ง่ายๆ

• ความสามารถในการนำเสนอข้อค้นพบที่เป็นหลักฐานในการพิจารณาคดี (กระบวนการทางกฎหมาย)

ตัวอย่างของหลักจรรยาบรรณที่เครือข่ายนิติวิทยาศาสตร์ระดับภูมิภาคนำมาใช้:

• ผู้อำนวยการห้องปฏิบัติการอาชญากรรมแห่งอเมริกา (ASCLD) – www.ascld.org

• เครือข่ายสถาบันนิติวิทยาศาสตร์แห่งยุโรป (ENFSI) – www.enfsi.eu

• สถาบันนิติวิทยาศาสตร์แห่งชาติ ออสเตรเลีย นิวซีแลนด์ (NIFS ANZ) – www.anzfss.org

• สถาบันการศึกษา Iberoamericana de Criminalística y Estudios Forenses (AICEF) – www.aicef.net

• เครือข่ายนิติวิทยาศาสตร์แห่งเอเชีย (AFSN) – www.asianforensic.net

1.2 การฝึกอบรม

ห้องปฏิบัติการควรมีเอกสารโปรแกรมการฝึกอบรมอย่างเป็นทางการสำหรับผู้ตรวจสอบ การฝึกอบรมควรจัดส่งโดยผู้ปฏิบัติงานที่มีความเชี่ยวชาญ มีความสามารถ และมีประสบการณ์ และพิจารณาความก้าวหน้าของผู้ตรวจสอบจากผู้ตรวจสอบทั่วไป (ผู้ตรวจสอบระดับล่าง) ไปจนถึงความเชี่ยวชาญเฉพาะทางในสาขาวิชาย่อย (สาขาวิชาย่อยนั้นกว้างขวาง และรวมถึงการประมวลผลภาพและเสียง การเข้ารหัส ระบบควบคุมอุตสาหกรรม นิติวิทยาศาสตร์ขั้นสูงในการตรวจพิสูจน์โทรศัพท์เคลื่อนที่ ฯลฯ)

อาจมีการพิจารณาจ้างโปรแกรมการฝึกอบรมจากองค์กรภายนอกหรือในส่วนที่ผู้ให้บริการนิติวิทยาศาสตร์ขาดทักษะและประสบการณ์ที่เหมาะสม (เช่น การวิเคราะห์ข้อมูลทางการเงิน สื่อมัลติมีเดีย ฯลฯ) หรือในกรณีที่จำนวนผู้ตรวจสอบที่เข้ารับการฝึกอบรมไม่มี แสดงให้เห็นถึงความพยายามในการสร้างและบำรุงรักษาที่จำเป็นในการพัฒนาและส่งมอบหลักสูตรภายใน

ทักษะทางเทคนิคที่ได้รับจากหลักสูตรการฝึกอบรมที่เป็นทางการและไม่เป็นทางการ ซึ่งได้จากหลักสูตรภายในหลักสูตรภายนอกองค์กร หรือหลักสูตรภายนอก ควรมีการบันทึกเป็นอย่างดี ควรเน้นที่ความถี่ของการฝึกอบรมโดยพิจารณาจากพลวัตที่เหนือชั้นและความก้าวหน้าอย่างต่อเนื่องในด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะมีการนำส่งโปรแกรมเชิงพาณิชย์หรือภายในองค์กร ผู้สอบที่เข้ารับการฝึกอบรมควรได้รับการรับรองหลังจากการประเมินที่อธิบายขอบเขตของความสามารถอย่างชัดเจนและกรอบเวลาใดๆ สำหรับการหมดอายุของความสามารถนั้น แม้ว่าหลักสูตรฝึกอบรมที่ไม่ได้ประเมินจะมีคุณค่าที่ชัดเจนในการพัฒนาผู้ตรวจสอบ แต่ก็ไม่ควรพึ่งพาเพียงลำพังในการพัฒนาสมาชิกใหม่

พนักงานควรได้รับการประเมินว่ามีความสามารถพอๆ กับที่เชี่ยวชาญก่อนที่จะมีการพิจารณากรณีศึกษาที่เป็นอิสระ และควรรับรองการรับรองอย่างต่อเนื่องผ่านการประเมินและการทดสอบเป็นประจำ

เอกสารประกอบการรับรองและการพัฒนาวิชาชีพอย่างต่อเนื่องเป็นสิ่งสำคัญ

โปรแกรมการฝึกอบรมควรมีจุดมุ่งหมายเพื่อพัฒนาทักษะดังต่อไปนี้:

• การระบุเบื้องต้น การเก็บรักษา และการจัดการที่ปลอดภัยของแหล่งหลักฐานดิจิทัลทั่วไป

• รับข้อมูลดิจิทัลทางนิติวิทยาศาสตร์เพื่อการตรวจสอบ

• ความคุ้นเคยของเทคนิคการ "ลงนาม" การเข้ารหัสเพื่อแสดงให้เห็นถึงความสมบูรณ์ของหลักฐาน และความคุ้นเคยกับอัลกอริธึมทั่วไป (MD5, SHA1, SHA256);

• รักษาข้อมูลดั้งเดิมในรูปภาพ "กระจก" ที่ลงนามด้วยการเข้ารหัสลับ

• ตรวจสอบความสมบูรณ์ของไฟล์และห่วงโซ่การดูแลในทุกขั้นตอนของการตรวจสอบ (ผ่านแอปพลิเคชันการลงนามด้วยการเข้ารหัส)

• การตรวจสอบและวิเคราะห์สำเนาหลักฐานการทำงานสำหรับรายการที่เกี่ยวข้องกับขอบเขตของการวิเคราะห์

• เอกสารของผลการวิจัย;

• การตีความและการรายงานผล; และ

• การนำเสนอในศาล

2. อุปกรณ์และวัสดุสิ้นเปลือง

2.1 สิ่งอำนวยความสะดวก

เมื่อใดก็ตามที่เป็นไปได้ การรับหลักฐาน การจัดการและการจัดเก็บควรแยกออกจากพื้นที่ตรวจสอบการจัดแสดง (เพื่อป้องกันความสับสนและโอกาสในการสูญเสียหลักฐาน เนื่องจากมีรายการดิจิทัลจำนวนมากที่ดูคล้ายคลึงกัน)

พื้นที่ที่ใช้เพื่อวัตถุประสงค์ในการได้มาและวิเคราะห์หลักฐานดิจิทัลควรเชื่อมต่อกับเครื่องสำรองไฟฟ้า (UPS) เพื่อลดความเสียหายของข้อมูลและการสูญเสียหลักฐาน อาหาร เครื่องดื่ม และของเหลวที่ไม่บรรจุอยู่ในพื้นที่ใดๆ ที่ดำเนินการประมวลผลหลักฐานทางอิเล็กทรอนิกส์

หากดำเนินการประมวลผลเสียง การจัดหาสภาพแวดล้อม "การแยกเสียง" แบบพิเศษจะช่วยเพิ่มความสามารถของผู้ตรวจสอบได้อย่างมาก ในทำนองเดียวกัน การจัดแสงแบบพิเศษจะช่วยในการตรวจสอบเนื้อหาวิดีโอ

พื้นที่ทั้งหมดที่เกี่ยวข้องกับการจัดเก็บ การจัดการ และการวิเคราะห์ควรมีความปลอดภัยและควบคุมการเข้าถึง โดยที่บุคคลที่ไม่ได้รับอนุญาตจะต้องถูกคุ้มกันภายในโรงงานเสมอ

ห้องค้นหา "วัตถุประสงค์ทั่วไป" ที่สามารถทำความสะอาดได้ง่ายนั้นเป็นประโยชน์และช่วยให้สามารถประมวลผลรายการอิเล็กทรอนิกส์ (เช่น แล็ปท็อป) ได้พร้อมกันสำหรับหลักฐานทางอิเล็กทรอนิกส์และไบโอเมตริกซ์ (เช่น ลายนิ้วมือ ดีเอ็นเอ)

2.2 อุปกรณ์

อุปกรณ์ที่ใช้ในการจัดการ การได้มา และการประมวลผลหลักฐานทางอิเล็กทรอนิกส์นั้นมีมากมาย อุปกรณ์ที่ถือว่าสำคัญสำหรับหลักฐานทางอิเล็กทรอนิกส์รวมถึง (แต่ไม่จำกัดเพียง):

• กล้อง (ภาพนิ่งและวิดีโอ) สำหรับบันทึกฉาก การจัดแสดง และการค้นพบ;

• คอมพิวเตอร์แล็ปท็อปสำหรับการประมวลผลฉากและห้องปฏิบัติการของนิทรรศการอิเล็กทรอนิกส์

• อุปกรณ์ป้องกันการเขียน (ฮาร์ดแวร์และ/หรือซอฟต์แวร์) เพื่อให้การเชื่อมต่อที่ปลอดภัยของการจัดแสดงอิเล็กทรอนิกส์กับคอมพิวเตอร์วิเคราะห์

• ซอฟต์แวร์ (เชิงพาณิชย์และ/หรือฟรีแวร์) เพื่อให้ได้รับสำเนาที่เก็บหลักฐานที่ลงนามด้วยการเข้ารหัสลับ

• "บูตดิสก์" เพื่อให้สามารถโต้ตอบและรับการจัดแสดงโดยไม่ต้องใช้คอมพิวเตอร์วิเคราะห์

• ซอฟต์แวร์ (เชิงพาณิชย์และ/หรือฟรีแวร์) เพื่อให้สามารถประมวลผลและวิเคราะห์สำเนาที่เป็นหลักฐานได้

• ซอฟต์แวร์ (เชิงพาณิชย์และ/หรือฟรีแวร์) เพื่อให้สามารถประมวลผลหลักฐานภาพและเสียง

• ถุงและอุปกรณ์ปิดกั้นคลื่นความถี่วิทยุ (ปกติเรียกว่า "ถุงฟาราเดย์") เพื่อปกป้องหลักฐานจากการเช็ดและการรบกวนจากระยะไกล

• อุปกรณ์สกัดโทรศัพท์เคลื่อนที่เพื่อการพาณิชย์; และ

• อุปกรณ์สำหรับผลิตหลักฐานในรูปแบบศาล (เช่น เครื่องเขียนดีวีดี)

ผู้ตรวจสอบควรดูแลรักษาและทำความคุ้นเคยกับระบบปฏิบัติการหลายระบบ (รวมถึง Windows, MacOS และ Linux)

แล็ปท็อปวิเคราะห์ทั้งหมด อุปกรณ์ป้องกันการเขียน และซอฟต์แวร์ควรได้รับการประเมินว่าเหมาะสมกับงานที่จำเป็น การบำรุงรักษาและบันทึกการตรวจสอบของอุปกรณ์ที่สำคัญทั้งหมดควรได้รับการบำรุงรักษาเพื่อวัตถุประสงค์ด้านคุณภาพและการตรวจสอบย้อนกลับ

เฉพาะสมาชิกที่ได้รับการฝึกอบรมให้ใช้อุปกรณ์ดังกล่าวอย่างปลอดภัยเท่านั้นที่จะเชื่อมต่อและโต้ตอบกับรายการที่เป็นหลักฐาน

2.3 วัสดุสิ้นเปลือง

รายการวัสดุสิ้นเปลืองทั่วไปที่ใช้ในการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ได้แก่ :

• สื่อสำหรับจัดเก็บสำเนาและรูปภาพที่เป็นหลักฐาน:

o สื่อแฟลชสำหรับใช้ในกล้องและอุปกรณ์บันทึก

สื่อ Flash/USB สำหรับจัดเก็บและนำเสนอชุดข้อมูลขนาดเล็กถึงกลาง

o ฮาร์ดไดรฟ์หลวมสำหรับจัดเก็บชุดข้อมูลขนาดใหญ่

• ถุงมือแบบใช้แล้วทิ้งที่สวมใส่เพื่อป้องกันผู้ตรวจสอบจากการปนเปื้อนของวัตถุอันตราย ตลอดจนเพื่อรักษาความสมบูรณ์ของหลักฐานทางนิติวิทยาศาสตร์อื่นๆ (โดยปกติคือไบโอเมตริกซ์)

• มาสก์หน้าแบบใช้แล้วทิ้งเพื่อรักษาความสมบูรณ์ของหลักฐานทางนิติวิทยาศาสตร์อื่น ๆ (โดยปกติคือไบโอเมตริกซ์); และ

• กระดาษ ปากกา/ดินสอ และสิ่งของอื่นๆ เพื่อให้สามารถจดบันทึกได้อย่างแม่นยำและพร้อมๆ กันในการสอบฉาก

เมื่อนำอุปกรณ์จัดเก็บข้อมูลกลับมาใช้ใหม่ระหว่างการตรวจสอบและกรณีต่างๆ ควรมีนโยบายและขั้นตอนในการป้องกันการรั่วไหลของข้อมูลและการปนเปื้อนของอุปกรณ์จัดเก็บข้อมูลระหว่างงาน บันทึกการล้างข้อมูลบนดิสก์ (ตัวอย่าง) และขั้นตอนการตรวจสอบความถูกต้องควรถูกเก็บรักษาไว้เป็นส่วนหนึ่งของไฟล์เคส

3 การรวบรวม การวิเคราะห์ การตีความ และการรายงาน

3.1 การเก็บรวบรวม

หลักฐานทางอิเล็กทรอนิกส์ประกอบด้วยข้อมูลที่สร้างหรือบันทึกไว้ในอุปกรณ์อิเล็กทรอนิกส์ได้หลายวิธี ชนิดข้อมูลทั่วไปที่ระบุโดยทั่วไปในระหว่างการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ได้แก่:

• ข้อมูลที่ใช้งานอยู่ (นี่คือข้อมูลที่ผู้ใช้ทั่วไปของระบบมองเห็นได้ เอกสารนี้เป็นตัวอย่างของ "ข้อมูลที่ใช้งานอยู่");

• Embedded Metadata (ซึ่งรวมถึงข้อมูลเกี่ยวกับไฟล์ที่จัดเก็บโดยระบบ และอาจรวมถึงเวลาและวันที่ สถานที่ และหมายเลขซีเรียลของฮาร์ดแวร์และซอฟต์แวร์)

• การสำรองข้อมูล (รวมถึงข้อมูลสำหรับการกู้คืนจากภัยพิบัติหรือการสำรองข้อมูลที่สำคัญขององค์กรอย่างเป็นทางการ การสำรองข้อมูลทั่วไปที่อยู่ระหว่างการตรวจสอบคือของโทรศัพท์เคลื่อนที่);

• ข้อมูลที่ไม่ใช้งาน (ถูกลบ) (โดยทั่วไปรวมถึงข้อมูลที่ผู้ใช้ทั่วไปของระบบไม่สามารถมองเห็นได้ แต่สามารถกู้คืนได้โดยใช้ความรู้และเครื่องมือเฉพาะ ไฟล์อาจถูกลบผ่านกิจกรรมของผู้ใช้หรือระบบอัตโนมัติ)

• ข้อมูลระเหย (นี่คือข้อมูลที่มีอยู่ในสถานะที่ไม่ใช่ทางกายภาพ และอาจไม่ปรากฏบนฮาร์ดไดรฟ์หรือสื่อเก็บข้อมูลของระบบ ตัวอย่างข้อมูลที่ระเหย ได้แก่ ข้อมูลที่เก็บไว้ในหน่วยความจำระบบและข้อมูลที่จัดเก็บไว้ในตำแหน่งนอกสถานที่ เช่น ระบบคลาวด์คอมพิวติ้ง); และ

• ข้อมูลโทรคมนาคม (ซึ่งรวมถึงการรับส่งข้อมูลเครือข่ายที่ส่งและรับซึ่งเป็นส่วนหนึ่งของการโต้ตอบตามปกติของระบบกับอินเทอร์เน็ตหรืออินทราเน็ต)

การพิจารณาลักษณะของข้อมูลประเภทต่างๆ มีความสำคัญ เนื่องจากมีความท้าทายที่แตกต่างกันในด้านการตรวจสอบข้อมูล การดึงข้อมูล การบันทึกผล การเตรียมการนำเสนอมูลค่าของหลักฐาน การจัดเก็บและการจัดเก็บหลักฐาน การนำเสนอเป็นหลักฐานในศาล กฎหมาย ฯลฯ นอกจากนี้ ควรมีการวางแผนลำดับการตรวจสอบอย่างรอบคอบเพื่อให้แน่ใจว่ามีการรวบรวมข้อมูลที่ไม่แน่นอนและเปลี่ยนแปลงได้ก่อนที่จะปิดระบบ หรือโต้ตอบกับระบบเพื่อรวบรวมข้อมูลที่ใช้งานอยู่

ความหมายทางการเงินของการจัดการหลักฐานทางอิเล็กทรอนิกส์ทั้งสำหรับผู้ให้บริการทางนิติวิทยาศาสตร์และลูกค้า (เช่น ผู้เสียหาย ผู้ถูกกล่าวหา บุคคลภายนอก ฯลฯ) เป็นข้อพิจารณาที่สำคัญ เนื่องจากอาจจำกัดคุณภาพ ขอบเขต และมูลค่าของหลักฐาน ระบบยุติธรรมทางอาญา.

ในระหว่างการรวบรวมและประมวลผลรายการอิเล็กทรอนิกส์ เป็นเรื่องปกติที่จะพบข้อมูลที่อาจได้รับการคุ้มครองหรือให้สิทธิพิเศษในทางใดทางหนึ่ง (เช่น ภายใต้สิทธิ์ของทนายความ-ลูกค้า สิทธิพิเศษทางวิชาชีพทางกฎหมาย หรือเกี่ยวกับรัฐสภา/รัฐบาล) สิ่งอำนวยความสะดวกควรมีกระบวนการเพื่อให้มีการจัดการที่ปลอดภัยของวัสดุดังกล่าว รวมถึงการจำกัดให้เฉพาะสมาชิกที่จำเป็นต้องรู้เท่านั้น

ข้อกำหนดด้านโครงสร้างพื้นฐานที่ควบคุมโดยความก้าวหน้าของเทคโนโลยีสารสนเทศตลอดจนการเติบโตของข้อมูลที่เพิ่มขึ้นแบบทวีคูณทำให้เกิดความท้าทายที่สำคัญต่อผู้ให้บริการนิติวิทยาศาสตร์เนื่องจากเครื่องมือห้องปฏิบัติการ (ฮาร์ดแวร์และซอฟต์แวร์) ที่เหมาะสมสำหรับวิธีการที่ห้องปฏิบัติการใช้ได้รับการปรับปรุงอย่างต่อเนื่องและ ความซ้ำซ้อนเป็นเรื่องธรรมดา

ฮาร์ดแวร์และซอฟต์แวร์ที่ออกแบบมาเพื่อจัดการกับข้อมูลที่ซับซ้อนที่พบในอุปกรณ์อิเล็กทรอนิกส์ส่วนหน้า และระบบองค์กรมีจำนวนเพิ่มมากขึ้น เนื่องจากเครื่องมือเหล่านี้มีจุดมุ่งหมายเพื่อจัดการการเติบโตแบบทวีคูณของข้อมูลที่สร้างขึ้น และจำเป็นอย่างยิ่งที่เครื่องมือที่ใช้จะต้องคำนึงถึงลักษณะเฉพาะ นิติวิทยาศาสตร์. อาจเป็นไปไม่ได้ที่จะหาเครื่องมือฟรีเพื่อจัดการและตรวจสอบที่เก็บหลักฐานทางอิเล็กทรอนิกส์ ในกรณีเหล่านี้ ทางเลือกเดียวคือผลิตภัณฑ์เชิงพาณิชย์ ซึ่งอาจมีราคาแพงมาก

กระบวนการรวบรวมจะต้องได้รับการออกแบบเพื่อพิจารณาถึงความท้าทายเฉพาะที่พบในเทคโนโลยีสารสนเทศ และควรพิจารณาประเด็นต่อไปนี้:

• ระบุสิ่งที่คุณกำลังมองหา (ก่อนเริ่มการสอบ);

• ปฏิบัติตามข้อกำหนดทางกฎหมายสำหรับการยึดข้อมูลและการจัดแสดงอิเล็กทรอนิกส์ (เช่น เงื่อนไขของหมายค้น)

• ลดการหยุดชะงักของการดำเนินงาน โดยเฉพาะอย่างยิ่งกับบุคคลที่สามหรือสิ่งอำนวยความสะดวกในการจัดเก็บข้อมูลที่ "เป็นมิตร";

• ลดผลกระทบทางการเงินของการจัดเก็บ ซึ่งรวมถึงการระบุและกำจัดแหล่งข้อมูลภายนอก ณ ที่เกิดเหตุ เพื่อป้องกันการรวบรวมและจัดเก็บข้อมูลที่ไม่จำเป็น

• ใช้ระบบและเครือข่ายผู้ตรวจสอบทางนิติวิทยาศาสตร์ที่แยกจากกัน (ตรงข้ามกับเจ้าหน้าที่แผนกระบบไอทีภายใน) เพื่อจัดเก็บและวิเคราะห์หลักฐาน

• ปฏิบัติตามโปรโตคอลและกระบวนการที่สร้างขึ้นโดยห้องปฏิบัติการ และ

• เก็บบันทึกกระบวนการรวบรวมและการตัดสินใจที่สำคัญ

3.2 การวิเคราะห์

ขั้นตอนต่อไปนี้เป็นเรื่องปกติของกระบวนการค้นหา/จับกุมปกติที่เกี่ยวข้องกับหลักฐานทางอิเล็กทรอนิกส์:

3.2.1 ค้นหา

การค้นหาจะดำเนินการเพื่อค้นหาและเลือกข้อมูลของค่าหลักฐานที่เป็นไปได้สำหรับกรณี ซึ่งมักจะเกิดขึ้นหลังจากการตรวจสอบอุปกรณ์จัดเก็บข้อมูล เครือข่ายท้องถิ่น เครือข่ายบริเวณกว้าง สภาพแวดล้อมระบบคลาวด์ เครือข่ายส่วนตัวเสมือน และอุปกรณ์โทรคมนาคมอย่างละเอียดถี่ถ้วน เพื่อพิจารณาว่าควรรวมหรือยกเว้นอุปกรณ์หรือ

สภาพแวดล้อมเฉพาะเท่าที่เป็นไปได้หรือไม่ การตัดสินใจว่าทำไมรายการจึงถูกค้นหรือไม่ถูกค้นและยึดควรได้รับการบันทึกเป็นการตัดสินใจที่สำคัญในแฟ้มคดี

3.2.2 การได้มาและการวิเคราะห์

เมื่อกำหนดความเกี่ยวข้องและมูลค่าของข้อมูลที่มีอยู่หรือจัดเก็บไว้ในอุปกรณ์หรือสภาพแวดล้อมแล้ว กระบวนการดึงข้อมูลได้รับการออกแบบมาเพื่อเพิ่มการรวบรวมหลักฐานให้ได้มากที่สุด ควรพิจารณาอย่างรอบคอบถึงปริมาณข้อมูล การเก็บรักษาข้อมูล ความเสี่ยงที่ข้อมูลจะสูญหายและ/หรือการทำลาย และความเสี่ยงที่อาจเกิดขึ้นกับทุกฝ่ายที่ได้รับผลกระทบจากการดึงข้อมูลที่เป็นปัญหา

3.2.3 การรวบรวมข้อมูล

ในการพิจารณาข้อกำหนดเฉพาะของระบบยุติธรรมทางอาญาที่เกี่ยวข้องกับเขตอำนาจศาลที่ทำการตรวจสอบ การรายงานผลการพิจารณาเช่น Courts of Law จำเป็นต้องมีการวางแผนอย่างพิถีพิถัน เนื่องจากการผลิตวิธีการรายงานแบบดั้งเดิมมักไม่สามารถทำได้เมื่อมีการนำเสนอหลักฐานทางอิเล็กทรอนิกส์ การเกิดขึ้นของศาลเฉพาะทางเพื่อจัดการกับหลักฐานประเภทนี้ได้รับการจัดตั้งขึ้นเพื่อเอาชนะความท้าทายเฉพาะอันเป็นผลมาจากการนำเสนอหลักฐานทางอิเล็กทรอนิกส์

3.3 การตีความ

3.3.1 การจัดผลลัพธ์:

3.3.1.1 การจัดระเบียบ:

ลักษณะของข้อมูลที่ฝังอยู่ในอุปกรณ์อิเล็กทรอนิกส์อาจดูเหมือนไม่มีการรวบรวมกันเนื่องจากอัลกอริธึมการจัดเก็บข้อมูลที่แตกต่างกัน เกือบจะทุกครั้งจะได้รับและวิเคราะห์ข้อมูลที่นำเสนอในศาลยุติธรรมซึ่งตรงข้ามกับข้อมูลดิบ การจัดเตรียมข้อมูลดังกล่าวควรก่อให้เกิดข้อมูลที่ชัดเจนและรัดกุม โดยไม่เปลี่ยนแปลงลักษณะหรือผลกระทบของข้อมูลเมตาแต่อย่างใด เครื่องมือและวิธีการที่ออกแบบมาโดยเฉพาะเพื่อดำเนินการภายใต้ข้อกำหนดที่เข้มงวดสำหรับกฎของหลักฐาน ควรใช้แทนเครื่องมือเทคโนโลยีสารสนเทศทั่วไป นี้เพิ่มการยอมรับของหลักฐานสูงสุด

3.3.1.2 การลดปริมาณข้อมูล:

ด้วยขนาดอุปกรณ์จัดเก็บข้อมูลที่เพิ่มขึ้น และจำนวนไฟล์ที่แท้จริงในระบบทั่วไป ทำให้ผู้ตรวจสอบไม่สามารถตรวจดูทุกสิ่งที่มีอยู่ในอุปกรณ์ได้ ดังนั้น การใช้คำสำคัญ คำค้นหา และลายเซ็นไฟล์จึงมีความสำคัญในการลดปริมาณข้อมูลให้อยู่ในระดับที่จัดการได้ กลยุทธ์การลดข้อมูลดังกล่าวควรนำไปใช้กับเป้าหมายของการตรวจสอบ

อยู่เสมอ และควรบันทึกเป็นการตัดสินใจที่สำคัญเพื่อให้บุคคลที่สามสามารถทำซ้ำเส้นทางการวิเคราะห์ได้ แม้จะมีกลยุทธ์การลดข้อมูล ปริมาณข้อมูลที่ได้รับจากระบบองค์กรมักจะอยู่นอกเหนือความสามารถของผู้ให้บริการนิติวิทยาศาสตร์ที่พัฒนามากที่สุด และจำเป็นต้องได้รับการพิจารณาเป็นพิเศษ

3.3.1.3 รูปแบบ:

รูปแบบที่เข้าใจยากและไม่สามารถเข้าใจได้ (ซึ่งมนุษย์ไม่สามารถอ่านได้) ของข้อมูลเลขฐานสองหรือเลขฐานสิบหกทั่วไปโดยทั่วไปต้องมีการแปลงเป็นรูปแบบที่เป็นมิตรสำหรับการนำเสนอต่อศาลยุติธรรมและฆราวาส เมื่อแปลงข้อมูลเพื่อเพิ่มความสามารถในการอ่าน ลิงก์ควรรักษาไว้กับแหล่งข้อมูลเดิมที่ไม่ได้แปลงเพื่อให้สามารถติดตามได้

ตัวอย่างทั่วไปของสิ่งนี้คือ “ไทม์ไลน์” เมื่อนำเสนอข้อมูลโทรคมนาคม เช่น บันทึกการโทรที่พบในอุปกรณ์มือถือ หากไม่มีการนำเสนอหลักฐานตามลำดับเวลา อาจเกิดความสับสน

3.3.1.4 การทบทวน:

การตรวจสอบข้อมูลที่ดึงมาจากอุปกรณ์อิเล็กทรอนิกส์มักต้องมีการตรวจสอบข้อมูลดิบอย่างครอบคลุมร่วมกับเจ้าหน้าที่สอบสวน ลูกค้า เจ้าหน้าที่ฝ่ายกฎหมายในระหว่างการประชุมก่อนการพิจารณาคดี เพื่อพิจารณาความเกี่ยวข้องและป้องกันการรวบรวมข้อมูลที่ไม่เกี่ยวข้องอย่างกว้างขวาง และการเปิดเผยประเภทข้อมูลที่ได้รับการคุ้มครอง

3.3.2 การเก็บรักษา:

ผู้ตรวจสอบหลักฐานทางอิเล็กทรอนิกส์มีหน้าที่เก็บรักษาหลักฐานเพื่อป้องกันการสูญหายและการทำลายข้อมูล และควรปฏิบัติหน้าที่ดังนี้

- ดูแลรักษาและควบคุมข้อมูลที่ได้รับจากแหล่งที่มา
- เข้าใจข้อจำกัดของความเชี่ยวชาญภายในองค์กร
- ค้นหาและรักษาหลักฐานดิจิทัล
- จัดทำเอกสารกลยุทธ์การนำเสนอหลักฐานและการตัดสินใจที่สำคัญ
- ประเมินปัญหาเขตอำนาจศาล ปริมาณข้อมูล และความจำเพาะ/ขอบเขตของคำขอ
- เมื่อใดก็ตามที่เป็นไปได้ จำกัดการเก็บรวบรวมข้อมูลเฉพาะคำสำคัญ วันที่ ชื่อไฟล์ ฯลฯ ;

• ดึงข้อมูลลงในโฟลเดอร์เฉพาะที่กำหนด

• มีส่วนร่วมกับผู้ตรวจสอบเพื่อให้แน่ใจว่าคำขอจะไม่ส่งผลให้เกิดการยึดข้อมูลที่มีขนาดใหญ่เกินไปและยุ่งยาก

3.3.3 การตรวจสอบมัลติมีเดีย:

สามารถใช้ซอฟต์แวร์ประมวลผลสัญญาณเพื่อปรับปรุงหลักฐานเสียงและวิดีโอเพื่อวัตถุประสงค์ในการสืบสวน โดยเฉพาะอย่างยิ่งในกรณีที่มีการบันทึกหลักฐานภายใต้สภาวะที่ไม่ดีที่สุด การเลือกเทคนิคการประมวลผลสัญญาณ เช่น การกรอง จะขึ้นอยู่กับการวิเคราะห์สัญญาณ ลักษณะเสียง และการบิดเบือนของการบันทึกวิดีโอเสียง หากมีการนำเสนอเนื้อหาที่ปรับปรุงเพื่อวัตถุประสงค์ของศาล ผู้ตรวจสอบจะต้องอธิบายวิธีการประมวลผลสัญญาณและข้อจำกัดของวิธีการนั้น โดยทั่วไป ผู้ตรวจสอบทางนิติวิทยาศาสตร์ทางนิติวิทยาศาสตร์จะไม่นำเสนอการตีความคำพูดหรือเนื้อหาวิดีโอ เว้นแต่จะสามารถแสดงความสามารถในการใช้วิธีการที่ได้รับการตรวจสอบอย่างเพียงพอสำหรับสถานการณ์เฉพาะกรณี และเข้าใจข้อจำกัดและสมมติฐานที่เกี่ยวข้องกับวิธีการดังกล่าว

ในทำนองเดียวกัน การตีความเกี่ยวกับแหล่งที่มาของการบันทึกเสียงหรือวิดีโอ หรือกิจกรรมที่เกี่ยวข้องกับการผลิตการบันทึก ควรนำเสนอเฉพาะในกรณีที่ผู้ตรวจสอบสามารถแสดงความสามารถในการใช้วิธีการที่เกี่ยวข้องและผ่านการตรวจสอบอย่างเพียงพอ

3.3.4 ความท้าทาย:

ผู้ตรวจสอบหลักฐานทางอิเล็กทรอนิกส์อาจประสบปัญหาดังต่อไปนี้:

• ปรับปรุงมาตรฐานและการพิจารณากระบวนการรวบรวมให้สอดคล้องกับแนวปฏิบัติที่ดีที่สุดระดับสากล

• การสุ่มตัวอย่างการเก็บรวบรวมข้อมูล โดยที่การรวบรวมทั้งหมดเป็นสิ่งต้องห้ามหรือเป็นไปไม่ได้

• ข้อกำหนดสำหรับการพัฒนาความสามารถในการประมวลผลอย่างต่อเนื่องเพื่อเปลี่ยนแปลงด้วยแหล่งข้อมูลที่ซับซ้อนมากขึ้น

• การใช้ระบบการตรวจสอบขององค์กร

• รวมระบบการตรวจสอบขององค์กรเพื่อประมวลผลหลายระบบ

• การเปิดเผยของผู้ตรวจสอบหลักฐานดิจิทัลต่อเนื้อหาและภาพที่ "ไม่เหมาะสม" ตามที่ระบุไว้ทั่วไปในการแสวงหาประโยชน์จากเด็กและการสืบสวนต่อต้านการก่อการร้าย และ

• การปรับปรุงในการตรวจสอบหลักฐานบนคลาวด์

3.4 การรายงาน

ผู้จัดการห้องปฏิบัติการควรตรวจสอบให้แน่ใจว่ารายงานหรือคำแถลงใด ๆ ที่จัดทำโดยผู้ตรวจสอบมีรายการข้อมูลขั้นต่ำดังต่อไปนี้:

• หมายเลขประจำตัวกรณีที่ไม่ซ้ำกันหรือการอ้างอิง;

• ชื่อเต็มและบทบาทของผู้สอบ

• คำชี้แจงหน้าที่ที่มีบทบาทและประเภทของการสอบที่ผู้สอบได้รับอนุญาตให้ดำเนินการ

• คุณสมบัติใดๆ (รวมถึงการศึกษา/การฝึกอบรมอย่างเป็นทางการ การศึกษาตามอัธยาศัย และการวิจัย) ที่ผู้ตรวจสอบได้ดำเนินการที่เกี่ยวข้องกับเรื่องต่อศาล

• การปฏิบัติตามจรรยาบรรณที่เกี่ยวข้องหรือข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับเขตอำนาจศาล;

• ข้อจำกัดใดๆ ในการตรวจสอบ (ไม่ว่าจะกำหนดโดยผู้ตรวจสอบหรือผู้วิจัย) และสมมติฐานใดๆ ที่ผู้ตรวจสอบทำขึ้นในส่วนที่เกี่ยวกับการวิเคราะห์

• การวางขั้นตอนและการดำเนินการที่ชัดเจนโดยผู้ตรวจสอบ รวมถึงข้อค้นพบที่เกี่ยวข้อง

• อธิบายอย่างชัดเจนและระบุหลักฐานที่เป็นข้อเท็จจริง ซึ่งตรงข้ามกับหลักฐานความคิดเห็นที่ผู้ตรวจสอบได้รับอนุญาตให้ทำ

• การอ้างอิงถึงห่วงโซ่การควบคุมสำหรับหลักฐานใด ๆ ที่อ้างถึงในรายงานหรือคำแถลง; และ

• ควรระบุบันทึกที่เกี่ยวข้องหรือหลักฐานต้นฉบับที่แนบมากับรายงานหรือข้อความ (ไม่ว่าจะในรูปแบบกระดาษหรือดิจิทัล)

3.5 ฐานข้อมูล

เพื่อลดการเปิดเผยของผู้ตรวจสอบต่อเนื้อหาที่ไม่เหมาะสมและไม่เหมาะสม (ซึ่งอาจส่งผลให้เกิดความเครียดเกินควรและส่งผลต่อสุขภาพจิต) ขอแนะนำให้ใช้ฐานข้อมูลลายเซ็นไฟล์

สิ่งเหล่านี้สามารถสร้างขึ้นและดูแลได้โดยเขตอำนาจศาลและหน่วยงานแต่ละแห่ง อย่างไรก็ตาม ควรพิจารณาฐานข้อมูลที่มีอยู่ทั่วไป เช่น ฐานข้อมูลที่เผยแพร่โดย Interpol และ Project VIC

ไม่ควรอาศัยฐานข้อมูลลายเซ็นไฟล์เพียงอย่างเดียวสำหรับการระบุไฟล์และการประมวลผล เนื่องจากข้อผิดพลาดของมนุษย์อาจส่งผลให้มีการจัดประเภทที่ไม่ถูกต้อง หรือการจำแนกประเภทอาจแตกต่างกันระหว่างเขตอำนาจศาล

4 ขั้นตอน โปรโตคอล และการตรวจสอบ

4.1 ขั้นตอนและระเบียบการ

กระบวนการที่ใช้ในการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ควรได้รับการออกแบบโดยคำนึงถึงแรงจูงใจที่หลากหลาย เช่น

- ขโมยทรัพย์สินทางปัญญา;
- การบอกเลิกโดยมิชอบ;
- การผิดสัญญา;
- ล่วงละเมิดทางเพศ;
- การใช้อีเมลในทางที่ผิด;
- การฉ้อโกง;
- การควบรวมกิจการ; และ
- การทำลายข้อมูลโดยเจตนา

การพัฒนาโปรโตคอลโดยผู้ให้บริการนิติวิทยาศาสตร์ที่รับผิดชอบในการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ควรมีจุดมุ่งหมายเพื่อให้แน่ใจว่ามีความเกี่ยวข้องและพิจารณาลักษณะการพัฒนาของภาคเทคโนโลยีสารสนเทศที่มุ่งเป้าไปที่ต่อไปนี้:

- การสื่อสารที่เหมาะสมระหว่างผู้มีส่วนได้ส่วนเสียในการสืบสวนเป็นสิ่งสำคัญและจะรับรองว่า:
  - การระบุและค้นพบแหล่งที่มาทั้งหมดอย่างครบถ้วน
  - หลักฐานที่เก็บไว้มีความเกี่ยวข้อง และ
  - มีการสร้างหลักฐานที่เกี่ยวข้อง

โปรโตคอลที่กำหนดและจัดทำเอกสารขั้นตอนต้องแน่ใจว่า:

• ผู้ตรวจสอบต้องเข้าใจและปฏิบัติตามระเบียบวิธีปฏิบัติที่เป็นแนวทางในกระบวนการต่างๆ

• ผู้ตรวจสอบต้องเข้าใจโครงสร้างพื้นฐานที่สนับสนุนกระบวนการ

• ผู้ตรวจสอบต้องเข้าใจและปฏิบัติตามขั้นตอนที่กำหนดในการสอบที่เกี่ยวข้องทั้งหมด

• ควรพิจารณาความเสี่ยงที่เกี่ยวข้องกับการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ และขั้นตอนทั้งหมดควรพิจารณาถึงผลกระทบทางการเงิน การหยุดชะงักของการดำเนินงาน และการทำลายหลักฐาน การขัดขวางกระบวนการยุติธรรมที่อาจเกิดขึ้น และการสูญเสียการควบคุมและความครอบคลุมเนื่องจากการออกคำสั่งการเข้าถึงแบบครอบคลุม ข้อควรพิจารณาทั่วไปคือ:

o ระบุเอกสารที่เกี่ยวข้อง

o แจ้งเจ้าของเอกสารหรือผู้ดูแล

o เห็นด้วยกับฝ่ายต่างๆ เกี่ยวกับขั้นตอนการตรวจสอบโดยเฉพาะอย่างยิ่งเมื่อจำเป็นต้องมีการตรวจสอบระบบขององค์กร

o เก็บรักษาเอกสารที่เกี่ยวข้อง

o ตรวจสอบการปฏิบัติตามข้อกำหนดการเก็บรักษา

o จัดทำเอกสารกระบวนการ

จำเป็นต้องมีขั้นตอนบางอย่างในการจัดการหลักฐานทางอิเล็กทรอนิกส์ ซึ่งส่วนใหญ่ประกอบด้วย:

• การรวบรวมหลักฐานทางอิเล็กทรอนิกส์

• การจัดเรียงและการจัดระเบียบข้อมูลเมตา

• ทบทวนข้อมูลที่ดึงออกมาเพื่อกำหนดความเกี่ยวข้อง

• การผลิตผลลัพธ์และการรายงาน

4.2 การตรวจสอบความถูกต้อง

เครื่องมือใดๆ (ฟรีแวร์หรือเชิงพาณิชย์) ที่ใช้ในการประมวลผลและวิเคราะห์หลักฐาน ควรได้รับการประเมินความเหมาะสมผ่านการทดสอบด้วยชุดข้อมูลที่รู้จัก สิ่งนี้ทำให้มั่นใจได้ว่าผลลัพธ์สามารถเชื่อถือได้

เนื่องจากเครื่องมือเชิงพาณิชย์ไม่สามารถใช้ได้กับทุกสถานการณ์ จึงเป็นเรื่องปกติที่ผู้ตรวจสอบจะผลิตและพัฒนาเครื่องมือซอฟต์แวร์แบบใช้ครั้งเดียว (โดยทั่วไปเรียกว่า "สคริปต์") เพื่อช่วยในการประมวลผลหลักฐาน เครื่องมือดังกล่าวควรได้รับการทดสอบกับชุดข้อมูลที่รู้จักเพื่อให้แน่ใจว่าทำงานในลักษณะที่ถูกต้อง และข้อมูลที่ได้รับหรือหลักฐานใด ๆ ที่สามารถเชื่อถือได้

เครื่องมือบล็อกการเขียนที่ใช้สำหรับการปกป้องแหล่งข้อมูลที่เป็นหลักฐานควรได้รับการตรวจสอบเป็นระยะๆ เพื่อการทำงานที่เหมาะสม เพื่อให้แน่ใจว่าผู้ตรวจสอบไม่สามารถเปลี่ยนแปลงแหล่งที่มาของหลักฐานโดยไม่ได้ตั้งใจได้ สิ่งนี้สำคัญอย่างยิ่งเมื่อมีการใช้เครื่องมือบล็อกการเขียนใหม่ หรือเครื่องมือที่มีอยู่ได้รับการอัพเกรด (ไม่ว่าจะด้วยซอฟต์แวร์หรือการอัพเกรดเฟิร์มแวร์) บันทึกที่แสดงการทำงานที่ถูกต้องของเครื่องมือบล็อกการเขียนควรได้รับการบำรุงรักษาสำหรับการผลิตตามความจำเป็นในศาลยุติธรรมหรือกระบวนการตรวจสอบ

5 การจัดการคุณภาพ

การจัดการคุณภาพเป็นกระบวนการที่อาศัยความถูกต้องของงานของผู้ตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ คุณภาพควรสร้างขึ้นในแต่ละขั้นตอนของกระบวนการ และไม่ตรวจสอบในตอนท้าย และควรสะท้อนถึงการปรับปรุงอย่างต่อเนื่อง

หลักฐานทางอิเล็กทรอนิกส์ค่อนข้างแตกต่างไปจากนิติวิทยาศาสตร์แบบดั้งเดิมที่เขตอำนาจศาลและสิ่งอำนวยความสะดวกหลายแห่งไม่ได้แสวงหาหรือคงไว้ซึ่งการรับรองระบบคุณภาพ เช่น ISO/IEC 17020 หรือ ISO/IEC 17025 แม้ว่าจะไม่ได้รับการรับรองโดยสมบูรณ์ก็ตาม ควรพิจารณาถึง การนำส่วนต่างๆ ของมาตรฐานสากลมาใช้ เนื่องจากสามารถช่วยปรับปรุงคุณภาพของงานห้องปฏิบัติการได้อย่างมาก และด้วยเหตุนี้ศาลจึงพิจารณาว่าผู้ให้บริการทางนิติวิทยาศาสตร์เป็นผู้รับผิดชอบ

อย่างน้อยที่สุด ผู้ตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ควรมีรายการตรวจสอบการดำเนินการหลักที่พวกเขาเฝ้าติดตามในขณะที่กำลังดำเนินการกับที่เกิดเหตุและการจัดแสดงที่ได้รับมาเพื่อช่วยในการรักษาความสมบูรณ์ของหลักฐานและการจัดการหลักฐาน (หรือห่วงโซ่การควบคุม)

สถานประกอบการควรรักษาและปฏิบัติตามขั้นตอนเกี่ยวกับการเก็บรักษาเอกสารที่กล่าวถึงโดยเฉพาะ:

- การทดสอบความชำนาญ;
- ความสามารถของผู้ปฏิบัติงาน;
- ผลการวิเคราะห์;
- ตัวอย่างการรับและบันทึกการประมวลผล;
- การเก็บรักษาข้อมูล;
- การดำเนินการแก้ไข;
- การตรวจสอบ;
- บันทึกการฝึกอบรม;
- การพัฒนาวิชาชีพอย่างต่อเนื่อง และ
- ติดตามคำให้การของศาล

โปรแกรมการจัดการคุณภาพควรระบุและจัดทำเอกสารความรับผิดชอบ อำนาจหน้าที่ และความสัมพันธ์ของบุคลากรทั้งหมดที่จัดการ ดำเนินการ หรือตรวจสอบงานที่มีผลกระทบต่อความถูกต้องของการสืบสวนที่เกิดเหตุ

6 อภิธานศัพท์

อภิธานศัพท์ต่อไปนี้ไม่ถือเป็นรายการคำศัพท์ที่ครบถ้วนสมบูรณ์ที่พบในหลักฐานดิจิทัลและมัลติมีเดีย อย่างไรก็ตาม คำศัพท์เหล่านี้ใช้กันอย่างแพร่หลายในแวดวงนิติวิทยาศาสตร์

DVD: ดิจิตอลดิสก์เอนกประสงค์

USB: ยูนิเวอร์แซลซีเรียลบัส

Electronic Evidence: หลักฐานอิเล็กทรอนิกส์คือข้อมูลที่จัดเก็บหรือส่งในรูปแบบดิจิทัลหรืออนาล็อกที่เกี่ยวข้องกับการสอบสวนหรือเรื่องในศาล

DIGITAL EVIDENCE: หลักฐานดิจิทัลมักใช้แทนกันได้กับหลักฐานทางอิเล็กทรอนิกส์ แต่สามารถใช้เพื่ออ้างอิงเฉพาะข้อมูลที่จัดเก็บหรือส่งในรูปแบบดิจิทัลที่เกี่ยวข้องกับการสอบสวนหรือเรื่องในศาล

Multimedia Evidence: หลักฐานอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการบันทึกเสียงและวิดีโอและภาพ

IFSA MEMBERS

STRATEGIC PARTNERS

INTERPOL

UNODC
United Nations Office on Drugs and Crime

Leverhulme Research Centre
for Forensic Science
LEVERHULME
TRUST