

แนวทางการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในระบบคลาวด์เพื่อการพิสูจน์ ทางนิติวิทยาศาสตร์

Approaches to Collecting Electronic Evidence in Cloud Computing for Forensic Purposes

ภาณุภท กิตติพันธ์^{1*} และ ศิริรัตน์ ชูสกุลเกรียง²

Panuphat Kittiphan^{1*} and Sirirat Choosakoonkriang²

¹หลักสูตรนิติวิทยาศาสตร์และงานยุติธรรม

²ภาควิชาเคมี คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

¹Forensic Science and Justice Program

²Department of Chemistry, Faculty of Science, Silpakorn University

*Corresponding author's email address: phat.tcsd@gmail.com

วันที่รับบทความ (Received)

8 เมษายน 2569

วันที่แก้ไขบทความ (Revised)

2 กรกฎาคม 2569

วันที่ตอบรับบทความ (Accepted)

3 กรกฎาคม 2569

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษาแนวทางที่มีประสิทธิภาพในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ในระบบคลาวด์คอมพิวเตอร์ให้สอดคล้องกับมาตรฐานทางกฎหมาย และวิเคราะห์ความท้าทายในการปฏิบัติงานการวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยใช้การวิเคราะห์เอกสารร่วมกับการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญจำนวน 10 ราย ได้แก่ เจ้าหน้าที่ตำรวจ ผู้เชี่ยวชาญด้านดิจิทัลฟอเรนสิก พนักงานอัยการ และผู้พิพากษา และวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เนื้อหา ผลการวิจัยพบว่า การยอมรับพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรมขึ้นอยู่กับความน่าเชื่อถือของกระบวนการและความสมบูรณ์ของข้อมูล โดยต้องคำนึงถึงความชอบด้วยกฎหมาย การรักษาห่วงโซ่การครอบครองพยานหลักฐาน และความสามารถในการตรวจสอบย้อนกลับในทุกขั้นตอน แนวปฏิบัติที่สำคัญ ได้แก่ การเก็บข้อมูลโดยไม่กระทบต่อข้อมูลต้นฉบับ การทำสำเนาข้อมูลเชิงนิติวิทยาศาสตร์ และการบันทึกขั้นตอนอย่างเป็นระบบ ซึ่งช่วยเพิ่มความโปร่งใสและลดข้อโต้แย้งในชั้นศาล อย่างไรก็ตาม ยังพบความท้าทาย ได้แก่ ความซับซ้อนของเทคโนโลยีปัญหาด้านเขตอำนาจศาลข้ามพรมแดน และข้อจำกัดด้านความเชี่ยวชาญของบุคลากร ดังนั้น ควรพัฒนาแนวทางการเก็บและจัดการพยานหลักฐานอิเล็กทรอนิกส์ในสภาพแวดล้อมคลาวด์คอมพิวเตอร์แบบบูรณาการทั้งด้านกฎหมาย เทคโนโลยี และทรัพยากรมนุษย์ เพื่อเพิ่มประสิทธิภาพของกระบวนการยุติธรรมในยุคดิจิทัล

คำสำคัญ: พยานหลักฐานอิเล็กทรอนิกส์, สภาพแวดล้อมคลาวด์คอมพิวเตอร์, ดิจิทัลฟอเรนสิก,

ห่วงโซ่การครอบครองพยานหลักฐาน, กระบวนการยุติธรรม

ABSTRACT

This study aims to examine effective approaches for collecting electronic evidence in cloud computing systems in compliance with legal standards and to analyze practical challenges. This qualitative research employs document analysis and in-depth interviews with ten key informants, including police officers, digital forensic experts, prosecutors, and judges. Data were analyzed using content analysis. The findings indicate that the admissibility of electronic evidence in judicial proceedings depends on process reliability and data integrity. Key considerations include legal compliance, preservation of the chain of custody, and traceability throughout all stages. Essential practices include non-intrusive data acquisition, forensic imaging, and systematic documentation, which enhance transparency and reduce disputes in court. However, several challenges remain, including technological complexity, cross-border jurisdictional issues, and limitations in personnel expertise. Therefore, an integrated approach to collecting and managing electronic evidence in cloud computing environments encompassing legal frameworks, technological development, and human resource capacity is necessary to strengthen the effectiveness of the justice system in the digital era.

Keywords: Electronic Evidence, Cloud Computing Environments, Digital Forensics, Chain of Custody, Justice System

บทนำ

ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารในยุคดิจิทัลได้ส่งผลกระทบอย่างมีนัยสำคัญต่อโครงสร้างทางสังคม เศรษฐกิจ และกฎหมาย โดยเฉพาะในมิติของอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี ซึ่งมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในรูปแบบการใช้เทคโนโลยีเป็นเครื่องมือและการกระทำความผิดผ่านระบบสารสนเทศโดยตรง ส่งผลให้เกิดความเสียหายในวงกว้างและมีความซับซ้อนมากยิ่งขึ้น อาชญากรรมทางเทคโนโลยี เช่น การหลอกลวงลงทุนในสินทรัพย์ดิจิทัลและการฟอกเงินผ่านระบบคริปโตเคอร์เรนซี สะท้อนให้เห็นถึงลักษณะของอาชญากรรมยุคใหม่ที่เชื่อมโยงกับเครือข่ายข้ามชาติ และจำเป็นต้องอาศัยพยานหลักฐานอิเล็กทรอนิกส์ในการพิสูจน์ข้อเท็จจริงในกระบวนการยุติธรรม (ไทยรัฐออนไลน์, 2567) ทั้งนี้ ในระบบกระบวนการยุติธรรมของไทยซึ่งยึดหลักระบบกล่าวหา คู่ความมีหน้าที่นำเสนอพยานหลักฐานเพื่อพิสูจน์ข้อเท็จจริง ขณะที่ศาลทำหน้าที่วินิจฉัยคดีโดยความเป็นกลาง พยานหลักฐานจึงเป็นองค์ประกอบสำคัญที่มีผลต่อผลของคดี โดยเฉพาะพยานหลักฐานอิเล็กทรอนิกส์ซึ่งมีลักษณะเฉพาะ คือ มีความเปราะบาง สามารถเปลี่ยนแปลงหรือถูกดัดแปลงได้ง่าย และต้องอาศัยกระบวนการเก็บรวบรวมที่ถูกต้องตามหลักวิชาการและ

กฎหมาย หากดำเนินการไม่เหมาะสม อาจทำให้พยานหลักฐานขาดความน่าเชื่อถือหรือไม่สามารถรับฟังได้ในชั้นศาล ภายใต้กรอบกฎหมายไทย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้รับรองสถานะของข้อมูลอิเล็กทรอนิกส์ในฐานะพยานหลักฐาน โดยกำหนดว่าห้ามปฏิเสธการรับฟังเพียงเพราะอยู่ในรูปแบบอิเล็กทรอนิกส์ อย่างไรก็ตาม การพิจารณาน้ำหนักของพยานหลักฐานยังคงขึ้นอยู่กับความน่าเชื่อถือของวิธีการได้มา การจัดเก็บ และความครบถ้วนของข้อมูล (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2567) แม้กฎหมายจะรองรับในเชิงหลักการ แต่ในทางปฏิบัติยังพบว่าการกำหนดมาตรฐานและแนวทางการเก็บพยานหลักฐานยังไม่เป็นเอกภาพ ในบริบทของเทคโนโลยีสมัยใหม่ระบบคลาวด์คอมพิวเตอร์ได้เข้ามามีบทบาทสำคัญในการจัดเก็บและประมวลผลข้อมูล เนื่องจากมีความยืดหยุ่นและสามารถเข้าถึงข้อมูลได้ทุกที่ทุกเวลา ส่งผลให้มีการใช้งานเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะในประเทศไทยที่มีแนวโน้มการเติบโตของการลงทุนด้านคลาวด์อย่างมีนัยสำคัญ (Gartner, 2024) อย่างไรก็ตาม ลักษณะเฉพาะของคลาวด์ เช่น การจัดเก็บข้อมูลบนเซิร์ฟเวอร์ต่างประเทศ การเข้ารหัสข้อมูล และความสามารถในการจัดการข้อมูลจากระยะไกล ได้ก่อให้เกิดความท้าทายต่อการรวบรวมและตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ ทั้งในด้านการรักษาความสมบูรณ์ของข้อมูลและการพิสูจน์แหล่งที่มา (Casey, 2011)

นอกจากนี้ การเข้าถึงข้อมูลในระบบคลาวด์ยังเกี่ยวข้องกับข้อจำกัดด้านเขตอำนาจศาลและความร่วมมือระหว่างประเทศ ซึ่งภายใต้กรอบกฎหมายที่มีอยู่ยังมีข้อจำกัดด้านระยะเวลาและประสิทธิภาพในการประสานงาน ส่งผลให้การรวบรวมพยานหลักฐานอาจล่าช้าหรือไม่ครบถ้วน (สำนักงานกิจการยุติธรรม, 2565) ประกอบกับข้อจำกัดด้านเครื่องมือและองค์ความรู้ของเจ้าหน้าที่ ทำให้เกิดปัญหา เช่น การขาดช่วงของห่วงโซ่การครอบครองพยานหลักฐาน และการปนเปื้อนของข้อมูล ซึ่งล้วนส่งผลต่อความน่าเชื่อถือของพยานหลักฐานในชั้นศาล

จากการทบทวนวรรณกรรม พบว่า พยานหลักฐานอิเล็กทรอนิกส์โดยเฉพาะในระบบคลาวด์มีความซับซ้อนและต้องอาศัยมาตรฐานเฉพาะทาง โดยความน่าเชื่อถือของพยานหลักฐานขึ้นอยู่กับกระบวนการเก็บรักษาและการตรวจสอบที่เป็นระบบ รวมถึงการมีส่วนร่วมของผู้เชี่ยวชาญด้านดิจิทัลฟอเรนสิกในการอธิบายหลักฐานต่อศาล (Moussa, 2021) ในระดับนานาชาติ หลายประเทศได้พัฒนากฎหมายและมาตรฐานรองรับพยานหลักฐานอิเล็กทรอนิกส์อย่างเป็นระบบ ขณะที่บางประเทศยังประสบปัญหาด้านความไม่ชัดเจนของกฎหมายและแนวปฏิบัติ ส่งผลให้การบังคับใช้กฎหมายขาดประสิทธิภาพ (Kerr, 2005) นอกจากนี้ แนวคิดด้าน Cloud Forensics ยังชี้ให้เห็นถึงความจำเป็นในการบูรณาการองค์ความรู้ทั้งด้านเทคนิค กฎหมาย และองค์กร เพื่อรองรับความท้าทายของพยานหลักฐานในสภาพแวดล้อมคลาวด์ (Ruan et al., 2011; Martini & Choo, 2012)

จากประเด็นดังกล่าว สะท้อนให้เห็นว่าประเทศไทยยังมีช่องว่างด้านมาตรฐาน แนวปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการเก็บพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะในบริบทของคลาวด์ดิจิทัล การศึกษานี้จึงมุ่งศึกษาถึงแนวทางที่มีประสิทธิภาพในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ให้สอดคล้องกับมาตรฐานทางกฎหมาย ศึกษาบทบาทของเทคโนโลยีสมัยใหม่ ปัญหาและอุปสรรคในการปฏิบัติงาน ตลอดจนเสนอ

แนวทางในการปรับปรุงกฎหมายและมาตรฐานที่เกี่ยวข้อง เพื่อเพิ่มความน่าเชื่อถือของพยานหลักฐานและเสริมประสิทธิภาพของกระบวนการยุติธรรมในประเทศไทยให้สอดคล้องกับบริบทของเทคโนโลยีในปัจจุบัน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวทางที่มีประสิทธิภาพและบทบาทของเทคโนโลยีในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ประเภทคลาวด์ดิจิทัล ให้มีความน่าเชื่อถือและสอดคล้องกับมาตรฐานทางกฎหมายของประเทศไทย
2. เพื่อศึกษาปัญหา อุปสรรค และเสนอแนวทางในการปรับปรุงกฎหมายหรือมาตรฐานที่เกี่ยวข้อง เพื่อให้พยานหลักฐานอิเล็กทรอนิกส์สามารถรับฟังได้ในชั้นศาลอย่างมีประสิทธิภาพและเป็นธรรม

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

กรอบแนวคิดการวิจัยนี้มุ่งอธิบายความสัมพันธ์ของปัจจัยสำคัญที่มีผลต่อความน่าเชื่อถือและการยอมรับพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม โดยประกอบด้วย แนวทางการเก็บพยานหลักฐาน แนวปฏิบัติของเจ้าหน้าที่ และบทบาทของเทคโนโลยีสมัยใหม่ ซึ่งล้วนเป็นองค์ประกอบหลักที่ส่งผลโดยตรงต่อประสิทธิภาพของกระบวนการเก็บพยานหลักฐาน

อย่างไรก็ตาม ความสัมพันธ์ดังกล่าวอาจได้รับผลกระทบจากปัจจัยด้านปัญหาและอุปสรรคในการปฏิบัติงาน อาทิ ความซับซ้อนของเทคโนโลยี ข้อจำกัดทางกฎหมาย และข้อจำกัดด้านศักยภาพของบุคลากร ซึ่งอาจส่งผลให้กระบวนการเก็บพยานหลักฐานขาดความสมบูรณ์หรือความน่าเชื่อถือ ขณะเดียวกัน การพัฒนาในมิติต่าง ๆ ได้แก่ การปรับปรุงกฎหมายที่เกี่ยวข้อง การกำหนดมาตรฐานการปฏิบัติที่เป็นเอกภาพ การพัฒนาศักยภาพของบุคลากร และการเสริมสร้างความร่วมมือระหว่างประเทศ จะมีบทบาทสำคัญในการสนับสนุนและยกระดับกระบวนการเก็บพยานหลักฐานให้มีความถูกต้อง โปร่งใส และสามารถตรวจสอบได้ อันจะนำไปสู่การเพิ่มความน่าเชื่อถือของพยานหลักฐาน และการยอมรับในชั้นศาลอย่างมีประสิทธิภาพ

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ มีวัตถุประสงค์เพื่อศึกษากระบวนการและแนวทางการเก็บพยานหลักฐานอิเล็กทรอนิกส์ประเภทคลาวด์ดิจิทัลในบริบทของกระบวนการยุติธรรม ซึ่งเป็นประเด็นที่มีความซับซ้อนและเกี่ยวข้องกับทั้งมิติทางกฎหมาย เทคโนโลยี และการปฏิบัติงานของเจ้าหน้าที่ในหลายภาคส่วน การออกแบบการวิจัยจึงมุ่งเน้นการทำความเข้าใจเชิงลึกจากประสบการณ์ของผู้ปฏิบัติงานจริง ควบคู่กับการสังเคราะห์องค์ความรู้จากเอกสารที่เกี่ยวข้อง โดยใช้การวิเคราะห์ข้อมูลด้วยวิธีการวิเคราะห์เนื้อหา ซึ่งนำไปสู่การจัดโครงสร้างข้อมูลในรูปแบบ Coding–Category–Theme–Quotation ตามที่ปรากฏในผลการวิจัย

การดำเนินการวิจัยประกอบด้วยการวิจัยเชิงเอกสารและการวิจัยภาคสนาม โดยในส่วนของ การวิจัยเชิงเอกสาร ผู้วิจัยได้ศึกษาข้อมูลจากหนังสือ บทความวิจัย รายงานทางวิชาการ กฎหมาย และแนวปฏิบัติที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ โดยมุ่งเน้นประเด็นเกี่ยวกับแนวคิดพยานหลักฐานอิเล็กทรอนิกส์ กระบวนการเก็บรวบรวมพยานหลักฐานดิจิทัลในระบบคลาวด์ มาตรฐานสากลด้านดิจิทัลฟอเรนซิก และปัญหาในการบังคับใช้กฎหมายในบริบทเทคโนโลยีสมัยใหม่ นอกจากนี้ยังได้วิเคราะห์กฎหมายไทยที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อใช้เป็นกรอบแนวคิดในการวิจัยและพัฒนาแนวคำถามสำหรับการสัมภาษณ์เชิงลึก ในการวิจัยภาคสนามใช้วิธีการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured Interview) เพื่อเปิดโอกาสให้ผู้ให้ข้อมูลสามารถสะท้อนประสบการณ์และมุมมองจากการปฏิบัติงานจริงได้อย่างอิสระ ภายใต้กรอบคำถามที่ครอบคลุมประเด็นสำคัญ ได้แก่ แนวทางการเก็บพยานหลักฐานอิเล็กทรอนิกส์ แนวปฏิบัติของเจ้าหน้าที่ บทบาทของเทคโนโลยีสมัยใหม่ ปัญหาและอุปสรรคในการปฏิบัติงาน และแนวทางในการพัฒนาและปรับปรุงมาตรฐานการปฏิบัติ ผู้ให้ข้อมูล

สำคัญถูกคัดเลือกโดยวิธีการเลือกแบบเจาะจง จำนวน 10 คน โดยกำหนดคุณสมบัติว่าต้องมีประสบการณ์ในงานที่เกี่ยวข้องไม่น้อยกว่า 5 ปี ประกอบด้วย เจ้าหน้าที่ตำรวจ ผู้เชี่ยวชาญด้านดิจิทัลฟอเรนสิก พนักงานอัยการ และผู้พิพากษา เพื่อให้ครอบคลุมมุมมองจากทุกภาคส่วนในกระบวนการยุติธรรม การเก็บข้อมูลดำเนินการจนถึงจุดอิ่มตัวของข้อมูล ซึ่งเป็นช่วงที่ข้อมูลมีลักษณะซ้ำกันและไม่พบประเด็นใหม่เพิ่มเติม

ตารางที่ 1 รายละเอียดและจำนวนผู้ให้ข้อมูล

กลุ่มผู้ให้ข้อมูล	จำนวน (คน)
เจ้าหน้าที่ตำรวจ (สายสืบสวน/พิสูจน์หลักฐาน)	4
ผู้เชี่ยวชาญด้านดิจิทัลฟอเรนสิก	2
พนักงานอัยการ	2
ผู้พิพากษา	2
รวม	10

เครื่องมือที่ใช้ในการวิจัยคือแบบสัมภาษณ์กึ่งโครงสร้าง ซึ่งพัฒนาจากการทบทวนวรรณกรรม โดยมีลักษณะเป็นคำถามปลายเปิด การเก็บรวบรวมข้อมูลดำเนินการโดยการสัมภาษณ์แบบตัวต่อตัว พร้อมทั้งบันทึกข้อมูลทั้งในรูปแบบการจดบันทึกและการบันทึกเสียง เพื่อให้ได้ข้อมูลที่ครบถ้วนและสามารถตรวจสอบย้อนหลังได้ การวิเคราะห์ข้อมูลใช้วิธีการวิเคราะห์เนื้อหา โดยเริ่มจากการถอดความคำสัมภาษณ์แบบคำต่อคำ จากนั้นทำการกำหนดรหัสแนวคิด (Coding) จากข้อมูลจริง และจัดกลุ่มรหัสเป็นหมวดหมู่ (Category) ก่อนจะสังเคราะห์เป็นประเด็นหลัก (Theme) พร้อมเชื่อมโยงกับคำให้สัมภาษณ์ (Quotation) เพื่อสนับสนุนข้อค้นพบ ทั้งนี้ การวิเคราะห์ดำเนินการอย่างเป็นระบบและมีการเปรียบเทียบข้อมูลระหว่างกลุ่มผู้ให้ข้อมูลเพื่อเพิ่มความน่าเชื่อถือของผลการวิจัย และเพื่อให้ผลการวิจัยมีความน่าเชื่อถือ ผู้วิจัยได้ใช้การตรวจสอบข้อมูลแบบสามเส้า โดยเปรียบเทียบข้อมูลจากเอกสารและผู้ให้ข้อมูลจากหลายกลุ่มอาชีพ รวมทั้งใช้คำให้สัมภาษณ์จริงประกอบการตีความ นอกจากนี้ ยังมีการบันทึกขั้นตอนการวิจัยอย่างเป็นระบบเพื่อให้สามารถตรวจสอบได้ในภายหลัง ในการดำเนินการวิจัยครั้งนี้เป็นไปตามหลักจริยธรรมการวิจัยในมนุษย์ โดยผู้วิจัยได้ขอความยินยอมจากผู้ให้ข้อมูลก่อนการสัมภาษณ์ เคารพสิทธิและศักดิ์ศรีของผู้ให้ข้อมูล และไม่เปิดเผยตัวตนของผู้ให้ข้อมูล ทั้งนี้ ข้อมูลทั้งหมดถูกนำมาใช้เพื่อวัตถุประสงค์ทางวิชาการเท่านั้น

ผลการวิจัย

จากการศึกษาวิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยการวิเคราะห์เอกสารร่วมกับการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญในกระบวนการยุติธรรม จำนวน 10 ราย ได้แก่ เจ้าหน้าที่ตำรวจ ผู้เชี่ยวชาญด้านดิจิทัลฟอเรนสิก พนักงานอัยการ และผู้พิพากษา ผลการวิจัยถูกวิเคราะห์ด้วยวิธีการวิเคราะห์เนื้อหา และสังเคราะห์

เชิงระบบในรูปแบบ Coding–Theme–Quotation สามารถจัดกลุ่มข้อค้นพบออกเป็น 5 ประเด็นหลัก ดังแสดงในตารางที่ 3 การวิเคราะห์เนื้อหา

ตารางที่ 2 การวิเคราะห์เนื้อหา

Theme (ประเด็นหลัก)	Category (หมวดหมู่)	Code	Quotation (ตัวอย่างคำให้สัมภาษณ์)
1.แนวทางการเก็บพยานหลักฐานที่มีประสิทธิภาพ	ความชอบด้วยกฎหมาย	LEG-01	“พยานหลักฐานต้องได้มาโดยชอบ มิฉะนั้นศาลอาจไม่รับฟัง”
	ความสมบูรณ์ของข้อมูล	INT-01	“ต้องพิสูจน์ได้ว่าข้อมูลไม่ถูกแก้ไข”
	การตรวจสอบย้อนกลับ	TRC-01	“ต้องบันทึกว่าใครเป็นผู้ยึด เวลา สถานที่”
	มาตรฐานสากล	STD-01	“ต้องอ้างอิงมาตรฐานสากลเพื่อให้ศาลเชื่อถือ”
	กระบวนการเก็บข้อมูล	PRC-01	“ใช้หลัก digital forensics แบบ read-only”
2. แนวปฏิบัติของเจ้าหน้าที่	การบันทึกขั้นตอน	DOC-01	“ต้องบันทึกทุกขั้นตอนอย่างละเอียด”
	เครื่องมือที่ใช้	TOL-01	“ใช้เครื่องมือที่ได้รับการยอมรับ”
	การควบคุมความเสี่ยง	RSK-01	“ตัดการเชื่อมต่ออินเทอร์เน็ตเพื่อป้องกันแก้ไขข้อมูล”
	ความแม่นยำของข้อมูล	TEC-01	“ช่วยเพิ่มความแม่นยำและลดความผิดพลาด”
	การจัดการข้อมูลขนาดใหญ่	TEC-02	“สามารถจัดการข้อมูลจาก cloud ได้”
3.บทบาทของเทคโนโลยีสมัยใหม่	ความปลอดภัยข้อมูล	SEC-01	“มีการใช้ hash เพื่อยืนยันข้อมูล”
	การตรวจสอบย้อนกลับ	LOG-01	“ต้องมี log file แสดงกิจกรรมทั้งหมด”
	ความน่าเชื่อถือของหลักฐาน	REL-01	“ศาลยังต้องพึ่งพาผู้เชี่ยวชาญ”
4. ปัญหาและอุปสรรค	เทคโนโลยีซับซ้อน	TEC-03	“ข้อมูลถูกเข้ารหัสทำให้เข้าถึงยาก”
	ข้อจำกัดกฎหมาย	LAW-01	“ข้อมูลอยู่ต่างประเทศทำให้ล่าช้า”
	การลบข้อมูล	TEC-04	“ผู้ต้องหาลบข้อมูลผ่าน cloud ได้ทันที”
	ขาดผู้เชี่ยวชาญ	HUM-01	“เจ้าหน้าที่บางคนอธิบายศาลไม่ได้”

ตารางที่ 2 (ต่อ)

Theme (ประเด็นหลัก)	Category (หมวดหมู่)	Code	Quotation (ตัวอย่างคำให้สัมภาษณ์)
5.แนวทางพัฒนาและปรับปรุง	การพัฒนากฎหมาย	LAW-02	“ควรมีกฎหมายเฉพาะด้านพยานหลักฐานดิจิทัล”
	มาตรฐานกลาง	STD-02	“ควรมีแนวปฏิบัติเดียวกันทั่วประเทศ”
	การพัฒนาบุคลากร	HUM-02	“ต้องอบรมผู้พิพากษาและอัยการด้านดิจิทัล”
	ความร่วมมือระหว่างประเทศ	INT-01	“ควรมีช่องทางขอข้อมูลที่รวดเร็วขึ้น”
	ความร่วมมือเอกชน	TEC-05	“ควรทำ MOU กับผู้ให้บริการคลาวด์”

จากการวิจัยเชิงเนื้อหาทำให้ได้ข้อค้นพบเชิงประจักษ์ที่สามารถสังเคราะห์เป็นประเด็นสำคัญได้ 5 ประการ ดังต่อไปนี้

1) แนวทางที่มีประสิทธิภาพในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ที่สอดคล้องกับมาตรฐานทางกฎหมายของประเทศไทย พบว่า การเก็บพยานหลักฐานจำเป็นต้องดำเนินการอย่างเป็นระบบ มีขั้นตอนที่ชัดเจน และสามารถตรวจสอบย้อนกลับได้ โดยต้องคำนึงถึงหลักสำคัญ ได้แก่ ความชอบด้วยกฎหมายในการได้มา ความครบถ้วนสมบูรณ์ของข้อมูล และความน่าเชื่อถือของกระบวนการเก็บรักษา ทั้งนี้ การอ้างอิงกฎหมายที่เกี่ยวข้อง เช่น ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ มีบทบาทสำคัญในการกำหนดกรอบการดำเนินงาน นอกจากนี้ การใช้หลักการทางนิติวิทยาศาสตร์ดิจิทัล เช่น การตรวจสอบค่าแฮช (Hash Value) และการจัดทำห่วงโซ่การครอบครองพยานหลักฐาน เป็นปัจจัยสำคัญที่ช่วยยืนยันความถูกต้องแท้จริงของข้อมูลและเพิ่มน้ำหนักในการรับฟังในชั้นศาล

2) แนวปฏิบัติในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ของเจ้าหน้าที่ พบว่า การปฏิบัติงานที่ถูกต้องตามหลักวิชาการและมาตรฐานสากลจะช่วยเพิ่มความน่าเชื่อถือของพยานหลักฐานและลดข้อโต้แย้งในกระบวนการพิจารณาคดี โดยเจ้าหน้าที่ต้องมีการกำหนดบทบาทหน้าที่อย่างชัดเจน ใช้เครื่องมือที่เหมาะสมและได้รับการยอมรับ บันทึกข้อมูลทุกขั้นตอนอย่างละเอียด รวมถึงดำเนินการภายใต้หลักการไม่กระทบต่อข้อมูลต้นฉบับ เช่น การเก็บข้อมูลแบบ Read-only การทำสำเนาข้อมูล และการจัดเก็บอุปกรณ์ในสภาพที่ปลอดภัย ทั้งนี้ การดำเนินการดังกล่าวจะช่วยสะท้อนความโปร่งใสและสามารถตรวจสอบได้ในทุกขั้นตอนของกระบวนการ

3) บทบาทของอุปกรณ์เทคโนโลยีสมัยใหม่ในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ พบว่า เทคโนโลยีมีบทบาทสำคัญอย่างยิ่งในการเพิ่มประสิทธิภาพของการรวบรวมและวิเคราะห์พยานหลักฐาน โดยเฉพาะเครื่องมือด้านดิจิทัลฟอเรนสิกที่สามารถจัดการข้อมูลขนาดใหญ่จากระบบคลาวด์ได้อย่างมีประสิทธิภาพ ช่วยลดความเสี่ยงของการสูญหายหรือการเปลี่ยนแปลงของข้อมูล อุปกรณ์ที่ใช้ต้องมี

คุณสมบัติในการรักษาความถูกต้องของข้อมูล เช่น การบันทึกค่าแฮช การเข้ารหัสข้อมูล การควบคุมสิทธิ์ การเข้าถึง และการบันทึกข้อมูลการใช้งาน อย่างครบถ้วน รวมทั้งควรผ่านการรับรองตามมาตรฐานสากล เพื่อให้พยานหลักฐานมีความน่าเชื่อถือและสามารถใช้ในบริบทของคดีระหว่างประเทศได้

4) สภาพปัญหาและอุปสรรคในการเก็บพยานหลักฐานอิเล็กทรอนิกส์ให้สามารถรับฟังได้ในชั้นศาล พบว่า ปัญหาหลักยังคงอยู่ที่ความน่าเชื่อถือของพยานหลักฐานและกระบวนการพิสูจน์ โดยเฉพาะในกรณีที่ข้อมูลสามารถถูกแก้ไข เปลี่ยนแปลง หรือลบได้ง่าย นอกจากนี้ ยังพบข้อจำกัดด้านเทคโนโลยี เช่น การเข้ารหัสข้อมูลขั้นสูง และการจัดเก็บข้อมูลในระบบคลาวด์ของผู้ให้บริการต่างประเทศ ซึ่งก่อให้เกิดปัญหาด้านเขตอำนาจศาลและความล่าช้าในการขอความร่วมมือระหว่างประเทศ อีกทั้งยังมีข้อจำกัดด้านความรู้และความเชี่ยวชาญของผู้ปฏิบัติงาน รวมถึงความเข้าใจของศาลต่อพยานหลักฐานอิเล็กทรอนิกส์ ส่งผลให้การประเมินน้ำหนักพยานหลักฐานยังต้องพึ่งพาพยานผู้เชี่ยวชาญเป็นสำคัญ

5) แนวทางในการปรับปรุงและพัฒนากฎหมายหรือมาตรฐานที่เกี่ยวข้อง พบว่า ควรมีการกำหนดกฎหมายเฉพาะเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์เพื่อสร้างความชัดเจนและเป็นเอกภาพในทางปฏิบัติ รวมถึงการปรับปรุงกฎหมายที่มีอยู่ให้รองรับเทคโนโลยีสมัยใหม่ โดยเฉพาะพยานหลักฐานจากระบบ คลาวด์ นอกจากนี้ ควรกำหนดมาตรฐานกลางในการเก็บ รักษา และวิเคราะห์พยานหลักฐานดิจิทัลที่สอดคล้องกับมาตรฐานสากล ตลอดจนพัฒนาศักยภาพของบุคลากรในกระบวนการยุติธรรม และส่งเสริมความร่วมมือระหว่างประเทศ รวมถึงความร่วมมือกับผู้ให้บริการเทคโนโลยี เพื่อให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ

อภิปรายผลการวิจัย

ผลการวิจัยเชิงวิเคราะห์เนื้อหา (Coding–Theme–Quotation) สะท้อนให้เห็นอย่างชัดเจนว่า ความน่าเชื่อถือ และ ความสมบูรณ์ของข้อมูล เป็นแกนหลักของการยอมรับพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม โดยเฉพาะในบริบทของระบบคลาวด์ที่มีความซับซ้อนและกระจายตัวสูง ข้อค้นพบดังกล่าวสอดคล้องกับแนวคิดร่วมสมัยด้านดิจิทัลฟอเรนซิกที่เน้น ความถูกต้องตามหลักนิติวิทยาศาสตร์ และความสามารถในการตรวจสอบยืนยันได้ เป็นเงื่อนไขสำคัญของการรับฟังพยานหลักฐาน (Quick & Choo, 2014; Kebande & Venter, 2018) ซึ่งขยายกรอบเดิมของมาตรฐานสากล เช่น ISO/IEC 27037 ที่เน้นการรักษาสภาพเดิมของพยานหลักฐานและความสามารถในการตรวจสอบย้อนกลับ ให้ครอบคลุมบริบทคลาวด์มากยิ่งขึ้น

ประเด็นหลักที่ 1 (LEG-01, INT-01, TRC-01, STD-01) แสดงให้เห็นว่าการได้มาซึ่งพยานหลักฐานต้องชอบด้วยกฎหมาย ควบคู่กับการรักษาห่วงโซ่การครอบครองพยานหลักฐาน เป็นปัจจัยชี้ขาดในการเพิ่มน้ำหนักพยานหลักฐานในชั้นศาล โดยเฉพาะการตรวจสอบย้อนกลับได้ในทุกขั้นตอน สอดคล้องกับการศึกษาของ Scanlon และ Battistoni (2020) ที่ระบุว่าแหล่งที่มา และ ความสามารถในการตรวจสอบย้อนกลับของข้อมูลในระบบคลาวด์เป็นกลไกสำคัญในการสร้างความเชื่อมั่นของศาล นอกจากนี้ Alenezi et al. (2023)

ยังเสนอว่าการบูรณาการ metadata และร่องรอยการตรวจสอบ สามารถช่วยยืนยันความถูกต้องของหลักฐานในระดับที่ตรวจสอบได้เชิงนิติวิทยาศาสตร์

ประเด็นหลักที่ 2 เกี่ยวกับแนวปฏิบัติของเจ้าหน้าที่ (PRC-01, DOC-01, TOL-01, RSK-01) ผลการวิจัยชี้ให้เห็นว่า การดำเนินการตามหลัก forensic soundness เช่น การเก็บข้อมูลแบบ read-only การทำ forensic imaging และการบันทึกขั้นตอนอย่างละเอียด เป็นกลไกสำคัญในการลดข้อโต้แย้งในชั้นศาล ซึ่งสอดคล้องกับงานของ Horsman (2021) ที่ชี้ว่าความโปร่งใสของกระบวนการ และการจัดทำบันทึกเชิงระบบ มีผลโดยตรงต่อการประเมินน้ำหนักพยานหลักฐาน นอกจากนี้ Casey et al. (2022) ยังเน้นว่าความสามารถในการทำซ้ำของกระบวนการตรวจพิสูจน์ เป็นองค์ประกอบสำคัญที่ทำให้พยานหลักฐานดิจิทัลได้รับการยอมรับในระดับสากล

ประเด็นหลักที่ 3 บทบาทของเทคโนโลยีสมัยใหม่ (TEC-01, TEC-02, SEC-01, LOG-01) ผลการวิจัยยืนยันว่าเทคโนโลยีดิจิทัลฟอเรนสิกมีบทบาทสำคัญในการเพิ่มประสิทธิภาพของการจัดการพยานหลักฐาน โดยเฉพาะในบริบทของคลาวด์ที่มีข้อมูลขนาดใหญ่ และมีความซับซ้อนสูง การใช้เทคนิค เช่น Hash Function, Encryption และ Log Analysis ช่วยยืนยันความถูกต้องและแหล่งที่มาของข้อมูล ซึ่งสอดคล้องกับการศึกษาของ Kemande และ Venter (2021) ที่เสนอกรอบการเตรียมความพร้อมด้านการตรวจพิสูจน์หลักฐานดิจิทัลในระบบคลาวด์ ว่าการเตรียมระบบให้สามารถเก็บ log และ metadata อย่างเป็นระบบตั้งแต่ต้น จะช่วยเพิ่มประสิทธิภาพในการสืบสวน อย่างไรก็ตาม ผลการวิจัยนี้ยังชี้ให้เห็นว่า เทคโนโลยีเพียงอย่างเดียวไม่เพียงพอ หากขาดการบูรณาการกับกฎหมายและกระบวนการยุติธรรม

ประเด็นหลักที่ 4 ปัญหาและอุปสรรค (REL-01, TEC-03, LAW-01, TEC-04, HUM-01) ผลการวิจัยสะท้อนให้เห็นความท้าทายเชิงโครงสร้างของการจัดการพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะประเด็นความน่าเชื่อถือของหลักฐาน การเข้ารหัสข้อมูล และข้อจำกัดด้านเขตอำนาจศาล ซึ่งสอดคล้องกับ Ruan et al. (2011) ที่เสนอว่า Cloud Forensics มีความซับซ้อนใน 3 มิติ ได้แก่ มิติทางเทคนิค กฎหมาย และองค์กร นอกจากนี้ การพึ่งพาพยานผู้เชี่ยวชาญในการอธิบายหลักฐานต่อศาลยังสอดคล้องกับ Moussa (2021) ที่ระบุว่าดุลพินิจของศาลขึ้นอยู่กับความน่าเชื่อถือของกระบวนการและความสามารถในการอธิบายหลักฐานของผู้เชี่ยวชาญ

อีกประเด็นหนึ่งที่มีความสำคัญ คือข้อจำกัดด้านความร่วมมือระหว่างประเทศ (INT-01) ซึ่งเป็นอุปสรรคต่อการเข้าถึงข้อมูลจากผู้ให้บริการคลาวด์ในต่างประเทศ โดยผลการวิจัยสอดคล้องกับแนวทางของ Europol (2022) และ INTERPOL (2023) ที่เน้นย้ำถึงความจำเป็นของการพัฒนากรอบความร่วมมือข้ามพรมแดน และการใช้เครื่องมือทางกฎหมายระหว่างประเทศ เช่น ความช่วยเหลือทางกฎหมายระหว่างประเทศ (MLAT) หรือกรอบกฎหมายลักษณะเดียวกับ CLOUD Act เพื่อเร่งรัดและเพิ่มประสิทธิภาพในการเข้าถึงพยานหลักฐานดิจิทัลในบริบทสากล

ประเด็นหลักที่ 5 แนวทางพัฒนา (LAW-02, STD-02, HUM-02, INT-01, TEC-05) ผลการวิจัยชี้ให้เห็นว่า การพัฒนาแบบบูรณาการ เป็นแนวทางที่จำเป็น โดยเฉพาะ การตรากฎหมายเฉพาะด้านพยานหลักฐานดิจิทัล การกำหนดมาตรฐานกลางระดับชาติ และ การพัฒนาศักยภาพบุคลากรในกระบวนการยุติธรรม ซึ่งสอดคล้องกับแนวคิดเรื่อง การบริหารจัดการและกำกับดูแลพยานหลักฐานดิจิทัลอย่างเป็นระบบของ (Kohn et al., 2013) ที่เสนอให้มีการกำกับดูแลพยานหลักฐานดิจิทัลอย่างเป็นระบบทั้งในเชิงนโยบายและการปฏิบัติ นอกจากนี้ การสร้างความร่วมมือกับภาคเอกชน (CSPs) ยังสอดคล้องกับแนวโน้มสากลที่เน้นความร่วมมือเชิงหุ้นส่วนระหว่างภาครัฐและภาคเอกชนในการจัดการอาชญากรรมไซเบอร์

โดยสังเคราะห์ในภาพรวม ผลการวิจัยสามารถอธิบายได้ภายใต้ กรอบแนวคิดเชิงบูรณาการของนิติวิทยาศาสตร์ดิจิทัลในระบบคลาวด์ (Ruan et al., 2011) ที่ประกอบด้วย 3 มิติหลัก ได้แก่ (1) มิติทางเทคนิค (Technology) เกี่ยวข้องกับการใช้เครื่องมือและมาตรฐานดิจิทัลฟอเรนสิก (2) มิติทางกฎหมาย (Legal) เกี่ยวข้องการรับรองและกำหนดหลักเกณฑ์การใช้พยานหลักฐาน และ (3) มิติด้านองค์กรและบุคลากร (Organizational/Human) เกี่ยวข้องกับความเชี่ยวชาญและการประสานงานทั้งสามมิตินี้มีความเชื่อมโยงกันอย่างใกล้ชิด และหากขาดมิติใดมิติหนึ่ง จะส่งผลต่อความน่าเชื่อถือของพยานหลักฐานโดยรวม

ดังนั้น การยกระดับการเก็บพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยให้สอดคล้องกับมาตรฐานระดับสากล จำเป็นต้องดำเนินการแบบองค์รวม โดยบูรณาการการพัฒนากฎหมาย เทคโนโลยี และทรัพยากรมนุษย์ควบคู่กัน ซึ่งจะช่วยเพิ่มประสิทธิภาพของกระบวนการยุติธรรม และรองรับอาชญากรรมทางเทคโนโลยีที่มีความซับซ้อนในยุคดิจิทัลได้อย่างยั่งยืน

สรุปผลการวิจัย

ผลการวิจัยเรื่องนี้ชี้ให้เห็นว่า การยอมรับพยานหลักฐานในกระบวนการยุติธรรมขึ้นอยู่กับความน่าเชื่อถือของกระบวนการ และ ความสมบูรณ์ของข้อมูล เป็นสำคัญ โดยต้องดำเนินการภายใต้หลักความชอบด้วยกฎหมาย การรักษาห่วงโซ่การครอบครองพยานหลักฐาน และความสามารถในการตรวจสอบย้อนกลับได้ ในเชิงปฏิบัติ การดำเนินงานตามหลักนิติวิทยาศาสตร์ดิจิทัล เช่น การเก็บข้อมูลแบบไม่กระทบต้นฉบับ การทำสำเนาข้อมูล และการบันทึกขั้นตอนอย่างเป็นระบบ มีบทบาทสำคัญในการเพิ่มความโปร่งใสและลดข้อโต้แย้งในชั้นศาล ขณะเดียวกัน การใช้เทคโนโลยี เช่น การตรวจสอบค่าแฮช การเข้ารหัส และระบบบันทึกเหตุการณ์ ช่วยเสริมความถูกต้องและความน่าเชื่อถือของพยานหลักฐาน อย่างไรก็ตาม ยังพบข้อจำกัดสำคัญ ได้แก่ ความซับซ้อนของเทคโนโลยี ปัญหาด้านเขตอำนาจศาลในกรณีข้อมูลข้ามพรมแดน และข้อจำกัดด้านความเชี่ยวชาญของบุคลากร รวมถึงความล่าช้าในการเข้าถึงข้อมูลจากผู้ให้บริการต่างประเทศ

ดังนั้น การยกระดับการจัดการพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยควรมุ่งเน้นการพัฒนาแบบบูรณาการทั้งด้านกฎหมาย เทคโนโลยี และทรัพยากรมนุษย์ เพื่อรองรับความท้าทายของอาชญากรรมในยุคดิจิทัลอย่างมีประสิทธิภาพ

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติ

ควรมีการพัฒนากฎหมายเฉพาะด้านพยานหลักฐานดิจิทัลหรือปรับปรุงกฎหมายที่เกี่ยวข้องให้รองรับการจัดการพยานหลักฐานในระบบคลาวด์อย่างชัดเจน เพื่อลดความคลุมเครือในการตีความในชั้นศาล ควบคู่กับการกำหนดมาตรฐานกลางระดับชาติในการเก็บ รักษา และวิเคราะห์พยานหลักฐานดิจิทัลให้สอดคล้องกับมาตรฐานสากล เพื่อสร้างความเป็นเอกภาพในการปฏิบัติงาน

นอกจากนี้ ควรส่งเสริมการพัฒนาศักยภาพบุคลากรในกระบวนการยุติธรรมอย่างต่อเนื่อง เพื่อเพิ่มความเชี่ยวชาญด้านดิจิทัลฟอเรนสิก รวมถึงพัฒนากลไกความร่วมมือระหว่างประเทศเพื่อให้สามารถเข้าถึงข้อมูลข้ามพรมแดนได้อย่างรวดเร็ว และสนับสนุนความร่วมมือระหว่างภาครัฐกับผู้ให้บริการคลาวด์ในการกำหนดแนวปฏิบัติที่มีประสิทธิภาพและเป็นมาตรฐานเดียวกัน.

2. ข้อเสนอแนะสำหรับการวิจัยในอนาคต

ควรมีการศึกษาวิจัยเชิงเปรียบเทียบกฎหมายและแนวปฏิบัติของต่างประเทศ รวมถึงการพัฒนาโมเดลหรือกรอบการดำเนินงาน สำหรับการจัดการพยานหลักฐานในระบบคลาวด์ที่เหมาะสมกับบริบทของประเทศไทย ตลอดจนการวิจัยเชิงปริมาณเพื่อประเมินประสิทธิภาพของแนวปฏิบัติที่นำไปใช้จริงในกระบวนการยุติธรรม

เอกสารอ้างอิง

ไทยรัฐออนไลน์. (2567). รู้ทันกลลวงมิจฉาชีพ 2567 ใช้ AI ก่ออาชญากรรมออนไลน์ เช็กก่อนตกเป็นเหยื่อ.

https://www.thairath.co.th/news/society/2749252#google_vignette

พิชศาล พันธุ์วัฒนา. (2562). ความน่าเชื่อถือในการนำเอกสารอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐาน.

วารสารวิชาการอาชีวศึกษาและนิติวิทยาศาสตร์, 5(1), 142–161.

วรินทร์า ศรีวิชัย. (2563). การตรวจพิสูจน์พยานหลักฐานดิจิทัลกับคดีเกี่ยวกับความมั่นคง. *CMU Journal of Law and Social Sciences*, 13(1), 78–101.

สำนักงานกิจการยุติธรรม. (2565). รายงานสถานการณ์อาชญากรรมทางเทคโนโลยีในประเทศไทย.

<https://www.oja.go.th/justicedata/>

Carrier, B., & Spafford, E. H. (2004). An event-based digital forensic investigation framework. *Digital Investigation*, 1(2), 133–147.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Casey, E., Ferraro, M., and Nguyen, L. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences*, 54(6), 1353–1364. <https://doi.org/10.1111/j.1556-4029.2009.01150.x>

- Horsman, G. (2021). Contemporaneous notes for digital forensic examinations. *Forensic Science International: Digital Investigation*, 37, Article 301173. <https://doi.org/10.1016/j.fsidi.2021.301173>
- Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review*, 105(1), 279–318.
- Kohn, M. D., Eloff, M. M., and Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Martini, B., and Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), 71–80.
- Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11, Article 20. <https://doi.org/10.1186/s41935-021-00234-6>
- Quick, D., and Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), 273–294. <https://doi.org/10.1016/j.diin.2014.09.002>
- Ruan, K., Carthy, J., Kechadi, T., and Crosbie, M. (2011). Cloud forensics: An overview. In *Advances in digital forensics VII* (pp. 35–46). Springer.