การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์
A Study of Guidelines in Digital Forensic Evidence Examination

จิตชนก อินถามา และ วงศ์ยศ เกิดศรี
คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

Jitchanok Inthama and Wongyos Keardsri
Faculty of Forensic Science, Royal Police Cadet Academy

Received January 25, 2021 | Revised May 19, 2021 | Accepted June 13, 2021

บทคัดย่อ

ปัจจุบันอุปกรณ์ดิจิทัลมีการใช้งานกันอย่างแพร่หลายในชีวิตประจำวันของมนุษย์ทำให้อัตราการเกิดเหตุอาชญากรรมบนระบบออนไลน์มีเพิ่มมากยิ่งขึ้น ดังนั้นขั้นตอนหรือแนวทางการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับอุปกรณ์ดิจิทัลจึงต้องมีความซับซ้อนและความน่าเชื่อถือสูงขึ้นเช่นเดียวกัน งานวิจัยเรื่องนี้จึงมีวัตถุประสงค์เพื่อศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์ของประเทศไทย โดยเป็นการศึกษาเชิงคุณภาพซึ่งแบ่งออกเป็น 2 ส่วน ส่วนแรกเป็นการศึกษาเอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานทั้งภายในและภายนอกประเทศจำนวน 4 หน่วยงาน ได้แก่ 1) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ 2) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ 3) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล และ 4) องค์การมาตรฐานสากล ส่วนที่สองเป็นการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลหลักในหน่วยงานทางด้านนิติวิทยาศาสตร์ของประเทศไทยจำนวน 4 หน่วยงาน ได้แก่ 1) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี 2) สถาบันนิติวิทยาศาสตร์ 3) กรมสอบสวนคดีพิเศษ และ 4) สำนักงานพิสูจน์หลักฐานตำรวจ ผลการศึกษาเอกสารสามารถสรุปขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลออกเป็น 9 ขั้นตอนและ ผลการสัมภาษณ์ผู้ให้ข้อมูลหลักทำให้เห็นถึงสภาพปัญหาในขั้นตอนการตรวจพิสูจน์หลักฐาน เช่น การไม่เข้าใจถึงวัตถุประสงค์ในการส่งตรวจพิสูจน์และการขาดองค์ความรู้และความเชี่ยวชาญของผู้ปฏิบัติงาน งานวิจัยเรื่องนี้สามารถนำไปใช้พัฒนาเป็นมาตรฐานการตรวจพิสูจน์หลักฐานทางดิจิทัลของประเทศไทยได้ในอนาคต

คำสำคัญ: ตรวจพิสูจน์หลักฐาน, หลักฐานทางดิจิทัล, แนวทาง

Abstract

Nowadays, digital devices have been widely used in the daily life of humans. Consequently, the number of cybercrimes has been increasing significantly. Moreover, the

processes and methods of dealing with forensic evidence examination involving digital devices must have more complexity and credibility.

The purpose of this research was to study the guidelines which were used in the digital forensic evidence examination in Thailand. The study, qualitative research, was divided into two sections. The first one was to conduct documentary research related to guidelines of digital forensic evidence examination of four internal and external agencies, namely 1) Electronic Transactions Development Agency (ETDA), 2) National Institute of Standards and Technology (NIST), 3) Scientific Working Group on Digital Evidence (SWGDE), and 4) International Organization for Standardization (ISO). The other part was the in-depth interviews. The interview data was collected from the key informants who currently work in forensic science agencies in Thailand, namely 1) Technology Crime Suppression Division 2) Central Institute of Forensic Science 3) Department of Special Investigation (DSI) and 4) Office of Police Forensic Science.

The results collected from the documentary research show that there are nine steps of the digital forensic evidence examination. Also, the results obtained from the interview reveal the problems which occurred during examining the forensic evidence such as lack of understanding the purpose of sending the evidence to the digital forensic laboratory and lack of professional expertise in the area of forensics. This research could be the standard for developing the digital forensic evidence examination in Thailand in the foreseeable future.

Keywords: Forensic Examination, Digital Evidence, Guideline

บทนำ

การดำเนินชีวิตของผู้คนในปัจจุบันมักมีเครือข่ายและอินเทอร์เน็ตเข้ามามีส่วนเกี่ยวข้องเกือบทุกช่วงเวลา ไม่ว่าจะเป็นการสื่อสารผ่านเครือข่ายโทรศัพท์มือถือ เช่น การโทรเข้าและออก เป็นต้น การติดต่อสื่อสารผ่านอินเทอร์เน็ตหรือวายฟาย (Wi-Fi) เช่น การติดต่อธุรกิจผ่านทางอีเมล (E-Mail) การติดต่อสื่อสารผ่านทางแอปพลิเคชัน เช่น ไลน์ (LINE) เฟซบุ๊ก (Facebook) วอทแอป (WhatsApp) เป็นต้น การซื้อขายสินค้าออนไลน์ผ่านแอปพลิเคชัน เช่น เฟซบุ๊ก (Facebook) อินสตาแกรม (Instagram) ช้อปปี้ (Shopee) และ ลาซาด้า (Lazada) เป็นต้น การทำธุรกรรมทางการเงินจากเดิมที่ต้องนำสมุดบัญชีไปดำเนินการที่ธนาคารได้เปลี่ยนเป็นการดำเนินการผ่านแอปพลิเคชันของทางธนาคารที่อำนวยความสะดวกให้แก่ลูกค้า โดยทางสำนักงานสถิติแห่งชาติได้ทำการสำรวจผู้ใช้งานคอมพิวเตอร์ อินเทอร์เน็ต และโทรศัพท์มือถือของประชากรชาวไทยในช่วงระยะเวลา 5 ปี ตั้งแต่ปี พ.ศ. 2557 ถึง พ.ศ. 2561 พบว่าผู้ใช้คอมพิวเตอร์มีจำนวนลดลงจาก 23.8 ล้านคน เป็น 17.9 ล้านคน คิดเป็นร้อยละ 28.3 จำนวนผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นจาก 21.8 ล้านคน เป็น 36.0 ล้านคน คิดเป็นร้อยละ 56.8 และจำนวนผู้ใช้โทรศัพท์มือถือเพิ่มขึ้นจาก 48.1 ล้านคน เป็น 56.7 ล้านคน คิดเป็นร้อยละ 89.6 (National Statistical Office, 2018)

จากข้อมูลของสำนักงานสถิติแห่งชาติแสดงให้เห็นถึงการใช้งานอุปกรณ์ดิจิทัลที่เพิ่มมากขึ้น แม้การใช้งานคอมพิวเตอร์จะมีจำนวนที่ลดลง แต่จำนวนผู้ใช้อินเทอร์เน็ตและโทรศัพท์มือถือกลับเพิ่มขึ้นอย่างมาก อาจเพราะโทรศัพท์มือถือเป็นอุปกรณ์ที่สามารถใช้งานได้อย่างครบครันและสะดวกรวดเร็ว อย่างไรก็ตามการเพิ่มขึ้นของจำนวนผู้ใช้อุปกรณ์ดิจิทัลนั้นไม่ได้เป็นผลดีเสียทีเดียว จากการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ถึงร้อยละของผู้ใช้อินเทอร์เน็ต เปรียบเทียบตามกิจกรรมการใช้งานผ่านอินเทอร์เน็ตที่มีการเปลี่ยนแปลงมากที่สุด 5 อันดับแรกในปี พ.ศ. 2560 ถึง พ.ศ. 2561 ได้แก่ อันดับ 1) การอ่านหนังสือทางออนไลน์ เพิ่มขึ้นจากเดิมร้อยละ 30.8 เป็น ร้อยละ 48.3 อันดับที่ 2) การขายสินค้าและบริการ เพิ่มขึ้นจากเดิมร้อยละ 13.7 เป็นร้อยละ 24.5 อันดับที่ 3) การจองโรงแรมหรือที่พัก เพิ่มขึ้นจากเดิมร้อยละ 11.0 เป็นร้อยละ 20.7 อันดับที่ 4) บริการเรียกรถแท็กซี่ เพิ่มขึ้นจากเดิมร้อยละ 4.8 เป็นร้อยละ 12.6 และอันดับที่ 5 การจองหรือซื้อตั๋วชมภาพยนตร์และการแสดงเพิ่มขึ้นจากเดิมร้อยละ 14.6 เป็นร้อยละ 21.7 (Electronic Transactions Development Agency (Public Organization), 2018) โดยการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) พบว่ากิจกรรมการใช้งานผ่านอินเทอร์เน็ตเป็นการใช้งานที่ต้องมีการเปิดเผยข้อมูลส่วนบุคคล ซึ่งถือเป็นความเสี่ยงที่อาจทำให้เกิดเหตุอาชญากรรมขึ้นได้

ปัจจุบันมีเหตุอาชญากรรมทางออนไลน์เพิ่มมากขึ้น โดยทางศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้จัดทำสถิติเกี่ยวกับภัยคุกคามทางไซเบอร์จากการรับแจ้งเหตุภัยคุกคามทางโทรศัพท์และอีเมล ในปี พ.ศ. 2557 ถึง พ.ศ. 2561 พบว่าในปี พ.ศ. 2557 ถึง พ.ศ. 2558 เกิดเหตุภัยคุกคามเพิ่มขึ้นจาก 4,007 เหตุ เป็น 4,371 เหตุ ปีพ.ศ. 2558 ถึง พ.ศ. 2561 เกิดเหตุภัยคุกคามลดลงจาก 4,371 เหตุ เป็น 2,520 เหตุ (Thailand Computer Emergency Response Team (ThaiCERT), 2020) แม้ว่าการเกิดเหตุภัยคุกคามจะมีจำนวนลดลงแต่ยังถือว่าเป็นตัวเลขที่สูงสำหรับการเกิดอาชญากรรม ซึ่งเหตุอาชญากรรมเหล่านี้เกิดจากการไม่ระมัดระวังของผู้ใช้งาน เช่น การเปิดเผยข้อมูลของตนเองผ่านโซเชียลมีเดีย (Social Media) เช่น วัน เดือน ปีเกิด เบอร์โทรศัพท์ หรือที่อยู่ เป็นต้น รวมถึงการที่มีผู้ไม่ประสงค์ดีหรือแฮกเกอร์ทำการหลอกลวงโดยการส่งลิงก์ (Link) หรืออีเมลฟิชชิ่ง (Phishing Mail) หรือเข้าระบบขององค์กรเพื่อนำข้อมูลส่วนตัวของผู้ใช้งานหรือองค์กรไปใช้ในทางที่ไม่ถูกต้อง ซึ่งการกระทำเหล่านี้ทำให้เกิดหลักฐานทางดิจิทัลที่ผู้กระทำได้ทิ้งร่องรอยไว้ ดังทฤษฎีของโลคาร์ด (Locard’s Theory) (Casey, 2011) ซึ่งกล่าวไว้ว่าเมื่อของสองสิ่งหรือมากกว่าสองสิ่งสัมผัสกันจะเกิดการแลกเปลี่ยนวัตถุพยานที่ผิวหน้าซึ่งกันและกันเสมอ และทั้งนี้ อาทิตย์ สุริยะวงศ์กุล กล่าวถึงลักษณะเฉพาะของพยานหลักฐานดิจิทัลว่าลักษณะเฉพาะของพยานหลักฐานดิจิทัลเป็นสิ่งที่สามารถเปลี่ยนแปลงแก้ไขได้ง่ายมากและสามารถทำได้โดยแทบไม่มีร่องรอย (Suriyawongkul, 2015) ดังนั้นในขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลควรมีขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลที่ถูกต้องตามหลักเกณฑ์และผู้ปฏิบัติงานจำเป็นต้องมีความเชี่ยวชาญเพื่อป้องกันการเปลี่ยนแปลงหรือทำลายหลักฐานโดยไม่ตั้งใจและควรมีมาตรฐานขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลกลางภายในประเทศเพื่อให้การตรวจพิสูจน์หลักฐานทางดิจิทัลเป็นไปอย่างมีระบบและทำให้หลักฐานมีความน่าเชื่อถือเมื่อนำไปใช้ในการพิจารณาคดีในชั้นศาล

วัตถุประสงค์

เพื่อศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์

คำถามในการวิจัย

การตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทยควรมีแนวทางปฏิบัติอย่างไร

ทบทวนวรรณกรรม

1. หลักฐานทางดิจิทัล (Working Group for Drafting Digital Forensic Examination Practice Standards, 2016)

มีลักษณะที่เฉพาะเจาะจงกว่าหลักฐานทั่วไป คือ สามารถเปลี่ยนแปลงหรือแก้ไขได้ง่ายและการแก้ไขนั้นอาจไม่เหลือร่องรอยให้ตรวจสอบในภายหลัง ดังนั้น การดำเนินการกับหลักฐานทางดิจิทัลจึงจำเป็นต้องมีกระบวนการจัดเก็บ ตรวจค้น วิเคราะห์และรายงานผลที่ได้มาตรฐานเช่นเดียวกับการดำเนินการกับหลักฐานประเภทอื่น ๆ

2. ลักษณะของหลักฐานทางดิจิทัล (Nassif, 2017)

2.1 เวลา เป็นลักษณะที่สำคัญของหลักฐานทางดิจิทัล เมื่อมีการตรวจพบหลักฐานผู้ตรวจสอบต้องมีการตอบสนองต่อหลักฐานโดยทันทีมิเช่นนั้นข้อมูลอาจสูญหายได้ ตัวอย่างเช่น อุปกรณ์ที่ทำงานโดยใช้แบตเตอรี่อาจถูกปิดการทำงานและการเชื่อมต่อเครือข่าย (Network) ที่มีการเชื่อมต่อในปัจจุบันอาจสูญหายได้

2.2 หลักฐานทางดิจิทัลมีลักษณะคล้ายกับลายพิมพ์นิ้วมือ (Fingerprints) หรือหลักฐานไบโอเมตริกซ์ (Biometric) อื่น ๆ คือ อาจมีการปกปิดหรือซ่อนเร้นหลักฐานเช่นกัน ซึ่งจำเป็นต้องมีวิธีการในการเปิดเผย

2.3 หลักฐานทางดิจิทัลอาจถูกทำลายหรือเสียหาย ซึ่งสิ่งสำคัญคือต้องมีการตอบสนองที่รวดเร็วและอยู่ในหลักของการครอบครองพยานหลักฐาน (Chain of Custody) โดยเจ้าหน้าที่ต้องปฏิบัติตามสถานการณ์ มิฉะนั้นข้อมูลที่สำคัญอาจเสียหายจากการกระทำที่ตั้งใจและไม่ตั้งใจ

3. การเก็บรวมรวมหลักฐานทางดิจิทัล (Nassif, 2017) สามารถแบ่งออกเป็น 4 ส่วน ดังนี้

3.1 การรวบรวมหลักฐานในสถานที่เกิดเหตุ เป็นการเก็บรวบรวมข้อมูลจากสถานที่เกิดเหตุ ซึ่งผู้ปฏิบัติงานจะต้องตัดสินใจเกี่ยวกับวิธีการในการรวบรวมหลักฐาน ได้แก่ ขนาดของหลักฐาน ปริมาณของหลักฐาน เวลาในการเก็บรวบรวม และการขนย้ายหลักฐาน เป็นต้น

3.2 การรวบรวมหลักฐานออนไลน์ เป็นการเก็บรวบรวมข้อมูลจากการเชื่อมต่อของเครือข่าย

3.3 การรวบรวมหลักฐานบนคลาวด์ (Clouds) เป็นการเก็บรวบรวมข้อมูลจากโซเชียลมีเดีย (Social Media) และ การให้บริการซอฟต์แวร์ (Software as a Service, SaaS)

3.4 การรวบรวมหลักฐานที่ห้องปฏิบัติการ เป็นการเก็บรวบรวมข้อมูลจากหลักฐานที่ได้รับมาจากสถานที่อื่น ๆ ที่ไม่สามารถทำการรวบรวมข้อมูลในสถานที่นั้น ๆ ได้

4. แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลที่เกี่ยวข้อง

ในปัจจุบันทั่วโลกได้มีการตระหนักถึงปัญหาเกี่ยวกับการใช้งานอุปกรณ์และสื่อดิจิทัล เนื่องจากการใช้งานอุปกรณ์หรือสื่อดิจิทัลที่เพิ่มมากขึ้น ทำให้อาชญากรรมเกี่ยวกับอุปกรณ์และสื่อดิจิทัลเพิ่มมากขึ้น ดังนั้น หลาย ๆ หน่วยงานทั่วโลกได้มีการจัดทำแนวทางในการตรวจพิสูจน์หลักฐานทางดิจิทัลขึ้นเพื่อใช้ในการตรวจพิสูจน์และจัดการกับหลักฐานที่เกิดในอาชญากรรม ซึ่งในงานวิจัยนี้ผู้วิจัยได้เลือกแนวทางในการตรวจพิสูจน์หลักฐานทางดิจิทัลมาจำนวน 4 หน่วยงาน ดังนี้

4.1 ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ คู่มือฉบับนี้ได้จัดทำขึ้นเพื่อเป็นแนวทางสำหรับการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานที่มีความสอดคล้องกับมาตรฐานสากล สำหรับการปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการ (Working Group for Drafting Digital Forensic Examination Practice Standards, 2016)

4.2 บทความฉบับพิเศษที่ 800-86 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ เรื่อง แนวทางการบูรณาการเทคนิคด้านนิติวิทยาศาสตร์ในการเผชิญเหตุ (NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response) คู่มือนี้ให้คำแนะนำทั่วไปสำหรับการดำเนินการทางนิติวิทยาศาสตร์ นอกจากนี้ยังให้ข้อมูลรายละเอียดเกี่ยวกับการใช้กระบวนการวิเคราะห์กับแหล่งข้อมูลหลัก 4 ประเภท ได้แก่ ไฟล์ ระบบปฏิบัติการ ข้อมูลบนเครือข่าย (Network Traffic) และแอปพลิเคชัน โดยคู่มือนี้จะอธิบายถึงส่วนประกอบพื้นฐานและลักษณะของแหล่งข้อมูลในแต่ละหมวดหมู่รวมถึงเทคนิคในการรวบรวม การตรวจสอบและการวิเคราะห์ข้อมูลจากแต่ละหมวดหมู่ นอกจากนี้ยังให้คำแนะนำเกี่ยวกับวิธีการใช้แหล่งข้อมูลหลาย ๆ แหล่งร่วมกันเพื่อให้เข้าใจเหตุการณ์ได้ดีขึ้น (Kent et al. 2006)

4.3 วิธีการปฏิบัติงานที่ดีสำหรับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ของคณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (SWGDE Best Practices for Computer Forensics) คู่มือฉบับนี้ให้ข้อมูลพื้นฐานในการได้มาทางตรรกะ (Logical) และกายภาพ (Physical) ของคอมพิวเตอร์และอุปกรณ์เก็บข้อมูลที่เกี่ยวข้อง โดยจะเน้นไปที่ผู้ตรวจสอบในห้องปฏิบัติการและบุคลากรที่รวบรวมหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence (SWGDE), 2014)

4.4 มาตรฐาน ISO/IEC 27037 เทคโนโลยีสารสนเทศ - เทคนิคการรักษาความปลอดภัย – แนวทางสำหรับการระบุ การรวบรวม การได้มาและการเก็บรักษาหลักฐานทางดิจิทัล (ISO/IEC 27037 Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence) มาตรฐานนี้จะให้แนวทางในการจัดการกับ

หลักฐานทางดิจิทัล เช่น การระบุตัวตน การรวบรวม การได้มาของหลักฐานและการเก็บรักษาหลักฐานทางดิจิทัลที่อาจเป็นหลักฐานที่สำคัญ (British Standard, 2016)

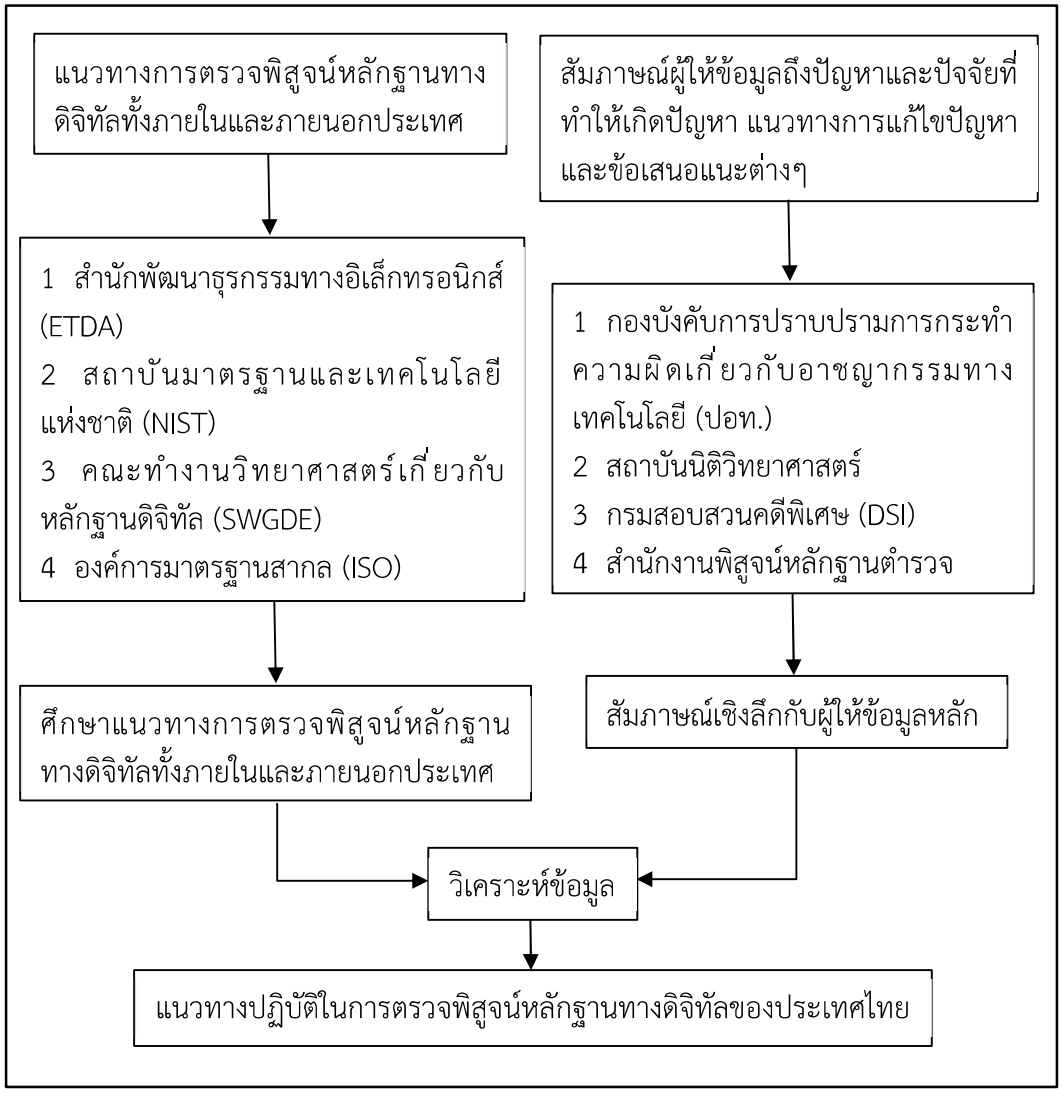
5. งานวิจัยที่เกี่ยวข้อง

Grobler (2010) ได้ทำการนำเสนอภาพรวมของมาตรฐานทางนิติวิทยาศาสตร์ดิจิทัลระดับสากล โดยอธิบายถึงโครงสร้างและความจำเป็นของมาตรฐานในระดับสากล นอกจากนี้ยังอธิบายถึงปัญหาในทางปฏิบัติที่ผู้จัดทำมาตรฐานต้องเผชิญโดยเฉพาะอย่างยิ่งในมาตรฐานทางนิติวิทยาศาสตร์ดิจิทัล ต่อมา Umberg และ Warden (2013) ได้จัดทำโปรโตคอลหรือขั้นตอนการสืบสวนทางไซเบอร์ โดยมีการแบ่งประเภทของหลักฐานทางดิจิทัลออกเป็น 3 ประเภท ได้แก่ 1. ข้อมูลที่มีการจัดเก็บในอุปกรณ์ทางกายภาพ 2. ข้อมูลที่ไม่ได้จัดเก็บไว้ในอุปกรณ์ที่ผู้ตรวจสอบสามารถเข้าถึงได้ทั้งทางกายภาพหรือทางออนไลน์ และ 3. ข้อมูลที่จัดเก็บในเซิร์ฟเวอร์และมีการจัดเก็บแบบส่วนตัวโดยผู้ให้บริการเซิร์ฟเวอร์ จากนั้น Mumba และ Venter (2014) ได้ทำการศึกษาเกี่ยวกับการทดสอบรูปแบบกระบวนการสืบสวนทางนิติวิทยาศาสตร์ทางดิจิทัล (Harmonized Digital Forensic Investigation Process, HDFIP) ที่ดำเนินการในร่างมาตรฐาน ISO/IEC 27043 โดยทำการจัดกลุ่มแบบจำลองกระบวนการที่แสดงโครงสร้างและการตัดสินใจที่แม่นยำ กรณีศึกษาที่ใช้นั้นจะช่วยในการวิเคราะห์ประสิทธิภาพของแบบจำลองเพื่อให้แน่ใจว่าหลักการของความถูกต้องและการยอมรับนั้นเป็นจริง ซึ่งกระบวนการที่มีคุณสมบัติเหล่านี้จะช่วยลดความเหลื่อมล้ำในด้านการสืบสวนทางนิติวิทยาศาสตร์ดิจิทัล นอกจากนี้ Chairangsinant (2016) ได้ทำการศึกษาเกี่ยวกับมาตรฐานที่เกี่ยวข้องทางนิติวิทยาศาสตร์ โดยกล่าวว่ามาตรฐานทางนิติวิทยาศาสตร์จะต้องมีความเกี่ยวข้องกับนโยบาย ระเบียบ และวิธีการปฏิบัติงานของหน่วยงาน นอกจากนี้มาตรฐานทางนิติวิทยาศาสตร์จะต้องสอดคล้องและเหมาะสมกับบริบทของงานที่ให้บริการ และ Horsman (2019) ได้ทำการศึกษาเกี่ยวกับการตัดสินใจของผู้ปฏิบัติงานในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล เนื่องจากการตัดสินใจของผู้ปฏิบัติงานมีผลทำให้การรายงานของหลักฐานมีความน่าเชื่อถือ ซึ่งความสามารถนี้ควรได้รับการพิจารณาว่าเป็นคุณสมบัติหลักของผู้ปฏิบัติงานและผู้ปฏิบัติงานทุกคนควรมีความสามารถนี้จริง โดยงานวิจัยนี้นำเสนอกรอบการรายงานและสนับสนุนการตัดสินใจเกี่ยวกับหลักฐานทางดิจิทัล (Digital Evidence Reporting and Decision Support, DERDS) ที่ออกแบบมาเพื่อช่วยผู้ปฏิบัติงานประเมินความน่าเชื่อถือของการอนุมานสมมติฐานของข้อสรุปที่เกี่ยวข้องกับการค้นพบหลักฐานที่อาจเกิดขึ้น ซึ่งมีโครงสร้างและการใช้กรอบการรายงานและสนับสนุนการตัดสินใจเกี่ยวกับหลักฐานทางดิจิทัลเพื่อแสดงให้เห็นถึงขั้นตอนในการตัดสินใจของผู้ปฏิบัติงานที่ต้องได้รับเมื่อมีการประมาณการความถูกต้องของการค้นพบหลักฐาน

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่าการจัดทำมาตรฐานการตรวจพิสูจน์หลักฐานทางดิจิทัลในต่างประเทศมีการพัฒนาอย่างต่อเนื่อง แตกต่างจากภายในประเทศไทยเนื่องจากข้อจำกัดทางเทคโนโลยีและข้อกฎหมาย รวมถึงวิธีการปฏิบัติงานของแต่ละหน่วยงานที่แตกต่างกัน ทำให้ผู้วิจัยเล็งเห็นถึงปัญหาที่เกิดขึ้น จึงต้องการศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลเพื่อให้หน่วยงานต่าง ๆ สามารถนำแนวทางดังกล่าวไปปรับใช้และพัฒนาเป็นมาตรฐานขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัล

6. กรอบแนวคิดการวิจัย

งานวิจัยนี้ผู้วิจัยได้กำหนดความสัมพันธ์ของแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ของประเทศไทยและต่างประเทศในการศึกษาแนวทางการตรวจพิสูจน์หลักฐานโดยมีคำถามการวิจัยคือ แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทยควรมีแนวทางปฏิบัติอย่างไร



ภาพที่ 1 กรอบแนวคิดการวิจัย

ระเบียบวิธีการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งใช้วิธีการศึกษาเอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลและการสัมภาษณ์เชิงลึก (In-Depth Interview) จากผู้ให้ข้อมูลหลัก โดยมีรายละเอียดขั้นตอนการดำเนินการวิจัย ดังนี้

1. ผู้ให้ข้อมูลหลัก (Key Informants)

1.1 หน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทยจำนวน 4 หน่วยงาน ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) และสำนักงานพิสูจน์หลักฐานตำรวจ

1.2 เจ้าหน้าที่ผู้เชี่ยวชาญที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัลจากหน่วยงานที่เกี่ยวข้อง ในหน่วยงานที่กล่าวไว้ก่อนหน้านี้ หน่วยงานละ 3 คน รวมเป็น 12 คน พิจารณาจากคุณสมบัติดังนี้

1.2.1 เจ้าหน้าที่ผู้เชี่ยวชาญต้องเป็นผู้ที่ทำงานเกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงาน

1.2.2 เจ้าหน้าที่ผู้เชี่ยวชาญต้องมีประสบการณ์การทำงานที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานอย่างน้อย 3 ปี หรือในกรณีที่คุณสมบัติของเจ้าหน้าที่ผู้เชี่ยวชาญไม่เป็นไปตามที่กำหนดสามารถปรับเปลี่ยนคุณสมบัติได้ดังนี้ เจ้าหน้าที่ผู้เชี่ยวชาญต้องมีประสบการณ์การทำงานที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานของหน่วยงานอย่างน้อย 2 ปี

2. เครื่องมือที่ใช้ในการวิจัย

ผู้วิจัยได้ใช้เครื่องมือในการวิจัย 2 เครื่องมือ ดังนี้

2.1 แบบวิเคราะห์เอกสาร ศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานในประเทศไทยและหน่วยงานในต่างประเทศ โดยเน้นศึกษาในขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัล

2.2 แบบสัมภาษณ์ ผู้วิจัยใช้คำถามในแบบสัมภาษณ์เป็นแบบกึ่งโครงสร้างเพื่อให้ได้คำตอบที่หลากหลายและได้ข้อเท็จจริงในการปฏิบัติงานของผู้ให้ข้อมูลหลัก

3. การเก็บรวบรวมและวิเคราะห์ข้อมูล

3.1 ขอหนังสือขอความอนุเคราะห์เก็บรวบรวมข้อมูลทำวิจัยจากคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจไปยังหน่วยงานของผู้ให้ข้อมูลหลัก ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) และสำนักงานพิสูจน์หลักฐานตำรวจ

3.2 การสัมภาษณ์เชิงลึก ผู้วิจัยได้เข้าสัมภาษณ์ผู้ให้ข้อมูลหลักด้วยตนเอง โดยใช้แบบสัมภาษณ์เชิงลึกที่ผู้วิจัยเป็นคนจัดทำขึ้น โดยใช้ระยะเวลาในการเก็บรวบรวมข้อมูลช่วงเดือนกุมภาพันธ์ พ.ศ. 2563 ถึง เดือนมีนาคม พ.ศ. 2563 จากนั้นวิเคราะห์ข้อมูลตามหัวข้อคำถาม ได้แก่ สภาพปัญหาและปัจจัยที่ทำให้เกิดปัญหา วิธีการแก้ไขปัญหาและข้อเสนอแนะต่าง ๆ ของผู้ให้ข้อมูลหลักเกี่ยวกับขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานตนเอง

3.3 การวิเคราะห์เอกสาร ผู้วิจัยศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานภายในประเทศ ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และ หน่วยงานใน

ต่างประเทศ ได้แก่ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) และ องค์การมาตรฐานสากล (International Organization for Standardization, ISO) จากนั้นทำการวิเคราะห์แนวทางเหล่านั้นโดยเน้นไปที่ขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัล

ผลการวิจัย

การวิจัยนี้ผู้วิจัยได้เก็บรวบรวมข้อมูลโดยการวิเคราะห์เอกสารจากแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานในประเทศไทย ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และ หน่วยงานในต่างประเทศ ได้แก่ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) และ องค์การมาตรฐานสากล (International Organization for Standardization, ISO) และการสัมภาษณ์เชิงลึก (In-Depth Interview) กับผู้ให้ข้อมูลหลักของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ทั้งหมด 4 หน่วยงาน ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) และสำนักงานพิสูจน์หลักฐานตำรวจ ซึ่งเป็นตัวแทนของหน่วยงาน จำนวนหน่วยงานละ 3 คน รวมทั้งหมด 12 คน โดยจะแบ่งการนำเสนอการวิเคราะห์ข้อมูลออกเป็น 3 ส่วน ดังนี้

1. การวิเคราะห์เอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลภายในและภายนอกประเทศไทย จำนวน 4 หน่วยงาน ได้แก่

1.1 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) มีขั้นตอนการตรวจพิสูจน์หลักฐานทั้งหมด 6 ขั้นตอน ได้แก่ การรวบรวม (Collection) การบรรจุและเคลื่อนย้าย (Packaging and Transportation) การสำเนาข้อมูล (Acquisition) การวิเคราะห์ (Analysis) การบันทึก (Document) และ การรายงาน (Report)

1.2 สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) มีขั้นตอนการตรวจพิสูจน์หลักฐานทั้งหมด 5 ขั้นตอน ได้แก่ การรวบรวม (Collection) การสำเนาข้อมูล (Acquisition) การตรวจสอบ (Examination) การวิเคราะห์ (Analysis) และ การรายงาน (Report)

1.3 คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) มีขั้นตอนการตรวจพิสูจน์หลักฐานทั้งหมด 5 ขั้นตอน ได้แก่ การรวบรวม (Collection) การบรรจุและเคลื่อนย้าย (Packaging and Transportation) การสำเนาข้อมูล (Acquisition) การบันทึก (Document) และ การรายงาน (Report)

1.4 องค์การมาตรฐานสากล (International Organization for Standardization, ISO) มีขั้นตอนการตรวจพิสูจน์หลักฐานทั้งหมด 4 ขั้นตอน ได้แก่ การระบุ (Identification) การรวบรวม (Collection) การสำเนาข้อมูล (Acquisition) และ การเก็บรักษา (Preservation) โดยทั้ง 4 หน่วยงานมีขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลที่เหมือนและแตกต่างกันออกไป ซึ่งสามารถสรุปขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลของแต่ละหน่วยงานได้ดังตารางที่ 1

ตารางที่ 1 สรุปขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องทางนิติวิทยาศาสตร์ทั้งภายในและภายนอกประเทศที่ได้จากการวิเคราะห์เอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของแต่ละหน่วยงาน

ขั้นตอน	หน่วยงาน			
	ETDA	NIST	SWGDE	ISO
การระบุ (Identification)	✗	✗	✗	✓
การรวบรวม (Collection)	✓	✓	✓	✓
การบรรจุและเคลื่อนย้าย (Packaging and Transportation)	✓	✗	✓	✗
การสำเนาข้อมูล (Acquisition)	✓	✓	✓	✓
การตรวจสอบ (Examination)	✗	✓	✗	✗
การวิเคราะห์ (Analysis)	✓	✓	✗	✗
การบันทึก (Document)	✓	✗	✓	✗
การรายงาน (Report)	✓	✓	✓	✗
การเก็บรักษา (Preservation)	✗	✗	✗	✓

2. การสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลหลักของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย จำนวน 4 หน่วยงาน ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) และสำนักงานพิสูจน์หลักฐานตำรวจ ซึ่งเป็นตัวแทนจากหน่วยงาน หน่วยงานละ 3 คน รวมทั้งหมด 12 คน โดยทำการสัมภาษณ์เกี่ยวกับสภาพปัญหาในขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลที่ผู้ให้ข้อมูลหลักพบระหว่างปฏิบัติงาน รวมถึงแนวทางการแก้ไขปัญหาและข้อเสนอแนะเพิ่มเติมเกี่ยวกับขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัล จากการสัมภาษณ์ผู้ให้ข้อมูลหลักทั้ง 12 คน พบว่าปัญหาที่พบเจอมากที่สุดระหว่างการตรวจพิสูจน์หลักฐานทางดิจิทัล คือ วัตถุประสงค์ในการตรวจพิสูจน์ไม่ชัดเจน ทำให้ผู้ปฏิบัติงานไม่สามารถตรวจพิสูจน์หลักฐานให้ตรงตามความต้องการของผู้ร้องขอหรือพนักงานสืบสวนได้ รองลงมาเป็นปัญหาเกี่ยวกับองค์ความรู้และความเชี่ยวชาญของผู้ปฏิบัติงาน จำนวนบุคลากร เครื่องมือและอุปกรณ์ที่ใช้ในการตรวจพิสูจน์หลักฐานทางดิจิทัล และงบประมาณ ตามลำดับ จากปัญหาที่กล่าวมาข้างต้นทางหน่วยงานทั้ง 4 หน่วยงานได้มีการจัดการแก้ไขปัญหาไปบ้างแล้วแต่ยังไม่สามารถแก้ไขได้ทั้งหมด นอกจากนี้ผู้ให้ข้อมูลหลักจากทั้ง 4 หน่วยงานได้ให้ข้อเสนอแนะเพิ่มเติมเกี่ยวกับขั้นตอนการตรวจพิสูจน์

หลักฐานทางดิจิทัลดังนี้ ให้มีการจัดสัมมนาหรืออบรมเชิงวิชาการเพื่อแลกเปลี่ยนความรู้ แนวทางและวิธีการแก้ไขปัญหาเกี่ยวกับการตรวจพิสูจน์หลักฐานทั้งภายในและภายนอกประเทศ รวมถึงการจัดตั้งศูนย์กลางเครื่องมือที่ใช้ในการตรวจพิสูจน์หลักฐานทางดิจิทัล

3. การศึกษาแนวทางกาตรวจพิสูจน์หลักฐานทางดิจิทัล

จากการศึกษาเอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานภายในประเทศ ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และหน่วยงานในต่างประเทศ ได้แก่ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) และองค์การมาตรฐานสากล (International Organization for Standardization, ISO) และปัญหาที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัลที่ได้จากการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลหลักทั้ง 4 หน่วยงาน ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) และ สำนักงานพิสูจน์หลักฐานตำรวจ สามารถแบ่งรายละเอียดของแนวทางปฏิบัติการตรวจพิสูจน์หลักฐานทางดิจิทัลออกเป็น 6 หัวข้อ ดังนี้

3.1 คุณสมบัติของผู้ปฏิบัติงานในการตรวจพิสูจน์หลักฐานทางดิจิทัล

3.1.1 ต้องสำเร็จการศึกษาในสาขาวิชาที่เกี่ยวข้องกับคอมพิวเตอร์

3.1.2 ต้องผ่านการฝึกอบรมก่อนปฏิบัติงานในส่วนงานที่รับผิดชอบอย่างน้อย 2 หลักสูตร

3.2 ขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัล สามารถแบ่งออกเป็น 5 ขั้นตอน ดังนี้

3.2.1 การรวบรวม (Collection) ควรดำเนินการดังนี้

3.2.1.1 ผู้ปฏิบัติงานเป็นผู้กำหนดเกี่ยวกับรูปแบบการค้นหาและจัดลำดับความสำคัญในการเก็บรวบรวมหลักฐานดิจิทัล

3.2.1.2 ห้ามบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าไปในสถานที่เกิดเหตุ

3.2.1.3 ถ่ายภาพรายละเอียดของหลักฐานดิจิทัลที่พบในสถานที่เกิดเหตุ โดยแบ่งออกเป็น 3 กรณี ดังนี้

(1) หากพบคอมพิวเตอร์หรือเครื่องมือสื่อสารเคลื่อนที่ ให้ถ่ายภาพทุกด้านและพื้นที่รอบๆ หลักฐานที่จะจัดเก็บ อุปกรณ์เชื่อมต่อภายนอกและจุดเชื่อมต่อ รวมทั้งสภาพโดยรวมให้เห็นว่าหลักฐานแต่ละชิ้นวางไว้ในตำแหน่งใด

(2) ข้อมูลเฉพาะของหลักฐาน เช่น หมายเลขเครื่อง (Serial Number) ผู้ผลิต รุ่นและความเสียหายที่พบ เป็นต้น

(3) สิ่งอื่นที่อาจเป็นประโยชน์เพิ่มเติม เช่น สิ่งพิมพ์ กระดาษบันทึกข้อความหรือหนังสือเกี่ยวกับความรู้ทางคอมพิวเตอร์เพื่อบ่งบอกถึงระดับความรู้ทางคอมพิวเตอร์ของผู้ต้องสงสัย

3.2.1.4 กรณีพบหลักฐานอยู่ภายนอกอาคารและสภาพอากาศขณะนั้นที่อาจส่งผลต่อหลักฐาน ควรพิจารณาดำเนินการกับหลักฐานนั้นเป็นลำดับแรก

3.2.1.5 กรณีที่ไม่สามารถเคลื่อนย้ายหลักฐานจากสถานที่เกิดเหตุได้ ผู้ปฏิบัติงานควรทำการสำเนาข้อมูลในสถานที่เกิดเหตุ

3.2.1.6 ควรจดบันทึกรายละเอียดของหลักฐานดิจิทัลที่พบในสถานที่เกิดเหตุ ได้แก่ สิ่งที่พบ, สภาพและรายการอุปกรณ์ภายนอกที่เชื่อมต่อกับหลักฐานและสิ่งที่ได้ดำเนินการรวมถึงสิ่งผิดปกติ เช่น ร่องรอยความเสียหายภายนอกของหลักฐาน เป็นต้น

ในขั้นตอนนี้ใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) และองค์การมาตรฐานสากล (International Organization for Standardization, ISO) เนื่องจากทั้ง 4 หน่วยงานมีแนวทางการปฏิบัติงานที่คล้ายคลึงกัน

3.2.2 การบรรจุและการเคลื่อนย้ายหลักฐาน (Packaging and Transportation) ควรดำเนินการดังนี้

3.2.2.1 ทำการแยกประเภทของหลักฐานทางดิจิทัลที่ทำการรวบรวมออกเป็น 2 ประเภทดังนี้

(1) หลักฐานประเภทเครื่องมือสื่อสาร ในกรณีที่อุปกรณ์มีการเปิดใช้งานให้ผู้ปฏิบัติงานทำการเปิดโหมดเครื่องบินในอุปกรณ์ดังกล่าวเพื่อปิดกั้นสัญญาณภายนอก จากนั้นบรรจุอุปกรณ์สื่อสารนั้นลงในถุงกันคลื่นสัญญาณ (Faraday Bag)

(2) หลักฐานประเภทสื่อบันทึกข้อมูล (Storage Media) ให้ผู้ปฏิบัติงานทำการบรรจุหลักฐานลงในถุงวัตถุพยานได้เลย

3.2.2.2 ปิดเทปกาวถุงวัตถุพยานให้มิดชิดไม่ให้มีรอยฉีกขาดหรือชำรุด ในกรณีที่หลักฐานเป็นเคสคอมพิวเตอร์ให้ผู้ปฏิบัติงานทำการปิดเทปกาวทับช่องเสียบอุปกรณ์ทุกช่อง

3.2.2.3 ติดหมายเลขกำกับวัตถุพยานทุกชิ้น พร้อมทั้งลงลายมือชื่อผู้ปฏิบัติงาน วันที่และเวลา คร่อมเทปกาว

3.2.2.4 กรอกข้อมูลของหลักฐานลงในแบบฟอร์มการครอบครองพยานหลักฐาน (Chain of custody) ให้ครบถ้วน

3.2.2.5 การเคลื่อนย้ายหลักฐานให้หลีกเลี่ยงการเก็บหลักฐานบริเวณที่มีสนามแม่เหล็กไฟฟ้าหรือไฟฟ้าสถิตและบริเวณที่มีความชื้นและอุณหภูมิสูง

ขั้นตอนนี้ใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) เนื่องจากขั้นตอนการดำเนินการมีความใกล้เคียงกับการปฏิบัติงานของหน่วยงานของผู้ให้ข้อมูลหลักที่ดำเนินการอยู่ในปัจจุบัน

3.2.3 การตรวจสอบ (Examination) ควรดำเนินการดังนี้

3.2.3.1 สวมถุงมือระหว่างการปฏิบัติงานและระมัดระวังในการแกะบรรจุภัณฑ์

3.2.3.2 ตรวจสอบและบันทึกสภาพทางกายภาพของหลักฐานทุกชิ้นก่อนนำมาตรวจพิสูจน์เช่น ฝาปิดเคสคอมพิวเตอร์พีซีถูกปิดขันน็อตอย่างเรียบร้อยหรือไม่ฝาหลังส่วนที่ปิดฮาร์ดดิสก์ของแล็ปท็อปถูกปิดขันน็อตอย่างเรียบร้อยหรือไม่ เป็นต้น

3.2.3.3 การทำสำเนาข้อมูลในหลักฐานควรปฏิบัติดังนี้

(1) สำเนาข้อมูลในหลักฐานด้วยขั้นตอนที่น่าเชื่อถือและสามารถตรวจสอบได้

(2) สำเนาข้อมูลลงในสื่อบันทึกข้อมูลที่พร้อมใช้งาน

(3) ยืนยันความสมบูรณ์ของข้อมูลที่ทำการสำเนาด้วยการคำนวณและเปรียบเทียบค่าแฮช (Hash Values) ของต้นฉบับและสำเนาหลักฐาน เช่น เอ็มดีไฟท์ (MD5) ชาร์วัน (SHA1) ชาร์ทูไฟท์ซิก (SHA256) เป็นต้น โดยดำเนินการอย่างน้อยสองรูปแบบและจัดเก็บข้อมูลลงในสื่อแบบอ่านอย่างเดียว เช่น ซีดีอาร์ (CD-R) และ ดีวีดีอาร์ (DVD-R)

(4) ต้องทำสำเนาข้อมูลทั้งหมด 3 ชุด ได้แก่ ต้นฉบับ สำเนาต้นฉบับและสำเนาสำหรับใช้งาน

3.2.3.4 ควรจัดเก็บสำเนาในอุปกรณ์ที่เชื่อถือได้และมีการเก็บรักษาให้สอดคล้องกับนโยบายขององค์กรและกฎหมายที่เกี่ยวข้อง

3.2.3.5 การกระทำและข้อผิดพลาดใด ๆ ที่พบในระหว่างการทำสำเนาควรมีการบันทึกไว้เป็นเอกสาร เช่น ชื่อผู้ปฏิบัติงาน วันที่และเวลาที่ทำการสำเนา รุ่นและหมายเลขเครื่อง (Serial Number) ของฮาร์ดไดรฟ์ (Hard Drive) ความจุของตัวกลางในการเก็บข้อมูลและข้อมูลที่เกี่ยวกับซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ เช่น ชื่อหมายเลขรุ่นและข้อมูลสิทธิ์ใช้งาน เป็นต้น
ขั้นตอนนี้ใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) และองค์การมาตรฐานสากล (International Organization for Standardization, ISO) เนื่องจากขั้นตอนการตรวจสอบนั้นรวมไปถึงการสำเนาข้อมูลหลักฐานทางดิจิทัลด้วย ผู้วิจัยจึงใช้ขั้นตอนการสำเนาข้อมูล (Acquisition) และการตรวจสอบ (Examination) ของทั้ง 4 หน่วยงานมาปรับให้เข้ากับการปฏิบัติงานของหน่วยงานของผู้ให้ข้อมูลหลักที่ดำเนินการอยู่ในปัจจุบัน

3.2.4 การวิเคราะห์ (Analysis) ควรดำเนินการดังนี้

3.2.4.1 ห้ามวิเคราะห์โดยตรงกับต้นฉบับของหลักฐานทางดิจิทัล ให้ดำเนินการวิเคราะห์หลักฐานจากสำเนาหลักฐานทางดิจิทัลสำหรับใช้งานเท่านั้น

3.2.4.2 ตรวจสอบเวลาที่ตั้งค่าในหลักฐานทางดิจิทัลให้แน่ใจ เช่น การตั้งค่าวันและเวลาในไบออส (BIOS) และค่าเขตเวลา (Time Zone) เพื่อให้สามารถตั้งค่าในซอฟต์แวร์ตรวจพิสูจน์หลักฐานทางดิจิทัลได้อย่างถูกต้อง

3.2.4.3 ปฏิบัติตามมาตรการควบคุมและมาตรฐานที่สอดคล้องกับข้อกำหนดขององค์กรและกฎหมายที่เกี่ยวข้อง

ขั้นตอนนี้ใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) เนื่องจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) เป็นหน่วยงานภายในประเทศทำให้ลดความกังวลในเรื่องของกฎหมาย

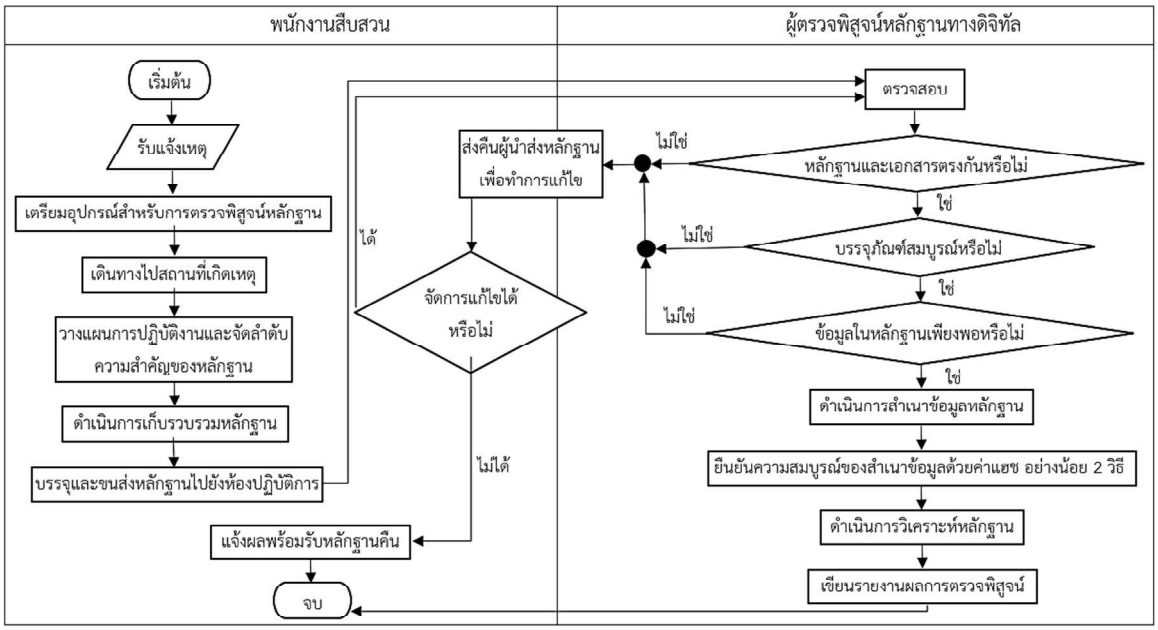
3.2.5 การรายงาน (Report) ควรดำเนินการดังนี้

3.2.5.1 ควรนำเสนอข้อมูลในรูปแบบที่เข้าใจง่ายและตอบสนองความต้องการของผู้ร้องขอ

3.2.5.2 ควรมีข้อมูลที่เกี่ยวข้องกับบันทึกการทำสำเนาข้อมูลและการจัดการหลักฐาน รวมถึงข้อมูลที่สำคัญ ได้แก่ ชื่อผู้ตรวจพิสูจน์ วันที่ตรวจพิสูจน์ วัตถุประสงค์และขอบเขตของการตรวจพิสูจน์ รายละเอียดของพยานหลักฐาน โดยระบุสภาพภายนอก วิธีการบรรจุและเคลื่อนย้ายหลักฐาน ความสมบูรณ์และความถูกต้องของหลักฐาน การปิดผนึกและการลงลายมือชื่อกำกับรายละเอียดของเครื่องมือที่ใช้ในการตรวจพิสูจน์และผลการตรวจพิสูจน์และบทสรุป

3.2.5.3 ผู้ปฏิบัติงานควรสามารถอธิบายข้อมูลที่มีอยู่ในรายงานได้ทั้งหมด

ขั้นตอนนี้ใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) และคณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล (Scientific Working Group on Digital Evidence, SWGDE) เนื่องจากการรายงานผลการตรวจพิสูจน์ของแต่ละหน่วยงานมีความแตกต่างกัน ผู้วิจัยจึงใช้แนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานข้างต้นทั้งหมดและปรับให้เข้ากับการปฏิบัติงานของหน่วยงานภายในประเทศ โดยสามารถสรุปขั้นตอนแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลดังภาพที่ 2



ภาพที่ 2 แผนภาพขั้นตอนแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัล

สรุปและอภิปรายผล

ในการวิจัยครั้งนี้ผู้วิจัยได้ทำการศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ทั้งภายในและภายนอกประเทศและสัมภาษณ์ผู้ให้ข้อมูลหลักจากหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ของประเทศไทย จากนั้นนำผลที่ได้มาจัดทำเป็นแนวทางปฏิบัติการตรวจพิสูจน์หลักฐานทางดิจิทัล

จากผลการวิจัยเรื่อง การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์ พบว่าแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลที่จัดทำขึ้นสามารถปรับใช้กับหน่วยงานที่เกี่ยวข้องทางนิติวิทยาศาสตร์ของประเทศได้ทั้งหมด แต่ต้องคำนึงถึงนโยบายของหน่วยงานเป็นหลัก เนื่องจากแนวทางดังกล่าวเป็นเพียงการวิเคราะห์เอกสารและปรับให้เหมาะสมกับความต้องการของผู้ปฏิบัติงานเท่านั้น ดังนั้นในบางขั้นตอนจึงมีข้อจำกัดอยู่บ้าง เช่น อุปกรณ์และเครื่องมือที่ใช้สำหรับการตรวจพิสูจน์หลักฐานทางดิจิทัล รวมถึงความรู้พื้นฐานของผู้ปฏิบัติงานเกี่ยวกับการตรวจพิสูจน์หลักฐานทางดิจิทัลของประเทศไทย ซึ่งแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลที่จัดทำขึ้นนั้นมีความสอดคล้องกับงานวิจัยของ Tommy Umberg และ Cherrie Warden (2013) และ Marthie Grobler (2010) ที่

ระบุว่างานตรวจพิสูจน์หลักฐานทางดิจิทัลจำเป็นต้องมีการยืนยันหลักฐานด้วยวิธีการที่ถูกต้องและแม่นยำโดยผู้ปฏิบัติงานที่มีความรู้ความเข้าใจในงานนั้น ๆ

นอกจากนี้ยังพบปัญหาที่ได้จากการสัมภาษณ์ผู้ให้ข้อมูลหลักหลายปัญหาที่ผู้วิจัยไม่สามารถทำการแก้ไขได้ เนื่องจากเป็นปัญหาที่ต้องได้รับการแก้ไขในระดับประเทศ ได้แก่

1. ปัญหาเกี่ยวกับงบประมาณในการซื้ออุปกรณ์และเครื่องมือที่ใช้ในการตรวจพิสูจน์หลักฐานทางดิจิทัล เนื่องจากเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่องทำให้มีหลักฐานทางดิจิทัลใหม่ ๆ เพิ่มขึ้นจำนวนมาก แต่ด้วยการสั่งซื้ออุปกรณ์และเครื่องมือต้องเป็นไปตามรอบงบประมาณ ซึ่งอุปกรณ์และเครื่องมือที่ได้มาไม่มีความทันสมัยในการใช้งาน ณ ขณะที่ปฏิบัติงาน ทำให้การตรวจพิสูจน์หลักฐานทางดิจิทัลอาจไม่ได้ประสิทธิภาพตามต้องการ

2. ปัญหาเกี่ยวกับบุคลากรที่ปฏิบัติหน้าที่ในการตรวจพิสูจน์หลักฐานทางดิจิทัล เนื่องจากการขอกำลังคนในการทำงานมีข้อจำกัดในแต่ละหน่วยงาน จึงไม่สามารถขอกำลังคนในจำนวนที่ต้องการได้ ทำให้การปฏิบัติงานอาจเกิดความล่าช้า

ข้อเสนอแนะ

1. ข้อเสนอแนะเพื่อนำผลการวิจัยไปใช้

1.1 องค์กรหรือหน่วยงานที่นำแนวทางปฏิบัติการตรวจพิสูจน์หลักฐานทางดิจิทัลไปใช้ควรปฏิบัติตามนโยบายขององค์กรหรือหน่วยงานเป็นหลัก

2. ข้อเสนอแนะในเชิงปฏิบัติสำหรับผู้ปฏิบัติงาน

2.1 ควรปฏิบัติตามนโยบายขององค์กรหรือหน่วยงานเป็นหลัก

2.2 ควรหารือการปฏิบัติงานร่วมกันระหว่างองค์กรหรือหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์

3. ข้อเสนอแนะในเชิงนโยบายสำหรับองค์กร

3.1 องค์กรหรือหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ของประเทศไทยควรกำหนดแนวทางปฏิบัติในการตรวจพิสูจน์หลักฐานทางดิจิทัลร่วมกัน

3.2 ควรหารือเพื่อออกแผนการปฏิบัติงาน นโยบาย หรือการปฏิบัติงานร่วมกันระหว่างองค์กรหรือหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ของประเทศไทย

4. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

4.1 ควรทำการศึกษาเกี่ยวกับกฎหมายที่เกี่ยวข้องในการตรวจพิสูจน์หลักฐานทางดิจิทัลเพื่อลดปัญหาเกี่ยวกับการเข้าถึงหลักฐานทางดิจิทัลของผู้ปฏิบัติงาน

4.2 ควรศึกษาขั้นตอนการปฏิบัติงานของแต่ละหน่วยงานอย่างละเอียด เพื่อให้ได้มาซึ่งข้อมูลที่ครบถ้วนและสามารถกำหนดแนวทางการปฏิบัติงานที่คล้ายคลึงกันในแต่ละหน่วยงานได้

เอกสารอ้างอิง

British Standard. (2016). **Information Technology – Security Technology – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (ISO/IEC 27037:2012.** London: The British Standards Institution.

Chairangsinant, C. (2559). International Standards Accreditation for Forensic science. **Journal of Criminology and Forensic Science**, 2(1), 60-71. (In Thai).

Casey, E. (2011). **Digital evidence and computer crime: forensic science, computers and the internet. 3rd ed.** The United States of America: British Library.

Electronic Transactions Development Agency (Public Organization). (2018). **Thailand Internet User Profile 2018.** Huai Khwang: Electronic Transactions Development Agency (Public Organization).

Grobler, M. (2010). Digital Forensic Standards: International Progress. **Proceedings of the South African Information Security Multi-Conference (SAISMC 2010).** 261- 271.

Horsman, G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. **Digital Investigation**, 28, 146-151.

Kent, K., Chevalier, S, Grance, T, and Dang, H. (2006). **NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response.** Gaithersburg: National Institute of Standards and Technology.

Mumba, E. R. and Venter, H. (2014). Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigations. **ADFSL Conference on Digital Forensics, Security and Law**, 83-97.

Nassif, L. N. (2017). Towards a Proof Acceptance by Overcoming Challenges in Collecting Digital Evidence. **International Science Index, Law and Political Sciences.** 11(1), 240-243.

National Statistical Office. (2018). **Survey of the use of information and communication technology in the household 2018 (Q1).** Lak Si: National Statistical Office. (In Thai).

Scientific Working Group on Digital Evidence (SWGDE). (2014). **SWGDE Best Practices for Computer Forensics Version 3.1.**

Suriyawongkul, A. (2015). **Digital evidence is everywhere. How to manage it reliably.** Retrieved 15 September 2019, from https://thainetizen.org/2015/07/digital-forensics-workshop/. (In Thai)

Thailand Computer Emergency Response Team (ThaiCERT) of Electronic Transactions Development Agency (Public Organization). (2020). **Threat statistics**. Retrieved 12 February 2020, from https://www.thaicert.or.th/statistics/statistics.html. (In Thai)

Umberg, T. and Warden, C. (2013). Digital Evidence and Investigatory Protocols. **Digital Evidence and Electronic Signature Law Review.** 11, 128-136.

Working Group for Drafting Digital Forensic Examination Practice Standards. (2016). **Recommendations for Digital Devices Management Standards in Forensic Examination.** Huai Khwang: Digital Forensics Center of Electronic Transactions Development Agency (Public Organization). (In Thai).

Working Group for Drafting Digital Forensic Examination Practice Standards. (2018) . **Thailand Internet User Behavior 2018.** Huai Khwang: Digital Forensics Center of Electronic Transactions Development Agency (Public Organization). (In Thai).

ผู้เขียน

คำนำหน้า ชื่อ-สกุล	**นางสาวจิตชนก อินถามา**
หน่วยงาน/สังกัด	นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
ที่อยู่หน่วยงาน/สังกัด	เลขที่ 90 หมู่ 7 ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
อีเมล	Jitchanok.inthama@gmail.com
คำนำหน้า ชื่อ-สกุล	**พันตำรวจตรี ดร.วงศ์ยศ เกิดศรี**
หน่วยงาน/สังกัด	คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
ที่อยู่หน่วยงาน/สังกัด	เลขที่ 90 หมู่ 7 ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
อีเมล	wongyos@gmail.com, wongyos@rpca.ac.th