2.3.32

ISSN 2408-2430

วารสารวิชาการ
อาชญาวิทยาและนิติวิทยาศาสตร์
Journal of Criminology and Forensic Science

ปีที่ 4 ฉบับที่ 1 เดือน มกราคม – มิถุนายน 2561

โรงเรียนนายร้อยตำรวจ : Royal Police Cadet Academy

วัตถุประสงค์

1. เพื่อเพิ่มช่องทางการเผยแพร่ผลงานวิชาการ องค์ความรู้ของคณาจารย์ นักวิจัย และนักศึกษาให้มีการตีพิมพ์เผยแพร่ในระดับชาติ
2. เพื่อกระตุ้นให้เกิดการวิจัย พัฒนาองค์ความรู้อย่างต่อเนื่อง ในด้านนิติวิทยาศาสตร์ กระบวนการยุติธรรม และด้านอื่นๆ ที่เกี่ยวข้อง สามารถนำมาอ้างอิง ประยุกต์ใช้ในการปฏิบัติงาน ตลอดจนเกิดประโยชน์แก่สังคมได้

สารบัญ

ความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟน

The Reliability of Electronic Evidence Obtained from Smartphone

พันตำรวจโท พิชศาล พันธุ์วัฒนา
คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ

Pol.Lt.Col. Pitsarn Phanwattana
Faculty of Police Science, Royal Police Cadet Academy

บทคัดย่อ

บทความนี้เป็นการทบทวนวรรณกรรม เพื่อหาองค์ความรู้ในเรื่องที่เป็นประเด็นข่าวที่สังคมให้ความสนใจ มีวัตถุประสงค์เพื่อศึกษารายละเอียดต่างๆ ที่มีส่วนส่งเสริมให้พยานหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่มีความน่าเชื่อถือ โดยรายละเอียดดังกล่าวประกอบด้วยวิธีปฏิบัติของเจ้าหน้าที่ในการเก็บรวบรวมหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่ การนำหลักฐานจากอุปกรณ์โทรศัพท์เคลื่อนที่ไปใช้เป็นหลักฐานทางกฎหมาย เครื่องมือที่ใช้พิสูจน์หลักฐานที่เกี่ยวกับโทรศัพท์เคลื่อนที่ และการรับฟังและชั่งน้ำหนักพยานของศาล ผลการศึกษาสรุปความได้ว่า การตรวจสอบความถูกต้องของข้อมูลด้วยวิธีตรวจสอบค่า CRC หรือ แฮช เป็นทางเลือกหนึ่งของวิธีการที่จะช่วยให้พยานหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่มีความน่าเชื่อถือ

คำสำคัญ: ความน่าเชื่อถือ, พยานหลักฐานทางอิเล็กทรอนิกส์, โทรศัพท์เคลื่อนที่

Abstract

This article was to review literature for knowledge about social interests. The purpose aimed to study the details that contributed to reliable mobile phone forensics. Those details include how the authorities collected electronic evidence from mobile phones, how it had been used as evidence, how to use proofreading tools related to smartphone, and hearing and admissibility of evidence in court. The results indicated that the validation of data by CRC or hash was an alternative way of making electronic evidence obtained from a smartphone more reliable.

Keywords: Reliability, Electronic Evidence, Mobile Phones

บทนำ

โทรศัพท์เคลื่อนที่หรือโทรศัพท์มือถือ คือ อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการสื่อสารสองทาง โดยใช้คลื่นวิทยุติดต่อกับเครือข่ายโทรศัพท์ผ่านสถานีฐานเครือข่ายโทรศัพท์ของผู้ให้บริการ โทรศัพท์เคลื่อนที่เครื่องแรกถูกผลิตขึ้นเมื่อปี พ.ศ.2516 โดย มาร์ติน คูเปอร์ (Martin Cooper) นักประดิษฐ์ของบริษัทโมโตโรลา จากนั้นได้พัฒนาอย่างต่อเนื่องกระทั่งปี พ.ศ.2529 องค์การโทรศัพท์แห่งประเทศไทยได้นำระบบ NMT (Nordic Mobile Telephone System) เปิดให้บริการโทรศัพท์เคลื่อนที่เป็นครั้งแรกในเขตกรุงเทพ ปริมณฑล และจังหวัดชายฝั่งด้านตะวันออก ก่อนขยายบริการไปทั่วประเทศในเวลาต่อมา กระทั่งปัจจุบันประเทศไทยมีผู้ใช้โทรศัพท์เคลื่อนที่มากถึง 38.2 ล้านคน (เปี่ยมศักดิ์ เมนะเศวต สันทัด ศิริอนันต์ไพบูลย์ และสมชัย บวรกิตติ, 2555) โทรศัพท์เคลื่อนที่เป็นอุปกรณ์ที่ผู้คนเกือบทั้งหมดจำเป็นต้องใช้เพื่อการติดต่อสื่อสารและเชื่อมต่อข้อมูลส่วนตัว ซึ่งยอมรับโดยทั่วกันว่า เป็นปัจจัยหนึ่งที่สำคัญในการดำรงชีวิตของคนในสังคมปัจจุบัน โดยเฉพาะอย่างยิ่งโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟน (Smartphone) ที่มีความสามารถมากกว่าการโทรออกและรับสาย ด้วยความที่สมาร์ทโฟนมีระบบปฏิบัติการอยู่ภายในทำให้สามารถทำงานได้ในลักษณะเดียวกันกับเครื่องคอมพิวเตอร์ มีพื้นที่เก็บข้อมูลเสมือนคอมพิวเตอร์ที่สามารถใช้งานได้หลากหลายทั้งบันทึกข้อมูล เก็บข้อมูล เผยแพร่ข้อมูล รวมถึงการใช้ทำธุรกรรมต่างๆ ได้ คุณสมบัติของโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟนที่สามารถใช้งานได้หลากหลายทำให้มิจฉาชีพใช้เป็นเครื่องมือในการก่ออาชญากรรม ในความผิดอาญาที่หลากหลายเช่นกัน เช่น ความผิดเกี่ยวกับความมั่นคง ความผิดเกี่ยวกับทรัพย์ ความผิดทางเพศ (สำนักงานตำรวจแห่งชาติ, 2553) ต่างกันอย่างสิ้นเชิงกับเจ้าหน้าที่ที่นำคุณสมบัติของโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟนใช้เป็นแหล่งข้อมูลของการใช้เป็นพยานหลักฐาน เช่น ข้อมูลการติดต่อสื่อสารทางโทรศัพท์ รายชื่อผู้ติดต่อ ปฏิทิน รวมถึงการระบุถึงฐานที่อยู่ของผู้ใช้ในช่วงขณะหนึ่ง เป็นต้น

การที่เจ้าหน้าที่นำแหล่งข้อมูลจากโทรศัพท์เคลื่อนที่ใช้เป็นพยานหลักฐานในชั้นศาล แม้ว่าจะมีกฎหมายกำหนดให้สามารถรับฟังเป็นพยานหลักฐานได้ แต่ปัญหาสำคัญคือ ความน่าเชื่อถือของพยานหลักฐานที่เจ้าหน้าที่นำไปแสดงต่อศาล ดังที่กล่าวไว้ว่า “การชั่งน้ำหนักพยานหลักฐานคดีอาญากฎหมายกำหนดให้เป็นดุลยพินิจของศาล” (สำนักงานคณะกรรมการกฤษฎีกา, 2551) เช่นนี้จึงจำต้องกำหนดหลักเกณฑ์ วิธีการ มาตรฐาน และขั้นตอนของการนำข้อมูลออกจากโทรศัพท์เคลื่อนที่และรูปแบบการนำเสนอพยานหลักฐาน เพื่อเป็นการรับรองพยานหลักฐานว่าเป็นหลักฐานที่ได้มาโดยผ่านกระบวนการที่ได้มาตรฐานสากล เพื่อให้ศาลสามารถนำไปประกอบการพิจารณาได้ในมาตรฐานเดียวกัน อย่างไรก็ดี แม้ปัจจุบันกฎหมายยังไม่มีการกำหนดหลักเกณฑ์ วิธีการ มาตรฐาน

และขั้นตอนของคดีอาญา ที่จะนำข้อมูลโทรศัพท์เคลื่อนที่ใช้เป็นพยานในรูปพยานอิเล็กทรอนิกส์ไว้อย่างชัดแจ้ง แต่ประมวลวิธีพิจารณาความอาญามาตรา 227 บัญญัติไว้ว่า "ให้ศาลใช้ดุลยพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง..." (สำนักงานคณะกรรมการกฤษฎีกา, 2551) เท่ากับเป็นการเปิดโอกาสให้ศาลใช้ดุลยพินิจในการพิจารณาว่า หลักฐานทางอิเล็กทรอนิกส์ที่อยู่ในกระบวนการพิจารณานั้นมีความน่าเชื่อถือหรือไม่ ดังนั้นการทำให้หลักฐานมีความน่าเชื่อถือจึงเป็นเรื่องที่สำคัญ

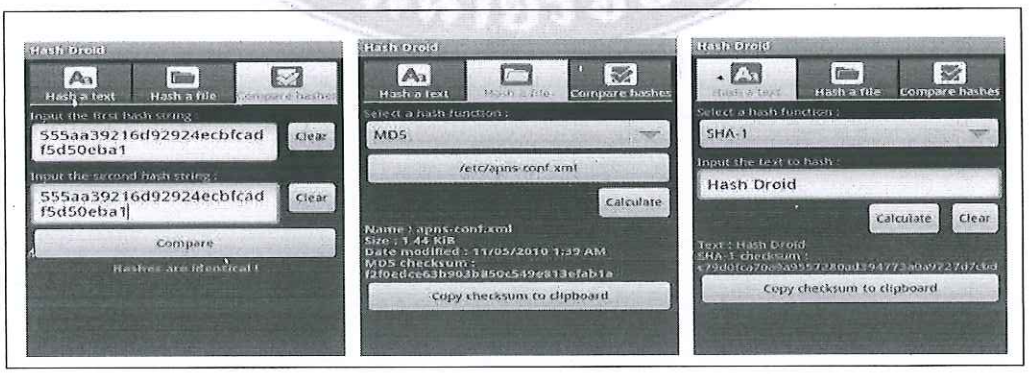
เมื่อมีการกระทำความผิดอาญาโดยใช้โทรศัพท์เคลื่อนที่ ข้อมูลที่ปรากฏในโทรศัพท์จึงถูกใช้เป็นพยานหลักฐานประเภทหนึ่งของการสืบสวน ดำเนินคดี และพิสูจน์ถึงการกระทำ แต่ข้อมูลดังกล่าว เช่น กระบวนการได้มาซึ่งข้อมูล การกู้ข้อมูลที่ถูกลบ การตรวจสอบฐานข้อมูล การคัดลอกหรือประมวลผลข้อมูลนั้น มีปัญหาด้านความน่าเชื่อถือในการที่ศาลจะรับฟังข้อมูลพยานหลักฐานเพื่อพิจารณาพิพากษาคดี หรือที่เรียกว่าการพิสูจน์หลักฐานจากอุปกรณ์โทรศัพท์เคลื่อนที่ (Mobile Phone Forensics) (สำนักงานตำรวจแห่งชาติ, 2553) ดังนั้นเจ้าหน้าที่พึงต้องปฏิบัติงานอย่างรอบคอบรัดกุมเริ่มตั้งแต่การเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับ (1) การตรวจสอบโทรศัพท์เคลื่อนที่ภายนอก (2) การบรรจุภัณฑ์ (3) การขนส่งไปที่ห้องปฏิบัติการ และ (4) การทำสำเนาพยานหลักฐานเพื่อให้หลักฐานนั้นมีความน่าเชื่อถือ (สุวิมล แก้วคูณ, 2557) ซึ่งมีแนวทางปฏิบัติดังนี้

การตรวจสอบโทรศัพท์เคลื่อนที่ภายนอก: พยานหลักฐานโทรศัพท์เคลื่อนที่ภายนอกมีหลากหลายชนิด ทั้งรอยนิ้วมือแฝง คราบเลือด ซึ่งพยานหลักฐานแต่ละชนิดต่างมีกระบวนการเก็บข้อมูลที่แตกต่างกัน โดยการตรวจสอบโทรศัพท์เคลื่อนที่เบื้องต้น เจ้าหน้าที่จำเป็นต้องตรวจสอบว่าโทรศัพท์อยู่ในสถานะปิดหรือเปิด มีการเชื่อมต่อระบบเครือข่ายต่างๆ อยู่หรือไม่ เมื่อทราบถึงสถานะแล้ว เพื่อป้องกันมิให้เกิดการปนเปื้อน หรือเปลี่ยนแปลงข้อมูลภายในของอุปกรณ์อิเล็กทรอนิกส์ในเบื้องต้น หากเครื่องโทรศัพท์เคลื่อนที่เปิดอยู่ห้ามปิด ตรงข้ามหากเครื่องโทรศัพท์เคลื่อนที่ปิดอยู่ห้ามเปิด การให้ความสำคัญต่อข้อมูลที่สามารถสูญหายได้เมื่อปิดหรือเปิด ตลอดจนการพิจารณาเรื่องการซ่อนอำพราง การทำลายข้อมูล และการเข้ารหัสลับข้อมูลในอุปกรณ์ต่างๆ ดังนั้นเจ้าหน้าที่จึงต้องมีมาตรฐานการปฏิบัติงานตามที่หน่วยงานได้กำหนด

การบรรจุภัณฑ์: การตรวจสอบภายนอกโทรศัพท์เคลื่อนที่ต้องทำการบรรจุภัณฑ์พยานหลักฐานที่ต้องการเคลื่อนย้ายกลับไปยังสถานีหรือห้องปฏิบัติการเพื่อทำการตรวจพิสูจน์ต่อไป เจ้าหน้าที่ต้องเลือกบรรจุภัณฑ์ที่เหมาะสมกับอุปกรณ์แต่ละชนิด เช่น โทรศัพท์มือถือ อุปกรณ์จีพีเอส อุปกรณ์เคลื่อนที่บางชนิดที่จำเป็น ต้องถูกบรรจุลงถุงป้องกันคลื่นแม่เหล็กไฟฟ้า (Faraday Bag) ขณะเดียวกันอุปกรณ์จัดเก็บข้อมูลจำพวกฮาร์ดดิสก์ ต้องถูกบรรจุในถุงป้องกันไฟฟ้าสถิต (Anti-Static Bag) เป็นต้น

การขนส่งไปที่ห้องปฏิบัติการ: เจ้าพนักงานต้องบันทึกข้อมูลลงเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน (Chain of Custody) ซึ่งหมายถึง ข้อมูลที่ระบุรายละเอียดของพยานหลักฐาน และการส่งต่อพยานหลักฐาน โดยเจ้าหน้าที่ที่รับผิดชอบต้องมีการบันทึกไว้ เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บจากที่เกิดเหตุมาอยู่ในความครอบครองของเจ้าหน้าที่ที่เกี่ยวข้อง จนถึงเมื่อสิ้นสุดคดี ไว้ในแบบฟอร์ม ซึ่งจะเป็นประโยชน์หากผู้ที่เกี่ยวข้องต้องไปให้การในศาล เพราะต้องสามารถยืนยันได้ว่าในระหว่างการครอบครองพยานหลักฐานชิ้นนั้นได้ถูกจัดเก็บไว้ที่ไหน ได้ถูกนำไปทำอะไรบ้าง มีปัจจัยที่จะทำให้พยานหลักฐานเปลี่ยนแปลงหรือไม่ ได้ส่งต่อให้กับบุคคลอื่นหรือไม่ อีกทั้งจะต้องสามารถระบุตัวตนของผู้รับผิดชอบได้ตลอดเวลาที่ครอบครองพยานหลักฐาน

การทำสำเนาพยานหลักฐาน: การทำ Mobile Phone Forensics ต้องรักษาไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐาน โดยเจ้าหน้าที่ผู้ปฏิบัติงานจะไม่ดำเนินการตรวจพิสูจน์หลักฐานใดๆ ต่อพยานหลักฐานต้นฉบับ แต่จำเป็นต้องทำสำเนาหลักฐานขึ้นมาอย่างน้อยสองชุด โดยชุดแรกไว้ใช้ในการตรวจพิสูจน์หลักฐาน และชุดที่สองเป็นชุดสำรอง กรณีเกิดความผิดพลาดขึ้นกับสำเนาชุดแรก ในขั้นตอนการทำสำเนานี้ เจ้าหน้าที่จำเป็นต้องอาศัยอุปกรณ์พิเศษที่เรียกว่า อุปกรณ์ป้องกันการเขียนทับข้อมูล (Write Blocker) ทำหน้าที่ป้องกันมิให้มีข้อมูลใดถูกเขียนเพิ่มลงไปยังพยานหลักฐานต้นฉบับ เพื่อป้องกันมิให้เกิดการปนเปื้อนของพยานหลักฐาน และเมื่อเสร็จสิ้นในขั้นตอนการทำสำเนาหลักฐานเจ้าหน้าที่จะต้องทำการยืนยันความถูกต้องแท้จริงของสำเนาหลักฐาน เพื่อให้แน่ใจว่าสำเนาหลักฐานนั้นมีข้อมูลตรงตามหลักฐานต้นฉบับทุกประการ โดยใช้กระบวนการทางคณิตศาสตร์ที่เรียกว่า การย่อยข้อมูล (Hashing) โดยการเข้ารหัสด้วยฟังค์ชั่นแฮช (Cryptographic Hash Function) ซึ่งทำให้เจ้าหน้าที่สามารถเปรียบเทียบ และได้ทราบว่าข้อมูลที่อยู่ภายในของสำเนาหลักฐานนั้นตรงกับข้อมูลของพยานหลักฐานต้นฉบับหรือไม่



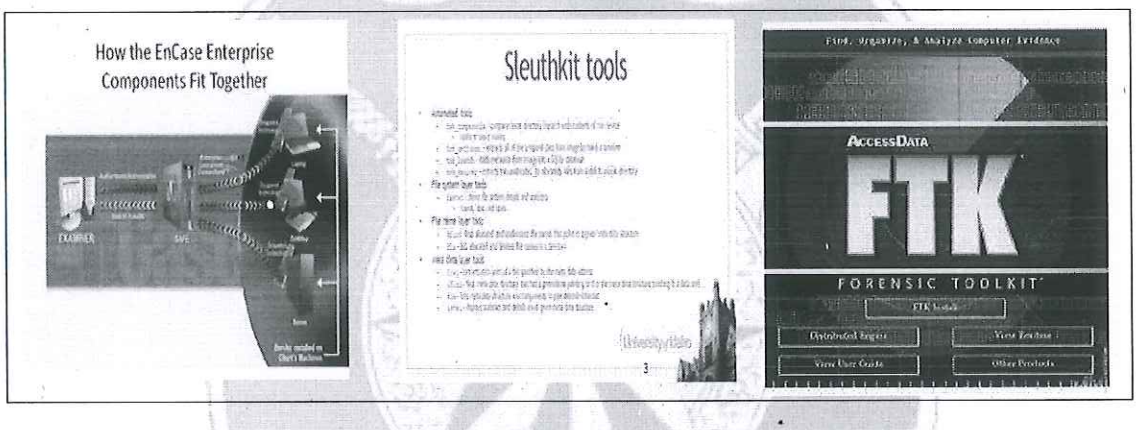
ภาพที่ 1 ตัวอย่างภาพหน้าจอของ Hash

การรวบรวมพยานหลักฐานของเจ้าหน้าที่ผู้ปฏิบัติงาน จำต้องจัดเตรียมเครื่องมืออุปกรณ์ที่จำเป็นที่มีอยู่มากมาย ได้แก่ กล้องถ่ายภาพดิจิทัล (Digital Camera) กล้องบันทึกวิดีโอ (Video Camera) กล้องป้องกันไฟฟ้าสถิต (Anti-Static Drive Box) กระเป๋าภาคสนาม (Pelican Bag) ถุงพลาสติกสำหรับเก็บพยานหลักฐาน (Plastic Evidence Bag) ถุงกระดาษสำหรับเก็บพยานหลัก ฐานขนาดเล็ก (Paper Evidence Bag) อุปกรณ์ทำสำเนาหน่วยความจำ (Memory Dump Tool) และชุดรวบรวม (Volatile Data) ชุดทำสำเนาข้อมูล (Forensic Duplicator) ชุดตรวจวิเคราะห์โทรศัพท์เคลื่อนที่ (Mobile Phone Forensics Tool) และ ถุงป้องกันคลื่นวิทยุ (Faraday Container) (สุวิมล แก้วคูณ, 2557) หลังจากเตรียมเครื่องมืออุปกรณ์เสร็จสิ้น ชุดเจ้าหน้าที่ปฏิบัติงานที่ประกอบด้วยหัวหน้าชุดปราบปราม ชุดตรวจค้นและรวบรวมพยานหลักฐาน ชุดเทคนิคและการถ่ายภาพ ชุดขนส่งและคุ้มครองพยานหลักฐาน ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ ร่วมกันเข้าดำเนินการตรวจค้นโทรศัพท์เคลื่อนที่รวมทั้งอุปกรณ์สื่อสาร

หลักของเจ้าหน้าที่ในการตรวจค้นโทรศัพท์เคลื่อนที่รวมทั้งอุปกรณ์สื่อสาร ควรปฏิบัติตามขั้นตอนดังนี้ (1) ตรวจสอบว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิต (2) หากโทรศัพท์เคลื่อนที่นั้นเปิดอยู่ห้ามปิด และหากโทรศัพท์เคลื่อนที่นั้นปิดอยู่ห้ามเปิด (3) ดำเนินการถ่ายภาพพยานหลักฐานให้ชัดเจน โดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อและรุ่นของโทรศัพท์เคลื่อนที่เพื่อแสดงถึงสภาพของพยานหลักฐานขณะเข้าเก็บหลักฐาน (4) บันทึกวิดีโอตลอดการปฏิบัติงาน พร้อมกับถ่ายหน้าจอเครื่องโทรศัพท์เคลื่อนที่ (5) ลงรายละเอียดลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน (6) ตรวจสอบสถานะของแบตเตอรี่ที่คงเหลือและจัดหาแหล่งจ่ายไฟกรณีจำเป็น (7) บรรจุโทรศัพท์เคลื่อนที่และอุปกรณ์สื่อสารลงในบรรจุภัณฑ์เฉพาะด้าน (8) ถ่ายภาพพยานหลักฐานหลังจากบรรจุลงบรรจุภัณฑ์เรียบร้อยแล้ว (9) ตรวจความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง (10) บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน พร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน (11) ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานให้ชุดขนส่ง และคุ้มครองพยานหลักฐาน พร้อมลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน (13) จัดเก็บและตรวจสอบอุปกรณ์ที่ใช้ในการปฏิบัติงานเพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ (ณัฐพงษ์ ลิ้มแดงสกุล, 2554)

ทั้งนี้การนำหลักฐานอุปกรณ์โทรศัพท์เคลื่อนที่ไปใช้เป็นหลักฐานทางกฎหมายต้องปฏิบัติตามหลักสากล 4 ประการ (1) การเก็บรักษาหลักฐาน รักษาข้อมูลในลักษณะที่ไม่มีการเปลี่ยนแปลงข้อมูล

ที่พบซึ่งเกี่ยวข้องกับการโคลนนิ่งฮาร์ดดิส (Forensic Images) (2) การแบ่งข้อมูล เมื่อมีการพบหลักฐานและจำเป็นต้องนำข้อมูลออกจาก Forensic Images การแสดงผลขึ้นอยู่กับปริมาณข้อมูลอาจใช้การพิมพ์ข้อมูลออกมา แต่กรณีข้อมูลมีจำนวนมาก เช่น ประวัติการใช้งานอินเทอร์เน็ตที่มีข้อมูลมากกว่า 100 หน้า ต้องแสดงผลในรูปของสื่ออิเล็กทรอนิกส์ (3) การระบุหลักฐาน และการนำมาแสดงเป็นหน้าที่ของเจ้าหน้าที่ Computer Forensic Examiners ที่จะนำข้อมูลที่ถูกต้องมาแสดงซึ่งถือเป็นเรื่องสำคัญมาก เจ้าหน้าที่ต้องไม่เชื่อผลของเครื่องมือเพียงอย่างเดียว และจำต้องสามารถตรวจสอบข้อมูลที่ได้จากซอฟท์แวร์นั้น (4) หลักฐานที่ได้ต้องมีการจดบันทึกการทำงานที่เกี่ยวกับสื่อดิจิทัลทุกขั้นตอนตลอดการค้นหาข้อมูล การจดบันทึกจะต้องมีข้อมูลเพียงพอที่จะทำให้บุคคลสามารถเข้าใจได้



ภาพที่ 2 ชุดโปรแกรม EnCase, Sleuthkit, FTK เพื่อพิสูจน์หลักฐาน (สถาบันฝึกอบรมและวิจัยการพิสูจน์หลักฐานตำรวจ, 2559)

เครื่องมือที่ใช้พิสูจน์หลักฐานที่เกี่ยวกับโทรศัพท์เคลื่อนที่ (Mobile Phone Forensics) มีหลากหลายตามแต่สถานการณ์และสภาพของพยานหลักฐาน เช่น การกู้ข้อมูลที่ถูกลบจากหน่วยความจำที่อาจจำเป็นต้องใช้เครื่องมือพิเศษ ซึ่งปัจจุบันมีชุดโปรแกรมในการพิสูจน์หลักฐานหลากหลายรูปแบบ เช่น EnCase, X-Ways, XRY, FTK, IEF, PYFlag, Sleuthkit, OCFA, DFF, Snorkel (Raghavan,2013) ขั้นตอนของเจ้าหน้าที่ ในการตรวจวิเคราะห์พยานหลักฐานโทรศัพท์เคลื่อนที่มีหลักปฏิบัติดังนี้ (1) ตรวจสอบสิทธิและอำนาจหน้าที่ก่อนจะปฏิบัติการเพื่อให้แน่ใจว่าการปฏิบัติงานเป็นไปโดยชอบด้วยกฎหมาย (2) พิจารณารูปแบบการกู้คืนข้อมูล เพื่อให้ทราบว่าจำเป็นต้องใช้วิธีการกู้คืนข้อมูลทางกายภาพ (Physical Extraction) หรือทางตรรกะ (Logical Extraction) ในเครื่องโทรศัพท์เคลื่อนที่เพื่อให้ได้ข้อมูลตรงตามที่ใช้เป็นหลักฐานทางกฎหมาย (3) ตรวจสอบประวัติการใช้งาน (Timeframe Analysis)

วัตถุประสงค์เพื่อมุ่งศึกษาพฤติกรรมการใช้งานเครื่องโทรศัพท์เคลื่อนที่ของผู้ต้องสงสัย ที่อาจช่วยให้เจ้าหน้าที่สามารถเข้าใจถึงวิธีการก่ออาชญากรรม และแหล่งข้อมูลที่สามารถใช้เป็นพยานหลักฐานในการดำเนินคดีต่อไป (4) ตรวจสอบข้อมูลที่ถูกซ่อน (Data Hiding Analysis) และข้อมูลที่ถูกเข้ารหัสลับ (Encryption File) เนื่องจากข้อมูลเหล่านี้อาจสำคัญต่อการสืบสวนก็เป็นได้ (5) ตรวจสอบการใช้งานโปรแกรมและเอกสารต่างๆ (Application and File Analysis) ในโทรศัพท์เคลื่อนที่ ที่อาจสามารถนำไปสู่พยานหลักฐานอื่นที่สำคัญ เช่น การตรวจสอบพบว่ามีการติดตั้งโปรแกรมตกแต่งรูปในโทรศัพท์เคลื่อนที่ เป็นต้น (6) ระบุแหล่งที่มาของข้อมูลและตัวผู้ใช้งานโทรศัพท์เคลื่อนที่ เจ้าหน้าที่ต้องสามารถระบุแหล่งที่มาของข้อมูลชัดเจน เช่น จดหมายอิเล็กทรอนิกส์ ข้อความสั้น รูปภาพ เอกสาร และข้อมูลที่ถูกบันทึกรับ – ส่งออกจากโทรศัพท์ เคลื่อนที่เครื่องใด เวลาเท่าไหร่ รวมทั้งการระบุตัวผู้อาจเข้าถึงโทรศัพท์เคลื่อนที่ในช่วงเวลาต่างๆ เมื่อเสร็จสิ้นขั้นตอนการตรวจวิเคราะห์พยานหลักฐาน จึงเข้าสู่ขั้นตอนการสรุปผล เจ้าหน้าที่จำต้องเขียนรายงานสรุปผลการตรวจวิเคราะห์ เพื่อแสดงข้อมูลและหลักฐานที่พบในโทรศัพท์เคลื่อนที่ หลักปฏิบัติที่สำคัญ คือเจ้าหน้าที่ต้องไม่มีการแสดงความเห็นใดต้องคงไว้ซึ่งข้อเท็จจริงที่ปรากฏเท่านั้น กรณีจำเป็นต้องอาศัยความเห็นผู้เชี่ยวชาญ ศาลจะทำการร้องขอต่อพยานผู้เชี่ยวชาญ ให้ส่งรายงานแสดงความคิดเห็นต่อศาลเอง

การที่ศาลจะวินิจฉัยหรือคัดเลือกว่า พยานหลักฐานชิ้นใดสามารถนำเข้าสู่สำนวนได้โดยชอบตามกฎหมาย หรือการรับฟังพยานหลักฐาน (Admissibility of Evidence) ในส่วนของหลักฐานที่ได้จากโทรศัพท์เคลื่อนที่ที่เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ แม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้บัญญัติอย่างชัดแจ้ง แต่ข้อความที่ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคล ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้” แสดงให้เห็นว่าหากพยานหลักฐานอิเล็กทรอนิกส์น่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ได้ โจทก์ก็สามารถอ้างเป็นพยานหลักฐานอิเล็กทรอนิกส์ได้ โดยการนำพยานดังกล่าวมาสืบได้หลายลักษณะ (สุวิมล แก้วคูณ, 2557)

1. การนำสืบพยานหลักฐานอิเล็กทรอนิกส์อย่างพยานเอกสาร เป็นการนำเอาข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในโทรศัพท์เคลื่อนที่ ทำการประมวลผลผ่านชุดคำสั่งและอุปกรณ์ดึงข้อมูลจากอุปกรณ์บันทึกความจำในโทรศัพท์เคลื่อนที่ และทำออกเป็นสิ่งพิมพ์ออก (Print Out) ซึ่งเป็นการแสดงข้อมูลออกมาในรูปเอกสาร โดยจะต้องมีคำเบิกความของผู้ที่ทำข้อมูลประกอบด้วยว่าได้มีการทำข้อมูลขึ้นมาจริงและมีเนื้อหาตรงกับที่แสดงในสิ่งพิมพ์ออก

2. การนำสืบพยานหลักฐานอิเล็กทรอนิกส์อย่างพยานวัตถุ การทำการพิสูจน์หลักฐานจากโทรศัพท์เคลื่อนที่อย่างพยานวัตถุ คือ ตัวเครื่องโทรศัพท์เคลื่อนที่ รวมถึงอุปกรณ์ภายในที่บันทึกข้อมูลไม่ใช่ตัวข้อมูลที่อยู่ภายใน ซึ่งต้องนำสืบพิสูจน์ให้ศาลเชื่อได้ว่า ข้อมูลที่ได้มานั้นได้มีการนำออกมาจากตัวเครื่องโทรศัพท์เคลื่อนที่ หรืออุปกรณ์ภายในที่บันทึกข้อมูลจริงปราศจากการดัดแปลงแก้ไข

3. การนำสืบโดยอาศัยผู้เชี่ยวชาญ ในการให้ความเห็นทางวิชาการหรืออธิบายถึงกระบวนการทำงานของระบบคอมพิวเตอร์ในการสร้างข้อมูลนั้น ซึ่งเป็นดุลยพินิจของศาลที่จะเชื่อหรือไม่ก็ได้ หากเป็นคำเบิกความที่ไม่ใช่ข้อมูลเชิงวิชาการ แต่เป็นคำเบิกความเกี่ยวกับข้อเท็จจริงก็จะมีน้ำหนักมากขึ้น เนื่องจากประเทศไทยไม่ใช้ระบบลูกขุน ดุลยพินิจในการชั่งน้ำหนักพยานหลักฐานต่างๆ จึงขึ้นอยู่กับศาล

การชั่งน้ำหนักพยาน (Weighing of Evidence) เพื่อพิจารณาว่าพยานหลักฐานเกี่ยวกับประเด็นหรือมีน้ำหนักเพียงพอหรือไม่นั้น กฎหมายได้บัญญัติไว้ในทิศทางเดียวกัน คือ ให้ศาลใช้ดุลยพินิจ เช่น

ประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 227 บัญญัติว่า “ให้ศาลใช้ดุลยพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำความผิดจริง และจำเลยเป็นผู้กระทำความผิดนั้น เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ ให้ยกประโยชน์แห่งความเสงสัยนั้นให้จำเลย” (สำนักงานคณะกรรมการกฤษฎีกา, 2551)

พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์มาตรา 11 วรรค 2 บัญญัติว่า “ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์ จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะ หรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษาความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง ให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย” (สำนักงานคณะกรรมการกฤษฎีกา, 2552)

จากบทบัญญัติข้างต้นทั้ง เรื่องการรับฟังพยานหลักฐาน และการชั่งน้ำหนักพยานหลักฐาน แสดงให้เห็นว่า ถึงแม้ว่าจะมีกฎหมายบางเรื่องรองรับให้เสนอข้อมูลทางอิเล็กทรอนิกส์ หรือข้อมูลจากโทรศัพท์เคลื่อนที่เป็นพยานหลักฐานได้ แต่ยังไม่มีบทบัญญัติในเรื่องการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ หรือพยานหลักฐานที่ได้จากโทรศัพท์เคลื่อนที่ที่ใช้กับคดีอาญาทั่วไป อีกทั้งไม่มีการกำหนดวิธีการนำเสนอ และนำสืบพยานหลักฐานที่ชัดเจน ซึ่งกฎหมายได้ให้อำนาจศาลในการใช้ดุลยพินิจในการชั่งน้ำหนักพยานหลักฐานตามที่ศาลเห็นสมควร ทำให้ศาลต้องอาศัยหลักปฏิบัติ หรือประสบการณ์ของศาลเองในการพิจารณาว่า พยานหลักฐานทางอิเล็กทรอนิกส์ที่นำเข้าสู่กระบวนการพิจารณานั้นมีความน่าเชื่อถือหรือไม่ ซึ่งอาจก่อให้เกิดปัญหาในการรับฟังพยานหลักฐาน และการชั่งน้ำหนักพยาน

ที่มีลักษณะเดียวกัน และมีวิธีการได้มาที่เหมือนกัน แต่ศาลอาจพิจารณารับฟัง และให้น้ำหนักแตกต่างกันขึ้นอยู่กับดุลยพินิจของผู้พิพากษาเป็นรายบุคคล

มิอาจปฏิเสธว่าข้อมูลที่ได้จากโทรศัพท์เคลื่อนที่ มีลักษณะเฉพาะตัวที่สามารถแก้ไขหรือปรับแต่งข้อมูลได้ จึงเป็นปัญหาในการรับฟังข้อมูลที่ได้จากโทรศัพท์เคลื่อนที่เป็นพยานหลักฐานว่า สามารถยืนยันความถูกต้องแท้จริง (Authentication) ได้หรือไม่ ดังนี้ (Hippel, 1994)

1. การระบุตัวผู้กระทำความผิดและใช้ข้อมูล โดยเฉพาะอย่างยิ่งการระบุว่าความผิดนั้นอยู่ที่ใดและใครเป็นผู้ส่ง นอกจากนี้ยังต้องระบุว่า ข้อมูลนั้นส่งมาจากผู้ใดและใครเป็นผู้ใช้ ใครเป็นเจ้าของข้อมูล เมื่อได้นำโทรศัพท์เคลื่อนที่มาเป็นพยานหลักฐาน แล้วต้องสามารถพิสูจน์ได้ว่าโทรศัพท์เคลื่อนที่ดังกล่าวเป็นของใคร ใครเป็นผู้ครอบครอง และผู้นั้นเป็นผู้ใช้งานในขณะกระทำผิดหรือไม่ รวมถึงพื้นที่ที่มีการใช้งาน เพื่อให้สามารถพิจารณาเขตอำนาจศาลที่จะพิจารณาพิพากษาคดีดังกล่าว

2. ความถูกต้องสมบูรณ์ของพยานหลักฐานที่ได้มา ดังที่กล่าวข้างต้นว่าข้อมูลที่ได้จากโทรศัพท์เคลื่อนที่มีลักษณะเฉพาะตัวที่สามารถแก้ไขหรือปรับแต่งข้อมูลได้ ทั้งก่อนและระหว่างรวบรวมพยานหลักฐาน ซึ่งเป็นปัญหาว่าจะสามารถพิสูจน์ได้อย่างไรว่าข้อมูลดังกล่าวเป็นข้อมูลที่แท้จริง ไม่มีการแก้ไขหรือปรับแต่ง ซึ่งนอกจากจะส่งผลถึงความน่าเชื่อถือของพยานหลักฐานแล้ว ยังอาจทำให้ศาลไม่รับพยานหลักฐานดังกล่าว หากไม่สามารถยืนยันความถูกต้องที่แท้จริงของข้อมูลจากโทรศัพท์เคลื่อนที่ได้

3. ปัญหาการลบข้อมูล (Stickiness Problem) สามารถทำได้ตั้งแต่เป็นการลบเพียงสารบัญ (Index) ของข้อมูล แต่เนื้อหาของข้อมูลยังคงมีอยู่จนกว่าจะถูกเขียนทับขึ้น หรือเป็นการใช้โปรแกรมในการลบข้อมูลทั้งหมด ปัญหาจะเกิดขึ้นในการกู้ข้อมูลคืน เพราะอาจได้ข้อมูลนั้นไม่สมบูรณ์ ทำให้ฝ่ายจำเลยสามารถยกปัญหานี้มาโต้แย้งในศาลได้

4. ปัญหาในการวิเคราะห์ข้อมูลและนำออกมาใช้เป็นพยานหลักฐาน เนื่องจากลักษณะของข้อมูลยังคงอยู่ในรูปแบบของรหัส (Code) หรือภาษาคอมพิวเตอร์ที่ไม่สามารถเข้าใจดั่งภาษามนุษย์ ดังนั้นจึงต้องมีผู้วิเคราะห์ที่จะต้องแปลงข้อมูลออกมาในรูปหรือภาษาที่บุคคลทั่วไปสามารถเข้าใจได้ ซึ่งในขั้นตอนนี้ต้องแสดงให้ศาลเชื่อได้ว่า ผู้วิเคราะห์มีความเชี่ยวชาญในการแปลงข้อมูล และไม่มีการแก้ไขหรือแปลงให้เนื้อหาผิดจากข้อเท็จจริง

จากปัญหาดังกล่าวจะเห็นได้ว่า แม้กฎหมายจะบัญญัติให้สามารถรับฟังข้อมูลจากโทรศัพท์ เคลื่อนที่เป็นพยานหลักฐานได้ แต่ปัจจุบันกฎหมายยังไม่มีการกำหนดขั้นตอน หลักเกณฑ์ วิธีการ กระบวนการพิสูจน์หลักฐานที่ได้จากโทรศัพท์เคลื่อนที่ (Mobile Phone Forensics) สำหรับใช้พิจารณาคดีอาญาทั่วไป มีเพียงการบัญญัติไว้เฉพาะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทำให้การชั่งน้ำหนักพยานหลักฐาน

ในคดีอาญาทั่วไป เป็นดุลยพินิจของศาลว่าจะเชื่อกระบวนการพิสูจน์ และผู้เชี่ยวชาญที่เป็นผู้วิเคราะห์หรือไม่ เพียงใด ซึ่งอาจก่อให้เกิดปัญหาความแตกต่างในการใช้ดุลยพินิจของผู้พิพากษารายบุคคล

บทสรุป

การนำข้อมูลจากโทรศัพท์เคลื่อนที่มาใช้เป็นพยานหลักฐาน นอกจากกระบวนการได้มาของข้อมูล การกู้ข้อมูลที่ถูกลบ การตรวจสอบฐานข้อมูล คัดลอกข้อมูล เครื่องมือและการแปลผล หลักการสำคัญ คือ "ต้องไม่มีการเปลี่ยนแปลงที่ตัวหลักฐานต้นฉบับ" การตรวจสอบความถูกต้องของข้อมูล (Error Detection and Correction) เป็นวิธีการที่จะช่วยให้เกิดการยอมรับและเชื่อถือในพยานหลักฐาน ซึ่งมี 2 วิธีการ ได้แก่ (1) Error Check Sum วิธีนี้สามารถทำให้รู้ได้ว่าสำเนาหลักฐานนั้นได้ถูกเปลี่ยนแปลงมาก่อนหรือไม่ โดยการตรวจสอบค่า CRC (Cyclic Redundancy Check) ซึ่งค่านี้ต้องมีค่าเหมือนกับไฟล์ที่มีต้นฉบับ จึงจะถือว่าไฟล์สำเนาดังกล่าวมีความสมบูรณ์ (Jain, & Chouhan, 2014) และ (2) แฮช (Hash) ใช้ตรวจสอบความสมบูรณ์ของข้อมูล เปรียบได้ว่าเป็น "ลายนิ้วมือ" ของข้อมูล ฟังก์ชั่นแฮชเป็นฟังก์ชั่นทางเดียว (One-way function) กระทำการโดยการรับอินพุตความยาว และได้เอาท์พุตที่มีความยาวสั้น เรียกว่า (Message Digest) ซึ่งขั้นตอนวิธีของฟังก์ชั่นแฮช (Hash function) ส่วนใหญ่เป็นการแบ่งย่อยข้อมูล และการผสมข้อมูลย่อยทั้งหมดเข้าด้วยกัน เพื่อให้ได้ผลลัพธ์สุดท้าย ผลลัพธ์นี้อาจเรียกว่า ผลบวกแฮช (Hash Sum), ค่าแฮช (Hash Value), รหัสแฮช (Hash Code)

สรุปได้ว่า การที่พยานหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟนจะมีความน่าเชื่อถือ จำต้องผ่านการตรวจสอบความถูกต้องของข้อมูล โดยการใช้เครื่องมือและวิธีการที่ได้มาตรฐานในระดับสากล เพื่อให้หลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่นั้นเป็นที่ยอมรับโดยทั่วกัน

เอกสารอ้างอิง

ณัฐพงษ์ ลิ้มแดงสกุล. (2554). **มาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานและแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์สำหรับกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี**. สารนิพนธ์หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ, มหาวิทยาลัยเทคโนโลยีมหานคร.

เปี่ยมศักดิ์ เมนะเศวต สันทัด ศิริอนันต์ไพบูลย์ และสมชัย บวรกิตติ. (2555). วิวัฒนาการโทรศัพท์ มือถือในช่วง 20 ปีที่ผ่านมา. **วารสารราชบัณฑิตยสถาน.** 37(4): 41-51.

สถาบันฝึกอบรมและวิจัยการพิสูจน์หลักฐานตำรวจ. (2559). **คุณลักษณะเฉพาะเครื่องมือทางวิทยาศาสตร์.** สืบค้นเมื่อ 11 เมษายน 2561. เข้าถึงได้จาก http://www.iftr.forensic.police.go.th/iftr/html/tor_science.php.

สุวิมล แก้วคูณ. (2557). **การใช้ข้อมูลที่ได้จากโทรศัพท์เคลื่อนที่เป็นพยานหลักฐานคดีอาญาในชั้นศาล.** เอกสารวิชาการหลักสูตรผู้บริหารกระบวนการยุติธรรมระดับสูงรุ่นที่ 18. วิทยาลัยการยุติธรรม สำนักงานศาลยุติธรรม.

สำนักงานคณะกรรมการกฤษฎีกา. (2552). **พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.** สืบค้นเมื่อ 11 เมษายน 2561. เข้าถึงได้จาก https://www.bot.or.th/Thai/PaymentSystems/PSServices/i as/ICAS_Printout/พรบ20%ธุรกรรมทางอิเล็กทรอนิกส์.pdf.

สำนักงานคณะกรรมการกฤษฎีกา. (2551). **พระราชบัญญัติให้ใช้ประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ.2477.** สืบค้นเมื่อ 11 เมษายน 2561. เข้าถึงได้จาก http://www.dnp.go.th/mfcd3/division/LAW1/ระเบียบ-กฎหมาย/ป.วิอาญา%202477.pdf.

สำนักงานตำรวจแห่งชาติ. (2553). **องค์ความรู้เรื่องกระบวนการเก็บรวบรวมและรักษาความน่าเชื่อถือของพยานหลักฐานทางอิเล็กทรอนิกส์.** สืบค้นเมื่อ 10 เมษายน 2561. เข้าถึงได้จาก http://pc.edupol.org/do wnload/KM2.pdf.

Hippel, E.V. (1994). "Sticky Information" and the Locus of Problem Solving: Implications for Innovation. **Management Science.** 40(4): 429-439.

Jain, S. and Chouhan, H.H. (2014). Cyclic Redundancy Codes: Study and Implementation. **International Journal of Emerging Technology and Advanced Engineering,** 4(4): 213-217.

Raghavan, S.V. (2013). **A Study of Forensic & Analysis Tools.** Retrieved April 10, 2018. from https://pdfs.semanticscholar.org/21d9/0ab811a068b12ace491c3ab301872163346e.pdf

ผู้เขียน

คำนำหน้า ชื่อ-สกุล	**พันตำรวจโท ดร.พิชศาล พันธุ์วัฒนา**
หน่วยงาน/สังกัด	คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ
ที่อยู่ของหน่วยงาน	เลขที่ 90 อำเภอสามพราน จังหวัดนครปฐม 73110
E-mail:	jodd0509@gmail.com