# เอ็ตด้า จับมือ ภาครัฐ-เอกชนเสนอกรอบการตรวจพยานหลักฐานดิจิทัล

ศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงไอซีที เดินหน้าสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ จับมือหน่วยงานรัฐร่วมพัฒนากรอบการทำงานการจัดเก็บและตรวจวิเคราะห์ข้อมูลอิเล็กทรอนิกส์ “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล” เพื่อยกระดับกระบวนการพิสูจน์หลักฐานดิจิทัล (Digital Forensics) และกระบวนการยุติธรรม ให้ได้ตามมาตรฐาน มอก. 17025: 2548 หรือ ISO 17025:2005 ในระดับสากล เพื่อให้ได้หลักฐานที่น่าเชื่อถือ สามารถใช้อ้างอิง และเป็นที่ยอมรับในชั้นศาล พร้อมประกาศให้หน่วยงานที่เกี่ยวข้องนำไปประยุกต์ใช้ภายในมิถุนายน 2559

สุรางคณา วายุภาพ ผู้อำนวยการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA (เอ็ตด้า) กล่าวว่า ศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) ซึ่งอยู่ภายใต้การดูแลของสพธอ. มีหน้าที่ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล และออกรายงานผลการตรวจวิเคราะห์ตามคำร้องขอของหน่วยงานรักษากฎหมาย ร่วมมือกับหน่วยงานภาครัฐ และเอกชน พัฒนามาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล เพื่อให้มั่นใจว่ากระบวนการเก็บหลักฐาน และตรวจตรวจวิเคราะห์ข้อมูลอิเล็กทรอนิกส์ในหน่วยงานต่างๆ ที่เกี่ยวข้องเป็นไปตามมาตรฐานสากล

ในฐานะที่ ETDA เป็นองค์กรที่มีส่วนร่วมในการดูแลด้านการขับเคลื่อนเศรษฐกิจดิจิทัล รวมถึงการสนับสนุนส่งเสริมและกระตุ้นการเติบโตของพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) เอ็ตด้าเล็งเห็นถึงความสำคัญของการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งการพิสูจน์หลักฐานทางดิจิทัล สามารถเข้ามาช่วยภาคเอกชนในการติดตามร่องรอย และแก้ไขปัญหาที่เกิดจากอาชญากรรมบนไซเบอร์ (Cybercrimes) ที่เพิ่มสูงขึ้นตามการเติบโตของธุรกิจอีคอมเมิร์ซ รวมถึงการทำธุรกรรมด้านการเงินที่มีการขยายตัวและมีมูลค่าทางธุรกิจอย่างมหาศาล ซึ่งจากการสำรวจมูลค่าอีคอมเมิร์ซในประเทศไทยของเอ็ตด้า พบว่าในปี 2557 มีมูลค่าสูงกว่า 2.03 ล้านล้านบาท และจะมูลค่าสูงถึง 2.1 ล้านล้านบาทในปี 2558

“เมื่อเกิดกรณีการโจมตีภาคธุรกิจ อาทิ การขโมยฐานข้อมูล หรือฐานข้อมูลลูกค้าขององค์กรธุรกิจ ตลอดจนกรณีการขโมยข้อมูลส่วนบุคคลเพื่อย้ายเส้นทางการโอนเงินผ่านระบบธนาคารออนไลน์ (e-Banking) หรือการทำผิดกฎหมายบนไซเบอร์อื่นๆ ทางศูนย์ดิจิทัลฟอเรนสิกส์จะเข้ามาช่วยพิสูจน์ วิเคราะห์พยานหลักฐานเพื่อช่วยหน่วยงาน

ยุติธรรมในการติดตามดำเนินคดีให้มีประสิทธิภาพสูงสุด” สุรางคณา กล่าว

โดยในเฟสแรก เอ็ตด้าได้ตั้งคณะทำงานซึ่งประกอบด้วยผู้เชี่ยวชาญจากหน่วยงานต่างๆ รวมถึง สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สถาบันนิติวิทยาศาสตร์, กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สำนักงานตำรวจแห่งชาติ, กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) สำนักงานตำรวจแห่งชาติ, สำนักงานอัยการสูงสุด หน่วยงานศาลและบริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส จำกัด เพื่อเสนอแนวคิดและกำหนดแนวการทำงานร่วมกัน และในเฟสที่สองจะขยายความร่วมมือไปยังหน่วยงานภายใต้การดูแลของศาล

โดยการกำหนดมาตรฐานการทำงาน ยังรวมถึงการปรับปรุงกระบวนการทำงาน (procedure) ข้อกำหนดในการดำเนินงาน (work instruction) และระบบการบริหารจัดการคุณภาพ (Quality Management System) ให้มีความเป็นระบบ และได้มาตรฐานตามหลักตรวจพิสูจน์พยานหลักฐานดิจิทัล และสอดคล้องกับมาตรฐาน ISO 17025:2005 หรือเป็นที่รู้จักตามมาตรฐาน มอก. 17025:2548 ในประเทศไทยอีกด้วย

“กระบวนการการเก็บหลักฐาน ขั้นตอนการตรวจพิสูจน์ถือเป็นหัวใจสำคัญ ที่จะทำให้ผลการตรวจได้รับการยอมรับในชั้นศาล เราต้องสามารถยืนยันได้ว่าหลักฐานที่นำมาตรวจสอบนั้น เป็นหลักฐานชิ้นเดียวกับที่เก็บมาจากสถานที่เกิดเหตุจริง (Authentication) และไม่มีการเปลี่ยนแปลงข้อมูลใดๆ ไปจากเดิม (Integrity) นั่นคือต้องสร้างแนวการทำงานของทุกหน่วยงานที่เกี่ยวข้องกับการตรวจพิสูจน์ให้อยู่บนมาตรฐานเดียวกัน เพื่อความโปร่งใส และความเชื่อถือได้ในการตรวจสอบการทำงาน ทั้งนี้ เราคาดว่าผลสรุปที่ได้จากการทำงานร่วมกันในครั้งนี้ จะสามารถประกาศให้หน่วยงานที่เกี่ยวข้องนำไปประยุกต์ใช้ภายในมิถุนายน 2559” สุรางคณา กล่าว

ในปี 2558 ที่ผ่านมา ศูนย์ดิจิทัลฟอเรนสิกส์ได้ให้บริการตรวจพิสูจน์จำนวน 57 กรณี โดยเกือบ 2 ใน 3 เป็นการตรวจพิสูจน์เพื่อหาพยานหลักฐาน เพื่อสนับสนุนหน่วยงานรักษากฎหมายในการดำเนินการกับผู้ต้องสงสัย หรือผู้กระทำความผิดจากหลักฐานดิจิทัลต่างๆ อาทิ การหาข้อมูลการสื่อสารผ่านโทรศัพท์มือถือ การหาข้อมูลเพื่อหาหลักฐานด้านการละเมิดทรัพย์สินทางปัญญาผ่านอินเทอร์เน็ต รวมถึงการวิเคราะห์คอมพิวเตอร์ เพื่อหาข้อมูล และร่องรอยของมัลแวร์เพื่อเรียกค่าไถ่ (Ransom Malware) เป็นต้น

เราพบว่าปริมาณพยานหลักฐานดิจิทัล ที่ถูกส่งมาพิสูจน์ที่ศูนย์ดิจิทัลฟอเรนสิกส์มีจำนวนสูงถึงกว่า 75 เทราไบต์ ซึ่งเพิ่มขึ้นมากกว่าปริมาณหลักฐานที่ตรวจพิสูจน์ในปี 2557 ถึง 10 เท่า โดยประเภทของหลักฐานแยกได้เป็นโทรศัพท์มือถือและแท็บเล็ต 935 เครื่อง, เมมโมรีการ์ด 128 ชิ้น และฮาร์ดดิสก์จากคอมพิวเตอร์ 67 ลูก และเนื่องจากปริมาณความจุของพื้นที่ในฮาร์ดดิสก์ในปัจจุบันมีขนาดมหาศาล กระบวนการตรวจสอบต่างๆ ทั้งการค้นหาหลักฐานและการทำสำเนาข้อมูล ต้องผ่านการจัดการที่เป็นระบบ สามารถรักษาความต่อเนื่องของการครอบครองพยานหลักฐาน หรือ Chain of Custody ที่ได้มาตรฐาน และสอดคล้องกับมาตรฐานที่เป็นสากล

ทั้งนี้ Chain of custody คือ ห่วงโซ่การคุ้มครองพยานหลักฐาน” หมายถึงข้อมูลที่ระบุรายละเอียดของพยานหลักฐาน และการส่งต่อพยานหลักฐานโดยเจ้าหน้าที่ที่รับผิดชอบ ซึ่งจะต้องมีการบันทึกไว้เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บมาจากที่เกิดเหตุมาอยู่ในความครอบครองของเจ้าหน้าที่ที่เกี่ยวข้องจนสิ้นสุดคดีที่ผ่านมา ศูนย์ดิจิทัลฟอเรนสิกส์มีส่วนช่วยหน่วยงานต่างๆ ในการวิเคราะห์พยานหลักฐานดิจิทัล และสืบค้นข้อมูลเพื่อช่วยเหลือในการคลี่คลายคดีเป็นจำนวนมาก โดยส่วนหนึ่งเกี่ยวข้องกับกรณีกลุ่มคนร้ายที่หลอกผู้เสียหายผ่าน online chat ให้ดาวน์โหลด และติดตั้งมัลแวร์เพื่อขโมยข้อมูลส่วนบุคคลในคอมพิวเตอร์ รวมถึงบันทึกพฤติกรรมการใช้งาน การพิมพ์ Web URL การกรอกชื่อผู้ใช้ ไปจนถึงการกรอกรหัสผ่านของบริการธนาคารอิเล็กทรอนิกส์ (e-Banking) เพื่อทำการล็อกอินเข้าบัญชีอีแบงค์กิ้งของเหยื่อแล้วโอนเงินในบัญชีไปที่อื่น

จากการวิเคราะห์พยานหลักฐานดิจิทัลของผู้เสียหาย ทางศูนย์พบว่าคนร้ายได้หลอกให้ผู้เสียหายดาวน์โหลด และติดตั้งมัลแวร์หลายครั้งเพื่อเลี่ยงการตรวจจับของโปรแกรมแอนตี้ไวรัส และคนร้ายจะซ่อนหมายเลขไอพีแอดเดรสทุกครั้งที่เข้ามาดูความเคลื่อนไหวของบัญชีธนาคารของเหยื่อ อย่างไรก็ตาม ทางศูนย์ฯ สามารถเปิดโปงตัวตน (Identity) ของคนร้ายสำเร็จ โดยสามารถสกัดไอพีแอดเดรสที่คนร้ายใช้ ซึ่งนำไปสู่การจับกุมตัวกลุ่มคนร้าย รวมทั้งตรวจยึดคอมพิวเตอร์ของคนร้ายมาตรวจวิเคราะห์เพื่อยืนยันพฤติกรรมการกระทำความผิด และสามารถเชื่อมโยงกับพยานหลักฐานที่ตรวจพบในคอมพิวเตอร์ของเหยื่อได้สำเร็จ

นอกจากนั้น ยังมีกรณีของมัลแวร์เรียกค่าไถ่ที่พบมากในปีผ่าน ซึ่งทางศูนย์ฯ ได้วิเคราะห์แล้วส่งข้อมูลเพื่อประสานงานไปยังผู้พัฒนาโปรแกรมแอนติไวรัส และหน่วยงานในเครือข่าย CERT เพื่อให้อัพเดตฐานข้อมูลการตรวจจับ และปิดกั้นเซิร์ฟเวอร์ที่เป็นแหล่งดาวน์โหลดมัลแวร์ และยังมีกรณีที่ศูนย์ดิจิทัลฟอเรนสิกส์ได้รับคำร้องขอให้ตรวจพิสูจน์เซิร์ฟเวอร์มากกว่า 20 เครื่องที่ต้องสงสัยว่าให้บริการซมวิดีโอออนไลน์ละเมิดลิขสิทธิ์ ซึ่งในการตรวจพิสูจน์ ต้องทำสำเนาข้อมูลในฮาร์ดดิสก์ทั้งหมดกว่า 150 TB ใช้เวลากว่า 1,000 ชั่วโมง

พร้อมกันนี้ ศูนย์ดิจิทัลฟอเรนสิกส์ยังได้จัดทำระบบอีเลิร์นนิ่ง และจัดอบรมหลักสูตรอบรมดิจิทัลฟอเรนสิกส์ให้กับเจ้าหน้าที่สายยุติธรรม เพื่อให้เข้าใจหลักการการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่เป็นสากล เพื่อเพิ่มความน่าเชื่อถือของกระบวนการยุติธรรมอีกด้วย ในปัจจุบันมีเจ้าหน้าที่ในสายยุติธรรมที่ได้รับการอบรมไปแล้วเป็นจำนวนกว่า 600 นาย