แนวทางการตรวจพิสูจน์อุปกรณ์สื่อสารเคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์

A Model for Mobile Forensic Investigation on Android Devices

ดร.อมรรัตน์ เล็กวิชัย
สถาบันนิติวิทยาศาสตร์

Dr.Amornrat Lekwichai
Central Institute of Forensic Science, Thailand

บทคัดย่อ

ปัจจุบันอุปกรณ์สื่อสารเคลื่อนที่ได้ถูกนำมาใช้เป็นเครื่องมือในการก่ออาชญากรรมทางคอมพิวเตอร์เป็นจำนวนมาก โดยเฉพาะอย่างยิ่งอุปกรณ์แอนดรอยด์ เนื่องจากอุปกรณ์ดังกล่าวมีราคาถูก สามารถหาซื้อได้ง่าย ใช้งานได้สะดวก และสามารถอำพราง ซ่อนเร้น หรือทำลายได้ง่าย รวมถึงมีเทคโนโลยีที่ทันสมัย มีประสิทธิภาพการทำงานสูงขึ้น มีฟังก์ชั่นการทำงานที่หลากหลาย และสามารถเก็บข้อมูลได้มาก ถึงแม้ปัจจุบันจะมีซอฟต์แวร์และฮาร์ดแวร์ที่มีประสิทธิภาพในการดึงข้อมูลการใช้งานต่างๆ เหล่านั้นได้เป็นอย่างดีแล้วก็ตาม แต่ในบางครั้งเราจะพบว่า เครื่องมือหรือซอฟต์แวร์เหล่านั้น ก็ไม่สามารถสกัดข้อมูลการใช้งานในบางประเภทได้ ทำให้ขาดข้อมูลการใช้งานที่สำคัญบางอย่างไป เช่น การติดต่อสื่อสารไม่ว่าจะเป็นด้วยข้อความ ด้วยเสียง หรือการติดต่อผ่าน Applications ต่างๆ รวมถึงการใช้งานอินเตอร์เน็ตและการจดบันทึกในรูปแบบต่างๆ ซึ่งปัญหาดังกล่าวอาจส่งผลกระทบต่อกระบวนการตรวจพิสูจน์ได้ การใช้เทคนิคการตรวจพิสูจน์โดยการดึงข้อมูลการใช้งานจากไฟล์ Database หรือไฟล์ Backup ที่บันทึกไว้ในหน่วยความจำของอุปกรณ์แอนดรอยด์ก็เป็นทางเลือกหนึ่งที่จะทำให้การตรวจพิสูจน์ข้อมูลการใช้งานจากอุปกรณ์เหล่านั้นทำได้ครบถ้วนมากยิ่งขึ้น ดังนั้นผู้ปฏิบัติหน้าที่ในฐานะผู้ตรวจพิสูจน์พยานหลักฐานดิจิทัลจำเป็นที่ต้องทราบถึงตำแหน่งที่จะสามารถเรียกดูข้อมูลการใช้งานต่างๆ เหล่านั้นได้ เพื่อให้ได้ข้อมูลการใช้งานที่มีความสมบูรณ์มากที่สุด อันจะทำให้การตรวจพิสูจน์มีประสิทธิภาพมากยิ่งขึ้น

คำสำคัญ: พยานหลักฐานดิจิทัล, อุปกรณ์สื่อสารเคลื่อนที่, อุปกรณ์แอนดรอยด์

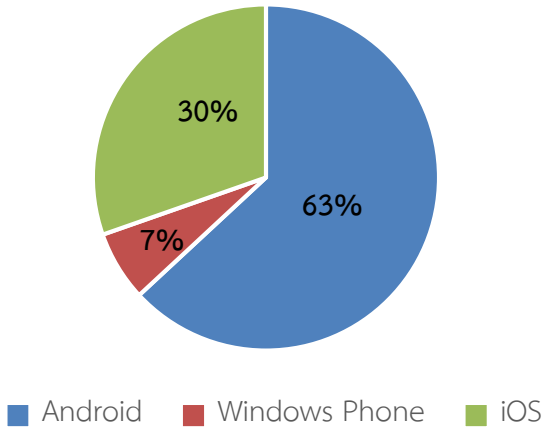
Abstract

Mobile devices, especially android devices have been used as a tool to commit many computer-related crimes. Since these devices are not too expensive for people to purchase, they can readily be camouflaged, hidden or destroyed. Due to modern technologies that enhance the performance of these devices, there are so many functions to be used, and the storage is extremely. Although we have various effective digital forensic tools to acquire usage data from mobile devices, sometimes we have found that some important usage information such as communication with voice messages or contacts from various applications via the Internet is unable to be acquired by commercial softwares. This problem can affect the verification process. Using a proven authentication technique by retrieving usage data from a database file or a backup file saved in an Android device memory is also an option to enable complete device authentication. Hence, digital forensic examiners need to know where to get access to those effectively android applications.

Keywords: Digital Evidence, Mobile Devices, Android Devices

บทนำ

ปัจจุบันอุปกรณ์สื่อสารเคลื่อนที่ได้ถูกนำมาใช้เป็นเครื่องมือในการก่ออาชญากรรมทางคอมพิวเตอร์เป็นจำนวนมาก โดยเฉพาะอุปกรณ์สื่อสารเคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ ดังภาพที่ 1 ด้วยเหตุที่ว่าอุปกรณ์ดังกล่าวมีราคาถูก สามารถหาซื้อได้ง่าย ใช้งานได้สะดวก และสามารถอำพราง ซ่อนเร้น หรือทำลายได้ง่าย รวมถึงมีเทคโนโลยีที่ทันสมัย มีประสิทธิภาพการทำงานสูงขึ้น มีฟังก์ชั่นการทำงานที่หลากหลาย และสามารถเก็บข้อมูลได้มาก จึงทำให้ปัจจุบันข้อมูลต่างๆ ในอุปกรณ์สื่อสารเคลื่อนที่นั้นมีความสำคัญและสามารถใช้เป็นพยานหลักฐานในการดำเนินคดีต่างๆ ได้เป็นอย่างดี เนื่องด้วยอุปกรณ์สื่อสารเคลื่อนที่นั้นเป็นอุปกรณ์อิเล็กทรอนิกส์ ซึ่งสามารถถูกเปลี่ยนแปลง แก้ไข ทำลายข้อมูลได้ง่าย จึงจำเป็นต้องใช้แนวทางการตรวจพิสูจน์ที่ได้มาตรฐาน และเหมาะสมกับรูปแบบการปฏิบัติงานในไทย เพื่อให้ได้ผลการตรวจพิสูจน์ที่ถูกต้อง มีคุณค่าน่าเชื่อถือ และสามารถนำไปใช้ในชั้นศาลได้



ภาพที่ 1 สถิติข้อมูลอุปกรณ์สื่อสารเคลื่อนที่แยกตามระบบปฏิบัติการที่ส่งตรวจพิสูจน์ ณ กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ สถาบันนิติวิทยาศาสตร์ ปี พ.ศ.2560 (สถาบันนิติวิทยาศาสตร์, 2560)

ปัญหาหนึ่งของการตรวจพิสูจน์อุปกรณ์สื่อสารเคลื่อนที่ในห้องปฏิบัติการที่ทำการตรวจยึดมาได้จากสถานที่เกิดเหตุ เพื่อหาข้อมูลความเชื่อมโยงของคดีประเภทต่างๆ นั้น ถึงแม้ปัจจุบันจะมีซอฟต์แวร์และฮาร์ดแวร์ที่มีประสิทธิภาพในการดึงข้อมูลการใช้งานต่างๆ เหล่านั้นได้เป็นอย่างดีแล้ว แต่ในบางครั้งจะพบว่า เครื่องมือหรือซอฟต์แวร์เหล่านั้นก็ไม่สามารถสกัดข้อมูลการใช้งานในบางประเภทได้ ทำให้ขาดข้อมูลการใช้งานที่สำคัญบางอย่างไป เช่น การติดต่อสื่อสารด้วยข้อความ เสียง หรือการติดต่อผ่าน Application ต่างๆ รวมถึงการใช้งานอินเตอร์เน็ตและการจดบันทึกในรูปแบบต่างๆ ซึ่งปัญหาดังกล่าวอาจส่งผลกระทบต่อกระบวนการตรวจพิสูจน์ได้

ดังนั้น จึงจำเป็นจะต้องใช้เทคนิคการตรวจพิสูจน์โดยการดึงข้อมูลการใช้งานจากไฟล์ Database หรือไฟล์ Backup ที่บันทึกไว้ในหน่วยความจำของตัวเครื่อง โดยข้อมูลการใช้งานต่างๆ เหล่านี้จะถูกจัดเก็บในตำแหน่งที่แตกต่างกันไป

จากความสำคัญดังกล่าวข้างต้น จึงทำให้ผู้ปฏิบัติหน้าที่ในฐานะผู้ตรวจพิสูจน์พยานหลักฐานดิจิทัลจำเป็นที่จะต้องทราบถึงตำแหน่งที่จะสามารถเรียกดูข้อมูลการใช้งานต่างๆ เหล่านั้นได้ เพื่อให้ได้ข้อมูลการใช้งานที่มีความสมบูรณ์มากที่สุด อันจะทำให้การตรวจพิสูจน์มีประสิทธิภาพมากยิ่งขึ้น

จากสถิติดังกล่าวข้างต้น จะพบว่าอุปกรณ์สื่อสารเคลื่อนที่ที่ส่งตรวจพิสูจน์เพื่อหาข้อมูลที่เกี่ยวข้องกับการกระทำความผิดนั้น เป็นอุปกรณ์สื่อสารเคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ถึงร้อยละ 63 ซึ่งมากกว่าอุปกรณ์สื่อสารเคลื่อนที่ที่ใช้ระบบปฏิบัติการ iOS ที่พบในอัตราร้อยละ 30

ถึงสองเท่า ดังนั้น ถ้าผู้ที่เกี่ยวข้องกับคดีหรือผู้ที่ปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานต่างๆ เหล่านี้ได้มีความรู้ความเข้าใจในการปฏิบัติต่อพยานหลักฐาน การเข้าถึงข้อมูลอย่างถูกต้อง รวมถึงหลักในการตรวจวิเคราะห์เป็นอย่างดี ก็จะทำให้ได้ข้อมูลการใช้งานจากพยานหลักฐานอย่างสมบูรณ์ครบถ้วน ส่งผลให้กระบวนการตรวจพิสูจน์ทำได้อย่างมีประสิทธิภาพ อันจะเป็นประโยชน์ต่อกระบวนการยุติธรรมต่อไป

1. ระบบปฏิบัติการแอนดรอยด์ (Android Operating System)

1.1 แอนดรอยด์ (Android) เป็นระบบปฏิบัติการสำหรับอุปกรณ์เคลื่อนที่ซึ่งประกอบไปด้วยระบบปฏิบัติการมิดเดิ้ลแวร์ (Middleware Operating System) และโปรแกรมประยุกต์หลัก (Key Application) โดย Android มีพื้นฐานอยู่บนระบบปฏิบัติการลินุกซ์ (Linux) ที่ได้รับความนิยมทั่วโลกในฐานะ Open Source ที่ถูกนำมาจำหน่ายหรือแจกฟรีในลักษณะเป็นแพ็คเกจ โดยผู้จัดทำซอฟต์แวร์จะรวมซอฟต์แวร์สาหรับใช้งานในด้านอื่นๆ เป็นชุดเข้าด้วยกัน ส่วนในการพัฒนาซอฟต์แวร์บน Androidนั้น จะใช้ภาษาจาวา (JAVA) ในการพัฒนาระบบงานต่างๆ โดยภาษา JAVA เป็นภาษาโปรแกรมเชิงวัตถุ (Object Oriented Programming Language หรือ OOP) ซึ่งข้อดีของภาษา JAVA คือการไม่ขึ้นกับแพลตฟอร์มใดๆ ทำให้ภาษา JAVA มีอิสระในการใช้งานสูง นอกจากลักษณะต่างๆ ที่กล่าวมานั้น Android ยังมีลักษณะเป็นซอฟต์แวร์ Open Source เหมือนกับ Linux ซึ่งเป็นผลดีที่ทำให้ Android ได้รับความนิยมอย่างสูงและยังมีการรวมตัวกันของกลุ่มบริษัทพัฒนาอุปกรณ์เคลื่อนที่เพื่อสนับสนุน Android อีกด้วย ทำให้ Android หรือ Google Android เป็นระบบปฏิบัติการที่ได้รับความนิยมสูง จึงได้มีการพัฒนารูปแบบของอุปกรณ์ออกมารองรับหลากหลายประเภท เช่น Smartphone, Tablet, Netbook, E-Reader, Google TV, Vehicles (In-board), Global Positioning System, Home Appliances, Media Players, Printers และ Dedicated Gaming Devices โดยเฉพาะอย่างยิ่งอุปกรณ์สื่อสารเคลื่อนที่นั้นได้มีบริษัทชั้นนำทั่วโลกทำการคิดค้นผลิตภัณฑ์ออกมารองรับเป็นจำนวนมาก เช่น Samsung, Huawei, OPPO, HTC, LG, Motorola และ Sony Ericsson เป็นต้น และเนื่องจาก Android เป็น Open Source จึงทำให้มีการพัฒนาและสร้าง Android ในฉบับของตนเองขึ้นเองได้ โดยโทรศัพท์มือถือเครื่องแรกที่ใช้ระบบปฏิบัติการแอนดรอยด์ คือ เอชทีซี ดรีม เปิดตัวเมื่อวันที่ 22 ตุลาคม พ.ศ. 2551 สร้างบนลินุกซ์ เคอร์เนล 2.6 โดยปัจจุบันระบบปฏิบัติการแอนดรอยด์ได้พัฒนาไปจนถึงเวอร์ชั่น 8.0 ดังตารางที่ 1

ตารางที่ 1 แสดงข้อมูลระบบปฏิบัติการแอนดรอยด์เวอร์ชั่นต่างๆ ตั้งแต่อดีตถึงปัจจุบัน

รุ่น	ชื่อเล่น	ระดับเอพีไอ	ลินุกซ์ เคอร์เนล	เปิดตัว
1.0	- (Alpha)	1		23 กันยายน 2551
1.1	- (Beta)	2		9 กุมภาพันธ์ 2552
1.5	Cupcake (คัปเค้ก)	3	2.6.27	30 เมษายน 2552
1.6	Donut (โดนัท)	4	2.6.29	15 สิงหาคม 2552
2.0	Eclair (เอแกลร์)	5	2.6.29	26 ตุลาคม 2552
2.0.1	Eclair (เอแกลร์)	6	2.6.29	3 ธันวาคม 2552
2.1	Eclair (เอแกลร์)	7	2.6.29	12 มกราคม 2553
2.2	Froyo (โฟรซเซนโยเกิร์ต)	8	2.6.32	20 พฤษภาคม 2553
2.3	Gingerbread (ขนมปังขิง)	9	2.6.35	6 ธันวาคม 2553
2.3.3	Gingerbread (ขนมปังขิง)	10	2.6.35	9 กุมภาพันธ์ 2554
3.0	Honeycomb (รวงผึ้ง)	11	2.6.36	22 กุมภาพันธ์ 2554
3.1	Honeycomb (รวงผึ้ง)	12	2.6.36	10 พฤษภาคม 2554
3.2	Honeycomb (รวงผึ้ง)	13	2.6.36	15 กรกฎาคม 2554
4.0	Ice Cream Sandwich (แซนด์วิชไอศกรีม)	14	3.0.1	19 ตุลาคม 2554
4.0.3	Ice Cream Sandwich (แซนด์วิชไอศกรีม)	15		16 ธันวาคม 2554
4.1	Jelly Bean (เจลลีบีน)	16	3.0.31	28 มิถุนายน 2555
4.2	Jelly Bean (เจลลีบีน)	17	3.4.0	29 ตุลาคม 2555
4.3	Jelly Bean (เจลลีบีน)	18	3.4.0	24 กรกฎาคม 2556
4.4	KitKat (คิตแคต)	19	3.10	31 ตุลาคม 2556
4.4W	KitKat (คิตแคตสำหรับอุปกรณ์สวมใส่)	20		25 มิถุนายน 2557

ตารางที่ 1 แสดงข้อมูลระบบปฏิบัติการแอนดรอยด์เวอร์ชั่นต่างๆ ตั้งแต่อดีตถึงปัจจุบัน (ต่อ)

รุ่น	ชื่อเล่น	ระดับเอพีไอ	ลินุกซ์ เคอร์เนล	เปิดตัว
5.0	Lollipop (อมยิ้ม)	21		15 ตุลาคม 2557
5.1	Lollipop (อมยิ้ม)	22		9 มีนาคม 2558
6.0	Marshmallow (มาร์ชเมลโลว์)	23		28 พฤษภาคม 2558
7.0	Nougat (นูกัต)	24		22 สิงหาคม 2559
7.1	Nougat (นูกัต)	25		4 ตุลาคม 2559
8.0	Oreo (โอรีโอ)	26		21 สิงหาคม 2560

1.2 ส่วนประกอบหลักของอุปกรณ์แอนดรอยด์ (Core Components)

อุปกรณ์แอนดรอยด์ (Android Device) จะประกอบไปด้วยส่วนที่เป็น Hardware และ Software ซึ่งจะมีอยู่มากมายหลายส่วนที่ทำหน้าที่แตกต่างกันไป โดยในบทความนี้จะกล่าวถึงเฉพาะส่วนที่ทำหน้าที่ในการประมวลผลและจัดเก็บข้อมูลการใช้งานเท่านั้น เนื่องจากเป็นแหล่งเก็บข้อมูลการใช้งานที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์

1.3 หน่วยประมวลผลกลาง (Central Processing Unit, CPU)

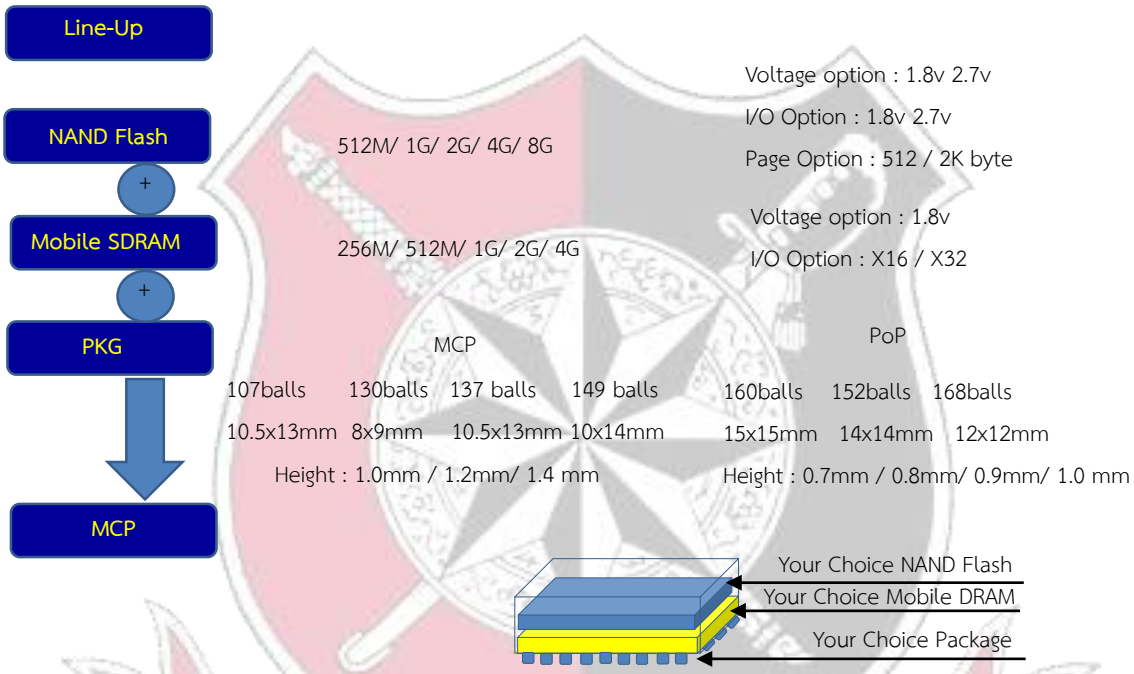
ในระบบคอมพิวเตอร์จำเป็นต้องมีหน่วยประมวลผล เพื่อให้ระบบปฏิบัติการ (Operating System) มีการตอบสนองต่อชุดคำสั่ง ในการที่จะควบคุมการทำงานของอุปกรณ์ต่างๆ เช่น ระบบเครือข่าย (Network), การจัดเก็บข้อมูล (Storage), การแสดงผล (Display) และการรับคำสั่ง (Input) เป็นต้น อุปกรณ์แอนดรอยด์ก็เช่นกัน จำเป็นต้องมีระบบประมวลผลกลาง โดยใช้ ARM (Acorn RISC Machine) เป็นหน่วยประมวลผลกลาง ซึ่งมีความเหมาะสมกับของอุปกรณ์สื่อสารเคลื่อนที่ เนื่องจากใช้พลังงานไฟฟ้าน้อยจึงไม่เปลืองพลังงานจากแบตเตอรี่มากนัก ทำให้ใช้งานได้นานหลายชั่วโมง

1.4 หน่วยความจำ (RAM and NAND Flash)

ในอุปกรณ์แอนดรอยด์มีหน่วยความจำภายใน (Internal Memory หรือ Internal Storage) 2 แบบ คือ Volatile (Random Access Memory, RAM) และ Nonvolatine (NAND Flash) โดย RAM

จะถูกใช้งานโดยระบบ (System) ในการเรียกใช้ (Load), การปฏิบัติ (Execute) และการจัดการ (Manipulate) ในส่วนที่สำคัญของระบบปฏิบัติการ (Operating System), Application และ Data ในขณะที่ NAND Flash ใช้ในการเก็บ Boot Loader, Operating System และ User Data

สำหรับอุปกรณ์สื่อสารเคลื่อนที่นั้น เนื่องด้วยข้อจำกัดทางด้านพื้นที่และขนาดของอุปกรณ์ ดังนั้น RAM และ NAND flash จึงถูกสร้างออกมาในรูปแบบของ Multichip Package (MCP) ดังภาพที่ 2



ภาพที่ 2 โครงสร้างของ MCP (Mobile Memory) (Andrew Hoog, 2011)

1.5 หน่วยความจำชนิดถอดได้ (Removable Memory)

ส่วนประกอบอีกประเภทที่ใช้ในการเก็บข้อมูลการใช้งานของอุปกรณ์แอนดรอยด์ คือ หน่วยความจำชนิดถอดได้ (Removable Memory) หรือ External Storage โดยอุปกรณ์แอนดรอยด์มักนิยมใช้ Secure Digital Card (SD Card) เป็นหน่วยความจำเสริม เพื่อเพิ่มขนาดความจุ ซึ่งหน่วยความจำดังกล่าวถือเป็นหน่วยความจำชนิด Nonvolatile และใช้เทคโนโลยี NAND Flash เช่นเดียวกัน

2. การตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Evidence Analysis)

หลักของการทำ Digital Forensic Analysis คือต้องไม่ให้เกิดการเปลี่ยนแปลงใดๆ ต่อพยานหลักฐานโดยผู้ตรวจพิสูจน์ แต่เนื่องด้วยอุปกรณ์สื่อสารเคลื่อนที่เองนั้นไม่มีระบบที่จะสามารถ Shutdown, เชื่อมต่อเข้ากับอุปกรณ์ป้องกันการเขียนข้อมูล (Write Blocker) และสำเนาข้อมูล (Imaged) ได้เหมือนอุปกรณ์คอมพิวเตอร์ ดังนั้น ทุกๆ การเชื่อมต่อเข้ากับอุปกรณ์สื่อสารเคลื่อนที่ จะทำให้เกิดการเปลี่ยนแปลงขึ้นไม่ทางใดก็ทางหนึ่ง ดังนั้นผู้ตรวจพิสูจน์ต้องมีวิจารณญาณและความรู้ในการปฏิบัติต่ออุปกรณ์เหล่านี้อย่างเพียงพอที่จะไม่ทำให้เกิดการเปลี่ยนแปลงต่อข้อมูลที่เป็นสาระสำคัญของคดี และทุกครั้งที่ทำการตรวจพิสูจน์ที่ทำให้เกิดการเปลี่ยนแปลงใดๆ กับพยานหลักฐานดังกล่าวเสียแล้วก็จำเป็นต้องอธิบายเหตุผลให้ได้ว่าเหตุใดจึงเลือกใช้วิธีการตรวจพิสูจน์ดังกล่าวนั้น

2.1 ขั้นตอนการปฏิบัติต่ออุปกรณ์สื่อสารเคลื่อนที่ในสถานที่เกิดเหตุ

หัวใจสำคัญของกระบวนการตรวจพิสูจน์อุปกรณ์สื่อสารเคลื่อนที่นั้น คือ การพยายามไม่ให้เกิดการเปลี่ยนแปลงต่ออุปกรณ์ หรือยอมให้มีการเปลี่ยนแปลงได้น้อยที่สุด แต่ต้องมีเหตุผลประกอบด้วย ดังนั้น การที่ผู้ปฏิบัติได้ปฏิบัติตามกระบวนการที่ถูกต้องเสียตั้งแต่ในสถานที่เกิดเหตุ หรือเมื่อได้ทำการตรวจยึดมาได้จากผู้ครอบครอง ดังแสดงในภาพที่ 3 จะทำให้พยานหลักฐานดังกล่าวมีความถูกต้องน่าเชื่อถือ อันจะทำให้ผลการตรวจพิสูจน์มีความน่าเชื่อถือ และทำให้กระบวนการยุติธรรมสิ้นสงสัยในผลการตรวจพิสูจน์ได้ มีขั้นตอน ดังนี้

(1) Secure the Device การปกป้องพยานหลักฐานไม่ให้เกิดการเปลี่ยนแปลงใดๆ ทั้งจากตัวผู้ต้องหาเอง และจากผู้ที่ไม่มีส่วนเกี่ยวข้องกับพยานหลักฐาน ซึ่งอาจมีการทำลายหลักฐานหรือทำให้เกิดการเปลี่ยนแปลงข้อมูลได้

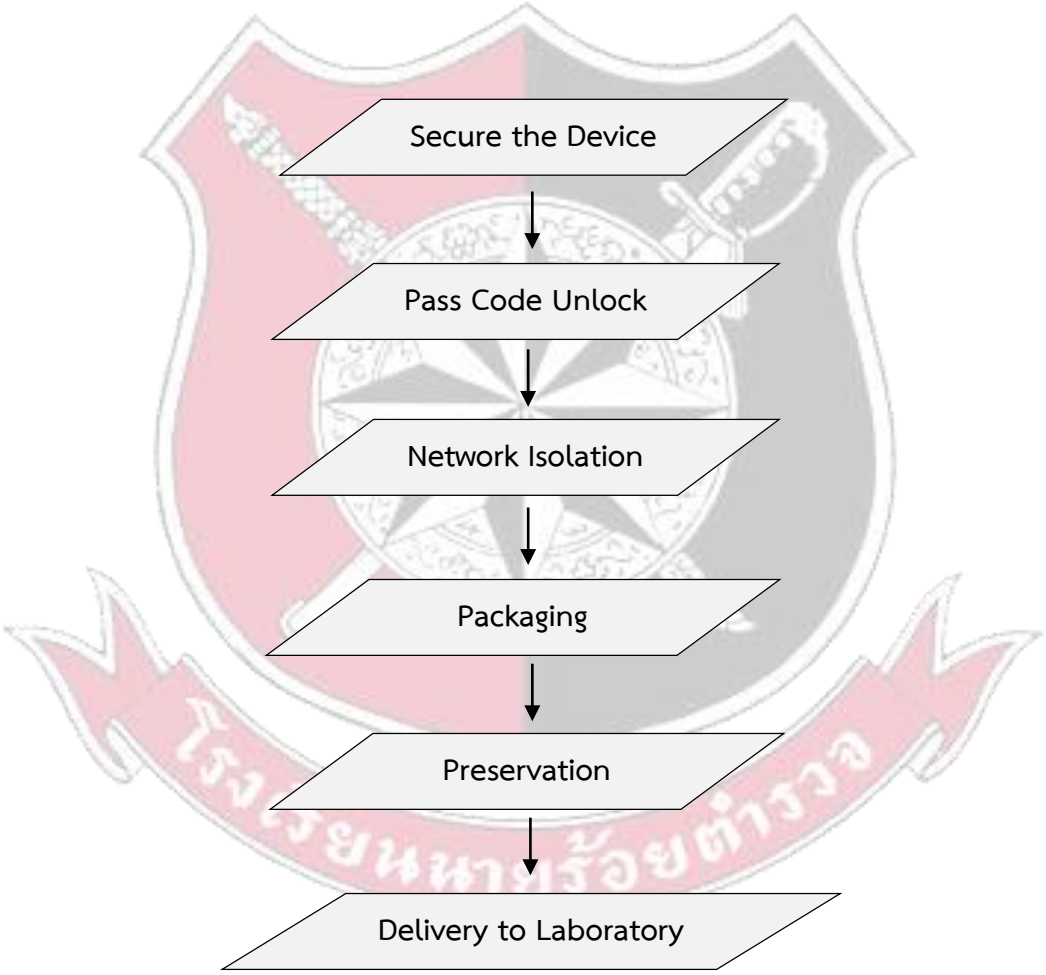
(2) Pass Code Unlock เมื่อทำการยึดอุปกรณ์สื่อสารเคลื่อนที่ได้แล้ว ควรคำนึงถึงรหัสผ่านเข้าใช้งานเครื่องเป็นอันดับแรก โดยให้รีบสอบถามข้อมูลจากเจ้าของเครื่องแล้วทำการปลดล็อครหัสจากนั้นให้ทำการทดสอบการเข้าใช้งานเครื่องอีกครั้ง เพื่อให้มั่นใจว่าผู้ตรวจพิสูจน์ในห้องปฏิบัติการจะสามารถเข้าถึงข้อมูลการใช้งานได้

(3) Network Isolation ตัดการเชื่อมต่อกับสัญญาณเครือข่ายเพื่อป้องกันการเข้าถึงข้อมูลจากระยะไกล และการเปลี่ยนแปลงข้อมูลการเชื่อมต่อกับเครือข่ายด้วย โดยการใช้ Airplane Mode หรือถอดซิมการ์ดออก

(4) Packaging ทำการบรรจุหีบห่อด้วยวัสดุภัณฑ์ที่เหมาะสม รวมถึงการเลือกใช้อุปกรณ์ป้องกันการเชื่อมต่อสัญญาณเครือข่าย เช่น Faraday Bag เป็นต้น แต่มีข้อควรคำนึงคือเมื่อนำอุปกรณ์ใส่ใน Faraday Bag แล้วนั้น จะทำให้แบตเตอร์รี่หมดเร็วเนื่องจากเครื่องต้องใช้พลังงานไฟฟ้ามากกว่าปกติเพื่อค้นหาสัญญาณเครือข่าย ดังนั้นควรนำสาย Power หรือ สาย Data มาด้วยทุกครั้ง

(5) Preservation ดูแลป้องกันพยานหลักฐานไม่ให้เกิดการเปลี่ยนแปลง หรือสูญหาย ก่อนนำส่งยังห้องปฏิบัติการ

(6) Delivery to Laboratory นำส่งห้องปฏิบัติการโดยเร็วที่สุด



ภาพที่ 3 ขั้นตอนการปฏิบัติต่ออุปกรณ์สื่อสารเคลื่อนที่ในสถานที่เกิดเหตุ

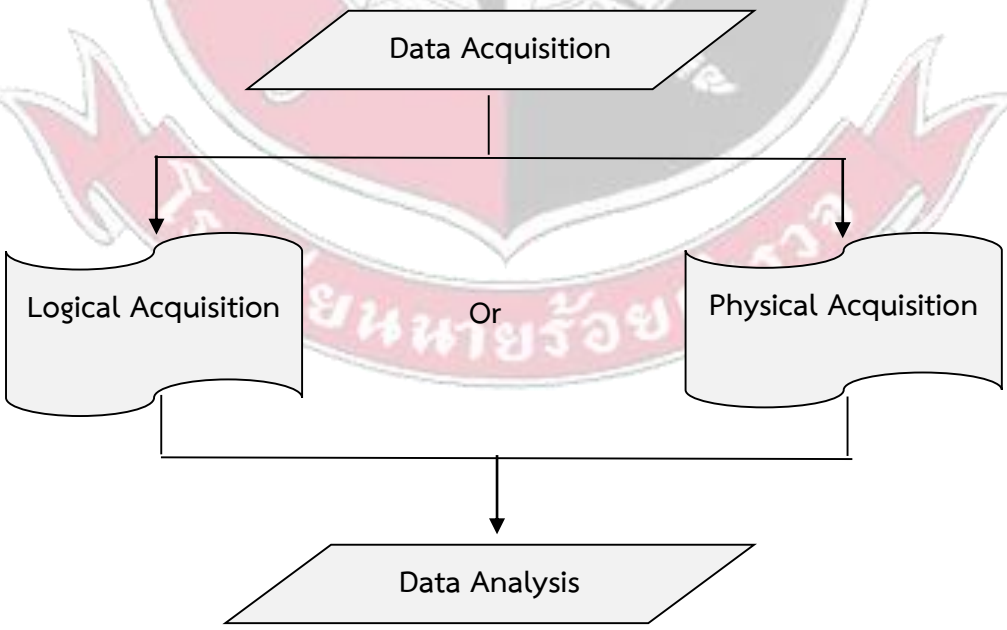
2.2 ขั้นตอนการตรวจพิสูจน์ในห้องปฏิบัติการ

2.2.1 Data Acquisition

ดังที่ได้กล่าวในเบื้องต้นแล้วว่ากระบวนการตรวจพิสูจน์อุปกรณ์สื่อสารเคลื่อนที่นั้น ต้องพยายามหลีกเลี่ยงการกระทำที่จะก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานให้ได้มากที่สุด ดังนั้น จึงต้องทำการสกัดข้อมูลการใช้งานจากอุปกรณ์ดังกล่าวเพื่อนำไปตรวจพิสูจน์ การตรวจดูข้อมูลการใช้งานโดยตรงที่พยานหลักฐานเป็นสิ่งที่ไม่ควรทำเป็นอย่างยิ่ง เพราะจะทำให้เกิดการปนเปื้อนต่อพยานหลักฐาน การสกัดข้อมูลการใช้งานอุปกรณ์แอนดรอยด์สามารถทำได้หลายวิธี ดังภาพที่ 4

2.2.2 Logical Technique

เป็นการสกัดข้อมูลการใช้งานอุปกรณ์ที่ยังคงมีอยู่ในเครื่อง (Allocated) ซึ่งเป็นการสกัดข้อมูลการใช้งานที่นิยมทำเป็นอันดับแรกในการตรวจพิสูจน์ เนื่องจากเป็นกระบวนการที่ทำให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานน้อยที่สุด กล่าวคือ ไม่มีการเขียนโปรแกรมเข้าไปภายในพยานหลักฐาน (Root Access) ต้องการเพียงแค่การเปิดใช้งานโหมด USB Debugging เท่านั้น ปัจจุบันมีซอฟต์แวร์ที่รองรับการสกัดข้อมูลการใช้งานจากอุปกรณ์แอนดรอยด์อยู่หลากหลายให้เลือกใช้ ทั้งแบบ Open Source และแบบ Commercial ขึ้นอยู่กับปัจจัยทางด้านงบประมาณของแต่ละหน่วยงาน ในที่นี้จะขอกล่าวถึงเทคนิคที่ใช้เครื่องมือที่เป็น Open Source เท่านั้น



ภาพที่ 4 ขั้นตอนการตรวจพิสูจน์ในห้องปฏิบัติการ

2.2.3 Backup Analysis

ปัจจุบันระบบปฏิบัติการแอนดรอยด์เองก็ได้สร้าง Application ขึ้นมารองรับการ Backup ข้อมูลการใช้งานให้แก่ผู้บริโภคโดยสามารถเข้าไปค้นหา Application ดังกล่าวได้จาก Android Market ซึ่งจะพบเครื่องมือที่ทำการ Backup ข้อมูลได้อย่างมีประสิทธิภาพ โดยสามารถเลือกได้ว่าจะเก็บข้อมูลไว้ที่ใด เช่น SD Card หรือ Cloud เป็นต้น หนึ่งใน Application ที่นิยมใช้กันคือ “RerWare’s My Backup Pro” ซึ่งผู้ใช้งานสามารถเลือกได้ว่าจะเก็บข้อมูลไว้ที่ SD Card หรือ RerWare’s server โดย Application ดังกล่าวจะรองรับการสกัดข้อมูลการใช้งาน ดังนี้

- Application เช่น Application install files, Integrated third-party application
- Communication เช่น Contacts, Call log, SMS (Text Message), MMS (รวมถึงข้อมูลที่ถูก Attached)
- Internet เช่น Browser bookmarks
- ข้อมูลอื่นๆ เช่น Home screens, Alarms, Dictionary, Calendars, Music Playlists, System settings

2.2.4 AFLogical

เครื่องมือนี้อนุญาตให้ใช้งานได้ฟรีเฉพาะผู้บังคับใช้กฎหมายหรือหน่วยงานทางราชการเท่านั้น โดยสามารถลงทะเบียน และ Download ได้จาก http://viaforensics.com/products/tools/aflogical/ Application นี้ถูกพัฒนาขึ้นโดยบริษัท viaForensics ซึ่งสามารถสกัดข้อมูลการใช้งาน (Logical Extraction) จากอุปกรณ์สื่อสารเคลื่อนที่ได้เช่นเดียวกับเครื่องมือที่จำหน่ายทางการค้า (Commercial Tools) โดยต้องเปิดใช้งานโหมด USB Debugging ที่อุปกรณ์แอนดรอยด์ก่อน แล้วจึงเชื่อมต่อเข้ากับเครื่องมือสำหรับสกัดข้อมูล (Ubuntu Workstation) โดยเครื่องมือดังกล่าวจะรองรับการสกัดข้อมูลการใช้งานที่มีขนาดข้อมูลมาก อย่างเช่น SMS database ที่มีข้อมูล SMS มากถึง 35,000 ข้อความได้ ผู้ใช้งานสามารถเลือกเก็บข้อมูลที่สกัดได้ไว้ที่ SD Card ในรูปแบบของ CSV และไฟล์ info.xml ซึ่งจะได้ข้อมูลเกี่ยวกับอุปกรณ์แอนดรอยด์และ Application ที่ถูกติดตั้งลงเครื่อง ปัจจุบันเครื่องมือนี้รองรับการสกัดข้อมูลได้ถึง 41 ประเภท ดังนี้

- Application เช่น Social Contacts Activities
- Communication เช่น Call Log, SMS, MMS, Contacts (Contact Method/ Extensions/ Groups/ Organizations/ Phones/Settings), IM (Accounts/ Chats/ Contacts Provider/ Invitation/ Messages/ Providers/ Provider Setting)

- Internet เช่น Browser (Bookmarks/Search), Search History

- Storage เช่น Phone Storage, External (Media/Image Media/Image Thumb Media/Videos), Internal (Image Media/Image Thumb Media/Videos)

- ข้อมูลอื่นๆ เช่น Notes, Calendars (Attendees/Events/Extended Properties/ Reminders), Maps (Friends/Friends extra/ Friends contacts), People (Deleted)

เนื่องจากข้อมูลการใช้งานที่สกัดได้จะถูกเขียนลงบนหน่วยความจำ SD Card ดังนั้นข้อควรระวังในการใช้เครื่องมือนี้คือต้องนำ SD Card ที่อยู่ในเครื่องพยานหลักฐานออกก่อน แล้วจึงใส่ SD Card ของผู้ตรวจพิสูจน์เข้าไปแทนที่ มิเช่นนั้น SD Card ของเครื่องพยานหลักฐานจะถูกเขียนข้อมูลทับลงไป ซึ่งถือว่าเป็นการทำให้พยานหลักฐานปนเปื้อน หรือในบางครั้งก็ไม่สามารถทำการสกัดข้อมูลการใช้งานได้เลย

นอกเหนือจากซอฟต์แวร์ที่ใช้ในการดึงข้อมูลการใช้งาน (Data Acquisition) จากอุปกรณ์สื่อสารเคลื่อนที่กล่าวมาข้างต้นนั้น เราสามารถใช้เครื่องมือที่เป็น Android Open Source อื่นๆได้ ดังนี้

- ซอฟต์แวร์ andriller สามารถ Download ได้ที่ https://www.andriller.com/license/

- ซอฟต์แวร์ sourceforge สามารถ Download ได้ที่ https://sourceforge.net/projects/osaftoolkit/

- ซอฟต์แวร์ ANDROPHSY สามารถ Download ได้ที่ https://github.com/scorelab/ANDROPHSY

2.2.5 Physical Technique

เป็นการสกัดข้อมูลการใช้งานของอุปกรณ์สื่อสารเคลื่อนที่ทั้งหมด ทั้งที่ยังคงมีอยู่ในเครื่อง (Allocated) และข้อมูลที่ถูกลบออกจากเครื่องไปแล้ว (Deleted data) รวมถึงข้อมูลที่ถูกเข้ารหัสด้วย ซึ่งสามารถทำได้ 2 รูปแบบ ดังนี้

(1) การสกัด โดยใช้ Hardware ปัจจุบันมี 2 เทคนิค คือ การทำ JTAG และ Chip-off ซึ่งวิธีนี้คือการนำเอา NAND Flash ออกมาจากอุปกรณ์สื่อสารเคลื่อนที่เพื่อสกัดข้อมูลการใช้งาน ถือเป็นการตรวจพิสูจน์แบบทำลายตัวอย่าง เหมาะสำหรับพยานหลักฐานที่ถูกทำลายเสียหาย ไม่สามารถเชื่อมต่อด้วยวิธีการตามปกติได้

(2) การสกัด โดยใช้ Software เป็นการสกัดข้อมูลที่ไม่ยุ่งยากเหมือนเทคนิค Hardware และไม่ทำให้อุปกรณ์พยานหลักฐานเสียหาย สามารถเข้าถึงข้อมูลของพยานหลักฐานในระดับ File System โดยในการสกัดข้อมูลนั้นต้องทำการ Root เครื่องเสียก่อน จากนั้นจึงทำการสกัดข้อมูลการใช้งานด้วย AFPhysical Technique ผ่านทาง Ubuntu Workstation ที่ถูกพัฒนาโดย viaForensics ซึ่งรองรับการสกัดข้อมูลการใช้งานจากอุปกรณ์แอนดรอยด์ทุกประเภท

2.2.6 Data Analysis

เมื่อทำการสกัดข้อมูลการใช้งานจากพยานหลักฐานแล้ว ขั้นตอนต่อไปคือการวิเคราะห์ข้อมูลเหล่านั้น ซึ่งปัจจุบันมีอยู่หลากหลายวิธีการ ขึ้นอยู่กับวัตถุประสงค์และข้อมูลที่ต้องการตรวจพิสูจน์ หนึ่งในเทคนิคที่มีประสิทธิภาพ คือการตรวจข้อมูลจากไฟล์ Database ที่สกัดได้

3. การตรวจพิสูจน์ข้อมูลการใช้งานจากไฟล์ Database หรือ ไฟล์ Backup

เทคนิคการตรวจพิสูจน์โดยการดึงข้อมูลการใช้งานจากไฟล์ Database หรือไฟล์ Backup ที่บันทึกไว้ในหน่วยความจำของตัวเครื่อง จะพบว่าข้อมูลการใช้งานต่างๆ เหล่านี้จะถูกจัดเก็บในตำแหน่งที่แตกต่างกันไป ตัวอย่างเช่น ข้อมูลการใช้งาน Application ในระบบปฏิบัติการแอนดรอยด์นั้น จะพบว่าข้อมูลจะถูกจัดเก็บไว้ 2 ที่ ทั้ง Internal Storage และ External Storage โดยใน External Storage (Memory Card) ข้อมูลจะถูกจัดเก็บลงตำแหน่งใดๆ ก็ได้ที่ต้องการ ในขณะที่การจัดเก็บข้อมูลลงใน Internal Storage จะถูกควบคุมด้วย Android APIs เมื่อ Application ถูกติดตั้ง ข้อมูลจะถูกเก็บไว้ใน Subdirectory ของ /data/data/name of package เช่น Package name ของ “com.android.browser” ของ Application “Android Browser” ข้อมูลจะถูกจัดเก็บใน /data/data/com.android.browser เป็นต้น

ดังนั้นจึงมีความจำเป็นที่เราต้องทราบถึงตำแหน่งที่จะสามารถเรียกดูข้อมูลการใช้งานเหล่านั้นได้ ดังแสดงในตารางที่ 2

ตารางที่ 2 ข้อมูลการใช้งานและตำแหน่งที่เก็บในโทรศัพท์เคลื่อนที่ ยี่ห้อ LG รุ่น LGE LGMS345

ลำดับ	ข้อมูลการใช้งาน	ตำแหน่งที่เก็บ (Path)
1	Device Name	data\com.android.providers.settings\databases\setting.db.
2	Time Zone	data\com.android.providers.calendar\databases\calendar.db
3	Wireless Connection and password	Data\misc\wifi\wpa_supplican.conf

ตารางที่ 2 ข้อมูลการใช้งานและตำแหน่งที่เก็บในโทรศัพท์เคลื่อนที่ ยี่ห้อ LG รุ่น LGE LGMS345 (ต่อ)

ลำดับ	ข้อมูลการใช้งาน	ตำแหน่งที่เก็บ (Path)
4	Bluetooth device name	Data\root\misc\bluedroid\bt_config.old
5	Information on Calendar Event	\data\com.android.providers.calendar\databases\calendar.db
6	Information for alarms	\data\com.lge.clock\databases\alarms.db
7	Information of third-party application	\data\com.android.vending\databases\localappstate.db
8	Information about what was searched in the Google Play	\data\com.android.vending\databases\suggestion.db
9	Information about Google map activity	\data\com.google.android.apps.maps\databases\gmm_storage.db
10	Information about Google search engine	\data\com.android.chrome\app_chrome\default\history
11	Information about Google Chrome download	\data\com.android.chrome\app_chrome\default\history
12	Instargram Images	\media\0\Pictures\Instagram.

ตารางที่ 2 ข้อมูลการใช้งานและตำแหน่งที่เก็บในโทรศัพท์เคลื่อนที่ ยี่ห้อ LG รุ่น LGE LGMS345 (ต่อ)

ลำดับ	ข้อมูลการใช้งาน	ตำแหน่งที่เก็บ (Path)
13	Information about attachments sent via Hangouts	\data\com.google.android.talk\databases\babel1.db
14	Information about messages in Skype	\data\com.skype.raider\files\AccountName\main.db
15	Information on the phone contact list	\data\com.google.android.googlequicksearchbox\databases\icingcorpora.db
16	Information about messages via application (Skype)	\data\com.skype.raider\files\AccountName\main.db
17	Information about messages via application (Google Hangouts)	\data\com.google.android.talk\databases\babel1.db
18	Information about calls	\data\com.android.providers.contacts\databases\contacts2.db
19	Information about e-mail attachments for g-mail	\data\com.google.android.gm\databases\e-mail address

ตารางที่ 2 ข้อมูลการใช้งานและตำแหน่งที่เก็บในโทรศัพท์เคลื่อนที่ ยี่ห้อ LG รุ่น LGE LGMS345 (ต่อ)

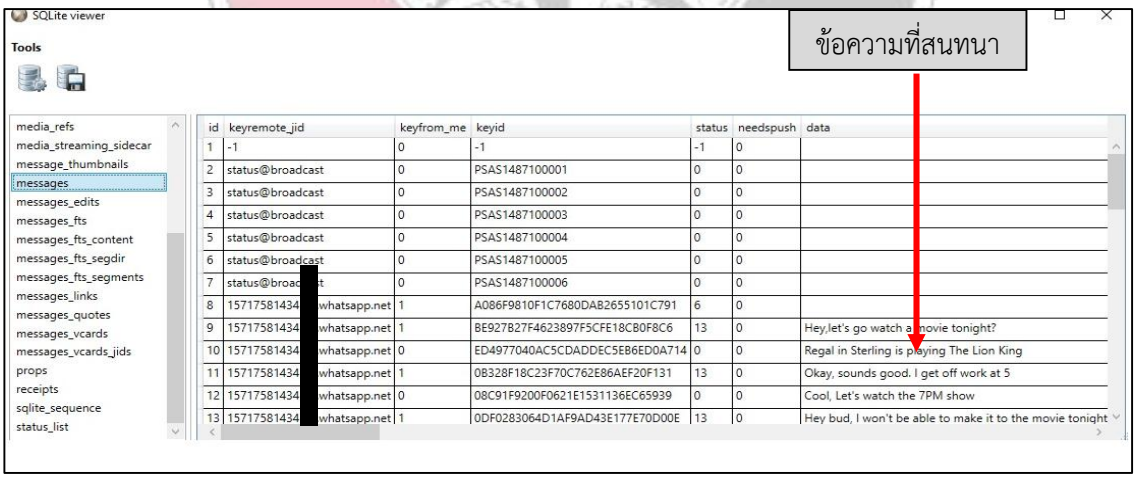
ลำดับ	ข้อมูลการใช้งาน	ตำแหน่งที่เก็บ (Path)
20	Information about the active G-Mail account	\data\com.google.android.gm\shared_prefs\Gmail.xml.
21	Information about the yahoo e-mail account	\data\com.android.browser\app_ace\databases\ databases.db
22	Information on yahoo e-mail	data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db
23	The account that downloaded the applications onto device	\data\com.android.vending\databases\localappstate.db ตัวอย่างข้อมูลที่ได้ปรากฏในตารางที่ 3
24	Information about messages via application (WhatsApp)	\userdata\media\0\WhatsApp\Databases\msgstore.db.crypt12.db รายละเอียดปรากฏดังภาพที่ 1
25	Information about messages via application (Line)	\data\data\jp.naver.line.android\databases\naver.line.db รายละเอียดปรากฏดังภาพที่ 2

ในบางคดีจำเป็นต้องหาข้อมูลผู้ใช้งาน (User Account) ที่ทำการ Download Application ต่างๆ เพื่อติดตั้งลงในอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งข้อมูลนี้สามารถเรียกดูได้โดยการค้นหาจากชื่อของ Application ที่ต้องการ ซึ่งจะปรากฏ e-mail address ที่ทำการ Download Application นั้นๆ รายละเอียดดังตารางที่ 3

ตารางที่ 3 ข้อมูล Account name ที่ใช้ในการ Download Application ลงในเครื่องอุปกรณ์เคลื่อนที่

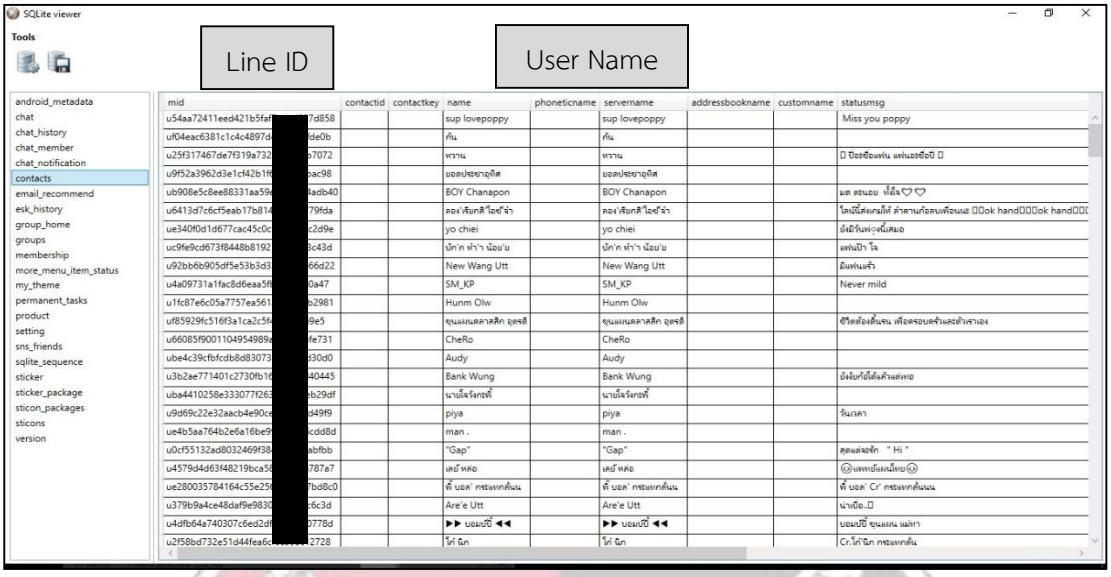
package_name	title	account
com.skype.raider	Skype-free IM & video calls	e-mail address
com.facebook.orca	Messenger	e-mail address
com.instagram.android	Instagram	e-mail address
Com.android.chrome	Chrome Browser-Google	e-mail address

ปัจจุบันข้อมูลการใช้งาน Application สำหรับการติดต่อสื่อสารและสนทนาต่างๆ นับเป็นข้อมูลที่สำคัญอย่างมากต่อการตรวจพิสูจน์ สามารถใช้เป็นหลักฐานในการระบุการกระทำความผิดของผู้เกี่ยวข้องในคดีได้ แต่ในบางครั้งการสกัดข้อมูลการใช้งานด้วยซอฟต์แวร์ทางการค้า ก็ไม่สามารถสกัดข้อมูลการใช้งาน Application นั้นๆ ได้อย่างครบถ้วน จึงจำเป็นต้องเรียกดูข้อมูลจากไฟล์ Database เช่น จากการสกัดข้อมูลการใช้งานด้วยซอฟต์แวร์ XRY พบมีการติดตั้ง Application WhatsApp แต่ไม่พบประวัติการใช้งาน แต่สามารถเรียกดูข้อมูลการใช้งานได้จากไฟล์ Database ดังแสดงในภาพที่ 5 และรายละเอียดข้อมูลการใช้งาน Application Line และ Facebook Messenger จากไฟล์ Database ดังภาพที่ 6 - ภาพที่ 9 ตามลำดับ (สถาบันนิติวิทยาศาสตร์, 2560)

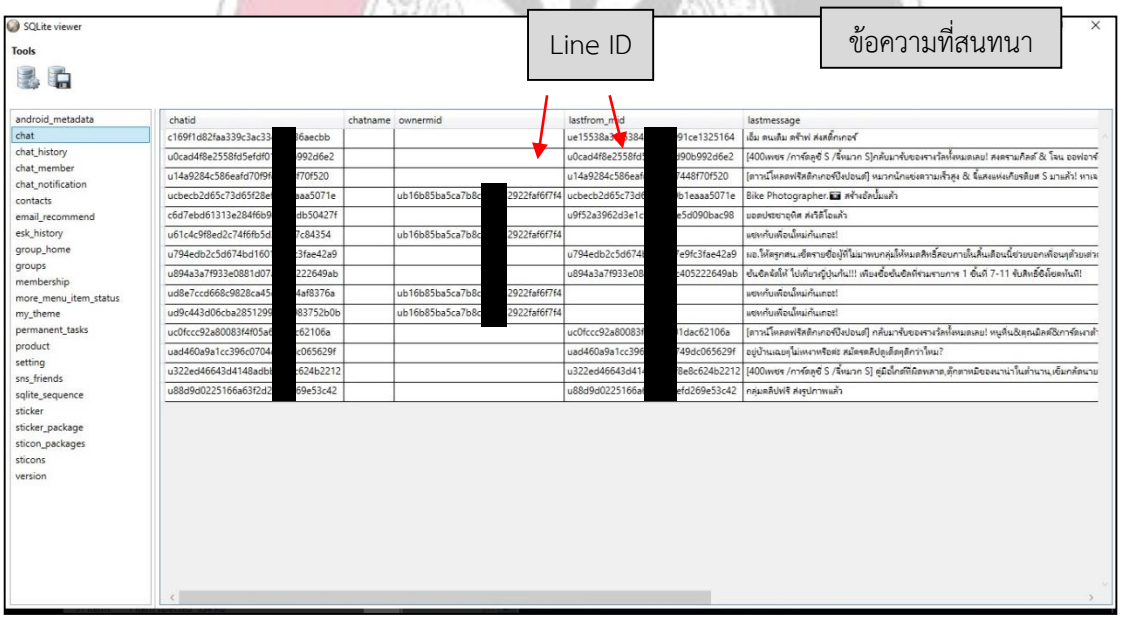


ภาพที่ 5 ข้อมูลการใช้งาน Application WhatsApp ที่พบในไฟล์ Database

จากภาพที่ 5 จะพบข้อมูลการใช้งานที่เป็นประโยชน์ต่อคดี ดังนี้ รายละเอียดข้อความที่สนทนาผ่านทาง Application (ศรชี้) รวมถึงวันเวลาที่ทำการสนทนาและหมายเลข ID ของคู่สนทนาด้วย

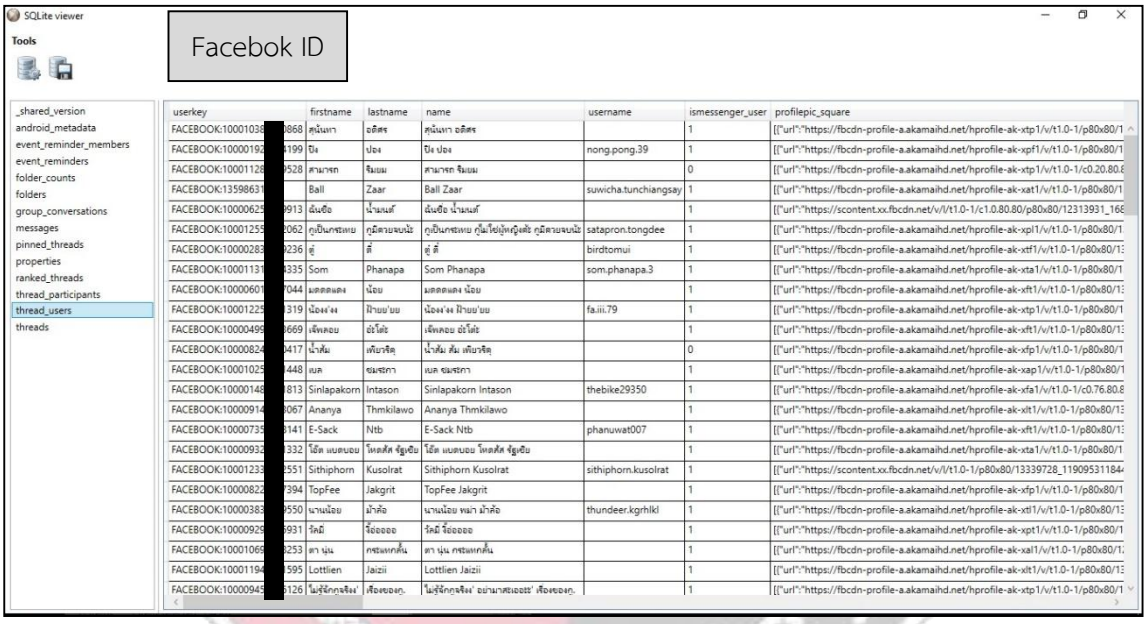


ภาพที่ 6 ข้อมูลบัญชีผู้ติดต่อจากการใช้งาน Application Line ที่พบในไฟล์ Database

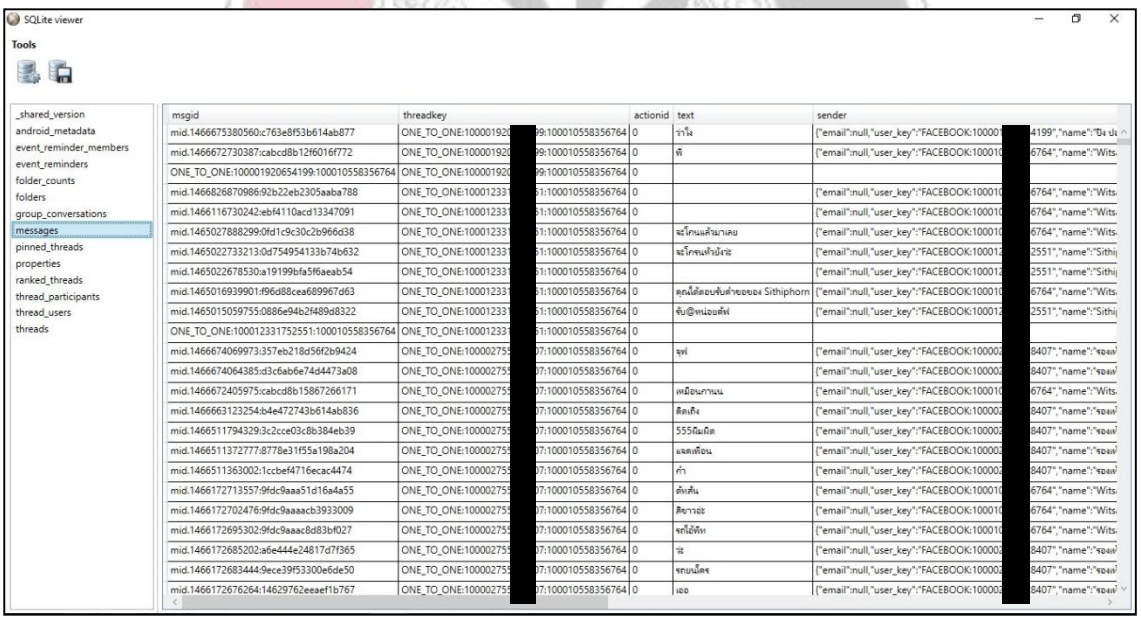


ภาพที่ 7 ข้อมูลการสนทนาผ่าน Application Line ที่พบในไฟล์ Database

จากภาพที่ 6 และ 7 ซึ่งเป็นข้อมูลการใช้งาน Application สำหรับการสื่อสารจากไฟล์ Database ของเครื่องผู้กระทำความผิดในคดีค้ายาเสพติด จะพบข้อมูลการใช้งานที่เป็นประโยชน์ต่อคดี ดังนี้ บัญชีรายชื่อผู้ติดต่อที่ใช้งาน Application Line ร่วมกัน และรายละเอียดข้อความที่สนทนาผ่านทาง Application รวมถึงวันเวลาที่ทำการสนทนาและหมายเลข Line ID ของคู่สนทนาด้วย



ภาพที่ 8 ข้อมูลบัญชีผู้ติดต่อจากการใช้งาน Application Facebook Messenger ที่พบในไฟล์ Database



ภาพที่ 9 ข้อมูลการสนทนาผ่าน Application Facebook Messenger ที่พบในไฟล์ Database

จากภาพที่ 8 และ 9 ซึ่งเป็นข้อมูลการใช้งาน Application สำหรับการสื่อสารจากไฟล์ Database ของเครื่องผู้กระทำความผิดในคดีค้ามนุษย์ จะพบข้อมูลการใช้งานที่เป็นประโยชน์ต่อคดี ดังนี้ บัญชีรายชื่อผู้ติดต่อที่ใช้งาน Facebook Messenger ร่วมกัน และรายละเอียดข้อความที่สนทนาผ่านทาง Application รวมถึงวันเวลาที่ทำการสนทนาและหมายเลข Facebook ID ของคู่สนทนาด้วย

บทสรุป

ในกรณีที่ห้องปฏิบัติการต้องทำการตรวจพิสูจน์ข้อมูลการใช้งานของอุปกรณ์สื่อสารเคลื่อนที่ที่ทำการตรวจยึดมาได้จากสถานที่เกิดเหตุ เพื่อหาข้อมูลความเชื่อมโยงของคดีประเภทต่างๆ นั้น การใช้เทคนิคการตรวจพิสูจน์โดยการดึงข้อมูลการใช้งานจากไฟล์ Database หรือไฟล์ Backup ที่บันทึกไว้ในหน่วยความจำของตัวเครื่องเป็นทางเลือกหนึ่งที่จะทำให้การตรวจพิสูจน์ข้อมูลการใช้งานจากอุปกรณ์เหล่านั้นทำได้ครบถ้วนมากยิ่งขึ้น เนื่องจากการสกัดข้อมูลการใช้งานด้วยซอฟต์แวร์ทางการค้าในบางครั้งไม่สามารถสกัดข้อมูลการใช้งานได้อย่างครบถ้วน ดังจะเห็นได้จากตัวอย่าง ดังนั้นจึงควรทราบถึงตำแหน่งที่จะสามารถเรียกดูข้อมูลการใช้งานเหล่านั้นได้ เพื่อทำให้การตรวจพิสูจน์สามารถกระทำได้รวดเร็วขึ้นและได้ข้อมูลที่สามารถนำไปใช้ในชั้นศาลได้มากขึ้น อันจะทำให้การตรวจพิสูจน์มีประสิทธิภาพมากยิ่งขึ้น

ข้อเสนอแนะ

เนื่องด้วยปัจจุบันเทคโนโลยีด้านการสื่อสารได้มีการพัฒนาขึ้นอย่างรวดเร็ว ทั้งทางด้านผู้ให้บริการเครือข่าย และ Applications ต่างๆ โดยเฉพาะอย่างยิ่งอุปกรณ์ที่ใช้งาน ซึ่งมีการพัฒนาทั้ง Hardware และ Software เพื่อตอบโจทย์ให้แก่ผู้บริโภค ทั้งด้านการใช้งานติดต่อสื่อสารและการจดบันทึก ดังนั้น ผู้มีหน้าที่ในการตรวจพิสูจน์พยานหลักฐานดังกล่าวนี้จำเป็นจะต้องทำการศึกษา Applications ใหม่ๆ ที่ถูกสร้างขึ้นมาใช้งาน รวมถึงเครื่องมือทางด้าน Digital Forensic โดยเฉพาะตระกูล Open Source ทั้งหลายเพื่อพัฒนาเทคนิคและกระบวนการตรวจพิสูจน์ให้ทันต่อเทคโนโลยีของอุปกรณ์สื่อสารเคลื่อนที่อยู่หลากหลายในปัจจุบัน เพื่อให้ทราบตำแหน่งที่เก็บข้อมูลและสามารถนำมาใช้ประโยชน์ในกระบวนการยุติธรรมได้

เอกสารอ้างอิง

กิตติชัย ปิ่นเลิศ. (2556). **Application Android Development**. สืบค้นเมื่อ 23 กุมภาพันธ์ 2561. เข้าถึงได้จาก https://pinlert.wordpress.com/ประวัติ-android.

Casey E. (2011). **Digital Evidence and Computer Crime**. (Third Edition). Waltham: Academic Press Publication.

CTSPortal. (2016). **Mobile Digital Evidence Summary Report**. สืบค้นเมื่อ 23 กุมภาพันธ์ 256. เข้าถึงได้จาก https://www.ctsforensics.com/reports/main.

Hoog A. (2011). **Android Forensics**. Wyman USA: Syngress publication.

Newman R.C. (2007). **Computer Forensics: Evidence Collection and management**. New York: Auerbach Publication**.**

.

ผู้เขียน

คำนำหน้า ชื่อ-สกุล	**ดร.อมรรัตน์ เล็กวิชัย**
หน่วยงาน/สังกัด	กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ กองตรวจพิสูจน์ทางวิทยาศาสตร์ สถาบันนิติวิทยาศาสตร์
ที่อยู่ของหน่วยงาน	สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม อาคารศูนย์ราชการเฉลิมพระเกียรติฯ ชั้น 8 ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพมหานคร 10210
E-mail:	amornrat.l@cifs.mail.go.th