# การเปรียบเทียบเครื่องมือตรวจพิสูจน์ระหว่างโปรแกรมรหัสเปิดกับโปรแกรมเชิงพาณิชย์สำหรับการตรวจพิสูจน์หลักฐานดิจิทัล

# A Comparative Evaluation of Open Source and Commercial Tools for Digital Forensics

**วันทนีย์ ตุลยเสวี [1] และ วรธัช วิชชุวาณิชย์ [2]**
[1,2]คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

**Wantanee Tunyasevee [1] and Woratouch Witchuwanich [2]**
[1,2]Faculty of Forensic Science, Royal Police Cadet Academy

รับบทความ (Received): 27 มิถุนายน 2562, แก้ไขบทความ (Revised): 25 กรกฎาคม 2562, ยอมรับการตีพิมพ์ (Accepted): 7 สิงหาคม 2562

**บทคัดย่อ**

ในการตรวจพิสูจน์หลักฐานดิจิทัลนั้น มีอยู่หลากหลายเทคนิควิธี ขึ้นอยู่กับความต้องการของรูปคดี ซึ่งในการตรวจพิสูจน์จำเป็นต้องใช้เครื่องมือหรือซอฟต์แวร์สำหรับตรวจพิสูจน์โดยเฉพาะ ไม่ว่าจะเป็นแบบเชิงพาณิชย์หรือแบบรหัสเปิด โดยเน้นความถูกต้องและความน่าเชื่อถือเป็นสิ่งที่สำคัญที่สุด ในการวิจัยนี้แสดงการเปรียบเทียบโปรแกรมรหัสเปิดกับโปรแกรมเชิงพาณิชย์เพื่อประเมินสมรรถนะการทำงานของโปรแกรมทั้งสองแบบ ซึ่งโปรแกรมรหัสเปิด ได้แก่ Autopsy เวอร์ชั่น 4.10 ส่วนโปรแกรมเชิงพาณิชย์ ได้แก่ EnCase เวอร์ชั่น 8.08 และ AXIOM เวอร์ชั่น 3.0 โดยกำหนดคุณลักษณะการทำงานขึ้น เช่น การทำสำเนาข้อมูล การคำนวณค่าแฮช MD5 SHA-1 การระบุข้อมูลที่ถูกลบ การกู้คืนข้อมูลที่ถูกลบ การออกรายงาน เป็นต้น โปรแกรมทั้ง 3 โปรแกรมนี้ จะถูกใช้วิเคราะห์กับพยานหลักฐานประเภท Solid State Drive (SSD) และ Hard Disk Drive (HDD) ซึ่งได้ทำการสร้างข้อมูลเพื่อใช้ในการวิเคราะห์บนไดรฟ์ทั้ง 2 ชนิดนี้ หลังจากการวิเคราะห์เปรียบเทียบ สามารถสรุปได้ว่าโปรแกรมเชิงพาณิชย์สามารถวิเคราะห์คุณลักษณะการทำงานได้มากกว่าโปรแกรมรหัสเปิด และจะเห็นว่าการกู้คืนข้อมูลที่ถูกลบไปจาก Solid State Drive (SSD) นั้น ไม่สามารถกู้คืนกลับมาได้ เนื่องจากมีผลมาจากคำสั่ง TRIM ของ Solid State Drive (SSD) นั่นเอง ซึ่งในทางตรงกันข้ามสามารถกู้คืนข้อมูลที่ถูกลบไปจาก Hard Disk Drive (HDD) ได้

**คำสำคัญ:** การตรวจพิสูจน์หลักฐานดิจิทัล, โปรแกรมรหัสเปิด, โปรแกรมเชิงพาณิชย์

**Abstract**

Techniques used in the examination of digital evidence vary greatly, depending on the purpose of certain cases that may require a specific tool or a forensic software. Whether it is an open source or a commercial one, the techniques must emphasize on the infallibility and reliability. In this research, a comparison of an open source tool (Autopsy version 4.10) and commercial tools (EnCase version 8.08 and AXIOM version 3.0) was conducted to evaluate the capability of forensic tools. Features were set, including image acquisition, hash value calculation (MD5, SHA-1), the identification of the deleted files, the recovery of the delete files, report making, The three program tools were used in analyzing and creating data for the analysis of Solid State Drive (SSD) and Hard Disk Drive (HDD). The comparative analysis concluded that commercial tools could analyze more features than those of the open source tools. In addition, the recovery of the data from SSD was failed due to the TRIM command whereas the deleted data from HDD were successfully recovered.

**Keywords:** Digital Forensics, Open Source Tools, Commercial Tools

**บทนำ**

ปัจจุบันจะพบว่าเครื่องคอมพิวเตอร์ อุปกรณ์บันทึกข้อมูลหรือโทรศัพท์เคลื่อนที่ เป็นอุปกรณ์ที่ทุกคนจำเป็นต้องใช้ในชีวิตประจำวันกันทั้งสิ้น ซึ่งอุปกรณ์เหล่านี้มีความก้าวหน้าทางเทคโนโลยีอย่างมาก ทำให้อุปกรณ์เหล่านี้มีอิทธิพลต่อการดำเนินชีวิตเป็นอย่างมากและทุกคนให้ความสำคัญ จึงเป็นสาเหตุที่อุปกรณ์เหล่านี้ถูกนำมาใช้เป็นเครื่องมือก่อเหตุอาชญากรรมขึ้นได้ เช่น คดีอาชญากรรมด้านการฉ้อโกง การฟอกเงิน การครอบครองสื่อลามกอนาจารเด็ก การค้ามนุษย์ การค้าประเวณี คดียาเสพติด คดีละเมิดลิขสิทธิ์ เป็นต้น ซึ่งจะพบว่าไม่ว่าจะเกิดคดีในด้านใดก็ตาม มักจะมีการใช้เครื่องคอมพิวเตอร์ อุปกรณ์บันทึกข้อมูลหรือโทรศัพท์เคลื่อนที่ในการกระทำความผิดอยู่เสมอ และอุปกรณ์เหล่านี้จะกลายเป็นพยานหลักฐานดิจิทัล ซึ่งพยานหลักฐานดิจิทัลนี้ จะถูกนำมาตรวจพิสูจน์ทางดิจิทัลเพื่อหาข้อมูลยืนยันการกระทำความผิดโดยผู้เชี่ยวชาญที่ได้รับการฝึกฝนสำหรับกระบวนการตรวจพิสูจน์และการใช้เครื่องมือตรวจพิสูจน์มาเป็นอย่างดี ซึ่งเครื่องมือการตรวจพิสูจน์ทางดิจิทัลนั้นมีหลากหลายประเภท จึงอาจทำให้เกิดข้อสงสัยได้ว่าเครื่องมือหรือซอฟต์แวร์หรือโปรแกรมใดที่สามารถตรวจพิสูจน์หลักฐานได้อย่างมีประสิทธิภาพ จากข้อสงสัยดังกล่าว ผู้วิจัยจึงได้มีความสนใจที่จะศึกษาเกี่ยวกับการเปรียบเทียบเครื่องมือตรวจพิสูจน์ระหว่างแบบเชิงพาณิชย์กับแบบรหัสเปิด ซึ่งได้นำมาวิเคราะห์พยานหลักฐาน

ประเภทไดรฟ์ชนิด Solid State Drive (SSD) และ ชนิด Hard Disk Drive (HDD) เนื่องจากไดร์ฟทั้งสองชนิดเป็นไดร์ฟที่บันทึกข้อมูลโดยเฉพาะสำหรับเครื่องคอมพิวเตอร์

**วัตถุประสงค์**

1. เพื่อเปรียบเทียบโปรแกรมตรวจพิสูจน์พยานหลักฐานดิจิทัลระหว่างโปรแกรมเชิงพาณิชย์กับโปรแกรมรหัสเปิด
2. เพื่อประเมินสมรรถนะการทำงานของโปรแกรมเชิงพาณิชย์กับโปรแกรมรหัสเปิดโดยวิเคราะห์บนพยานหลักฐานชนิด Solid State Drive และ Hard Disk Drive

**ทบทวนวรรณกรรม**

**1. การตรวจพิสูจน์พยานหลักฐานดิจิทัล**

หลักการพื้นฐานของการตรวจพิสูจน์พยานหลักฐานดิจิทัลครอบคลุมองค์ประกอบทั้ง 4 ด้าน ได้แก่

1.1 การรวบรวมพยานหลักฐาน (Acquisition) หมายถึง กระบวนการรวบรวมข้อมูลอิเล็กทรอนิกส์ หรือการรวบรวมพยานหลักฐานทางคอมพิวเตอร์จากสถานที่เกิดเหตุ แต่อีกความหมาย คือ การทำสำเนาข้อมูลดิจิทัลหรือข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นการทำสำเนาที่ได้ข้อมูลตรงตามต้นฉบับทุกประการ โดยที่ข้อมูลต้นฉบับจะไม่มีการเปลี่ยนแปลงหรือปนเปื้อนข้อมูลอื่นทั้งสิ้น การทำสำเนาข้อมูลในลักษณะนี้ เรียกว่า การทำ Image

1.2 การเก็บรักษาพยานหลักฐาน (Preservation) จะต้องมีการเก็บรักษาไว้ในสภาพที่เหมาะสมและปลอดภัย การเก็บรักษาเป็นกระบวนการสร้างห่วงโซ่วัตถุพยาน (Chain of Custody) เจ้าหน้าที่ต้องบันทึกข้อมูลลงเอกสารห่วงโซ่วัตถุพยาน หมายถึง ข้อมูลที่ระบุรายละเอียดของพยานหลักฐานและการส่งพยานหลักฐาน โดยเจ้าหน้าที่ที่รับผิดชอบต้องมีบันทึกไว้ เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บมาจากสถานที่เกิดเหตุจนถึงเวลาที่สิ้นสุดคดี (Phanwattana, 2018, p.79)

1.3 การวิเคราะห์ข้อมูล (Data Analysis) ซึ่งปัจจุบันมีอยู่หลายวิธีการ ขึ้นอยู่กับวัตถุประสงค์และข้อมูลที่ต้องการตรวจพิสูจน์ ตัวอย่างเช่น คดีลามกอนาจารเด็กหรือคดีค้ามนุษย์ เป้าหมายของการตรวจพิสูจน์ก็คือค้นหารูปภาพเปลือยกายหรือภาพยนตร์ที่ปรากฏภาพบุคคลเปลือยกาย ซึ่งบุคคลในภาพนั้นคาดว่าจะเป็นเด็กอายุไม่เกิน 18 ปี หรือคดีพนันออนไลน์ เป้าหมายการตรวจพิสูจน์ก็คือการตรวจสอบการเข้าถึงเว็บไซต์การพนันหรือเอกสารการพนันต่าง ๆ จะเห็นได้ว่าแต่ละคดีมีเป้าหมายในการตรวจพิสูจน์ที่แตกต่างกัน รวมถึงขั้นตอนการวิเคราะห์ แต่ละคดีก็จะมีการวิเคราะห์ วิธีการที่แตกต่างกัน

1.4 การออกรายงาน (Reporting) หรือการนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน (Presentation) ถือว่าเป็นขั้นตอนสุดท้ายในกระบวนการวิเคราะห์พยานหลักฐาน โดยการนำเสนอในรูปแบบรายงานการตรวจพิสูจน์ที่เป็นลายลักษณ์อักษร ซึ่งในการออกรายงานการตรวจพิสูจน์นั้น

จะขึ้นอยู่กับหน่วยงาน อาจมีแนวทางเป็นของตนเอง อย่างไรก็ตามการออกรายงานการตรวจพิสูจน์จะต้องระบุอย่างชัดเจนและถูกต้อง

**2. เครื่องมือตรวจพิสูจน์พยานหลักฐานดิจิทัล** ประเภทของเครื่องมือตรวจพิสูจน์พยานหลักฐานสามารถแบ่งได้ 3 ประเภท ดังนี้

2.1 เครื่องมือเชิงพาณิชย์ (Commercial Tools) คือ เครื่องมือหรือซอฟต์แวร์ที่ผลิตขึ้นมาเพื่อจำหน่ายหรือข้อบังคับหรือข้อตกลงไว้เพื่อจุดประสงค์เชิงพาณิชย์ ส่วนใหญ่มักจะเป็นซอฟต์แวร์ลิขสิทธิ์

2.2 เครื่องมือรหัสเปิด (Open Source Tools) คือ เครื่องมือหรือซอฟต์แวร์ที่เปิดเผยให้บุคคลภายนอกหรือบุคคลทั่วไปสามารถได้ใช้ โดยไม่มีค่าใช้จ่ายใด ๆ

2.3 เครื่องมือสำหรับผู้บังคับใช้กฎหมายเท่านั้น (Law Enforcement Only – LEO) คือ เครื่องมือตรวจพิสูจน์ที่ถูกพัฒนาขึ้นสำหรับใช้โดยผู้บังคับใช้กฎหมายเท่านั้น

**3. Solid State Drives (SSD)** เป็นไดรฟ์อีกชนิดหนึ่งในการเก็บบันทึกข้อมูล ที่บันทึกข้อมูลด้วยหน่วยความจำแฟลช ซึ่ง Solid State Drives ถูกนำมาใช้กันอย่างแพร่หลาย ไม่ว่าจะเป็นคอมพิวเตอร์ตั้งโต๊ะหรือคอมพิวเตอร์โน้ตบุ๊ก ซึ่งภายใต้การทำงานของ Solid State Drives นั้น มีคำสั่งควบคุมอยู่มากมาย และคำสั่งที่ถูกพัฒนามาให้ใช้กับ Solid State Drives นั้น ได้แก่

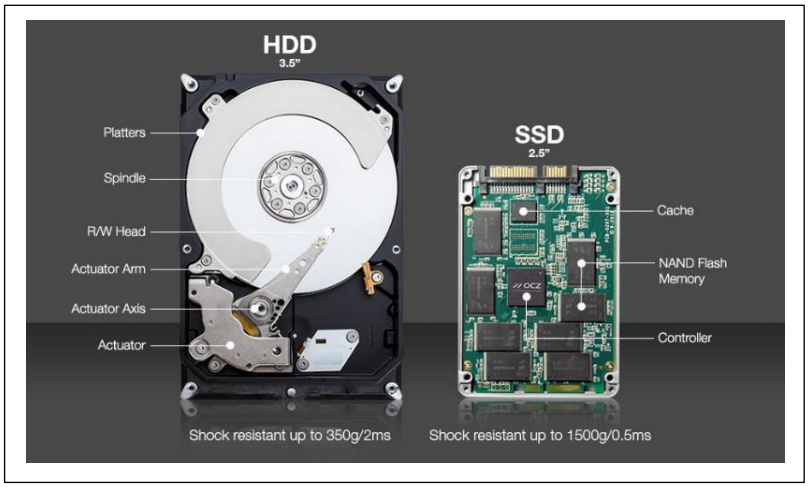
3.1 คำสั่ง TRIM เป็นคำสั่งที่ควบคุมการทำงานของหน่วยความจำแฟลช เมื่อผู้ใช้ได้ทำการลบข้อมูลออกไป คำสั่ง TRIM จะเริ่มทำงานทันที โดยลบข้อมูลที่ผู้ใช้สั่งลบไปและกำหนดค่าของข้อมูลเป็นศูนย์ในตำแหน่งเดิมที่ข้อมูลเคยบันทึกอยู่ ซึ่งคำสั่ง TRIM นี้ จะสามารถทำงานได้ใน Solid State Drives ที่มีการติดตั้งระบบปฏิบัติการตั้งแต่ Windows 7 ขึ้นไป และมีระบบการจัดการข้อมูลเป็น NTFS คำสั่ง TRIM จะไม่สามารถทำงานในระบบ RAID หรือนำไปใช้ในรูปแบบอุปกรณ์ต่อพ่วงเป็นอุปกรณ์ USB

3.2 Self-Corrosion คือ กระบวนการกัดกร่อนด้วยตนเองหรือการทำลายตัวเอง ซึ่งเป็นกระบวนการที่ควบคุมอยู่ภายในหน่วยความจำแฟลช เมื่อมีการลบข้อมูลออกจากตำแหน่งที่เคยบันทึกอยู่ กระบวนการนี้จะทำเครื่องหมายว่าตำแหน่งนี้ถูกลบไปแล้ว ทำให้สามารถเขียนข้อมูลใหม่ลงไปได้ทันที

3.3 Garbage Collection คือ กระบวนการรวบรวมข้อมูลที่ถูกลบไปแล้วหรือข้อมูลขยะที่ผู้ใช้ได้ทำการลบไป ซึ่งกระบวนการนี้อยู่ภายใต้คำสั่ง TRIM และคำสั่ง TRIM ช่วยทำให้กระบวนการนี้มีประสิทธิภาพมากขึ้น

**4. ความแตกต่างระหว่างไดรฟ์ชนิด Solid State Drive กับไดรฟ์ Hard Disk Drive**

Hard Disk Drive จะทำงานบนแผ่นจานแม่เหล็กที่เพื่อเก็บข้อมูลในรูปแบบแม่เหล็ก ดังนั้นข้อมูลทั้งหมดจะถูกเก็บไว้บนพื้นผิวด้านบนและด้านล่างของแผ่นดิสก์ซึ่งเป็นแทร็คจะแบ่งออกเป็นแต่ละส่วน ดังนั้นเมื่อเริ่มใช้งานเครื่องคอมพิวเตอร์จะไปอ่านข้อมูลบนดิสก์ โดยที่ต้องไปอ่านข้อมูลเพื่อเรียกใช้ระบบปฏิบัติอย่างเร็วที่สุด ส่วนกรณีของ Solid State Drive ทำงานบนหน่วยความจำแฟลช ส่วนประกอบที่สำคัญ คือตัวควบคุมและหน่วยความจำเพื่อจัดเก็บข้อมูล




ภาพที่ 1 ส่วนประกอบภายในของ Magnetic Disk กับ Flash Memory
ที่มา: Joshi & Hubbard (2016)

**5. EnCase Forensic** เป็นซอฟต์แวร์เชิงพาณิชย์สำหรับตรวจพิสูจน์หลักฐานดิจิทัล จากเดิมถูกพัฒนาขึ้นโดย Guidance Software แต่ในปี พ.ศ.2561 ได้เปลี่ยนมาเป็น บริษัท Open text ซอฟต์แวร์นี้ช่วยในการตรวจพิสูจน์ข้อมูลดิจิทัลได้อย่างมีประสิทธิภาพและได้รับความนิยมสูงมากในการตรวจพิสูจน์หลักฐานดิจิทัล

**6. Magnet AXIOM** เป็นซอฟต์แวร์เชิงพาณิชย์สำหรับตรวจพิสูจน์หลักฐานดิจิทัล พัฒนาโดย Magnet Forensics ช่วยในการตรวจพิสูจน์ข้อมูลดิจิทัล เพื่อสืบค้นและวิเคราะห์ข้อมูล ที่บันทึกอยู่ในสื่อบันทึกข้อมูลดิจิทัลต่าง ๆ อีกทั้งยังสามารถสืบค้นและวิเคราะห์ข้อมูลระบบโซเลียลเน็ตเวิร์คข้อมูลร่องรอยการใช้งานระบบโซเลียลเน็ตเวิร์คได้อีกด้วย

**7. Autopsy (Sleuth Kit)** เป็นซอฟต์แวร์รหัสเปิดสามารถวิเคราะห์พยานหลักฐานประเภทคอมพิวเตอร์ เพื่อตรวจสอบสิ่งที่เกิดขึ้นบนคอมพิวเตอร์และสามารถกู้คืนข้อมูลที่ถูกลบได้อีกด้วย

**งานวิจัยที่เกี่ยวข้อง**

Maurya และคณะ (2015) ได้ทำการวิจัยเพื่อตรวจสอบคุณสมบัติและหน้าที่ของเครื่องมือตรวจพิสูจน์เพื่อแสดงให้เห็นว่าซอฟต์แวร์แบบ Open Source อาจเป็นไปตามหลักเกณฑ์และอาจให้ผลลัพธ์ที่ใกล้เคียงกับซอฟต์แวร์แบบ Commercial บทความนี้ใช้การศึกษาเปรียบเทียบระหว่างซอฟต์แวร์แบบ Open Source ได้แก่ AUTOPSY 3.1.2 และ SIFT 3.0 ส่วนซอฟต์แวร์แบบ Commercial ได้แก่ FTK 3.0, ENCASE 4.20 และ OSFORENSICS 3.1 หลังจากการวิเคราะห์เปรียบเทียบซึ่งจะให้ภาพรวมของแต่ละเครื่องมือขึ้นอยู่กับคุณลักษณะการทำงานต่าง ๆ สามารถสรุปได้ว่ามีหลายคุณลักษณะที่มีอยู่ในเครื่องมือแบบ Open Source แต่เครื่องมือแบบ Commercial ไม่มี เช่น การคำนวณค่า SHA-1 ที่ ENCASE 4.20 ไม่สามารถทำได้ เป็นต้น และมีคุณลักษณะที่เครื่องมือแบบ Commercial ทำได้แต่เครื่องมือแบบ Open Source ทำไม่ได้ เช่น การระบุพื้นที่ Slack และการกู้คืนข้อมูลที่ถูกลบของ

Autopsy 3.1.2 ไม่สามารถทำได้ เป็นต้น การวิจัยครั้งนี้มีประโยชน์มากในการพิสูจน์คุณลักษณะการทำงานของเครื่องมือแบบ Open Source กับเครื่องมือแบบ Commercial ด้วยการเปรียบเทียบคุณลักษณะต่าง ๆ

Joshi, B.R., & Hubbard, R., (2016) ได้อธิบายไว้ว่า การตรวจพิสูจน์หลักฐานดิจิทัลเป็นสาขาวิชาขั้นสูงในฐานะที่เป็นวิชาชีพที่มีกฎหมายที่บังคับใช้กฎหมายและเทคโนโลยีคอมพิวเตอร์ซึ่งแพร่หลายมากขึ้น การวิจัยครั้งนี้ได้กล่าวถึงการทำงานของ Solid State Drive ซึ่งมีการทำงานบนหน่วยความจำแฟลช โดยปัจจุบัน Solid State Drive พร้อมใช้งานในคอมพิวเตอร์เดสก์ท็อป คอมพิวเตอร์โน้ตบุ๊ก จำนวนมากขึ้นเรื่อย ๆ บทความนี้ได้อธิบายถึงคำสั่ง TRIM ซึ่งเป็นคำสั่งที่ถูกพัฒนามาใช้ใน Solid State Drive และสร้างความท้าทายในการตรวจพิสูจน์หลักฐานอีกด้วย งานวิจัยนี้ได้ทำการทดลองเพื่อกู้คืนข้อมูลที่ถูกลบไปจาก Solid State Drive โดย Solid State Drive ที่ใช้ในการทดลองมีการติดตั้งระบบปฏิบัติการที่แตกต่างกัน และทำการเปิด ปิด การใช้งานคำสั่ง TRIM ทั้งนี้ได้ใช้ Write Blocker เพื่อเชื่อมต่อ Solid State Drive กับเครื่องคอมพิวเตอร์ตรวจพิสูจน์ด้วย จากการทดลองเห็นว่าไม่สามารถกู้คืนข้อมูลที่ถูกลบจาก Solid State Drive ที่ติดตั้งระบบปฏิบัติการรุ่นใหม่และมีการตั้งค่าเริ่มต้นให้เปิดใช้คำสั่ง TRIM ซึ่งคำสั่ง TRIM จะสั่งให้ระบบทำการลบข้อมูลที่ผู้ใช้ทำการลบไปและทำเครื่องหมายว่าข้อมูลนั้นถูกลบที่ตำแหน่งนั้น ๆ เพื่อให้ไม่สามารถกู้คืนข้อมูลกลับมาได้

**ระเบียบวิธีวิจัย**

การวิจัยครั้งนี้เป็นการวิจัยเชิงทดลอง เพื่อเปรียบเทียบและประเมินสมรรถนะการทำงานของโปรแกรมตรวจพิสูจน์พยานหลักฐานดิจิทัลระหว่างโปรแกรมเชิงพาณิชย์ ได้แก่ ซอฟต์แวร์ EnCase เวอร์ชั่น 8.08 และ ซอฟต์แวร์ AXIOM เวอร์ชั่น 3.0 กับโปรแกรมรหัสเปิด ได้แก่ ซอฟต์แวร์ Autopsy (Sleuth Kit) เวอร์ชั่น 4.10 โดยวิเคราะห์บนพยานหลักฐานชนิด Solid State Drive และ Hard Disk Drive

**1. การสร้างพยานหลักฐาน**

กระบวนการนี้เป็นการสร้างพยานหลักฐานเพื่อนำไปทดลองกับซอฟต์แวร์ทั้ง 3 ซอฟต์แวร์ โดยการสร้างพยานหลักฐานลงบนพยานหลักฐานทั้ง 2 ชิ้น ได้แก่

1.1 ไดรฟ์ ลูกที่ 1 ชนิด Solid State Drive ประเภท M.2 PCIe NVMe ยี่ห้อ SAMSUNG รุ่น MZ-VLW1280 ขนาด 128 GB

1.2 ไดรฟ์ ลูกที่ 2 ชนิด Hard Disk Drive ประเภท SATA ยี่ห้อ Western Digital รุ่น WD1600AAJS ขนาด 160 GB

โดยข้อมูลที่บันทึกอยู่ในพยานหลักฐานทั้งสองนั้นเป็นข้อมูลชุดเดียวกัน ประกอบด้วย

1) ติดตั้งระบบปฏิบัติการ Windows 10 Home เวอร์ชัน 6.3

2) สร้างโฟลเดอร์ จำนวน 5 โฟลเดอร์ เพื่อเก็บไฟล์ข้อมูลต่างๆ ได้แก่ Excel, Word, PDF, Pictures และ Extension Mismatch

3) สร้างไฟล์ จำนวน 15 ไฟล์ ในแต่ละโฟลเดอร์ ดังนี้

3.1) โฟลเดอร์ Excel ประกอบด้วย ไฟล์ที่มีนามสกุลไฟล์ *.xls และ *.xlsx

3.2) โฟลเดอร์ Word ประกอบด้วย ไฟล์ที่มีนามสกุลไฟล์ *.doc และ *.docx

3.3) โฟลเดอร์ PDF ประกอบด้วย ไฟล์ที่มีนามสกุลไฟล์ *.pdf

3.4) โฟลเดอร์ Pictures ประกอบด้วย ไฟล์ที่มีนามสกุลไฟล์ *.jpg และ *.png

4) โฟลเดอร์ Extension Mismatch ได้ทำการเปลี่ยนนามสกุลไฟล์ จำนวน 9 ไฟล์ ดังนี้

4.1) ไฟล์รูปภาพ (*.JPG) เปลี่ยนนามสกุลไฟล์เป็น *.xls และ *.doc

4.2) ไฟล์ Microsoft Excel (*.xlsx) เปลี่ยนนามสกุลไฟล์เป็น *.jpg

4.3) ไฟล์ Adobe Acrobat (*.pdf) เปลี่ยนนามสกุลไฟล์เป็น *.mp4

5) ทำการลบไฟล์ จำนวน 5 ไฟล์ ในโฟลเดอร์ Excel, Word, PDF และ Pictures ซึ่งไฟล์ที่ถูกลบไปนั้น ทั้งหมด 20 ไฟล์ จะไปปรากฏอยู่ในโฟลเดอร์ Recycle Bin ซึ่งผู้ใช้สามารถคืนค่าไฟล์นั้น กลับมาใช้งานได้เช่นเดิม หลังจากนั้น ทำการลบไฟล์ทั้งหมด 20 ไฟล์ ออกจากโฟลเดอร์ Recycle Bin และจะไม่มีไฟล์ใด ปรากฏในโฟลเดอร์ Recycle Bin เลย ผู้ใช้ไม่สามารถคืนค่าไฟล์กลับมาได้หรือเป็นการลบอย่างถาวรนั่นเอง

6) ทำการลบไฟล์ โดยกดปุ่ม “Shift + Delete” ที่แป้นพิมพ์ ออกจากโฟลเดอร์ Excel, Word, PDF และ Pictures ซึ่งไฟล์ที่ถูกลบไปนั้น จะไม่ปรากฏในโฟลเดอร์ Recycle Bin เพราะเป็นการลบอย่างถาวร

**2. วิธีการวิจัย**

2.1 นำ Solid State Drive เชื่อมต่อกับอุปกรณ์ป้องกันการปนเปื้อนข้อมูลลงพยานหลักฐาน (Write Blocker) ชนิด PCIe Bridge แล้วจึงเชื่อมต่อกับเครื่องคอมพิวเตอร์ตรวจพิสูจน์ประสิทธิภาพสูง

2.2 ทำการสร้าง Case และ Add Evidence เข้าซอฟต์แวร์แต่ละซอฟต์แวร์ และทำการ Process Evidence ก่อนที่จะวิเคราะห์ข้อมูล

2.3 หลังจากที่ Process Evidence เสร็จแล้ว จึงทำการวิเคราะห์ในแต่ละคุณลักษณะการทำงานของแต่ละซอฟต์แวร์

2.4 นำ Hard Disk Drive เชื่อมต่อกับอุปกรณ์ป้องกันการปนเปื้อนข้อมูลลงพยานหลักฐาน (Write Blocker) ชนิด SATA/IDE Bridge แล้วจึงเชื่อมต่อกับเครื่องคอมพิวเตอร์ตรวจพิสูจน์ประสิทธิภาพสูง

2.5 ดำเนินการตามข้อ 2.2 และ 2.3 เช่นเดียวกับ Solid State Drive

**3. คุณลักษณะการทำงานที่นำมาวิเคราะห์เปรียบเทียบ**

3.1 Image Acquisition and Integrity Verification การทำสำเนาข้อมูลจากต้นฉบับและการตรวจสอบความสมบูรณ์ของสำเนาข้อมูล

3.2 MD5 Hashing ค่าแฮช MD5 เป็นชุดข้อมูลค่าเฉพาะของหลักฐานนั้น หรือชุดข้อมูลค่าเฉพาะไฟล์ข้อมูล เพื่อตรวจสอบความสมบูรณ์ของหลักฐานหรือเพื่อยืนยันไฟล์ข้อมูลว่าเป็นไฟล์เดียวกันหรือไม่ ซึ่งค่าแฮช MD5 มีค่าเท่ากับ 128 บิต

3.3 SHA-1 Hashing ค่าแฮช SHA-1 เป็นชุดข้อมูลค่าเฉพาะของหลักฐานนั้น หรือชุดข้อมูลค่าเฉพาะไฟล์ข้อมูลต่าง ๆ เพื่อตรวจสอบความสมบูรณ์ของหลักฐานหรือเพื่อยืนยันไฟล์ข้อมูลว่าเป็นไฟล์เดียวกันหรือไม่ ซึ่งค่าแฮช SHA-1 มีค่าเท่ากับ 160 บิต

3.4 Support for Windows OS สามารถสนับสนุนและตรวจวิเคราะห์ระบบปฏิบัติการ

3.5 Timeline Analysis สามารถวิเคราะห์การทำงานที่เกิดขึ้นในระบบ

3.6 Finds, Identifies, Recovers Deleted Files ค้นหาหรือระบุหรือกู้คืนข้อมูลที่ถูกลบไปแล้ว

3.7 Identifies File Extension Mismatches สามารถระบุว่าไฟล์ข้อมูลใดมีการเปลี่ยนแปลงนามสกุลได้

3.8 Includes HEX Level Viewer มีการแสดงข้อมูลในรูปแบบ Hex

3.9 Provides an Image Gallery มีการแสดงข้อมูลภาพในรูปแบบแกลอรี่

3.10 Shows File Modified, Accessed, and Creation Dates and Times แสดงวันที่และเวลาของการเปลี่ยนแปลง การเข้าถึง การสร้างของไฟล์ข้อมูล

3.11 Reporting/Documentation สามารถออกรายงานได้หลายรูปแบบ เช่น PDF, HTML, Word, Excel เป็นต้น

**ผลการวิจัย**

หลังจากทำการวิเคราะห์ประมวลผลพยานหลักฐาน (Process Evidence) ของซอฟต์แวร์แต่ละซอฟต์แวร์เสร็จสิ้นแล้วนั้น ได้นำผลการทดลองมาสรุปในตารางเปรียบเทียบ โดยจะใส่เครื่องหมาย “/” คือ ซอฟต์แวร์นั้น สามารถวิเคราะห์ในคุณลักษณะการทำงานนั้นได้ และเครื่องหมาย “X” คือ ซอฟต์แวร์นั้น ไม่สามารถวิเคราะห์ในคุณลักษณะการทำงานนั้นได้

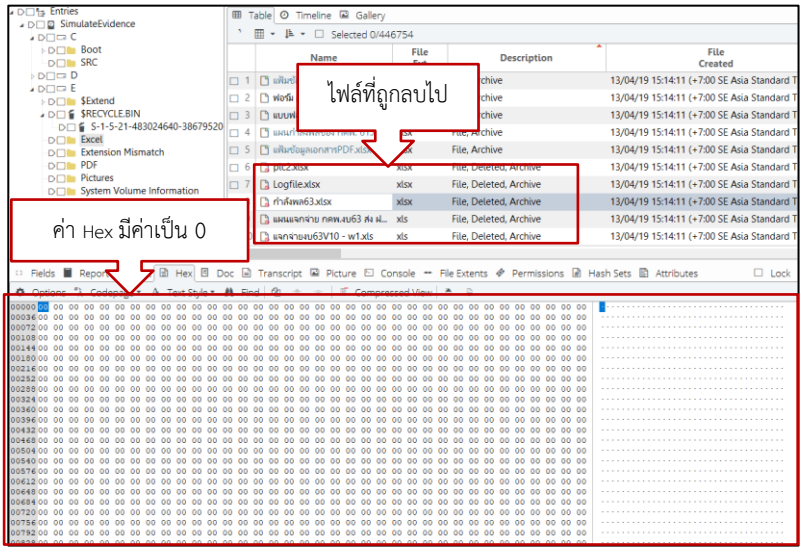
**ตารางที่ 1** ผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ ที่ทำการทดลองกับไดรฟ์ชนิด Solid State Drive

| คุณลักษณะการทำงาน | ซอฟต์แวร์ที่ใช้ | | |
|---|---|---|---|
| | EnCase 8.08 | AXIOM 3.0 | Autopsy 4.10 |
| Image Acquisition | / | / | X |
| Integrity Verification | / | / | / |
| MD5 Hashing | / | / | / |
| SHA-1 Hashing | / | / | X |
| Support for Windows OS | / | / | / |

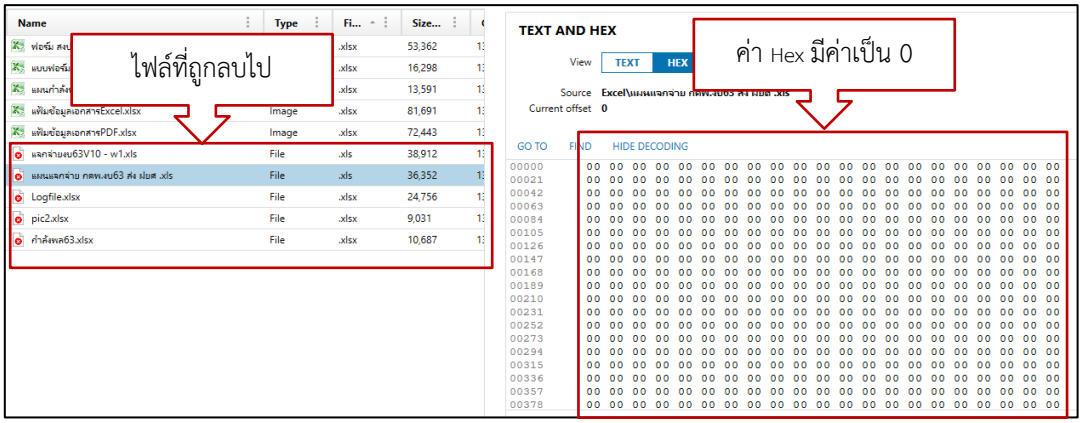
**ตารางที่ 1** ผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ที่ทำการทดลองกับไดรฟ์ชนิด Solid State Drive (ต่อ)

| คุณลักษณะการทำงาน | ซอฟต์แวร์ที่ใช้ | | |
|---|---|---|---|
| | EnCase 8.08 | AXIOM 3.0 | Autopsy 4.10 |
| Timeline Analysis | / | / | / |
| Finds Deleted Files | / | / | / |
| Identifies Deleted Files | / | / | / |
| Recovers Deleted Files | X | X | X |
| Identifies File Extension Mismatches | / | X | / |
| Includes HEX Level Viewer | / | / | / |
| Provides an Image Gallery | / | / | / |
| Shows File Modified, Accessed, and Creation Dates and Times | / | / | / |
| Reporting/Documentation | / | / | / |

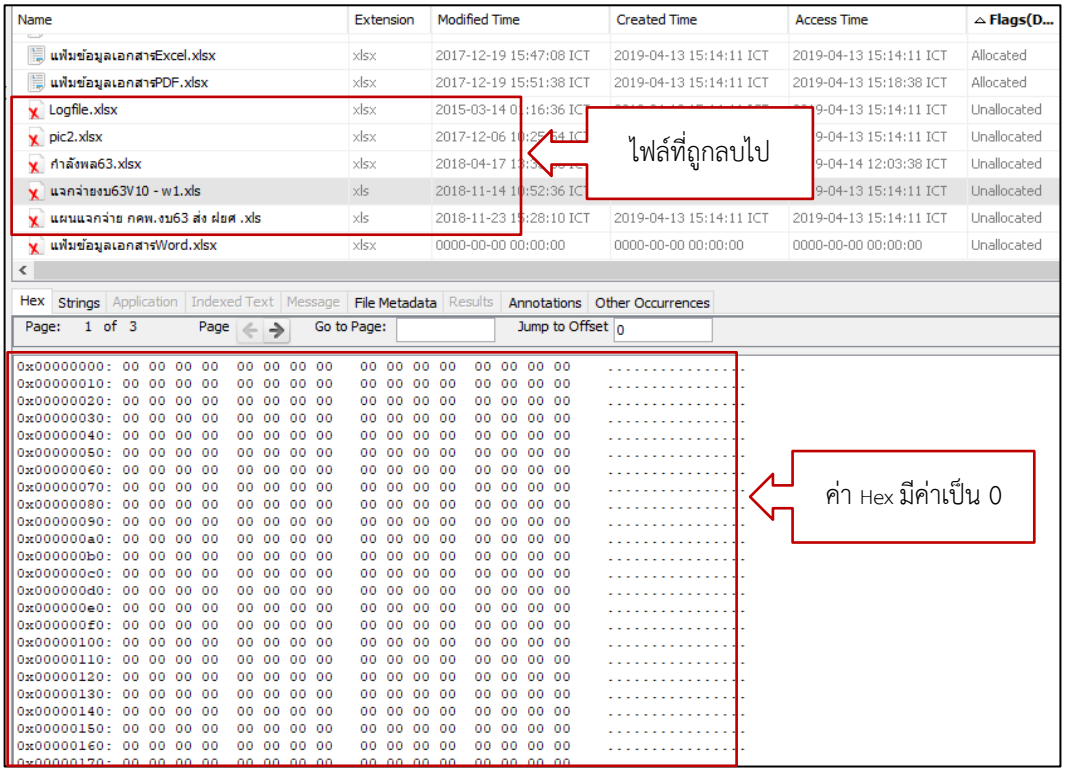
จากตารางที่ 1 ผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ที่ทำการทดลองกับไดรฟ์ชนิด Solid State Drive จะพบว่า ซอฟต์แวร์ EnCase 8.08 ไม่สามารถกู้คืนข้อมูลที่ถูกลบ (Recovers Deleted Files) ได้ ซอฟต์แวร์ AXIOM 3.0 ไม่สามารถกู้คืนข้อมูลที่ถูกลบได้และไม่สามารถวิเคราะห์คุณลักษณะการทำงาน Identifies file extension mismatches ได้ ส่วนซอฟต์แวร์ Autopsy 4.10 ไม่สามารถทำ Image Acquisition, คำนวณค่าแฮช SHA-1 และไม่สามารถกู้คืนข้อมูลที่ถูกลบได้




ภาพที่ 2 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Solid State Drive โดยใช้ซอฟต์แวร์ EnCase 8.08




ภาพที่ 3 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Solid State Drive โดยใช้ซอฟต์แวร์ AXIOM 3.0



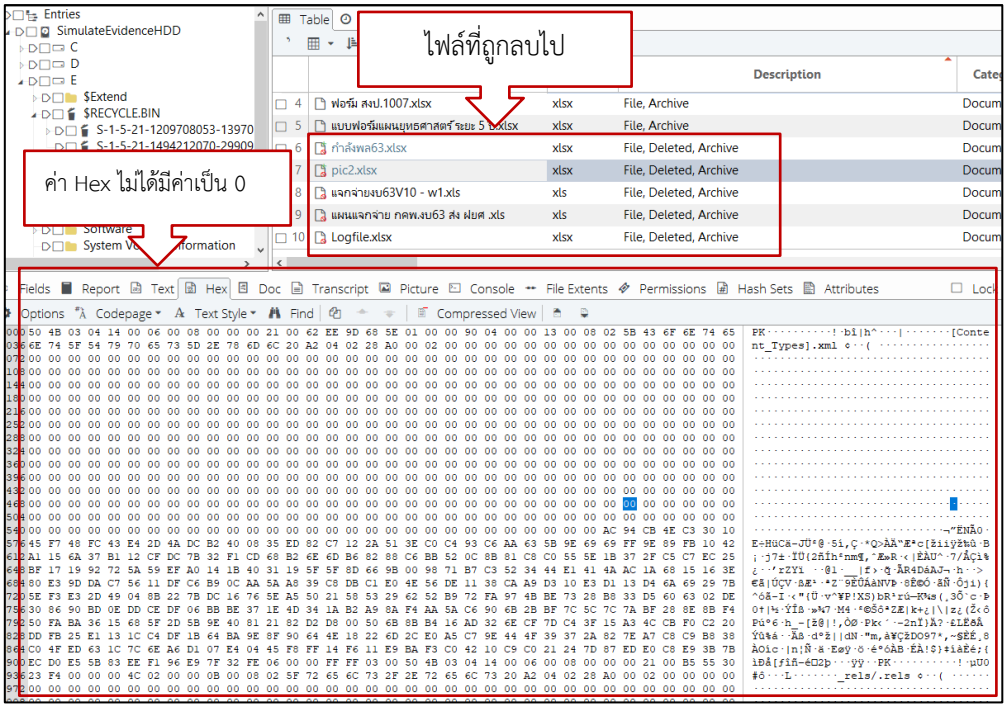

ภาพที่ 4 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Solid State Drive โดยใช้ซอฟต์แวร์ Autopsy 4.10

จากภาพที่ 2 – 4 แสดงให้เห็นว่าทั้งสามซอฟต์แวร์สามารถค้นหาและระบุชื่อไฟล์ข้อมูลที่ถูกลบไปได้ แต่ไม่สามารถกู้คืนไฟล์ข้อมูลดังกล่าวได้ เนื่องจากค่า Hex ถูกแทนค่าเป็น 0 ทั้งหมด ซึ่งเป็นผลมาจากคำสั่ง TRIM ของ Solid State Drive นั่นเอง

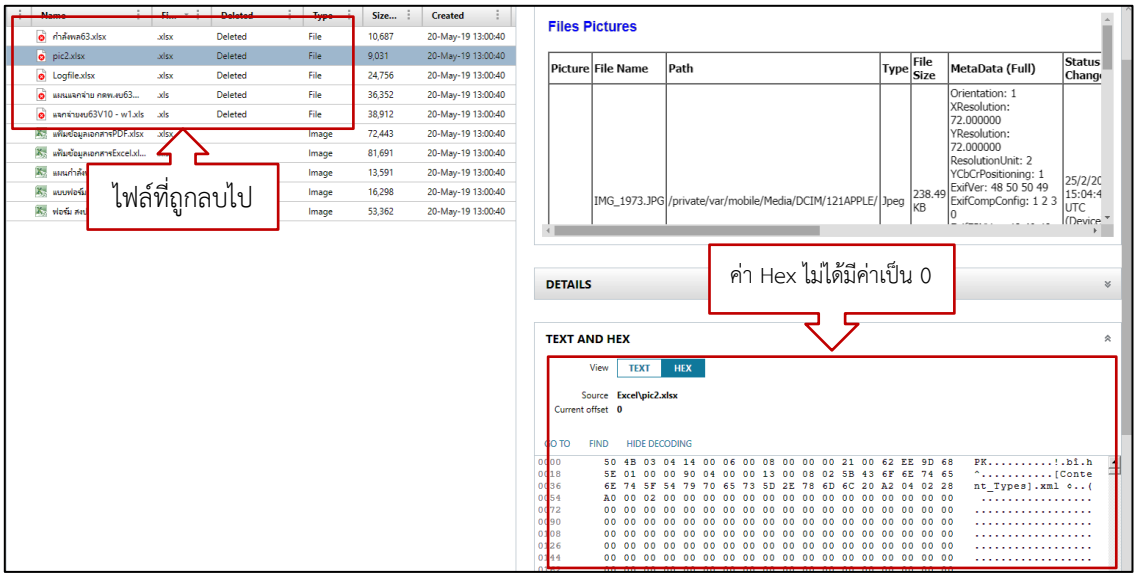
**ตารางที่ 2** ผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ที่ทำการทดลองกับไดรฟ์ชนิด Hard Disk Drive

| คุณลักษณะการทำงาน | ซอฟต์แวร์ที่ใช้ | | |
|---|---|---|---|
| | EnCase 8.08 | AXIOM 3.0 | Autopsy 4.10 |
| Image Acquisition | / | / | X |
| Integrity Verification | / | / | / |
| MD5 Hashing | / | / | / |
| SHA-1 Hashing | / | / | X |
| Support for Windows OS | / | / | / |
| Timeline Analysis | / | / | / |
| Finds deleted files | / | / | / |
| Identifies deleted files | / | / | / |
| Recovers deleted files | / | / | / |
| Identifies file extension mismatches | / | X | / |
| Includes HEX level viewer | / | / | / |
| Provides an image gallery | / | / | / |
| Shows file modified, accessed, and creation dates and times | / | / | / |
| Reporting/Documentation | / | / | / |

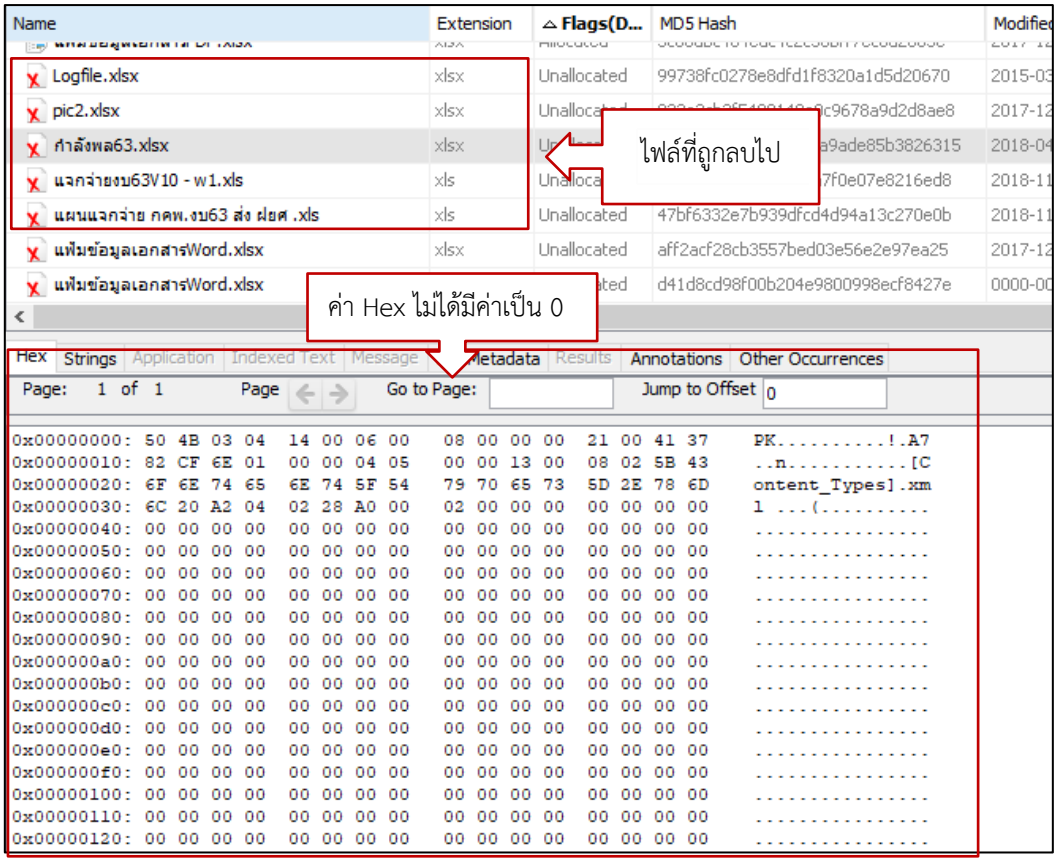
จากตารางที่ 2 ผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ที่ทำการทดลองกับไดรฟ์ชนิด Hard Disk Drive จะพบว่าซอฟต์แวร์ EnCase 8.08 สามารถวิเคราะห์คุณลักษณะการทำงานได้ทุกคุณลักษณะที่กำหนดขึ้น ซอฟต์แวร์ AXIOM 3.0 ไม่สามารถวิเคราะห์คุณลักษณะการทำงาน Identifies file extension mismatches ได้ ส่วนซอฟต์แวร์ Autopsy 4.10 ไม่สามารถทำ Image Acquisition และคำนวณค่าแฮช SHA-1 ได้




ภาพที่ 5 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Hard Disk Drive โดยใช้ซอฟต์แวร์ EnCase 8.08




ภาพที่ 6 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Hard Disk Drive โดยใช้ซอฟต์แวร์ AXIOM 3.0




ภาพที่ 7 ตัวอย่างข้อมูลไฟล์ที่ถูกลบไปจากโฟลเดอร์ Excel ใน Hard Disk Drive โดยใช้ซอฟต์แวร์ Autopsy 4.10

จากภาพที่ 5 – 7 จะพบว่าค่า Hex ของไฟล์ข้อมูลที่ถูกลบไปนั้น ไม่ได้มีค่าเป็น 0 ทำให้ทั้งสามซอฟต์แวร์ สามารถกู้คืนข้อมูลที่ถูกลบไปได้อย่างสมบูรณ์

**สรุปและอภิปรายผล**

กระบวนการตรวจพิสูจน์หลักฐานทางดิจิทัล จำเป็นจะต้องทำทุกขั้นตอนอย่างถูกต้องและสมบูรณ์ ซึ่งคุณลักษณะการทำงานที่ได้กำหนดขึ้นในการทดลองนั้นเป็นขั้นตอนที่จำเป็นอย่างยิ่งสำหรับการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล โดยผลการเปรียบเทียบคุณลักษณะการทำงานของแต่ละซอฟต์แวร์ที่ทำการทดลองกับไดรฟ์ชนิด Solid State Drive และ Hard Disk Drive จากที่ได้ทำการทดลองกับ Solid State Drive จะเห็นได้ว่าทั้งสามซอฟต์แวร์ ไม่สามารถกู้คืนข้อมูลที่ถูกลบไปได้ เนื่องจากคำสั่ง TRIM ที่ถูกกำหนดขึ้นโดยระบบปฏิบัติการ เมื่อผู้ใช้งานทำการลบข้อมูลไปหรือไฟล์ใดไฟล์หนึ่งถูกทำเครื่องหมายว่าถูกลบ คำสั่ง TRIM จะแทนค่าไฟล์เหล่านั้นเป็นค่า 0 ในบล็อกข้อมูลนั้น ๆ ซึ่งความหมายว่าไฟล์นั้นถูกลบไปอย่างสมบูรณ์และไม่สามารถกู้คืนไฟล์นั้น ๆ คืนมาได้เลย แต่ในทางตรงกันข้ามสามารถกู้คืนข้อมูลที่ถูกลบไปจาก Hard Disk Drive ได้อย่างสมบูรณ์ โดยซอฟต์แวร์ EnCase 8.08 สามารถวิเคราะห์คุณลักษณะการทำงานได้ครบทุกคุณลักษณะที่กำหนดขึ้น รองลงมาคือ

ซอฟต์แวร์ AXIOM 3.0 ซึ่งทั้งสองซอฟต์แวร์นี้เป็นโปรแกรมเชิงพาณิชย์จึงอาจใช้งบประมาณในการจัดหาสูง ส่วนซอฟต์แวร์ Autopsy 4.10 ไม่สามารถวิเคราะห์คุณลักษณะการทำงานได้ครบทุกคุณลักษณะที่กำหนด แต่ซอฟต์แวร์ Autopsy 4.10 เป็นโปรแกรมรหัสเปิด ซึ่งไม่เสียค่าใช้จ่ายในการใช้งาน อาจใช้ในการวิเคราะห์คุณลักษณะการทำงานเพื่อค้นหาและวิเคราะห์ข้อมูลเบื้องต้นได้

ส่วนคุณลักษณะการทำงานของซอฟต์แวร์แต่ละตัวที่ไม่สามารถวิเคราะห์ได้ ซึ่งซอฟต์แวร์ AXIOM ได้แก่ Identifies file extension mismatches ส่วนซอฟต์แวร์ Autopsy ได้แก่ Acquisition Image และการคำนวณค่าแฮช SHA-1 ซึ่งผลการทดลองที่ไม่สามารถวิเคราะห์ตามคุณลักษณะการทำงานเหล่านี้ได้นั้น เนื่องจากการพัฒนาของซอฟต์แวร์แต่ละตัวนั้น ยังไม่ถูกพัฒนาขึ้นในคุณลักษณะการทำงานดังกล่าว แต่ในอนาคตหรือในเวอร์ชั่นที่สูงขึ้น ซอฟต์แวร์เหล่านั้นอาจจะพัฒนาขึ้นและสามารถวิเคราะห์คุณลักษณะการทำงานได้มากขึ้น

**ข้อเสนอแนะ**

**1. ข้อเสนอแนะเพื่อนำผลการวิจัยไปใช้**

1.1 เครื่องมือตรวจพิสูจน์หลักฐานดิจิทัล มีอยู่หลากหลายและกว้างขวาง ไม่ว่าจะเป็นโปรแกรมเชิงพาณิชย์หรือโปรแกรมรหัสเปิดก็ตาม ผู้ใช้สามารถเลือกใช้เครื่องมือเหล่านั้นได้ตามจุดประสงค์ความต้องการ โดยในงานวิจัยนี้ได้เลือกวิจัยเครื่องมือตรวจพิสูจน์ทั้งโปรแกรมเชิงพาณิชย์และโปรแกรมรหัสเปิด จากผลการทดลองพบว่า ทั้งสองโปรแกรมนี้สามารถวิเคราะห์คุณลักษณะการทำงานได้เกือบจะเท่าเทียมกัน ในการวิเคราะห์ข้อมูลเบื้องต้นหรือใช้ในการสืบสวนเบื้องต้นหรือวิเคราะห์ข้อมูลที่ไม่ใช่รูปคดี อาจใช้โปรแกรมรหัสเปิดในการวิเคราะห์ได้ เนื่องจากไม่เสียค่าใช้จ่ายในการใช้งาน แต่การวิเคราะห์ข้อมูลในทางคดีหรือความผิดทางคดีอาญาหรือคดีแพ่งควรเลือกใช้โปรแกรมเชิงพาณิชย์ เนื่องจากเป็นโปรแกรมที่ใช้ในหน่วยงานบังคับใช้กฎหมายเท่านั้นและเป็นที่ยอมรับในชั้นศาล ทั้งนี้การใช้โปรแกรมทั้งสองชนิด ผู้ใช้จะต้องมีความชำนาญหรือได้รับการอบรมและฝึกฝนการใช้งานโปรแกรมก่อนเสมอ

1.2 ในงานวิจัยนี้ได้ใช้พยานหลักฐานประเภท Solid State Drive และ Hard Disk Drive ซึ่งจะพบว่า ผลของการกู้คืนข้อมูลที่ถูกลบไปนั้นแตกต่างกัน การกู้คืนข้อมูลที่ถูกลบไปจาก Solid State Drive นั้น ไม่สามารถทำได้ ซึ่งเป็นสิ่งที่ท้าทายสำหรับการตรวจพิสูจน์หลักฐานเพื่อหาข้อมูลการกระทำความผิดได้ยากยิ่งขึ้น และในอนาคตการใช้ Solid State Drive จะมีเพิ่มมากขึ้น จึงอาจก่อให้เกิดปัญหาและเกิดความยากในการที่จะกู้คืนข้อมูลที่ลบไปแล้วกลับมาได้ ดังนั้นทางบริษัทผู้ผลิตอาจมีการพัฒนาหรือแก้ไขในข้อปัญหาส่วนนี้

**2. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป**

2.1 เครื่องมือหรือซอฟต์แวร์สำหรับการตรวจพิสูจน์หลักฐานทางดิจิทัลมีอยู่หลากหลายและกว้างขวางมาก ทั้งแบบเชิงพาณิชย์และแบบรหัสเปิดซึ่งถูกพัฒนาขึ้นอย่างรวดเร็วเพื่อรองรับเทคโนโลยีที่เติบโตอย่างรวดเร็วและทันสมัย เช่น X-Ways, FTK หรือ SIFT เป็นต้น ซึ่งในอนาคตเครื่องมือหรือซอฟต์แวร์อื่น ๆ อาจสามารถใช้เพื่อให้ได้ผลลัพธ์ที่ละเอียดยิ่งขึ้นหรือสามารถวิเคราะห์คุณลักษณะการทำงานได้มากยิ่งขึ้น

2.2 ระบบปฏิบัติการรุ่นใหม่ที่ติดตั้ง Solid State Drive ได้ตั้งค่าเริ่มต้นให้เปิดใช้งานคำสั่ง TRIM จึงส่งผลให้ไม่สามารถทำการกู้คืนข้อมูลที่ถูกลบไปแล้วกลับคืนมาได้ แต่ถ้าหากทำการปิดการใช้งานคำสั่ง TRIM จะสามารถทำการกู้คืนข้อมูลที่ถูกลบไปแล้วได้หรือไม่ ซึ่งวิธีการนี้สร้างความท้าทายมากขึ้นในการตรวจพิสูจน์หลักฐานทางดิจิทัล

2.3 พยานหลักฐานทางดิจิทัลมีอยู่หลากหลายประเภท แม้กระทั่งพยานหลักฐานชนิดเดียวกัน เช่น Solid State Drive ที่มีการติดตั้งระบบปฏิบัติการ จะตั้งค่าเริ่มต้นให้เปิดใช้งานคำสั่ง TRIM แต่ถ้าใช้ Solid State Drive ในรูปแบบของ USB External Hard disk จะไม่มีการสร้างการใช้งานคำสั่ง TRIM ซึ่งวิธีการที่แตกต่างกันออกไปนี้ อาจส่งผลให้การวิเคราะห์หรือผลการตรวจพิสูจน์เปลี่ยนแปลงไป

**เอกสารอ้างอิง**

Joshi, B. R., & Hubbard, R. (2016) **Forensic Analysis of Solid State Drive (SSD).** Proceedings of 2016 Universal Technology Management Conference (UTMC). Minnesota. United State of America.

Daniel, L.E., & Daniel, L.E., (2016). **Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom.** Translated by Sunee Sakawrat. Bangkok: Foundation for Internet and Civic Culture. (In Thai).

Maurya, N., Awasthi, J., Singh, R.P., Vaish, A. (2015). Analysis of Open Source and Proprietary Source Digital Forensic Tools. **International Journal of Advanced Engineering and Global Technology,** 3(7), 916-922.

Phanwattana, P. (2018). The Reliability of Electronic Evidence Obtained from Smartphone **Journal of Criminology and Forensic Science 4.**, 2018 (1), 76-86. (In Thai).

Sanap, V.K. & Mane, V. (2015). **Comparative Study and Simulation of Digital Forensic Tools.** IJCA Proceedings on International Conference on Advances in Science and Technology ICAST. 2015 (1): 8-11, February 2016.

**ผู้เขียน**

**คำนำหน้า ชื่อ-สกุล** **ร้อยตำรวจเอกหญิง วันทนีย์ ตุลยเสวี**
หน่วยงาน/สังกัด หลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขานิติวิทยาศาสตร์ คณะนิติวิทยาศาสตร์
โรงเรียนนายร้อยตำรวจ
ที่อยู่ของหน่วยงาน/สังกัด เลขที่ 90 หมู่ 7 อำเภอสามพราน จังหวัดนครปฐม 73110
E-mail: wantanee.tulyasevee@gmail.com

**คำนำหน้า ชื่อ-สกุล** **รองศาสตราจารย์ พันตำรวจเอก วรธัช วิชชุวาณิชย์**
หน่วยงาน/สังกัด คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
ที่อยู่ของหน่วยงาน/สังกัด เลขที่ 90 หมู่ 7 อำเภอสามพราน จังหวัดนครปฐม 73110
E-mail: woratouch_w@yahoo.com