*ISSN: 1686-8420 (Print), 2651-2289 (Online)*

RMUTT Research Journal
Science and Technology
Rajamangala University of Technology Thanyaburi


# การศึกษาเปรียบเทียบการปกปิดร่องรอยหลักฐานดิจิทัล ที่ส่งผลต่อประสิทธิผลการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์

# A Comparative Study of Digital Anti-Forensic Techniques Affecting the Effectiveness of Forensic Data Recovery Software

**ทรงวุฒิ นาคศิลป์ และ วรธัช วิชชุวาณิชย์***

**Songwut Naksilp and Woratouch Vichuwanich***

คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ อ. สามพราน จ. นครปฐม 73110

Faculty of Forensic Science, Royal Police Cadet Academy, Sam Phran, Nakhon Pathom 73110, THAILAND

*Corresponding author e-mail: woratouch_w@yahoo.com

ARTICLE INFO

Article history:
Received: 5 June, 2020
Revised: 31 July, 2020
Accepted: 11 August, 2020
Available online: 20 October, 2020
DOI: 10.14456/rj-rmutt.2020.23

*Keywords:* anti-forensic, digital evidence, forensic software

ABSTRACT

This research aims (1) to examine anti-forensic techniques affecting data recovery software and (2) to compare each anti-forensic technique with impacts on efficiency of forensic data recovery software. The researcher conducted an experiment by utilizing simple and common digital anti-forensic techniques including delete, format and overwrite. After that, three forensic data recovery programs: EnCase Imager, FTK Imager and ProDiscover, were exercised to recover digital evidence and to compare the effectiveness in recovering data of the forensic software from each anti-forensic technique on data storage devices containing NTFS file system on Windows 7 operating system. The research findings revealed that the three forensic programs had similar effectiveness of forensic data recovery as follows. (1) The anti-forensic technique with commands "Delete" and "Format" without switching modes could recover digital evidence with 100% perfect condition because it was a technique that corrected or destroyed data in MFT Entry without getting involved with raw data in the file. (2) The anti-forensic technique with command "Format" and switching modes as Format

ISSN: 1686-8420 (Print), 2651-2289 (Online)

Drive: /P: Passes and overwrite could partially recover digital evidence for undestroyed raw data in the file or it was irrecoverable once the raw data in the file was demolished because the raw data in the file was damaged with overwriting. The success of data recovery was accounted for 35%, 50% and 75% from the original file. Therefore, to conclude, success of digital evidence recovery depended on the original raw data in the file.

## บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ (1) เพื่อศึกษาเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลที่ส่งผลต่อการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์ (2) เพื่อเปรียบเทียบเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลแต่ละเทคนิคที่ส่งผลต่อประสิทธิผลในการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์ โดยผู้วิจัยได้ทดลองปกปิดร่องรอยหลักฐานดิจิทัล ด้วยเทคนิคที่ไม่ซับซ้อนแต่เป็นเทคนิคที่พบเห็นได้โดยทั่วไป ได้แก่ Delete, Format และ Overwrite จากนั้นจึงใช้ซอฟต์แวร์นิติวิทยาศาสตร์จำนวน 3 โปรแกรม คือ EnCase Imager, FTK Imager และ ProDiscover กู้คืนข้อมูลหลักฐานดิจิทัล เพื่อเปรียบเทียบประสิทธิผลในการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์จากเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลแต่ละเทคนิคบนอุปกรณ์บันทึกข้อมูลที่มีระบบไฟล์แบบ NTFS ภายใต้ระบบปฏิบัติการ Windows 7 ผลจากการวิจัยพบว่า ซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม มีประสิทธิผลในการกู้คืนข้อมูลหลักฐานดิจิทัลไม่ต่างกัน คือ (1) การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete และคำสั่ง Format แบบไม่ระบุ Switch สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ในสภาพที่สมบูรณ์ 100% เนื่องจากเป็นเทคนิคที่แก้ไขหรือทำลายข้อมูลใน MFT Entry โดยไม่ยุ่งเกี่ยวกับเนื้อไฟล์ (2) การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Fomat แบบระบุ Switch คำสั่งเป็น Format Drive: /P: Passes และการ Overwrite สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ในส่วนที่เนื้อไฟล์ไม่ถูกทำลาย หรือไม่สามารถกู้คืนได้หากเนื้อไฟล์ทั้งหมดถูกทำลาย เนื่องจากเป็นเทคนิคที่ทำให้เนื้อไฟล์เสียหายด้วยการเขียนข้อมูลอื่นทับ ความสำเร็จของการกู้คืนข้อมูลคิดเป็นร้อยละจากขนาดไฟล์ต้นฉบับ เช่น 35% 50% และ 75% เป็นต้น จึงสรุปได้ว่าความสำเร็จของการกู้คืนข้อมูลหลักฐานดิจิทัลขึ้นอยู่กับเนื้อไฟล์ต้นฉบับ

***คำสำคัญ:*** การปกปิดร่องรอยหลักฐาน หลักฐานดิจิทัล ซอฟต์แวร์นิติวิทยาศาสตร์

## บทนำ

ในอดีตอาชญากรรม จะปรากฏให้เห็นในรูปแบบของอาชญากรรมพื้นฐานหรือที่เรียกว่าอาชญากรรมข้างถนน (Street Crime) ซึ่งเป็นอาชญากรรมที่สามารถพบเห็นได้โดยทั่วไปมีรูปแบบของการก่ออาชญากรรมที่ไม่สลับซับซ้อน สามารถกระทำได้โดยบุคคลเพียงคนเดียว และถึงแม้จะมีการรวมกลุ่มในการก่ออาชญากรรมก็จะเป็นการรวมกลุ่มกันในจำนวนที่ไม่มากนัก ผู้ที่ก่ออาชญากรรมส่วนใหญ่มักจะเป็นผู้ที่ด้อยโอกาสในสังคม ไม่มีการศึกษา และไม่มีการใช้เทคโนโลยีชั้นสูงในการก่ออาชญากรรม ตัวอย่างของอาชญากรรมในอดีต ได้แก่ ลักทรัพย์ ชิงทรัพย์ วิ่งราว จี้ ปล้น ทำร้ายร่างกาย ข่มขืน ฆาตกรรม เป็นต้น

ปัจจุบันรูปแบบของการก่ออาชญากรรมได้เปลี่ยนแปลงไป การก่ออาชญากรรมมีความสลับซับซ้อนมากขึ้น มีการรวมตัวกันของอาชญากร โดยจัดตั้งขึ้นเป็นกลุ่มในลักษณะองค์กร เรียกว่า องค์กรอาชญากรรม (Organized Crime) ทำให้ปัญหาการก่ออาชญากรรมในปัจจุบันมีแนวโน้มความรุนแรงมากขึ้นกว่าในอดีต

ISSN: 1686-8420 (Print), 2651-2289 (Online)

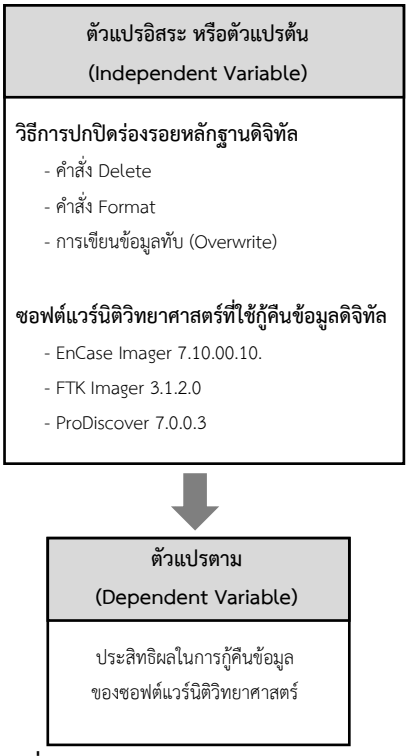
นอกจากนี้ในการก่ออาชญากรรมสมัยใหม่ก็มีการนำเอานวัตกรรมที่อาศัยเทคโนโลยีชั้นสูง (High Technology) มาใช้เป็นเครื่องมือสนับสนุนในการก่ออาชญากรรม ซึ่งเครื่องมือเหล่านั้นก็คืออุปกรณ์ดิจิทัลประเภทต่าง ๆ ได้แก่ คอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) คอมพิวเตอร์แบบพกพา (Laptop) คอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet) โทรศัพท์ประเภทสมาร์ทโฟน (Smart Phone) เป็นต้น

ในอนาคตการสืบสวนเพื่อหาตัวผู้กระทำผิดที่แท้จริงมาลงโทษตามกระบวนการยุติธรรม จึงมีความจำเป็นที่จะต้องนำเอาความรู้ทางนิติวิทยาศาสตร์ (Forensic Science) มาประยุกต์ใช้ เพื่อพิสูจน์ข้อเท็จจริงแห่งคดีและเพื่อบังคับใช้กฎหมายในการลงโทษทางอาญาแก่ผู้กระทำความผิด แต่เนื่องจากการก่ออาชญากรรมมีการเปลี่ยนแปลงรูปแบบไปจากเดิม ดังนั้น ข้อมูลหรือวัตถุพยานต่าง ๆ ที่ใช้เป็นเบาะแส หรือถูกนำมาใช้เป็นหลักฐานในการสืบสวนหาตัวผู้กระทำผิดจึงมีความสลับซับซ้อนมากยิ่งขึ้น เช่น การเผยแพร่ภาพลามกอนาจารโดยใช้เทคโนโลยีและอุปกรณ์ดิจิทัลเป็นเครื่องมือในการกระทำความผิด กรณีนี้การติดตามผู้กระทำผิด จึงจำเป็นจะต้องหาร่องรอยข้อมูลหลักฐานจากอุปกรณ์ดิจิทัลที่ใช้ในการก่ออาชญากรรมทางอินเทอร์เน็ต ดังนั้น พยานหลักฐานดิจิทัล (Digital Evidence) จึงเป็นหลักฐานที่สำคัญมากสำหรับการก่ออาชญากรรมในลักษณะนี้ แต่เนื่องจากพยานหลักฐานดิจิทัลมีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่าย และการแก้ไขนั้นอาจไม่เหลือร่องรอยให้ตรวจสอบในภายหลัง ทำให้การดำเนินการกับพยานหลักฐานดิจิทัลจำเป็นต้องมีกระบวนการจัดเก็บ ตรวจค้น วิเคราะห์ และรายงานผลที่ได้มาตรฐาน เพื่อให้พยานหลักฐานดิจิทัลคงไว้ซึ่งความน่าเชื่อถือและสามารถรับฟังได้ในการพิจารณาคดีชั้นศาล ถึงแม้ว่าในปัจจุบันศาลไทยจะให้การยอมรับและรับฟังพยานหลักฐานดิจิทัลแล้วก็ตาม แต่เนื่องจากข้อมูลดิจิทัลเป็นสิ่งที่ไม่มีรูปร่างและไม่สามารถจับต้องหรือสัมผัสได้โดยตรง การนำผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics) มาใช้อ้างอิงอาจเกิดข้อโต้แย้งเกี่ยวกับความน่าเชื่อถือของข้อมูลที่ได้มาว่ามีความครบถ้วนสมบูรณ์หรือไม่ ข้อโต้แย้งเกี่ยวกับการถูกเปลี่ยนแปลงข้อมูลดิจิทัลในระหว่างกระบวนการรวบรวมพยานหลักฐาน หรือข้อโต้แย้งเรื่องความน่าเชื่อถือของผลการวิเคราะห์และตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งหัวใจสำคัญที่จะทำให้ผลการตรวจพิสูจน์พยานหลักฐานดิจิทัลได้รับการยอมรับในชั้นศาลโดยไม่ถูกโต้แย้งก็คือจะต้องสามารถยืนยันได้ว่าพยานหลักฐานดิจิทัลที่นำมาใช้อ้างอิงนั้นเป็นหลักฐานชิ้นเดียวกับที่เก็บรวบรวมได้จากสถานที่เกิดเหตุจริงและไม่มีการเปลี่ยนแปลงข้อมูลใด ๆ ไปจากเดิม ปัจจัยที่สำคัญอีกประการหนึ่งก็คือมีผู้พัฒนาโปรแกรมสำหรับใช้ปกปิดร่องรอยหลักฐาน (Anti-forensic) ที่บันทึกไว้ในคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์เพื่อให้ยากต่อการสืบสวนคดีที่ต้องใช้พยานหลักฐานดิจิทัล โดยมีการนำโปรแกรมเหล่านี้ออกแจกจ่ายให้ใช้โดยไม่มีการเสียค่าตอบแทนแต่อย่างใด (Freeware) บางโปรแกรมสามารถนำไปใช้งาน ศึกษา แก้ไข และเผยแพร่ได้อย่างเสรีปราศจากเงื่อนไขเพิ่มเติม (Open Source License) ตัวอย่างของวิธีการที่ใช้ในการปกปิดร่องรอยพยานหลักฐานดิจิทัล ได้แก่ การเข้ารหัสข้อมูล (Encryption) การเขียนข้อมูลใหม่ทับข้อมูลเก่าเพื่อไม่ให้สามารถกู้คืนได้ (Overwrite) การแก้ไขข้อมูลเมทาดาต้า (Metadata) ของไฟล์ หรือการปลอมแปลงไฟล์ เป็นต้น

จากปัญหาที่กล่าวมาข้างต้นจะเห็นได้ว่าการสืบสวนที่ต้องนำพยานหลักฐานดิจิทัลไปใช้ในการพิสูจน์ข้อเท็จจริง จะต้องคำนึงถึงการรักษาคุณค่าของพยานหลักฐานและการแสดงความน่าเชื่อถือในกระบวนการที่เกี่ยวข้องกับการจัดการพยานหลักฐานอย่างสมเหตุสมผล เนื่องจากพยานหลักฐานดิจิทัลมีความเปราะบางและซับซ้อน โดยมีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่าย และเมื่อข้อมูลดิจิทัลถูกเปลี่ยนแปลงแก้ไขแล้วอาจไม่เหลือร่องรอยให้ตรวจสอบได้ในภายหลัง จึงนับว่าเป็นเรื่องที่ยากต่อการตรวจสอบทางนิติวิทยาศาสตร์ หาก

ISSN: 1686-8420 (Print), 2651-2289 (Online)

หลักฐานดิจิทัลเหล่านั้นถูกปกปิดร่องรอยหลักฐานด้วยเทคนิคต่าง ๆ ดังนั้น ผู้วิจัยจึงมีความสนใจเกี่ยวกับ “การศึกษาเปรียบเทียบการปกปิดร่องรอยหลักฐานดิจิทัลที่ส่งผลต่อประสิทธิผลการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์” โดยคาดหวังว่าผลการวิจัยครั้งนี้จะสามารถนำไปใช้เป็นข้อมูลในการพัฒนามาตรฐานการกู้คืนข้อมูลดิจิทัลในงานตรวจพิสูจน์หลักฐานทางนิติวิทยาศาสตร์ต่อไปในอนาคต

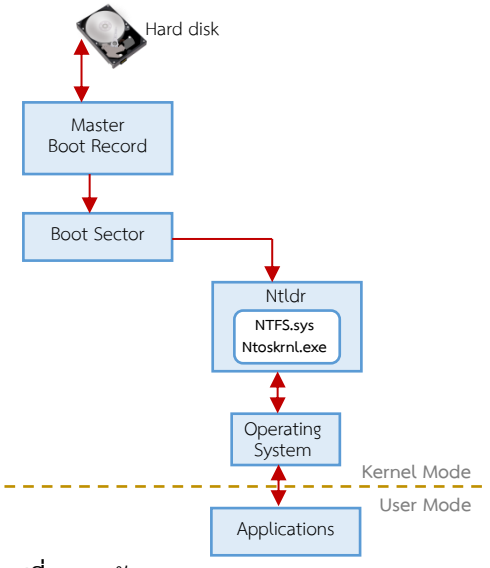



**รูปที่ 1** กรอบแนวคิดในการวิจัย

งานวิจัยนี้มีแนวคิดว่าเมื่อข้อมูลดิจิทัลถูกปกปิดร่องรอยหลักฐานด้วยเทคนิคที่ต่างกันย่อมส่งผลต่อการกู้คืนข้อมูลเหล่านั้นด้วย โดยทำการเปรียบเทียบกันระหว่างซอฟต์แวร์นิติวิทยาศาสตร์ที่ได้รับความนิยมใช้เป็นเครื่องมือในการสืบสวน (Investigation Tools) และเป็นซอฟต์แวร์ที่ใช้ในหน่วยงานที่มีหน้าที่พิสูจน์หลักฐานดิจิทัล การวิจัยครั้งนี้ผู้วิจัยได้เลือกใช้ซอฟต์แวร์นิติวิทยาศาสตร์ในรุ่นที่เปิดให้ผู้ที่สนใจสามารถนำไปทดลองใช้เพื่อการศึกษาโดยไม่มีค่าใช้จ่าย จำนวน 3 โปรแกรมประกอบด้วย

- โปรแกรม EnCase Imager 7.10.00.103
- โปรแกรม FTK Imager 3.1.2.0
- โปรแกรม ProDiscover 7.0.0.3

จากแนวคิดข้างต้น ผู้วิจัยจึงได้ออกแบบการทดลองกู้คืนข้อมูลดิจิทัลโดยพิจารณาคัดเลือกเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลที่ไม่ซับซ้อนแต่เป็นเทคนิคที่พบเห็นโดยทั่วไป จำนวน 3 เทคนิค ได้แก่ การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Format และ การปกปิดร่องรอยหลักฐานด้วยการเขียนทับหรือ Overwrite แสดงดังรูปที่ 1




**รูปที่ 2** สถาปัตยกรรม NTFS (1)

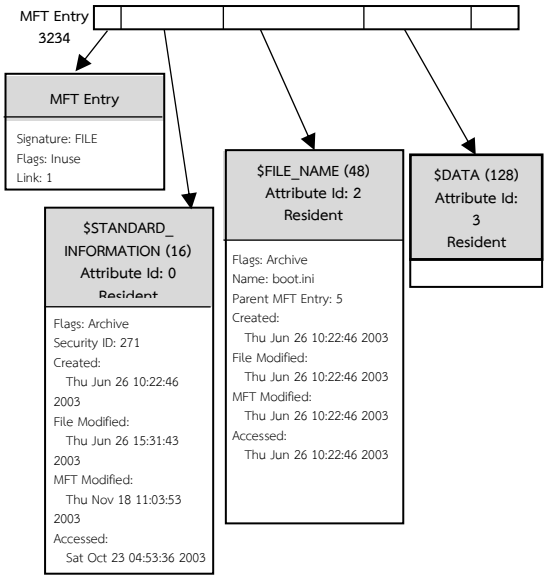
งานวิจัยนี้ได้ทำการทดลองกับอุปกรณ์บันทึกข้อมูลที่เป็น USB Flash Drive มีระบบไฟล์แบบ NTFS ภายใต้ระบบปฏิบัติการ Windows 7 จึงได้มีการศึกษาค้นคว้าและทบทวนวรรณกรรม ดังนี้

สถาปัตยกรรม NTFS ในระหว่างการสร้างพาร์ติชันให้กับฮาร์ดิสก์ โปรแกรมที่ใช้สร้างพาร์ติชันจะสร้างมาสเตอร์บูตเรกคอร์ด (MBR) ซึ่งภายในบันทึกตารางพาร์ติชัน และโค้ดสำหรับสั่งให้โปรแกรมทำงานที่เรียกว่ามาสเตอร์บูตโค้ดเอาไว้ ดังนั้นเมื่อเปิดเครื่องคอมพิวเตอร์ BIOS จะตรวจสอบการทำงานของอุปกรณ์ที่เชื่อมต่ออยู่บนเมนบอร์ด โดยอ่านค่าจาก MBR และเรียกใช้มาสเตอร์บูตโค้ดภายในตัวมันเอง แล้วส่งต่อการควบคุมไปยังบูตเซกเตอร์ในฮาร์ดดิสก์ หลังจากนั้น

*ISSN: 1686-8420 (Print), 2651-2289 (Online)*

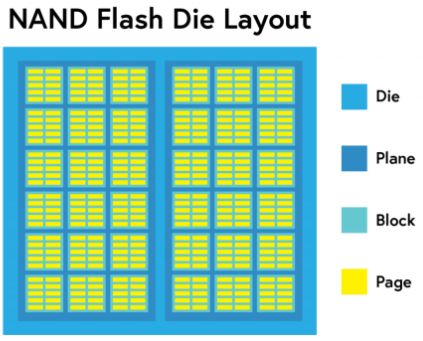
ระบบปฏิบัติการจะถูกทำการบูต เพื่อเริ่มใช้งานต่อไป แสดงดังรูปที่ 2

โดยในระบบไฟล์แบบ NTFS ประกอบด้วยส่วนสำคัญ 4 ส่วน คือ NTFS Boot Sector เป็นส่วนที่เก็บเค้าโครงและโครงสร้างระบบไฟล์ Master File Table (MFT) เป็นส่วนที่เก็บข้อมูลที่จำเป็นในการจัดเก็บไฟล์และเข้าถึงไฟล์ของระบบ NTFS ทั้งหมด File System Data เป็นส่วนที่เก็บข้อมูลอื่นที่ไม่มีใน MFT และ Master File Table Copy เป็นส่วนที่ใช้ในการทำสำเนาที่จำเป็นจาก MFT สำหรับกู้คืนระบบไฟล์ ในกรณีที่ MFT มีปัญหา ดังนั้น MFT จึงนับว่ามีความสำคัญอย่างยิ่ง เพราะเป็นส่วนที่ใช้ในการจัดเก็บข้อมูลพร้อมทั้งแสดงส่วนของ Header และระบุตำแหน่งของข้อมูลทั้งหมดโดยจะเก็บข้อมูลเป็น Entry โดยข้อมูลภายใน MFT Entry ของไฟล์พื้นฐานทุกไฟล์ Carrier B. (2) อธิบายว่าข้อมูลภายใน MFT Entry ประกอบด้วย MFT Entry Header เป็นส่วนที่มีหน้าที่อธิบายถึงโครงสร้างข้อมูลของแต่ละ MFT Entry มีข้อมูลเริ่มต้นเป็น ASCII String โดย “FILE” เป็นข้อมูลที่เรียกว่า Signature และในส่วนของเนื้อหา (Attribute Content) ประกอบด้วย $STANDARD INFORMATION, $DATA และ $FILE_NAME แสดงดังรูปที่ 3




**รูปที่ 3** ข้อมูลภายใน MFT Entry (2)

อุปกรณ์บันทึกข้อมูลแบบ SSD เป็นเทคโนโลยีที่คาดว่าจะมาแทนทีเทคโนโลยีฮาร์ดดิสก์ไดร์ฟ โดยในปัจจุบัน NAND Flash ถูกนำไปใช้เป็นส่วนประกอบสำคัญของอุปกรณ์บันทึกข้อมูลแบบ SSD เนื่องจาก NOR Flash มีความจุต่ำ และราคาสูง NAND Flash ประกอบด้วยส่วนสำคัญ 4 ส่วน คือ Die Plane Block และ Page โดย Page คือหน่วยที่เล็กที่สุดที่สามรถติดตั้งโปรแกรมหรือเขียนข้อมูลได้ ส่วนการลบข้อมูลสามารถทำได้ในระดับ Block เท่านั้น โครงสร้างของ NAND Flash แสดงดังรูปที่ 4




**รูปที่ 4** โครงสร้างของชิป NAND Flash (3)

Shimpi AL. (4) อธิบายถึงลักษณะทางกายวิภาคของ SSD ว่าในปัจจุบันมาตรฐานของ SSD จะมีขนาดของ Page เท่ากับ 4 กิโลไบต์ (KB) โดย Page จะถูกจัดกลุ่มเข้าด้วยกันเป็น Block แต่ละ Block มีจำนวน 128 Page (1 Block มีขนาด 512 กิโลไบต์) Block เป็นโครงสร้างที่เล็กที่สุดในหน่วยความจำ NAND Flash ที่สามารถลบข้อมูลได้ ดังนั้น ในขณะที่ทำการอ่านหรือเขียนข้อมูลบน Page ผู้ใช้งานจะสามารถลบข้อมูลใน Block ได้ครั้งละ 128 Page เท่านั้น

## วิธีดำเนินการวิจัย

*เครื่องมือและอุปกรณ์ที่ใช้ในการทดลอง*

1. อุปกรณ์บันทึกข้อมูลที่ใช้ในการทดลอง คือ USB Flash Drive ซึ่งเป็นอุปกรณ์บันทึกข้อมูลแบบ SSD (Solid State Drive) เนื่องจากในการทดลองแต่ละครั้งมีความจำเป็นต้องทำสำเนาหลักฐานดิจิทัลเพื่อใช้ในการ

ISSN: 1686-8420 (Print), 2651-2289 (Online)

วิเคราะห์ข้อมูล และป้องกันไม่ให้หลักฐานต้นฉบับเกิดความเสียหาย ประกอบกับการทำสำเนาหลักฐานดิจิทัลเป็นการทำสำเนาแบบบิตต่อบิต หรือที่เรียกว่า “Bit-stream Copy” เพื่อทำให้สำเนาเหมือนกับต้นฉบับทุกประการ จึงต้องใช้เวลาในการทดลองค่อนข้างนาน ดังนั้น ในการทดลองครั้งนี้ผู้วิจัยจึงเลือกใช้ USB Flash Drive ซึ่งมีความจุไม่มากนัก และการเข้าถึงข้อมูลจากอุปกรณ์บันทึกข้อมูลแบบ SSD ใช้เวลาน้อยกว่าอุปกรณ์แบบหัวอ่าน

2. ระบบปฏิบัติการ (Operating System: OS) ที่ใช้คือ Windows 7 เนื่องจากเป็นระบบปฏิบัติการที่นิยมใช้กันอย่างแพร่หลาย จากผลการสำรวจของ NetMarketShare.com (5) ระหว่างมี.ค. 2018 - ก.พ. 2019 พบว่าระบบปฏิบัติการ Windows7 มีส่วนแบ่งการตลาดของระบบปฏิบัติการคอมพิวเตอร์ส่วนบุคคล (Desktop/Laptop) เป็นอันดับ 1 ของโลก คิดเป็นร้อยละ 40.17 จากยอดการใช้งานทั้งหมด

3. ระบบไฟล์ (File System) ในการติดตั้งอุปกรณ์บันทึกข้อมูลใหม่ลงบนคอมพิวเตอร์ จำเป็นจะต้องจัดระบบโครงสร้างพื้นฐานด้วยการจัดระเบียบข้อมูลโดยการฟอร์แมท ซึ่งระบบไฟล์แบบ NTFS ถูกออกแบบให้มีคุณสมบัติหลายอย่างที่เหมาะกับการติดตั้งระบบปฏิบัติการ Windows 7

4. ซอฟต์แวร์ที่ใช้ในการทดลอง แบ่งออกเป็น 2 ประเภท คือ ซอฟต์แวร์นิติวิทยาศาสตร์ และซอฟต์แวร์ที่ใช้เป็นเครื่องมือในการปกปิดร่องรอยหลักฐาน

- ซอฟต์แวร์นิติวิทยาศาสตร์ ได้แก่ ซอฟต์แวร์ที่นิยมใช้ในหน่วยงานพิสูจน์หลักฐานคอมพิวเตอร์ เป็นรุ่นที่ให้ใช้โดยไม่มีค่าใช้จ่ายเพื่อการศึกษา จำนวน 3 โปรแกรมได้แก่ EnCase Imager 7.10.00.103, FTK Imager 3.1.2.0 และ ProDiscover 7.0.0.3

- ซอฟต์แวร์ที่ใช้เป็นเครื่องมือในการปกปิดร่องรอยหลักฐาน (Anti-forensic Tools) ได้แก่ Sdelete 2.02 และ Eraser 6.2.0.2986

5. ไฟล์ข้อมูลต้นฉบับที่ใช้ในการทดลอง เพื่อให้การทดลองเกิดความหลากหลายผู้วิจัยจึงได้สร้างไฟล์ข้อมูลที่มีส่วนขยายของไฟล์ในรูปแบบต่าง ๆ ประกอบด้วย Adobe Acrobat Document (.pdf), File folder, PNG image (.png), Microsoft Excel Worksheet (.xlsx), JPEG image (.jpg), Microsoft Word Document (.docx) และ GIF image (.gif)

*รูปแบบการทดลอง*

ผู้วิจัยได้ออกแบบการทดลองกู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานดิจิทัล ดังนี้

การทดลองที่ 1 กู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete ซึ่งเป็นคำสั่งพื้นฐานของระบบปฏิบัติการ Windows 7 ไม่ต้องติดตั้งเพิ่มเติม เพื่อทดสอบว่าซอฟต์แวร์นิติวิทยาศาสตร์สามารถกู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานจากการ Delete ได้จริง และเพื่อค้นหาตำแหน่งของข้อมูล (Physical Sector) ที่ถูกลบบนอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัล (Digital Evidence) ว่าไม่มีการเปลี่ยนแปลงตำแหน่ง

การทดลองที่ 2 กู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยคำสั่ง Format ซึ่งเป็นกระบวนการในการจัดรูปแบบของอุปกรณ์ที่ใช้ในการบันทึกข้อมูล เพื่อให้มีคุณสมบัติเหมาะสมกับระบบปฏิบัติการที่ใช้ โดยการล้างไฟล์ระบบเก่า แล้วสร้างไฟล์ระบบใหม่ขึ้นมา เพื่อทดสอบว่าเมื่อใช้คำสั่ง Format แล้ว สามารถพบร่องรอยของข้อมูลที่ต้องการกู้คืน และเพื่อทดสอบว่าอุปกรณ์บันทึกข้อมูลที่เป็นหลักฐานดิจิทัลเมื่อผ่านกระบวนการในการจัดรูปแบบระบบไฟล์ใหม่แล้วยังสามารถกู้คืนข้อมูลได้โดยจำนวนครั้งในการใช้คำสั่ง Format มีผลต่อการกู้คืนข้อมูล

การทดลองที่ 3 กู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยการ Overwrite ซึ่งเป็นวิธีการเขียนข้อมูลอื่น ๆ ทับลงไปบนข้อมูลที่ต้องการปกปิดร่องรอยหลักฐาน ป้องกันไม่ให้สามารถนำข้อมูลดังกล่าวกลับไปใช้ได้อีก เพื่อหาความเป็นไปได้ในการลบข้อมูลแบบถาวร และเพื่อทดสอบว่าอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัล

*ISSN: 1686-8420 (Print), 2651-2289 (Online)*

เมื่อถูกเขียนข้อมูลอื่น ๆ ทับลงไปในตำแหน่งของข้อมูลซึ่งเป็นหลักฐานดิจิทัลแล้ว ไม่สามารถกู้คืนข้อมูลได้

*วิธีการทดลอง*

ขั้นตอนการกู้คืนข้อมูลหลักฐานดิจิทัลจากการปกปิดร่องรอยหลักฐานด้วยเทคนิคต่าง ๆ ประกอบด้วย

1. ใช้เทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลแต่ละเทคนิคกับไฟล์ข้อมูลดิจิทัลต้นฉบับที่เตรียมไว้ ดังนี้

การทดลองที่ 1 คำสั่ง Delete เป็นคำสั่งพื้นฐานไม่ต้องติดตั้งเพิ่มเติม เรียกใช้คำสั่งได้จาก Command Line หรือ GUI (Graphic-User Interface) ด้วยการกดปุ่ม Shift+Delete หรือกดปุ่ม Shift พร้อมทั้งใช้เมาส์ลากข้อมูลที่ต้องการลบไปที่ Recycle Bin

การทดลองที่ 2 คำสั่ง Format ให้ทำการทดลอง Format จำนวน 1 ครั้ง, 3 ครั้ง, 5 ครั้ง และ 7 ครั้ง ตามลำดับ แบ่งออกเป็น 2 กรณี คือ

- Format โดยไม่ระบุคำสั่งย่อย (Switch) เรียกใช้คำสั่งได้จาก Command Line โดยมีรูปแบบคำสั่งคือ Format drive: หรือ GUI ด้วยการคลิกขวาไดร์ฟที่ต้องการ Format แล้วเลือกคำสั่ง Format จาก Context Menu

- Format ระบุ Switch ไม่สามารถเรียกใช้คำสั่งจาก GUI ได้ ต้องเรียกใช้คำสั่งจาก Command Line เท่านั้น โดยมีรูปแบบคำสั่งคือ Format drive: /P:Passes เช่น Format G: /P:5 หมายถึงการสั่งให้ Format ไดร์ฟ G: แล้วเขียน 0 ทับลงในทุกตำแหน่งของไดร์ฟ G: ตามจำนวนครั้งที่กำหนด คือ 5 ครั้ง

การทดลองที่ 3 การ Overwrite เป็นการเขียนข้อมูลอื่นทับลงบนตำแหน่งเดิมของข้อมูลที่ต้องการปกปิดร่องรอยหลักฐาน แบ่งออกเป็น 2 กรณี คือ

- Overwrite แบบใช้ซอฟต์แวร์ปกปิดร่องรอยหลักฐาน ได้แก่ Sdelete 2.02 และ Eraser 6.2.0.2986 โดยตั้งค่าการเขียนทับตั้งแต่ 1 ครั้ง แล้วเพิ่มขึ้นทีละ 1 จนซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรมไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้

- Overwrite แบบไม่ใช้ซอฟต์แวร์ โดยทำการลบข้อมูลหลักฐานดิจิทัลทั้งหมดแล้วบันทึกไฟล์ข้อมูลอื่นลงบนอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัลทีละไฟล์จนกว่าจะไม่สามารถกู้คืนหลักฐานดิจิทัลได้

2. สร้างสำเนาข้อมูลดิจิทัลแบบ Bit-stream Copy ด้วยซอฟต์แวร์นิติวิทยาศาสตร์ เพื่อให้สำเนาดิจิทัลที่สร้างขึ้นเหมือนกับต้นฉบับทุกประการ

3. นำสำเนาหลักฐานดิจิทัลไปทำการกู้คืนข้อมูลด้วยซอฟต์แวร์นิติวิทยาศาสตร์ ทั้ง 3 โปรแกรม

4. เปรียบเทียบประสิทธิผลในการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์ ทั้ง 3 โปรแกรม

## ผลการศึกษาและอภิปรายผล

การกู้คืนข้อมูลหลักฐานดิจิทัลที่ถูกปกปิดร่องรอยหลักฐาน สามารถอธิบายผลการทดลองได้ ดังนี้

*ผลการทดลอง*

การทดลองปกปิดร่องรอยหลักฐานดิจิทัลด้วยการ Delete, Format และ Overwrite มีผลการทดลองตามตาราง ดังต่อไปนี้

**ตารางที่ 1** การกู้คืนข้อมูลจากคำสั่ง Delete

| **ชนิดข้อมูล** | **ผลการกู้คืนข้อมูลจากคำสั่ง Delete** | | |
|---|---|---|---|
| | **EnCase Imager 7.10.00.103** | **FTK Imager 3.1.2.0** | **ProDiscover 7.0.0.3** |
| PDF | ✓ | ✓ | ✓ |
| FILE FOLDER | ✓ | ✓ | ✓ |
| XLSX | ✓ | ✓ | ✓ |
| PNG | ✓ | ✓ | ✓ |
| JPG | ✓ | ✓ | ✓ |
| DOCX | ✓ | ✓ | ✓ |
| GIF | ✓ | ✓ | ✓ |

ISSN: 1686-8420 (Print), 2651-2289 (Online)

จากตารางที่ 1 พบว่าซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ในสภาพที่สมบูรณ์ 100%

**ตารางที่ 2** การกู้คืนข้อมูลจากคำสั่ง Format

| ชนิดข้อมูล | ผลการกู้คืนข้อมูลจากคำสั่ง Format 1, 3, 5, 7 ครั้ง | | |
|---|---|---|---|
| | EnCase Imager 7.10.00.103 | FTK Imager 3.1.2.0 | ProDiscover 7.0.0.3 |
| PDF | ✓ | ✓ | ✓ |
| FILE | ✓ | ✓ | ✓ |
| FOLDER | | | |
| XLSX | ✓ | ✓ | ✓ |
| PNG | ✓ | ✓ | ✓ |
| JPG | ✓ | ✓ | ✓ |
| DOCX | ✓ | ✓ | ✓ |
| GIF | ✓ | ✓ | ✓ |

**ตารางที่ 2** (ต่อ)

| ชนิดข้อมูล | ผลการกู้คืนข้อมูลจากคำสั่ง Format drive: /P: 1 | | |
|---|---|---|---|
| | EnCase Imager 7.10.00.103 | FTK Imager 3.1.2.0 | ProDiscover 7.0.0.3 |
| PDF | ✗ | ✗ | ✗ |
| FILE | ✗ | ✗ | ✗ |
| FOLDER | | | |
| XLSX | ✗ | ✗ | ✗ |
| PNG | ✗ | ✗ | ✗ |
| JPG | ✗ | ✗ | ✗ |
| DOCX | ✗ | ✗ | ✗ |
| GIF | ✗ | ✗ | ✗ |

จากตารางที่ 2 พบว่าเมื่อใช้คำสั่ง Format โดยไม่ระบุคำสั่งย่อย (Switch) จำนวน 1 ครั้ง, 3 ครั้ง, 5 ครั้ง และ 7 ครั้ง ตามลำดับ ซอฟต์แวร์นิติวิทยาศาสตร์ ทั้ง 3 โปรแกรม สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ แต่กรณีใช้คำสั่ง Format ในรูปแบบ Format drive: /P:1 พบว่าการ Format โดยกำหนดให้ P มีค่าเท่ากับ 1 ไม่สามารถกู้คืนข้อมูลได้ ดังนั้น จึงไม่ได้ทำการทดลองกำหนดให้ค่า P เท่ากับ 3 5 และ 7 ตามที่ได้ออกแบบการทดลองไว้

**ตารางที่ 3** การกู้คืนข้อมูลจากการ Overwrite

| ชนิดข้อมูล | ใช้ซอฟต์แวร์ในการ Overwrite จำนวน 1 ครั้ง | | |
|---|---|---|---|
| | EnCase Imager 7.10.00.103 | FTK Imager 3.1.2.0 | ProDiscover 7.0.0.3 |
| PDF | ✗ | ✗ | ✗ |
| FILE | ✗ | ✗ | ✗ |
| FOLDER | | | |
| XLSX | ✗ | ✗ | ✗ |
| PNG | ✗ | ✗ | ✗ |
| JPG | ✗ | ✗ | ✗ |
| DOCX | ✗ | ✗ | ✗ |
| GIF | ✗ | ✗ | ✗ |

**ตารางที่ 3** (ต่อ)

| ชนิดข้อมูล | ผลการกู้คืนข้อมูลจากการ Overwrite โดยไม่ใช้ซอฟต์แวร์ | | |
|---|---|---|---|
| | EnCase Imager 7.10.00.103 | FTK Imager 3.1.2.0 | ProDiscover 7.0.0.3 |
| **ลบข้อมูลทั้งหมด** ครั้งที่ 1 เขียนข้อมูลทับ 324 MB | | | |
| PDF | ✓ | ✓ | ✓ |
| FILE | ✗ | ✗ | ✗ |
| FOLDER | | | |
| XLSX | ✓ | ✓ | ✓ |
| PNG | ✓ | ✓ | ✓ |
| JPG | ✓ | ✓ | ✓ |
| DOCX | ✓ | ✓ | ✓ |
| GIF | ✓ | ✓ | ✓ |

*ISSN: 1686-8420 (Print), 2651-2289 (Online)*

| ชนิดข้อมูล | ผลการกู้คืนข้อมูลจากการ Overwrite โดยไม่ใช้ซอฟต์แวร์ | | |
|---|---|---|---|
| | EnCase Imager 7.10.00.103 | FTK Imager 3.1.2.0 | ProDiscover 7.0.0.3 |
| **ลบข้อมูลทั้งหมด** ครั้งที่ 2 เขียนข้อมูลทับเพิ่ม 281 MB | | | |
| PDF | ✗ | ✗ | ✗ |
| FILE FOLDER | ✗ | ✗ | ✗ |
| XLSX | ✓ | ✓ | ✓ |
| PNG | ✓ | ✓ | ✓ |
| JPG | ✓ | ✓ | ✓ |
| DOCX | ✓ | ✓ | ✓ |
| **ลบข้อมูลทั้งหมด** ครั้งที่ 3 เขียนข้อมูลทับเพิ่ม 336 MB | | | |
| PDF | ✗ | ✗ | ✗ |
| FILE FOLDER | ✗ | ✗ | ✗ |
| XLSX | ✗ | ✗ | ✗ |
| PNG | ✗ | ✗ | ✗ |
| JPG | ✗ | ✗ | ✗ |
| DOCX | ✗ | ✗ | ✗ |

จากตารางที่ 3 พบว่าในกรณีปกปิดร่องรอยหลักฐานด้วยการ Overwrite โดยใช้ซอฟต์แวร์ปกปิดร่องรอยหลักฐาน 2 โปรแกรม คือ Eraser 6.2.0.2986 และ Sdelete 2.02 และ ซึ่งตั้งค่าให้แต่ละโปรแกรมทำการเขียนทับ จำนวน 1 ครั้ง ผลการทดลองพบว่าซอฟต์แวร์นิติวิทยาศาสตร์ ทั้ง 3 โปรแกรม ไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ สำหรับกรณี Overwrite แบบไม่ใช้ซอฟต์แวร์ โดยทำการลบข้อมูลหลักฐานดิจิทัลทั้งหมดแล้วบันทึกไฟล์ข้อมูลอื่นลงบนอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัลทีละไฟล์ ผลการกู้คืนข้อมูลหลักฐานดิจิทัลของซอฟต์แวร์นิติวิทยาศาสตร์ ทั้ง 3 โปรแกรม คือ ครั้งที่ 1 เมื่อบันทึกไฟล์ข้อมูลอื่นขนาด 324 MB สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ 6 ไฟล์ ครั้งที่ 2 บันทึกไฟล์ข้อมูลอื่นเพิ่มขนาด 281 MB สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ 5 ไฟล์ ครั้งที่ 3 บันทึกไฟล์ข้อมูลอื่นเพิ่มขนาด 336 MB ไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้

*อภิปรายผล*

ผลการวิจัยเรื่อง การศึกษาเปรียบเทียบการปกปิดร่องรอยหลักฐานดิจิทัล ที่ส่งผลต่อประสิทธิผลการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์ มีประเด็นที่สามารถนำมาอภิปรายผลได้ ดังนี้

1. วัตถุประสงค์การวิจัยข้อที่ 1 ที่ว่า “เพื่อศึกษาเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัล ที่ส่งผลต่อการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์” สามารถอธิบายได้จากเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลที่ใช้ในการวิจัยครั้งนี้ จำนวน 3 เทคนิค ประกอบด้วย

- การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete ผลการวิจัยพบว่าการลบไฟล์บนระบบไฟล์แบบ NTFS นั้น ระบบปฏิบัติการจะทำการเปลี่ยนค่าใน MFT Header ของ MFT Entry ให้เป็น “0” ซึ่งหมายถึงไฟล์ถูกลบจากค่าปกติคือ “1” ดังนั้น ข้อมูลไฟล์ที่ถูกลบจึงไม่ได้ถูกลบออกจากไดร์ฟหรืออุปกรณ์บันทึกข้อมูลจริง ๆ ด้วยเหตุผลดังกล่าวทำให้สามารถกู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete ในระบบไฟล์แบบ NTFS ภายใต้ระบบ ปฏิบัติการ Windows 7 กลับมาได้ในสภาพที่สมบูรณ์ซึ่งผลการวิจัยนี้สอดคล้องกับงานวิจัยของ Lin X (6) ที่พบว่าการลบไฟล์ในระบบไฟล์แบบ NTFS ถ้าหากข้อมูลเนื้อไฟล์ที่ ถูกลบยังไม่ถูกเขียนทับด้วยไฟล์ข้อมูลอื่น รายการดัชนีใน MFT Entry ยังสามารถใช้อ้างอิงไฟล์ที่ถูกลบได้ และทราบขนาดของคลัสเตอร์ ย่อมกู้คืนไฟล์ข้อมูลได้สำเร็จ โดยมีขั้นตอนในการกู้คืนไฟล์ข้อมูล 2 ขั้นตอน คือ ขั้นตอนที่ 1 ต้องกู้คืนข้อมูลในส่วนที่เป็นเนื้อหาของไฟล์ โดยทำการสแกนรายการใน MFT ทีละรายการเพื่อรวบรวมรายการของ Entry ที่ถูกทำเครื่องหมายแสดงว่าถูกลบ (Deletion Marker) ไว้ (ไบต์ที่ 22-23 ของ MFT

ISSN: 1686-8420 (Print), 2651-2289 (Online)

Entry คือ 0x0000) จากนั้นให้วิเคราะห์แอตทริบิวต์ $DATA เพื่อตรวจสอบสถานะในการจัดสรรคลัสเตอร์ หากสถานะเป็น 1 หมายความว่ากลุ่มข้อมูลเหล่านั้นถูกเขียนทับด้วยข้อมูลใหม่

- การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Format จากผลการทดลองพบว่าการใช้คำสั่ง Format แบบไม่ระบุคำสั่งย่อยเพื่อปกปิดร่องรอยหลักฐานดิจิทัล จำนวน 1 3 5 และ 7 ครั้ง ตามลำดับ สามารถค้นพบร่องรอยของข้อมูลดิจิทัลที่ถูกปกปิดร่องรอยหลักฐานด้วยคำสั่ง Format จึงกู้คืนข้อมูลหลักฐานดิจิทัลได้ โดยจำนวนครั้งของการใช้คำสั่ง Format ไม่มีผลต่อการกู้คืนข้อมูลแต่อย่างใด ซึ่งผลการวิจัยนี้สอดคล้องกับรายงานของ Blancco Technology Group (7) ที่พบว่าผลการสำรวจข้อมูลของเจ้าหน้าที่ฝ่ายไอทีมากกว่า 400 คน จากประเทศสหรัฐอเมริกา แคนาดา เม็กซิโก สหราชอาณาจักร เยอรมัน ฝรั่งเศส ญี่ปุ่น จีน และอินเดีย เกี่ยวกับแนวทางการทำลายข้อมูลจากไดร์ฟที่ไม่ได้ใช้งานแล้วมีเจ้าหน้าที่ไอทีร้อยละ 53 ซึ่งเกินกว่าครึ่งหนึ่งของผู้เชี่ยวชาญด้านไอทีจากทั่วโลก ลบข้อมูลคอมพิวเตอร์ แล็ปท็อป ไดร์ฟภายนอก และเซิร์ฟเวอร์ ด้วยวิธีที่สามารถ กู้คืนได้ง่าย โดยร้อยละ 31 ใช้วิธี Delete โดยลากไฟล์ไปที่ Recycle Bin และร้อยละ 22 ใช้วิธี Format ไดร์ฟทั้งหมด ซึ่งการลบข้อมูลทั้งสองวิธีสามารถกู้คืนข้อมูลได้ สำหรับกรณีใช้คำสั่ง Format ที่ระบุ Switch โดยมีรูปแบบคำสั่งเป็น Format drive: /P:1 เป็นการสั่งให้จัดรูปแบบของอุปกรณ์บันทึกข้อมูลที่เป็นหลักฐานดิจิทัล ให้มีระบบไฟล์ที่เหมาะกับระบบปฏิบัติการที่ใช้ พร้อมทั้งเขียน 0 ซึ่งเป็นตัวเลขแสดงสถานะว่าเป็นพื้นที่ว่าง ลงบนทุกตำแหน่งบนอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัล ซึ่งคำสั่ง Format drive: /P: 1 มีลักษณะเหมือนกันกับการปกปิดร่องรอยหลักฐานด้วยการ Overwrite ดังนั้น ถึงแม้จะเป็นการเขียนทับเพียงครั้งเดียวแต่ก็ทำให้ทุกตำแหน่งของข้อมูลเนื้อไฟล์เดิมที่ต้องการกู้คืนถูกแทนที่ด้วย 0 จึงไม่สามารถกู้คืนข้อมูลที่เป็นหลักฐานดิจิทัลได้ ซึ่งผลการวิจัยนี้สอดคล้องกับงานวิจัยของ Wright C, Kleiman D, Sundhar S (8) ที่พบว่าการเขียนทับเพียงครั้งเดียวก็เพียงพอแล้วที่จะลบข้อมูลเพื่อไม่ให้สามารถกู้คืนได้ และอธิบายเพิ่มเติมว่าบ่อยครั้งที่เกิดข้อโต้แย้งกันเกี่ยวกับจำนวนครั้งที่เหมาะสมในการเขียนข้อมูลทับ (Overwriting) ซึ่งขัดแย้งกับผลการวิจัยของ ปีเตอร์ กัทแมนน์ ที่พบว่าต้องทำการเขียนทับมากถึง 35 ครั้ง ข้อมูลจึงจะปลอดภัยจากการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาต โดยอธิบายว่าเมื่อเขียนข้อมูลใหม่ทับข้อมูลเดิมบนไดร์ฟแบบแม่เหล็ก ข้อมูลใหม่ที่เขียนไปยังไดร์ฟอาจไม่สามารถเขียนกลับไปยังตำแหน่งที่แน่นอนของข้อมูลต้นฉบับได้ โดยการเปลี่ยนบิตของข้อมูลเดิมจะไม่ได้เปลี่ยนจาก 0 เป็น 1 หรือจาก 1 เป็น 0 พอดี แต่จะมีส่วนที่เหลื่อมกัน เช่น เปลี่ยนจาก 1 เป็น 0.95 หรือ 1.05 เป็นต้น ดังนั้น ถ้าสามารถอ่านข้อมูลดิบที่อยู่บนไดร์ฟ แล้วนำไปวิเคราะห์รูปแบบ (Pattern) การเปลี่ยนค่าบิตของข้อมูลได้ จะทำให้ทราบว่าข้อมูลที่ถูกเขียนทับมีค่าเป็นอะไรมาก่อน โดยสามารถใช้กล้องจุลทรรศน์แรงแม่เหล็ก (MFM: Magnetic Force Microscope) ตรวจดูค่าการจัดเรียงของสนามแม่เหล็กบนพื้นผิวของไดร์ฟได้ แต่ในงานวิจัยไม่ได้ยืนยันว่าสามารถกู้คืนข้อมูลได้จริง เพียงแต่บอกว่ามีความเป็นไปได้เท่านั้น นอกจากนี้ Feenberg D (9) ยังได้ศึกษาเกี่ยวกับการอ่านข้อมูลที่เขียนทับของหน่วยงานข่าวกรอง โดยกล่าวว่างานวิจัยของกัทแมนน์ ถูกใช้อ้างอิงมาหลายสิบปีทำให้เกิดความเชื่อที่ว่าหน่วยงานข่าวกรองของสหรัฐอเมริกามีเครื่องมือที่สามารถกู้คืนข้อมูลที่ถูกเขียนทับได้ แต่จนถึงปัจจุบันก็ยังไม่มีข้อพิสูจน์หรือการยืนยันอย่างเป็นทางการว่าสามารถทำได้จริง ประกอบกับในปี 2003 กัทแมนน์ได้ออกมายอมรับว่าในส่วนที่เกี่ยวกับการเขียนข้อมูลทับ (Overwritten Sectors) บนไดร์ฟสมัยใหม่ (Modern Drives) ไม่สามารถอ่านค่าโดยใช้เทคนิคที่ระบุไว้ในงานวิจัยของเขาในปี 1996 ได้ แต่เขาไม่ได้ถอนการอ้างสิทธิ์ในงานวิจัยที่เกี่ยวกับไดร์ฟรุ่นเก่า ดังนั้น การกู้ข้อมูลที่ถูกเขียนทับไปแล้วด้วยการส่องดูสนามแม่เหล็กจึงไม่สามารถทำได้บนไดร์ฟสมัยใหม่

ISSN: 1686-8420 (Print), 2651-2289 (Online)

ในทางปฏิบัติหากต้องการทำลายข้อมูลเก่า การเขียนข้อมูลทับครั้งเดียวในตำแหน่งที่ถูกต้องก็ทำให้ไม่สามารถกู้คืนข้อมูลได้แล้ว

- การปกปิดร่องรอยหลักฐานด้วยการ Overwrite แบ่งเป็น 2 กรณี คือ ในกรณีใช้ซอฟต์แวร์ปกปิดร่องรอยหลักฐาน พบว่าการตั้งค่าให้ซอฟต์แวร์ให้เขียนข้อมูลทับ 1 ครั้ง ทำให้ไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ เนื่องจากเป็นเขียนข้อมูลทับทุกตำแหน่งบนอุปกรณ์บันทึกข้อมูลโดยมีการกำหนดรูปแบบ การเปลี่ยนค่าบิตของข้อมูลในการเขียนทับไว้หลายรูปแบบ ซึ่งผลการวิจัยนี้สอดคล้องกับงานวิจัยของ Yusof NA, Abdullah S, Senan MF, Abidin NZ, Sahri MB, Binti SN (10) ที่พบว่าการทำลายข้อมูลให้ไม่สามารถกู้คืนได้ (Data sanitization) ใช้วิธีการเขียนทับในการทำลายข้อมูล โดยกำหนดรูปแบบการเปลี่ยนค่าบิตของข้อมูล (Logical Data Bit Pattern) ในการเขียนทับไว้หลายรูปแบบ เพื่อให้แน่ใจว่าตำแหน่งของข้อมูลที่ต้องการทำลายทั้งหมดถูกแทนที่ด้วยรูปแบบบิตการเขียนทับข้อมูลที่เลือกใช้ โดยกล่าวว่าการลบ 35 ครั้งแบบกัทแมนน์ใช้เวลานานเกินไป นอกจากนี้ Kissel R, Regenscheid A, Scholl M, Stine K (11) ฝ่ายความปลอดภัยคอมพิวเตอร์ของ NIST ได้จัดทำคู่มือเป็นเอกสารเผยแพร่ NIST 800-88 (Guidelines for Media Sanitization) เพื่อยืนยันว่าการเขียนทับข้อมูลครั้งเดียวเพียงพอต่อการป้องกันข้อมูลที่ถูกลบจากการพยายามกู้คืนข้อมูลใด ๆ สำหรับกรณีการ Overwrite โดยการลบข้อมูลทั้งหมดแล้วเขียนข้อมูลอื่นทับทีละไฟล์ ผลการทดลองพบว่าเมื่อเขียนข้อมูลอื่นลงบนอุปกรณ์บันทึกข้อมูลจนเกือบเต็มความจุแล้วจะทำให้ไม่สามารถกู้คืนข้อมูลได้ เนื่องจากไฟล์ข้อมูลหลักฐานดิจิทัลถูกเขียนทับด้วยไฟล์อื่นทำให้เนื้อไฟล์เสียหาย จึงสรุปได้ว่าในระบบไฟล์แบบ NTFS เมื่อมีการ ลบไฟล์ข้อมูลแล้วสามารถกู้คืนได้ หากยังไม่มีการบันทึกไฟล์ข้อมูลอื่นทับในตำแหน่งของไฟล์ข้อมูลเดิม

2. จากวัตถุประสงค์ของการวิจัยในข้อที่ 2 ที่ว่า “เพื่อเปรียบเทียบเทคนิคการปกปิดร่อยรอยหลักฐานดิจิทัลแต่ละเทคนิคที่ส่งผลต่อประสิทธิผลในการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์” เนื่องจากเป็นงานวิจัยที่ต้องการสังเกตว่าการปกปิดร่องรอยหลักฐานดิจิทัลแต่ละเทคนิคส่งผลต่อการกู้คืนข้อมูลของซอฟต์แวร์นิติวิทยาศาสตร์อย่างไร หรือกล่าวอีกนัยหนึ่งก็คือต้องการทราบถึงผลการกู้คืนข้อมูลหลักฐานดิจิทัลที่ถูกปกปิดร่องรอยหลักฐานด้วยเทคนิคต่าง ๆ เท่านั้น จึงไม่ได้ พิจารณาในด้านประสิทธิภาพของซอฟต์แวร์ ได้แก่

- ด้านความคุ้มค่า เช่น เป็นซอฟต์แวร์ที่มีฟังก์ชันหลากหลายเมื่อเทียบกับราคา

- ด้านคุณภาพ เช่น เป็นซอฟต์แวร์ที่สามารถสแกนหาไฟล์ที่ถูกลบได้อย่างรวดเร็ว ไม่สิ้นเปลืองทรัพยากร (Resource) ของระบบ (ใช้พื้นที่ในการติดตั้งโปรแกรมน้อย ใช้หน่วยความจำน้อย)

- ด้านอื่น ๆ เช่น สร้างระบบป้องกันการเขียนทับข้อมูลแบบซอฟต์แวร์ หรือ Software Write Blocker ได้ วิเคราะห์ระบบอิมเมจไฟล์ได้ รองรับภาษาไทย เป็นต้น

ดังนั้น ประสิทธิผลในการกู้คืนข้อมูลหลักฐานดิจิทัลของซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรมจึงไม่แตกต่างกัน นั่นคือ ไฟล์ข้อมูลที่ยังไม่ถูกเขียนทับสามารถกู้คืนได้ ส่วนไฟล์ข้อมูลที่ถูกเขียนทับแล้วบางส่วนหรือถูกเขียนทับทั้งหมดไม่สามารถกู้คืนได้ แต่ในความเป็นจริงซอฟต์แวร์นิติวิทยาศาสตร์ยังมีช่องทางสำหรับให้ผู้ใช้งานที่มีความสามารถด้านการเขียนโปรแกรมทำการพัฒนาซอฟต์แวร์ได้ตามความต้องการ เช่น โปรแกรม EnCase รองรับการเขียนโปรแกรมสคริปต์ชื่อว่า EnScript ที่อนุญาตให้ผู้ใช้งานสร้างสคริปต์ด้วยการใช้ภาษา C++ หรือ JavaScript สำหรับใช้ในการตรวจสอบค้นหาไฟล์ที่ต้องการเฉพาะเจาะจงเป็นพิเศษ และมี API ซึ่งบรรจุชุดคำสั่งต่าง ๆ เอาไว้ภายในเพื่อให้ผู้เขียนโปรแกรมสามารถเรียกใช้งานได้ทันที โดยไม่จำเป็นต้องเขียนโปรแกรมในส่วนนั้น ๆ เองทั้งหมด หรือหากใช้ซอฟต์แวร์

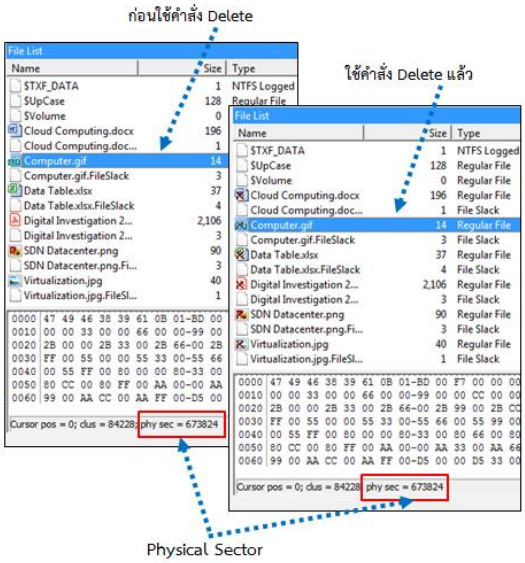
ISSN: 1686-8420 (Print), 2651-2289 (Online)

นิติวิทยาศาสตร์ประเภท Commercial Ware จะทำให้กู้คืนข้อมูลเนื้อไฟล์ที่ยังไม่ถูกเขียนทับหรือมีร่องรอยให้กู้คืนได้บางส่วนโดยคิดเป็นร้อยละจากขนาดไฟล์ข้อมูลที่กู้คืนได้ เช่น กู้คืนได้ 35% 50% หรือ 75% เป็นต้น ซึ่งสอดคล้องกับงานวิจัยของ ศุภชัย หวั่นแสง (12) ที่อธิบายไว้ว่าซอฟต์แวร์กู้คืนข้อมูลที่ใช้สำหรับพิสูจน์หลักฐานดิจิทัล (Digital Forensic) เปิดช่องให้ผู้ใช้งานปรับปรุงการใช้งานเพิ่มเติมหรือที่เรียกว่า Plugin ได้โดยจะต้องทำการเขียนโปรแกรมเพิ่มเติมเอง ซึ่งจะสะดวกกว่าการเขียนโปรแกรมตั้งแต่แรก เนื่องจากจะมี Application Programming Interface (API) โดยในส่วนนี้ผู้ที่ใช้งานจำเป็นจะต้องเข้าใจทั้งในส่วนของ API และกระบวนการทำงานของระบบจัดการไฟล์เพื่อให้สามารถกู้คืนข้อมูลได้อย่างถูกต้อง

## สรุปผล

จากผลการศึกษาพบว่าการปกปิดร่องรอยหลักฐานแต่ละเทคนิคส่งผลต่อประสิทธิผลในการกู้คืนข้อมูลหลักฐานดิจิทัล ดังนี้

1. การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete สามารถกู้ข้อมูลคืนได้ในสภาพที่สมบูรณ์ 100% และตำแหน่งของข้อมูล (Physical Sector) ในหลักฐานดิจิทัลที่ถูก Delete ไม่มีการเปลี่ยนตำแหน่ง เนื่องจากระบบไฟล์แบบ NTFS ภายใต้ระบบปฏิบัติการ Windows 7 จะสร้าง Master File Table (MFT) ขึ้นมาโดยอัตโนมัติ MFT เป็นส่วนที่ใช้เก็บข้อมูลรายละเอียดของไฟล์และไดเร็กทอรี่ทั้งหมด โดยมีการเก็บข้อมูลเป็น Entry หรือที่เรียกว่า MFT Entry ข้อมูลรายละเอียดของ MFT Entry ถูกเรียกว่าเมทาดาต้า (Metadata) เก็บไว้ในไฟล์ $MFT ส่วนข้อมูลเนื้อไฟล์เก็บใน $DATA การลบไฟล์บนระบบไฟล์แบบ NTFS นั้น Huang W, Meisheng Y (13) อธิบายว่าระบบ ปฏิบัติการจะทำการเปลี่ยน Flag ในตำแหน่งไบต์ที่ 16 ใน MFT Header ของ MFT Entry ให้เป็น “0” ซึ่งหมายถึงไฟล์ถูกลบจากค่าปกติคือ “1” ข้อมูลไฟล์ที่ถูกลบจึงไม่ได้ถูกลบออกจากไดร์ฟหรืออุปกรณ์บันทึกข้อมูลจริง ๆ ทำให้สามารถกู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยคำสั่ง Delete กลับมาได้ในสภาพที่สมบูรณ์ 100% Physical Sector หรือตำแหน่งของข้อมูล ก่อนใช้คำสั่ง Delete และหลังจากใช้คำสั่ง Delete คือตำแหน่งเดิมไม่มีการเปลี่ยนแปลง แสดงดังรูปที่ 5



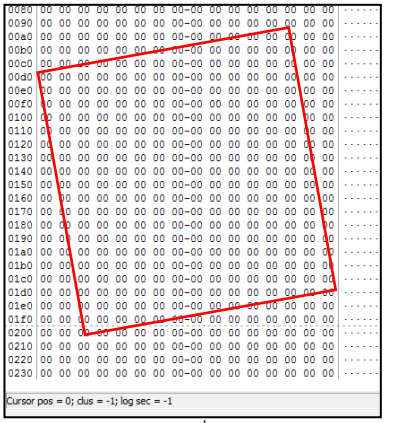

**รูปที่ 5** ตำแหน่งของข้อมูลบนหลักฐานดิจิทัล

2. การปกปิดร่องรอยหลักฐานด้วยคำสั่ง Format แบ่งออกเป็น 2 กรณี คือ กรณีใช้คำสั่ง Format แบบไม่ระบุคำสั่งย่อย (Switch) เมื่อทำการ Format จำนวน 1 3 5 และ 7 ครั้ง ตามลำดับ พบว่าสามารถพบร่องรอยของข้อมูล โดยสามารถกู้คืนข้อมูลจากการใช้คำสั่ง Format ได้จริง และจำนวนครั้งในการ Format ไม่มีผลต่อการกู้คืนข้อมูลแต่อย่างใด สำหรับกรณีใช้คำสั่ง Format แบบระบุ Switch โดยกำหนดรูปแบบคำสั่งเป็น Format drive: /P:1 (1 คือจำนวนครั้งในการ Format) พบว่าไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ จากผลการทดลองดังกล่าวอธิบายได้ว่าการใช้คำสั่ง Format โดยไม่ระบุคำสั่งย่อยสามารถกู้คืนข้อมูลดิจิทัลได้โดยมีชื่อแตกต่างจากไฟล์ข้อมูลต้นฉบับเนื่องจากทุกครั้งที่ใช้คำสั่ง Format จะมีการสร้างไฟล์ $MFT ใหม่ ไปแทนไฟล์ $MFT เดิม ทำให้ข้อมูลภายใน $MFT เดิมถูกทำลาย ไฟล์ข้อมูลหลักฐานดิจิทัลที่กู้คืนได้จึงมีชื่อแตกต่างกันตาม

ISSN: 1686-8420 (Print), 2651-2289 (Online)

ซอฟต์แวร์นิติวิทยาศาสตร์ที่ใช้ในการกู้คืนข้อมูล ซึ่งสอดคล้องกับงานวิจัยของ ศุภชัย หวั่นแสง (12) เกี่ยวกับการกู้คืนข้อมูลจากซอฟต์แวร์คงสภาพฮาร์ดดิสก์ ซึ่งจากผลการวิจัยพบว่าการกู้คืนข้อมูลที่หลงเหลือจากซอฟต์แวร์คงสภาพฮาร์ดิสก์ เมื่อกู้คืนข้อมูลได้ทั้งในส่วนของข้อมูล MFT Entry และข้อมูลเนื้อไฟล์จะทำให้สามารถนำมาหาความสัมพันธ์ระหว่างข้อมูล MFT Entry และข้อมูลเนื้อไฟล์ด้วยขนาดและชนิดของไฟล์ ดังนั้น จึงทำให้สามารถทราบได้ว่าเนื้อไฟล์ที่กู้คืนมาได้นั้นมีชื่อไฟล์และรายละเอียดที่เกี่ยวข้องกับไฟล์หรือไม่

สำหรับกรณีการใช้คำสั่ง Format drive: /P:1 เป็นการสั่งให้จัดรูปแบบของอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัลให้มีระบบไฟล์ที่เหมาะกับระบบปฏิบัติการที่ใช้พร้อมทั้งเขียน 0 ซึ่งเป็นตัวเลขแสดงสถานะว่าเป็นพื้นที่ว่างลงบนทุกตำแหน่งของอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัล จำนวน 1 ครั้ง ทำให้ตำแหน่งของข้อมูลเนื้อไฟล์เดิมที่ต้องการกู้คืน ถูกแทนที่ด้วย 0 จึงไม่สามารถกู้คืนข้อมูลที่เป็นหลักฐานดิจิทัลได้แม้จะถูกเขียน 0 ทับเพียง 1 ครั้ง แต่เป็นการเขียนทับทุกตำแหน่งบนอุปกรณ์บันทึกข้อมูล ซึ่งสามารถสังเกตได้จากผลการวิเคราะห์ข้อมูลด้วยซอฟต์แวร์นิติวิทยาศาสตร์ที่แสดงผลในรูปแบบของค่า Hex (เลขฐานสิบหก) เมื่อใช้คำสั่ง Format drive: /P:1 จะมีชุดตัวเลข 0 ต่อเนื่องกัน จึงเป็นหลักฐานสำคัญที่ทำให้ทราบว่าอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัลถูกล้างข้อมูลด้วยซอฟต์แวร์หรือคำสั่งล้างข้อมูล สอดคล้องกับที่ แดนเนียล แอลอี (14) อธิบายไว้ และสุนีย์ สกาวรัตน์ ได้นำมาแปลลงในหนังสือการตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย: เข้าใจพยานหลักฐานดิจิทัลจากขั้นตอนหมายถึงห้องพิจารณาคดี ว่าซอฟต์แวร์ลบล้างข้อมูลถูกใช้ในการทำลายข้อมูลเพื่อที่จะทำให้ไม่สามารถกู้คืนได้โดยวิธีการตรวจพิสูจน์พยานหลักฐาน ซึ่งสามารถทำได้โดยการเขียนทับเซกเตอร์ ด้วยเลขหนึ่งหรือเลขศูนย์หรือข้อมูลแบบสุ่ม หากสังเกตเห็นชุดตัวเลขศูนย์ต่อเนื่องแล้วสำหรับผู้พิสูจน์พยานหลักฐาน ย่อมถือได้ว่าเป็นหลักฐานที่ชัดเจนว่าไดรฟ์ได้รับการลบข้อมูลด้วยวอฟต์แวร์ล้างดิสก์ หลักฐานแสดงการล้างข้อมูลในอุปกรณ์บันทึกข้อมูลด้วยคำสั่ง Format drive: /P:1 แสดงดังรูปที่ 6



**รูปที่ 6** การล้างข้อมูลด้วยคำสั่ง Format

3. การปกปิดร่องรอยหลักฐานด้วยการ Overwrite จากผลการทดลองพบว่าข้อมูลดิจิทัลที่ถูกปกปิดร่องรอยหลักฐานด้วยการ Overwrite เป็นการลบข้อมูลแบบถาวร และไม่สามารถกู้คืนข้อมูลซึ่งเป็นหลักฐานดิจิทัลได้ โดยแบ่งออกเป็น 2 กรณี คือ กรณีใช้ซอฟต์แวร์ที่มีความสามารถในการ Overwrite เป็นเครื่องมือในการปกปิดร่องรอยหลักฐาน จำนวน 2 โปรแกรม คือ Sdelete 2.02 และ Eraser 6.2.0.2986 พบว่าซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม ไม่สามารถกู้คืนข้อมูลที่ถูกปกปิดร่องรอยหลักฐานด้วยการ Overwrite จำนวน 1 รอบได้ เนื่องจากการปกปิดร่องรอยหลักฐานด้วยการ Overwrite ใช้วิธีการเขียนข้อมูลอื่น ๆ ทับลงไปบนตำแหน่งของข้อมูลเดิมเพื่อป้องกันไม่ให้สามารถนำข้อมูลเดิมกลับไปใช้ได้อีก ทำให้ข้อมูลในส่วนของ MFT และข้อมูลเนื้อไฟล์ถูกทำลาย

กรณี Overwrite ด้วยวิธีลบข้อมูลหลักฐานดิจิทัลทั้งหมดแล้วเขียนข้อมูลอื่นทับลงไปทีละไฟล์จนเกือบเต็มความจุของอุปกรณ์บันทึกข้อมูลที่ใช้เป็นหลักฐานดิจิทัล โดยมีขั้นตอนการทดลองคือ นำ USB Flash drive ขนาดความจุ 1 GB ซึ่งใช้เป็นหลักฐานดิจิทัลไปลบข้อมูลทั้งหมด แล้วบันทึกไฟล์ข้อมูลอื่นลงไปทีละไฟล์ จำนวน 3 ครั้ง คือ

ISSN: 1686-8420 (Print), 2651-2289 (Online)

- ครั้งที่ 1 NewFile_1.mp4 ขนาด 324 MB
- ครั้งที่ 2 NewFile_2.mp4 ขนาด 281 MB
- ครั้งที่ 3 NewFile_3.mp4 ขนาด 336 MB

พบว่าเมื่อทำการบันทึกไฟล์อื่นลงบนอุปกรณ์บันทึกข้อมูลที่เป็นหลักฐานดิจิทัลครั้งที่ 1 แล้วนำไปกู้คืนข้อมูลด้วยซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ 6 ไฟล์ เมื่อบันทึกไฟล์อื่นเพิ่มลงไปในอุปกรณ์บันทึกข้อมูลที่เป็นหลักฐานดิจิทัลครั้งที่ 2 แล้วนำไปกู้คืนด้วยซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ 5 ไฟล์ และเมื่อบันทึกไฟล์อื่นเพิ่มลงบนอุปกรณ์บันทึกข้อมูลที่เป็นหลักฐานดิจิทัลครั้งที่ 3 แล้วนำไปกู้คืนด้วยซอฟต์แวร์นิติวิทยาศาสตร์ทั้ง 3 โปรแกรม พบว่าไม่สามารถกู้คืนข้อมูลหลักฐานดิจิทัลได้ เนื่องจากในแต่ละครั้งที่เขียนไฟล์ทับลงไปในอุปกรณ์บันทึกข้อมูล ตำแหน่งของไฟล์ใหม่ไปทับตำแหน่งของไฟล์ข้อมูลหลักฐานดิจิทัลที่ต้องการกู้คืน ทำให้เนื้อไฟล์ข้อมูลหลักฐานดิจิทัลเกิดความเสียหาย จนไม่สามารถกู้คืนได้

จากการวิจัยครั้งนี้จึงสรุปได้ว่าเทคนิคการปกปิดร่องรอยหลักฐานดิจิทัลบนอุปกรณ์บันทึกข้อมูลที่มีระบบไฟล์แบบ NTFS ภายใต้ระบบปฏิบัติการ Windows 7 การกู้คืนข้อมูลหลักฐานดิจิทัลจะสำเร็จหรือไม่นั้นขึ้นอยู่กับว่าเทคนิคนั้นทำให้เนื้อไฟล์เสียหายหรือไม่ หากเป็นเทคนิคที่แก้ไขเฉพาะในส่วนของเมทาดาต้า โดยไม่ทำให้เนื้อไฟล์เสียหายการกู้คืนข้อมูลหลักฐานดิจิทัลย่อมประสบผลสำเร็จ แต่ถ้าหากทำให้เนื้อไฟล์เกิดความเสียหายย่อมไม่สามารถกู้คืนข้อมูลดิจิทัลนั้นได้

## กิตติกรรมประกาศ

ขอขอบคุณคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจที่สนับสนุนสถานที่ในการวิจัย และขอขอบคุณกรมสรรพสามิตที่สนับสนุนทุนการศึกษา

## เอกสารอ้างอิง

1. Microsoft Docs. How NTFS Works [Internet]. Redmond, WA: Microsoft Corporation; 2009 [cited 2019 Sep 17]. Available from: https://bit.ly/2RmmbBz
2. Carrier B. File System Forensic Analysis. New Jersey: Addison-Wesley Professional; 2005.
3. Painter Z. Silicon Power Blog [Internet]. Taipei: Silicon Power. 2018 [cited 2020 April 15]. Available from: https://bit.ly/3jhEP9c
4. Shimpi AL. The SSD Anthology: Understanding SSDs and New Drive from OCZ [Internet]. 2009 [cited 2020 April 3]. Available from: https://www.anandtech.com/Show/Index/2738?cPage=4&all=False&sort=0&page=5
5. NetMarketShare.com [Internet]. Newport Beach, CA: Net Applications; 2017. [updated 2019 Feb 28; cited 2019 Mar 1]. Available from: https://netmarketshare.com/
6. Lin X. Introductory Computer Forensics: A hands-on Practical Approach. Basel: Springer Nature Switzerland AG; 2018.
7. Blancco Technology Group. Improper Data Removal & Poor Enforcement of Data Retention Policies Create the ‘Perfect Storm’ for Data Breaches [Internet]. Austin, TX: Blancco; 2016 [cited 2018 Mar 1]. Available from: https://bit.ly/3bUe5JT
8. Wright C, Kleiman D, Sundhar S. Overwriting Hard Drive Data: The Great Wiping Controversy. ICISS. 2008;4:243-57.

*ISSN: 1686-8420 (Print), 2651-2289 (Online)*

9. Feenberg D. Can Intelligence Agencies Read Overwritten Data? [Internet]. Cambridge, MA: National Bureau of Economic Research; 2013 [cited 2020 April 15]. Available from: https://www.nber.org/sys-admin/overwritten-data-gutmann.html

10. Yusof NA, Abdullah S, Senan MF, Abidin NZ, Sahri MB, Binti SN. Data Sanitization Framework for Computer Hard Disk Drive: A Case Study in Malaysia. IJACSA. 2019;10:398-406.

11. Kissel R, Regenscheid A, Scholl M, Stine K. Guidelines for Media Sanitization [Internet]. Maryland: National Institute of Standards and Technology; 2014 [cited 2020 April 15]. Available from: http://dx.doi.org/10.6028/NIST.SP.800-88r1/.

12. ศุภชัย หวั่นแสง. การกู้คืนข้อมูลจากซอฟต์แวร์คงสภาพฮาร์ดดิสก์ [วิทยานิพนธ์มหาบัณฑิต]. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีมหานคร; 2557.

13. Huang W, Meisheng Y. The Quickly Solving Method of File Recovery in Windows Environment. CSSE. 2008;3:859-62.

14. แดนเนียล แอลอี. การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย: เข้าใจพยานหลักฐานดิจิทัลจากขั้นตอนหมาย ถึงห้องพิจารณาคดี. กรุงเทพฯ: ซีเอ็ดยูเคชั่น; 2559.