การเปรียบเทียบการเปิดและปิดการใช้งานคำสั่งทริมบนโซลิดสเตตไดรฟ์
The Comparison of Enable and Disable Usage of TRIM Command on Solid State Drive

ณรงค์ฤทธิ์ คำแสนราช และ วรธัช วิชชุวาณิชย์
คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

Narongrid Kamsaenrat and Woratouch Witchuvanit
Faculty of Forensic Science, Royal Police Cadet Academy

Received December 31, 2022 | Revised June 14, 2023 | Accepted June 19, 2023

บทความวิจัย (Research Article)

บทคัดย่อ

งานวิจัยมีวัตถุประสงค์เพื่อเปรียบเทียบโปรแกรมตรวจพิสูจน์พยานหลักฐานทางดิจิทัลระหว่างการเปิด และปิดการใช้งานคำสั่งทริม (TRIM) ในโปรแกรมเอ็นเคส (Encase) และโปรแกรมแอคเซียม (AXIOM) และเปรียบเทียบประเภทของแฟ้มข้อมูลระหว่างเรสซิเดนซ์และนอนเรซิเดนซ์ ในกรณีเปิดและปิดการใช้งานคำสั่งทริมในงานวิจัยนี้ใช้แฟ้มข้อมูลสำหรับการทดลองจำนวน 4 ประเภท คือ แฟ้มข้อมูลข้อความ (.txt) ประเภทเรซิเดนต์ (Resident) และ นอนเรซิเดนต์ (Non-resident) แฟ้มข้อมูลภาพ (.png) ประเภทเรซิเดนต์ และนอนเรซิเดนต์ จำนวน 1,000 รายการ โดยผู้วิจัยได้กู้คืนข้อมูล ทั้งก่อนและหลังการเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ด้วยโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียม ผลการศึกษาพบว่าในกรณีระบบที่มีการเปิดใช้งานคำสั่งทริม ทั้งโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียม สามารถกู้คืนแฟ้มข้อมูลประเภทเรซิเดนต์ ได้ทั้งหมด แต่ไม่สามารถกู้คืนแฟ้มข้อมูลประเภทนอนเรซิเดนต์ได้ ในระบบที่มีการปิดใช้งานคำสั่งทริม ทั้งโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียม สามารถกู้คืนแฟ้มข้อมูลประเภทเรซิเดนต์ได้ทั้งหมด แต่กู้คืนแฟ้มข้อมูลประเภทนอนเรซิเดนต์ได้บางส่วน และการเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ส่งผลให้สามารถกู้คืนข้อมูลได้น้อยลง

คำสำคัญ: โซลิตสเตทไดรฟ์, คำสั่งทริม, โปรแกรมตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

Abstract

The purposes of this study were: 1) to compare digital forensics programs between enabled and disabled TRIM command in Encase and AXIOM and 2) to compare types of data between a resident and a non-resident in the case of enabled and disabled TRIM command. Four sample types of data files were used, including a resident txt file, a non-a resident txt file, a resident png file, and a non-resident png file with 1,000 sample files on a solid state drive. We recovered the data before and after rebooting the computer with

Encase and AXIOM and to compare the experimental results between enabling the TRIM command and disabling the TRIM command. The results revealed that in the system with the enabled TRIM command, Both Encase and AXIOM could recover all the resident files while non-resident files could not be recovered. On the other hand, in the systems with disabled TRIM commands, both Encase and AXIOM could recover resident files, but partially recovering non-resident data files by Encase and AXIOM provided the same results and rebooting your computer results in less data recovery.

Keywords: Solid State Drive, TRIM Command, Digital Forensics Software

บทนำ

ในปัจจุบัน มีการใช้งานอินเทอร์เน็ต และคอมพิวเตอร์อย่างแพร่หลายในสังคม จากการสำรวจของสำนักงานสถิติแห่งชาติพบว่าปี พ.ศ. 2559 ถึง 2563 การใช้งานอินเตอร์เน็ต และคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มขึ้นตลอด 5 ปีที่ผ่านมา อย่างไรก็ตามการใช้งานเครื่องคอมพิวเตอร์นั้นมีแนวโน้มลดลง แม้จะเพิ่มขึ้นเล็กน้อยในปี พ.ศ. 2563 โดยมีจำนวนผู้ใช้งานคอมพิวเตอร์ จำนวน 16 ล้านคน หรือคิดเป็นร้อยละ 26.4 ของประชากรที่มีอายุ 6 ปีขึ้นไป ถึงแม้ว่าแนวโน้มการใช้คอมพิวเตอร์จะลดลง แต่ก็นับว่าเป็นปริมาณที่สูงในระดับหนึ่งในสี่ของประชากรทั้งประเทศ โดยวัตถุประสงค์การใช้เครื่องคอมพิวเตอร์มักจะใช้เพื่อตอบสนองความต้องการของตนเอง เช่น การทำงานด้านเอกสาร ดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น

นอกจากนั้นการใช้งานคอมพิวเตอร์อาจจะไม่ได้มีวัตถุประสงค์เพื่อความบันเทิงเพียงเท่านั้นจากการรายงานของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติในช่วงเวลา 1 มีนาคม 2565 ถึง 18 มีนาคม 2566 พบว่ามีการแจ้งความผ่านระบบดังกล่าว จำนวน 246,135 เรื่อง โดยเป็นคดีออนไลน์ที่เกี่ยวข้องกับการใช้งานอินเตอร์ และคอมพิวเตอร์เพื่อกระทำความผิด จำนวน 222,485 เรื่อง ส่วนใหญ่แล้วคดีออนไลน์นั้นมักใช้อุปกรณ์คอมพิวเตอร์ในการกระทำความผิด ซึ่งข้อมูลพยานหลักฐานหรือร่องรอยการกระทำความผิดนั้นถูกอยู่ในหน่วยความจำของอุปกรณ์นั้น และคอมพิวเตอร์จะใช้หน่วยเก็บข้อมูลที่เรียกว่า ฮาร์ดดิสก์ไดรฟ์ (Hard Disk Drive)

ฮาร์ดดิสก์ไดรฟ์ เป็นหน่วยเก็บข้อมูลดิจิทัลที่ถูกสร้างขึ้นในยุคแรกของบริษัทไอบีเอ็ม โดยเรย์โนล์ด จอห์นสัน ในปี 1956 ในการเขียนข้อมูลฮาร์ดดิสก์ไดรฟ์ จะใช้หัวอ่านเขียนที่เป็นแม่เหล็กขนาดเล็ก ไปเหนี่ยวนำให้แผ่นที่เคลือบด้วยสารแม่เหล็กเกิดขั้วแม่เหล็กขึ้น ซึ่งมีสองทิศทางแทนการเก็บข้อมูลในรูปดิจิทัล คือ 0 และ 1 โดยการทำงานของฮาร์ดดิสก์ไดรฟ์ นั้นใช้ขั้วแม่เหล็กในการบันทึกข้อมูล และมีชิ้นส่วนที่มีการเคลื่อนไหวตลอดการบันทึกข้อมูล ส่งผลให้ฮาร์ดดิสก์ ไม่ทนต่อสนามแม่เหล็ก และไม่ทนต่อแรงกระแทก อีกทั้งยังมีความเร็วในการอ่านหรือเขียนข้อมูลที่ไม่สูงมากนัก (Marupudi, 2017) นั่นจึงเป็นที่มาของการคิดค้นโซลิดสเตตไดรฟ์ (Solid State Drive) ขึ้น

โซลิดสเตตไดรฟ์ เป็นอุปกรณ์จัดเก็บข้อมูลชนิดหนึ่ง ซึ่งใช้วงจรรวมเป็นหน่วยความจำเพื่อใช้เก็บข้อมูลแบบถาวรเช่นเดียวกับฮาร์ดดิสก์ไดรฟ์ ซึ่งภายในโซลิดสเตตไดรฟ์ มีเพียงวงจรอิเล็กทรอนิกส์ และอุปกรณ์ที่อยู่ภายในไม่มีการเคลื่อนไหว ส่งผลให้การกระแทกหรือการตกหล่นของโซลิดสเตตไดรฟ์ นั้นมีความเสียหายน้อยกว่าฮาร์ดดิสก์ไดรฟ์ และส่งผลให้โซลิดสเตตไดรฟ์ ใช้พลังงานน้อยกว่า รวมถึงใช้เวลาในการเข้าถึงข้อมูล (Access Time) และเวลาในการหน่วงข้อมูล (Latency) น้อยกว่าฮาร์ดดิสก์ไดร์ฟ

(Vieyra, 2018) ราคาของโซลิดสเตตไดรฟ์ ค่อนข้างสูงกว่าฮาร์ดดิสก์ไดรฟ์ แต่เนื่องจากอุปกรณ์ดังกล่าวมีประสิทธิภาพที่สูงกว่า จึงส่งผลให้ผู้ใช้งานคอมพิวเตอร์นิยมเลือกใช้มากกว่า (Kasavajhala, 2011) ด้วยเหตุดังกล่าวผู้ตรวจพิสูจน์จึงเกิดปัญหาในการวิเคราะห์วัตถุพยานเนื่องจากส่วนควบคุมการทำงานของโซลิดสเตตไดรฟ์ จะมีการลบข้อมูลที่ไม่ได้ใช้แล้วอยู่เบื้องหลังตลอดเวลาเรียกว่า คำสั่งทริม ส่งผลให้การกู้ข้อมูลในโซลิดสเตตไดรฟ์ยากขึ้น และเป็นอุปสรรคสำคัญในการตรวจพิสูจน์ (Marupudi, 2017)

โปรแกรมที่ใช้ในงานวิจัยนี้ คือ โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และ โปรแกรมแอคเซียม รุ่น 5.1.0.24999 โปรแกรมดังกล่าวได้รับความนิยมในหน่วยงานบังคับใช้กฎหมาย ซึ่งหน่วยงานในประเทศไทยที่ใช้โปรแกรมนี้คือ สำนักงานพิสูจน์หลักฐานตำรวจที่เป็นหน่วยงานที่ให้บริการในการตรวจพิสูจน์หลักฐานให้กับตำรวจทั่วประเทศ ผู้วิจัยจึงเลือกโปรแกรมทั้งสองมาทำการทดสอบ

ดังนั้นในงานวิจัยนี้จะทดสอบการตรวจพิสูจน์โซลิดสเตตไดรฟ์ โดยการเปิดคำสั่งทริม และปิดคำสั่งทริม โดยใช้โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และ โปรแกรมแอคเซียม รุ่น 5.1.0.24999 เพื่อหาความแตกต่างของผลการตรวจพิสูจน์ในกรณีที่เปิด และปิดคำสั่งทริม บนโซลิดสเตตไดรฟ์

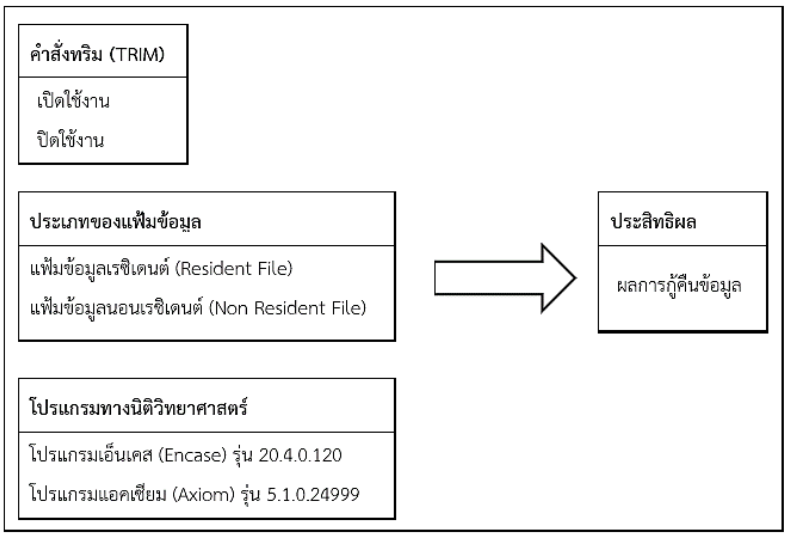
วัตถุประสงค์

1) เพื่อเปรียบเทียบโปรแกรมตรวจพิสูจน์พยานหลักฐานทางดิจิทัลระหว่างการเปิด และปิดการใช้งานคำสั่งทริมในโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียม

2) เพื่อเปรียบเทียบประเภทของแฟ้มข้อมูลระหว่างเรสซิเดนซ์และนอนเรซิเดนซ์ ที่ส่งผลต่อประสิทธิผลในการกู้คืนข้อมูล ในกรณีเปิดและปิดการใช้งานคำสั่งทริมในโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียม

กรอบแนวคิดการวิจัย

จากกรอบแนวคิดที่ได้จากการทบทวน แนวคิดและทฤษฎีที่เกี่ยวข้อง ผู้วิจัยได้ตั้งสมมติฐานการวิจัย คือ ผลการกู้คืนข้อมูลขึ้นอยู่กับคำสั่งทริม ประเภทของแฟ้มข้อมูล และโปรแกรมทางนิติวิทยาศาสตร์ ดังแสดงตามภาพที่ 1



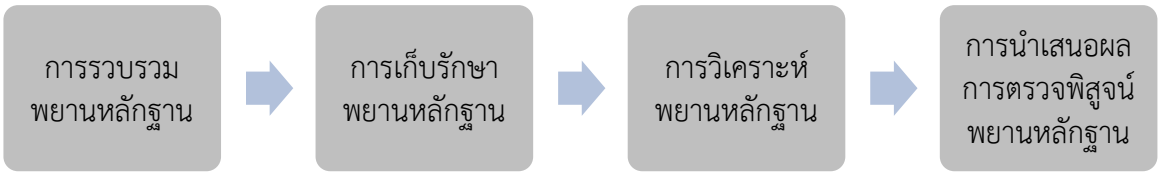
ภาพที่ 1 กรอบแนวคิดการวิจัย

ทบทวนวรรณกรรม

1) ทฤษฎีที่เกี่ยวข้อง

1.1 การตรวจพิสูจน์พยานหลักฐานดิจิทัล

การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล คือ การนำหลักฐานนิติวิทยาศาสตร์มาประยุกต์ใช้กับพยานหลักฐานอิเล็กทรอนิกส์ ในประเด็นข้อทางกฎหมาย ซึ่งพยานหลักฐานทางดิจิทัลนั้นมีหลักการพื้นฐานสำหรับการตรวจพิสูจน์ 4 ด้าน คือ การรวบรวมพยานหลักฐาน (Acquisition) การเก็บรักษาพยานหลักฐาน (Preservation) การวิเคราะห์พยานหลักฐาน (Analysis) และการนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน (Presentation) (Daniel & Daniel, 2019) ดังภาพที่ 2



ภาพที่ 2 หลักการพื้นฐานสำหรับการตรวจพิสูจน์

1.1.1 การรวบรวมพยานหลักฐาน

การรวบรวมพยานหลักฐาน คือ กระบวนการรวบรวมข้อมูลอิเล็กทรอนิกส์ที่เกิดขึ้นจริง เช่น การยึดเครื่องคอมพิวเตอร์จากสถานที่เกิดเหตุ การเข้าครอบครองเครื่องคอมพิวเตอร์ของคนร้าย หรือการทำสำเนาข้อมูลดิจิทัลจากฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ โดยการทำสำเนาต้องจัดทำให้เหมือนกับต้นฉบับทุกประการเพื่อป้องการการเปลี่ยนแปลงวัตถุพยาน ดังนั้นการรวบรวมพยานหลักฐานเป็นการเริ่มต้นของกระบวนการตรวจพิสูจน์พยานหลักฐานที่สำคัญมาก เนื่องจากเป็นสิ่งที่สร้างความเชื่อมั่นในเรื่องความสมบูรณของพยานหลักฐานทางดิจิทัล (Daniel & Daniel, 2019) โดย Srisuwan & Jitsawang (2021) ให้ความหมายของ การรวบรวมพยานหลักฐานดิจิทัล (Acquisition) เช่นเดียวกันว่าความสมบูรณ์ของพยานหลักฐานเป็นสิ่งที่สำคัญที่สุด โดยจะต้องการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใด ๆ

1.1.2 การเก็บรักษาพยานหลักฐาน

หลังจากที่เก็บรวบรวมพยานหลักฐานแล้วต้องมีการเก็บรักษาหลักฐานดังกล่าวไว้ในสถานที่ที่เหมาะสมเพื่อเก็บรักษากระบวนการห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) ซึ่งจะต้องรักษาพยานหลักฐานให้ปลอดภัยจากการทำให้เสียหาย โดยผู้ไม่ประสงค์ดี หรือ การเปลี่ยนแปลงหลักฐานโดยไม่ตั้งใจของบุคคลอื่นที่ไม่มีความเชี่ยวชาญ และ มีการจดบันทึกซึ่งเป็นวิธีที่ดีที่สุดของการเก็บรักษาวัตถุพยาน โดยผู้ตรวจพิสูจน์จะต้องจดบันทึกทุกครั้ง เมื่อวัตถุพยานมีการเปลี่ยนมือไปยังบุคคลอื่นเพื่อให้ห่วงโซ่วัตถุพยานนี้ ไม่ขาดตอนไม่วากรณีใด ๆ ทั้งสิ้น (Daniel & Daniel, 2019) ซึ่ง Srisuwan และ Jitsawang (2021) ได้กล่าวในกรณีนี้เช่นเดียวกัน โดยการเก็บรักษาวัตถุพยานจะต้องเก็บรักษาไว้ในสภาพที่น่าเชื่อถือได้ในชั้นศาล และเป็นไปตามกระบวนการห่วงโซ่คุ้มครองพยานหลักฐานตามมาตรฐานสากลพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของกระบวนการยุติธรรมต้องมีการบันทึกขั้นตอนการคุ้มครองพยานหลักฐาน และ วิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากสถานที่เกิดเหตุ

1.1.3 การวิเคราะห์พยานหลักฐาน

การวิเคราะห์เป็นกระบวนการค้นหา และเก็บรวบรวมวัตถุพยานที่ได้จากหลักฐานทั้งหมด หลังจากการรวบรวมไว้ ซึ่งแต่ละคดีจะมีลักษณะเฉพาะที่แตกต่างกัน เช่น คดีภาพลามกอนาจารเด็ก เป้าหมายของการตรวจสอบภาพ และภาพยนตร์ผิดกฎหมาย เป็นต้น การวิเคราะห์เป็นการดำเนินการที่ใช้ทักษะเฉพาะตัวของผู้ตรวจพิสูจน์ ซึ่งมีความแตกต่างทั้งเครื่องมือ และการฝึกอบรมของผู้ตรวจพิสูจน์ ทักษะดังกล่าวส่งผลต่อการวิเคราะห์ เพราะพยานหลักฐานอิเล็กทรอนิกส์ที่ได้รับมีหลายรูปแบบ และมาจากสถานที่ที่แตกต่างกัน ดังนั้นการฝึกอบรมและประสบการณ์ของผู้ตรวจพิสูจน์จึงเริ่มมีบทบาทต่อผลลัพธ์ของการตรวจพิสูจน์ (Daniel & Daniel, 2019) ซึ่ง Srisuwan & Jitsawang (2021) ได้กล่าวไว้เช่นเดียวกันกล่าวคือพยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะผู้ตรวจพิสูจน์ที่แตกต่างกัน ดังนั้นการฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญต่อการวิเคราะห์พยานหลักฐานดิจิทัล และต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์เท่านั้น

1.1.4 การนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานเป็นขั้นตอนสุดท้ายในกระบวนการวิเคราะห์พยานหลักฐานอิเล็กทรอนิกส์ ซึ่งไม่ใช่แค่นำเสนอผลการตรวจพิสูจน์เป็นลายลักษณ์อักษรหรือรายงานการตรวจพิสูจน์เท่านั้น แต่ยังรวมถึงการจัดทำบันทึกคำให้การของผู้ตรวจพิสูจน์ โดยข้อมูลที่ควรจะนำเสนอลงไปในรายงานผลการตรวจพิสูจน์พยานหลักฐานดิจิทัลต้องมี ประวัติ และประสบการณ์ของผู้ตรวจพิสูจน์ เครื่องมือที่ใช้ตรวจพิสูจน์ วิธีที่ใช้ในการยืนยันความถูกต้องของข้อมูล กระบวนการที่ใช้ในการกู้คืนและทำสำเนาข้อมูล รายงานแสดงผลการค้นพบโดยผู้พิสูจน์ และข้อมูลจริงที่ได้ทำการกู้คืนเพื่อสนับสนุนรายงานผลการตรวจพิสูจน์ (Daniel & Daniel, 2019)

1.2 โซลิดสเตตไดรฟ์

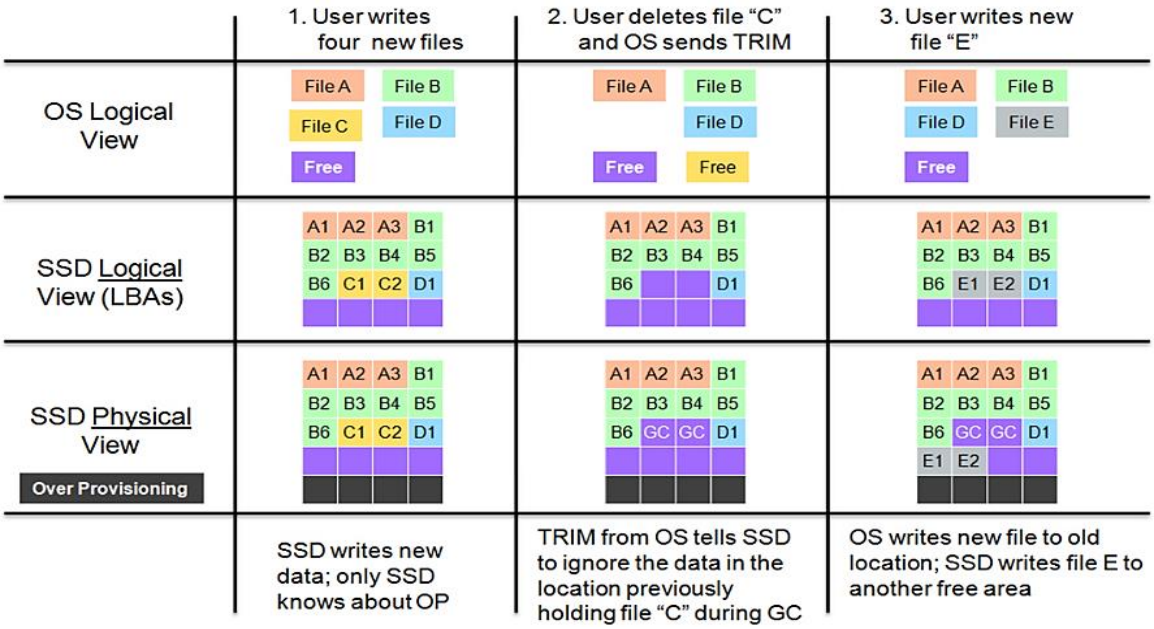
การออกแบบคอมพิวเตอร์ถูกพัฒนามาจนถึงปัจจุบัน จากเทคโนโลยีดั้งเดิมเป็นเทคโนโลยีใหม่ เช่น ฮาร์ดดิสก์ไดรฟ์ พัฒนาเป็นโซลิดสเตตไดรฟ์ ซึ่งเป็นไดรฟ์ที่มีขนาดเล็ก แต่มีความแข็งแรง และไม่มีเสียงที่เกิดจากการสั่น โดยมีช่องข้อมูลขาเข้า และช่องข้อมูลขาออกในการโอนถ่ายข้อมูลที่รวดเร็วกว่า นอกจากนี้ยังเก็บข้อมูลบิต (bit) ซึ่งเป็นหน่วยที่เล็กที่สุดของข้อมูลไว้ในหน่วยความจำแฟลช (Flash Memory) ซึ่งสามารถบันทึกข้อมูลได้มากกว่าบนจานแม่เหล็กของฮาร์ดดิสก์ไดรฟ์ ถึงแม้ว่าเทคโนโลยีใหม่ที่เป็นโซลิดสเตตไดรฟ์ นั้นจะมีข้อดี แต่ก็มีข้อจำกัดบางอย่าง คือจำนวนในการเขียนต่อเซลล์ (Cell) ที่สามารถเขียนได้ทีละเพจ (page) และการลบต้องลบทั้งบล็อก (block) ก่อนที่จะบันทึกข้อมูลใหม่ลงในแต่ละเพจ (page) (Vieyra, 2018)

สิ่งที่ทำให้ระบบปฏิบัติการสามารถติดต่อสื่อสารกับโซลิดสเตตไดรฟ์ และเห็นมองข้อมูลภายในได้เรียกว่า แฟลชทรานสเลชั่นเลเยอร์ (Flash Translation Layer) ซึ่งจะทำให้ระบบปฏิบัติการมองเห็นโซลิดสเตตไดรฟ์ เป็นแบบฮาร์ดดิสก์ไดรฟ์ได้ และมีการรวบรวมข้อมูลขยะ (Garbage Collection) และ แวร์เลเวลลิ่ง (wear levelling) (Vieyra,2018) ทำงานอยู่เบื้องหลังซึ่งเป็นกระบวนการพื้นฐานของโซลิดสเตตไดรฟ์

1.3 คำสั่งทริม

ในระบบปฏิบัติการรุ่นใหม่ เช่น วินโดวส์ 7 (Windows 7) ลินุกซ์ (Linux) 2.6.33 แมค โอเอส เอ็ก ไลออน (Mac OS X Lion) คำสั่งทริม จะเปิดใช้งานเพื่อแจ้งระบบปฏิบัติการให้ทราบว่า

โซลิดสเตตไดรฟ์ มีข้อมูลเก่าที่ไม่ได้ใช้อยู่อีกต่อไป ข้อดีของคำสั่งทริม คือ สามารถเปิดใช้งาน การรวบรวมข้อมูลขยะของโซลิดสเตตไดรฟ์ เพื่อข้ามข้อมูลที่ไม่ถูกต้องทดแทนการย้ายข้อมูลนั้น วิธีนี้จะช่วยประหยัดเวลาในการเขียนข้อมูลที่ไม่ถูกต้อง และลดจำนวนรอบการลบหน่วยความจำแฟลช และเปิดใช้งานอุปกรณ์ดังกล่าวในประสิทธิภาพที่สูงขึ้น นอกจากนี้ระหว่างการเขียนโซลิดสเตตไดรฟ์ ไม่จำเป็นต้องรวบรวมข้อมูลขยะ หรือลบตำแหน่งเหล่านี้ทันที ระบบจะสามารถแค่ทำได้เพียงแสดงเครื่องหมายว่าไม่ถูกต้องอีกต่อไป (Tokar, 2012)



ภาพที่ 3 การทำงานของคำสั่งทริม
ที่มา : Tokar, L. (2012).

จากภาพที่ 3 แสดงการทำงานของคำสั่งทริมอธิบายได้ดังนี้

1. ผู้ใช้งานสร้างแฟ้มข้อมูล จำนวน 4 รายการ ได้แก่ แฟ้มข้อมูลเอ (File A) แฟ้มข้อมูลบี (File B) แฟ้มข้อมูลซี (File C) แฟ้มข้อมูลดี (File D) และมีพื้นที่ว่าง (Free) ในมุมมองของปฏิบัติการ (OS Logical View) จะเห็นแฟ้มข้อมูลทั้ง 4 รายการและพื้นที่ว่าง ในมุมของโซลิดสเตตไดรฟ์เชิงฟิสิกส์ (SSD Physical View) จะเห็นแฟ้มข้อมูลเป็นคลัสเตอร์ (Cluster) และมองเห็นพื้นที่ส่วนเกิน (Over Provisioning)

2. ผู้ใช้งานลบแฟ้มข้อมูลซี ในมุมมองของปฏิบัติการพบว่าแฟ้มข้อมูลซี ไม่ปรากฏให้เห็น และปรากฏพื้นที่ว่างขึ้นมาแทน ในมุมของโซลิดสเตตไดรฟ์เชิงฟิสิกส์พบว่าพื้นที่เดิมของแฟ้มข้อมูลซีถูกคำสั่งทริมให้ข้ามพื้นที่ส่วนนี้เพื่อเตรียมให้กระบวนการรวบรวมข้อมูลขยะลบไปอย่างถาวร

3. ผู้ใช้งานสร้างแฟ้มข้อมูลอี ในมุมมองของปฏิบัติการ พบว่าแฟ้มข้อมูลอีถูกสร้างขึ้น ในมุมมองของโซลิดสเตตไดรฟ์เชิงฟิสิกส์พบว่าแฟ้มข้อมูลอี (File E) ที่ถูกสร้างขึ้นมานั้นไม่ได้ถูกเขียนในพื้นที่เดิมของแฟ้มข้อมูลซี แต่ถูกเขียนลงบนพื้นที่ว่างอื่น ๆ

1.4 ระบบไฟล์ที่ใช้เทคโนโลยีใหม่ (New Technology File System)

ระบบไฟล์ที่ใช้เทคโนโลยีใหม่หรือ เอ็นทีเอฟเอส (NTFS) เป็นระบบที่ถูกสร้างโดยบริษัทไมโครซอฟท์ นำมาใช้ครั้งแรกในระบบปฏิบัติการวินโดวส์ เอ็นที (Windows NT) เพื่อมาแก้ไขปัญหาของระบบไฟล์แฟท (FAT) ที่ถูกใช้มาก่อนหน้านี้ เช่น ขนาดของไฟล์ ความยาวของชื่อไฟล์ เป็นต้น ต่อมา เอ็นทีเอฟเอส กลายเป็นระบบไฟล์พื้นฐานที่ใช้กับระบบปฏิบัติการรุ่นใหม่ ๆ เช่น วินโดวส์ เอ็กพี (Windows XP) วินโดวส์ วิสต้า (Windows Vista) วินโดวส์ 7 และ วินโดวส์ 10 (Windows 10) เป็นต้น นอกจากนี้ได้รับการปรับปรุงให้เหมาะสม และมีฟังก์ชั่นความปลอดภัยเพิ่มขึ้น เช่น การขออนุญาตของไฟล์และแฟ้มข้อมูล การเข้ารหัสข้อมูล เป็นต้น (Xiaodong Lin,2018)

โครงสร้างของเอ็นทีเอฟเอส ซึ่งประกอบไป 2 ส่วน ดังแสดงตามภาพที่ 4

1) เซกเตอร์เริ่มต้นระบบของพาร์ติชัน (Partition Boot Sector) ประกอบไปด้วย ข้อมูลเกี่ยวกับโครงสร้างของเอ็นทีเอฟเอส

2) พื้นที่ของข้อมูล (Data Area) ประกอบไปด้วย ส่วนสำคัญในเอ็นทีเอฟเอส เรียกว่า ตารางแฟ้มข้อมูลหลัก (Master File Table) หรือ เอ็มเอฟที (MFT) และ พื้นที่ของแฟ้มข้อมูล (File Area)

ภาพที่ 4 โครงสร้างของเอ็นทีเอฟเอส
ที่มา : Xiaodong Lin. (2018)

เซกเตอร์เริ่มต้นระบบของพาร์ติชันของเอ็นทีเอฟเอส เก็บข้อมูลของโครงสร้างข้อมูลของเอ็นทีเอฟเอส เช่น ขนาดของคลัสเตอร์ขนาดของเอ็มเอฟทีเอ็นที (MFT Entry) และจุดเริ่มต้นของคลัสเตอร์ (Xiaodong Lin,2018)

พื้นที่ของข้อมูลประกอบไปด้วยสองส่วนทสำคัญคือ เอ็มเอฟทีและ พื้นที่ของแฟ้มข้อมูลโดยที่เอ็มเอฟทีเป็นส่วนสำคัญที่สุดในเอ็นทีเอฟเอส และเป็นฐานข้อมูลที่ระบุความสัมพันธ์ของทุก ๆ ข้อมูลในระบบ โดยข้อมูลที่บันทึกอยู่ในเอ็มเอฟทีประกอบไปด้วยข้อมูลทั่วไปของเอ็มเอฟที เช่น ขนาดและตำแหน่งของเอ็มเอฟที โดยแต่ละเอ็มเอฟทีประกอบไปด้วย เอฟทีเอ็นที ที่มีขนาด 1024 ไบต์ โดยภายในเอฟทีเอ็นทีประกอบไปด้วยคุณลักษณะ (Attributes) ต่าง ๆ เช่น คุณลักษณะ ที่บ่งบอกถึงชื่อแฟ้มข้อมูล หรือคุณลักษณะที่บ่งบอกถึงขนาดแฟ้มข้อมูล หรือคุณลักษณะที่บ่งบอกถึงเนื้อหาของแฟ้มข้อมูล เป็นต้น

แฟ้มข้อมูลที่มีขนาดเล็กที่สามารถเก็บไว้ในเอ็มเอฟทีเอ็นทีได้อย่างสมบูรณ์ เรียกว่า แฟ้มข้อมูลประเภทเรซิเดนต์ ส่วนไฟล์ที่มีขนาดใหญ่เกินว่าจะที่เขียนได้ในเอ็มเอฟทีเอ็นที ได้อย่างสมบูรณ์นั้น ถูกเขียนไว้ในส่วนของพื้นที่ของแฟ้มข้อมูลเรียกว่า แฟ้มข้อมูลประเภทนอนเรซิเดนต์ (Xiaodong Lin,2018)

2) งานวิจัยที่เกี่ยวข้อง

Marupudi (2017) ดำเนินการวิจัยในการกู้คืนแฟ้มข้อมูลบนฮาร์ดดิสก์ไดรฟ์ และโซลิดสเตตไดรฟ์ โดยใช้โปรแกรมเอฟทีเค ทูลคิต (FTK Toolkit) พบว่าการกู้คืนบนฮาร์ดดิสก์ไดรฟ์ได้ข้อมูลประมาณร้อยละ

70-80 ของแฟ้มข้อมูลทั้งหมด และการกู้คืนบนโซลิดสเตตไดรฟ์ได้น้อยกว่าร้อยละ 10 ของแฟ้มข้อมูลทั้งหมด วิจัยฉบับนี้มีความเห็นว่ากระบวนการ แวร์ เลเวลลิ่ง คำสั่งทริม และกระบวนการการรวบรวมข้อมูลขยะของโซลิดสเตตไดรฟ์ มีส่วนช่วยให้แฟ้มข้อมูลถูกลบอย่างถาวร ส่งผลให้การกู้คืนแฟ้มข้อมูลได้ยากมากขึ้น และส่งผลเสียแก่ผู้ตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

Vieyra et al. (2018) ดำเนินการวิจัยในการกู้คืนแฟ้มข้อมูลบนโซลิดสเตตไดรฟ์ ในกรณีเปิดและปิดคำสั่งทริม ระยะเวลาหลังจากลบแฟ้มข้อมูล และพื้นที่ว่างของโซลิดสเตตไดรฟ์ โดยใช้โปรแกรมเอ็กซ์ เวย์ ฟอเรนสิกส์ (X-ways Forensics) พบว่าในกรณีปิดคำสั่งทริมสามารถกู้คืนแฟ้มข้อมูลได้มากกว่ากรณีเปิดคำสั่งทริม และปริมาณการเพิ่มหรือลบแฟ้มข้อมูลส่งผลต่อการกู้คืนแฟ้มข้อมูล ส่วนระยะเวลาหลังจากแฟ้มข้อมูลถูกลบไม่ได้ส่งผลต่อการกู้คืนแฟ้มข้อมูล ซึ่งเป็นผลมาจากคำสั่งทริมและกระบวนการการรวบรวมข้อมูลขยะ วิจัยฉบับนี้มีข้อเสนอแนะว่า ในอนาคตผู้ตรวจพิสูจน์ต้องถอดหน่วยความจำแฟลช เพื่อข้ามในส่วนของ กระบวนการการรวบรวมข้อมูลขยะ

Tunyasevee (2019) ดำเนินการวิจัยในการกู้คืนแฟ้มข้อมูลโดยใช้โปรแกรมสองแบบคือโปรแกรมรหัสเปิดและโปรแกรมเชิงพาณิชย์ ซึ่งโปรแกรมรหัสเปิด ได้แก่ ออทอปซี (Autopsy) รุ่น 4.10 ส่วนโปรแกรมเชิงพาณิชย์ ได้แก่ เอ็นเคส รุ่น 8.08 และ แอคเซียม รุ่น 3.0 บนวัตถุพยานโดยกำหนดคุณลักษณะการทำงานขึ้น เช่น การทำสำเนาข้อมูล การคำนวณค่าแฮช เอ็มดี 5 (MD5) ชา1 (SHA-1) การระบุข้อมูลที่ถูกลบ การกู้คืนข้อมูลที่ถูกลบ การออกรายงาน เป็นต้น โปรแกรมทั้ง 3 โปรแกรมนี้ จะถูกใช้วิเคราะห์กับพยานหลักฐานประเภทโซลิดสเตตไดรฟ์และฮาร์ดดิสก์ไดรฟ์ หลังจากการวิเคราะห์เปรียบเทียบสามารถสรุปได้ว่าโปรแกรมเชิงพาณิชย์สามารถวิเคราะห์คุณลักษณะการทำงานได้มากกว่าโปรแกรมรหัสเปิด และจะเห็นว่าการกู้คืนข้อมูลที่ถูกลบไปจากโซลิดสเตตไดรฟ์นั้น ไม่สามารถกู้คืนกลับมาได้ เนื่องจากคำสั่งทริมของโซลิดสเตตไดรฟ์

Nisbet et al. (2013) ได้อธิบายว่า โซลิดสเตตไดรฟ์มีข้อได้เปรียบกว่าฮาร์ดดิสก์ไดรฟ์ในส่วนที่ไม่มีอุปกรณ์ที่เคลื่อนไหว ทนทานต่อแรงกระแทก ใช้พลังงานน้อย อย่างไรก็ตามโซลิดสเตตไดรฟ์มีความเสี่ยงที่หน่วยความจำแฟลชเสียหายได้ง่าย ในโซลิดสเตตไดรฟ์จึงมีกระบวนการแวร์ เลเวลลิ่ง เพื่อควบคุมการเขียนข้อมูลลงบนหน่วยความจำแฟลชให้เท่ากันในแต่ละเซลล์ ซึ่งจะถูกควบคุมโดยคำสั่งทริม ในงานวิจัยนี้ทดลองกู้คืนข้อมูลบนโซลิดสเตตไดรฟ์ ในกรณีเปิดและปิดการใช้งานคำสั่งทริม บนระบบปฏิบัติการ 3 ระบบปฏิบัติการ ได้แก่ วินโดวส์ ลินุกซ์ และ แมค โอเอส (Mac OS) พบว่าในกรณีเปิดใช้งานคำสั่งทริมกู้คืนข้อมูลได้น้อยกว่าในกรณีปิดใช้งานทริม

โปรแกรมทางนิติวิทยาศาสตร์มีหลากหลายโปรแกรม ซึ่งก็มีวัตถุประสงค์ในการใช้งานและมีประสิทธิภาพที่แตกต่างกันไป งานวิจัยที่ยกตัวอย่างมาข้างต้นไม่ได้กล่าวถึงขนาดของแฟ้มข้อมูลที่ใช้ในการทดลอง ซึ่งขนาดของแฟ้มข้อมูลสามารถแบ่งประเภทของแฟ้มข้อมูลได้เป็น 2 ประเภท ได้แก่ เรสซิเดนซ์และนอนเรซิเดนซ์ ทำให้ผู้วิจัยเห็นปัญหาที่เกิดขึ้น จึงสนใจศึกษาเกี่ยวกับเพื่อเปรียบเทียบโปรแกรมตรวจพิสูจน์พยานหลักฐานทางดิจิทัลระหว่างการเปิด และปิดการใช้งานคำสั่งทริม ในโปรแกรมเอ็นเคส และ โปรแกรมแอคเซียมและเปรียบเทียบประเภทของแฟ้มข้อมูลระหว่างเรสซิเดนซ์และนอนเรซิเดนซ์ ที่ส่งผลต่อประสิทธิผลในการกู้คืนข้อมูล ในกรณีเปิดและปิดการใช้งานคำสั่งทริม

ระเบียบวิธีวิจัย

1) เครื่องมือการวิจัย

(1) โซลิดสเตตไดรฟ์ ยี่ห้อ ซีเกท (Seagate) รุ่น บาร์ราคูดา (Barracuda) ขนาด 250 กิกะไบต์

(2) เครื่องคอมพิวเตอร์ประสิทธิภาพสูง (Workstation) ติดตั้งระบบปฏิบัติการ วินโดวส์ 10 โปร (Windows 10 Pro) ติดตั้งหน่วยประมวลผลกลาง (CPU) อินเทล ซีออน ซิลเวอร์ (Intel Xeon Silver) 4114 มีสัญญาณนาฬิกา 2.20 กิกะเฮิรตซ์ จำนวน 2 หน่วย และติดตั้งหน่วยความจำหลัก (RAM) ขนาด 64.0 กิกะไบต์

(3) อุปกรณ์ทำสำเนาข้อมูล ยี่ห้อ แท็บโบลว์ (Tableau) รุ่น ทีเอ็กวัน (TX1)

(4) เครื่องคอมพิวเตอร์สำหรับติดตั้งโซลิดสเตตไดรฟ์ ติดตั้งหน่วยประมวลผลกลาง (CPU) อินเทล คอร์ ไอ 5-8400 (Intel Core(TM) i5-8400) มีสัญญาณนาฬิกา 2.80 กิกะเฮิรตซ์ และติดตั้งหน่วยความจำหลัก (RAM) ขนาด 16 กิกะไบต์

(5) โปรแกรมเชิงพาณิชย์ ได้แก่ โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และ โปรแกรมแอคเซียม รุ่น 5.1.0.24999

(6) แฟ้มข้อมูลที่ใช้ในการทดลอง

ผู้วิจัยทำการสร้างแฟ้มข้อมูลที่ใช้ในการทดลองจำนวน 4 ประเภท โดยแต่ละประเภทมีจำนวนแฟ้มข้อมูลทั้งหมด 1,000 รายการ แสดงดังตารางที่ 1

ตารางที่ 1 จำนวนของแฟ้มข้อมูลที่ถูกสร้างขึ้นเพื่อการทดลอง

ประเภทของแฟ้มข้อมูล	จำนวนแฟ้มข้อมูล (รายการ)
แฟ้มข้อมูลข้อความ ประเภทเรซิเดนต์	1,000
แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์	1,000
แฟ้มข้อมูลภาพ ประเภทเรซิเดนต์	1,000
แฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์	1,000

2) รูปแบบการทดลอง

ผู้วิจัยได้ออกแบบการทดลอง ดังนี้

(1) การทดลองที่ 1 ทำการกู้คืนข้อมูลแฟ้มข้อมูลทั้ง 4 ประเภท ภายใต้การทำงานของคำสั่งทริม โดยการเริ่มใหม่ของระบบปฏิบัติการส่งผลต่อการกู้คืนข้อมูล

(2) การทดลองที่ 2 ทำการกู้คืนข้อมูลแฟ้มข้อมูลทั้ง 4 ประเภท ภายใต้การปิดการทำงานของคำสั่งทริม โดยการเริ่มใหม่ของระบบปฏิบัติการส่งผลต่อการกู้คืนข้อมูล

3) วิธีการทดลอง

กรณีเปิดใช้งานคำสั่งทริม

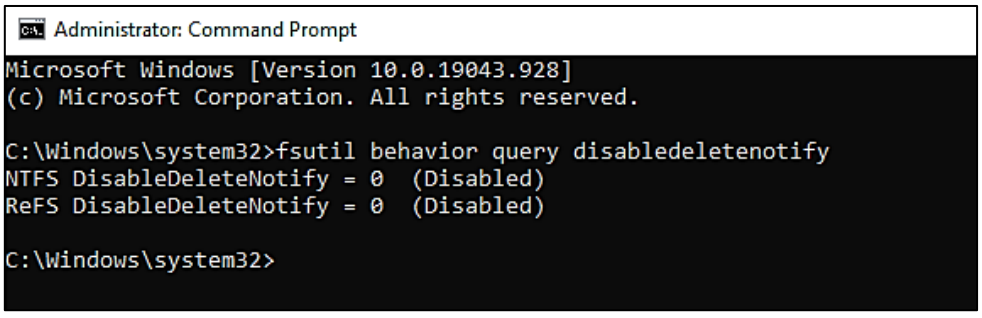
(1) ติดตั้งระบบปฏิบัติการวินโดวส์ 10 บนเครื่องคอมพิวเตอร์ที่ติดตั้งโซลิดสเตตไดรฟ์ที่ใช้สำหรับการทดลอง

(2) สร้างแฟ้มข้อมูลที่ใช้สำหรับการทดลอง ทั้ง 4 ประเภท คือ แฟ้มข้อมูลข้อความ และแฟ้มข้อมูลภาพที่เป็นเรซิเดนต์ และนอนเรซิเดนต์

(3) นำโซลิดสเตตไดรฟ์ที่ติดตั้งระบบปฏิบัติการวินโดวส์ 10 และสร้างแฟ้มข้อมูลที่ใช้สำหรับการทดลองแล้ว นำมาทำสำเนาใส่โซลิดสเตตไดรฟ์ อีกอันนึง
ดังแสดงตามภาพที่ 5

ภาพที่ 5 การทำสำเนาข้อมูล

(4) เมื่อทำสำเนาเสร็จสิ้นแล้ว จะได้โซลิดสเตตไดรฟ์ ที่เหมือนกันทุกประการ
กรณีเปิดใช้งานคำสั่งทริม
(5) นำโซลิดสเตตไดรฟ์ ที่ใช้ทดลองในกรณีเปิดใช้งานคำสั่งทริม ติดตั้งลงบนเครื่องคอมพิวเตอร์และเปิดเครื่องคอมพิวเตอร์
(6) ตรวจสอบการทำงานของคำสั่งทริม
ตรวจสอบการทำงานของคำสั่งทริม โดยการเข้าโปรแกรม คอมมาน พรอม (Command Prompt) เข้าผ่านทาง ผู้ดูแลระบบ (Administrator) ใช้คำสั่ง `fsutil behavior query disabledeletenotify` ถ้าปรากฏข้อความว่า NTFS DisableDeleteNotify = 0 หมายความว่าคำสั่งทริม กำลังทำงานอยู่เบื้องหลัง ดังแสดงตามภาพที่ 6



ภาพที่ 6 การตรวจสอบการเปิดใช้งานคำสั่งทริม

(7) ลบแฟ้มข้อมูลที่ใช้ในการทดลอง โดยการกดปุ่ม shift พร้อมกับ delete ที่แป้นพิมพ์
(8) ปิดเครื่องคอมพิวเตอร์ แล้วนำโซลิดสเตตไดรฟ์ ไปทำสำเนาข้อมูล โดยใช้อุปกรณ์ทำสำเนาข้อมูลรุ่นทีเอ็กวัน

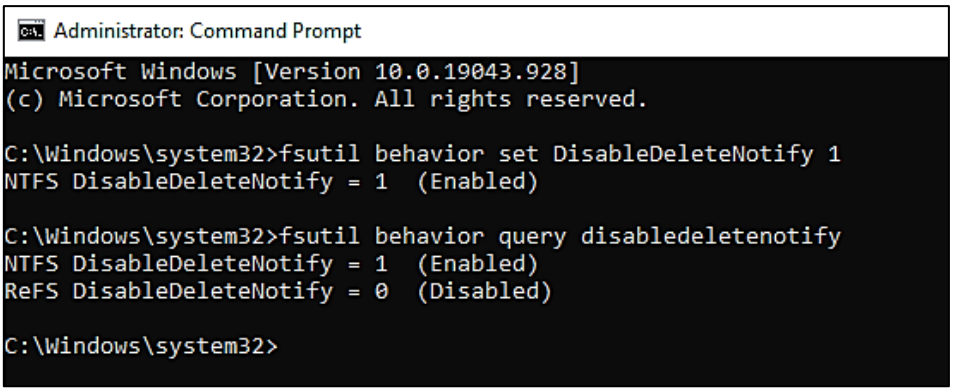
(9) เมื่อทำสำเนาเรียบร้อยแล้ว ให้นำไปติดตั้งที่เครื่องคอมพิวเตอร์ แล้วทำการเปิดเครื่องคอมพิวเตอร์ทิ้งไว้ประมาณ 1 นาที จากนั้นจึงทำการปิดเครื่อง แล้วนำโซลิดสเตต ไปทำสำเนาข้อมูล โดยใช้อุปกรณ์ทำสำเนาข้อมูล รุ่น ทีเอ็กวัน

กรณีปิดใช้งานคำสั่งทริม

(10) นำโซลิดสเตตไดรฟ์ ที่ใช้ทดลองในกรณีปิดใช้งานคำสั่งทริม ติดตั้งลงบนเครื่องคอมพิวเตอร์และเปิดเครื่องคอมพิวเตอร์

(11) ทำการปิดการใช้งานคำสั่งทริม โดยการเข้าคอมมาน พรอม ผ่านทาง Administrator ใช้พิมพ์คำสั่ง `fsutil behavior set DisableDeleteNotify 1`

(12) ตรวจสอบการทำงานของคำสั่งทริม อีกครั้ง โดยการเข้าคอมมาน พรอม ผ่านทางผู้ดูแลระบบ (Administrator) ใช้คำสั่ง `fsutil behavior query disabledeletenotify` ถ้าปรากฏข้อความว่า NTFS DisableDeleteNotify = 1 หมายความว่าคำสั่งทริม ถูกปิดใช้งานแล้ว ดังแสดงตามภาพที่ 7



ภาพที่ 7 การปิดใช้งานคำสั่งทริมและตรวจสอบการปิดใช้งานคำสั่งทริม

(13) ปฏิบัติตามข้อ 7 ถึง 9 เช่นเดียวกับในกรณีเปิดใช้งานคำสั่งทริม

(14) หลังจากนั้นทำสำเนาข้อมูลไปทำการกู้คืนข้อมูลโดยโปรแกรมทางนิติวิทยาศาสตร์ทั้ง 2 โปรแกรม

ผลการวิจัย

การกู้คืนข้อมูลหลักฐานดิจิทัล สามารถอธิบายผลการทดลองได้ ดังนี้

1) ผลการทดลองกรณีเปิดใช้งานคำสั่งทริม

ผลการกู้คืนข้อมูลกรณีเปิดใช้คำงานคำสั่งทริม ก่อนเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ (Reboot) จากตารางที่ 2 พบว่าโปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืน ชื่อของแฟ้มข้อมูลและสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลประเภทเรซิเดนต์ได้ทั้งหมด จำนวน 1,000 รายการ แต่แฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่ไม่สามารถกู้คืนเนื้อหาของแฟ้มข้อมูลได้

ตารางที่ 2 ผลการกู้คืนข้อมูลกรณีเปิดใช้คำงานคำสั่งทริม ก่อนเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์

ประเภทของแฟ้มข้อมูล	ชื่อแฟ้มข้อมูล	เนื้อหาแฟ้มข้อมูล
แฟ้มข้อมูลข้อความ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลภาพ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์	1,000	0
แฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์	1,000	0

ผลการกู้คืนข้อมูลกรณีเปิดใช้คำงานคำสั่งทริม หลังเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์จากตารางที่ 3 พบว่าโปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืนชื่อของแฟ้มข้อมูล และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลประเภทเรซิเดนต์ได้ทั้งหมด จำนวน 1,000 รายการ แต่แฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่ไม่สามารถกู้คืนเนื้อหาของแฟ้มข้อมูลได้

ตารางที่ 3 ผลการกู้คืนข้อมูลกรณีเปิดใช้คำงานคำสั่งทริม หลังเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์

ประเภทของแฟ้มข้อมูล	ชื่อแฟ้มข้อมูล	เนื้อหาแฟ้มข้อมูล
แฟ้มข้อมูลข้อความ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลภาพ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์	1,000	0
แฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์	1,000	0

2) ผลการทดลองกรณีปิดใช้งานคำสั่งทริม

ผลการกู้คืนข้อมูลกรณีปิดใช้คำงานคำสั่งทริม ก่อนเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์จากตารางที่ 4 พบว่าโปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืน ชื่อของแฟ้มข้อมูล และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลประเภทเรซิเดนต์ได้ทั้งหมด จำนวน 1,000 รายการ แต่แฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลข้อความได้ 956 รายการ แฟ้มข้อมูลภาพ ได้ 999 รายการ

ตารางที่ 4 ผลการกู้คืนข้อมูลกรณีปิดใช้คำงานคำสั่งทริม ก่อนเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์

ประเภทของแฟ้มข้อมูล	ชื่อแฟ้มข้อมูล	เนื้อหาแฟ้มข้อมูล
แฟ้มข้อมูลข้อความ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลภาพ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์	1,000	956

ประเภทของแฟ้มข้อมูล	ชื่อแฟ้มข้อมูล	เนื้อหาแฟ้มข้อมูล
แฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์	1,000	999

ผลการกู้คืนข้อมูลกรณีปิดใช้คำงานคำสั่งทริม หลังเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ จากตารางที่ 5 พบว่าโปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืน ชื่อของแฟ้มข้อมูล และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลประเภทเรซิเดนต์ ได้ทั้งหมด จำนวน 1,000 รายการ แต่แฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลข้อความได้ 617 รายการ แฟ้มข้อมูลภาพได้ 969 รายการ

ตารางที่ 5 ผลการกู้คืนข้อมูลกรณีปิดใช้คำงานคำสั่งทริม หลังเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์

ประเภทของแฟ้มข้อมูล	ชื่อแฟ้มข้อมูล	เนื้อหาแฟ้มข้อมูล
แฟ้มข้อมูลข้อความ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลภาพ ประเภทเรซิเดนต์	1,000	1,000
แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์	1,000	617
แฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์	1,000	969

สรุปและอภิปรายผล

1) ผลการตรวจพิสูจน์กรณีเปิดใช้งานคำสั่ง ทริม

การทำสำเนาข้อมูลทันทีก่อนเริ่มต้นการทำงานใหม่และการทำสำเนาทันทีหลังปิดเครื่องคอมพิวเตอร์ พบว่าแฟ้มข้อมูลประเภทเรซิเดนต์ โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และ โปรแกรมแอคเซียม รุ่น 5.1.0.24999 ให้ผลเหมือนกันคือสามารถกู้คืนชื่อของแฟ้มข้อมูล และสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลได้ทั้งหมด อย่างไรก็ตามแฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่ไม่สามารถกู้คืนเนื้อหาของแฟ้มข้อมูลได้ เนื่องจากว่าคำสั่งทริมคอยทำการส่งสัญญาณให้กระบวนการรวบรวมข้อมูลขยะลบข้อมูลที่ถูกลบตลอดเวลา อย่างไรก็ตามคำสั่งทริมไม่ได้มีผลต่อข้อมูลที่เก็บไว้ในเอ็มเอฟที ส่งผลให้สามารถกู้คืนชื่อของแฟ้มข้อมูลและแฟ้มข้อมูลประเภทเรสซิเดนซ์ได้

2) ผลการตรวจพิสูจน์กรณีปิดใช้งานคำสั่งทริม

การทำสำเนาข้อมูลทันทีก่อนเริ่มต้นการทำงานใหม่แฟ้มข้อมูลประเภทเรซิเดนต์ โปรแกรมทางนิติวิทยาศาสตร์ทั้งสอง สามารถกู้คืนชื่อของแฟ้มข้อมูลและสามารถกู้คืนเนื้อหาของแฟ้มข้อมูลได้ทั้งหมด นอกจากนี้แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่สามารถกู้คืนเนื้อหาได้เพียง 956 รายการ และแฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่กู้คืนเนื้อหาได้เพียง 999 รายการ แต่ในกรณีของการทำสำเนาข้อมูลหลังเริ่มต้นการทำงานใหม่ พบว่าแฟ้มข้อมูลประเภทเรซิเดนต์ โปรแกรมทางนิติวิทยาศาสตร์ทั้งสอง สามารถกู้คืนชื่อของแฟ้มข้อมูล และเนื้อหาได้ทั้งหมด นอกจากนี้แฟ้มข้อมูลข้อความ ประเภทนอนเรซิเดนต์สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน

1,000 รายการ แต่สามารถกู้คืนเนื้อหาได้เพียง 617 รายการ และแฟ้มข้อมูลภาพ ประเภทนอนเรซิเดนต์ สามารถกู้คืนชื่อของแฟ้มข้อมูลได้ทั้งหมด จำนวน 1,000 รายการ แต่กู้คืนเนื้อหาได้เพียง 969 รายการ เนื่องจากว่าคำสั่งทริมถูกปิดการใช้งาน ส่งผลให้ไม่มีการส่งสัญญาณไปยังกระบวนการรวบรวมข้อมูลขยะลบข้อมูลที่ถูกลบทันที ส่งผลให้สามารถกู้คืนข้อมูลได้บางส่วน อย่างไรก็ตามกระบวนการรวบรวมข้อมูลขยะลบยังคงทำงานอยู่ แม้จะไม่มีการทำงานของคำสั่งทริม สังเกตได้จากเมื่อเริ่มต้นการทำงานใหม่พบว่าแฟ้มข้อมูลที่กู้คืนได้ มีจำนวนน้อยลง ซึ่งเกิดจากการทำงานของกระบวนการรวบรวมข้อมูลขยะ

3) อภิปรายผล

จากการทดลองพบว่า ในระบบที่มีการเปิดใช้งานคำสั่งทริม โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืนแฟ้มข้อมูลประเภทเรซิเดนต์ มาได้ทั้งหมด เนื่องจากว่า ชื่อแฟ้มข้อมูลถูกเก็บไว้ในส่วนของเอ็มเอฟที จึงไม่ถูกคำสั่งทริมลบออกไป โดยโปรแกรมเอ็นเคส รุ่น 20.4.0.120 และโปรแกรมแอคเซียม รุ่น 5.1.0.24999 ให้ผลกันทดลองเหมือนกัน และสอดคล้องกับงานวิจัยของ ทรงวุฒิ (2019) ที่รายงานความสามารถในการกู้คืนแฟ้มข้อมูลที่ถูกลบด้วยคำสั่งลบขึ้นมาได้ แต่ไม่สามารถกู้คืนแฟ้มข้อมูลประเภทนอนเรซิเดนต์ ได้ เนื่องจากแฟ้มข้อมูลประเภทนี้ข้อมูลถูกเก็บไว้นอกเอ็มเอฟที จึงถูกคำสั่งทริมลบออกไปได้ รวมถึงยังสอดคล้องกับงานวิจัยของ Shiva Sai Ram Marupudi (2017) ที่รายงานว่าคำสั่งทริมส่งผลให้การกู้คืนข้อมูลเป็นไปได้ยากมากขึ้น และส่งผลเสียแก่การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล นอกจากนี้งานวิจัยยังสอดคล้องกับการรายงานของ Zubair Shah และคณะ (2014) พบว่าไม่สามารถกู้คืนข้อมูล ในกรณีที่เชื่อมต่อโซลิดสเตตไดรฟ์ ในช่องทางซาต้า (SATA) หลัก ซึ่งคำสั่งทริม ทำงานผ่านช่องทางนี้

ในระบบที่มีการปิดใช้งานคำสั่งทริม โปรแกรมเอ็นเคส รุ่น 20.4.0.120 และ โปรแกรมแอคเซียม รุ่น 5.1.0.24999 สามารถกู้คืนแฟ้มข้อมูลประเภทเรซิเดนต์ได้ทั้งหมด แต่สามารถกู้คืนแฟ้มข้อมูลประเภทนอนเรซิเดนต์ได้บางส่วน และเมื่อทำการเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ พบว่า แฟ้มข้อมูลประเภทนอนเรซิเดนต์ สามารถกู้ได้น้อยลง เนื่องจากว่า ในโซลิดสเตตไดรฟ์ ยังมีกระบวนเบื้องหลังที่คอยจัดการข้อมูล ซึ่งก็คือ การรวบรวมข้อมูลขยะ (Shiva Sai Ram Marupudi , 2017) ที่คอยจัดการข้อมูลที่อยู่บนโซลิดสเตตไดรฟ์ และทุกครั้งที่เปิดเครื่องคอมพิวเตอร์กระบวนการนี้คอยจัดการข้อมูลและส่งผลให้กู้คืนข้อมูลได้น้อยลง

ข้อเสนอแนะ

1) ข้อเสนอแนะเพื่อนำผลการวิจัยไปใช้

เนื่องจากการทำงานของคำสั่ง ทริม และการรวบรวมข้อมูล เป็นอุปสรรคในการกู้คืนข้อมูล คำสั่งทริม ถูกตั้งค่าเปิดการใช้งาน ไว้เป็นค่าเริ่มต้น ซึ่งการตั้งค่าดังกล่าวส่งผลเสียให้แก่การตรวจพิสูจน์ให้ทำการตรวจพิสูจน์ข้อมูลในโซลิดสเตตไดรฟ์ยากมากขึ้น ผู้ทำวิจัยจึงมีข้อเสนอแนะให้ผู้ผลิตทำการตั้งค่าให้ปิดใช้งานคำสั่งทริม เป็นค่าเริ่มต้น และให้ผู้ผลิตโซลิดสเตตไดรฟ์ ปรับปรุงการทำงานของกระบวนการรวบรวมข้อมูลขยะ ไม่ให้ส่งผลต่อข้อมูลที่ถูกลบ เพื่อที่จะสามารถตรวจพิสูจน์หลักฐานในโซลิดสเตตไดรฟ์ได้ง่ายมากขึ้น

2) ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

ในงานวิจัยนี้ ทำการทดลองศึกษาผลของการเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ พบว่าในกรณีปิดใช้งานคำสั่งทริม ก่อนเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ส่งผลให้กู้คืนข้อมูลได้

น้อยลง และงานวิจัยนี้ทำเพียงครั้งเดียวเท่านั้น ซึ่งควรศึกษาการเริ่มต้นการทำงานใหม่ของเครื่องคอมพิวเตอร์ หลาย ๆ ครั้ง เพื่อเป็นประโยชน์ต่อผู้ปฏิบัติงานในสถานที่เกิดเหตุ

เอกสารอ้างอิง

Daniel, L. and Daniel, L. (2016). *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom.*

Kasavajhala, V. (2011). *Solid State Drive vs. Hard Disk Drive Price and Performance Study*. A Dell Technical White Paper.

Lin, X. (2018). *Introductory Computer Forensics. A Hands-on Practical Approach. Springer Cham*, Switzerland.

Marupudi, S. (2017). *Solid State Drive: New Challenge for Forensic Investigation*. Culminating Projects in Information Assurance. 30.

Naksilp, S. (2019). *A Comparative Study of Digital Aniti-Forensic Techniques Affecting The Effectiveness of Forensic Data Recovery Software*. Master of Science Thesis, Royal Police Cadet Academy,Nakhon Pathom. (In Thai).

Naksilp, S. (2019). *A comparative Study of Digital Anti-Forensic Techniques Affecting The Effectiveness of Forensic Data Recovery Software.* Master of Science Thesis, Royal Police Cadet Academy, Nakhon Pathom. (In Thai).

National Statistical Office Thailand. (2020) *Survey on the use of information and communication technology in households 2020*. (In Thai).

Nisbet, L., Lawrence, S. and Ruff, M. (2013). *Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator.*

Police Cyber Taskforce. (2022). *Press release on new vaccines.* Thai police online, Technology Crime Immunity Working Group, Royal Thai Police. (In Thai).

Srisuwan, K., and Jitsawang, S. (2564). *Digital Forensic Process: Policy Development Analysis*. Chulalongkorn University, Bangkok. (In Thai).

Tokar, L. (2012). *Garbage Collection and TRIM in SSDs Explained – An SSD Primer*. Retrieved December 1, 2022. from https://www.thessdreview.com/daily-news/latest-buzz/garbage-collection-and-trim-in-ssds-explained-an-ssd-primer/2/.

Tunyasevee, W. (2019). *Comparative Evaluation of Open Source and Commercial Tools for Digital Forensic*. Master of Science Thesis, Royal Police Cadet Academy, Nakhon Pathom. (In Thai).

Vieyra, J., Scanlon, M. and Le-Khac N. (2018). *Solid State Drives Forensics: Where Do We Stand?.* Conference: 10th EAI International Conference on Digital Forensics and Cybercrime (ICDF2C) At: New Orleans, USA

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล **ร้อยตำรวจเอก ณรงค์ฤทธิ์ คำแสนราช ***
ตำแหน่ง/สถานะ นักศึกษาปริญญาโท
ที่อยู่หน่วยงาน/สังกัด คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
ไปรษณีย์อิเล็กทรอนิกส์ narongrid78@gmail.com

คำนำหน้า ชื่อ-สกุล **รองศาสตราจารย์ พันตำรวจเอก วรธัช วิชชุวาณิชย์**
ตำแหน่ง/สถานะ คณบดี/อาจารย์ (สัญญาบัตร 5)
ที่อยู่หน่วยงาน/สังกัด คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
ไปรษณีย์อิเล็กทรอนิกส์ woratouch_w@yahoo.com

*ผู้ประพันธ์บรรณกิจ (Corresponding Author)