



การพิสูจน์หลักฐานทางดิจิทัล

พ.ศ. ๒๕๖๖

โดย

กองรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์ไซเบอร์กองทัพอากาศ



บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๒๔๖๓)

ที่ กท ๐๖๐๙.๓/ ๑๒๒๕

วันที่ ๑๓ ก.ย.๖๖

เรื่อง ส่งคู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เสนอ ศชบ.ทอ.

๑. ตามอนุมัติ จก.ทสส.ทอ.เมื่อ ๑๓ ก.ย.๖๖ ท้ายหนังสือ สนผ.ทสส.ทอ.ที่ กท ๐๖๐๙.๓(๒)/๒๐๓ ลง ๑๒ ก.ย.๖๖ ให้ใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ นั้น

๒. ทสส.ทอ.จึงขอส่งคู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ เพื่อใช้ในการฝึกความชำนาญของจำพวกทหารไซเบอร์ รายละเอียดตามแนบ

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ต.

ผอ.สนผ.ทสส.ทอ.ทำการแทน

จก.ทสส.ทอ.



บันทึกข้อความ

ทสส.ทอ.	๕๗/๒๓
เลขรับ	๑๓ ก.ย. ๒๕๖๖
วันที่	๑๕/๙/๖๖
เวลา	๑๕๐๖

ส่วนราชการ สนม.ทสส.ทอ.(กณผ.โทร.๒-๑๐๕๖)

ที่ กท ๐๖๐๔.๓(๒)/ ๒๐๓

วันที่ ๑๒ ก.ย.๖๖

เรื่อง ขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เรียน จก.ทสส.ทอ.

๑. ตามหนังสือ ศชบ.ทอ.ที่ กท ๐๖๕๐.๑/๗๔๖ ลง ๒๘ ส.ค.๖๖ ขอให้พิจารณาคำราของ
หลักสูตรสายวิทยาการไซเบอร์ นั้น

๒. สนม.ทสส.ทอ.ตรวจสอบแล้ว มีข้อมูล ดังนี้

๒.๑ ระเบียบ ทอ.ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓ และฉบับแก้ไขเพิ่มเติม
ข้อ ๓๑.๑๔ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่า
ทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อให้ประกอบการฝึกงานในหน้าที่
ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ
ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แบบท้ายระเบียบนี้ (แบบ ๑)

๒.๒ ทสส.ทอ.เป็นหน่วยรับผิดชอบสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์
และสายวิทยาการไซเบอร์ ได้จัดทำคู่มือการฝึกงานในหน้าที่ เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญ
การปฏิบัติงานในสายวิทยาการไซเบอร์ จำนวน ๕ วิชา (แบบ ๒) ประกอบด้วย

๒.๒.๑ วิชา การป้องกันทางไซเบอร์

๒.๒.๒ วิชา การป้องกันทางไซเบอร์

๒.๒.๓ วิชา การข่าวกรองทางไซเบอร์

๒.๒.๔ วิชา การพิสูจน์หลักฐานทางดิจิทัล

๒.๒.๕ วิชา ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์

๓. สนม.ฯ พิจารณาแล้ว เพื่อให้การดำเนินการฝึกงานในหน้าที่ของสายวิทยาการไซเบอร์
เป็นไปด้วยความเรียบร้อย จึงขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึก
ความชำนาญของจำพวกทหารไซเบอร์ต่อไป

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

พล.อ.ต.

ผอ.สนม.ทสส.ทอ.

- อนุมัติตามข้อ ๓

พล.อ.ท.

จก.ทสส.ทอ.

๑๗ ก.ย.๖๖



บันทึกข้อความ

ทสส.ทอ.	๕๕๕๐
เลขรับ	๒๘ ส.ค. ๕๕๖๖
วันที่	๑๓๕๕
เวลา	

ส่วนราชการ ศษบ.ทอ.(นทพ.๗ โทร.๒-๒๗๑๒)

ที่ กท ๐๖๕๐.๑/ ๑๗๕๖

วันที่ ๒๓ ส.ค.๖๖

สนม.ทสส.ทอ.	
เลขรับ	๒๓๗/๖๑
วันที่	๒๘/๘/๖๖
เวลา	๑๓๕๕

เรื่อง ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์

เสนอ ทสส.ทอ.

ส่วน ๕-5
กท
๒๘ ส.ค. ๕๕๖๖

๑. ตามหนังสือ ทสส.ทอ.ที่ กท ๐๖๐๘.๓/๑๐๘๘ ลง ๘ ส.ค.๖๖ ให้ ศษบ.ทอ.ปรับปรุงเนื้อหาตำราของหลักสูตรสายวิทยาการไซเบอร์จำนวน ๕ วิชา นั้น
๒. ศษบ.ทอ.ตรวจสอบและพิจารณาแก้ไขเนื้อหา รายละเอียดตามความเหมาะสม ร่วมกับ ร.อ.หญิง สุธิดา บพสันเทียะ นมฐ.ณมทส.กนผ.สนม.ทสส.ทอ.แล้วเมื่อวันที่ ๒๓ ส.ค.๖๖ ดังมี รายละเอียดตามแนบ จึงเสนอมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต.

ผอ.ศษบ.ทอ.

กนผ.สนม.ทสส.ทอ.	
เลขรับ	๑๑๐๘
วันที่	๒๘ ส.ค. ๕๕
เวลา	๑๓๕๕

ทราบแล้ว

- รอง ผอ.กนผ.สนม.ทสส.ทอ.ทราบ
- พลต.๗ อำนวยการในส่วนที่๗๒

น.อ.

ผอ.กนผ.สนม.ทสส.ทอ.
๒๘/๘/๕๕

ทราบแล้ว

น.อ.

รอง ผอ.กนผ.สนม.ทสส.ทอ.
๒๘/๘/๕๕

ทราบแล้ว

น.อ.

รอง ผอ.กนผ.สนม.ทสส.ทอ.
๒๘/๘/๕๕



ระเบียบกองทัพอากาศ
ว่าด้วยการฝึกงานในหน้าที่
พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงแก้ไขแนวทางปฏิบัติเกี่ยวกับการฝึกงานในหน้าที่ของกองทัพอากาศ ให้เป็นไปด้วยความเรียบร้อย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๕๔

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

๔.๑ “การฝึกงานในหน้าที่” หมายความว่า การให้นายทหารประทวนเข้ารับ การฝึกงานตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญ ให้สูงขึ้น ตามลักษณะความชำนาญทหารอากาศของเหล่าทหารหรือจำพวกทหาร โดยใช้ตามมาตรฐานการฝึก ความชำนาญ และหนังสือคู่มือการฝึกงานในหน้าที่เป็นแนวทางการฝึก

๔.๒ “การฝึก” หมายความว่า การฝึกงานในหน้าที่

๔.๓ “นายทหารฝึกงานในหน้าที่” หมายความว่า นายทหารสัญญาบัตร ที่แต่งตั้งขึ้น ให้มีหน้าที่รับผิดชอบ และดำเนินการ ควบคุม กำกับ ดูแล เกี่ยวกับการฝึกงานในหน้าที่ของหน่วยขึ้นตรง กองทัพอากาศ ให้ใช้คำย่อว่า “นฝน.”

๔.๔ “ผู้ช่วยนายทหารฝึกงานในหน้าที่” หมายความว่า นายทหารสัญญาบัตร จำพวกทหารกำลังพลที่แต่งตั้งขึ้น ให้มีหน้าที่ช่วยเหลือนายทหารฝึกงานในหน้าที่ ให้ใช้คำย่อว่า “ผช.นฝน.”

๔.๕ “เจ้าหน้าที่ฝึกงานในหน้าที่” หมายความว่า นายทหารสัญญาบัตร หรือ นายทหารประทวน หรือลูกจ้างที่แต่งตั้งขึ้น ให้มีหน้าที่ด้านธุรการเกี่ยวกับการฝึกงานในหน้าที่ ให้ใช้คำย่อว่า “จนท.ฝน.”

๔.๖ “ผู้ควบคุมการฝึก” หมายความว่า นายทหารสัญญาบัตรที่เป็นเหล่าหรือ จำพวกทหารเดียวกันกับผู้รับการฝึกที่แต่งตั้งขึ้น ให้มีหน้าที่ดำเนินการ ควบคุม กำกับ ดูแลการฝึกงานในหน้าที่ ภาคปฏิบัติประจำปีให้เป็นไปตามมาตรฐานการฝึกความชำนาญ

๔.๗ “ผู้ช่วยผู้ควบคุมการฝึก” หมายความว่า นายทหารสัญญาบัตรที่แต่งตั้งขึ้น ให้มีหน้าที่ช่วยเหลือผู้ควบคุมการฝึก

๔.๘ “ครูฝึก”...

๓๑.๑๘.๒.๒ ระดับ ๕๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ไม่เกินร้อยละ ๘๐ ของจำนวนชั่วโมงรวมในระดับ ๗๐

๓๑.๑๘.๒.๓ ระดับ ๗๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ตรงกับความมุ่งหมายเฉพาะและวัตถุประสงค์การเรียนรู้ในระดับ ๗๐

๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า “หนังสือคู่มือการฝึก” และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้

หมวด ๖

การควบคุมกำกับดูแล

ข้อ ๓๒ หน่วยฝึกจะต้องดำเนินการฝึกตามระยะเวลาที่กำหนดไว้ในวงรอบการฝึก

ข้อ ๓๓ ผู้รับการฝึก จะต้องทำการฝึกครบทุกหัวข้อวิชา หรือหมวดวิชาที่เป็นวิชาหลักของจำพวกทหารตามที่กำหนดในมาตรฐานการฝึกความชำนาญ

ข้อ ๓๔ เมื่อผู้รับการฝึกย้ายสังกัด ในระหว่างการฝึกภาคปฏิบัติ หรือรอการทดสอบภาควิชาการ ให้ส่วนราชการต้นสังกัดเดิมแจ้งให้ส่วนราชการต้นสังกัดใหม่ทราบถึงสถานภาพการฝึกที่ผ่านมา และเรื่องที่จะต้องดำเนินการต่อไป พร้อมกับส่งประวัติการฝึก กับมาตรฐานการฝึกความชำนาญไปยังส่วนราชการต้นสังกัดใหม่ โดยส่วนราชการต้นสังกัดใหม่จะต้องแต่งตั้งผู้รับผิดชอบในชั้นตอนที่ยังเหลืออยู่ เพื่อดำเนินการฝึกต่อไปให้ครบตามหัวข้อที่กำหนดไว้ หากจะให้ทำการฝึกที่ส่วนราชการเดิมต่อไป ให้ประสานตกลงกันแล้วแจ้งการเปลี่ยนแปลงให้ กรมกำลังพลทหารอากาศทราบ เพื่อแก้ไขเปลี่ยนแปลงหลักฐานการควบคุมการฝึกงานในหน้าที่ให้ถูกต้อง

ข้อ ๓๕ ผู้ที่ไม่สามารถทำการฝึกได้ครบตามที่กำหนด และอยู่ในกรณีที่จะต้องพ้นจากการฝึก ให้ส่วนราชการต้นสังกัดรายงานพร้อมหลักฐานประกอบให้กรมกำลังพลทหารอากาศ ดำเนินการนำเรียนขออนุมัติผู้บัญชาการทหารอากาศ หากจะเข้ารับการฝึกในปีต่อไปจะต้องเริ่มดำเนินการใหม่ ซึ่งการพ้นจากการฝึกจะต้องอยู่ในกรณี ดังนี้

๓๕.๑ ลาออก ให้ออก ปลดออก

๓๕.๒ ต้องหาคดีอาญา ยกเว้นความผิดลหุโทษ หรือความผิดตามกฎหมายอื่น ที่มีอัตราโทษไม่สูงกว่าความผิดลหุโทษ

๓๕.๓ ย้าย โอน ไปสังกัดนอกกองทัพอากาศ

๓๕.๔ มีราชการจำเป็นเร่งด่วนและสำคัญ

๓๕.๕ มีเวลาการฝึกภาคปฏิบัติไม่ถึงร้อยละ ๘๕ ของเวลาการฝึกทั้งหมด โดยมีเหตุผล

อันสมควร

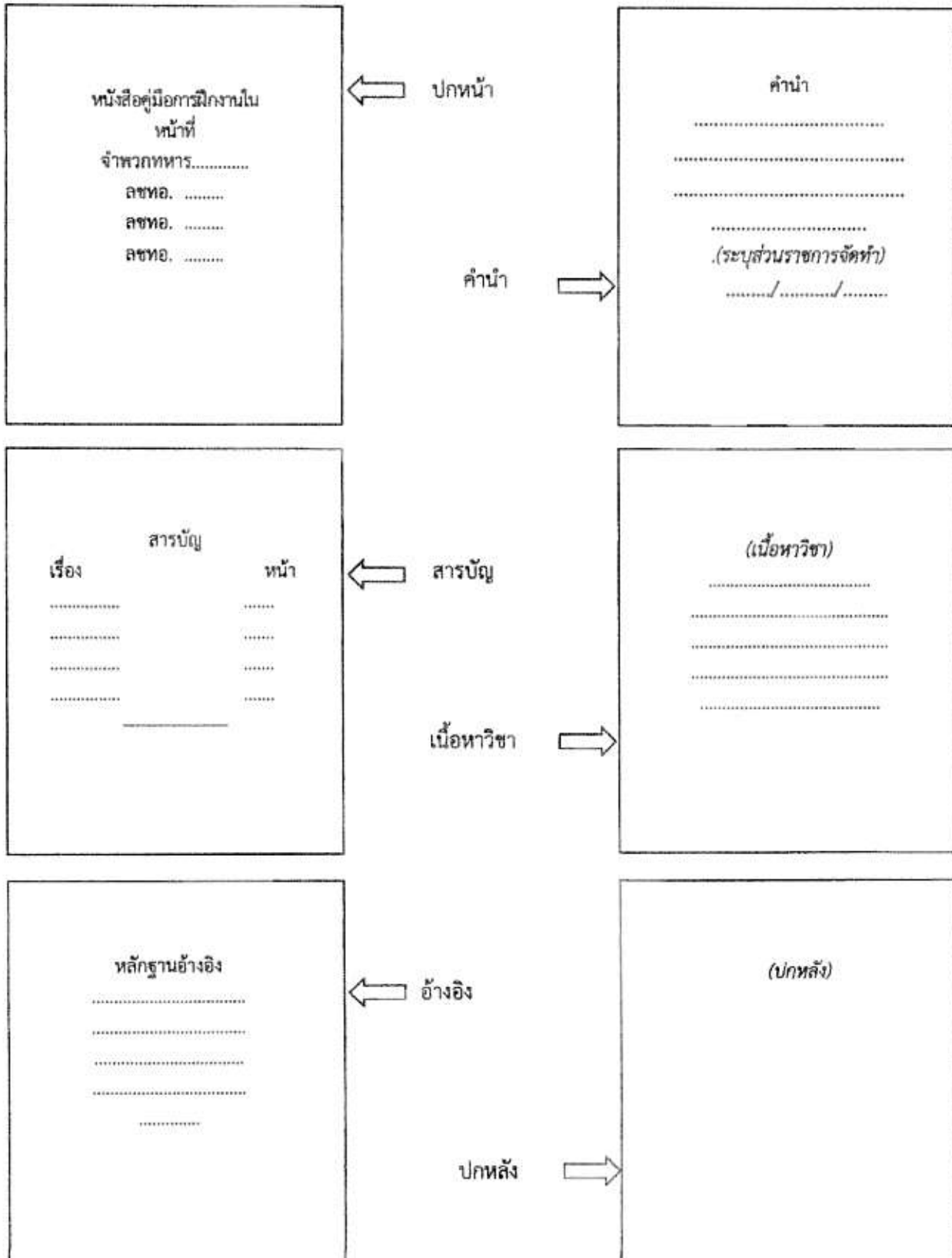
๓๕.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาคปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอันสมควร

ข้อ ๓๖ การลา ...

ผนวก ๗ ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

หนังสือคู่มือการฝึกงานในหน้าที่





คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

ลชทอ.๒๘๑๓๐

ลชทอ.๒๘๑๕๐

ลชทอ.๒๘๑๗๐

กองรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

คำนำ

คู่มือการฝึกงานในหน้าที่วิชาการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) จัดทำขึ้นเพื่อประกอบการฝึกความชำนาญ ตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ เนื้อหาความรู้ของคู่มือเล่มนี้กล่าวถึงนิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) มาตรฐานงาน Digital Forensics การค้นหาข้อมูลทางไซเบอร์ และเครือข่าย การเก็บหลักฐาน การเตรียมหลักฐาน การวิเคราะห์ข้อมูล การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน และการออกรายงานผลการวิเคราะห์ เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่มีความรู้ความเข้าใจ เสริมสร้างทักษะในการนำไปปฏิบัติงานในสายวิทยาการไซเบอร์ เพื่อให้เกิดความปลอดภัยสูงสุด ต่อผู้ปฏิบัติงานระบบคอมพิวเตอร์ และระบบสารสนเทศของกองทัพอากาศ

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณเจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
๒๘ สิงหาคม ๒๕๖๖

สารบัญ

	หน้า
คำนำ	ก
สารบัญ	ข
สารบัญตาราง	ง
สารบัญภาพ	จ
บทที่ ๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)	๑
๑.๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)	๑
๑.๒ Chain of Custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน”	๓
บทที่ ๒ มาตรฐานงาน Digital Forensics	๔
๒.๑ มาตรฐาน SANS Institute	๖
๒.๒ คู่มืองาน Forensic จากกระทรวงดิจิทัล ฯ	๑๐
บทที่ ๓ การค้นหาข้อมูลทางไซเบอร์และเครือข่าย	๑๒
๓.๑ OSINT Framework	๑๒
๓.๒ การค้นหาข้อมูลทางไซเบอร์ (Maltego, Shodan, Google Hacking)	๑๓
๓.๓ พื้นฐานการใช้งาน WireShark	๒๔
บทที่ ๔ การเก็บหลักฐาน	๕๒
๔.๑ การเตรียมการ	๕๒
๔.๒ การเข้าพื้นที่	๕๒
๔.๓ การจำกัดการแพร่กระจาย	๕๒
๔.๔ การจัดลำดับการเก็บหลักฐาน	๕๒
๔.๕ การเก็บหลักฐานเครือข่าย	๕๒
๔.๖ การเก็บหลักฐานเครื่องโฮส	๕๓
๔.๗ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)	๖๐
๔.๘ การจำกัดพื้นที่เครื่องเกิดเหตุ	๖๐
บทที่ ๕ การเตรียมหลักฐาน	๖๑
๕.๑ การสร้างไฟล์เพื่อทำการเก็บหลักฐานไฟล์ Image ด้วย Mandiant Redline	๖๑
๕.๒ การโคลนฮาร์ดดิสเป็น Master และ Slab	๖๘
บทที่ ๖ การวิเคราะห์ข้อมูล	๘๒
๖.๑ การแสดงผลโดยการใช้งาน IO Graph	๘๒
๖.๒ การวิเคราะห์ Host Forensic	๘๙
๖.๓ การวิเคราะห์ Malware Analysis	๙๗

สารบัญ (ต่อ)

	หน้า
บทที่ ๗ การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน	๑๐๒
๗.๑ กระบวนการจัดเก็บหลักฐาน	๑๐๔
๗.๒ การเก็บรักษา การถ่ายโอน และการส่งมอบหลักฐาน	๑๐๕
๗.๓ กระบวนการส่งคืนหลักฐาน	๑๐๕
บทที่ ๘ การออกรายงานผลการวิเคราะห์	๑๐๖
๘.๑ รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์	๑๐๖
๘.๒ ข้อมูลเบื้องต้น	๑๐๘
นิยามคำศัพท์ที่เกี่ยวข้องกับงานด้าน Forensic Computer	๑๐๙
อ้างอิง	๑๑๘

สารบัญตาราง

	หน้า
ตารางที่ ๑ คุณสมบัติของ Input Filter	๓๙
ตารางที่ ๒ การใช้งาน Filter	๓๙
ตารางที่ ๓ Logical Operator	๓๙

สารบัญภาพ

ภาพที่	หน้า
ภาพที่ ๑	๓
ภาพที่ ๒	๔
ภาพที่ ๓	๕
ภาพที่ ๔	๖
ภาพที่ ๕	๖
ภาพที่ ๖	๘
ภาพที่ ๗	๘
ภาพที่ ๘	๙
ภาพที่ ๙	๑๐
ภาพที่ ๑๐	๑๑
ภาพที่ ๑๑	๑๒
ภาพที่ ๑๒	๑๓
ภาพที่ ๑๓	๑๓
ภาพที่ ๑๔	๑๔
ภาพที่ ๑๕	๑๕
ภาพที่ ๑๖	๑๕
ภาพที่ ๑๗	๑๖
ภาพที่ ๑๘	๑๖
ภาพที่ ๑๙	๑๗
ภาพที่ ๒๐	๑๘
ภาพที่ ๒๑	๑๙
ภาพที่ ๒๒	๒๐
ภาพที่ ๒๓	๒๑
ภาพที่ ๒๔	๒๒
ภาพที่ ๒๕	๒๒
ภาพที่ ๒๖	๒๓
ภาพที่ ๒๗	๒๓
ภาพที่ ๒๘	๒๓
ภาพที่ ๒๙	๒๔
ภาพที่ ๓๐	๒๔
ภาพที่ ๓๑	๒๖
ภาพที่ ๓๒	๒๖
ภาพที่ ๓๓	๒๘
ภาพที่ ๓๔	๒๘

สารบัญภาพ (ต่อ)

ภาพที่	หน้า
ภาพที่ ๓๕	๒๙
ภาพที่ ๓๖	๓๐
ภาพที่ ๓๗	๓๑
ภาพที่ ๓๘	๓๑
ภาพที่ ๓๙	๓๒
ภาพที่ ๔๐	๓๓
ภาพที่ ๔๑	๓๔
ภาพที่ ๔๒	๓๔
ภาพที่ ๔๓	๓๕
ภาพที่ ๔๔	๓๖
ภาพที่ ๔๕	๓๖
ภาพที่ ๔๖	๓๗
ภาพที่ ๔๗	๓๘
ภาพที่ ๔๘	๔๐
ภาพที่ ๔๙	๔๐
ภาพที่ ๕๐	๔๑
ภาพที่ ๕๑	๔๒
ภาพที่ ๕๒	๔๓
ภาพที่ ๕๓	๔๔
ภาพที่ ๕๔	๔๕
ภาพที่ ๕๕	๔๕
ภาพที่ ๕๖	๔๖
ภาพที่ ๕๗	๔๗
ภาพที่ ๕๘	๔๘
ภาพที่ ๕๙	๔๘
ภาพที่ ๖๐	๔๙
ภาพที่ ๖๑	๕๐
ภาพที่ ๖๒	๕๑
ภาพที่ ๖๓	๕๓
ภาพที่ ๖๔	๕๓
ภาพที่ ๖๕	๕๔
ภาพที่ ๖๖	๕๔
ภาพที่ ๖๗	๕๕
ภาพที่ ๖๘	๕๖
ภาพที่ ๖๙	๕๖

สารบัญภาพ (ต่อ)

ภาพที่	หน้า
ภาพที่ ๗๐ การเก็บหลักฐาน RAM	๕๗
ภาพที่ ๗๑ การเก็บหลักฐาน RAM	๕๗
ภาพที่ ๗๒ การเก็บหลักฐาน RAM	๕๘
ภาพที่ ๗๓ การเก็บหลักฐาน RAM	๕๘
ภาพที่ ๗๔ การเก็บหลักฐาน RAM	๕๙
ภาพที่ ๗๕ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)	๖๐
ภาพที่ ๗๖ การจำกัดพื้นที่เครื่องเกิดเหตุ	๖๐
ภาพที่ ๗๗ โปรแกรม Mandiant Redline	๖๑
ภาพที่ ๗๘ รันไฟล์โปรแกรม Mandiant RedLine 2	๖๒
ภาพที่ ๗๙ โปรแกรม Mandiant RedLine 3	๖๓
ภาพที่ ๘๐ โปรแกรม Mandiant RedLine 4	๖๓
ภาพที่ ๘๑ โปรแกรม Mandiant RedLine 5	๖๔
ภาพที่ ๘๒ โปรแกรม Mandiant RedLine 6	๖๔
ภาพที่ ๘๓ โปรแกรม Mandiant RedLine 7	๖๕
ภาพที่ ๘๔ โปรแกรม Mandiant RedLine 8	๖๕
ภาพที่ ๘๕ โปรแกรม Mandiant RedLine 9	๖๖
ภาพที่ ๘๖ โปรแกรม Mandiant RedLine 10	๖๖
ภาพที่ ๘๗ โปรแกรม Mandiant RedLine 11	๖๗
ภาพที่ ๘๘ การโคลนฮาร์ดดิสก์เป็น Master และ Slab	๖๘
ภาพที่ ๘๙ โปรแกรม StarWind V2V Converter	๖๘
ภาพที่ ๙๐ โปรแกรม StarWind V2V Converter 1	๖๙
ภาพที่ ๙๑ โปรแกรม StarWind V2V Converter 2	๗๐
ภาพที่ ๙๒ โปรแกรม StarWind V2V Converter 3	๗๐
ภาพที่ ๙๓ โปรแกรม StarWind V2V Converter 4	๗๑
ภาพที่ ๙๔ โปรแกรม StarWind V2V Converter 5	๗๑
ภาพที่ ๙๕ โปรแกรม StarWind V2V Converter 6	๗๒
ภาพที่ ๙๖ โปรแกรม StarWind V2V Converter 7	๗๒
ภาพที่ ๙๗ โปรแกรม StarWind V2V Converter 8	๗๓
ภาพที่ ๙๘ โปรแกรม StarWind V2V Converter 9	๗๓
ภาพที่ ๙๙ โปรแกรม StarWind V2V Converter 10	๗๓
ภาพที่ ๑๐๐ โปรแกรม StarWind V2V Converter 11	๗๔
ภาพที่ ๑๐๑ โปรแกรม StarWind V2V Converter 12	๗๔
ภาพที่ ๑๐๒ โปรแกรม StarWind V2V Converter 13	๗๕
ภาพที่ ๑๐๓ โปรแกรม StarWind V2V Converter 14	๗๕
ภาพที่ ๑๐๔ โปรแกรม StarWind V2V Converter 15	๗๖

สารบัญภาพ (ต่อ)

ภาพที่	หน้า	
ภาพที่ ๑๐๕	โปรแกรม StarWind V2V Converter 16	๗๖
ภาพที่ ๑๐๖	โปรแกรม StarWind V2V Converter 17	๗๗
ภาพที่ ๑๐๗	โปรแกรม StarWind V2V Converter 18	๗๗
ภาพที่ ๑๐๘	โปรแกรม StarWind V2V Converter 19	๗๘
ภาพที่ ๑๐๙	โปรแกรม StarWind V2V Converter 20	๗๘
ภาพที่ ๑๑๐	การทำ Sandbox	๗๙
ภาพที่ ๑๑๑	คำสั่ง #> sudo fakedns	๘๐
ภาพที่ ๑๑๒	แสดงการ รันโปรแกรม Process Hacker	๘๐
ภาพที่ ๑๑๓	เว็บไซต์ Joesanbolbox.com	๘๑
ภาพที่ ๑๑๔	วิเคราะห์กระบวนการทำงานของมัลแวร์	๘๒
ภาพที่ ๑๑๕	การแสดงผลด้วย IO Graph	๘๓
ภาพที่ ๑๑๖	แสดงข้อมูลสรุปที่ได้จาก Expert Information	๘๔
ภาพที่ ๑๑๗	การแสดงผลโดย Custom Profile	๘๕
ภาพที่ ๑๑๘	การแสดงผลโดย Default Profile	๘๕
ภาพที่ ๑๑๙	โปรแกรม Imperva	๘๗
ภาพที่ ๑๒๐	การวิเคราะห์ลักษณะของ URL โดยโปรแกรม Imperva	๘๗
ภาพที่ ๑๒๑	Security Onion	๘๘
ภาพที่ ๑๒๒	Set ค่าวันเวลาของ Logs	๘๘
ภาพที่ ๑๒๓	สถิติที่ทำการโจมตี	๘๙
ภาพที่ ๑๒๔	โปรแกรม FTK Imager	๘๙
ภาพที่ ๑๒๕	การวิเคราะห์ Disk Image	๙๐
ภาพที่ ๑๒๖	ประวัติการใช้งาน Word Error หรือข้อความแจ้งเตือนของ Microsoft Office	๙๐
ภาพที่ ๑๒๗	วงจรรชีวิตของไฟล์	๙๑
ภาพที่ ๑๒๘	Regedit	๙๕
ภาพที่ ๑๒๙	โปรแกรมตั้งเวลาทำงานอัตโนมัติ	๙๖
ภาพที่ ๑๓๐	การตั้งค่า Firewall เพื่อเปิด - ปิด Port	๙๖
ภาพที่ ๑๓๑	โปรแกรม Powershell	๙๗
ภาพที่ ๑๓๒	โปรแกรม Volatility	๙๗
ภาพที่ ๑๓๓	การตรวจสอบไฟล์มัลแวร์เบื้องต้น	๙๘
ภาพที่ ๑๓๔	แสดง Dashboard ของโปรแกรม Deep Instinct	๙๙
ภาพที่ ๑๓๕	การทดสอบรันไฟล์มัลแวร์บนสภาพแวดล้อมจำลอง	๙๙
ภาพที่ ๑๓๖	คำสั่ง foremost & binwork	๑๐๐
ภาพที่ ๑๓๗	คำสั่งเกี่ยวกับไฟล์ zip	๑๐๐
ภาพที่ ๑๓๘	rockyou.txt.gz	๑๐๑
ภาพที่ ๑๓๙	Brute-Force	๑๐๑

สารบัญภาพ (ต่อ)

ภาพที่		หน้า
ภาพที่ ๑๔๐	แบบฟอร์มควบคุมหลักฐาน	๑๐๒
ภาพที่ ๑๔๑	แบบฟอร์มการรับ - ส่งหลักฐาน	๑๐๓
ภาพที่ ๑๔๒	ตัวอย่างห้องเก็บพยานหลักฐาน	๑๐๔
ภาพที่ ๑๔๓	ตัวอย่างรายงานผลการตรวจพิสูจน์หลักฐานทางดิจิทัล	๑๐๗

บทที่ ๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

Digital Forensics หรือ นิติวิทยาดิจิทัลเป็นกระบวนการที่ใช้สำหรับหาตัวผู้กระทำความผิดหรือใช้สำหรับเก็บรวบรวม ข้อมูล หลักฐานต่าง ๆ ที่อาจเกี่ยวข้องกับคดีความต่าง ๆ ที่เกิดขึ้นและการค้นหาข้อมูลมีอยู่หลายวิธีการ เช่น ติดตามจาก ที่อยู่ หมายเลขไอพี (IP Address) ตามพิกัด (GPS) การดูล็อกกล้องวงจรปิด การสืบหาผู้กระทำความผิดจากข้อมูลอัตลักษณ์บุคคล (Biometric Data) ต่าง ๆ หรือการเจาะข้อมูลเข้าไปในเครื่องเซิร์ฟเวอร์ (Server) เป็นต้น เพื่อระบุตัวผู้กระทำความผิดซึ่ง Digital Forensics นั้นมีความละเอียดและซับซ้อน

๑.๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

เป็นหนึ่งในศาสตร์ของนิติวิทยาที่ใช้เครื่องมืออิเล็กทรอนิกส์เข้ามาช่วยเพื่อการวิเคราะห์ พิจารณา และตรวจพิสูจน์หลักฐานทางดิจิทัล เพื่อนำเอาข้อมูลและหลักฐานต่าง ๆ เหล่านั้นมาประกอบรูปคดีจนสามารถเชื่อมโยงไปถึงตัวคนร้าย หรือผู้ที่อยู่เบื้องหลังการก่อเหตุอาชญากรรมเพื่อดำเนินการจับกุมต่อไปได้ โดย Digital Forensics จะแบ่งออกเป็น ๓ ประเภท คือ

๑.๑.๑ นิติวิทยาเครือข่าย (Network Forensics) เป็นการเฝ้าติดตาม ตรวจสอบ เก็บรวบรวม และวิเคราะห์การเคลื่อนไหวบนเครือข่ายดิจิทัลต่าง ๆ เช่น ประวัติการเข้าใช้งานเว็บไซต์ ระยะเวลาที่ใช้ในการอยู่หน้าเว็บไซต์ การรับ-ส่งข้อมูล เป็นต้น หรือการเคลื่อนไหวบนเครือข่ายดิจิทัลที่นำไปสู่การโจมตีทางไซเบอร์ ทั้งในเรื่องของความปลอดภัยของข้อมูล การเจาะเข้าระบบความปลอดภัย การปล่อยไวรัส และการใช้งานเครือข่ายที่ผิดไปจากวิสัยที่ควรจะเป็น

๑.๑.๒ นิติวิทยาไวรัสคอมพิวเตอร์ (Malware Analysis) เป็นการวิเคราะห์และเฝ้าดูพฤติกรรมการทำงานของไวรัสคอมพิวเตอร์ ตั้งแต่การยืนยันไฟล์ว่าเป็นภัยคุกคาม การจำลองการทำงานบนสภาพแวดล้อมสมมติ (Sandbox) และการวิเคราะห์ฟังก์ชันการทำงาน เพื่อค้นหาพฤติกรรมที่ซ่อนเร้น หรือนำมาซึ่งความเสียหายต่อระบบ ทั้งนี้จำเป็นต้องใช้ความรู้และประสบการณ์ในการทำงานสูงมากในการทำงานด้าน Digital Forensics หรือการพิสูจน์หลักฐานทางดิจิทัลของกองทัพอากาศ จะเน้นไปที่การเก็บหลักฐานให้ถูกต้องตามหลักของ Forensic และการวิเคราะห์ข้อมูลภัยคุกคาม โดยกระบวนการเหล่านี้ได้นำเอามาตรฐานหลายตัวในระดับโลกมาใช้เป็นหลักเกณฑ์ในการปฏิบัติงาน แต่เนื่องด้วยงานของกองทัพอากาศไม่ได้เน้นพิสูจน์หลักฐานแล้วนำไปสู่การดำเนินคดี แต่เป็นการให้ความสำคัญไปที่การค้นหาและพิสูจน์ช่องทางที่ถูกโจมตีด้วยเทคนิคขั้นสูงต่าง ๆ เพื่อเสนอผู้บังคับบัญชาในการออกมาตรการป้องกันหรือเพื่อค้นหาช่องโหว่ที่ถูกใช้งาน รวมทั้งดำเนินการปิดช่องโหว่ดังกล่าวเป็นหลัก

๑.๑.๓ หลักฐานดิจิทัล หมายถึง พยานหลักฐานที่อยู่ในรูปแบบข้อมูลที่คอมพิวเตอร์สามารถจัดเก็บและจัดการได้ โดยปัจจุบันพยานหลักฐานดิจิทัลเกิดขึ้นโดยทั่วไปจากสภาพสังคมในปัจจุบันที่คนในสังคมใช้คอมพิวเตอร์ในชีวิตประจำวันเป็นปกติ เมื่อเกิดอาชญากรรมขึ้น พยานหลักฐานในรูปแบบดิจิทัลจึงเข้ามามีบทบาทในกระบวนการยุติธรรมเพิ่มมากขึ้นตามความเจริญของสังคม ดังนั้นในการรวบรวมพยานหลักฐานและการพิจารณาคดี หากทุกฝ่ายที่เกี่ยวข้องกับกระบวนการยุติธรรม

มีความรู้ ความเข้าใจเกี่ยวกับพยานหลักฐานดิจิทัล ก็จะทำให้เกิดความยุติธรรมขึ้นอย่างแท้จริง เพราะพยานหลักฐานดิจิทัลสามารถพิสูจน์ได้ว่าบุคคลที่ถูกดำเนินคดีกระทำความผิด ทำให้ศาลสามารถมั่นใจได้มากยิ่งขึ้นว่าผลการตัดสินคดีนั้นถูกต้อง ทั้งเพื่อให้สามารถใช้นำเสนอเป็นหลักฐานในชั้นศาล หรือเพื่อรับฟังเป็นพยานหลักฐานในชั้นศาลตามขอบเขตอำนาจได้ และเพื่อให้มีมาตรฐานในการนำไปใช้กับผู้ใช้งานที่ไม่ได้เป็นผู้เชี่ยวชาญ ผลการวิเคราะห์หลักฐานอาจจะหลีกเลี่ยงการใช้คำศัพท์เฉพาะได้ โดยต้องเป็นไปตามขอบเขตอำนาจศาล และจะไม่ครอบคลุมการวิเคราะห์หลักฐานดิจิทัลหรือการยอมรับหรือการชั่งน้ำหนักพยานหลักฐาน รวมถึงความเกี่ยวข้องอันเป็นการพิจารณาของศาล นอกจากนี้ยังไม่มีกำหนดให้ใช้เครื่องมือหรือวิธีการเฉพาะอันอาจทำให้ได้มาซึ่งหลักฐานมัดตัวผู้กระทำความผิด โดยทั่วไปจะมีหลักการสำคัญเกี่ยวกับการจัดการหลักฐานทางดิจิทัล อยู่ ๔ รูปแบบ คือ

๑.๑.๓.๑ Identification Process กระบวนการระบุข้อมูล IP วันเวลาที่มีการบันทึก พฤติกรรมของการกระทำต่าง ๆ การแจ้งเตือนของระบบหรือข้อความที่ใช้ในการสนทนาระหว่างกัน ต้องมีครบถ้วนและสามารถสืบย้อนหลังได้

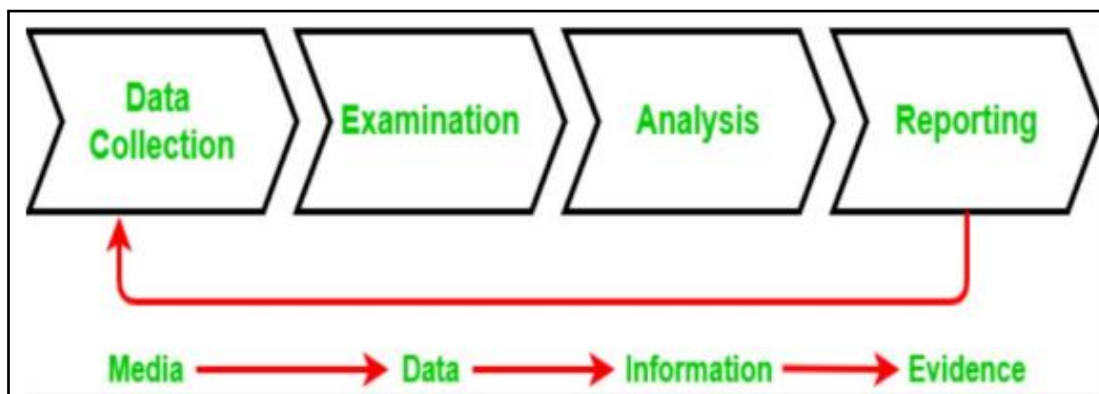
๑.๑.๓.๒ Collection Process กระบวนการรวบรวมข้อมูลหรือกระบวนการของข้อมูลที่มีความอ่อนไหวต่อการเปลี่ยนแปลงได้ ได้แก่ ข้อมูลใน RAM และข้อมูลที่มีความคงทน เช่น เอกสารบันทึก หรือระบบการบันทึกที่ไม่สามารถแก้ไขได้ เป็นต้น

๑.๑.๓.๓ Preservation Process กระบวนการปกป้องหลักฐาน ประกอบด้วย การป้องกันหลักฐานให้ได้มากที่สุด การกระทำใด ๆ จะต้องส่งผลต่อการเปลี่ยนแปลงน้อยที่สุด หรือไม่มีการเปลี่ยนแปลงเลย ที่สำคัญคือสามารถตรวจสอบกลับได้ด้วยกระบวนการเดียวกัน แต่บุคคลอื่นก็สามารถทำได้เช่นกัน และได้ผลลัพธ์เหมือนกัน

๑.๑.๓.๔ Acquisition Process กระบวนการเข้าถึงอุปกรณ์และข้อมูล ไม่ว่าจะเป็นทางกายภาพหรือทางตรรกะ (Logic) จะต้องไม่ก่อให้เกิดผลกระทบกับพยานหลักฐานจากหลักการที่ได้กล่าวมา เพื่อให้กระบวนการบริหารจัดการหลักฐานเป็นไปในแนวทางเดียวกัน และเป็นการคุ้มครองพยานหลักฐาน จึงได้มีการกำหนดกระบวนการคุ้มครองพยานหลักฐานหรือ Chain of Custody เพื่อให้สามารถแสดงถึงกระบวนการแก้ไขเปลี่ยนแปลงใด ๆ กับหลักฐานแล้ว สามารถยืนยันความถูกต้องของกระบวนการและไม่ก่อให้เกิดความคลาดเคลื่อนของผลการวิเคราะห์ได้ ซึ่งเป็นลักษณะของการมีเอกสารกำกับทุกเหตุการณ์หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบนั้นสามารถนำไปใช้ในยืนยันในชั้นศาลได้ หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบ เพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา ในการบันทึกจะไม่บันทึกเพียงแค่ว่าหลักฐานคือหลักฐานอะไรเท่านั้น แต่เราจะต้องบันทึกข้อมูลอื่น ๆ ด้วย เช่น ใครเป็นคนเก็บหลักฐาน เวลาที่เก็บหลักฐาน และรายละเอียดอื่น ๆ ที่เราพบขณะเก็บหลักฐาน กล่าวโดยสรุป คือ เอกสาร Chain of Custody จะประกอบด้วยข้อมูลที่เกี่ยวข้องกับการรวบรวมหลักฐาน การขนย้ายหลักฐาน การจัดเก็บหลักฐาน และการจัดการกับหลักฐานทางอิเล็กทรอนิกส์

๑.๒ Chain of Custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน”

เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงขอลกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา



ภาพที่ ๑ ข้อมูลในเอกสาร Chain of Custody

- ๑.๒.๑ ข้อมูลในเอกสาร Chain of Custody ควรมี ดังนี้
 - ๑.๒.๑.๑ วันและเวลาของการเก็บหลักฐาน
 - ๑.๒.๑.๒ สถานที่ที่เก็บหลักฐาน
 - ๑.๒.๑.๓ รายชื่อผู้เชี่ยวชาญ
 - ๑.๒.๑.๔ รายชื่อเจ้าของเครื่องคอมพิวเตอร์
 - ๑.๒.๑.๕ เหตุผลในการเก็บรวบรวมหลักฐาน
 - ๑.๒.๑.๖ หมายเลขของคดี
 - ๑.๒.๑.๗ ชนิดของอุปกรณ์
 - ๑.๒.๑.๘ หมายเลข Serial Number ของอุปกรณ์ (ถ้ามี)
 - ๑.๒.๑.๙ รุ่นของอุปกรณ์
 - ๑.๒.๑.๑๐ ความจุของอุปกรณ์ หรือ Hard Disk
 - ๑.๒.๑.๑๑ คำอธิบาย ทางกายภาพของคอมพิวเตอร์
 - ๑.๒.๑.๑๒ สถานะ เช่น กำลังเปิดใช้งาน หรือปิดอยู่
 - ๑.๒.๑.๑๓ ชื่อของไฟล์ทั้งหมดที่ถูกเก็บรวบรวม
 - ๑.๒.๑.๑๔ ค่าแฮชของไฟล์ต้นฉบับ
 - ๑.๒.๑.๑๕ ค่าแฮชของไฟล์ปลายทาง
 - ๑.๒.๑.๑๖ ความคิดเห็น ข้อเสนอแนะ และปัญหาที่พบ
 - ๑.๒.๑.๑๗ ลายมือชื่อของบุคคลที่ดำเนินการกับหลักฐาน
 - ๑.๒.๑.๑๘ รายละเอียดอื่น ๆ ที่เราพบขณะเก็บหลักฐาน

บทที่ ๒ มาตรฐานงาน Digital Forensics

มาตรฐานที่นำมาใช้ในทางด้าน Digital Forensics แต่ละประเทศจะใช้ไม่เหมือนกัน แต่โดยรวมแล้วก็จะเหมือนกันขึ้นอยู่กับลักษณะกฎหมายและความเหมาะสมของแต่ละประเทศ เช่น สหรัฐอเมริกาและยุโรป เป็นต้น จะใช้มาตรฐานของ SAN Institute ซึ่งเป็นบริษัทด้านการรักษาความปลอดภัยทางไซเบอร์ชั้นนำของสหรัฐ ฯ ร่วมกับ International Organization for Standardization (ISO) ซึ่งเป็นมาตรฐาน การวัดคุณภาพองค์กร เป็นการรับรองระบบการบริหารและการดำเนินงานขององค์กรในแต่ละประเทศ เพื่อให้เป็นมาตรฐานเดียวกันทั่วโลก ซึ่งกระบวนการเหล่านี้ได้นำมาตรฐานหลายตัวในระดับโลกมาใช้เป็นหลักเกณฑ์ในการปฏิบัติงาน ในบางครั้งหลักฐานที่นำมาวิเคราะห์เพื่อนำไปสู่การดำเนินคดีความจะมีการให้ความละเอียดรอบคอบเป็นพิเศษ ได้แก่ มาตรฐานระดับโลกที่นิยมนำมาใช้เป็นมาตรฐานการปฏิบัติงานด้านการพิสูจน์หลักฐานทางดิจิทัล ดังภาพ



ภาพที่ ๒ Association of Chief Police Officers

องค์กร Association of Chief Police Officers หรือ ACPO เป็นองค์กรด้านกระบวนการสืบสวนทางดิจิทัลของสมาคมตำรวจของสหราชอาณาจักร ซึ่งสามารถนำมาใช้เป็นแนวทางในงานตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

Scientific Working Group on Digital Evidence (SWGDE) เป็นคณะทำงานทางวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล ของสหรัฐ ฯ ที่รวบรวมองค์ความรู้เกี่ยวกับการบังคับใช้กฎหมายด้านนิติดิจิทัล เพื่อพัฒนาแนวทางและมาตรฐานของงานการกู้คืน การเก็บรักษา และการตรวจสอบหลักฐานดิจิทัล โดยได้รับการสนับสนุนจากสำนักงานสืบสวนกลางสหรัฐอเมริกา โดยมีเอกสารแนะนำแนวทางงานพิสูจน์หลักฐานทางดิจิทัลและยังสนับสนุนให้มีการใช้เอกสารเผยแพร่จำนวนมากในการสร้างมาตรฐานระดับชาติและระดับสากลสำหรับงานด้านพิสูจน์หลักฐานและมัลติมีเดีย

ISO/IEC 27037 เป็นแนวทางในการจัดการหลักฐานดิจิทัล ซึ่งครอบคลุมในเรื่องของ การระบุ การรวบรวม การได้มา และการเก็บรักษาหลักฐานดิจิทัล ตามมาตรฐานของ ISO ที่จะเน้นไปในเรื่องของกระบวนการทำงานเป็นหลัก

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The National Institute of Standards and Technology: NIST) เป็นหน่วยงานรัฐบาลกลางที่ดำเนินงานโดยกระทรวงพาณิชย์ของสหรัฐอเมริกา เป็นเอกสารที่ใหญ่ที่สุดโดยละเอียดเกี่ยวกับวิธีที่องค์กรจะสามารถสร้างความสามารถทางนิติวิทยาศาสตร์ พัฒนานโยบายและขั้นตอนพื้นฐานที่จำเป็น โดยมีจุดเด่นในเรื่องของการช่วยให้องค์กรสามารถใช้เทคนิคทางนิติวิทยาศาสตร์เพื่อช่วยในการตรวจสอบเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์และในการแก้ไขปัญหาตามการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

National Institute of Justice (NIJ) เป็นแนวทางการตรวจพิสูจน์พยานหลักฐานดิจิทัลสำหรับหน่วยงานบังคับใช้กฎหมายและสำนักงานอัยการ โดยจะมีเนื้อหาเกี่ยวกับการจัดการกับหลักฐานดิจิทัลให้อยู่ในกระบวนการสอบสวนที่สมบูรณ์ โดยในส่วนของกองทัพอากาศ จะใช้มาตรฐานของสถาบัน System Administration, Networking and Security (SANS) และ ISO/IEC 27037 : 2012 เป็นหลัก โดยจะมีเอกสาร “ข้อเสนอแนะมาตรฐาน การจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เป็นคู่มือประกอบการดำเนินการใด ๆ ทาง Digital Forensics ของกองทัพอากาศ โดยมีรายละเอียด ดังนี้



ภาพที่ ๓ เว็บไซต์ของ National Institute of Justice (NIJ)

๒.๑ มาตรฐาน SANS Institute

SANS Institute เป็นองค์กรที่ทำงานเกี่ยวกับการออกใบรับรองความสามารถด้านไซเบอร์และยังเป็นผู้พัฒนาเครื่องมือที่จำเป็นทั้งหมดบนระบบปฏิบัติการ Linux Ubuntu ที่เรารู้จักกันในชื่อ Sift เพื่อใช้เป็นเครื่องมือในการตรวจสอบทาง Forensic รวมถึงระบบการตอบสนองต่อเหตุการณ์แบบดิจิทัล ทั้งนี้ SANS Institute ไม่ได้ดำเนินการเฉพาะในส่วนของ Forensic เท่านั้น แต่ยังออกใบรับรองความสามารถทางไซเบอร์ในด้านอื่น ๆ อีกด้วย โดยในส่วนของ Forensic จะแบ่งออกเป็นหลายหลักสูตร ซึ่งจะมี Logo ของแต่ละหลักสูตร ดังภาพ



ภาพที่ ๔ Logo ของหลักสูตรต่าง ๆ ของ SANS Institute

สาเหตุที่นำ SANS Institute มากล่าวเพราะเป็นมาตรฐานที่ได้รับการยอมรับจากทั่วโลก และเป็นกลุ่มนักพัฒนาเครื่องมือที่เปิดให้ใช้งานโดยไม่มีค่าใช้จ่าย ทั้งนี้ยังมีมาตรฐานระดับโลกอีกมากที่สามารถนำมาใช้เป็นมาตรฐานในการปฏิบัติงานได้ เช่น ISO และ NIST เป็นต้น ซึ่งขึ้นอยู่กับความต้องการและความเหมาะสมของแต่ละองค์กร โดยในที่นี้จะไม่แยกย่อยตามหลักสูตรของ SANS Institute แต่จะแสดงให้เห็นเป็นภาพกว้าง ๆ และจะกล่าวถึงรายละเอียดการปฏิบัติที่สามารถนำมาใช้งานได้จริงโดยมีกระบวนการปฏิบัติงานดังภาพ



ภาพที่ ๕ Digital Forensics

๒.๑.๑ การจัดลำดับกระบวนการทำงาน Forensics ตามมาตรฐานของ SANS Institute ประกอบด้วย ๘ ขั้นตอน ดังนี้

- ๒.๑.๑.๑ ยืนยัน ระบุให้ชัดเจน (Identification)
- ๒.๑.๑.๒ ปกป้องพยานหลักฐานให้สมบูรณ์ให้มากที่สุด (Preservation)
- ๒.๑.๑.๓ กำหนดรูปแบบการทำงานให้เหมาะสม (Collection)
- ๒.๑.๑.๔ ดำเนินการจัดเตรียมและตรวจสอบ (Examination)
- ๒.๑.๑.๕ ดำเนินการวิเคราะห์ (Analysis)
- ๒.๑.๑.๖ ตีความ แปลความหมาย (Interpretation)
- ๒.๑.๑.๗ บันทึกผล (Documentation)
- ๒.๑.๑.๘ รายงานผล (Evidence Presentation)

นอกจากนี้ในเอกสาร Poster เกี่ยวกับงานด้าน Forensics ของ SANS Institute ซึ่งกล่าวถึงคำสั่งต่าง ๆ ที่มักจะต้องใช้ในการสืบค้นข้อมูล รวมถึงคำแนะนำกระบวนการทำงานและโปรแกรมที่จะใช้ในการวิเคราะห์ ซึ่งสามารถนำมาเป็นมาตรฐานในการปฏิบัติงานได้เช่นกัน ทั้งนี้สำหรับรายละเอียดเนื้อหาจะกล่าวในหัวข้อการวิเคราะห์ข้อมูล

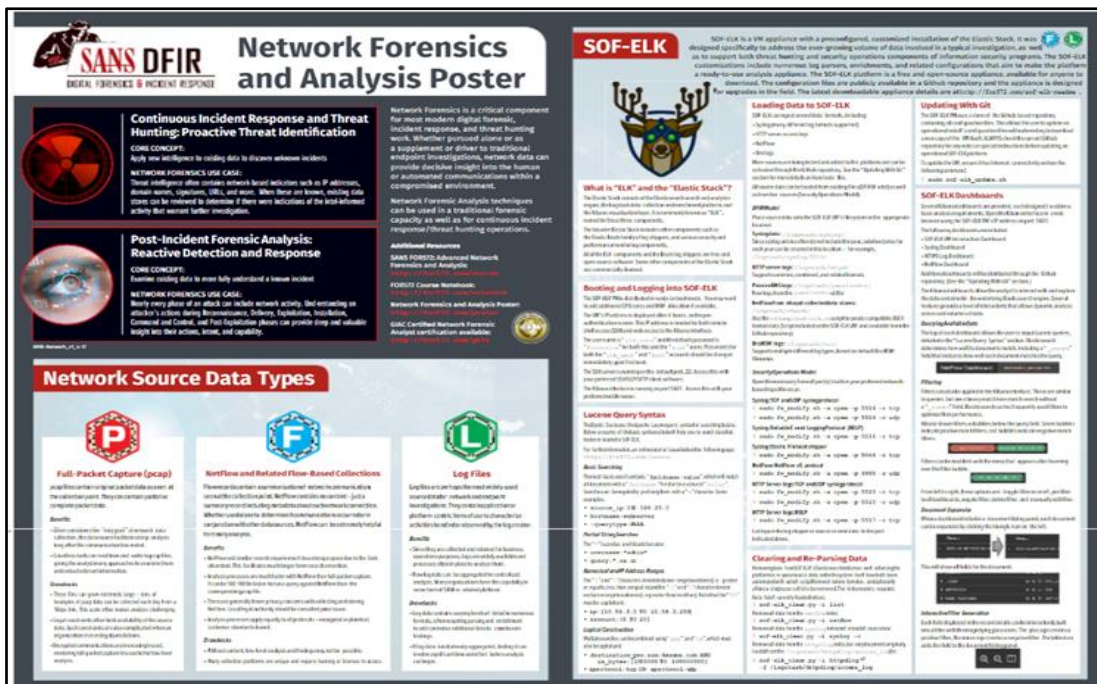
๒.๑.๒ รายละเอียดของแผ่นโปสเตอร์ (Poster) ที่นำมาใช้เป็นมาตรฐานงาน Forensic มีดังนี้

๒.๑.๒.๑ ด้าน Network Forensic จะเป็นการแนะนำเครื่องมือและแนวทางในการค้นหาหลักฐานทาง Network Forensic โดยจะแบ่งออกเป็น ๓ ส่วนใหญ่ ๆ คือ P หมายถึง ไฟล์ข้อมูลการจราจรใน Network (Packet Capture : pcap), F หมายถึง แผนผังเครือข่าย (Flow-Based or network diagram) และ L หมายถึง ล็อกไฟล์ (Logs File) โดยใช้ตัวย่อว่า PFL โดยมีรายละเอียดความหมาย ดังนี้

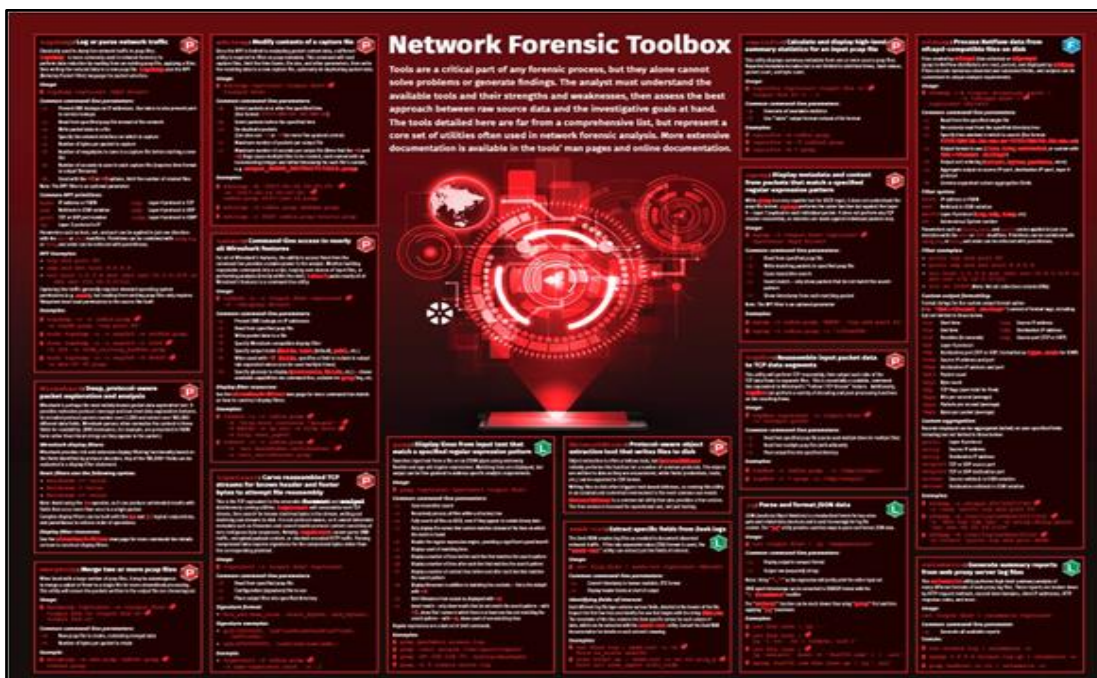
๒.๑.๒.๑ (๑) P หมายถึง ไฟล์ข้อมูลการจราจรใน Network (Packet Capture: pcap) เป็นส่วนสำคัญที่สุดเพราะจะทำให้ทราบว่าใครคุยกับใครในระบบ มีการรับส่งข้อมูลอะไรบ้างระหว่างกัน ปัจจุบันเครื่องมือที่ทำการวิเคราะห์ไฟล์ pcap ที่ดีที่สุดคือโปรแกรม WireShark

๒.๑.๒.๑ (๒) F หมายถึง แผนผังเน็ตเวิร์ค (Flow-Based or Network Diagram) เพื่อให้ทราบว่าอุปกรณ์แต่ละส่วนมีการเชื่อมต่ออย่างไร

๒.๑.๒.๑ (๓) L หมายถึง ล็อกไฟล์ (Logs File) จัดเป็นข้อมูลที่มีความสำคัญอีกตัวหนึ่ง ซึ่งสามารถบอกได้ว่าใครทำอะไรกับระบบบ้าง โดยจะมีรายละเอียดที่ค่อนข้างแปลผลได้ง่าย เนื่องจากเป็นข้อความธรรมดา ทั้งยังมีรายละเอียดของวันเวลาซึ่งนำไปสร้างเป็นไทม์ไลน์ของเหตุการณ์ ทั้งนี้ยังมีรายละเอียดอีกมาก ซึ่งจะสรุปในรูปแบบของแผ่น Poster โดยจะกล่าวเป็นด้าน ๆ ในหัวข้ออื่นต่อไป



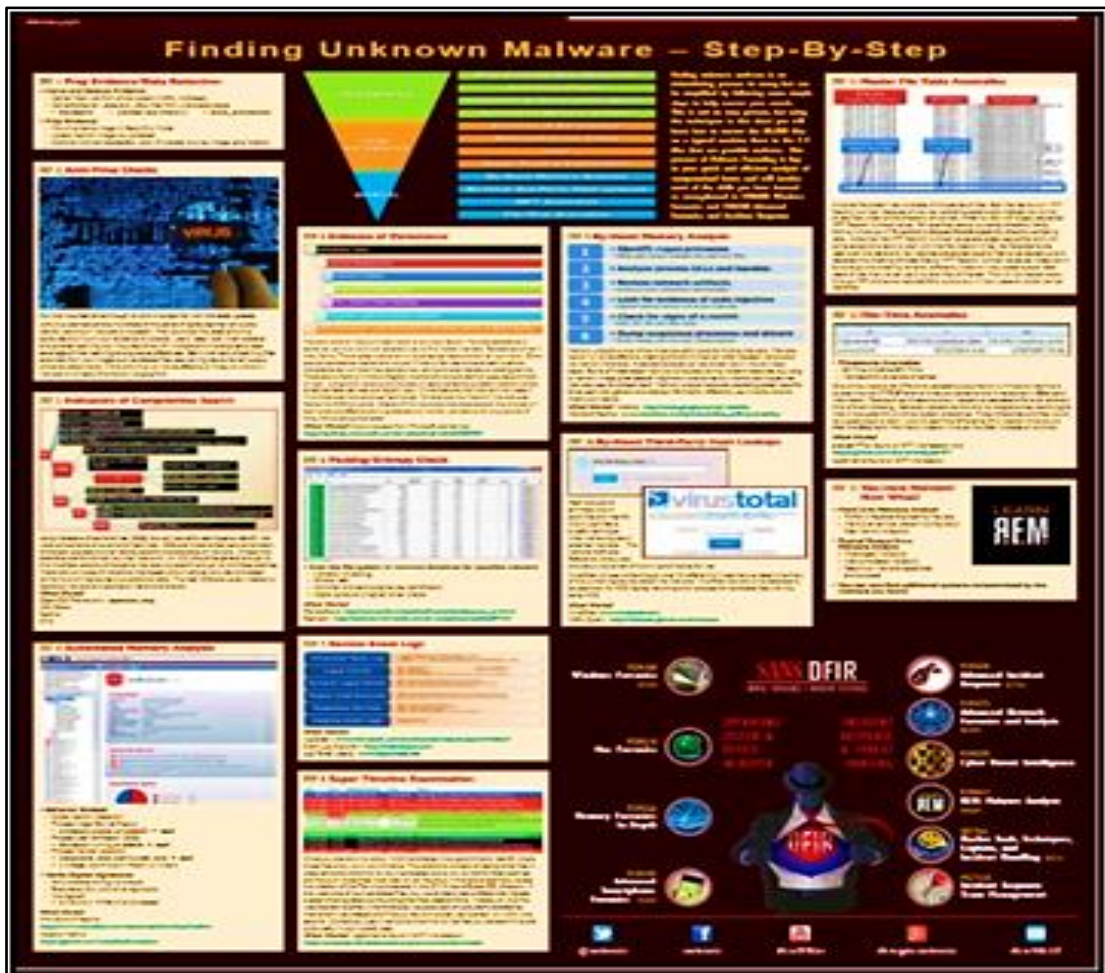
ภาพที่ ๖ แผ่น Poster เรื่อง Network Forensic



ภาพที่ ๗ แผ่น Poster เรื่อง Network Forensic Toolbox

๒.๑.๒.๒ ด้าน Host Forensic จะเป็นการศึกษาและทำความเข้าใจเกี่ยวกับการเปลี่ยนแปลงของเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นในส่วนของฮาร์ดแวร์หรือซอฟต์แวร์ โดยในที่นี่จะเน้นไปที่เรื่องของซอฟต์แวร์เป็นหลัก เนื่องจากการโจมตีทางไซเบอร์จะส่งผลกระทบต่อระบบปฏิบัติการ ไฟล์ ระบบเก็บ Logs และระบบเซิร์ฟเวอร์ที่ให้บริการ นอกจากนี้ยังมีส่วนที่เป็นฮาร์ดแวร์ที่สามารถใช้เป็นหลักฐานทาง Forensic ได้ เช่น RAM, Hard Disk และ USB เป็นต้น โดยจะมุ่งไปที่การค้นหาหลักฐานในระบบเมื่อมีการสร้างหรือรันไฟล์ใด ๆ ขึ้นมาใช้งาน จะก่อให้เกิด Logs หรือการเปลี่ยนแปลงของข้อมูลบางอย่างของไฟล์ ทั้งนี้ยังรวมไปถึงการเปิดใช้งานไฟล์ การแก้ไข การคัดลอก การใช้คำสั่งคัดไฟล์ และการลบไฟล์ทั้งด้วย สำหรับการหาข้อมูลประวัติการใช้งานบราวเซอร์ จะเป็นการสำรวจพฤติกรรมผู้ใช้งานว่ามีการท่องเว็บไซต์ที่เป็นอันตรายหรือไม่

๒.๑.๒.๓ ด้าน Malware Forensic จะมุ่งเน้นไปในเรื่องของ การหาความผิดปกติหรือไฟล์ที่ต้องสงสัยว่าเป็นไฟล์มัลแวร์หรือไม่ โดยการหาจากร่องรอยการเปลี่ยนแปลงของไฟล์หรือโปรเซส (Process) ที่มีพฤติกรรมการรับส่งข้อมูลหรือมีการเรียกใช้งาน Port ที่ผิดปกติ จนถึง การทดลองรันไฟล์ที่ต้องสงสัยเพื่อหาพฤติกรรมแอบแฝง ทั้งนี้ กระบวนการที่นำมาใช้จะเป็นดังรูป



ภาพที่ ๘ แผ่น Poster เรื่องกระบวนการวิเคราะห์ Malware Forensic

๒.๒ คู่มืองาน Forensic จากกระทรวงดิจิทัล ฯ

เป็นเอกสารอ้างอิงที่ใช้เป็นมาตรฐานในการวิเคราะห์ข้อมูล โดยเนื้อหาจะกล่าวถึงหลักการเกี่ยวกับงานพิสูจน์หลักฐานและพยานหลักฐานดิจิทัล การปฏิบัติงานในสถานที่เกิดเหตุ เครื่องมือที่ใช้ การประเมินและวางแผนการเก็บรวบรวมหลักฐานในสถานที่เกิดเหตุ การบรรจุ การเคลื่อนย้าย การปฏิบัติงานในห้องปฏิบัติการ การบันทึกข้อมูล การทำรายงาน รวมไปถึงคุณสมบัติเบื้องต้นของผู้ทำการวิเคราะห์หลักฐาน ทั้งนี้รายละเอียดสามารถศึกษาเพิ่มเติมจากเอกสารดังภาพแสดง



ภาพที่ ๙ ข้อเสนอแนะมาตรฐาน

คณะกรรมการจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล	
ผู้ตรวจแก้ร่างข้อเสนอแนะ	
นางสุรางคณา วายุภาพ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางสาวพิชญลักษณ์ คำทองสุข	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ปรึกษา	
พลตำรวจโท วิสนุ ปราสาททองโอสถ	สำนักงานตำรวจแห่งชาติ
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ประธาน	
นายธงชัย แสงศิริ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ผู้ทำงาน	
พันตำรวจเอก นิเวศน์ อากาศิน	สำนักงานตำรวจแห่งชาติ
พันตำรวจโท หญิง จีรบูรณ์ บำเพ็ญกรกิจ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
พันตำรวจโท นันทวุฒิ รอดมณี	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับ อาชญากรรมทางเทคโนโลยี
นายปกรณ์ ธรรมโรจน์	สำนักงานอัยการสูงสุด
นางสาวอมรรรัตน์ เล็กวิชัย	สถาบันนิติวิทยาศาสตร์
นางสาวธนีสรา ลีนสุวรรณ	สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี สารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการ สื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
นายโสฬส พานิชปริษา	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายธันวา วาหงษ์	บริษัท ไพร่ซอว์เตอร์เฮาส์คูเปอร์ส คอนซัลติง (ประเทศไทย) จำกัด
เลขานุการ	
นางสาวกรรณิกา ภัทรวิศิษฏ์สันต์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ภาพที่ ๑๐ คณะกรรมการจัดทำร่างมาตรฐานการปฏิบัติฯ

ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน Version 1.0
จัดทำโดย คณะกรรมการจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล

ศูนย์ดิจิทัลฟอเรนสิคส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9

แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

โทรศัพท์ 0 2123 1234 โทรสาร 0 2123 1200

E-mail: dfc@thaicert.or.th

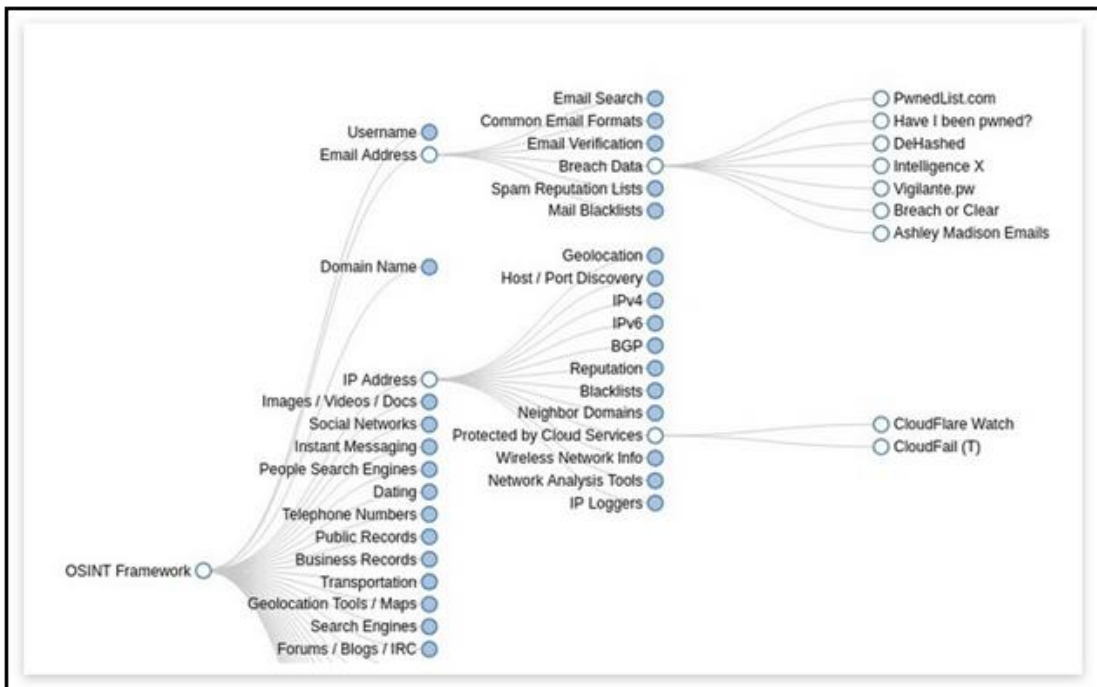
w w w . e t d a . o r . t h

บทที่ ๓ การค้นหาข้อมูลทางโซเชียลและเครือข่าย

การค้นหาข้อมูลทางโซเชียลและเครือข่าย มีความสำคัญอย่างมากในการสืบค้นข้อมูล เช่น เครื่องมือที่ใช้ตรวจสอบหมายเลข IP Address , URL และ DNS เป็นต้น เพื่อหาความสัมพันธ์ของเหตุการณ์ นำไปสู่การดำเนินการสืบสวนสอบสวนเพื่อหาบุคคลผู้กระทำความผิด

๓.๑ OSINT Framework

เป็นเครื่องมือที่ใช้ในการค้นหาข้อมูล โดยมีการรวบรวมลิงก์เว็บไซต์ของเครื่องมือที่ต้องการและจัดเป็นหมวดหมู่ ทำให้สามารถไล่ลำดับการค้นหาได้ง่าย การใช้งาน เช่น ถ้ามีข้อมูล IP หากต้องการหาต่อว่าจะสามารถนำไปใช้ประโยชน์ในการค้นหาข้อมูลประเภทอื่น ๆ ได้อย่างไร เราก็จะสามารถคลิกหัวข้อ IP Address ได้เลย โดย OSINT Framework จะทำการเชื่อมโยงข้อมูลอื่น ๆ ที่เกี่ยวข้องเป็นลักษณะกราฟเส้น แสดงความสัมพันธ์เป็นชื่อเครื่องมือ ดังภาพ

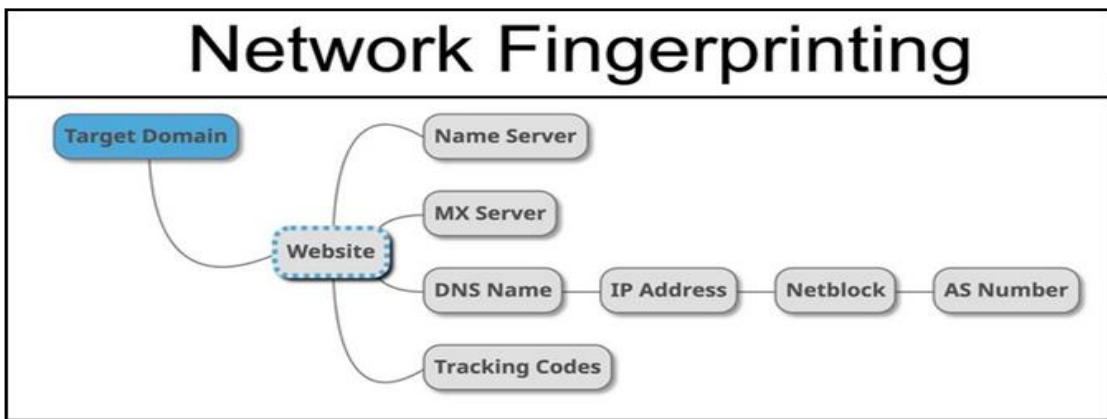


ภาพที่ ๑๑ OSINT Framework

๓.๒ การค้นหาข้อมูลทางไซเบอร์ (Maltego, Shodan และ Google Hacking)

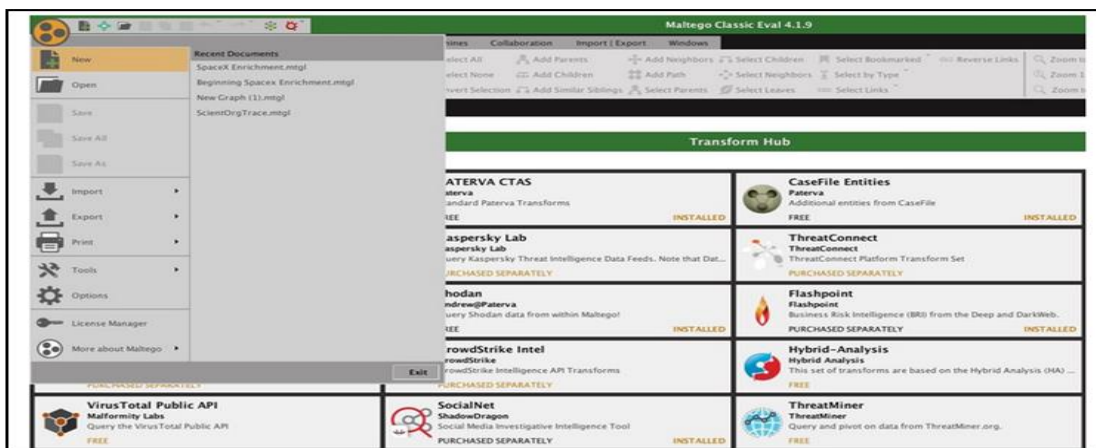
โดยโครงสร้างของเว็บไซต์หรือโดเมนมีส่วนช่วยให้การค้นหาข้อมูลและโครงสร้างเว็บเป้าหมายทำได้ง่ายและเป็นระบบมากขึ้น ทั้งนี้เครื่องมือที่ได้รับความนิยมในลำดับต้น ๆ สำหรับการวิเคราะห์ข้อมูลและมีขั้นตอนการใช้งาน ดังนี้

๓.๒.๑ Maltego เป็นเครื่องมือที่นิยมสำหรับการวิเคราะห์เครือข่ายที่ไม่ซับซ้อน โดยใช้ชื่อโดเมนหรือเว็บไซต์ที่ต้องการค้นหาข้อมูล ระบบจะดึงเอาข้อมูลความสัมพันธ์ต่าง ๆ และเชื่อมโยงเป็นโครงสร้างแสดงเป็นภาพรวม ทำให้ทราบความเชื่อมโยงของเว็บไซต์ ทั้งนี้ เครื่องมือดังกล่าวเป็นโปรแกรมฟรีแวร์ ไม่มีค่าใช้จ่าย โดยมีเงื่อนไขต้องเป็นสมาชิกของเว็บไซต์เท่านั้น โดยมีขั้นตอนในการใช้งาน ดังนี้



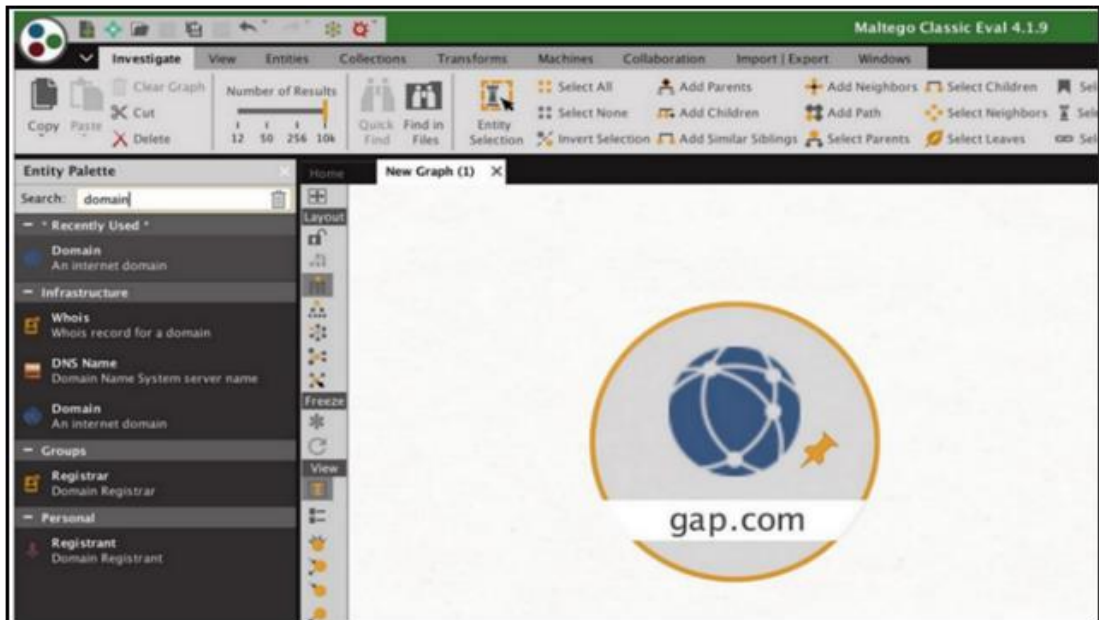
ภาพที่ ๑๒ Network Fingerprinting

๓.๒.๑.๑ ขั้นตอนที่ ๑ เลือกจุดหมายปลายทางและค้นหาเว็บไซต์ จากภาพจะใช้เว็บไซต์ Gap ซึ่งมาจากการค้นหาของ Google อย่างรวดเร็วในโดเมน gap.com เปิดโปรแกรม Maltego และรอให้หน้าต่างหลักเปิดขึ้น จากนั้นคลิกที่ไอคอน Logo ที่มุมบนด้านซ้ายและเลือก "New"



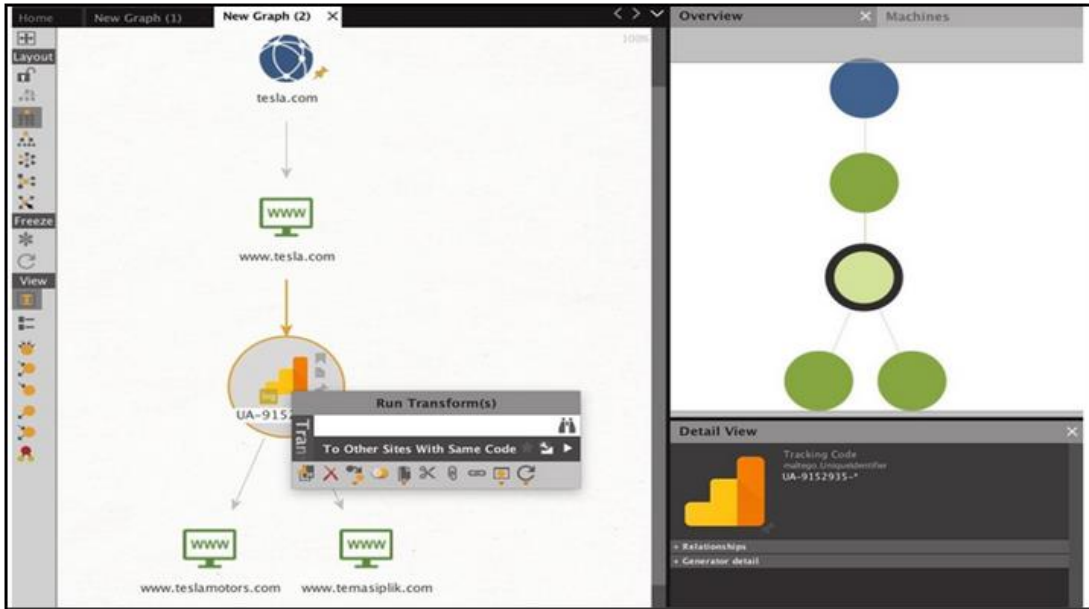
ภาพที่ ๑๓ ขั้นตอนที่ ๑ เลือกจุดหมายปลายทางและค้นพบเว็บไซต์

จากตัวอย่างจะทำการค้นหาโดยใช้ชื่อโดเมนชื่อเดียวซึ่งระบบจะแสดงหน้าว่างเปล่าขึ้นมา โดยสามารถเพิ่มเอนทิตี (Entity) แรกได้ โดยสามารถดู Entity Palette ทางด้านซ้าย และพิมพ์ "domain" ในแถบค้นหาเพื่อเรียกใช้เอนทิตีของโดเมน เมื่อขึ้นภาพสัญลักษณ์ให้ทำการลากและวางลงบนหน้าจอเพื่อเริ่มการตรวจสอบได้




ภาพที่ ๑๔ ตัวอย่างการกำหนดเว็บไซต์เป้าหมาย

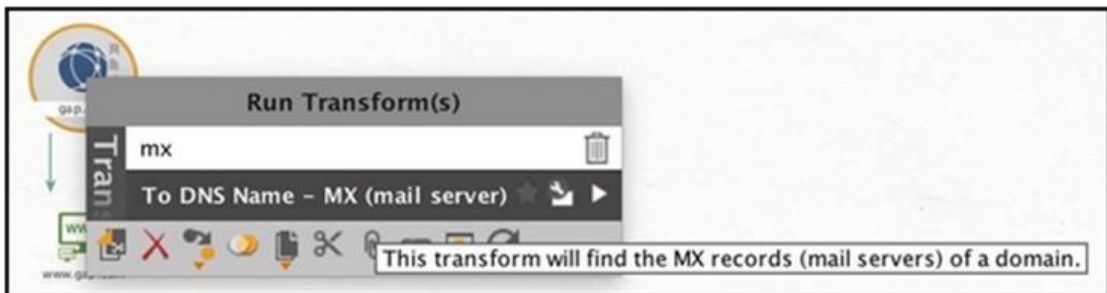
๓.๒.๑.๒ ขั้นตอนที่ ๒ ค้นหาเว็บไซต์อื่น ๆ ด้วยรหัสติดตาม (Tracking Code) สิ่งแรกที่ต้องตรวจสอบคือรหัสติดตามที่องค์กรใช้ ด้วยการเตรียมการวิเคราะห์สำหรับโดเมนเว็บไซต์ บ่อยครั้งที่สามารถเชื่อมโยงโดเมนต่าง ๆ เข้าด้วยกันได้เนื่องจากใช้รหัสติดตามร่วมกัน รหัสติดตามสามารถแตกต่างกันไปตามรหัส Google Analytics ของ Amazon Affiliates codes และสามารถใช้เพื่อระบุข้อมูลการสร้างรายได้หรือต้องการค้นหารหัสติดตามที่เชื่อมโยงกับเว็บไซต์ ในขั้นต้นต้องดำเนินการแปลงเป็นโดเมนเว็บก่อน ทำได้โดยการคลิกขวาที่ Public Domain และพิมพ์ "ชื่อเว็บไซต์" ในแถบค้นหาเพื่อดูโดเมนทั้งหมดที่เชื่อมโยงไปยังความละเอียดของเว็บไซต์ โดย "Quick Lookup" ที่เ ร รี ย บ ี่ ง ่า บ ย จะทำงานได้ดี และควรแก้ไขโดเมนของเราไปยังเว็บไซต์จากที่นี่เราสามารถคลิกขวาและป้อน "To Tracking Codes" เพื่อดำเนินการแปลงรหัสติดตาม จากตัวอย่างไม่ได้ส่งผลใด ๆ แต่มีการส่งข้อมูลต่อไปยังเว็บไซต์ของ เทสลา (tesla.com) ด้านล่างเราจะเห็นผลลัพธ์ของการแปลงของโดเมนที่เกี่ยวข้องอีกสองโดเมน หากต้องการค้นหาโดเมนเหล่านี้ต่อ สามารถคลิกขวาที่โค้ดติดตาม จากนั้นคลิกที่ "ไซต์อื่น ๆ ที่มีรหัสเดียวกัน" เพื่อค้นหาไซต์อื่น ๆ ที่มีรหัสติดตามเดียวกัน



ภาพที่ ๑๕ ขั้นตอนที่ ๒ ค้นหาไซต์อื่น ๆ

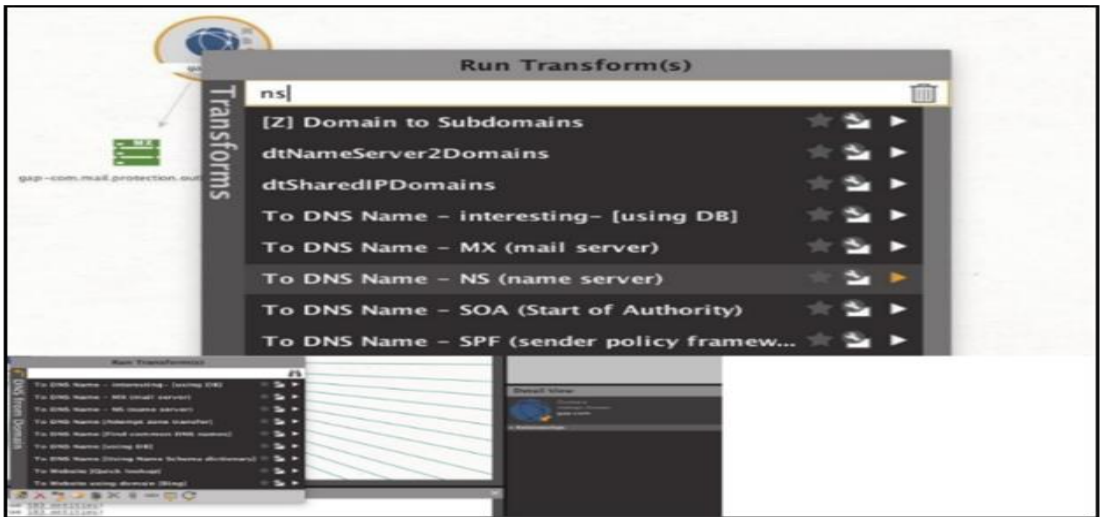
การเชื่อมโยงเหล่านี้สามารถใช้ประโยชน์ได้ในการค้นหาโดเมนอื่น ๆ ของบุคคลเดียวกัน แต่ในบางกรณีโดเมนที่ได้อาจไม่ได้รับการยอมรับอย่างเป็นทางการ ทำให้ผู้โจมตีสามารถค้นพบส่วนที่เชื่อมโยงกันขององค์กรได้ การติดตามว่าองค์กรเหล่านั้นติดตามผู้ใช้อย่างไร องค์กรส่วนใหญ่จะใช้รหัสติดตามเหมือนกันเพื่อช่วยในการวิเคราะห์โครงสร้างความสัมพันธ์ในองค์กรให้ง่ายขึ้น

๓.๒.๑.๓ ขั้นตอนที่ ๓ การเปิดเผยชื่อ DNS ที่เป็น Mail Server (MX) ของโดเมนสามารถแจ้งเตือนเกี่ยวกับบริการ E-mail ที่องค์กรใช้และบริการของโฮสต์ได้ โดยบางองค์กรจะมีโฮสต์เซิร์ฟเวอร์เหล่านี้อยู่ภายใน ซึ่งส่วนใหญ่ไม่ได้ใช้บริการของบุคคลที่สาม(เซิร์ฟเวอร์ E-mail ที่ไม่ใช่ขององค์กร) ข้อมูลนี้เป็นประโยชน์สำหรับแฮกเกอร์เนื่องจากสามารถนำข้อมูลไปใช้ในเชิงลึกได้ เช่น การโทรหาบริษัท จากผู้ให้บริการเฉพาะรายที่ใช้อินเทอร์เน็ตหรือเว็บไซต์ การค้นหาข้อมูลนี้สามารถทำได้โดย คลิกขวาที่โดเมนที่เราสร้างขึ้นก่อนหน้านี้และพิมพ์ "mx" (ตัวแปรแทนชื่อของ Server E-mail) ในแถบค้นหาเพื่อดู Conversion ที่จะแก้ไขเซิร์ฟเวอร์ MX จากนั้นคลิกที่ปุ่มสัญลักษณ์  เพื่อแสดงข้อมูล MX ซึ่งมีระบุว่าผู้ให้บริการรายใดใช้



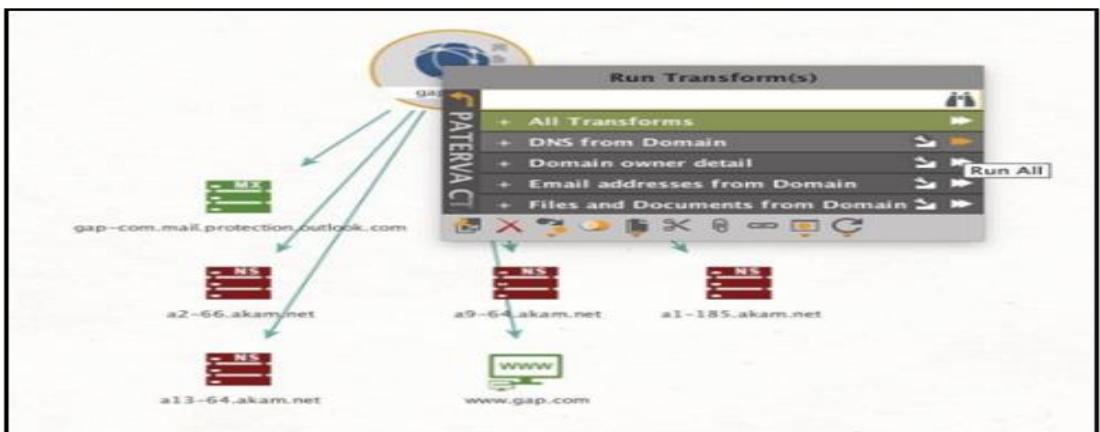
ภาพที่ ๑๖ ขั้นตอนที่ ๓ การเปิดเผยชื่อ & MX Server เซิร์ฟเวอร์ NS และ MX

หากต้องการดูระเบียบ NS ของไซต์เราสามารถคลิกขวาที่โดเมนและพิมพ์ "ns" เพื่อดูการแปลงที่เกิดกับเซิร์ฟเวอร์ เลือก "To DNS - NS (Name Server)" เพื่อรับข้อมูลเซิร์ฟเวอร์ โดยสามารถให้ข้อมูลเกี่ยวกับองค์กรว่ากำลังใช้บริการของบุคคลที่สามเพื่อโฮสต์โดเมนของตนหรือไม่ หากต้องการดูระเบียบ NS ของไซต์เราสามารถคลิกขวาที่โดเมนและพิมพ์ "ns" เพื่อดูการแปลงที่เกิดกับเซิร์ฟเวอร์ แล้วเลือก "To DNS Name - NS (Name Server)" เพื่อรับข้อมูลเซิร์ฟเวอร์ โดยสามารถให้ข้อมูลเกี่ยวกับองค์กรว่ากำลังใช้บริการของบุคคลที่สามเพื่อโฮสต์โดเมนของตนหรือไม่



ภาพที่ ๑๗ To DNS Name - NS (Name Server)

๓.๒.๑.๔ ขั้นตอนที่ ๔ หากต้องการเรียกใช้กลุ่มข้อมูลทั้งหมดให้คลิกขวาที่หน่วยโดเมนที่เราเพิ่มไว้ก่อนหน้านี้ แล้วเลือก "PATERVA CTAS" เพื่อเรียกใช้การแสดงกลุ่มการเปลี่ยนแปลงต่าง ๆ คุณสามารถเลือกไอคอน "All Transforms" ถัดจากการแปลง "DNS from Domain" ที่กำหนดให้ดำเนินการแปลงทั้งหมดที่มีอยู่



ภาพที่ ๑๘ ขั้นตอนที่ ๔ หากต้องการเรียกใช้กลุ่มข้อมูล

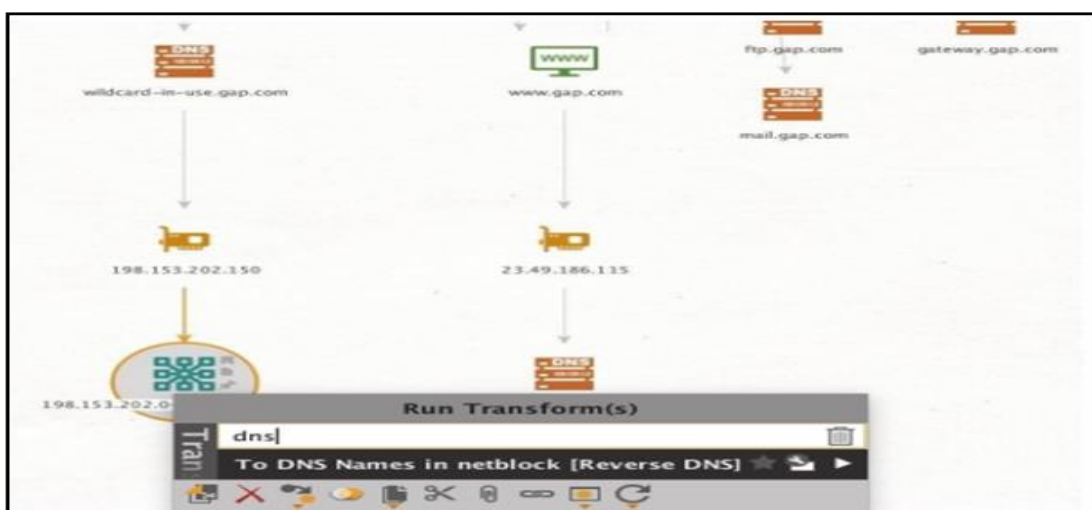
เมื่อการแปลงข้อมูลเหล่านี้เสร็จสิ้นแล้วจะเห็นผลการค้นหาด้านล่าง ซึ่งเป็นผลมาจากข้อมูลความสัมพันธ์ในโดเมน single, gap.com การดึงเหล่านี้เราจะพบ ๑๘๓ ระเบียบ โดย DNS เพียงอย่างเดียวจะมีระเบียบ NS และ MX เพิ่มเติม นอกจากนี้เรายังสามารถดูเว็บไซต์อื่น ๆ ที่เชื่อมโยงกับโดเมนได้

๓.๒.๑.๕ ขั้นตอนที่ ๕ ค้นหาที่อยู่ IP หลังจากที่เรามีชุดระเบียบ DNS เราสามารถนำข้อมูลเหล่านี้ไปใช้ในการค้นหาไปยังที่อยู่ IP เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับ Service ที่องค์กรขนาดใหญ่หลายแห่งจะเป็นเจ้าของเครือข่ายในการให้บริการของตนเองและเป็นโอกาสในการหาข้อมูลเพิ่มเติมซึ่งสามารถเริ่มต้นค้นหาได้ว่าเป็นโฮสต์ภายในหรือภายนอก ต่อมาคือวิธีใช้ Maltego เพื่อจับภาพเครือข่ายทั้งหมดโดยใช้ชื่อโดเมนเดียว สามารถทำได้โดยการเลือกระเบียบ DNS ที่พบจากนั้นคลิกขวาที่ไฟล์เหล่านั้นเพื่อรับแพ็คเกจการแปลง ซึ่งจะมีการเปลี่ยนแปลงเพียงอย่างเดียว ดังนั้นจึงสามารถเลือก "เรียกใช้ทั้งหมด" เพื่อเชื่อมโยงระเบียบ DNS ที่อยู่ของ IP โดยจะมีข้อมูลมากมายเกี่ยวกับเครือข่ายขนาดใหญ่ที่ประกอบขึ้นด้วยโครงสร้างพื้นฐานที่เชื่อมต่อ



ภาพที่ ๑๙ ขั้นตอนที่ ๕ ค้นหาที่อยู่ IP

๓.๒.๑.๖ ขั้นตอนที่ ๖ ค้นหาบล็อกเครือข่าย IP บล็อกเครือข่ายเป็นกลุ่มที่อยู่ของ IP ขนาดใหญ่ ซึ่งโดยปกติจะถูกกำหนดให้กับเอนทิตีตัวเดียวเมื่อสามารถระบุ Netblock ที่เป็นขององค์กรเป้าหมายสามารถทำทุกอย่างได้ การสแกนที่อยู่ IP ภายในช่วงเพื่อค้นหาบริการที่ยังไม่ได้ค้นพบ หากต้องการค้นพบ Netblocks ที่องค์กรเป้าหมายสามารถเป็นเจ้าของได้ สามารถเลือกที่อยู่ IP ที่ได้ค้นพบก่อนหน้านี้และคลิกขวาเพื่อเลือกการแปลง Maltego หนึ่งในสามเพื่อค้นหา Netblock ได้ด้วยการพิมพ์ "netblocks" ในแถบค้นหา เมื่อ Maltego พบ Netblock จะสามารถขยายการค้นหาของ DNS อื่น ๆ ภายใน Netblock ได้ โดยคลิกขวาที่ Netblock จากนั้นเลือกการแปลง "To DNS Names in Netblock"



ภาพที่ ๒๐ ขั้นตอนที่ ๖ ค้นหาบล็อกเครือข่าย IP

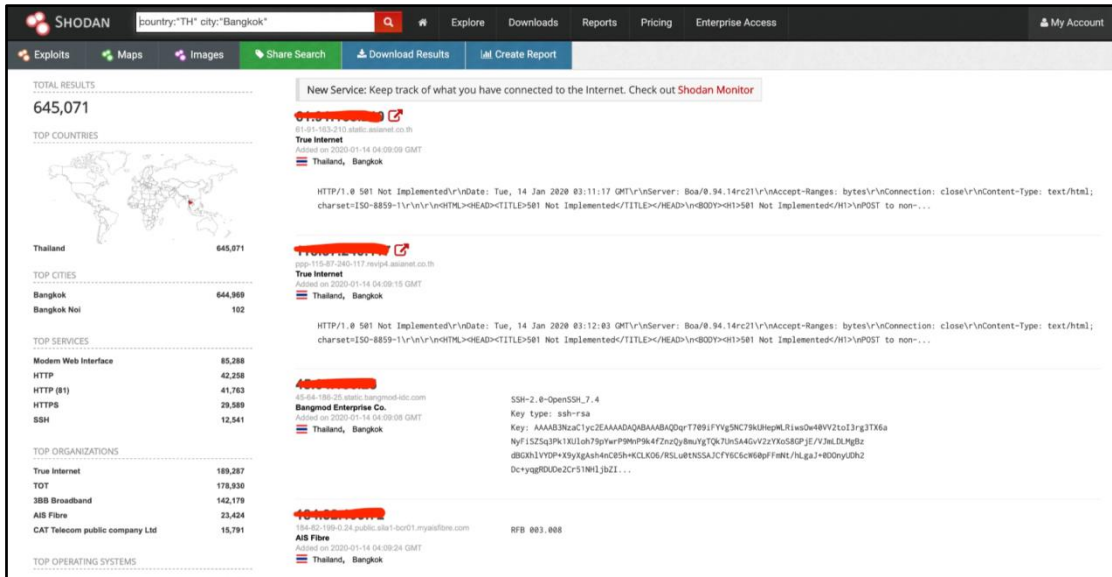
๓.๒.๑.๗ ขั้นตอนที่ ๗ ระบุหมายเลข Access Systems (AS) เมื่อมีกลุ่มที่เป็นสมาชิกขององค์กรเป้าหมายแล้ว หมายเลข AS จะถูกใช้อ้างอิงองค์กรขนาดใหญ่ ซึ่งมักเป็นผู้ให้บริการอินเทอร์เน็ต ทั้งนี้เราต้องการระบุพื้นที่บล็อกเครือข่ายที่มีโปรโตคอลใช้งานเส้นทางเดียวกัน ถ้าสามารถระบุหมายเลข AS ของเป้าหมายได้ เราจะสามารถหาบล็อกเครือข่ายทั้งหมดได้เช่นกัน จากนั้นจะค้นพบชื่อ DNS ทั้งหมดที่อยู่ในแต่ละบล็อกเครือข่ายเหล่านั้น และเพื่อให้สามารถแก้ไขชื่อ DNS เหล่านั้นลงในที่อยู่ IP ของบริการเป้าหมายอื่น ๆ ได้ จึงจำเป็นต้องระบุหมายเลข AS ในขั้นตอนนี้ด้วย



ภาพที่ ๒๑ Logo ของเว็บไซต์ Shodan

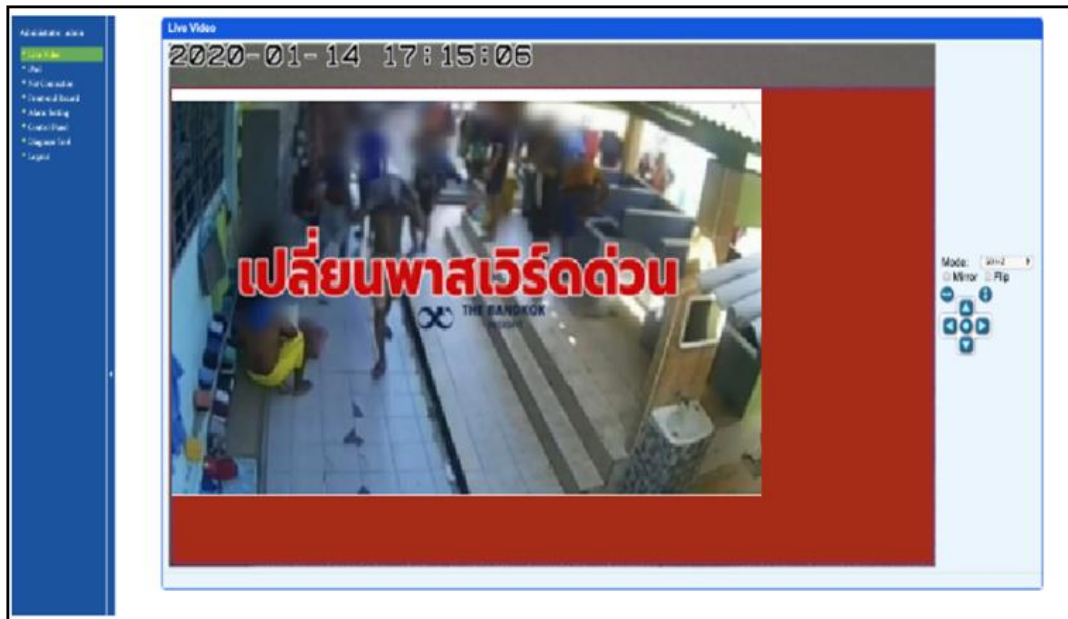
๓.๒.๒ Shodan คือเว็บไซต์ Search Engine ที่ทำหน้าที่เหมือน Google แต่คนละ Concept โดย Shodan Concept คือสามารถทำการค้นหาอุปกรณ์ที่เชื่อมต่อ Internet หรือมีการ Online อยู่ได้ทั่วโลก เพียงกรอก Keyword เช่น Website URL, ยี่ห้อกล้อง CCTV, ชื่อ Server และอื่น ๆ เป็นต้น Google Hacking Shodan จะทำการค้นหาอุปกรณ์เหล่านี้ โดยดึงข้อมูลที่ได้รับการ Response จาก Banner (เป็นบริการที่ให้ข้อมูลของ Computer System, Network หรือ Services ต่าง ๆ ที่ Run อยู่บน Open Port) ตัวอย่าง Filters คำค้นหาเบื้องต้น Country - จำกัดประเทศ, City - จำกัดชื่อจังหวัด, OS - จำกัดระบบปฏิบัติการ, Port - จำกัดเลข Port ซึ่ง Shodan จะนำข้อมูลมาตรวจสอบ ช่องโหว่ในระบบความปลอดภัยของอุปกรณ์หรือระบบนั้น ๆ เพื่อเป็นแนวทางในการปรับปรุงแก้ไข ป้องกันการถูกเจาะระบบความปลอดภัยของอุปกรณ์เบื้องต้น หรือ คือผู้ใช้งานสามารถสวมบทบาทเป็น Hacker จำเป็น เพื่อไปทดสอบระบบหรืออุปกรณ์ของผู้อื่นได้ อีกทั้งยังเปิดให้สามารถนำ API ไปใช้เพื่อตรวจสอบความปลอดภัยของระบบได้ซึ่งผู้ไม่หวังดีอาจใช้ความสามารถของ Shodan ในการโจรกรรม ข้อมูล (Hack) ได้ เนื่องจากทุกวันนี้ อุปกรณ์ภายในองค์กรมีการเชื่อมต่อ Internet หรือเป็น Always Online เช่น กล้องวงจรปิด หรือ CCTV เป็นต้น จึงกลายเป็นภัยใกล้ตัวที่มักถูกมองข้ามไป

ทั้งนี้ความอันตรายอันดับต้น ๆ เมื่อทุกสิ่งเชื่อมต่อเข้ากับ Internet เนื่องจาก Shodan สามารถค้นหาข้อมูลของอุปกรณ์และระบบต่าง ๆ ที่เชื่อมต่อ Internet จากทั่วโลกได้นั้น ทำให้เกิดเป็นความอันตรายลำดับที่ ๑



ภาพที่ ๒๒ Shodan ค้นหาข้อมูลของอุปกรณ์

ผู้ใช้งานทั่วไปสามารถมีความเสี่ยงถูกผู้ไม่ประสงค์ดีเข้าถึงความเป็นส่วนตัวโดยที่ไม่รู้ตัว ซึ่ง Shodan สามารถสร้างความอันตรายได้มากกว่าที่คิด จากภาพที่จะเห็นได้ว่ามีอุปกรณ์หรือระบบที่ทำการเชื่อมต่อ Internet และพบช่องโหว่ทางด้านความปลอดภัย มากถึง ๖๕๕,๐๗๑ ช่องโหว่ แต่นี่เป็นการค้นหาภาพรวมแบบกว้าง ๆ หากต้องการจำกัดวงการค้นหาให้แคบลง สามารถเพิ่ม Keyword ที่เราต้องการได้ เช่น ต้องการตรวจสอบความปลอดภัยของกล้องวงจรปิด สามารถนำชื่อ Server Name หรือ Brand ของกล้อง ไปค้นหาเพิ่มร่วมกับค่า Filters ได้ เป็นต้น (ตัวอย่าง : ใช้ ipcamera เป็น Keyword) จะเห็นได้ว่าทางด้านซ้าย จะมีการบอกถึง ประเทศ จังหวัด บริการที่ใช้ ผู้ให้บริการ Internet หรือ ระบบปฏิบัติการ (OS) ที่อยู่ในขอบเขตของคำที่ทำการค้นหา ซึ่งสามารถจำกัดให้แคบลงได้มากกว่าเดิม เพียงคลิกเข้าไปที่หัวข้อทางด้านซ้าย เช่น ต้องการดูเฉพาะ Devices ที่ใช้ บริการ Internet ของ True เมื่อกดเลือกก็จะ Scope เหลือเพียง ๑๒ ชิ้น ตามตัวเลขด้านหลัง จากนั้นทำการเลือกมา ๑ ตัว เพื่อมาทดสอบความปลอดภัย โดยสามารถใช้ในการส่งกล้องวงจรปิดของผู้อื่นได้ โดยมีขั้นตอนในการปฏิบัติขั้นต้น ดังนี้



ภาพที่ ๒๓ หน้าจอแสดงผลของ IP Camera

๓.๒.๒.๑ ใช้เว็บ Shodan.io ทำการค้นหา หน้าเว็บที่ใช้เข้าไปดูกล้องวงจรปิด โดยหลักการคือ Shodan จะสแกนกวาด IP ทั้งโลกและรวบรวมว่า IP ไหนเปิด Port อะไรอยู่และถ้า Port นั้น เป็นเว็บไซต์ก็จะเก็บข้อความบนหน้าเว็บไซต์และข้อมูลอื่น ๆ ไว้ (HTTP Response Header) เพื่อให้คนให้สามารถค้นหาด้วยคำที่ตรงกัน (Keyword) ได้

๓.๒.๒.๒ สแกนกวาด IP ไปจนกว่าจะพบ Public IP ที่เป็นของผู้ดูแลระบบสามารถ เข้าไปดูกล้องวงจรปิด แม้ว่าหน้านั้นจะไม่มีลิงก์ไปจากเว็บไหน หรือแม้ว่า Google จะค้นหาไม่พบก็ตาม

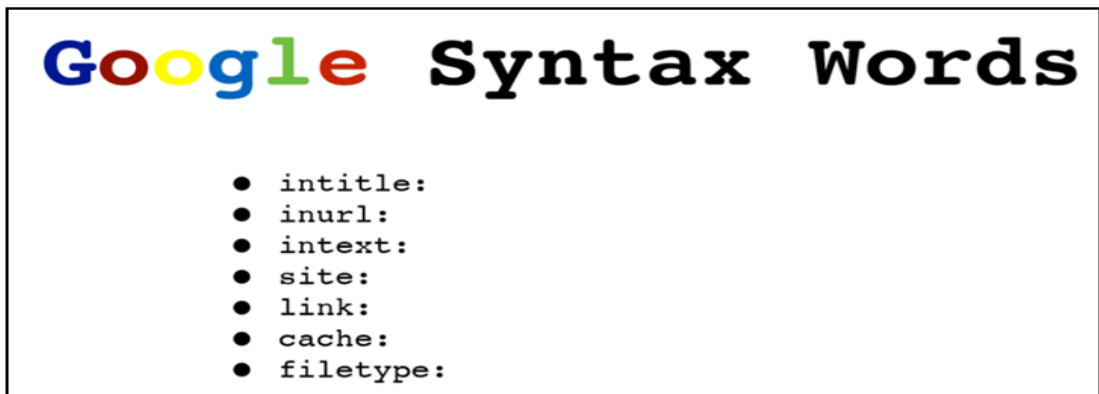
๓.๒.๒.๓ จากนั้นเข้าเว็บไซต์ไปดูกล้องวงจรปิด เมื่อมีข้อความเฉพาะ เช่น ชื่อรุ่นอยู่ ซึ่งเมื่อเราใช้ Shodan.io ค้นหา ถ้าเราใส่ข้อความเฉพาะ (Keyword) นี้ได้ถูกต้อง เราจะสามารถ ค้นหาเว็บสำหรับจัดการกล้องวงจรปิดที่เข้าผ่าน Public IP โดยไม่มีการป้องกันได้

๓.๒.๒.๔ เมื่อเข้าหน้าเว็บได้แล้ว จะถูกถามรหัสผ่าน ที่โดยปกติแล้วเมื่อติดตั้งกล้อง วงจรปิด เว็บที่แสดงภาพวงจรปิดจะถูกตั้งเป็นรหัสเริ่มต้น (Default Password) ถ้าไม่ได้ทำการแก้ไข โจรจะทำการลองเดารหัสเริ่มต้นหรือรหัสง่าย ๆ ไป ทำให้อาจจะสามารถเข้าไปดูกล้องวงจรปิดได้

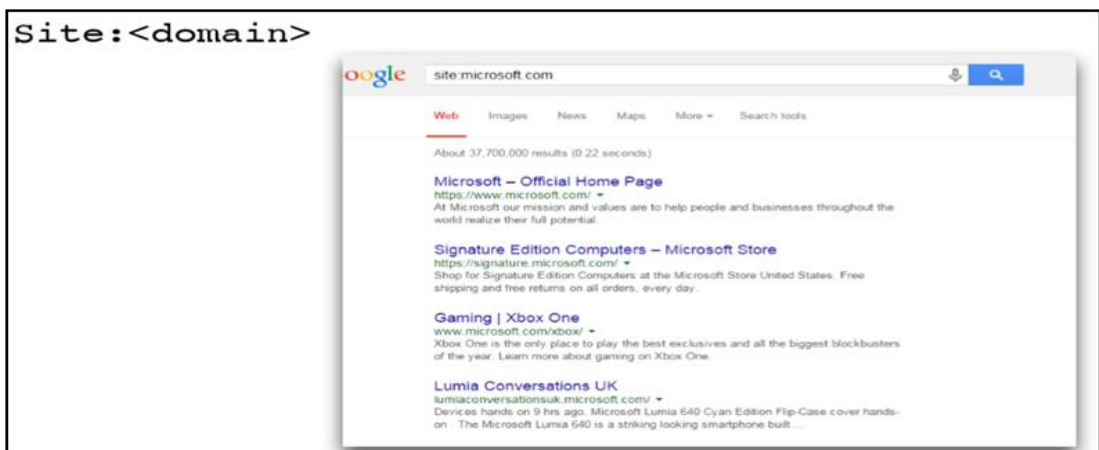
๓.๒.๒.๕ วิธีการแก้ไขคือ ควรแยก Network สำหรับใช้เข้าไปดูกล้องวงจรปิด ให้เป็น ระบบภายใน (Private Network) อาจจะต้องอยู่ในองค์กรหรือต่อผ่าน VPN ก่อนถึงเข้าหน้าเว็บกล้อง วงจรปิด พร้อมทั้งอัปเดตเฟิร์มแวร์ให้เป็นรุ่นล่าสุด และเปลี่ยนรหัสผ่านที่คาดเดาได้ยาก นอกจากนี้ Shodan ได้ร่วมมือกับ Recorded Future เพื่อพัฒนาระบบ Search Engine สำหรับค้นหา Malware Command & Control (C&C) Server โดยเฉพาะภายใต้ชื่อ Malware Hunter ที่เปิดให้บริการ อยู่ที่ <https://malware-hunter.shodan.io/> การทำงานจะการใช้ Search Bot ทำการ Crawl ไปทั้ง Internet เพื่อค้นหาเครื่อง Server หรืออุปกรณ์ที่มี IP Address จริง ซึ่งถูกตั้งค่าให้ทำหน้าที่ เป็น C&C Server ด้วยการใส่ Request หลากหลายรูปแบบที่ถูกออกแบบมาเพื่อตรวจสอบ Server แต่ละเครื่องว่าเป็น C&C Server หรือไม่นั่นเอง ซึ่ง Request เหล่านี้แท้จริงแล้วก็คือ Request สำหรับ

ปลอมตัวว่าเป็นเครื่องคอมพิวเตอร์ที่ติด Malware และพยายามติดต่อกลับไปยังเครื่อง C&C Server เพื่อหลอกให้ C&C Server ที่แอบแฝงอยู่บน Internet ตอบกลับมา จากนั้นจะทำการเก็บ IP Address ที่ตอบ Request เหล่านั้นเอาไว้ว่าเป็น IP Address ของเครื่องที่เป็น C&C Server พร้อมกับข้อมูลประกอบว่าเป็น C&C Server ของ Remote Access Trojan (RAT) ตระกูลใด เช่น Dark Comet, njRAT, Poison Ivy, Ghost RAT และอื่น ๆ เป็นต้น ปัจจุบัน Malware Hunter นี้ตรวจพบ C&C Server เกินกว่า ๕,๗๐๐ เครื่องไปเป็นที่เรียบร้อยแล้ว

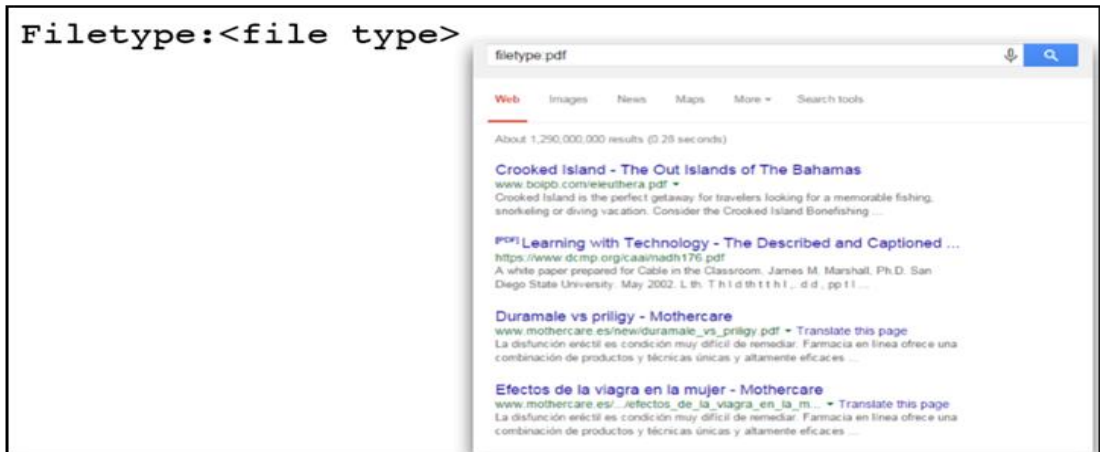
๓.๒.๓ Google Hacking เป็นการใช้คำค้นหากับเว็บไซต์ Google ที่ลงลึกในรายละเอียดได้ และยังสามารช่วยใ้เราตีกรอบข้อมูลจำเพาะในสิ่งที่เราสนใจได้ มีประโยชน์ช่วยในการค้นหาข้อมูลให้รวดเร็วและเจาะจงได้ดีขึ้น ตัวอย่างเช่น intitle, inurl, intext, site, link, cach และ filetype เป็นต้น



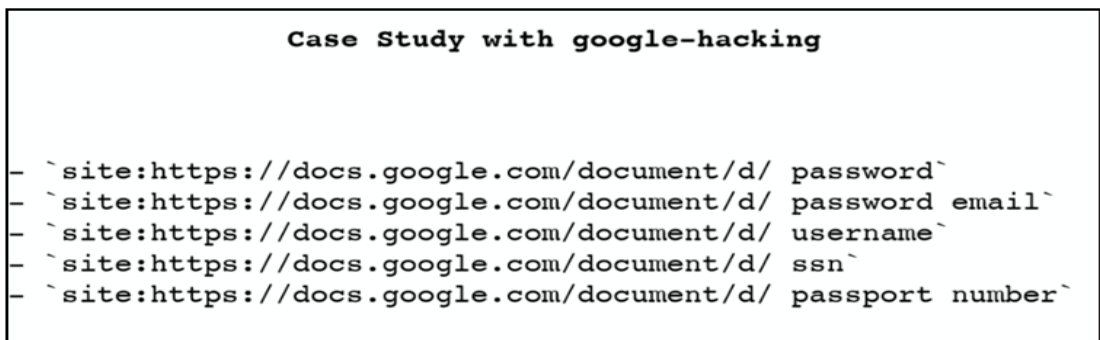
ภาพที่ ๒๔ การใช้คำค้นหาบนเว็บไซต์ Google



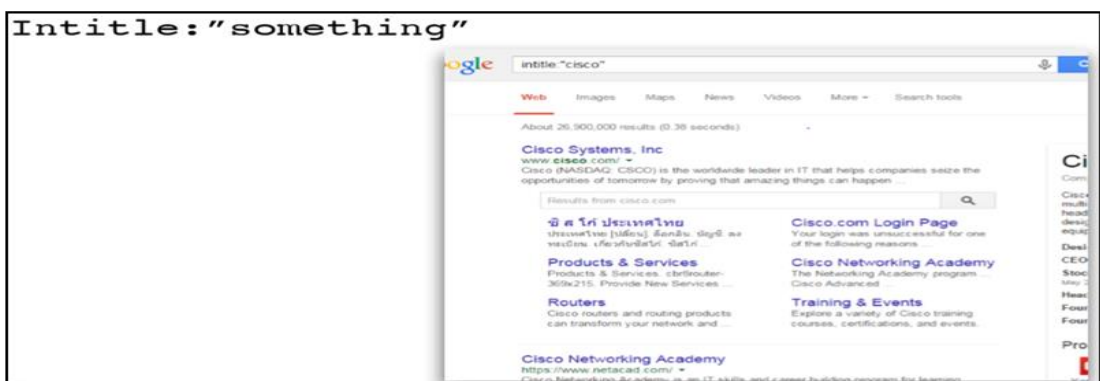
ภาพที่ ๒๕ Site domain



ภาพที่ ๒๖ Filetype



ภาพที่ ๒๗ Case Study

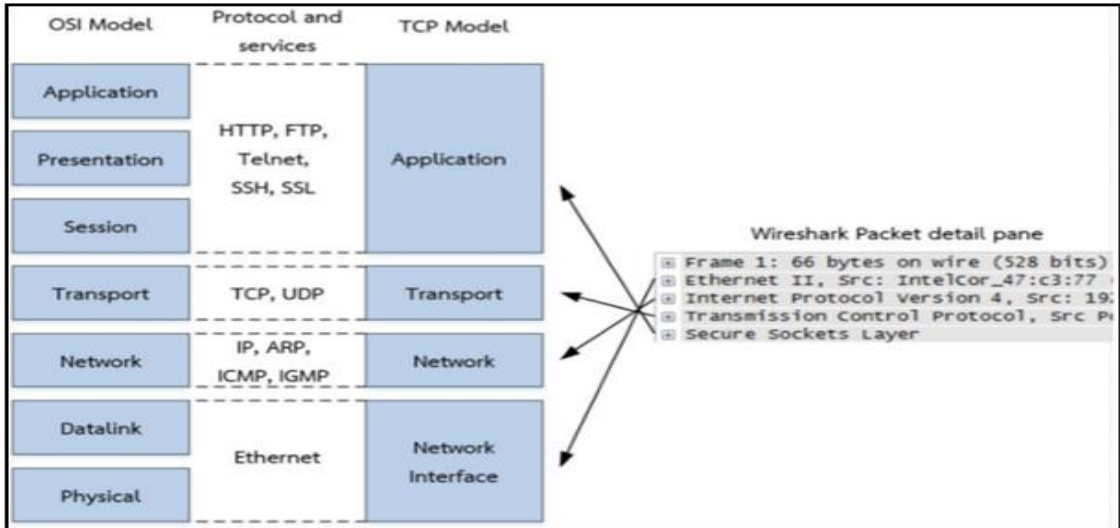


ภาพที่ ๒๘ Intitle

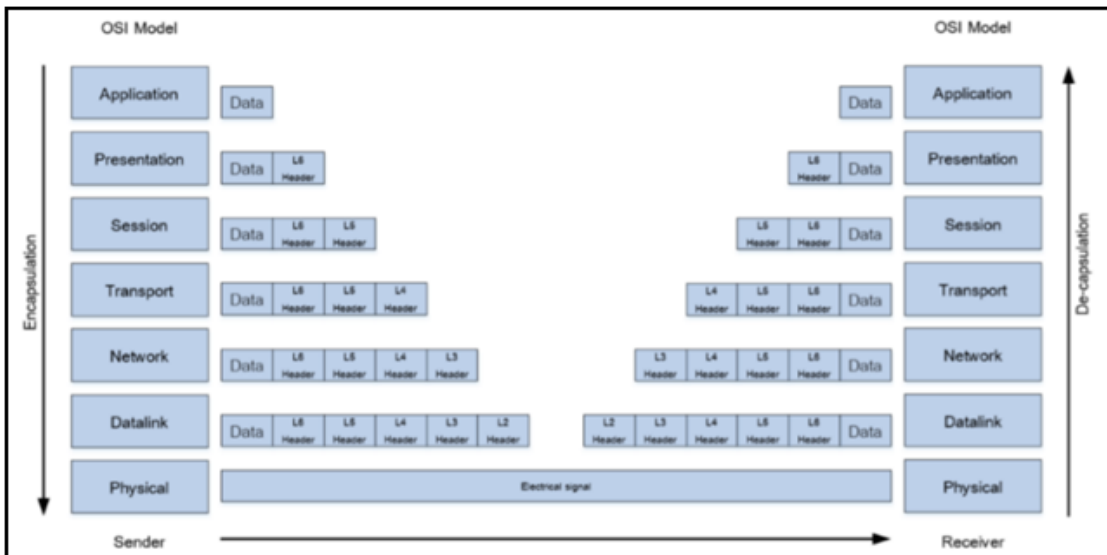
ทั้งนี้การใช้ประโยชน์จาก Google Hacking ก็จะไม่คล้าย ๆ กับตัว Shodan โดยกล่าวได้ว่า เป็นวิธีการใช้งานทั่วไปแบบที่ใช้กันในการค้นหาข้อมูลจากเว็บไซต์ Google แต่อีกหนึ่งสิ่งที่ Google ทำได้ก็คือ “การค้นหาข้อมูลแห่งช่องโหว่เพื่อใช้เป็นเครื่องมือในการแสกข้อมูล” การใช้งาน Google แบบเต็ม ๆ จึงเปลี่ยนไปเป็น “เครื่องมือชั้นยอดของเหล่าแฮกเกอร์ในการค้นหาเป้าหมายและค้นหาเครื่องมือโจมตีนั่นเอง”

๓.๓ พื้นฐานการใช้งาน Wireshark

Wireshark เป็นเครื่องมือที่ใช้สำหรับตรวจจับแพ็กเก็ตและวิเคราะห์ แพ็กเก็ตไปในตัวโดยจะมีผลต่อการวิเคราะห์ที่เมื่อเปรียบเทียบกับสถาปัตยกรรม OSI แล้วจะได้ ดังภาพที่ ๒๙



ภาพที่ ๒๙ โครงสร้างของ OSI 7 Layer เปรียบเทียบกับ TCP Model ในโปรแกรม Wireshark



ภาพที่ ๓๐ กระบวนการส่งข้อมูล จากบนลงล่าง จากซ้ายไปขวา

เมื่อมีการรับส่งข้อมูลระหว่างสองระบบผ่านสถาปัตยกรรม OSI Model ข้อมูลจะเริ่มส่งจาก Application ไปสู่ Presentation และ Presentation ส่งต่อให้ Session เป็นแบบนี้ไปเรื่อย ๆ จนสิ้นสุดที่ Physical จากนั้น Physical ก็จะทำการส่งผ่านสาย LAN หรือระบบ Wifi แล้วแต่กรณี เพื่อให้อีกฝั่งหนึ่งรับข้อมูล โดยในกระบวนการรับข้อมูลจะเริ่มจาก Physical อ่านค่าสัญญาณจากสาย LAN หรือ Wifi แล้วส่งค่าที่ได้ไปให้กับ Datalink แล้วส่งต่อไปแบบนี้เรื่อย ๆ จนสุดที่ Application

ซึ่งถ้าหากมีกระบวนการประมวลผลสิ้นสุดไปก่อน ก็อาจไม่จำเป็นต้องส่งขึ้นไปจนถึงจุดสูงสุดก็ได้ แต่ถ้าเป็นการส่งจากกรณีแรกจะต้องส่งลงมาให้สุดเท่านั้น

๓.๓.๑ ตัวอย่างสิ่งที่พบอยู่ในแต่ละ Layer มีดังนี้

๓.๓.๑.๑ Layer 1 (Physical Layer) เช่น สาย LAN, อุปกรณ์ Wifi, เเราเตอร์ และ Switch เป็นต้น

๓.๓.๑.๒ Layer 2 (Data link Layer) เช่น MAC Address เป็นต้น

๓.๓.๑.๓ Layer 3 (Network Layer) ในระบบเน็ตเวิร์คจะมีการใช้โปรโตคอล TCP/IP เป็นหลัก ดังนั้นข้อมูลที่ใช้อ้างอิงคือ IP Address

๓.๓.๑.๔ Layer 4 (Transport Layer) หากต้องการความแม่นยำใช้ TCP หากต้องการความรวดเร็วใช้ UDP

๓.๓.๑.๕ Layer 5 (Session Layer) คอมพิวเตอร์ต้องทำงานได้มากกว่า ๑ ช่องทาง ดังนั้นจึงต้องมี Port เป็นช่องทางหรือ Session ในการติดต่อสื่อสาร เช่น เว็บไซต์ใช้ Port 80 ในขณะที่การแชร์ไฟล์ใช้ Port 21 เป็นต้น

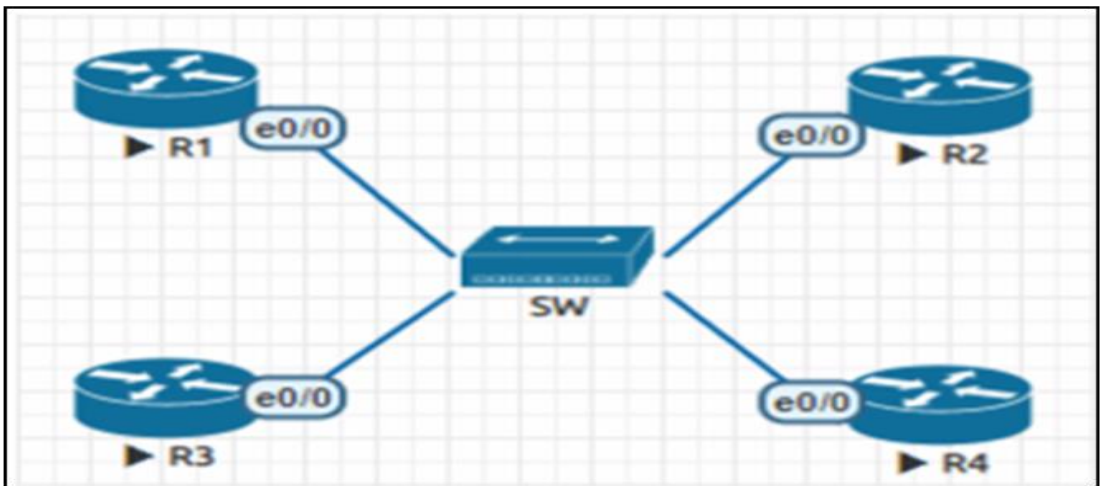
๓.๓.๑.๖ Layer 6 (Presentation Layer) เป็นการระบุชนิดของข้อมูลที่สื่อสารออกไปว่าเป็นชนิดใด เช่น ในการเปิดเว็บเพจหนึ่งหน้าจะมีส่วนประกอบอื่น ๆ เพื่อให้เว็บเพจทำงานอยู่หลายตัว เช่น HTML, Java Script และ Video Streaming เป็นต้น สิ่งเหล่านี้ที่เราเรียกว่า Presentation

๓.๓.๑.๗ Layer 7 (Application Layer) คือโปรแกรมที่ทำงานหรือเรียกใช้งานระบบต่าง ๆ โดยจะรับข้อมูลมาจากเลเยอร์ต่าง ๆ ที่กล่าวมาทำงาน

๓.๓.๒ โพรโทคอล ARP

เป็นโพรโทคอลที่มีการทำงานอยู่ใน Layer 2 ของแบบจำลอง OSI โดยทั่วไปแล้วองค์กรส่วนใหญ่ ที่มีการใช้งานระบบเครือข่ายจะมีการเชื่อมต่ออุปกรณ์ในระบบเครือข่ายเข้าด้วยกัน โดยใช้มาตรฐาน Ethernet ดังนั้น ข้อมูลที่อยู่ใน Layer 2 ของ Ethernet ก็คือ MAC Address ใน Layer 2 ของแบบจำลอง OSI จะเป็นการเชื่อมต่อกันในลักษณะ “จุดต่อจุด” ซึ่งจะมองการเชื่อมต่อเพื่อส่งข้อมูลกันในระยะสั้น ๆ คือจาก MAC Address บนการ์ด LAN บนเครื่องคอมพิวเตอร์ไปยัง MAC Address บนเครือข่ายของสวิตช์ที่เชื่อมต่ออยู่กับการ์ด LAN นั้น ๆ เป็นอันสิ้นสุดการสื่อสารใน Layer 2 ของ แบบจำลอง OSI ในกรณีที่ต้องการส่งข้อมูลไปที่จุดอื่น ใน Layer 2 ของแบบจำลอง OSI จะเป็นหน้าที่ของ สวิตช์ซึ่งจะต้องทำการค้นหา MAC Address ของอุปกรณ์ปลายทางที่เครื่องคอมพิวเตอร์นั้นต้องการที่จะติดต่อด้วยว่าต้องทำการส่งข้อมูลไปที่ปลายทางที่การเชื่อมต่อใดของสวิตช์ โดยการค้นหา MAC Address ของสวิตช์นั้นจะต้องมีกระบวนการ “จับคู่” ข้อมูลของ MAC Address ใน Layer 2 และ IP Address ใน Layer 3 ของแบบจำลอง OSI ซึ่งกระบวนการทำงานในการจับคู่ระหว่าง MAC Address และ IP Address เข้าด้วยกันนี้ จะมีการทำงานผ่านโปรโตคอล ARP โดยการทำงานของโปรโตคอล ARP จะมีอยู่ ๒ ขั้นตอนคือ ARP request และ ARP reply โดย ARP จะเกิดขึ้นก็ต่อเมื่ออุปกรณ์นั้นไม่ทราบ MAC Address ของอุปกรณ์ในเครือข่ายเดียวกันที่ต้องการที่จะติดต่อด้วย ขั้นตอนนี้จะมีการส่ง IP Address

ที่ต้องการทราบออกไปพร้อมกับ Broadcast Destination MAC Address กระจายออกไปในเครือข่าย ด้วย MAC Address ปลายทางคือ FFFF.FFFF.FFFF พร้อมกับส่ง MAC/IP Address ของเครื่องต้นทางออกไปด้วย เมื่อเครื่องปลายทางที่มี IP Address ตรงกับเครื่องต้นทางประกาศหา ก็จะตอบกลับด้วย ARP reply แพ็กเก็ตซึ่งจะมีข้อมูล IP/MAC Address ของเครื่องปลายทางกลับไปให้เครื่องต้นทาง ในกรณีที่ต้องการเห็นการทำงานของโปรโตคอล ARP ให้ได้ชัดเจนนั้นจะต้องนำโปรแกรม Wireshark หรือ TCPDump มาช่วยในการจับแพ็กเก็ตขึ้นมาแสดงผล ในกรณีตัวอย่างเราสามารถนำโปรแกรม EVE-NG มาประยุกต์ใช้งานในการเรียนรู้การทำงานของโปรโตคอลต่างๆได้อย่างง่ายดาย รวมทั้งในกรณีที่เป็น โปรโตคอล ARP ก็เช่นกัน จากในรูปที่ ๓๑ เราจะทำการต่อ Topology โดยมี PC ทั้งหมด ๔ เครื่อง เชื่อมต่อกันผ่านสวิตช์ ให้ทำการจับแพ็กเก็ตที่เครือข่ายใดเครือข่ายหนึ่งของสวิตช์ เพื่อสังเกตการทำงาน ในบางครั้งเราอาจจะไม่เห็นโปรโตคอล ARP อยู่ในส่วนของแพ็กเก็ตที่แสดงผลในโปรแกรม Wireshark จะต้องทำการเคลียร์ ARP บนอุปกรณ์เพื่อให้อุปกรณ์ทำการสร้าง ARP Request ก่อน



ภาพที่ ๓๑ การเชื่อมต่อ Topology ในโปรแกรม EVE-NG เพื่อศึกษาการทำงานของ ARP

เมื่อโปรโตคอล ARP แสดงผลที่โปรแกรม Wireshark แล้วจะลองมาทำการเปรียบเทียบที่ได้จากโปรแกรม Wireshark กับทฤษฎีก่อนหน้านี้ที่ว่าในกระบวนการส่ง ARP Request นั้น ต้องมีการส่ง IP/MAC Address ของเครื่องต้นทางออกไป พร้อมกับ Broadcast Destination Address ที่เป็น MAC Address FFFF.FFFF.FFFF เมื่อลองดูแพ็กเก็ตที่โปรแกรม Wireshark แสดงผลในรูปแบบพบว่าในโปรโตคอล ARP แพ็กเก็ตแรกจะมีการส่งข้อมูลตามที่ได้กล่าวไว้ในทฤษฎีจริงตามผล

Source	Destination	Protocol	Frame Leng!	Info
00:00:00:00:00:01	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.10.10.2? Tell 10.10.10.1
00:00:00:00:00:02	00:00:00:00:00:01	ARP	60	10.10.10.2 is at 00:00:00:00:00:02

ภาพที่ ๓๒ แพ็กเก็ตของ ARP ที่โปรแกรม Wireshark ได้รับเข้ามา

๓.๓.๓ รายละเอียดของแพ็กเก็ต ARP Request

การทำงานของโปรโตคอล TCP ในส่วนนี้จะกล่าวถึงการทำงานของโปรแกรมที่ต้องการใช้งานอยู่บนโปรโตคอล TCP ซึ่งเป็นโปรแกรม ประเภทที่ต้องการความถูกต้องของข้อมูล ในการสื่อสารบนระบบเครือข่าย โดยทั่วไปแล้วการสื่อสารโดยใช้ โปรโตคอล TCP จะเป็นการสื่อสารแบบ Client-Server การสื่อสารกันจะต้องเริ่มต้นด้วยการส่งคำขอใช้งาน จากเครื่อง Client ไปที่เครื่อง Server ซึ่งการเริ่มต้นการสื่อสารนี้จะต้องเริ่มต้นด้วยการส่งแพ็กเก็ต Syn จาก เครื่อง Client ไปหาเครื่อง Server หลังจากนั้นเครื่อง Server จะทำการตอบรับแพ็กเก็ต Syn กลับไปที่เครื่อง Client เป็นแพ็กเก็ต Syn/ACK เมื่อเครื่อง Client ได้รับการตอบรับจากเครื่อง Server ก็จะมีการส่งแพ็กเก็ต ACK กลับไปที่เครื่อง Server เพื่อเป็นการยืนยันและเริ่มต้นการส่งข้อมูลต่อไป สำหรับขั้นตอนการส่งแพ็กเก็ต Syn – Sync/ACK – ACK ที่มีลำดับขั้นตอนแบบนี้ จะถูกเรียกว่ากระบวนการ Three Way Handshaking ของโปรโตคอล TCP นั่นเอง เมื่อสิ้นสุดกระบวนการ Three Way Handshaking แล้ว เครื่อง Client ที่ต้องการรับข้อมูลจะส่งแพ็กเก็ต REQ ไปแจ้งให้ Server ส่งข้อมูลกลับมาให้ เมื่อเครื่อง Server ได้รับ REQ แล้วเครื่อง Server ก็จะเริ่มส่งข้อมูลมายังเครื่อง Client โดยในขั้นตอนนี้จะมีการแจ้งขนาดของ Window Size ที่ใช้ในการรับส่งข้อมูลระหว่างกันด้วย เป็นการกำหนดขนาดของการส่งข้อมูลให้มีความสัมพันธ์กันกับข้อมูลที่ถูกรับและส่ง โดยกระบวนการนี้จะอยู่ในส่วนของ Data Transfer และ ขั้นตอนสุดท้าย เมื่อเครื่อง Server ส่งข้อมูลให้กับเครื่อง Client จนครบแล้ว เครื่อง Server จะทำการส่งแพ็กเก็ต FIN ไปแจ้งให้เครื่อง Client ทราบว่าสิ้นสุดการส่งข้อมูลแล้ว หลังจากนั้นเครื่อง Client จะทำการตอบกลับด้วยแพ็กเก็ต FIN/ACK เพื่อตอบรับการปิดการสื่อสาร เมื่อเครื่อง Server ได้ รับแพ็กเก็ตแล้วก็จะส่งแพ็กเก็ต ACK ตอบกลับ เพื่อทำการปิดการสื่อสารเช่นกัน เป็นอันจบกระบวนการสื่อสารในแบบ TCP กระบวนการนี้จะอยู่ในส่วนของ Close Connection สำหรับกระบวนการทั้งหมดจะแสดงดังภาพที่ ๓๓

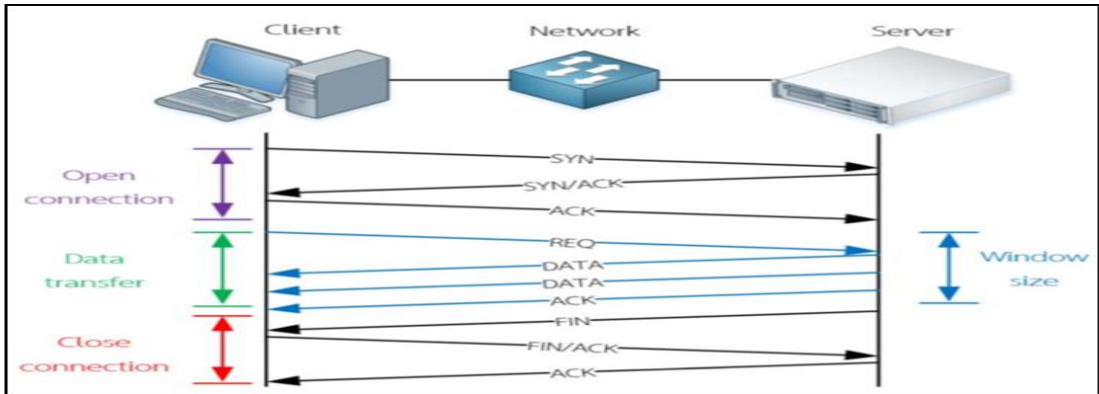
จากคำอธิบายข้างต้นเมื่อนำมาประยุกต์ใช้ในการแก้ไขปัญหาที่เกี่ยวข้องกับระบบเครือข่ายสรุปเป็นข้อ ๆ จะได้ดังต่อไปนี้

๓.๓.๓.๑ ถ้าไม่พบแพ็กเก็ต SYN จากเครื่อง Client ไปที่เครื่อง Server จะทำให้พบปัญหาที่เกี่ยวกับการเชื่อมต่อ คือเครื่อง Client ไม่สามารถเชื่อมต่อกับ Server ได้

๓.๓.๓.๒ ถ้าเครื่อง Client ไม่ส่งแพ็กเก็ต ACK กลับไปที่ Server ก็จะไม่สามารถติดต่อกับ Server ได้เช่นเดียวกัน

๓.๓.๓.๓ ถ้าไม่มีการส่งแพ็กเก็ต FIN ก็จะไม่เกิดขั้นตอนการปิดการสื่อสาร

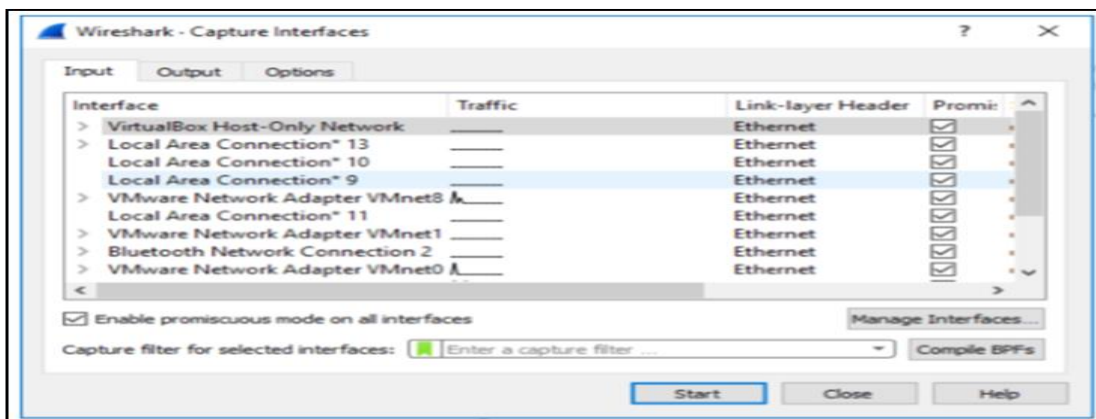
๓.๓.๓.๔ ฝั่งใดที่มีการส่ง FIN Packet ออกมาแสดงว่าฝั่งนั้นต้องการขอปิดการสื่อสาร



ภาพที่ ๓๓ Client, Network, Server

จากภาพที่ ๓๓ คือ ตัวอย่างการสื่อสารโดยใช้โปรโตคอล TCP เนื้อหาที่กล่าวมาเป็นเพียงตัวอย่างการสรุปข้อมูลเบื้องต้นที่ได้จากรูปแบบการสื่อสารโดยใช้โปรโตคอล TCP เท่านั้น ไม่ใช่ข้อมูลทั้งหมด การจะแสดงให้เห็นตัวอย่างคร่าว ๆ ในการสรุปปัญหาที่อาจจะเกิดขึ้นในระบบเครือข่ายเมื่อมีการใช้งานจริงนั้นยังคงเป็นเรื่องที่ต้องทำความเข้าใจและทดลองต่อ ๆ ไป โดยบางหน่วยงานอาจจะพบรูปแบบของแพ็กเก็ตที่แตกต่างจากที่ได้กล่าวไปในเบื้องต้นก็ได้ ซึ่งหากเรามีความเข้าใจถึงรูปแบบของการสื่อสารได้แล้ว การวิเคราะห์และแก้ปัญหาที่เกิดขึ้นก็จะอาศัยหลักการจากพื้นฐานการสื่อสารที่เราได้เรียนรู้กันมานั่นเอง ทั้งนี้ การเก็บข้อมูลในระบบเครือข่ายจะนิยมใช้โปรแกรม Wireshark โดยทั่วไปแล้วข้อมูลจะอยู่ในรูปแบบของไฟล์นามสกุล .pcap หรือ .pcapng ทั้งที่ได้จากตัวโปรแกรม Wireshark หรือจากโปรแกรม TCPDump บนระบบปฏิบัติการ Linux แต่ตัวโปรแกรม Wireshark ก็ยังสนับสนุนการอ่านข้อมูลจากไฟล์ชนิดอื่น ๆ ได้ด้วย เช่น .cap เป็นต้น

จากภาพที่ ๓๓ จะเห็นได้ว่าเราสามารถทำการเลือกระบบเครือข่ายที่ถูกแสดงอยู่ได้ในโปรแกรม Wireshark โดยโปรแกรมจะแสดงข้อมูลมาให้ทุกเครือข่ายที่มีการเชื่อมต่ออยู่กับคอมพิวเตอร์ เมื่อเราทำการเลือกแล้ว โปรแกรม Wireshark ก็จะเริ่มทำการเก็บข้อมูล จากเครือข่ายที่เราเลือกมาทั้งหมด สำหรับเครือข่ายที่สามารถใช้งานได้จะแสดงดังภาพที่ ๓๔



ภาพที่ ๓๔ รูปแสดงเครือข่ายบนคอมพิวเตอร์ที่โปรแกรม Wireshark ตรวจสอบได้

เมื่อโปรแกรม Wireshark เริ่มทำการเก็บข้อมูลจากเครือข่ายที่ได้เลือกไว้แล้ว Wireshark จะแสดงผลข้อมูลออกมาด้วยหน้าโปรแกรมดังภาพที่ ๓๕

No.	Time	Source	Destination	Protocol	Frame Length	Info
55	25.007311	111.221.77...	192.168.1.102	TCP	54	40018 → 50808 [ACK] Seq=19 Ack=7 Win=83 Len=0
56	25.110814	162.125.17...	192.168.1.102	TLSv1.2	388	Application Data
57	25.118831	192.168.1...	162.125.17.3	TLSv1.2	493	Application Data
58	25.234470	192.168.16...	192.168.160.2	NBNS	110	Refresh NB LENOVO-E130<20>
59	25.480144	192.168.1...	157.55.235.1...	UDP	183	64930 → 40018 Len=141
60	25.495295	192.168.1...	162.125.17.3	TCP	493	[TCP Retransmission] 50793 → 443 [PSH, ACK] Seq=1 Ack=335
61	25.509785	162.125.17...	192.168.1.102	TCP	54	443 → 50793 [ACK] Seq=335 Ack=440 Win=83 Len=0
62	25.788741	157.55.235...	192.168.1.102	UDP	63	40018 → 64930 Len=21
63	25.802813	162.125.17...	192.168.1.102	TCP	66	[TCP Dup ACK 61#1] 443 → 50793 [ACK] Seq=335 Ack=440 Win=

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: 68:17:29:47:c3:77, Dst: f8:d1:11:96:90:c2
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 119.235.235.84
> Transmission Control Protocol, Src Port: 50736, Dst Port: 443, Seq: 1, Ack: 1, Len: 12
> Transport Layer Security

```
0000 f8 d1 11 96 90 c2 68 17 29 47 c3 77 08 00 45 00  ....h. )G.w.E.  
0010 00 34 74 02 40 00 80 06 61 73 c0 a8 01 66 77 eb  -4t.~...as...fM  
0020 ab 54 c6 30 01 bb da 88 08 b7 09 01 cd ce 50 18  T0.....P.  
0030 00 fe 86 fb 00 00 80 02 00 06 00 00 00 04 00 00  .....  
0040 00 71  g
```

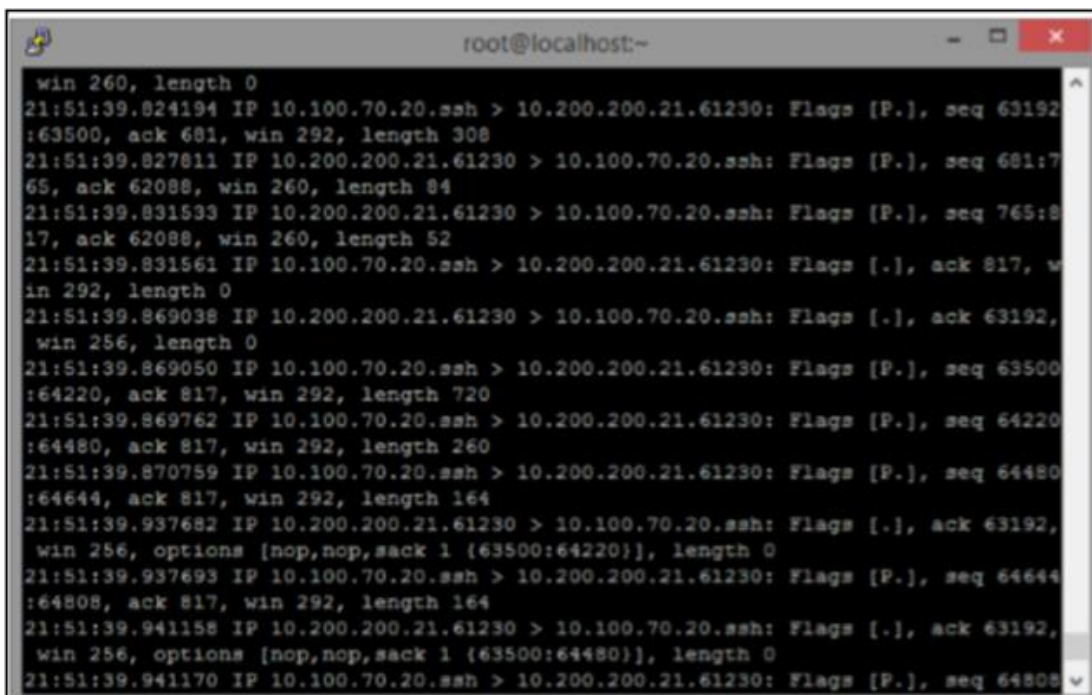
ภาพที่ ๓๕ การแสดงรายละเอียดของแพ็กเก็ตที่โปรแกรม Wireshark

เมื่อทำการเก็บข้อมูลเพื่อนำไปใช้งานได้ตามที่ต้องการแล้วให้ทำการบันทึกเป็นข้อมูลเพื่อนำไปวิเคราะห์ผลที่ได้ภายหลัง โดย Wireshark สามารถทำการบันทึกข้อมูลเก็บไว้ได้ในหลากหลายรูปแบบไฟล์ชนิดต่าง ๆ ที่โปรแกรม Wireshark สามารถจัดเก็บได้

การเก็บข้อมูลด้วย TCPDump โดยปกติแล้วระบบปฏิบัติการตระกูล Unix/Linux จะมีแพ็กเก็ตโปรแกรมพื้นฐานสำหรับการเก็บข้อมูลแพ็กเก็ตมาให้เป็นพื้นฐานเป็นปกติอยู่แล้วไม่จำเป็นต้องติดตั้งเพิ่มนั่นคือ TCPDump โดย TCPDump สามารถทำการเก็บข้อมูลแพ็กเก็ตได้เหมือนกับโปรแกรม Wireshark สำหรับการใช้งาน TCPDump นั้น จะมีการทำงานในลักษณะ Command Line ซึ่งจะต้องมีการระบุคำสั่ง เช่น โพรโทคอล เครือข่าย และขนาดของข้อมูลที่ต้องการจัดเก็บ เป็นต้น

๓.๓.๘ รูปแบบคำสั่งในการใช้งาน TCPDump จะมีโครงสร้าง ดังนี้

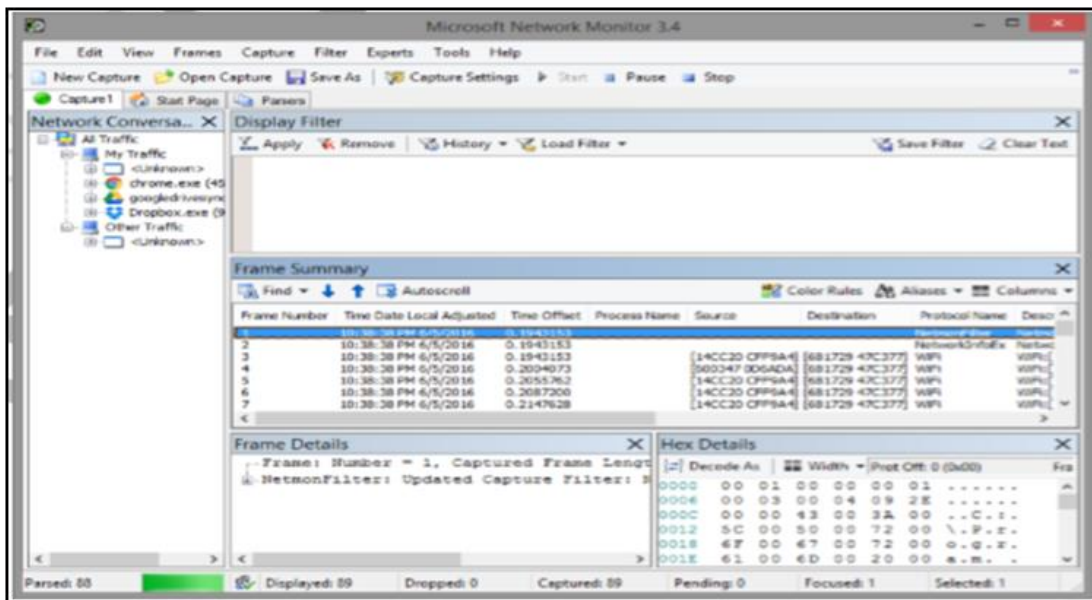
คำสั่ง `# tcpdump -i eth0 tcp dst port ๘๐๘๐ -w capfile.pcap` จากตัวอย่างคำสั่ง จะเป็นการสั่งให้ TCPDump ทำการเก็บข้อมูลที่เครือข่าย eth0 โดยจะต้องมี TCP ปลายทางเป็น Port 8080 หลังจากนั้นให้ทำการเขียนลงเก็บไว้เป็นไฟล์ชื่อ capfile.pcap และการใช้คำสั่งให้ TCPDump เพื่ออ่านไฟล์ที่ถูกเขียนไว้ชื่อ capfile.pcap ขึ้นมาแสดงผลด้วยคำสั่ง `# tcpdump -r capfile.pcap`



```
win 260, length 0
21:51:39.824194 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 63192
:63500, ack 681, win 292, length 308
21:51:39.827811 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Flags [P.], seq 681:7
65, ack 62088, win 260, length 84
21:51:39.831533 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Flags [P.], seq 765:8
17, ack 62088, win 260, length 52
21:51:39.831561 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [.], ack 817, w
in 292, length 0
21:51:39.869038 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Flags [.], ack 63192,
win 256, length 0
21:51:39.869050 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 63500
:64220, ack 817, win 292, length 720
21:51:39.869762 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 64220
:64480, ack 817, win 292, length 260
21:51:39.870759 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 64480
:64644, ack 817, win 292, length 164
21:51:39.937682 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Flags [.], ack 63192,
win 256, options [nop,nop,sack 1 (63500:64220)], length 0
21:51:39.937693 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 64644
:64808, ack 817, win 292, length 164
21:51:39.941158 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Flags [.], ack 63192,
win 256, options [nop,nop,sack 1 (63500:64480)], length 0
21:51:39.941170 IP 10.100.70.20.ssh > 10.200.200.21.61230: Flags [P.], seq 64808
```

ภาพที่ ๓๖ แสดงผลการใช้งาน TCPDump เพื่ออ่านข้อมูลแพ็กเก็ตที่ได้บันทึกเก็บไว้

๓.๓.๙ การเก็บข้อมูลด้วย Microsoft Network Monitor (GUI) สำหรับบางองค์กรที่มีกฎระเบียบเคร่งครัดในการจัดการโปรแกรมต่าง ๆ ที่ติดตั้งลงในเครื่อง เช่น มีข้อกำหนดให้ใช้โปรแกรมที่ต้องได้รับรองความถูกต้องปลอดภัยจาก Microsoft เท่านั้น ในกรณีที่ไม่ได้รับอนุญาตจะไม่สามารถติดตั้งโปรแกรมได้ ในกรณีที่ Microsoft Network Monitor จะเป็นตัวช่วยในการแก้ปัญหาในส่วนของ การเก็บข้อมูลเครือข่ายจากเครื่องที่ต้องการได้เช่นเดียวกัน สำหรับการทำงานของ Microsoft Network Monitor ก็จะมีหลักการเดียวกันกับโปรแกรม Wireshark แต่สามารถแยกแยะข้อมูลที่มี อยู่ออกมาได้ตามโปรแกรมที่มีการใช้งานอยู่



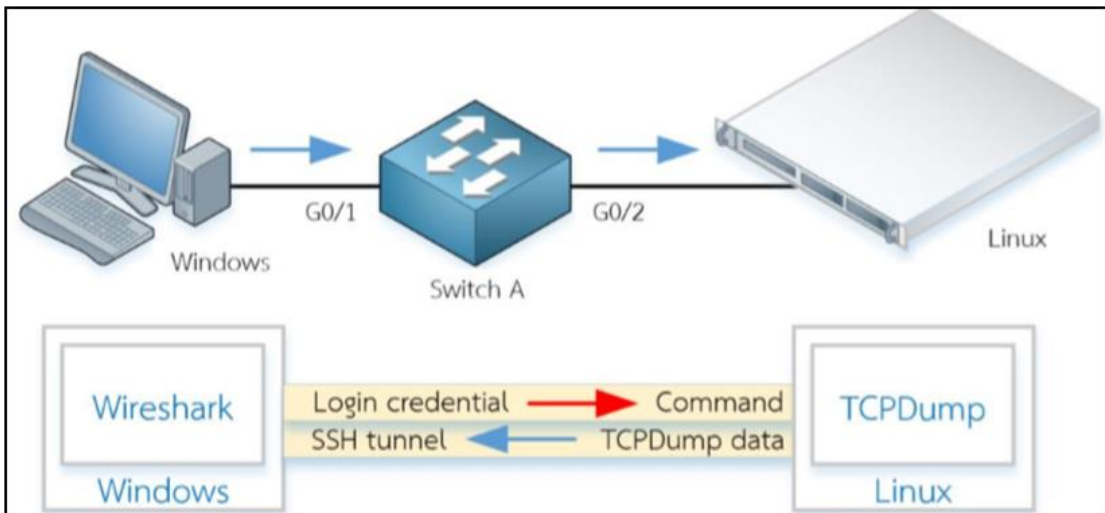
ภาพที่ ๓๗ โปรแกรม Microsoft Network Monitor

การเก็บข้อมูลด้วย Microsoft “netsh” (Command Line) กรณีนี้เป็นการใช้งานโปรแกรมที่มากับ Microsoft Windows เช่นเดียวกับกับ Network Monitor แต่จะมีข้อได้เปรียบมากกว่า Microsoft Network Monitor ตรงที่ netsh เป็นคำสั่งที่ถูกติดตั้งมาพร้อมกับ Windows เลยตั้งแต่ตอนติดตั้งไม่จำเป็นต้องดาวน์โหลดและติดตั้งโปรแกรมเพิ่มเติมอีก สำหรับการใช้งาน netsh จะเป็นในลักษณะ Command Line เท่านั้น ซึ่งอาจจะไม่สะดวกสำหรับท่านที่มีความคุ้นเคยกับการใช้งานโปรแกรมในลักษณะของ GUI สำหรับตัวอย่างการใช้งานโปรแกรม Microsoft netsh จะเป็นดังภาพที่ ๓๘



ภาพที่ ๓๘ ตัวอย่างการใช้งาน Microsoft netsh เพื่อเก็บข้อมูลในระบบเครือข่าย

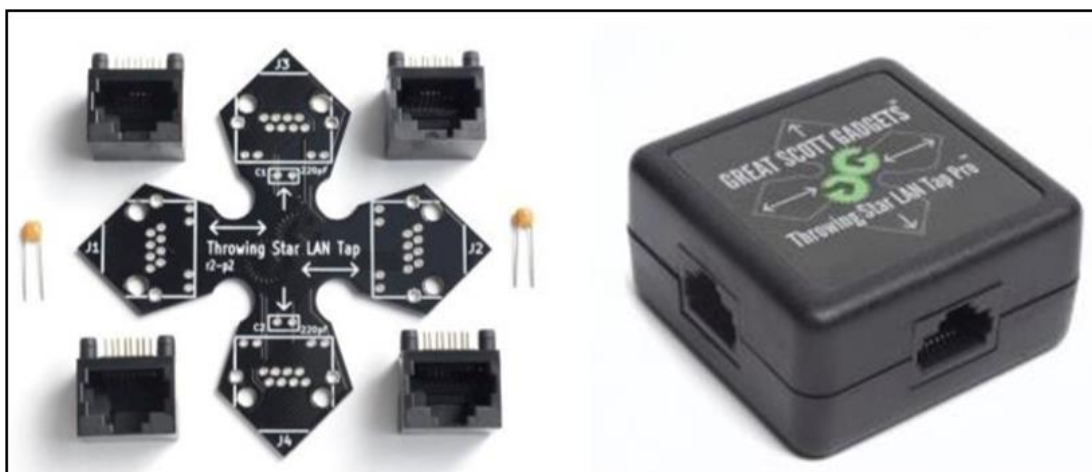
๓.๓.๑๐ การเก็บข้อมูลด้วยการทำ Remote capture (Wireshark+ TCPDump) สำหรับการใช้งานในรูปแบบ Remote capture จะเป็นการผสมผสานการทำงานของ Wireshark บน Windows และโปรแกรม TCPDump บน Linux หลักการทำงานคือ บนเครื่อง Windows จะต้องทำการสร้าง สคริปต์สำหรับการ Login เข้าไปที่เครื่อง Linux โดยจะต้องทำการกำหนดค่า Parameter Username และ Password ที่จำเป็นต่อการใช้งานให้ครบถ้วน รวมทั้งคำสั่งของ TCPDump ที่ต้องการ ประโยชน์ของการใช้งาน Remote Capture คือสามารถทำการมอนิเตอร์ข้อมูลที่เกิดบนเครื่อง Linux เครื่องใดก็ได้ที่สามารถเข้าถึงได้ และนำข้อมูลที่ได้มาแสดงผลที่ Wireshark บน Windows ได้ในทันทีเพื่อแก้ปัญหาในกรณีที่ต้องการวิเคราะห์ปัญหาที่เกิดขึ้นในลักษณะ Real Time แต่การทำงานในลักษณะนี้ก็จะมีความเสี่ยงด้วยเช่นกัน คือ ในกรณีข้อมูลที่ได้มาจากการใช้งาน TCPDump มีมากเกินไปอาจจะทำให้เกิดการรบกวนการทำงานของอุปกรณ์อื่น ๆ ในระบบ ซึ่งจะทำให้การใช้งานเครือข่ายโดยรวมช้าลงได้ สำหรับสคริปต์เพื่อการใช้งาน Remote Capture ดังภาพที่ ๓๙ จะเห็นได้ว่าในคำสั่งตัวอย่าง Script เพื่อให้สามารถ Remote Capture ได้ จะต้องมีการใช้งานโปรแกรม plink โดยโปรแกรมจะต้องติดตั้งอยู่ที่ C:\Telnet\plink.exe -ssh -pw [password] root@[IP Address] "tcpdump -n -i eth0 -w -" | "C:\Program Files\Wireshark\wireshark-gtk.exe" -k -i ด้วยจึงจะสามารถใช้งานเก็บข้อมูลเครือข่ายได้อย่างสมบูรณ์



ภาพที่ ๓๙ การเก็บข้อมูลด้วยการทำ Remote Capture (Wireshark+TCPDump)

๓.๓.๑๑ การทำ Remote Capture ตัวอย่างการนำ Remote Capture ที่เห็นได้ชัดเจนที่สุด ตัวอย่างหนึ่งคือการใช้งาน Wireshark ในการทำแลปบน UnetLab/EVE-NG และ EVE-NG นั้นเอง การเก็บข้อมูลด้วยวิธีการพิเศษ การเก็บข้อมูลด้วย Network TAP การเก็บข้อมูลด้วย Network TAP เป็นวิธีการที่อาศัยการทำงานพื้นฐานคือการเชื่อมต่อกันของ วงจรไฟฟ้า เริ่มตั้งแต่การต่อสายแลนเข้าหากันแบบง่าย ๆ ไปจนถึงการออกแบบเป็นฮาร์ดแวร์เพื่อการใช้งาน เพื่อใช้งานเฉพาะทาง เช่น Network TAP แบบสาย UTP CAT5/6 และแบบสาย Fiber Optic เป็นต้น โดยทั่วไป Network TAP

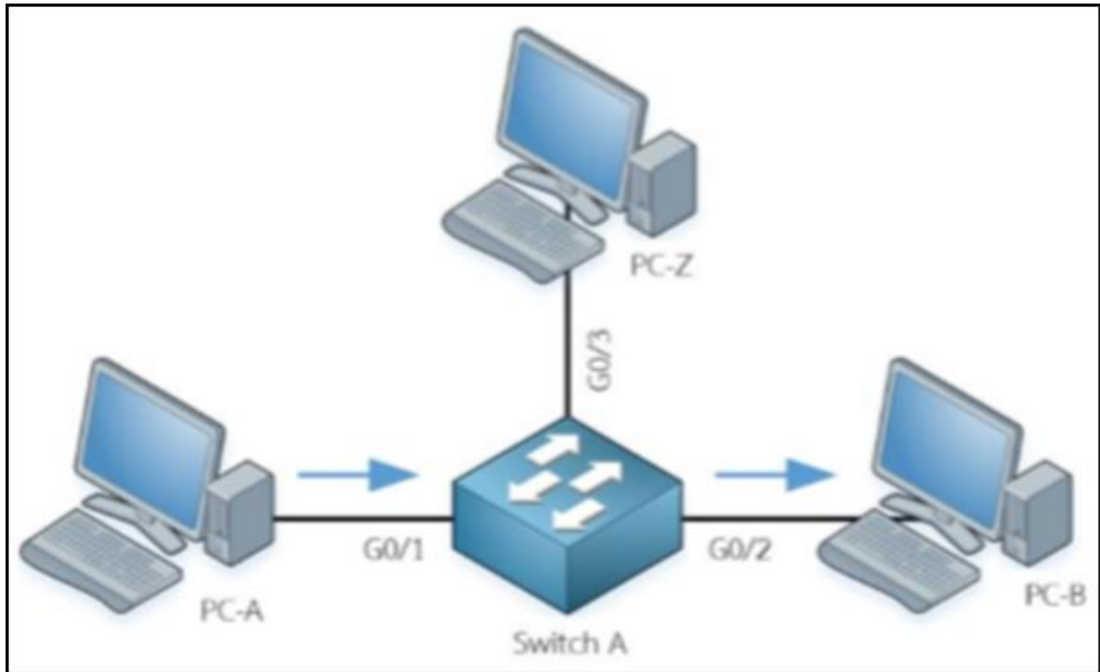
จะถูกนำมาใช้งานในบางสถานการณ์ ได้แก่ นำมาใช้ในการวิเคราะห์ ปัญหาทางด้านระบบเครือข่ายที่ต้องการตัดประเด็นการทำงานที่ผิดพลาดของอุปกรณ์ออกไปอย่างชัดเจน เช่น ไม่แน่ใจว่าการที่ระบบเครือข่ายมีปัญหา นั้นเกิดจากการที่สวิตช์ทำงานผิดปกติหรือไม่ เป็นต้น การใช้งาน Network TAP จึงเป็นทางออกที่น่าสนใจสำหรับกรณีนี้ หรือการนำ Network TAP ไปใช้งานกับการ Audit PCI-DSS ของเครื่อง POS ที่ไม่สามารถทำการติดตั้งโปรแกรมต่าง ๆ เพิ่มเติมได้และอุปกรณ์ POS เองก็ไม่รองรับการทำงานในการเก็บข้อมูลเครือข่าย



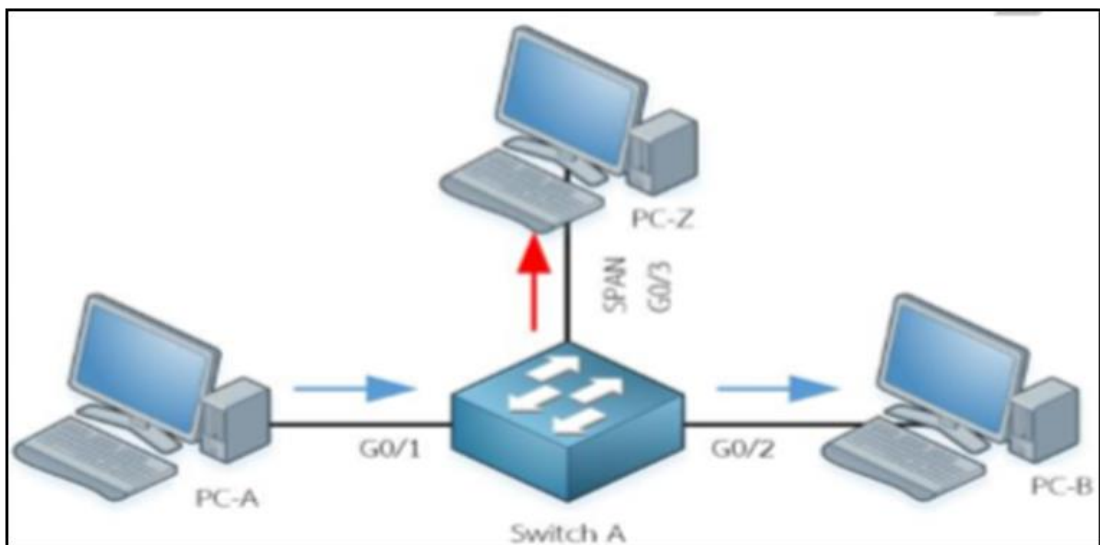
ภาพที่ ๔๐ Network TAP

๓.๓.๑๒ การสื่อสารระหว่างอุปกรณ์เมื่อสวิตช์ทำงานตามปกติ อุปกรณ์ Network Tap ก็มีข้อเสียในการใช้งานด้วยเช่นกันคือ กรณีใดก็ตามที่มีการใช้งาน Network TAP แบบ Passive หรือ Network TAP ที่ไม่มีการออกแบบที่ดีพอ ตัว Network TAP เองก็จะเป็นอุปกรณ์ที่ทำให้เกิดปัญหาขึ้นเสียเอง เนื่องจาก Network TAP จะทำให้สัญญาณที่ใช้ในการสื่อสารในระบบ LAN อ่อนลง ซึ่งจะทำให้รับข้อมูลผิดพลาดได้ อีกประเด็นหนึ่งคือ เมื่อต้องการนำ Network TAP มาใช้งาน จะต้องทำการถอดสายแลนของเครื่องที่ต้องการตรวจสอบออกและนำ Network TAP เข้ามาเชื่อมต่อแทน ดังนั้นในกรณีนี้จะทำให้เกิด Downtime ขึ้นกับอุปกรณ์ การเก็บข้อมูลด้วยการใช้งาน SPAN และ RSPAN โดยปกติแล้วสวิตช์จะทำการเชื่อมต่อสื่อสารระหว่างเครื่องสองเครื่องที่มีการสื่อสารกันโดยตรงไม่ได้การกระจายการสื่อสารนั้นออกไปทุกเครือข่าย (Broadcast) แบบเดียวกับฮับ (Hub) ซึ่งวิธีการนี้ทำให้การสื่อสารระหว่างคอมพิวเตอร์สองเครื่องที่เชื่อมต่อกันผ่านสวิตช์มีประสิทธิภาพสูงกว่าการใช้งานฮับ และยังเป็นการป้องกันการดักเก็บข้อมูลกลางทางระหว่างการสื่อสารของคอมพิวเตอร์สองเครื่องได้ด้วยเช่นเดียวกัน แต่ในมุมมองของการแก้ปัญหาทางเครือข่ายโดยใช้งานโปรแกรม Wireshark นั้นจะพบว่าเมื่อมีการใช้งานสวิตช์จะไม่สามารถนำข้อมูลของเครื่องที่มีปัญหา มาวิเคราะห์การทำงานได้ แต่หากต้องการข้อมูลจากสวิตช์โดยตรงมาใช้ในการวิเคราะห์ จะต้องใช้ฟังก์ชัน SPAN (Switch Port Analyzer) ซึ่งการใช้งาน SPAN หรือในอีกชื่อหนึ่งคือ Port Mirror เป็นเทคนิคในการสั่งให้สวิตช์ทำการคัดลอกข้อมูลจากเครือข่ายหนึ่งไปยังเครือข่ายอื่นที่ไม่ใช่ปลายทางที่แท้จริงของอุปกรณ์นั้น การทำงานแบบนี้

มีลักษณะการทำงานคล้ายกับการทำงานของฮับ แต่จะเป็นการทำงานแบบเฉพาะเจาะจงบนเครือข่ายที่ต้องการเท่านั้น



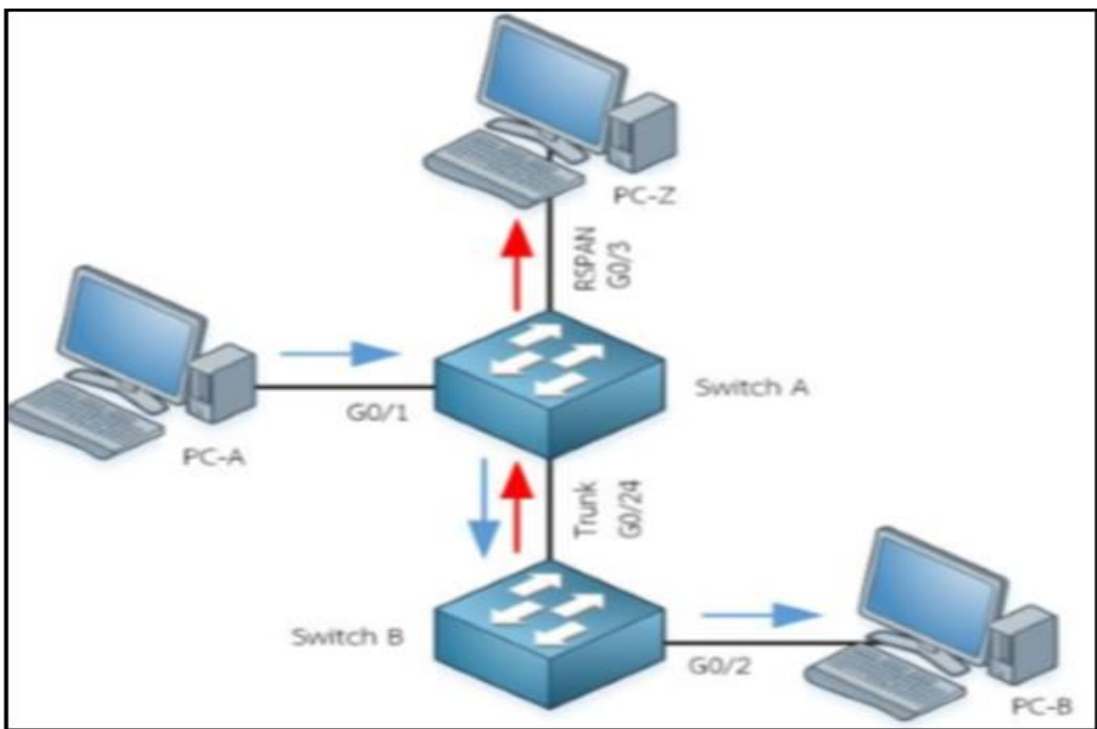
ภาพที่ ๔๑ การสื่อสารระหว่างอุปกรณ์เมื่อสวิตช์ทำงานตามปกติ



ภาพที่ ๔๒ การทำงานของสวิตช์เมื่อมีการตั้งค่าให้ทำงานในรูปแบบ SPAN

๓.๓.๑๓ คำสั่ง SPAN เป็นการนำข้อมูลเครือข่ายที่มีปัญหาวิเคราะห์บนระบบเครือข่ายขนาดใหญ่ ซึ่งในกรณีที่มีการเชื่อมต่อของสวิตช์หลาย ๆ ตัวเข้าไว้ด้วยกันมักจะทำได้ยาก เนื่องจาก

การใช้งาน SPAN นั้น จะต้องทำการเชื่อมต่อเครื่องที่ติดตั้งโปรแกรม Wireshark เพื่อทำการวิเคราะห์ปัญหาไปอยู่บนสวิตช์ตัวเดียวกันกับสวิตช์ของอุปกรณ์ที่ต้องการตรวจสอบข้อมูลบนระบบเครือข่ายในกรณีที่มีปัญหา ซึ่งในกรณีนี้อาจจะทำได้ยากหรือมีความไม่สะดวก เช่น สวิตช์อยู่คนละอาคาร หรืออยู่ในห้องศูนย์ข้อมูลซึ่งต้องมีการกำหนดเวลาในการเข้าออก ไม่อาจจะทำให้การวิเคราะห์หรือแก้ไขปัญหาได้ ดังนั้นจึงมีวิธีการพัฒนาฟังก์ชันการทำงานแบบ Remote Switch Port Analysis : (RSPAN) เพื่อแก้ไขปัญหาดังกล่าว การทำงานของ RSPAN จะต้องทำการเพิ่ม VLAN พิเศษขึ้นมาอีกหนึ่ง VLAN เพื่อนำ VLAN ที่เพิ่มมาใช้งานเป็น Remote VLAN สำหรับการส่งข้อมูล SPAN ไปที่สวิตช์อื่น ตัวอย่างการทำงานของ RSPAN ดังภาพที่ ๔๓

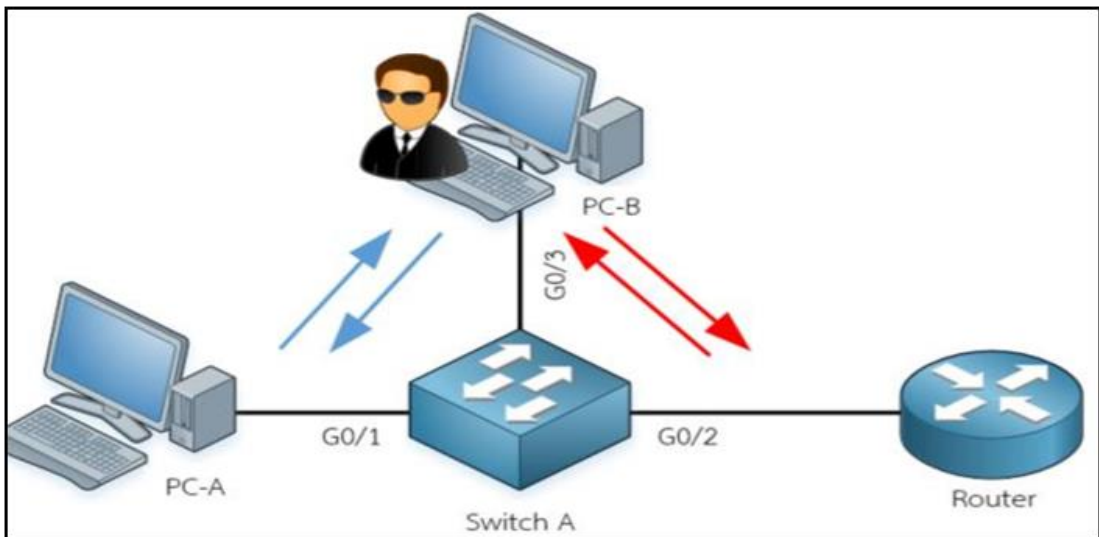


ภาพที่ ๔๓ ตัวอย่างการทำงานของ RSPAN

จากภาพที่ ๔๓ เครื่องที่ทำการติดตั้งโปรแกรม Wireshark เพื่อทำการวิเคราะห์ข้อมูลคือ PC-Z ติดตั้งอยู่ที่ Switch A และเครื่อง PC-B เป็นเครื่องที่มีปัญหาเกิดขึ้น ผู้ดูแลระบบต้องการที่จะทำการ ส่งข้อมูลการ SPAN ของ Switch B กลับไปที่ Switch A ดังนั้นเมื่อการเชื่อมต่อไม่ได้อยู่บนสวิตช์ตัวเดียวกัน จึงต้องใช้ฟังก์ชัน RSPAN แทน SPAN ตามปกติ โดยสิ่งที่เพิ่มขึ้นมาคือการตั้งค่า Remote VLAN ตามที่ได้กล่าวไว้ข้างต้น และอนุญาตให้มีการส่งข้อมูลออกไปที่ Trunk ที่เชื่อมต่อกับสวิตช์ทั้งสองตัว

๓.๓.๑๔ การเก็บข้อมูลด้วยการใช้ Hacking Technique การเก็บข้อมูลเครือข่ายแบบนี้เป็นวิธีที่ไม่แนะนำให้นำไปใช้งานในระบบจริง เนื่องจากเป็นการกระทำ ที่เข้าข่ายในการทำผิดกฎหมายอาญารูปแบบหนึ่ง การแนะนำการทำงานของวิธีนี้จะใช้ตัวอย่างของเทคนิคที่ เรียกว่า ARP Spoofing ซึ่งถือเป็นรูปแบบหนึ่งของการทำ Man In The Middle (MITD) ยกตัวอย่างการทดลองในระบบปิด

โดยใช้การจำลองการทำงานผ่านโปรแกรมจะลงระบบเครือข่าย คือ EVE-NG โดยใช้การทำงานร่วมกับโปรแกรม VirtualBox เพื่อให้เห็นการทำงานที่สมบูร์มมากขึ้น สำหรับ การทำงานโดยละเอียด จะมีการกล่าวถึงในส่วนของการทำการทดลองต่อไป การเก็บข้อมูลในระบบเครือข่ายโดยการใช้งาน ARP Spoofing นี้จะเป็นการลอบให้อุปกรณ์ PC-A ส่งข้อมูลการสื่อสารไปที่ PC-B ที่มีการทำ ARP Spoofing ไว้เพื่อทำการเก็บข้อมูลการเชื่อมต่อที่ภายนอกเครือข่ายที่โดยปกติจะต้องมีการส่งข้อมูลไปที่เราท์เตอร์เมื่อมีการลอบให้ PC-A ทำการส่งข้อมูล การสื่อสารไปที่ PC-B แทนดังนั้น PC-B จึงสามารถทำการบันทึกข้อมูลการสื่อสารของ PC-A ได้ ดังภาพที่ ๔๔



ภาพที่ ๔๔ ตัวอย่างการทำงานของ ARP Spoofing

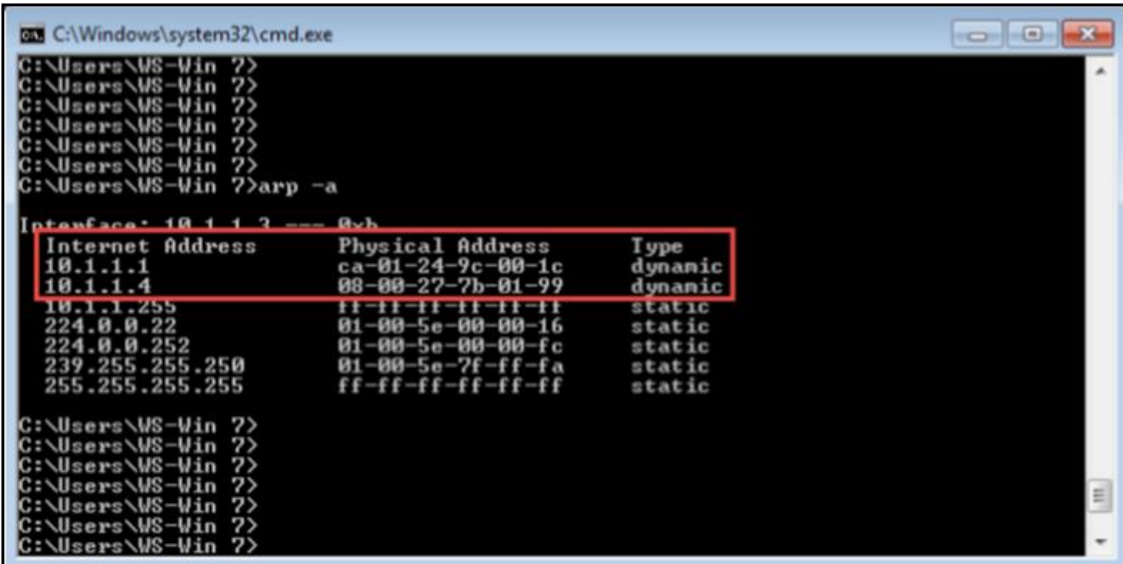
```
C:\Windows\system32\cmd.exe
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??>arp -a

Interface: 10.1.1.2 --- 8-b
Internet Address      Physical Address      Type
10.1.1.1              ca-01-24-5e-00-00    dynamic
10.1.1.4              08-00-27-7b-01-99    dynamic
10.1.1.255           11-11-11-11-11-11    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
C:\Users\MS-Win ??
```

ภาพที่ ๔๕ MAC table บนเครื่อง PC ก่อนการทำ ARP Spoofing

๓.๓.๑๕ ผลที่เกิดจากการทำ ARP Spoofing นั้นสามารถดูได้จากภาพที่ ๔๕ โดยปกติแล้ว PC-A จะมีตาราง ARP ของการเชื่อมต่อกับเราเตอร์ดังในรูป แต่เมื่อใดก็ตามที่ PC-A ถูกทำการดักเก็บข้อมูลไปโดยการใช้งาน ARP Spoofing ในระบบเครือข่ายตาราง ARP ของเครื่อง PC-A จะเปลี่ยนไปดังในภาพที่ ๔๖ ซึ่งจะทำให้ PC-A ส่ง ข้อมูลการใช้งานระบบเครือข่ายไปที่ PC-B ที่กำลังทำ ARP Spoofing อยู่นั่นเอง หากสังเกต MAC Address ของรูปจะเห็นได้ว่าผลของการทำ ARP Spoofing จะทำให้ MAC Address ของ Router เปลี่ยนไปเป็น MAC Address ของ PC-B แทน



```
ca C:\Windows\system32\cmd.exe
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>arp -a
Interface: 10.1.1.2 --- 8xb
Internet Address      Physical Address      Type
10.1.1.1              ca-01-24-9c-00-1c    dynamic
10.1.1.4              08-00-27-7b-01-99    dynamic
10.1.1.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
C:\Users\WS-Win 7>
```

ภาพที่ ๔๖ ผลที่เกิดจากการทำ ARP Spoofing บนเครื่องที่ต้องการเก็บข้อมูล

๓.๓.๑๖ เมนูการใช้งานของโปรแกรม Wireshark มีการแบ่งหน้าต่างหลัก ๆ ออกเป็น ๕ ส่วน โดยแต่ละส่วนจะมีชื่อและมีหน้าที่ต่าง ๆ ดังนี้

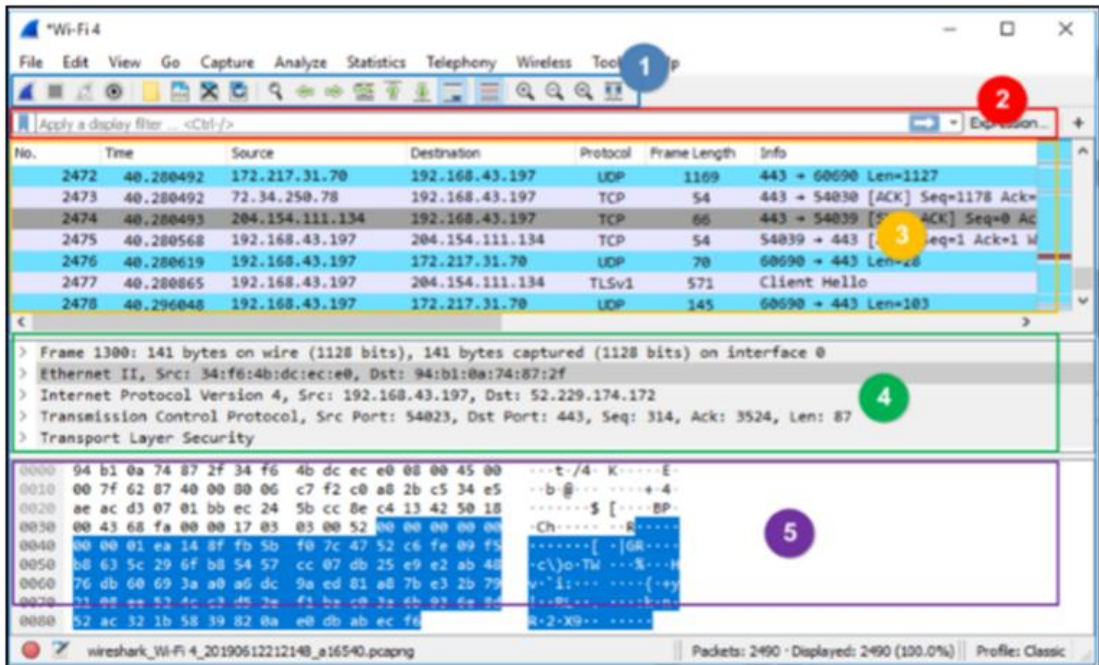
๓.๓.๑๖.๑ Main Toolbar เป็นเมนูของเครื่องมือหลักเมื่อต้องการใช้งานโปรแกรม Wireshark โดยจะมีคำสั่งที่สำคัญคือ Start และ Stop Capture ใช้สำหรับการบันทึก Packet ข้อมูลในระบบเครือข่าย ต่อมาคือ Edit/Apply Display Filter, Edit Coloring Rules และ Edit Preferences โดยจะมีการกล่าวถึงรายละเอียดในส่วนต่อไป

๓.๓.๑๖.๒ Display Filter Area เป็นส่วนที่สำคัญที่สุดที่จะถูกกล่าวถึงในส่วนนี้ เนื่องจากเป็นส่วนที่เราจะใช้ในการทำการกรองข้อมูลที่ต้องการ เพื่อนำมาแสดงผลและวิเคราะห์การทำงานในลำดับต่อไป

๓.๓.๑๖.๓ Packet List Pane เป็นส่วนที่ใช้แสดงรายละเอียดของแพ็กเก็ตที่เก็บข้อมูลมาได้ โดยจะแสดงรายละเอียดเบื้องต้นทั้ง IP Address โพรโทคอลและรายละเอียดเบื้องต้นของแพ็กเก็ตนั้น ๆ

๓.๓.๑๖.๔ Packet Detail Pane เป็นส่วนที่ใช้แสดงรายละเอียดต่าง ๆ ของแต่ละแพ็กเก็ตโดยละเอียด โดยจะแสดงข้อมูลในรายละเอียดไล่ขึ้นมาตั้งแต่ระดับเฟรมไปจนถึงข้อมูลที่อยู่ใน Layer Application

๓.๓.๑๖.๕ Packet Byte Pane จะเป็นการแสดงข้อมูลของแพ็กเก็ตที่เกิดขึ้นในรูปแบบของข้อมูลฐานสิบหกและตัวอักษร ASCII โดยในกรณีที่ข้อมูลไม่มีการเข้ารหัสจะสามารถทำการอ่านข้อมูลในส่วนนี้ออกมาได้ทันที สำหรับตำแหน่งของเมนูต่าง ๆ ของโปรแกรม Wireshark สามารถดูได้ ดังภาพที่ ๔๗



ภาพที่ ๔๗ โปรแกรม Wireshark

๓.๓.๑๗ การสร้างและนำ Filter ไปใช้งานในโปรแกรม Wireshark เมื่อเราทำการเก็บข้อมูลในระบบเครือข่ายขึ้นมาแล้ว ในขั้นตอนต่อไปเราจะต้องนำข้อมูลที่ได้มาศึกษาการทำงานหรือวิเคราะห์หาการทำงานที่ผิดปกติ แต่โดยทั่วไปแล้วในขั้นตอนการเก็บข้อมูลส่วนใหญ่มักจะทำการเก็บข้อมูลมาในลักษณะให้ “เยอะที่สุดเอาไว้ก่อน” เพื่อในกรณีที่ไม่สามารถที่จะทำการเก็บข้อมูลเข้าได้บ่อย ๆ โดยอาจจะมีความเสี่ยงมาจากการต้องทำการขอ Change Request ตามขั้นตอน ซึ่งอาศัยระยะเวลาและขั้นตอนในการดำเนินการที่นาน หรือเหตุที่เกิดขึ้นนั้นอาจจะไม่สามารถสร้างสถานการณ์แบบเดียวกันได้อีก (Re - Produce) หรือเป็นเหตุการณ์ที่ต้องออกมาเก็บข้อมูลนอกสถานที่ซึ่งไม่สามารถออกมาได้บ่อย ๆ ดังนั้น เมื่อข้อมูลที่จัดเก็บมาได้มีขนาดใหญ่และมีความซับซ้อนสูงการใช้งาน Filter ในโปรแกรม Wireshark จึงเป็นเรื่องสำคัญ โดยเป็นขั้นตอนที่จะสามารถทำให้เราระบุขอบเขตของข้อมูลที่ต้องการได้ละเอียดและลึกซึ้งจากข้อมูลพื้นฐานที่มีขนาดใหญ่ โดยทั่วไปแล้วการใช้งาน Filter ในโปรแกรม Wireshark จะประกอบด้วยข้อมูลที่มีคุณสมบัติของ Input Filter ทั้งหมด ๓ รูปแบบ ตามตารางที่ ๑

คุณสมบัติ	คำอธิบาย	ตัวอย่าง
ชนิดของข้อมูล	ใช้ระบบ ID หรือข้อมูลที่ต้องการอ้างอิงถึง	Host, Net, Port
ทิศทาง	ใช้ระบุทิศทางของข้อมูลหรือของ ID	Src, Dst
โปรโตคอล	ใช้ระบุโปรโตคอลที่มีการใช้งานแบบเฉพาะเจาะจง	Ether, IP, UDP, HTTP

ตารางที่ ๑ คุณสมบัติของ Input Filter

๓.๓.๑๘ โดยในการใช้งาน Filter จะมี Input Filter อยู่เพียงแค่นี้หรือทั้งสามก็ได้ เช่น
 Filter -> ip.addr==192.168.10.1 เลือก IP Address 192.168.10.1 มาแสดงผล และ
 Filter -> ip.src==192.168.10.1 เลือก Source IP Address 192.168.10.1 มาแสดงผล,
 Filter -> tcp.port==80 เลือกโปรโตคอล TCP Port 80 มาแสดงผล เป็นต้น

จากตัวอย่างที่ยกมาให้ดูทั้งสามแบบ จะเห็นได้ว่าการใช้งานเครื่องหมาย “=” อยู่ โดยที่
 เครื่องหมาย “=” จะเป็นกลุ่มของ Operator ที่ทำหน้าที่เชื่อมข้อมูล Input Filter สองตัว
 เข้าไว้ด้วยกัน และตัว Operator นี้ยังถูกแบ่งออกได้เป็นอีกสองกลุ่มย่อย ๆ คือ Operator แบบ
 เปรียบเทียบ (Comparison) และ Operator แบบตรรกะ (Logical หรือ Boolean) โดยจะแสดง
 กลุ่มของ Operator ทั้งสองแบบนี้ไว้ตามตารางที่ ๒ และ ๓ ดังนี้

Comparison operator	คำอธิบาย
==	มีค่าเท่ากับ
!=	มีค่าไม่เท่ากับ
>	มีค่ามากกว่า
<	มีค่าน้อยกว่า
>=	มีค่ามากกว่าหรือเท่ากับ
<=	มีค่าน้อยกว่าหรือเท่ากับ

ตารางที่ ๒ การใช้งาน Filter

Logical Operator	คำอธิบาย
And / &&	Logical AND
Or /	Logical OR
Not / !	Logical NOT

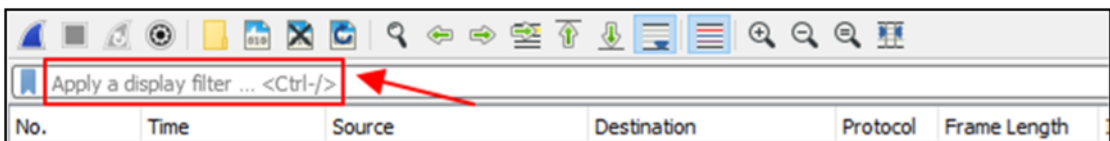
ตารางที่ ๓ Logical Operator

๓.๓.๑๙ การแยกกลุ่มของ Input Filter สามารถทำได้ซับซ้อนมากขึ้น โดยการใช้งานร่วมกับการใช้เครื่องหมาย “()” เพื่อใช้ในการแยกกลุ่มของ Input Filter ให้ชัดเจนขึ้นได้ด้วยดังตัวอย่างต่อไปนี้

Filter -> ip.src==10.1.1.1 && ip.dst==10.1.1.2 เลือก Source IP Address 10.1.1.1 และ Destination IP Address 10.1.1.2 มาแสดงผล และ

Filter -> !(ip.src==10.1.1.1 & ip.dst==10.1.1.2) เลือกแสดงผล IP Address อะไรก็ได้ที่ไม่ใช่ Source IP Address 10.1.1.1 และ Destination IP Address 10.1.1.2 มาแสดงผล

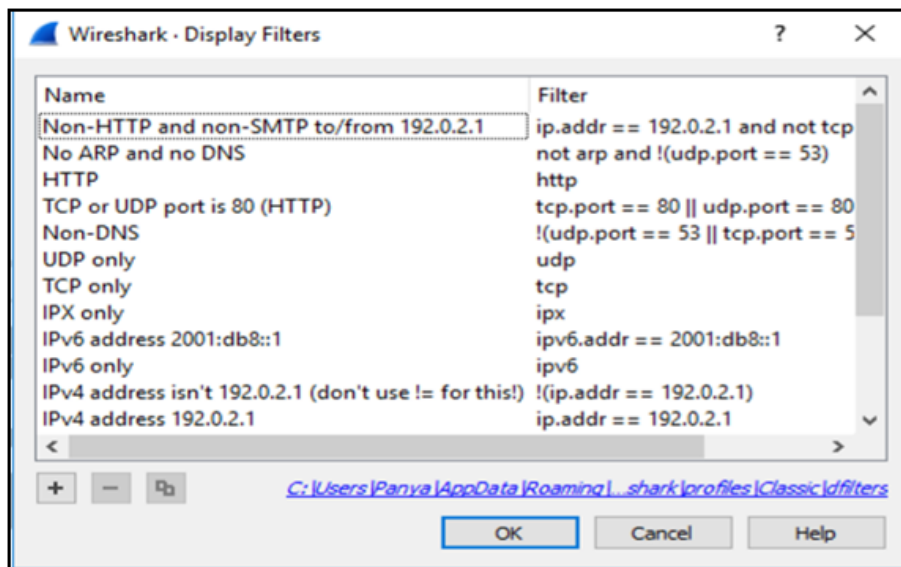
จากตัวอย่าง กรณีที่ไม่สามารถใช้ Filter !ip.src==10.1.1.1 && !ip.dst==10.1.1.2 แทนได้หรือไม่สามารถจำ Input Filter หรือ Operator แบบต่าง ๆ ได้ ตัวโปรแกรม Wireshark ก็จะมีตัวช่วยอำนวยความสะดวกในการใช้งาน Filter ให้ โดยทำการคลิกที่ Filter บนเมนู ดังภาพที่ ๔๘



ภาพที่ ๔๘ การแยกกลุ่มของ Input Filter

๓.๓.๒๐ Display Filter

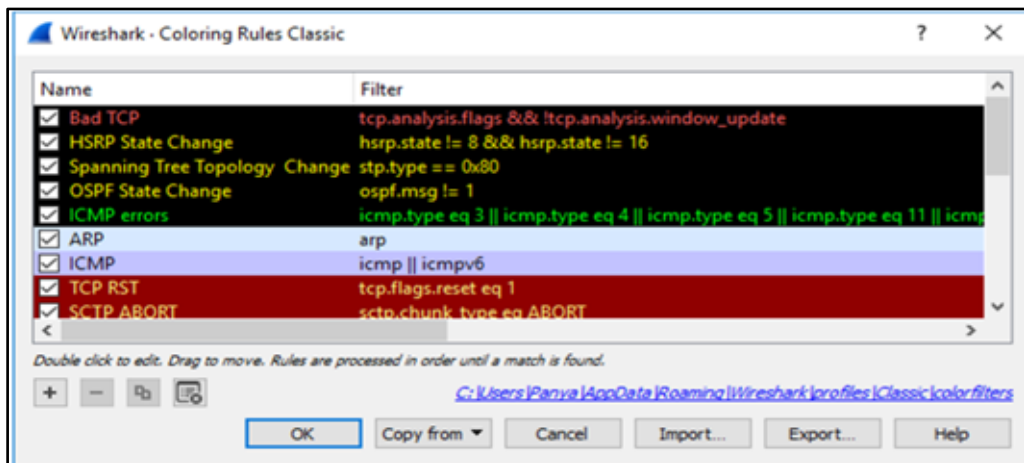
ในกรณีที่ต้องการเพิ่ม Operator เข้ามาใช้งาน ให้ทำการกด Filter แล้วจะมีหน้าต่างใหม่ถูกเปิดขึ้นมา ให้เราสามารถเลือกเป็น Display Filter แล้วทำการกด Expression เพื่อเพิ่ม Option ก็จะพบคำสั่งต่าง ๆ สำหรับการใช้งาน Operator ดังภาพที่ ๔๙



ภาพที่ ๔๙ Display Filter

๓.๓.๒๑ การใช้งาน Coloring Rules

Coloring Rules เป็นการให้สีกับข้อมูลตัวอักษรและ Background ที่แสดงขึ้นมาในช่องของ Packet List Pane ให้มีความแตกต่างกันไปตามค่าที่ได้ตั้งไว้ให้กับแพ็คเก็ต โดยโปรแกรม Wireshark จะทำการตั้งค่ามาให้แล้วส่วนหนึ่ง โดยสามารถดูได้ที่เมนู View -> Coloring Rules หลังจากเลือกแล้วโปรแกรม Wireshark จะแสดง Coloring Rules ที่ได้มีการตั้งค่าเริ่มต้น (Default) ของโปรแกรมไว้แล้ว และจากภาพที่ ๕๐ จะเห็นได้ว่า Coloring Rule ต้องมี Filter String กำกับอยู่ด้วยเพื่อใช้ในการจับคู่สีของ Filter String ให้เข้ากับสีของ Coloring Rule แต่ละตัวนั่นเอง และในกรณีที่จำค่าของ Filter ที่ต้องการใช้งานไม่ได้ ก็สามารถเข้ามาที่เมนู Coloring Rule และทำการนำ Filter String ไปใช้งานเป็นต้นแบบในการทำ Filter ได้ด้วยเช่นกัน



ภาพที่ ๕๐ Coloring Rule

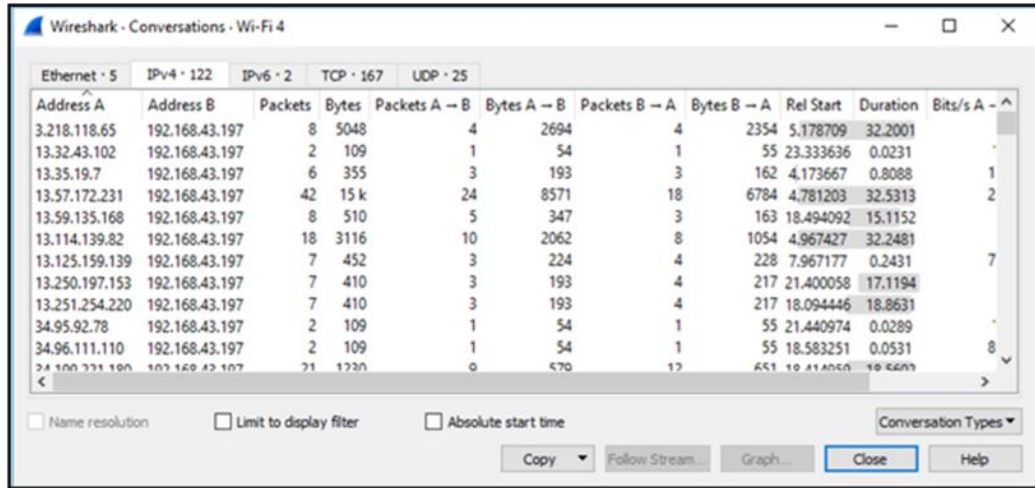
๓.๓.๒๒ Coloring Rule

เนื่องจากโปรแกรม Wireshark มีการแสดงผลที่ซับซ้อนและ Coloring Rule ที่ได้สร้างมาให้อาจจะไม่เพียงพอต่อการใช้งานของผู้ใช้ ดังนั้นโปรแกรม Wireshark จึงอนุญาตให้ผู้ใช้สามารถสร้าง Coloring Rule เองได้ด้วยการกดปุ่ม New ใน Coloring Rule โดยเมื่อกดแล้วจะมีหน้าต่างขึ้นมาทำการตั้ง Coloring Rule ตัวใหม่ตามที่เรากำลังต้องการได้ โดยจะต้องทำการตั้งชื่อและ Filter ไว้ด้วย นอกจากนี้ยังสามารถทำการแก้ไขสีของ Foreground และ Background ได้ตามที่ต้องการจากเมนูนี้ด้วย

๓.๓.๒๓ Statistics Conversations ในการใช้งาน Wireshark

โดยปกติแล้วจะมีแพ็คเก็ตที่เราทำการเก็บข้อมูลเข้ามาเป็นจำนวนมาก แต่ในการระบุปัญหาหรือการตรวจสอบการทำงานระหว่างเครื่อง Client และ Server จะมีการติดต่อกันเพียงสองเครื่อง เป็นการจับคู่การสื่อสาร ในกรณีที่เรากำลังหาคู่ระหว่าง Client และ Server สามารถดูได้จากช่อง Packet List Pane ดังนั้น Wireshark จึงมีการเตรียมเมนูที่มีการแสดงผลการสื่อสารระหว่างเครื่อง Client และ Server เอาไว้ให้ เพื่ออำนวยความสะดวกในการใช้งาน สำหรับการใช้งานเมนูนี้สามารถเข้าไปที่เมนู Statistics -> Conversations โดยโปรแกรม Wireshark จะเปิดหน้าต่าง

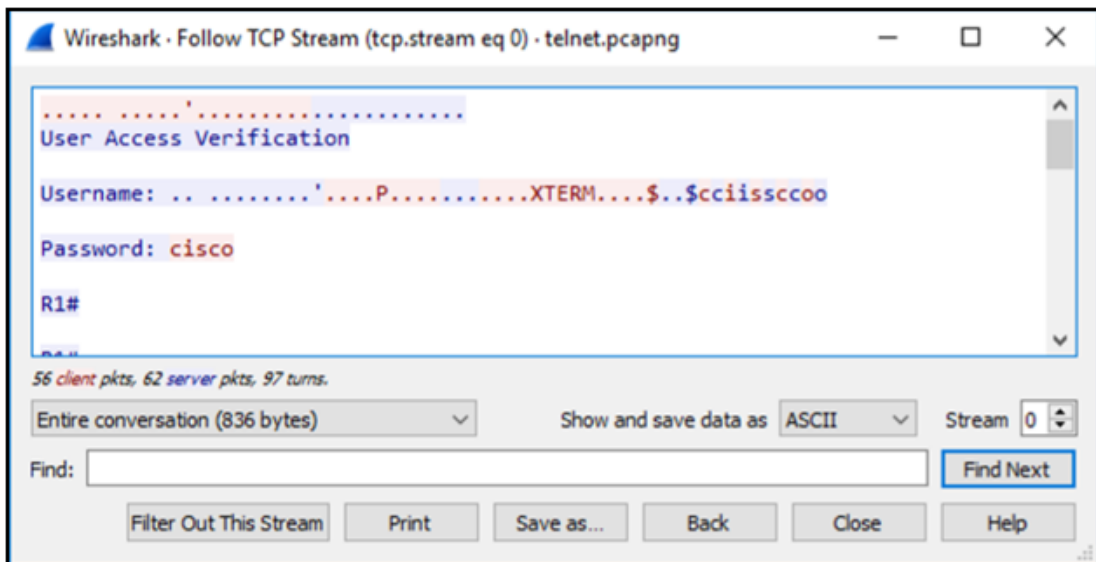
Conversations ขึ้นมาใหม่อีกหนึ่งอัน โดยจะแสดงรายละเอียดของการสื่อสารระหว่างเครื่องเป็นคู่ ๆ ไว้ให้ โดยสามารถทำการเลือกดูค่า Conversation ระหว่างเครื่องต่าง ๆ ตามโปรโตคอลที่ใช้งานได้ตามภาพที่ ๕๑



ภาพที่ ๕๑ Conversation

๓.๓.๒๔ การใช้งาน Feature ของโปรแกรม Wireshark

เพื่อวิเคราะห์การทำงานของโปรโตคอลต่าง ๆ ในส่วนนี้จะเป็นการแนะนำ Feature ของโปรแกรม Wireshark ควบคู่ไปกับการยกตัวอย่างการนำไปใช้งานเพื่อให้เห็นตัวอย่างการนำ Feature ไปใช้งานและได้เห็นการทำงานจริงของโปรโตคอล Telnet, SSH และ HTTP การใช้งาน Follow TCP Stream และ Feature Follow TCP Stream โดยจะเป็นการแสดงรายละเอียดของข้อมูลที่อยู่ใน TCP Stream โดยทั่วไปแล้วการสื่อสารระหว่าง Client – Server จะมีการส่งข้อมูลที่มากกว่าหนึ่งชุดข้อมูลระหว่างกัน โดยเมื่อมีการส่งข้อมูลหนึ่งชุดจบไปแล้ว จะมีการหยุดส่งข้อมูลก่อน แต่กระบวนการของ TCP Connection จะยังไม่มีมีการตัดการเชื่อมต่อ โดยในโปรแกรม Wireshark จะเรียกการนับชุดข้อมูลที่มีการส่งในหนึ่งชุดนี้ว่า “Stream index” เพื่อใช้ในการอ้างอิงชุดข้อมูล TCP ร่วมกับ Follow TCP Stream สำหรับการทำงานของ Feature Follow TCP Stream จะใช้ งานโปรโตคอลจำนวน ๓ โปรโตคอล คือ Telnet, SSH และ HTTP โดยการ ใช้ Follow TCP Steam เพื่อดูข้อมูลของโปรโตคอล ทั้งนี้ Telnet จะเป็นการแสดงผลที่ได้จากการเก็บข้อมูลการใช้งาน Telnet ของอุปกรณ์เครือข่าย โดยปกติแล้ว Telnet เป็นการสื่อสารในแบบที่ไม่ได้ทำการเข้ารหัส การสื่อสาร ดังนั้น เราจะสามารถใช้ Follow TCP Stream เพื่อดูข้อมูลการใช้งาน Telnet ในการติดต่อ สื่อสารระหว่างเครื่องคอมพิวเตอร์ได้ ดังภาพที่ ๕๒



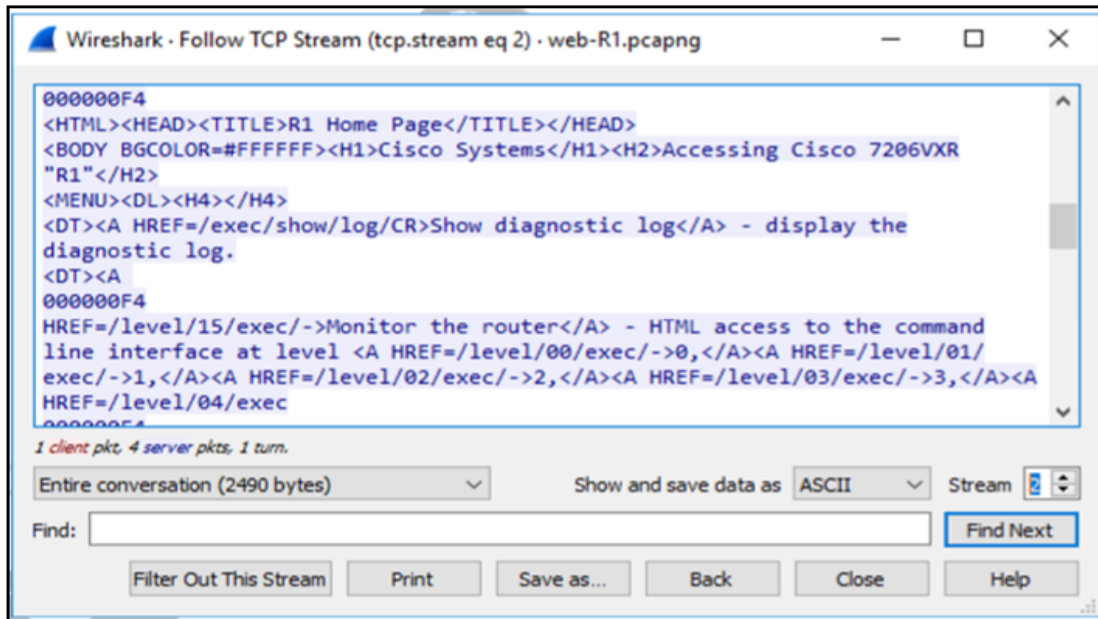
ภาพที่ ๕๒ แสดงข้อมูลการ Login เข้าเราท์เตอร์ด้วย Telnet

๓.๓.๒๕ การใช้ Follow TCP Steam กับ SSH

เพื่อดูข้อมูลของโปรโตคอล SSH จากตัวอย่างการใช้งาน Telnet จะเห็นได้ว่าข้อมูลที่ถูกส่งอยู่ในระบบเครือข่ายจะไม่ถูกเข้ารหัส ทำให้สามารถเห็นข้อมูลทั้งหมดได้ ดังนั้น SSH จึงถูกพัฒนาขึ้นมาเพื่อแก้ไขปัญหาดังกล่าว เช่น ข้อมูลถูกส่งเข้าไปที่อุปกรณ์เดียวกันแต่เมื่อมีการใช้งาน SSH จะทำให้ไม่สามารถเห็นข้อมูลที่ใช้ในการสื่อสารกันได้ แต่ยังคงใช้งานผ่าน Feature Follow TCP Steam เป็นต้น

๓.๓.๒๖ การใช้ Follow TCP Steam กับ HTTP

เพื่อดูข้อมูลของโปรโตคอล HTTP เช่นเดียวกับกับ Telnet และ SSH โปรโตคอล HTTP จะมีการสื่อสารผ่านโปรโตคอล TCP เราจึงสามารถใช้ Follow TCP Stream ได้ โดยจะเห็นได้ว่าโปรโตคอล HTTP ไม่มีการเข้ารหัสในการสื่อสารเช่นเดียวกัน ดังนั้นข้อมูล HTML ในหน้าจอของ Follow TCP Stream ก็จะสามารถสังเกตได้เช่นเดียวกับกับ Telnet

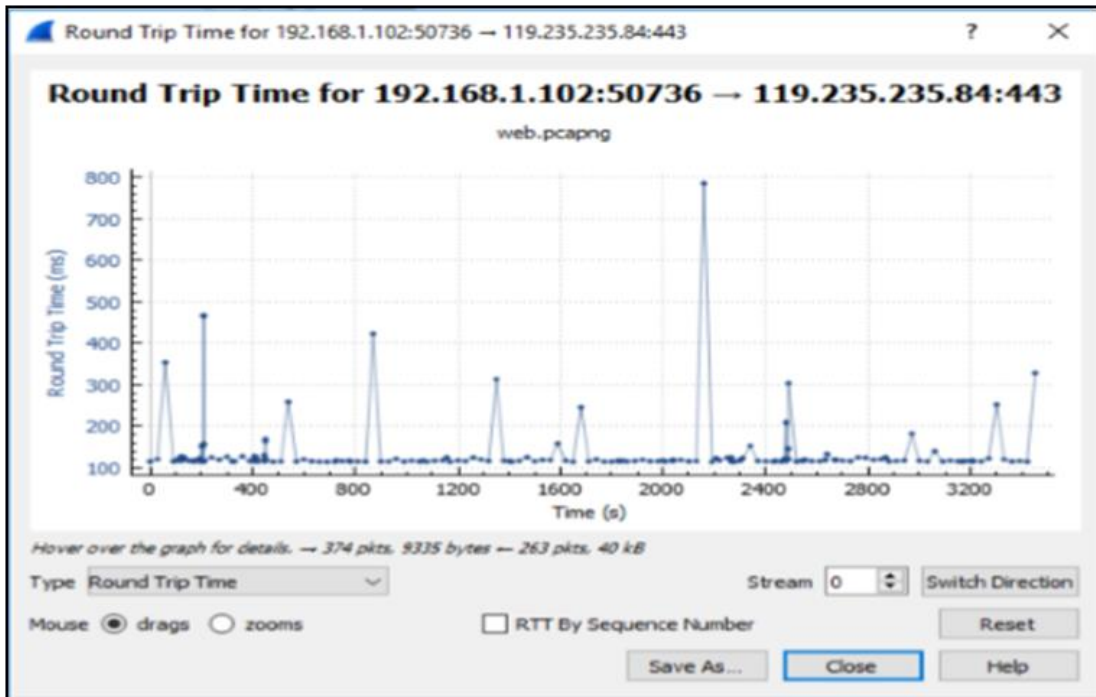


ภาพที่ ๕๓ แสดงข้อมูลในการสื่อสารของ HTTP

๓.๓.๒๗ การใช้งาน TCP Stream Graph

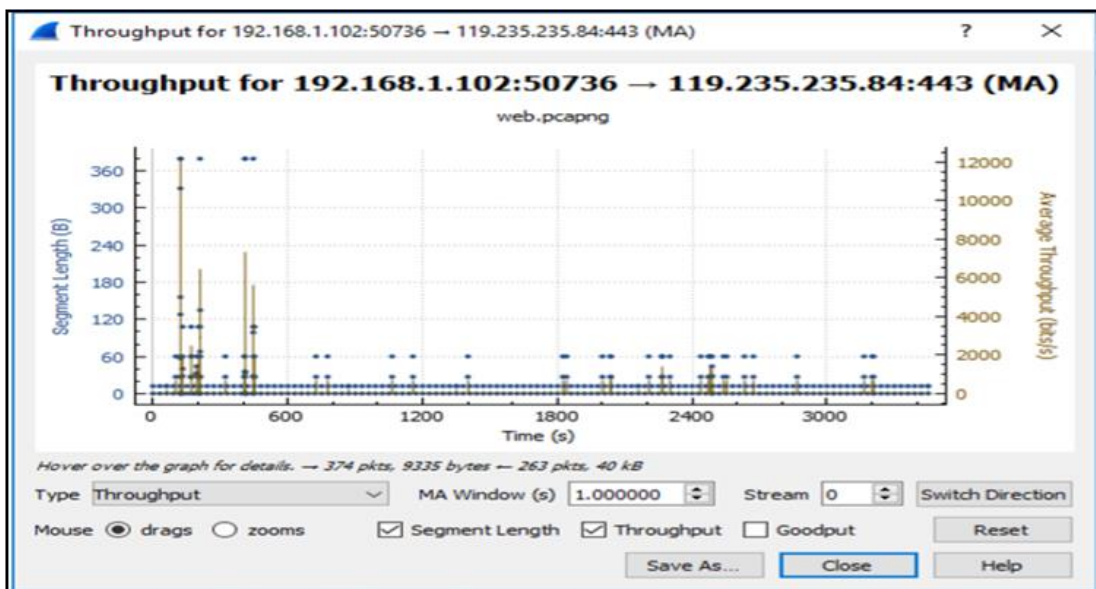
TCP Stream Graph เป็นอีก Feature หนึ่งที่น่าสนใจของโปรแกรม Wireshark เนื่องจากความสามารถของ TCP Stream Graph คือ การแสดงค่าต่าง ๆ ที่แฝงอยู่ในแพ็กเก็ตข้อมูลที่ได้มาให้อยู่ในรูปแบบของกราฟ ซึ่งจะช่วยให้เราสามารถนำความสัมพันธ์ของกราฟที่ได้มาใช้ในการวิเคราะห์การทำงานหรือค้นหาปัญหาที่อาจจะเกิดขึ้นได้อย่างสะดวกแม่นยำ ข้อมูลที่ TCP Stream Graph สามารถแสดงผลออกมาได้จะถูกแบ่งเป็น ๕ กราฟ โดยจะมีกราฟในส่วน Time/Sequence ที่ซ้ำกันอยู่จำนวนสองกราฟ แต่ทั้งสองกราฟนี้จะทำหน้าที่ในการแสดงผลในส่วนของ Time/Sequence ที่แตกต่างกันแยกตามชนิดของกราฟได้ ดังต่อไปนี้

๓.๓.๒๗.๑ Round – Trip Time Graph เป็นกราฟที่ใช้แสดงค่าของช่วงเวลา ที่แพ็กเก็ตเดินทางในระบบเครือข่าย หลักการสังเกตง่าย ๆ ในการนำ Round – Trip Time มาใช้ กล่าวคือ กราฟจะมีความหนาแน่นใกล้กับแกน X มากที่สุด หรือก็คือแพ็กเก็ตสามารถเดินทางในเครือข่ายได้รวดเร็วนั่นเอง โดยแต่ละจุดในกราฟคือแพ็กเก็ตแต่ละชิ้นส่วน และจากกราฟแสดงให้เห็นว่าค่า Round-Trip Time ของแพ็กเก็ตชุดนี้อยู่ในระดับที่ต่ำ เนื่องจากค่าเฉลี่ยของ RTT จะอยู่ใกล้เคียงกับเวลา ๐.๑ วินาทีนั่นเอง



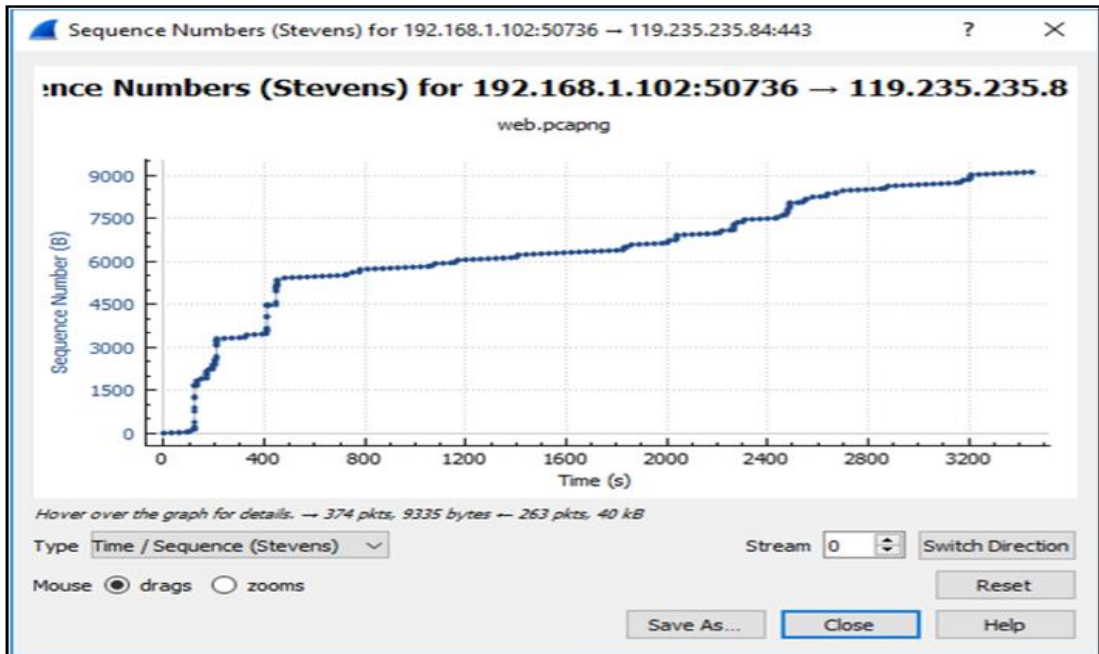
ภาพที่ ๕๔ แสดงค่า Round - Trip Time ของเครือข่าย

๓.๓.๒๗.๒ กราฟ Throughput เป็นกราฟที่ใช้แสดงค่า Throughput จาก Source -> Destination ในทิศทางเดียว ดังนั้นกรณีที่ต้องการดูค่า Throughput แล้วในกราฟไม่แสดงค่าใด ๆ ขึ้นมา ให้ลองทำการสลับค่า Source <-> Destination ดูก่อนทุกครั้ง การใช้งานกราฟ Throughput โดยทั่วไปแล้วจะใช้สังเกตแนวโน้มของข้อมูลที่ผ่านเข้าออกในระบบเครือข่าย หรือนำไปใช้ในการสังเกตการลดค่าหรือ Throughput Drop ในกรณีที่มีการสื่อสารมีปัญหา



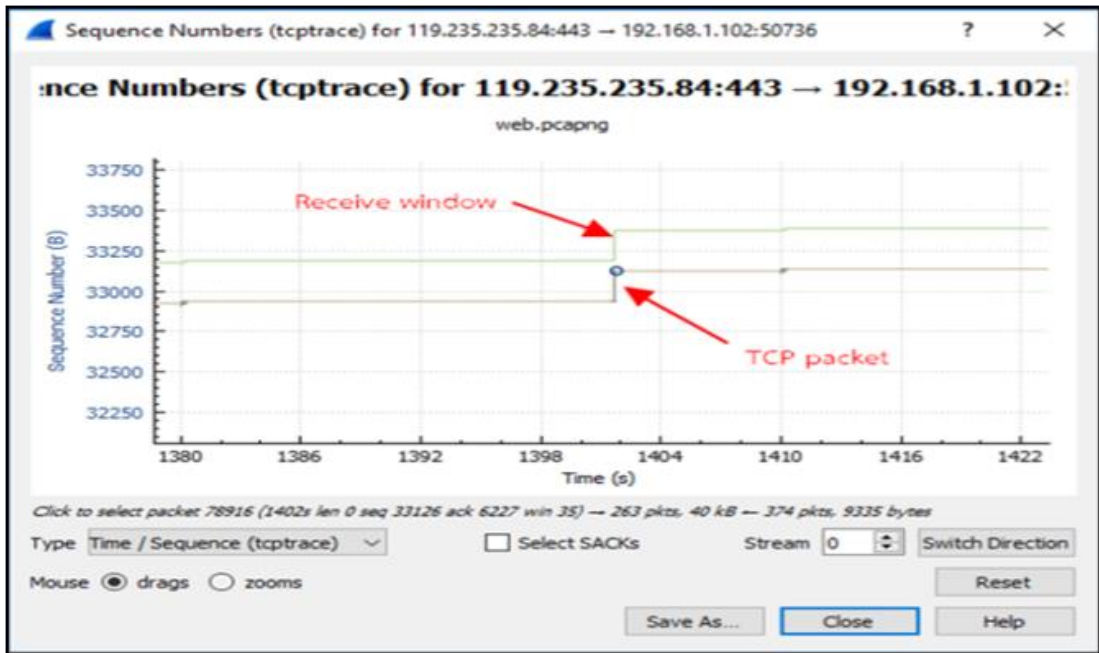
ภาพที่ ๕๕ แสดงค่า Time/Sequence (Steven's - Style)

๓.๓.๒๗.๓ Time/Sequence (Steven's – Style) กราฟ Time/Sequence แบบ Steven เป็นกราฟแสดงความสัมพันธ์ของ TCP แพ็กเก็ตกับ Sequence Number อย่างง่าย โดยในแต่ละจุดคือแพ็กเก็ตเช่นเดียวกันกับใน Round – Trip Time กราฟแต่ใน ส่วนของแกน Y จะเป็นการแสดงหมายเลขของ Sequence number รูปกราฟแบบ Steven เมื่อมีการใช้งานอินเทอร์เน็ต



ภาพที่ ๕๖ แสดงค่า Time/Sequence (tcptrace – Style)


๓.๓.๒๗.๔ Time/Sequence (tcptrace – Style) กราฟ Time/Sequence แบบ Tcptrace เป็นกราฟที่ใช้แสดงความสัมพันธ์ของแพ็กเก็ตกับ Sequence Number เช่นเดียวกับกับแบบ Steven แต่มีความพิเศษตรงที่กราฟแบบ Tcptrace จะแสดงค่า Window size และค่า ACK ทำให้เราสามารถเห็นการเกิด Network Retransmission, Window Size Update และ Window Size Zero ได้ละเอียดและชัดเจนกว่าการใช้กราฟแบบ Steven



ภาพที่ ๕๗ แสดงค่า TCP Packet

๓.๓.๒๗.๕ Window Scaling เป็นกราฟที่ใช้แสดงขนาด ของข้อมูลจาก Source -> Destination ในแบบทิศทางเดียว โดยแต่ละจุดจะเป็นการแสดงความขนาดของ Window size ในช่วงเวลานั้น ๆ การใช้งานกราฟนี้สามารถเห็นความเปลี่ยนแปลงได้อย่างชัดเจนของค่า Window Scaling แต่ข้อเสียของการใช้งาน TCP Stream Graph คือ กราฟที่แสดงผลนั้นในส่วนของ แกน x จะเป็นส่วนที่ใช้สำหรับการแสดงค่าเวลาที่เริ่มนับจาก “๐” กล่าวคือ เวลาที่เริ่มต้นในการเก็บ แพ็กเก็ตนั้นจะมีการนับต่อไปเรื่อย ๆ ซึ่งไม่ได้มีการแสดงค่าเวลาที่แท้จริงในขณะที่เริ่มทำการเก็บแพ็กเก็ต เช่น เราเริ่มทำการเก็บแพ็กเก็ตเพื่อนำมาวิเคราะห์การทำงานของโปรแกรมหนึ่งใช้เวลา ๑๓๔๐ แต่การแสดงผลค่าเวลาของ TCP Stream Graph จะทำการแสดงผลเริ่มต้นที่เวลาเท่ากับ “๐” และเพิ่มขึ้นไปเรื่อย ๆ ไม่ได้แสดงค่าเวลาเป็น ๑๓๔๐ ตามเวลาจริงที่เราเริ่มทำการเก็บข้อมูล เป็นต้น ส่วนต่อมาก็คือการแสดงผลของ TCP Stream Graph นั้น จะเป็นการแสดงผลรวมทั้งหมดที่เกิดจากแพ็กเก็ตที่เราเก็บข้อมูลมาได้แล้ว ทำการบีบอัดการแสดงผลให้พอดีอยู่ในหน้าเดียว ดังนั้นการแสดงผลจะไม่มีรายละเอียดมากพอ เช่น กรณีที่เราทำการเก็บข้อมูลแพ็กเก็ตในระยะเวลา ๕ นาที และนำมาแสดงผลที่ TCP Stream Graph จะมีการแสดงผลในแกน x เท่ากับข้อมูลแพ็กเก็ตที่ใช้ระยะเวลาในการเก็บเป็นระยะเวลา ๒ หรือ ๔ ชั่วโมงก็ได้ ดังนั้นต้องระมัดระวังในการนำ TCP Stream Graph ไปใช้งานในส่วนนี้ด้วยการจัดการไฟล์ .pcapng ในหลายสถานการณ์เรามีความจำเป็นที่จะต้องมีการลองดึงข้อมูลที่ต้องการ วิเคราะห์ปัญหาออกมาจากอุปกรณ์ Network เป็นเวลานานแบบต่อเนื่อง เพื่อให้ได้ข้อมูลที่มากพอ หรือเพื่อให้ครอบคลุมช่วงเวลาที่เกิดปัญหาเพื่อที่จะนำข้อมูลที่ได้มาใช้งานต่อไป ถึงแม้ในบางครั้ง ข้อมูลที่เราอยากได้นั้นอาจจะมีจำนวนแค่หลักสิบหรือหลักร้อยแพ็กเก็ต (Packet) ไม่สามารถคาดเดาได้ว่าปัญหาที่เกิดขึ้นนั้นจะเกิดขึ้นในช่วงใดได้บ้าง ทำให้เราอาจต้องเก็บข้อมูลค้างไว้นานหลายชั่วโมง หรืออาจจะต้องเก็บข้อมูลกันข้ามวันเลยทีเดียว

จากภาพที่ ๕๘ เป็นข้อมูลตัวอย่างจากการเก็บข้อมูลเพื่อนำไปวิเคราะห์การปัญหาที่เกิดขึ้นในช่วงเวลาประมาณไม่เกินสามชั่วโมง จะเห็นได้ว่าไฟล์มีขนาดใหญ่ถึง 3.7GB

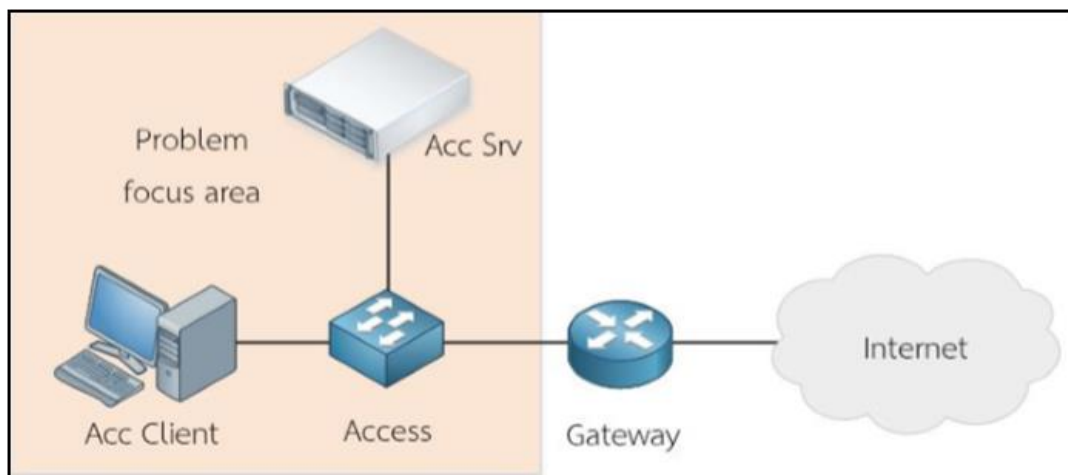
Name	Size	Type
 demo.pcapng	3,798,536 KB	Wireshark capture file

ภาพที่ ๕๘ ตัวอย่างขนาดของแพ็คเกจไฟล์ที่นำมาใช้วิเคราะห์ปัญหา

ดังภาพที่ ๕๘ ถ้าจะนำไฟล์มาใช้งานจะเกิดเหตุการณ์อะไรบ้าง ทั้งในระหว่างการเก็บข้อมูลเพื่อให้ได้ไฟล์มา หากจะสรุปเหตุการณ์ที่เป็นไปได้ จะสามารถเขียนออกมาได้ ดังนี้

(๑.) ระหว่างเก็บข้อมูลของไฟล์ a. ถ้า Disk ที่ใช้เก็บข้อมูลมีขนาดไม่พอเนื่องจากประเมินไม่ได้ว่าจะต้องเก็บไฟล์ขนาดไหนจะเป็นอย่างไร กรณี Disk IO ที่ใช้รองรับการเขียนไฟล์จะพอหรือไม่ ถ้าไม่พอก็ได้ข้อมูลไม่ครบตามต้องการ หรือเมื่อเก็บข้อมูลเสร็จแล้วจะทำการ Save ข้อมูลเพื่อนำไปใช้งานต่อจะสามารถดำเนินการได้หรือไม่

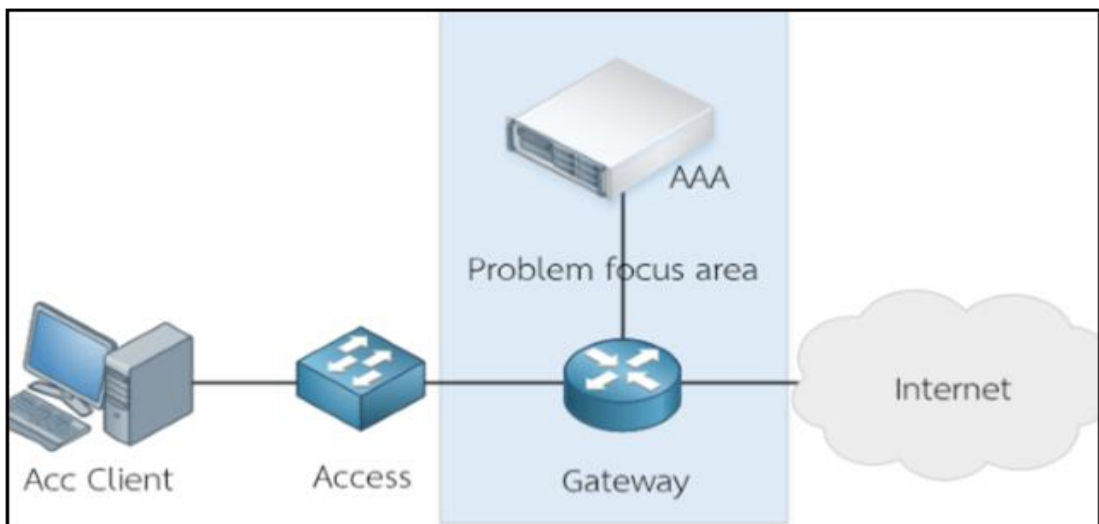
(๒.) ระหว่างนำไฟล์ไปใช้ เครื่องที่นำไฟล์นี้ไปเปิดใช้งานจะสามารถเปิดไฟล์นี้ได้หรือไม่ ในการประมวลผลจากไฟล์นี้จะต้องใช้เครื่องที่มีประสิทธิภาพขนาดไหน ในการกรองหาข้อมูลที่ต้องการและนำมาแสดงผล จะสามารถแสดงผลได้หรือไม่ ราวกับว่าไม่อาจนำข้อมูลไปใช้งานต่อได้ ดังนั้น เพื่อให้สามารถนำข้อมูลที่ได้นำไปใช้งานต่อได้อย่างมีประสิทธิภาพ สิ่งที่สำคัญที่สุดก่อนการเริ่มเก็บข้อมูลคือ การวางแผนและเตรียมการให้เหมาะสมทั้งก่อนและหลังการเก็บข้อมูล เช่น บริษัท A มีปัญหาการใช้งาน Application ของฝ่ายบัญชีตัวหนึ่งในช่วงเวลาประมาณ ๑๖๓๐ ของทุกวัน เป็นระยะเวลาติดต่อกันมานานกว่า ๓ เดือน โดยไม่ทราบสาเหตุ โดยอาการคือในช่วงเวลา ๑๖๓๐ - ๑๗๓๐ ฝ่ายบัญชีจะไม่สามารถดึงข้อมูลจาก Database ได้ หรือถ้าดึงข้อมูลได้ก็จะใช้เวลามากกว่าปกติมาก เป็นต้น



ภาพที่ ๕๙ ตัวอย่างการกำหนดขอบเขตเพื่อจำกัดการเก็บข้อมูลเพื่อแก้ปัญหาของบริษัท A

แนวทางในการแก้ไขปัญหา เพื่อที่จะได้เห็นการเปลี่ยนแปลงทั้งก่อนและหลัง ช่วงเวลาที่เกิดปัญหา เราอาจจะต้องเก็บข้อมูลในระหว่างเวลา ๑๖๐๐ - ๑๘๐๐ ก่อนที่ปัญหา จะเกิดขึ้น โดยอาจเลือกเก็บข้อมูลแค่ฝ่ายบัญชีก็ได้ แต่ในการเก็บข้อมูลที่ต้องการวิเคราะห์ ควรจะมี แค่การใช้งานในส่วนของ Datacenter และฝ่ายบัญชีเท่านั้น การใช้งาน Internet ไม่ควรเก็บมาด้วย ทั้งนี้การเก็บข้อมูลต่อเนื่องยาวนาน ๒ ชั่วโมงอาจจะทำให้ได้ไฟล์ขนาดใหญ่มาก ดังนั้นอาจจะต้องตั้ง ค่าให้โปรแกรม Wireshark หรือ TCPDump มีการจำกัดขนาดของไฟล์ให้เป็นขนาดเล็ก ๆ ในแต่ละรอบก็ได้ เช่น กำหนดให้โปรแกรม Save ไฟล์ เมื่อไฟล์มีขนาด 200M เป็นต้น

อีกกรณีหนึ่งที่น่าสนใจ คือ บริษัท B มีปัญหาจากการที่ Network Admin ไม่สามารถ Configure อุปกรณ์ที่ตนเองมีหน้าที่รับผิดชอบได้ แต่สามารถ Login เข้าไปในอุปกรณ์ เพื่อแสดงค่าต่าง ๆ ได้ แต่ต้องใช้ Local Admin เท่านั้นจึงจะสามารถ Configure อุปกรณ์ได้ตามปกติ



ภาพที่ ๖๐ ตัวอย่างการกำหนดขอบเขตเพื่อจำกัดการเก็บข้อมูลเพื่อแก้ปัญหาของบริษัท B

รูปแบบของปัญหาของบริษัท B จะเน้นไปที่การทำงานร่วมกันของ AAA และอุปกรณ์ Network เป็นหลัก อาจจะใช้การดู Log ที่อุปกรณ์เพื่อตรวจสอบปัญหาเบื้องต้นก่อน ในบางกรณีก็ อาจจะแก้ปัญหาได้ แต่ก็เห็นได้ว่าปัญหาที่เกิดขึ้นมีเฉพาะเวลาแบบเจาะจงและเกิดขึ้นเฉพาะตอน Login ดังนั้น การเก็บข้อมูลมาเฉพาะที่เกิดปัญหามาดูก็น่าจะเพียงพอ

๓.๓.๒๘ การแบ่งขนาดของไฟล์ระหว่างเก็บข้อมูลโดย Wireshark

การกำหนดให้ Wireshark แบ่งข้อมูลออกเป็นส่วน ๆ ในระหว่างเก็บข้อมูล แพ็กเก็ต สามารถสามารถเลือก Option ได้ ๓ แบบ ดังนี้

๓.๓.๒๘.๑ แบ่งโดยใช้จำนวนของ Packet เช่น เมื่อมี แพ็กเก็ต 100,000 Packet เป็นต้น

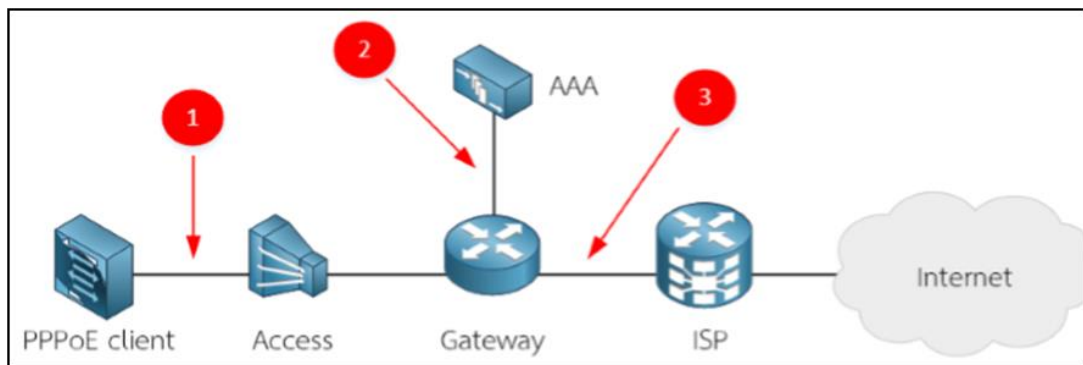
๓.๓.๒๘.๒ แบ่งโดยคำนวณจากขนาดของข้อมูล เช่น เมื่อมีขนาดของไฟล์ 200 MB เป็นต้น

๓.๓.๒๘.๓ แบ่งโดยใช้ระยะเวลา เช่น ให้แบ่งไฟล์ใหม่ทุก ๆ ๕ นาที เป็นต้น

ทั้งนี้ การแบ่งไฟล์โดยกำหนดจากขนาดของไฟล์จะสะดวกมากที่สุด เนื่องจากในการทำงานจริง ส่วนมากปัญหาที่พบจะไม่สามารถกำหนดระยะเวลาที่แน่นอนได้ ทำให้บางครั้งอาจใช้เวลามากกว่า ๑๒ ชั่วโมง และข้อมูลในแต่ละช่วงเวลาก็มีขนาดไม่เท่ากัน เช่น ถ้าเก็บข้อมูลในช่วงเช้า พนักงานทุกคนจะใช้ระบบ Network เป็นจำนวนมาก เนื่องจากต้องเข้าใช้งานระบบพร้อม ๆ กัน และจะเริ่มลดปริมาณการใช้งานลงหลังจากนั้นอีกประมาณ ๒ ชั่วโมง และเริ่มมีการใช้งานมากอีกครั้งหลังจากช่วงพักกลางวัน หรือกรณีของ ISP ที่ให้บริการ FTTH จะมีปริมาณการใช้งานมากเป็นพิเศษในช่วงเย็นไปจนถึงเวลาประมาณเที่ยงคืนหรือถึงตีสาม และจะลดลงในช่วงเวลากลางวัน ทั้งนี้การแบ่งข้อมูลออกเป็นส่วน ๆ ตามขนาดของข้อมูลที่ได้จึงเหมาะสมในกรณีแบบนี้ โดยขนาดของไฟล์ที่เหมาะสมจะอยู่ที่ประมาณ 150MB - 250MB ต่อหนึ่งไฟล์ เนื่องจากไฟล์จะมีขนาดพอดีในการใช้เครื่องที่มี Spec เครื่องที่ไม่สูงมากในการเปิดไฟล์เปิดขึ้นมาทำการวิเคราะห์ข้อมูล

๓.๓.๒๙ การรวมไฟล์ .pcapng หลายไฟล์เข้าด้วยกัน

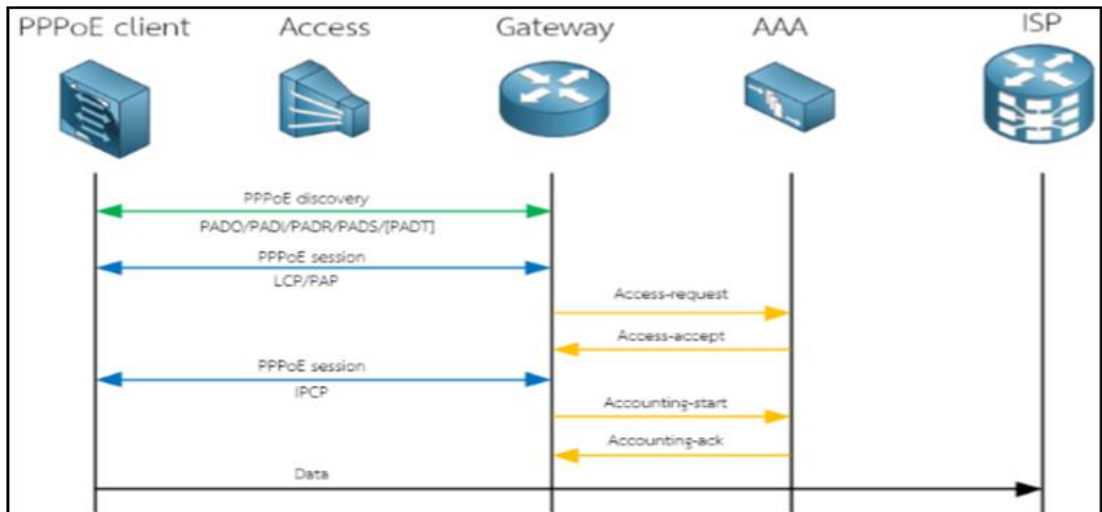
บ่อยครั้งที่การวิเคราะห์ปัญหาไม่สามารถตรวจสอบได้จากการดูข้อมูลจากจุด ๆ เดียว เช่น เราไม่สามารถตอบได้ว่าปัญหาเกิดขึ้น ณ จุดที่ ๑ หรือ ๒ หรือ ๓ ได้ ถ้าหากเราไม่สามารถเห็นภาพรวมของระบบ เป็นต้น ทำให้ในหลายครั้งการตัดสินใจแก้ปัญหาอาจจะทำไปโดยไม่มีข้อสรุปที่ชัดเจน เช่น จากภาพที่ ๖๑ เราไม่พบว่าเกิดการ Authentication ที่จุดที่ ๒ ซึ่งบางครั้งผู้วิเคราะห์ระบบอาจจะตีความไปว่าอุปกรณ์ Gateway มีปัญหา เพราะไม่ส่ง Authentication Message ออกมาทั้ง ๆ ที่อาจจะเป็นที่อุปกรณ์ Access หรือ PPPoE Client ไม่มีการส่ง Message ออกมาก็เป็นได้ ทั้งนี้การมาเปิด Session ก่อนแล้วจึงจะเกิด Authentication Message จาก Gateway ไปที่ AAA นั้นก็สามารถเกิดขึ้นได้เช่นกัน เป็นต้น



ภาพที่ ๖๑ การเก็บข้อมูลและมองปัญหาจากจุดต่าง ๆ ใน Network

ดังภาพที่ ๖๑ จะเห็นได้ว่าถ้าพบปัญหาเพียงจุดเดียวเราอาจจะวิเคราะห์ปัญหาผิดพลาดได้ ดังนั้น การเก็บข้อมูลให้ครบถ้วนจากจุดต่าง ๆ ในระบบ Network เป็นเรื่องที่ต้องทำ เพื่อให้สามารถเห็น แพ็กเก็ต ในภาพรวมได้อย่างถูกต้องครบถ้วน แต่การเก็บ แพ็กเก็ต เข้ามาจากจุดต่าง ๆ ใน ระบบ Network โดยทั่วไปแล้วจะเก็บมาจากอุปกรณ์ต่างชนิดกัน กรณีที่ต้องการเก็บข้อมูลจาก Network ในจุดที่ ๑ - ๓ อาจจะต้องใช้ Server ถึง ๓ ตัวแยกกันในการเก็บข้อมูล เมื่อได้ข้อมูลที่ต้องการแล้ว โดยทั่วไปจะทำการเปิดไฟล์แต่ละชุดแล้วจึงตรวจสอบใหม่ ซึ่งอาจจะพอมองเห็น

ปัญหาได้ครอบคลุมได้ ทั้งนี้เราต้องใช้วิธีการรวมไฟล์ชุดต่าง ๆ เข้าด้วยกันก่อนแล้วจึงค่อยตรวจสอบสิ่งที่เกิดขึ้นจากภาพรวม เพื่อที่จะสรุปปัญหาออกมาเป็นจุดต่าง ๆ ได้แม่นยำขึ้น



ภาพที่ ๖๒ ภาพรวมการให้บริการ Internet โดยใช้ PPPOE

เมื่อลองเปรียบเทียบการทำงานโดยใช้ Application Flow Diagram จะเห็นได้ว่าปัญหาที่เจอเป็นการที่ Gateway ไม่ส่ง Authentication Message ไปหา AAA ทำให้ทราบมาก่อนที่จะมีการส่ง Authentication Message (Access-Request) จะต้องเกิด Message จาก PPPoE Client กล่าวคือ กลุ่มของ PPPoE Discovery และ PPPoE Session ประเภท LCP/PAP จะมีการรับส่งข้อมูลไปมาหากันให้ครบก่อนที่ Gateway จะมีการส่ง Authentication Message (Access-Request) ออกไปที่ AAA ดังนั้น ปัญหาอาจจะเกิดจากการที่ Client มีการส่ง Message ไม่เป็นไปตามขั้นตอนการทำงาน จากภาพที่ ๖๒ ทำให้เห็นถึงปัญหาในภาพรวมผ่าน Application Flow Diagram โดยมีขั้นตอนโดยสรุป ดังนี้

- (๑) ใช้โปรแกรม Wireshark รวมไฟล์ที่กำหนดให้เพื่อให้เป็นแพ็คเกจทั้งหมดในภาพรวมก่อน
- (๒) ใช้งาน Filter Command เพื่อแยกเฉพาะข้อมูลที่สนใจออกมาจากแพ็คเกจทั้งหมด
- (๓) ใช้งาน Flow Graph เพื่อสร้าง Protocol/Application Flow ออกมาจากส่วนที่ทำงานถูกต้อง มาใช้เป็นข้อมูลในการอ้างอิงการทำงาน เพราะเมื่อใดก็ตามที่มีการทำงานที่ผิดปกติ เราก็จะสามารถใช้ Protocol/Application Flow ในการอ้างอิงได้ และยังเป็นการช่วยให้เราหาจุดที่ทำงานผิดพลาดได้รวดเร็วมากขึ้นอีก
- (๔) เมื่อได้ Protocol/Application Flow จาก Wireshark แล้วก็ให้ลองสร้าง Protocol/Application Flow ออกมาด้วยตนเอง โดยให้วาดลงกระดาษใช้โปรแกรมต่าง ๆ ช่วยก็ได้ โดยมีหลักการคือพยายามจัด Packet ให้เป็นกลุ่มก่อน และใช้ลูกศรแสดงทิศทางการทำงานของ Protocol/Application ด้วย เพียงเท่านี้ก็ทำให้เราสามารถวิเคราะห์ปัญหาทางเครือข่ายผ่านเครื่องมือของ Wireshark ได้อย่างมีประสิทธิภาพ

บทที่ ๔ การเก็บหลักฐาน

การเก็บหลักฐาน ในขั้นตอนแรกจะต้องดำเนินการตรวจสอบคำร้องก่อนว่าต้องการให้ดำเนินการเก็บหลักฐานแบบฟอเรนสิคหรือไม่ หากต้องนำไปฟอเรนสิคจำเป็นต้องปฏิบัติตาม “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” แต่ถ้าไม่ก็ให้ตรวจสอบดูก่อนว่าเครื่องได้ทำการปิดอยู่หรือไม่ (แนะนำให้เปิดอยู่ดีที่สุด) กรณีที่เครื่องเปิดอยู่ควรให้ผู้รับผิดชอบหรือเจ้าของเครื่องทำการ Login เข้าสู่ระบบพร้อมทั้งรวบรวมข้อมูล User และ Password ของเจ้าของระบบมาด้วย จากนั้นจึงทำการถ่ายภาพหน้าจอ หมายเลขเครื่อง Port หรือจุดที่มีการเชื่อมต่อ รวมถึงบริเวณโดยรอบด้วย จากนั้นจึงดำเนินการเก็บหลักฐาน RAM เป็นอันดับแรกด้วยโปรแกรมใดโปรแกรมหนึ่ง โดยลำดับขั้นตอนการดำเนินการเก็บหลักฐานจะมีรายละเอียด ดังนี้

๔.๑ การเตรียมการ

ต้องทราบขนาดของฮาร์ดดิสก์เครื่องเกิดเหตุมีขนาดเท่าใด เพื่อที่จะสามารถจัดเตรียมฮาร์ดดิสก์ของเราให้เพียงพอกับขนาดข้อมูลที่จะดำเนินการเก็บหลักฐาน และควรทราบประเภทคอมพิวเตอร์ที่จะดำเนินการเก็บหลักฐานว่าเป็นเครื่อง Server, VMware , PC หรือ Notebook เพื่อจะได้เตรียมเครื่องมือสำหรับจัดเก็บหลักฐานได้ถูกต้อง

๔.๒ การเข้าพื้นที่

ต้องขออนุญาตเจ้าของพื้นที่และควรให้เจ้าของพื้นที่เป็นผู้นำทางไปพร้อมสอบถามอาการเบื้องต้นเพื่อประเมินการเก็บหลักฐาน

๔.๓ การจำกัดการแพร่กระจาย

ในกรณีที่เป็นพวงมัลแวร์จำเป็นต้องทำการตัดการเชื่อมต่อระบบ Network โดยรอบก่อนเพื่อป้องกันการแพร่กระจายของมัลแวร์

๔.๔ การจัดลำดับการเก็บหลักฐาน

ให้เริ่มจากการสำรวจจุดเชื่อมต่อทาง Network จากนั้นจึงไล่เรียงเส้นทางมายังเครื่องที่เกิดเหตุ โดยจะต้องสังเกตว่าเครื่องคอมพิวเตอร์ ณ เวลาที่เข้าไปดำเนินการเก็บหลักฐานมีการเปิดใช้งานอยู่หรือไม่ ถ้าเป็นเครื่องมีการเปิดใช้งานอยู่ ก็ต้องทำการเก็บ RAM ของระบบเป็นอันดับแรก ตามด้วยฮาร์ดดิสก์ และข้อมูลอื่น ๆ ของเครื่อง รวมถึงช่วงเวลาในการใช้งานของระบบ

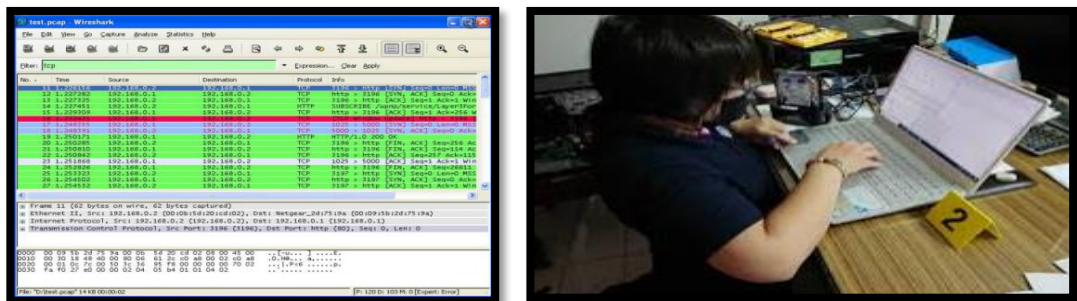
๔.๕ การเก็บหลักฐานเครือข่าย

๔.๕.๑ เครือข่ายภายนอก หรือกายภาพเครือข่าย เช่น อุปกรณ์ Switch มีการเชื่อมต่อไปยังหน่วยงานใด ได้รับ IP วงไหน มีการกระจาย Wifi ในหน่วยงานหรือไม่ มีการแบ่งระบบ VLAN ในระบบหรือไม่ มีการกำหนด Gateway ไปยังที่ใด ทั้งนี้หากได้แผนผังระบบเครือข่าย ของหน่วยงานที่เกิดเหตุมาได้อีกก็จะช่วยให้สามารถวิเคราะห์ปัญหาได้รวดเร็วยิ่งขึ้น



ภาพที่ ๖๓ การเก็บหลักฐานด้าน Network ภายนอก

๔.๕.๒ เครือข่ายภายใน คือ ข้อมูลที่เป็นการติดต่อสื่อสารผ่านเครือข่ายซึ่งเกิดขึ้นภายใน อุปกรณ์เครือข่าย ประกอบด้วยข้อมูล Logs จากอุปกรณ์ Network หมายเลข IP ที่มีการเชื่อมต่อ โดยควรรวบรวมข้อมูลผลการ Scan IP ของเครือข่ายที่เกิดเหตุมาด้วย หรืออาจใช้โปรแกรม Nmap เพื่อทำการ Scan ช่องโหว่ของระบบที่เกิดเหตุ รวมถึงข้อมูลการติดต่อสื่อสารหรือ .pcap ไฟล์ ที่มีการดักจับแพ็กเก็ตเอาไว้



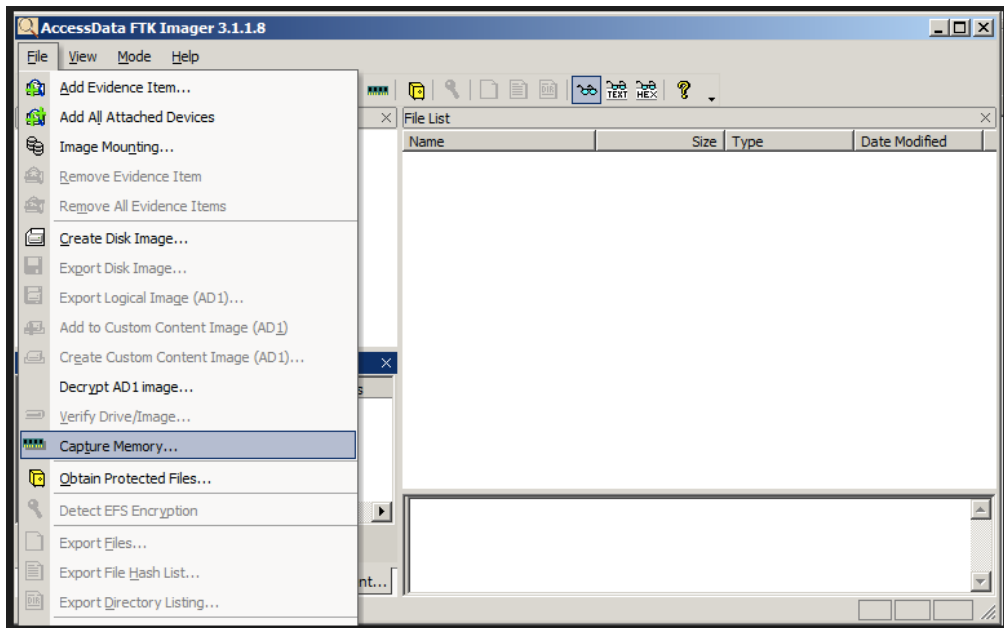
ภาพที่ ๖๔ การเก็บหลักฐานด้านเครือข่าย ภายใน

๔.๖ การเก็บหลักฐานเครื่องโฮส

๔.๖.๑ ข้อมูลโฮสพื้นฐาน เป็นการรวบรวมข้อมูลระบบปฏิบัติการที่ใช้ รุ่น เวอร์ชัน Password เข้าสู่ระบบ (เก็บเป็นความลับใช้แค่ใน lab เท่านั้น ห้ามพิมพ์ลงเอกสารรายงาน ให้ใช้สัญลักษณ์ #### แทน) และซอฟต์แวร์ที่ต้องสงสัยภายใน ข้อมูลช่องเสียบอุปกรณ์มีอะไรบ้าง ต่อใช้งานหรือไม่ เชื่อมต่อกับอะไร ใครมีสิทธิใช้งานบ้าง ใครเป็นคนใช้งานคนล่าสุดก่อนเกิดเหตุการณ์ รวมถึงอุปกรณ์ต่อพ่วงอื่น ๆ เช่น การ์ดแลน ๒ ตัว, เครื่องปริ้นท์, กล้อง, CD และ DVD เป็นต้น

๔.๖.๒ RAM ควรทราบว่าเครื่องที่เกิดเหตุใช้ RAM รุ่นอะไร DDR1, 2, 3 หรือ 4 มีความจุรวมเท่าไร ที่สำคัญคือ เราจะสามารถเก็บข้อมูล RAM ได้ก็ต่อเมื่อเหตุการณ์เกิดขึ้นแล้วเครื่องคอมพิวเตอร์ยังคงเปิดใช้งานอยู่ และห้ามทำการปิดเครื่องคอมพิวเตอร์ เพราะจะทำให้บางโปรแกรมลบตัวเองหลังจาก Restart หรือ Shutdown ไป

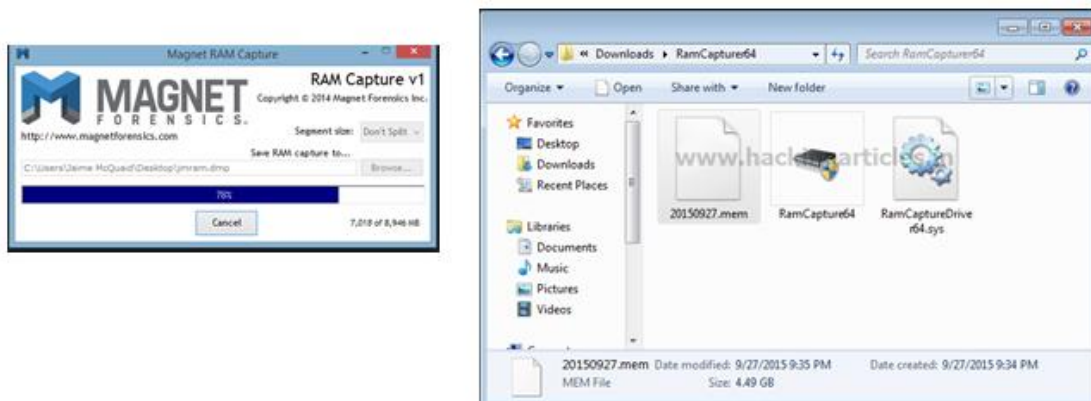
๔.๖.๒.๑ การเก็บ Image Ram ด้วย FTK Imager



ภาพที่ ๖๕ การเก็บหลักฐาน RAM

ต้องติดตั้งโปรแกรม FTK Image ลงไปในเครื่องก่อน จากนั้นให้เปิดโปรแกรม แล้วไปที่ File > Capture Meory จากนั้นในช่องที่ ๑ ทำการเลือกไฟล์ไปที่ USB ที่จะใช้เก็บไฟล์ ในช่องที่ ๒ ทำการตั้งชื่อโดยมีนามสกุล .mem จากนั้นคลิกเครื่องหมายถูกที่ Icludepagefile แล้วกดปุ่ม Capture Memory

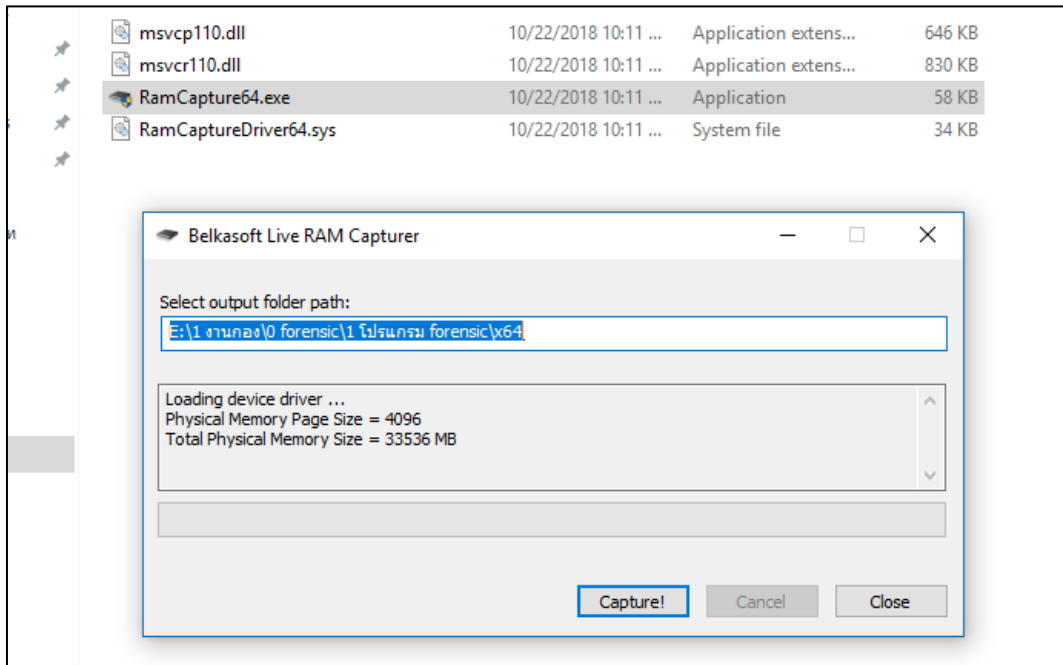
๔.๖.๒.๒ โปรแกรม MagnetRamCapture



ภาพที่ ๖๖ การเก็บหลักฐาน RAM

ให้เสียบ USB ที่มีโปรแกรม MagnetRAMCapture.exe จากนั้นทำการรันโปรแกรม โดยโปรแกรมจะให้เราเลือกตำแหน่งในการจัดเก็บไฟล์ โดยในที่นี้จะสร้างไฟล์ไว้ที่หน้าจอ จากนั้นทำการตั้งชื่อไฟล์ โดยจะต้องมีนามสกุลเป็น .raw กรณีที่ไม่สามารถคัดลอกไฟล์ได้อาจมีสาเหตุมาจาก RAM มีเนื้อที่ทำงานไม่เพียงพอ ให้ทำการ .zip/.rar ไฟล์ก่อนแล้วค่อยคัดลอกไฟล์ .zip มา

๔.๖.๒.๓ โปรแกรม RamCapturer



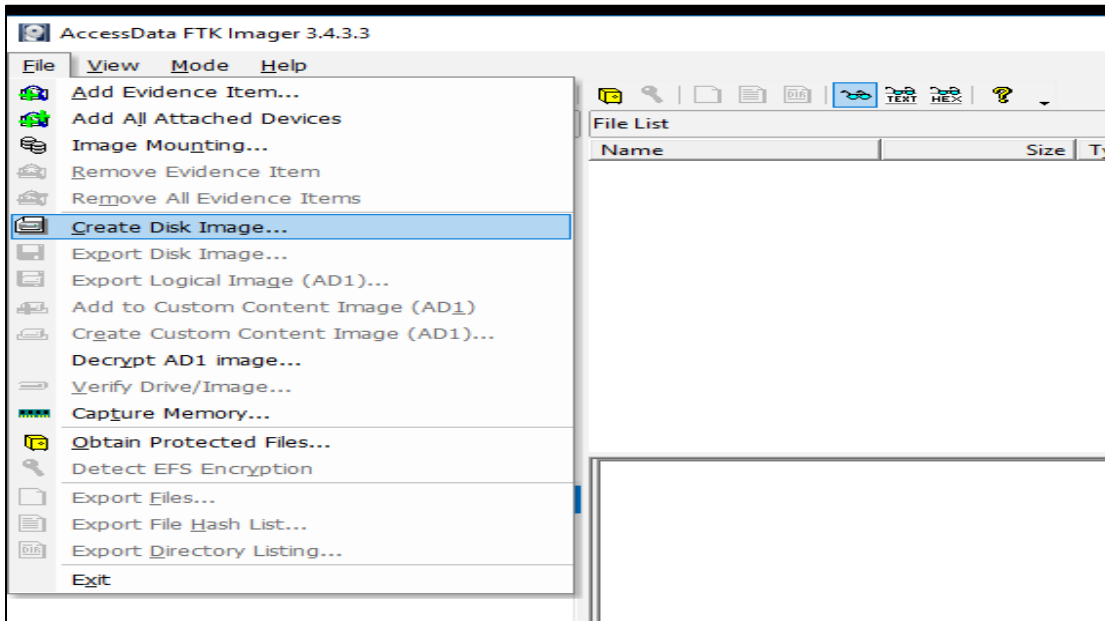
ภาพที่ ๖๗ การเก็บหลักฐาน RAM

โปรแกรม RAMCapture.exe มีข้อดีตรงที่ไม่ต้องติดตั้งโปรแกรมลงในเครื่อง เพียง Run โปรแกรมก็สามารถทำการคัดลอก RAM ได้ทันที ทั้งนี้หลังจากเก็บข้อมูล RAM และควรทำการ Hash ไฟล์ด้วย เพื่อใช้เป็นหลักฐานเวลานำไปวิเคราะห์สามารถใช้เปรียบเทียบเพื่อยืนยันความเที่ยงตรงว่าไม่เกิดการเปลี่ยนแปลงไประหว่างการคัดลอกข้อมูล หรือระหว่างการวิเคราะห์ โดยในระบบ ปฏิบัติการ kali เราจะสามารถใช้คำสั่ง md5sum แล้วตามชื่อไฟล์ได้เลย

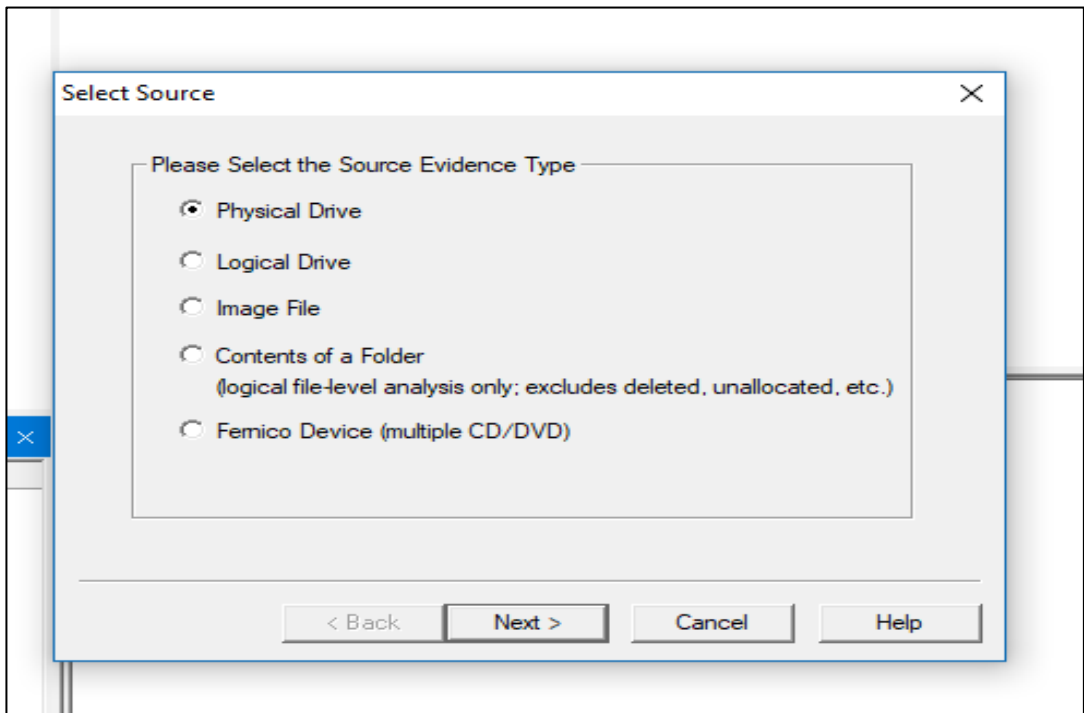
๔.๖.๓ ฮาร์ดดิสก์ ควรตรวจสอบสถาปัตยกรรมในการเชื่อมต่อของฮาร์ดดิสก์ (Raid) ขนาด ความจุ ของฮาร์ดดิสก์ ยี่ห้อ หรือ Version

การเก็บ Image Hardies ด้วยโปรแกรม FTK Imager

การทำงานจะเริ่มจากคลิกที่ File > Create Disk Image... > Physical Drive

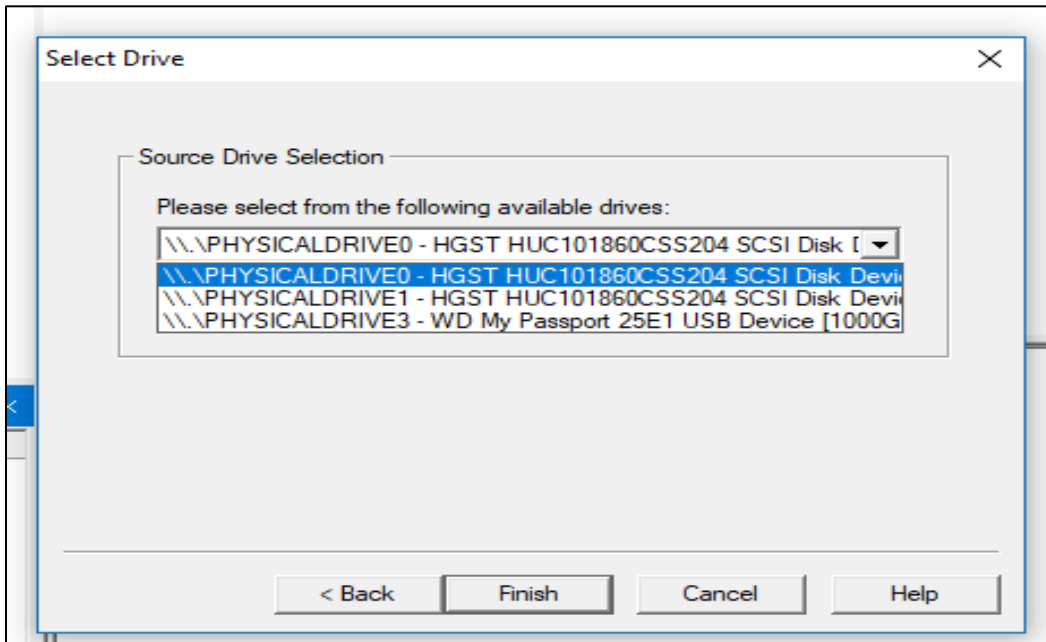


ภาพที่ ๖๘ การเก็บหลักฐาน RAM



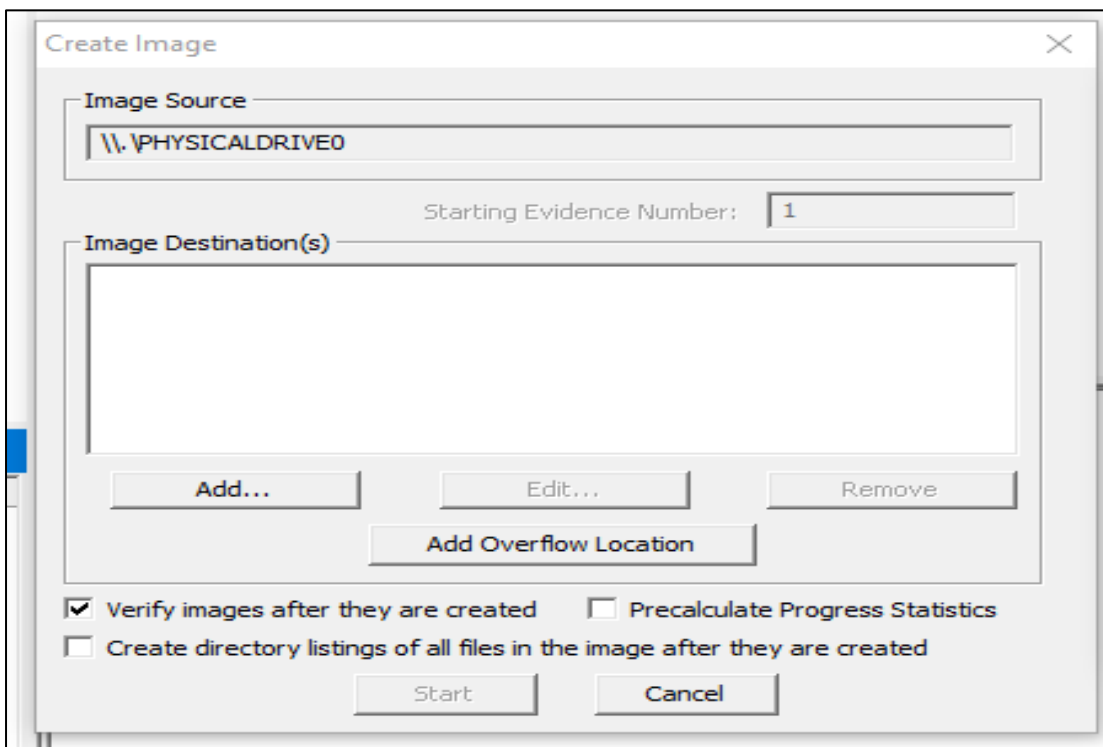
ภาพที่ ๖๙ การเก็บหลักฐาน RAM

จากนั้นทำการเลือกฮาร์ดดิสก์ที่จะทำการสร้าง Image



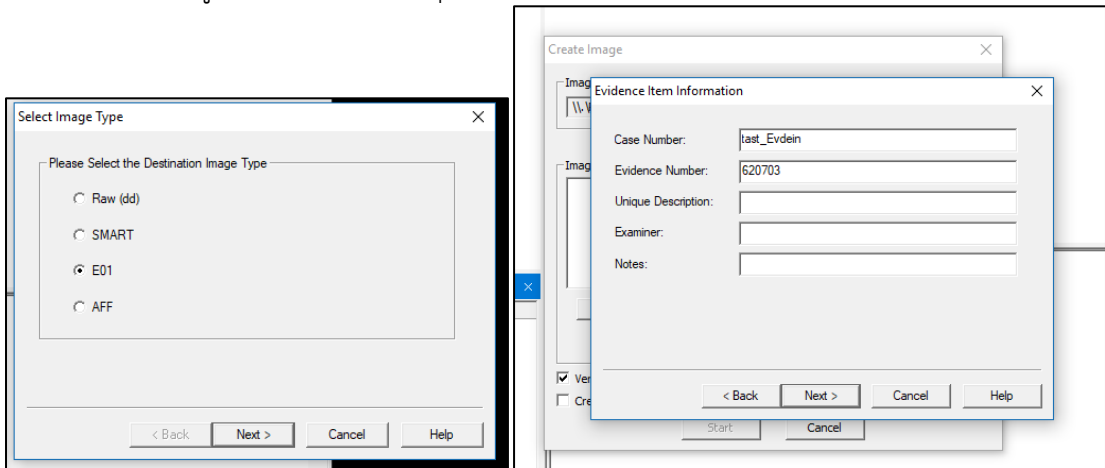
ภาพที่ ๗๐ การเก็บหลักฐาน RAM

ตามด้วยการกดปุ่ม Add



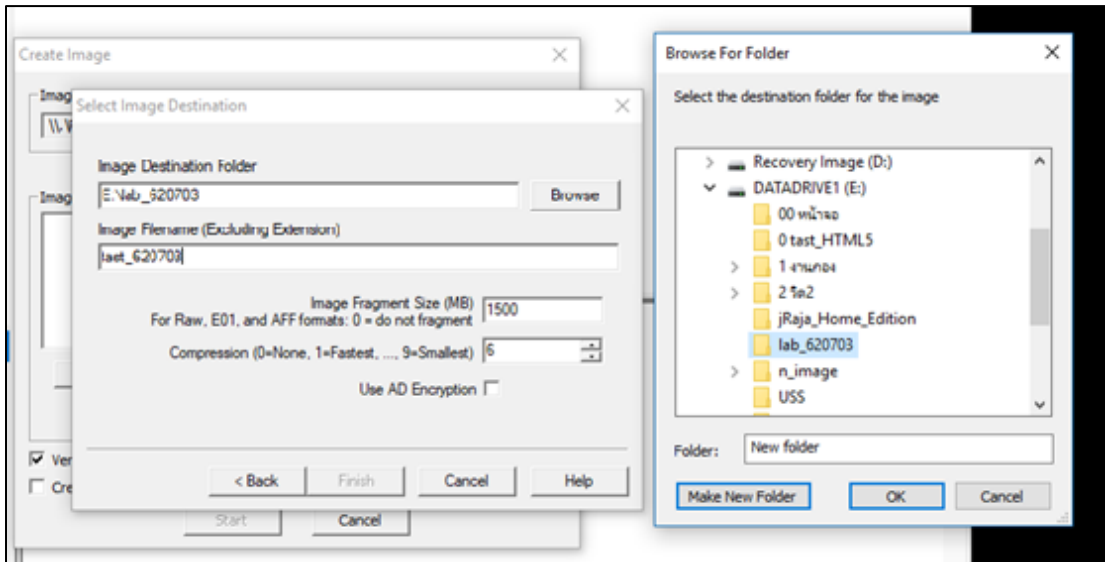
ภาพที่ ๗๑ การเก็บหลักฐาน RAM

ตามด้วยการเลือกรูปแบบไฟล์ (E01ดีที่สุด) พร้อมทั้งชื่อไฟล์



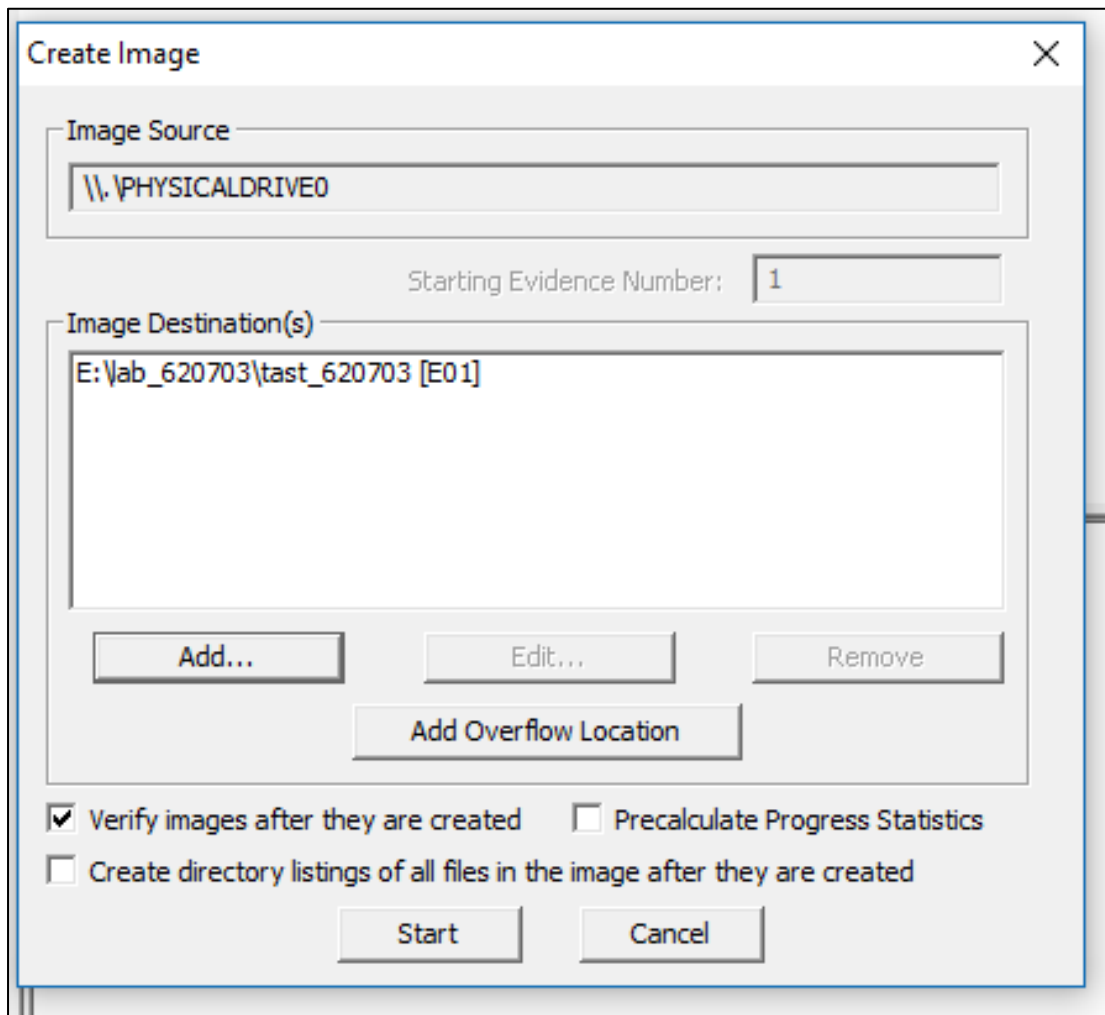
ภาพที่ ๗๒ การเก็บหลักฐาน RAM

เลือกที่แหล่งที่จะเก็บไฟล์ Image



ภาพที่ ๗๓ การเก็บหลักฐาน RAM

จากนั้นก็กดปุ่ม start ได้เลย ซึ่งกระบวนการจะใช้เวลาค่อนข้างนานหลายชั่วโมงขึ้นอยู่กับปริมาณข้อมูลในฮาร์ดดิสก์



ภาพที่ ๗๔ การเก็บหลักฐาน RAM

๔.๗ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)

จะมีความแตกต่างจากกรณีที่แล้วมา เนื่องจากเป็นหลักฐานที่สามารถทำให้เกิดความเสียหาย ทั้งต่อเครื่องมือในการเก็บและข้อมูลที่กำลังจะเก็บด้วย ส่วนใหญ่จะใช้อุปกรณ์พิเศษในการจัดเก็บนั้น คือ Blue Box หรือเครื่องป้องกันการเขียนข้อมูลย้อนกลับ



ภาพที่ ๗๕ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)

๔.๘ การจำกัดพื้นที่เครื่องเกิดเหตุ

ในการเข้าพื้นที่ที่เกิดเหตุ เรามีความจำเป็นต้องทำการควบคุมพื้นที่ที่เกิดเหตุเพื่อป้องกันไม่ให้หลักฐานทางกายภาพเสียหาย โดยทั่วไปจะมีการกางเทปกัน เพื่อควบคุมพื้นที่ ดังภาพที่ ๖๕



ภาพที่ ๗๖ การจำกัดพื้นที่เครื่องเกิดเหตุ

บทที่ ๕ การเตรียมหลักฐาน

กระบวนการเตรียมหลักฐานมีความสำคัญอย่างยิ่งสำหรับงาน Forensics นอกจากจะทำให้ทำงานได้รวดเร็วขึ้นแล้ว ยังช่วยให้กระบวนการทดสอบมีความแม่นยำเพิ่มขึ้นอีกด้วย ทั้งนี้การเตรียมหลักฐานจะเน้นไปที่การจัดสภาพความพร้อมของข้อมูลที่จะทำการวิเคราะห์เป็นหลัก โดยงานหลัก ๆ จะเป็นการทำให้ข้อมูลอยู่ในสภาพที่พร้อมจะทำการวิเคราะห์ ซึ่งโดยธรรมชาติของหลักฐานทางดิจิทัลเมื่อเป็นข้อมูลที่มีปริมาณมาก และไม่อยู่ในรูปแบบที่จะทำการวิเคราะห์ผลได้ทันที หรือแม้แต่อยู่ในหลักฐานของจริงซึ่งไม่สามารถทำการวิเคราะห์ได้ทันที จำเป็นต้องมีการทำสำเนาออกมาก่อน โดยจะค่อนข้างใช้ระยะเวลาพอสมควร ดังนั้นหากกระบวนการเตรียมหลักฐานสามารถทำได้รวดเร็ว การวิเคราะห์หลักฐานทางดิจิทัลก็จะสามารถได้ผลลัพธ์รวดเร็วด้วยเช่นกัน ทั้งนี้ยังรวมถึงการเตรียมไฟล์สำหรับใช้เก็บหลักฐานด้วย โดยในที่นี้จะขอเริ่มจากหลักฐานที่เป็น RAM ก่อน ซึ่งมีโปรแกรม Mandiant Redline ในการทำหน้าที่วิเคราะห์ Process ของระบบปฏิบัติการ Windows ให้เบื้องต้นก่อน หากต้องใช้วิเคราะห์จะใช้เวลาานเนื่องจาก Process ในระบบคอมพิวเตอร์มีปริมาณมากมาย

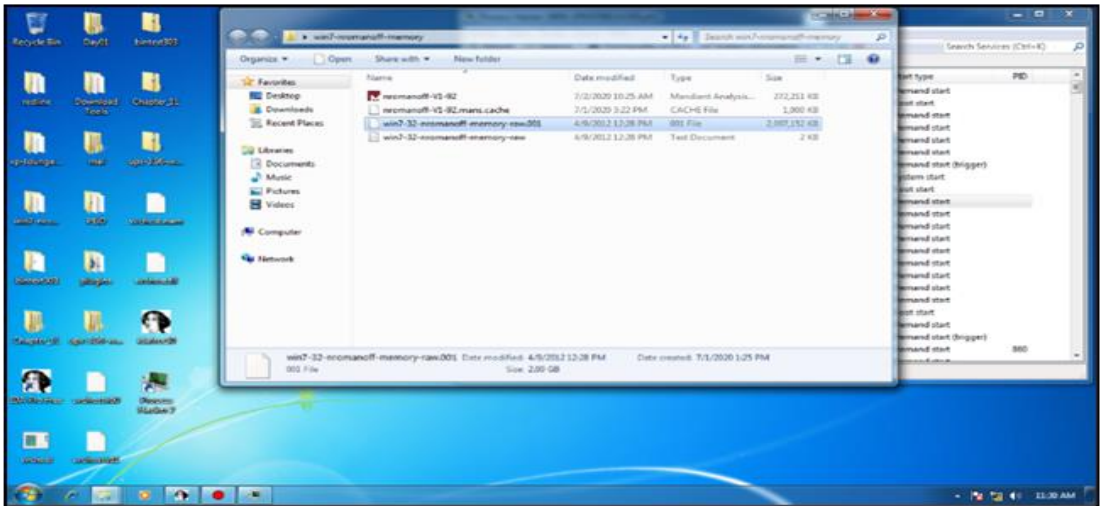
๕.๑ การสร้างไฟล์เพื่อทำการเก็บหลักฐานไฟล์ Image ด้วย Mandiant Redline



ภาพที่ ๗๗ โปรแกรม Mandiant Redline

การสร้างไฟล์เพื่อทำการเก็บหลักฐานไฟล์ Image ด้วย Mandiant Redline จะมีทั้งหมด ๓ หัวข้อ คือ แบบมาตรฐาน, แบบมีตัวเลือกมากขึ้น และแบบ ICO เพื่อให้สามารถค้นหารายละเอียดได้ โดยในที่นี้แนะนำให้เลือกแบบที่ ๒ จากนั้นเลือกระบบปฏิบัติการที่ต้องการเก็บข้อมูล กำหนด Option เพิ่มเติม คลิกเครื่องหมายถูกในช่องสี่เหลี่ยม สามารถทำการเลือก Option ได้หลากหลาย

แ บ ที่ บ
เช่น Memory, ฮาร์ดดิสก์, เซอร์วิสของระบบ, เน็ตเวิร์ค และ รายการเพิ่มเติมอื่น ๆ เป็นต้น ตามด้วย
ทำการสร้างโฟลเดอร์ปลายทางสำหรับบันทึกไฟล์เก็บข้อมูล แนะนำให้เป็น USB ที่ Format
แล้วจากนั้นกด OK เมื่อกล่องข้อความแจ้งเตือน (อาจต้องปิด Antivirus ในเครื่อง) เพื่อบอกขั้นตอน
การนำไฟล์ไปใช้งาน โดยสามารถกดปิดได้เลย เวลาใช้งานให้ Run ไฟล์ชื่อ RenRedlineAudit.bat
แล้วจะเกิดหน้าต่าง cmd ขึ้น เมื่อทำงานเสร็จหน้าต่าง cmd จะหายไป (อาจใช้เวลาค่อนข้างนาน)
ถ้าต้องการยกเลิกสามารถปิด cmd หลังจาก cmd เมื่อปิดแล้วจะได้ไฟล์



ภาพที่ ๗๘ รันไฟล์โปรแกรม Mandiant RedLine 2

กรณี VM-Ware ถ้ามีการ Part ไฟล์ไว้แล้ว ให้ทำการเก็บข้อมูลไฟล์ .vmem ก่อน ถ้าไม่มีหรือเป็น
ไฟล์ .vmdk หลังจากเปิด VM แล้วให้ Snapshot ไว้ จากนั้นใช้โปรแกรมดัมพ์พรเซสที่ชื่อ Mandiant
Redline ผ่าน USB ทำการดัมพ์พรเซสของเครื่องออกมาแล้ว Re Snapshot กลับเหมือนเดิม จากนั้น
ให้ทำการ Collect Data จาก Memory ในหัวข้อ Collect Data เป็นไฟล์ Redline เพื่อใช้ใน
โปรแกรม Redline ดังภาพ

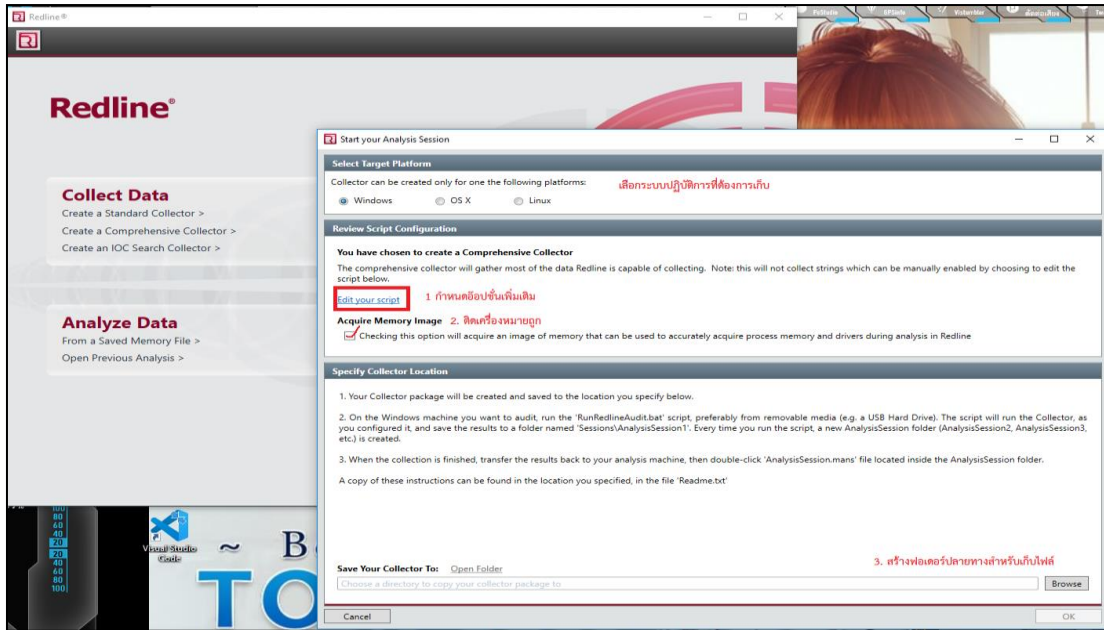


ภาพที่ ๗๙ โปรแกรม Mandiant RedLine 3



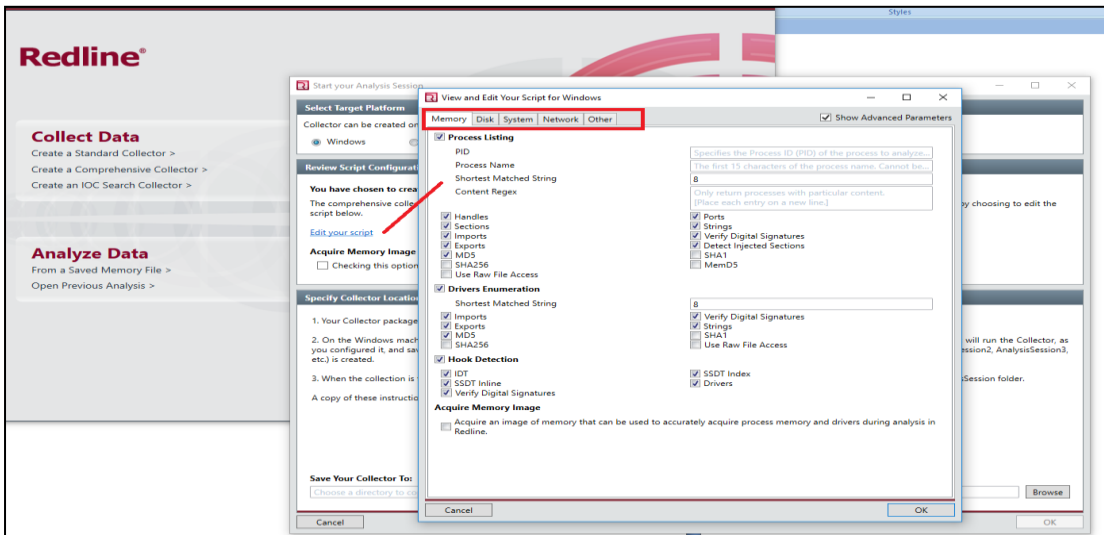
ภาพที่ ๘๐ โปรแกรม Mandiant RedLine 4

จากนั้นเลือกระบบปฏิบัติการที่ต้องการเก็บข้อมูล กำหนดการตั้งค่าเพิ่มเติม คลิกเครื่องหมาย ถูกในช่องสี่เหลี่ยม



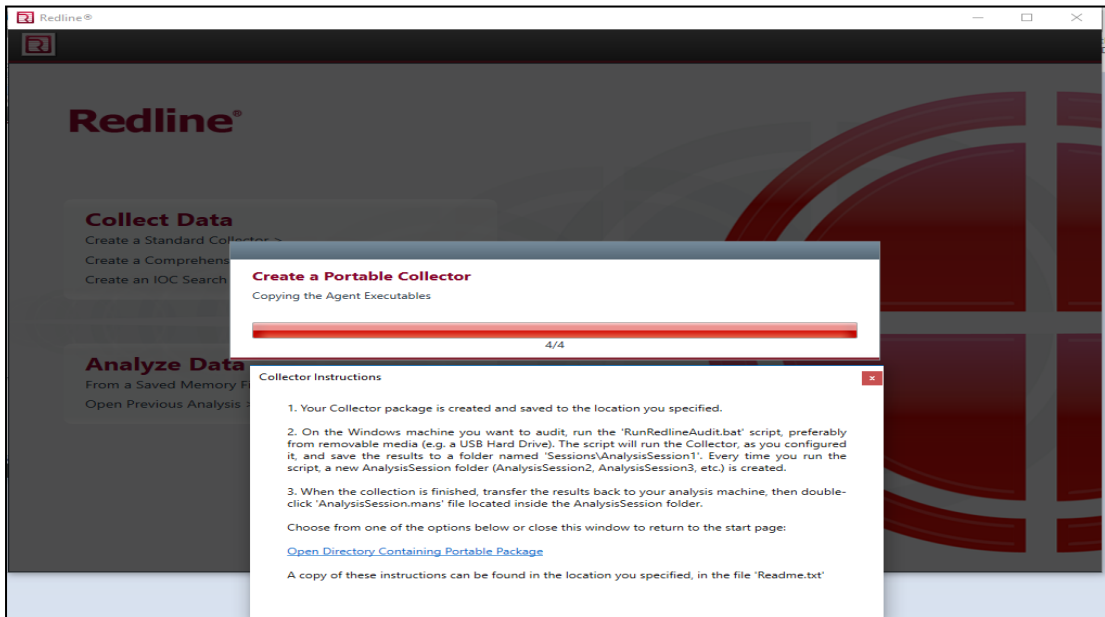
ภาพที่ ๘๑ โปรแกรม Mandiant RedLine 5

เราสามารถทำการกำหนดการตั้งค่าเพิ่มเติม ได้หลากหลายแท็บ เช่น Memory, ฮาร์ดดิสก์, เซอร์วิสของระบบ, เครือข่าย และรายการเพิ่มเติมอื่น ๆ เป็นต้น ตามด้วยทำการสร้างโฟลเดอร์ปลายทางสำหรับใช้เก็บข้อมูล แนะนำให้เป็น USB ที่ Format เป็น USB ที่ไม่มีข้อมูล และกด OK



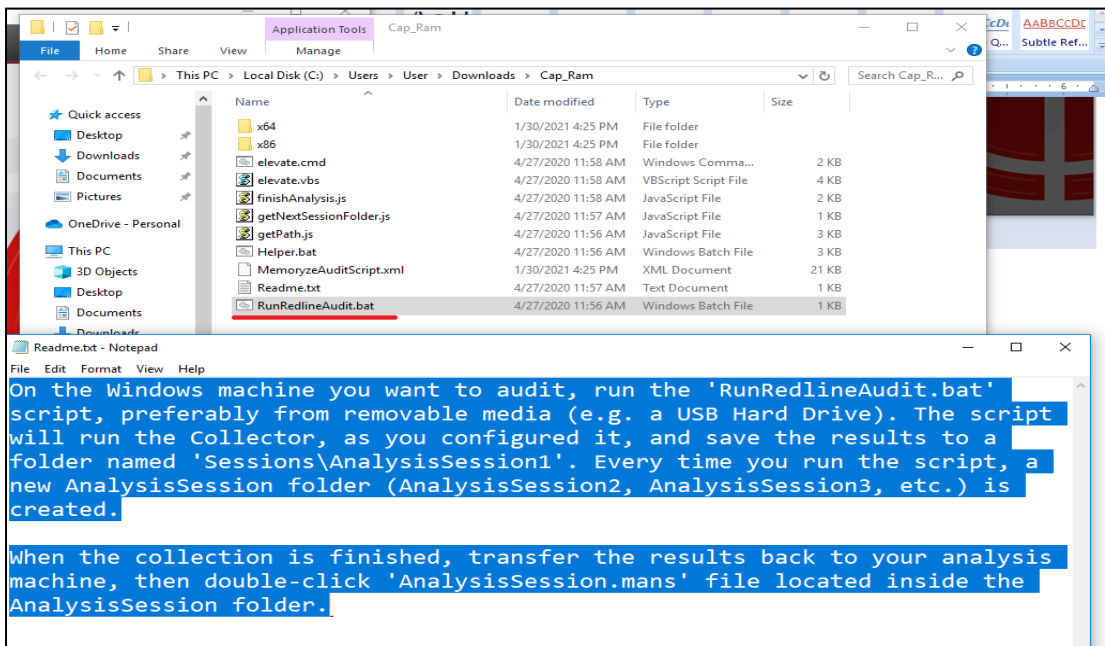
ภาพที่ ๘๒ โปรแกรม Mandiant RedLine 6

จากนั้นจะมีกล่องข้อความแจ้งเตือน (ต้องปิดแอนต์ไวรัสในเครื่องคอมพิวเตอร์) เพื่อบอกขั้นตอนการนำไฟล์ไปใช้งานสามารถกดปิดได้

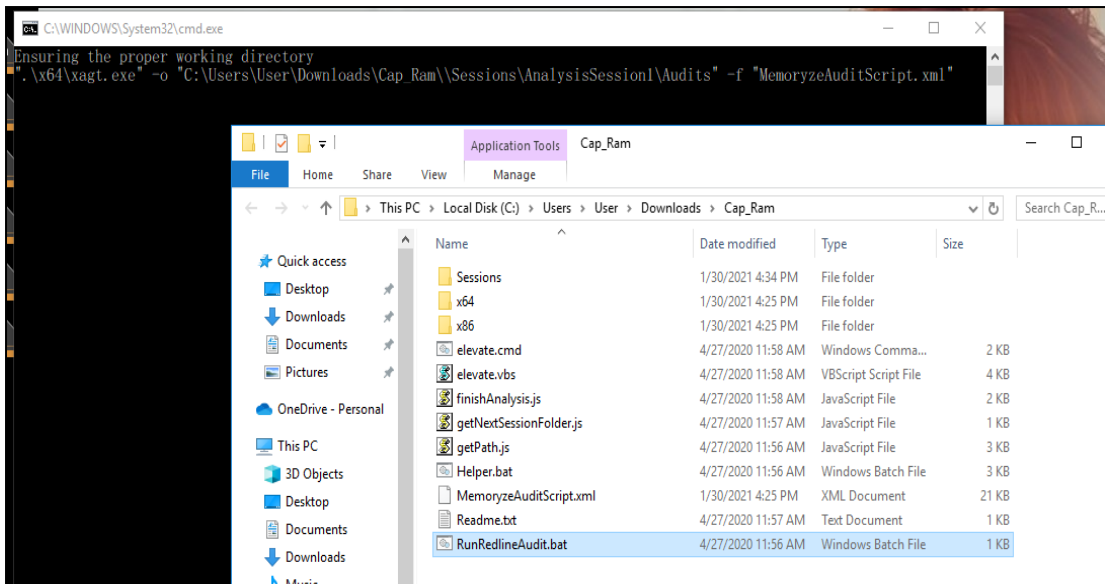


ภาพที่ ๘๓ โปรแกรม Mandiant RedLine 7

เวลาใช้งานให้รันไฟล์ชื่อ RenRedlineAudit.bat จะแสดงหน้า cmd ขึ้น เมื่อทำงานเสร็จ หน้า cmd จึงจะหายไป (อาจใช้เวลาค่อนข้างนาน) ถ้าต้องการยกเลิกให้ทำการปิด cmd

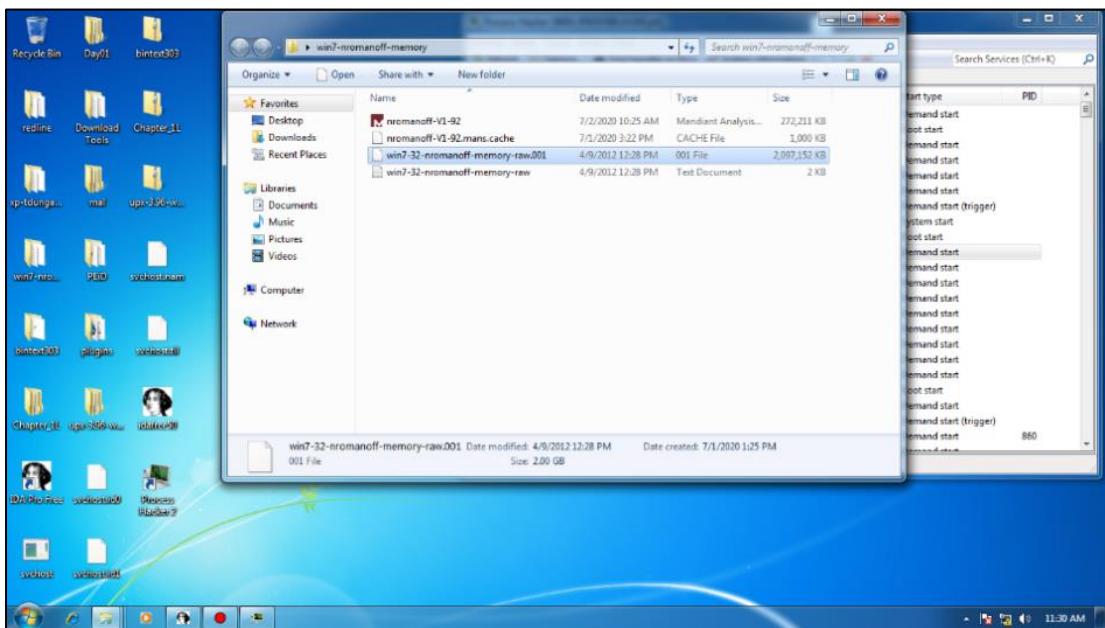


ภาพที่ ๘๔ โปรแกรม Mandiant RedLine 8



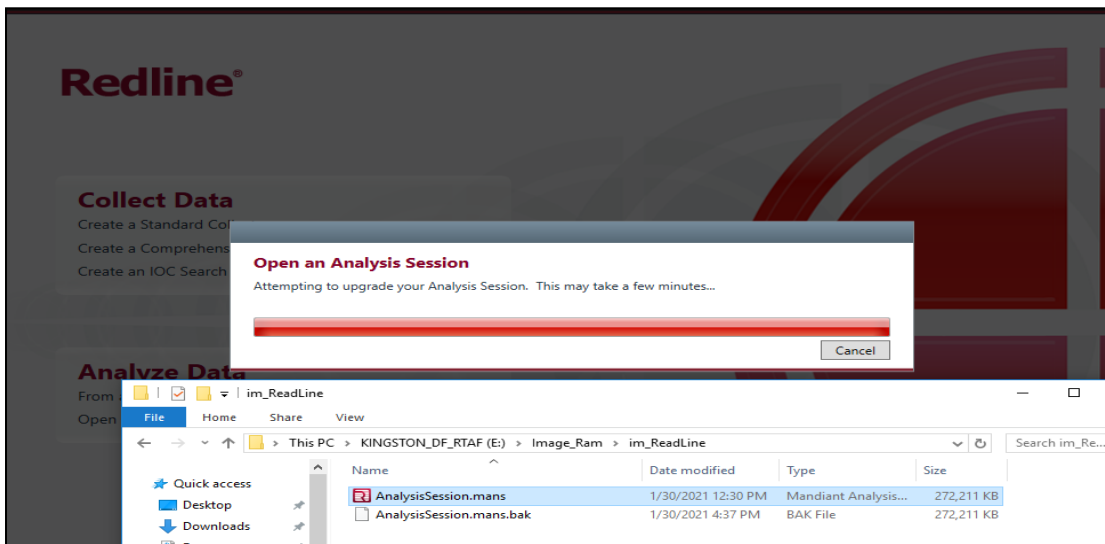
ภาพที่ ๘๕ โปรแกรม Mandiant RedLine 9

หลังจาก cmd ปิดไปแล้วเราจะได้ไฟล์ ดังนี้



ภาพที่ ๘๖ โปรแกรม Mandiant RedLine 10

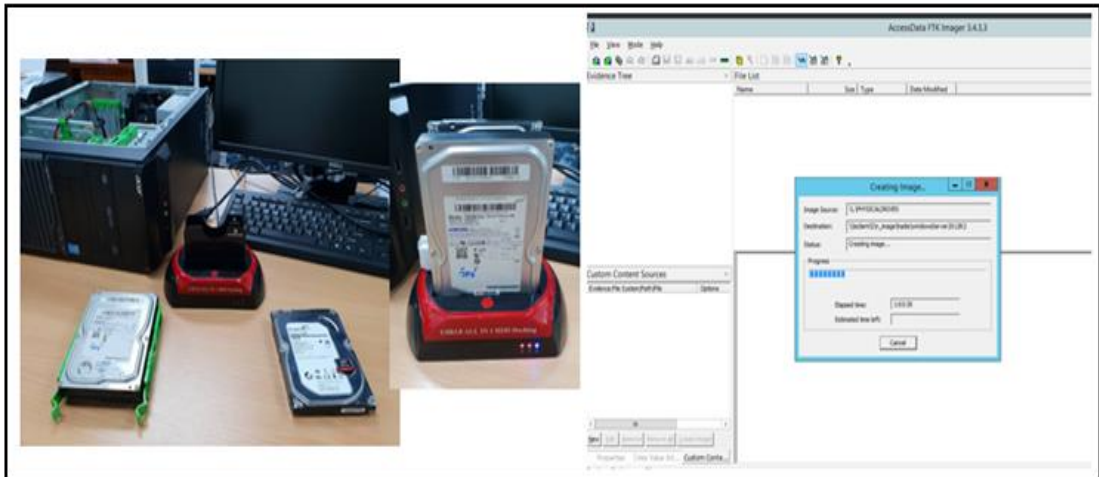
เมื่อเปิดใช้งานสามารถเข้าไปที่ Analyze data > From a Saved Memory File หรือสามารถเปิดจากไฟล์ที่มีนามสกุล `.mans` ได้โดยตรง



ภาพที่ ๘๗ โปรแกรม Mandiant RedLine 11

๕.๒ การโคลนฮาร์ดดิสก์เป็น Master และ Slab

กรณีเครื่อง PC ให้ทำการโคลนฮาร์ดดิสก์เป็น Master และ Slab โดยเก็บตัวหลักฐานไว้แล้วใช้ Slab ในการวิเคราะห์หรือทำ Image ด้วย FTK ถ้าเสียหายหรือต้องการทำใหม่ให้ทำการโคลน Master ทั้งนี้ต้องดูสถาปัตยกรรมการต่อฮาร์ดดิสก์ของเครื่องเกิดเหตุด้วย



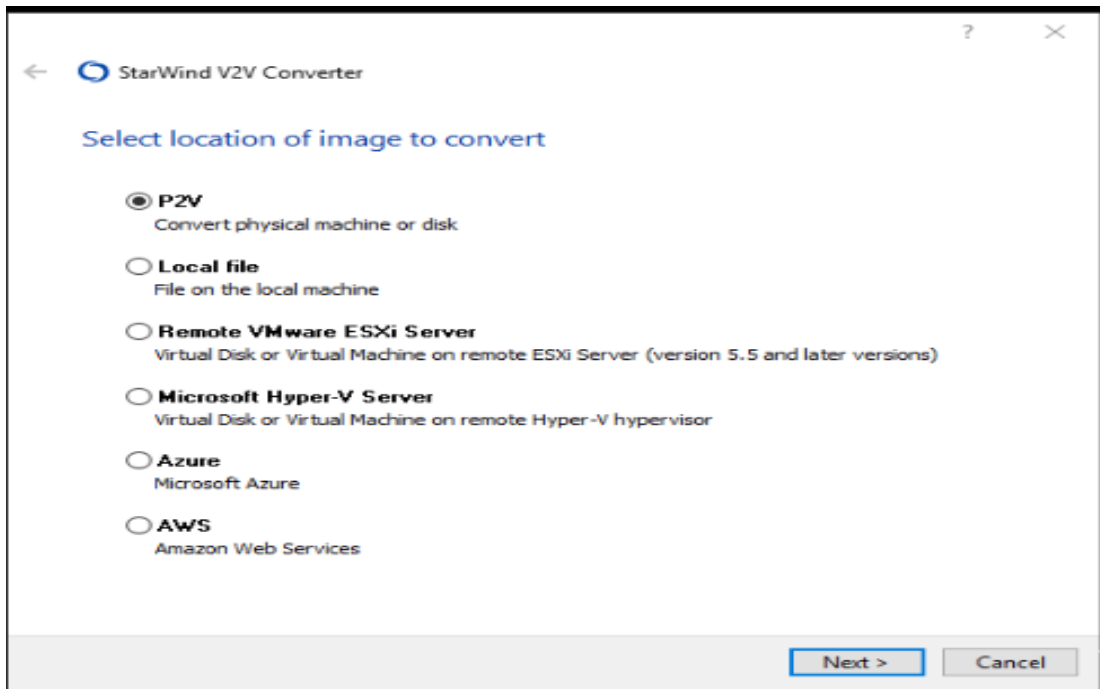
ภาพที่ ๘๘ การโคลนฮาร์ดดิสก์เป็น Master และ Slab

๕.๒.๑ โปรแกรม StarWindconverter กรณีที่เครื่องคอมพิวเตอร์ที่เกิดเหตุเป็นเครื่อง Notebook หรือเครื่องที่ไม่สามารถแกะเอาฮาร์ดดิสก์ออกมาได้ให้ใช้วิธีการทำ Image ให้เป็นไฟล์ .vmdk



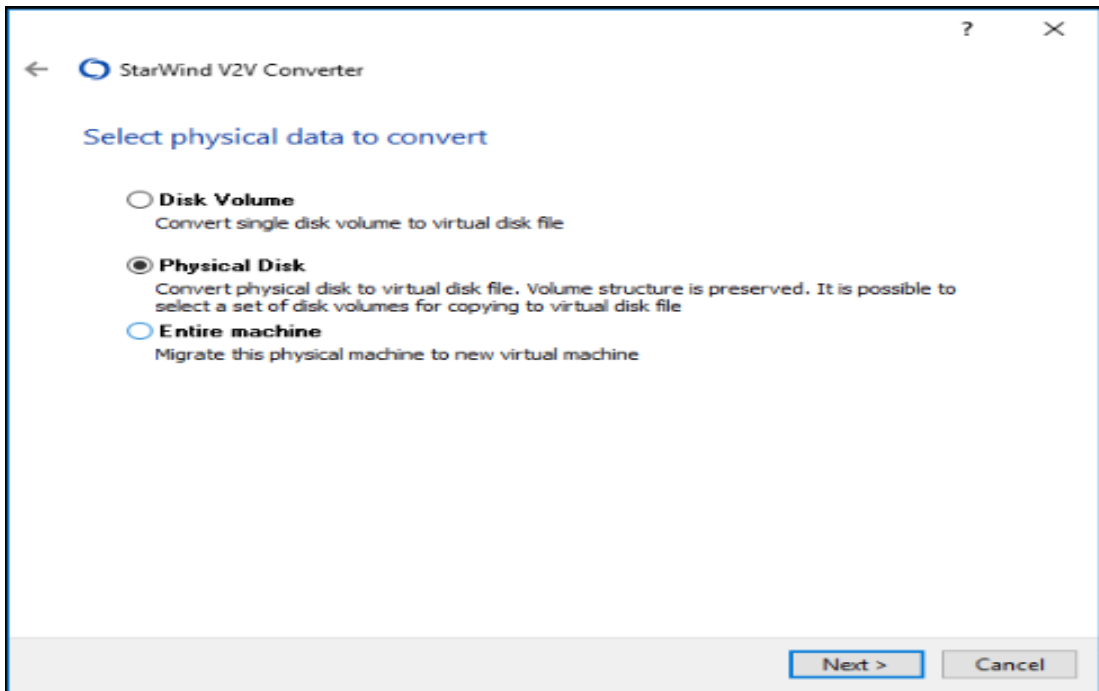
ภาพที่ ๘๙ โปรแกรม StarWind V2V Converter

เมื่อทำการ Run โปรแกรมขึ้นมาแล้วให้ทำการเลือก P2V และกด Next



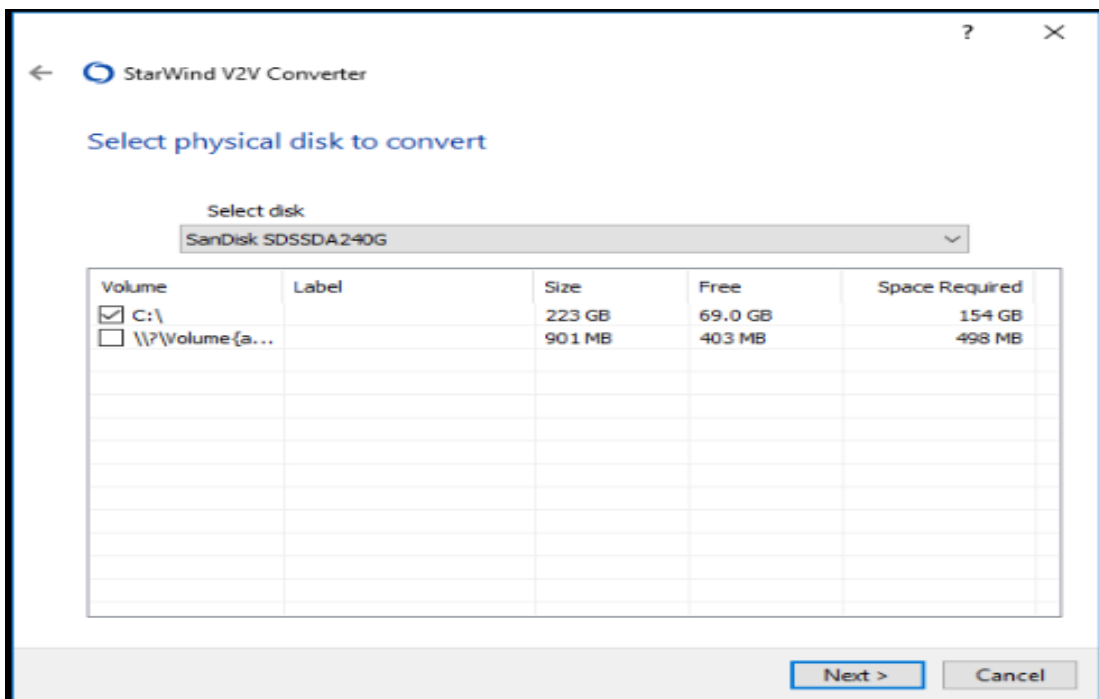
ภาพที่ ๙๐ โปรแกรม StarWind V2V Converter 1

เลือก Physical Disk และกด Next



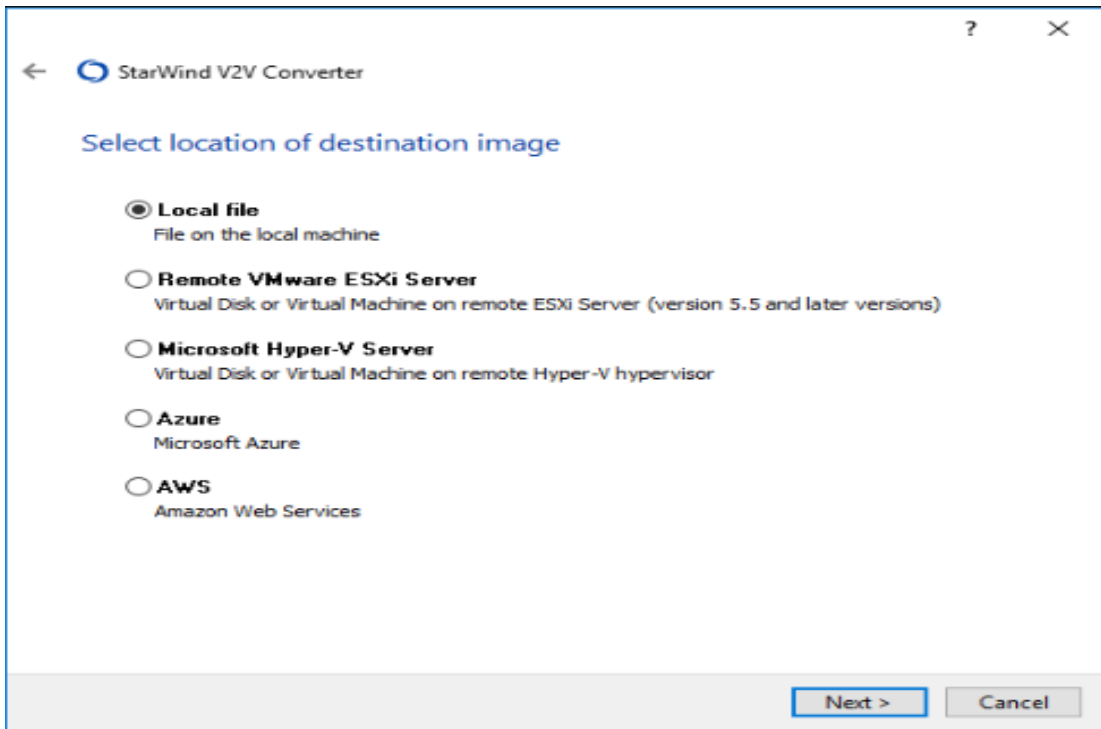
ภาพที่ ๙๑ โปรแกรม StarWind V2V Converter 2

เลือก Disk ที่เก็บข้อมูลของระบบที่ต้องการจะทำ VM-Ware



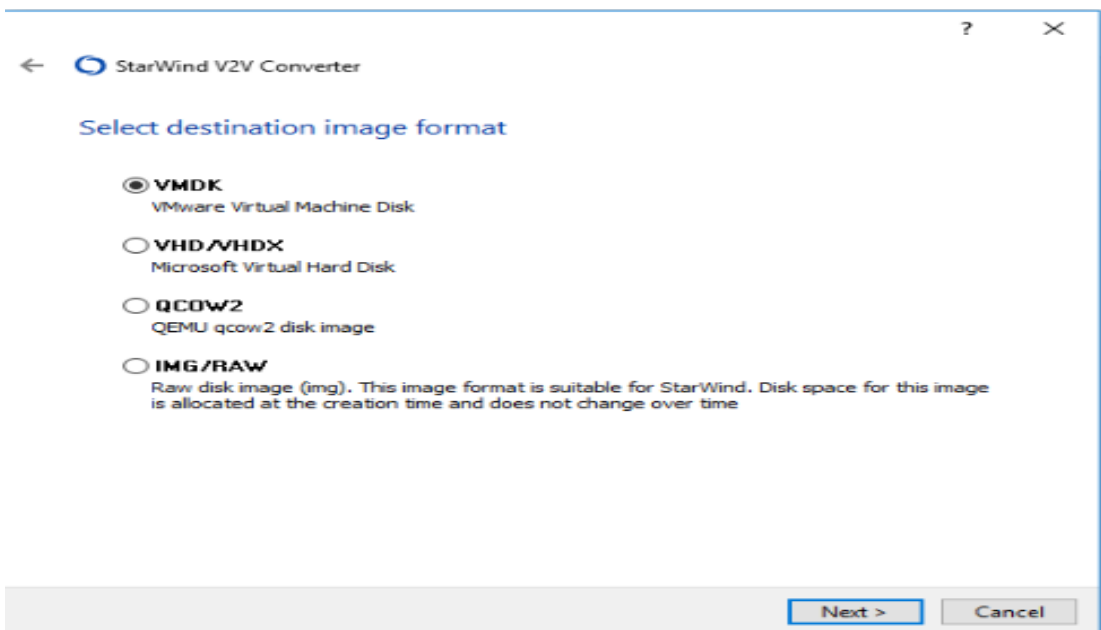
ภาพที่ ๙๒ โปรแกรม StarWind V2V Converter 3

เลือก Local File และกด Next



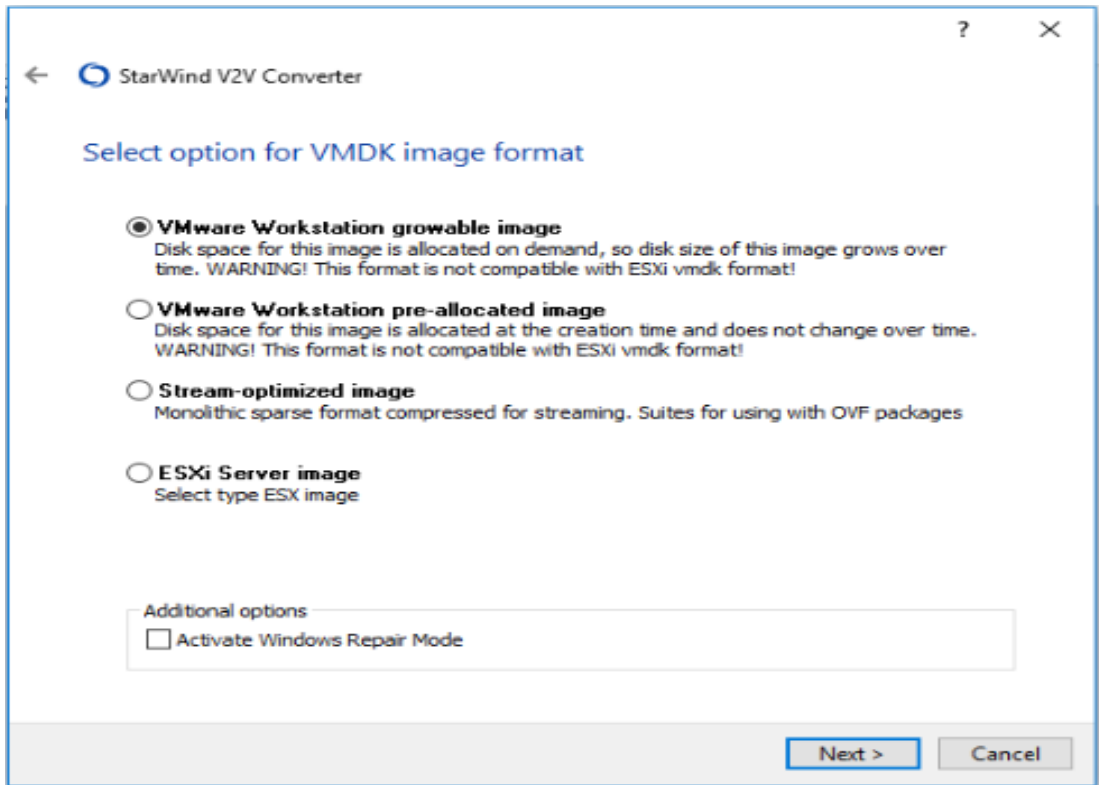
ภาพที่ ๙๓ โปรแกรม StarWind V2V Converter 4

เลือก VMDK และกด Next



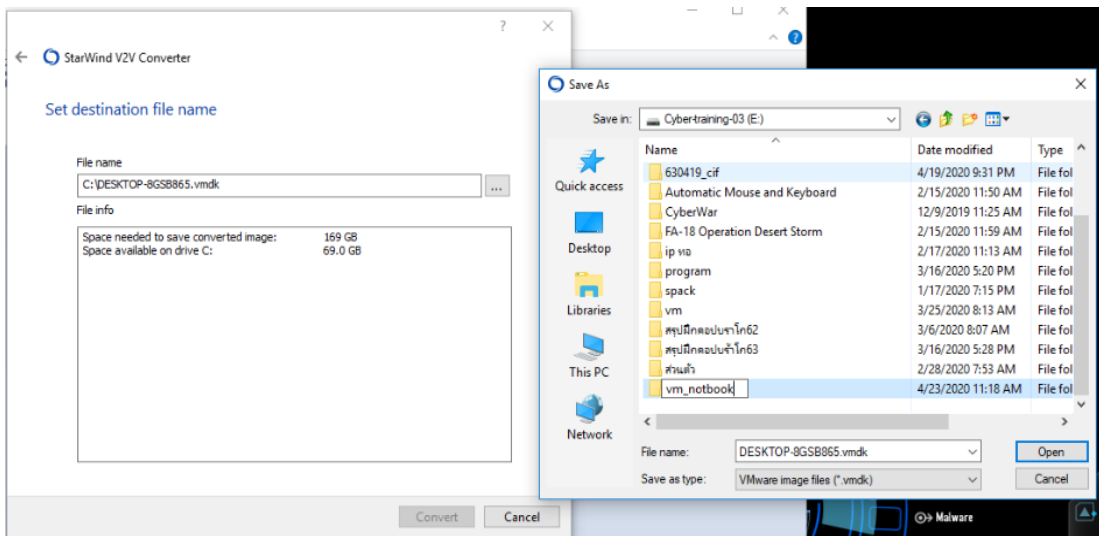
ภาพที่ ๙๔ โปรแกรม StarWind V2V Converter 5

เลือก VMware Workstation growable image และกด Next



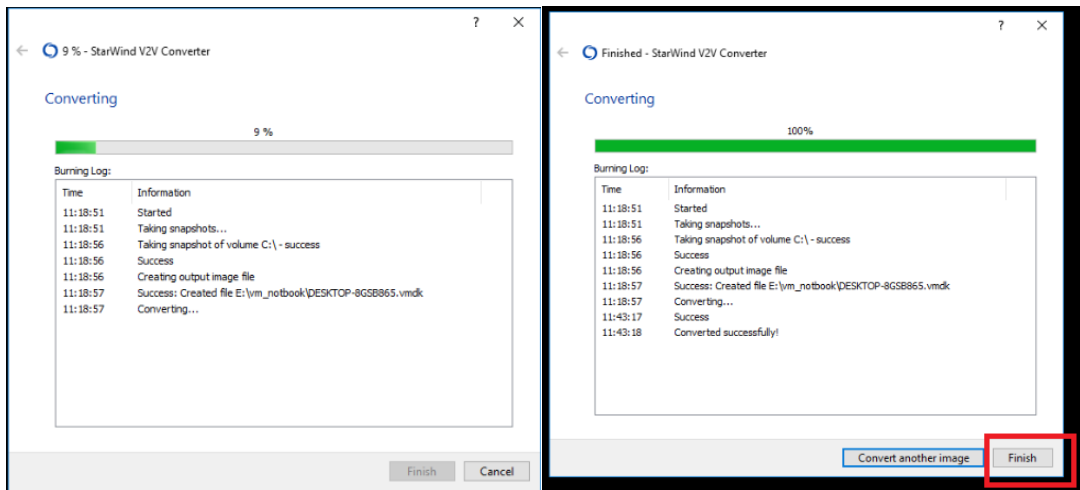
ภาพที่ ๕๕ โปรแกรม StarWind V2V Converter 6

ทำการสร้างไฟล์เตอร์สำหรับเก็บไฟล์ VM-ware



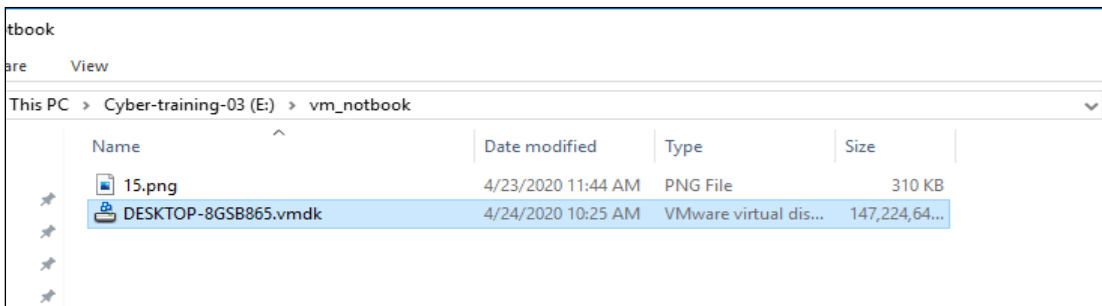
ภาพที่ ๕๖ โปรแกรม StarWind V2V Converter 7

เมื่อกระบวนการเสร็จสิ้นและกด Finish



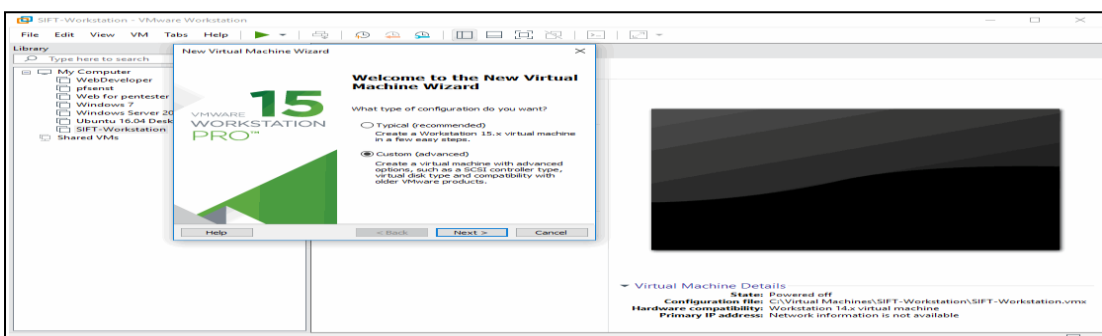
ภาพที่ ๗๗ โปรแกรม StarWind V2V Converter 8

ไฟล์ .vmdk ดังรูป ไม่สามารถเปิดกับโปรแกรม VMware Workstation ได้ ต้องทำการนำเข้าไฟล์ก่อน

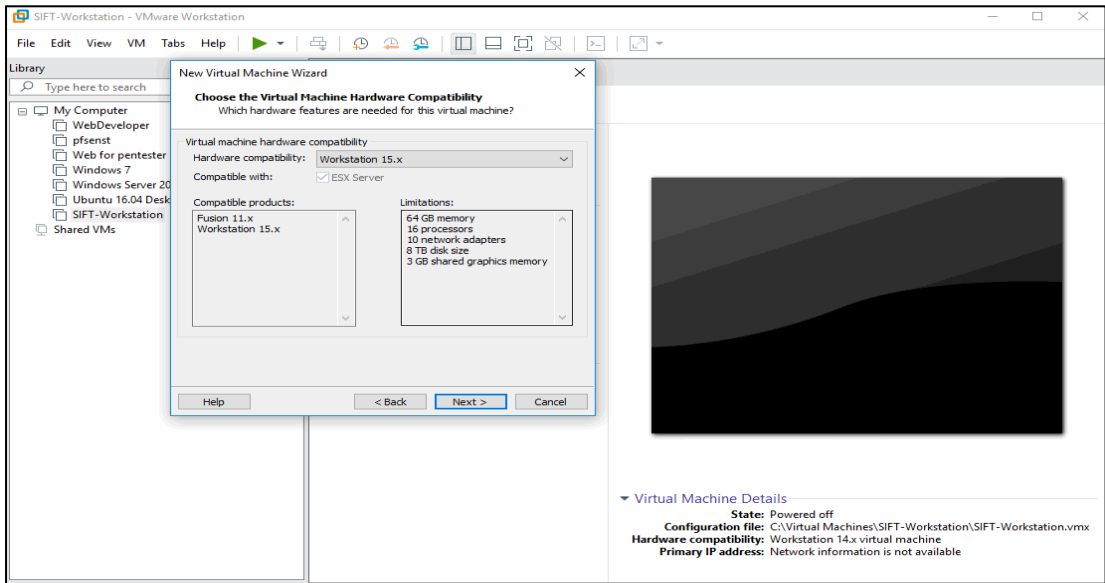


ภาพที่ ๗๘ โปรแกรม StarWind V2V Converter 9

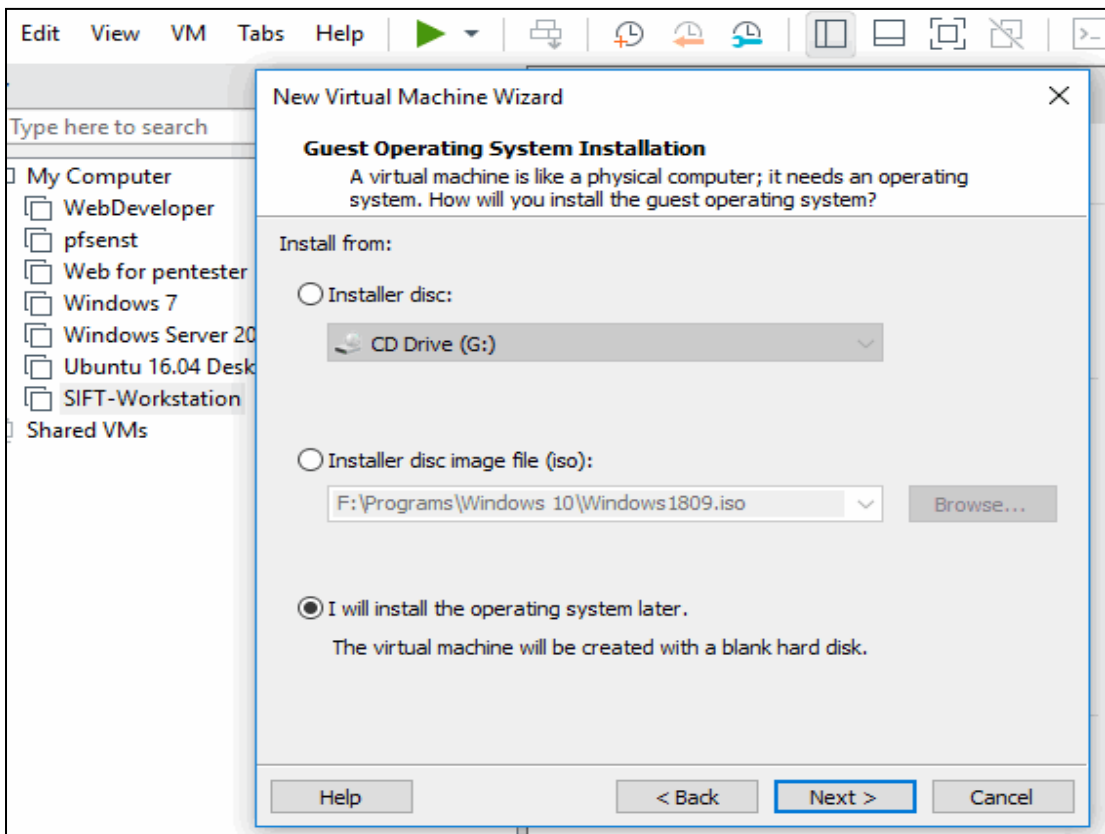
จากนั้นให้ทำการนำเข้าไฟล์ vmdk โดยไปที่เมนู File > New Virtual Machine Wizard..



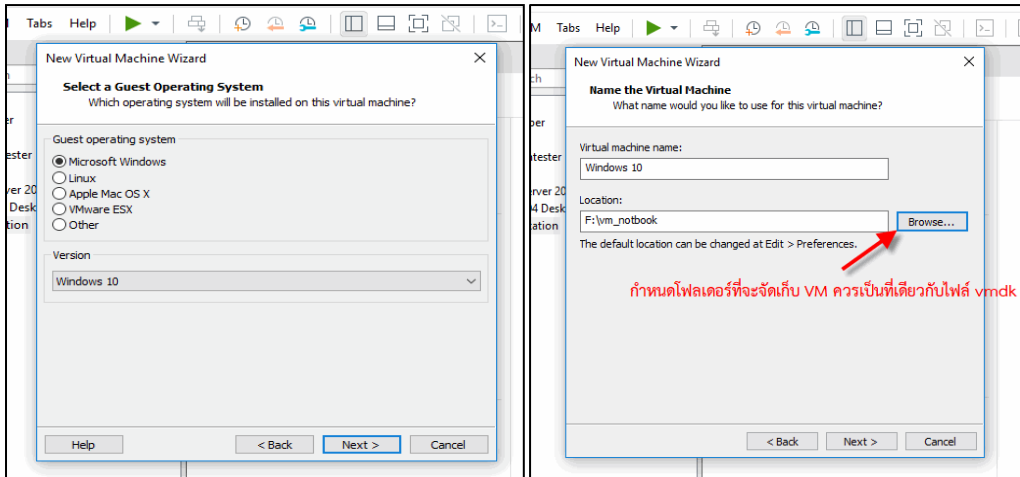
ภาพที่ ๗๙ โปรแกรม StarWind V2V Converter 10



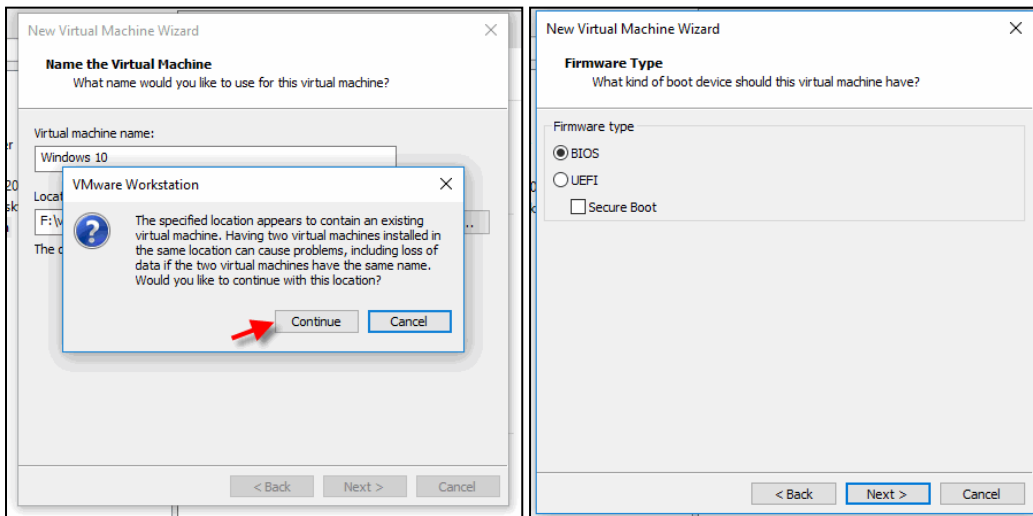
ภาพที่ ๑๐๐ โปรแกรม StarWind V2V Converter 11



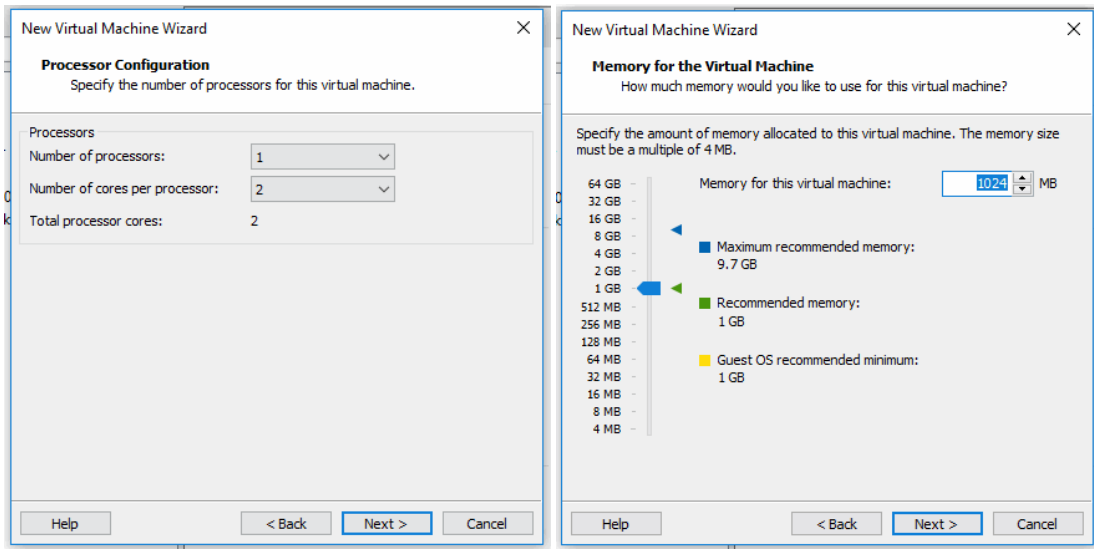
ภาพที่ ๑๐๑ โปรแกรม StarWind V2V Converter 12



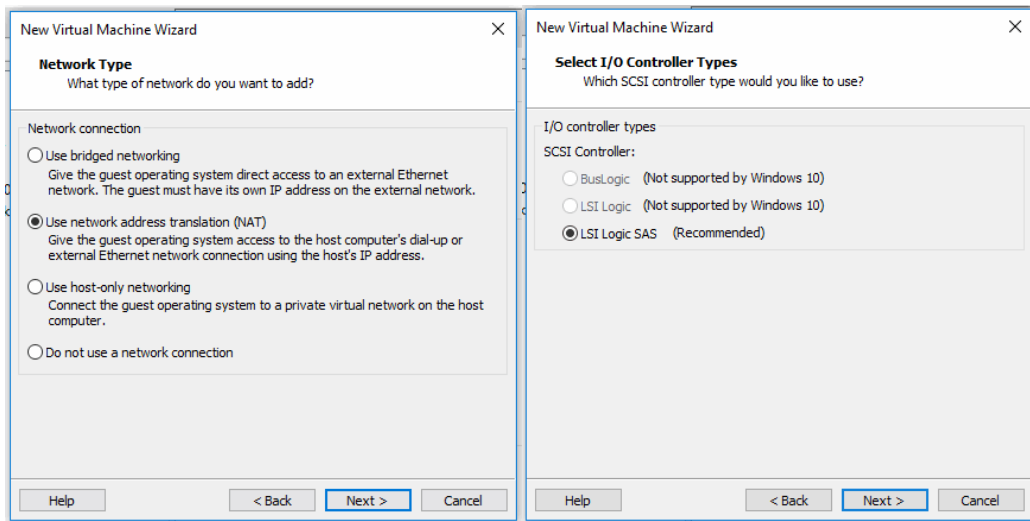
ภาพที่ ๑๐๒ โปรแกรม StarWind V2V Converter 13



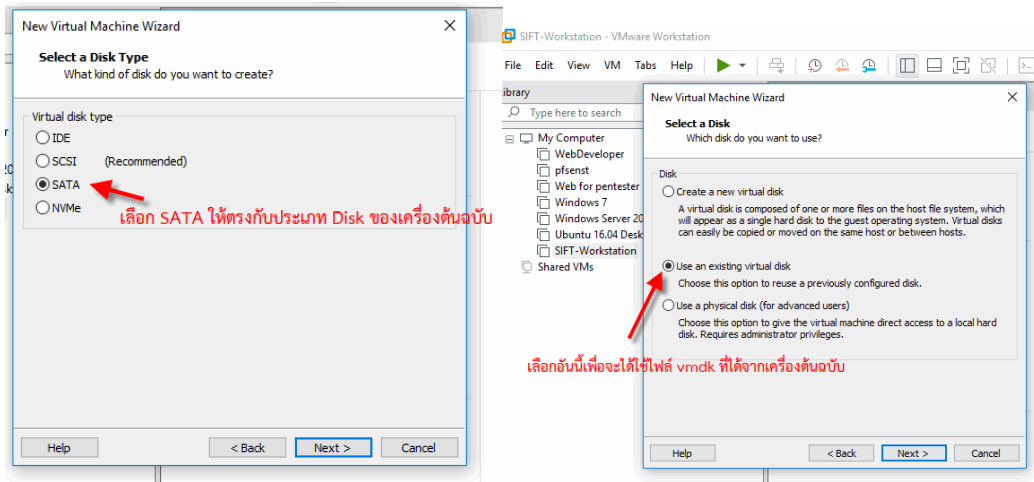
ภาพที่ ๑๐๓ โปรแกรม StarWind V2V Converter 14



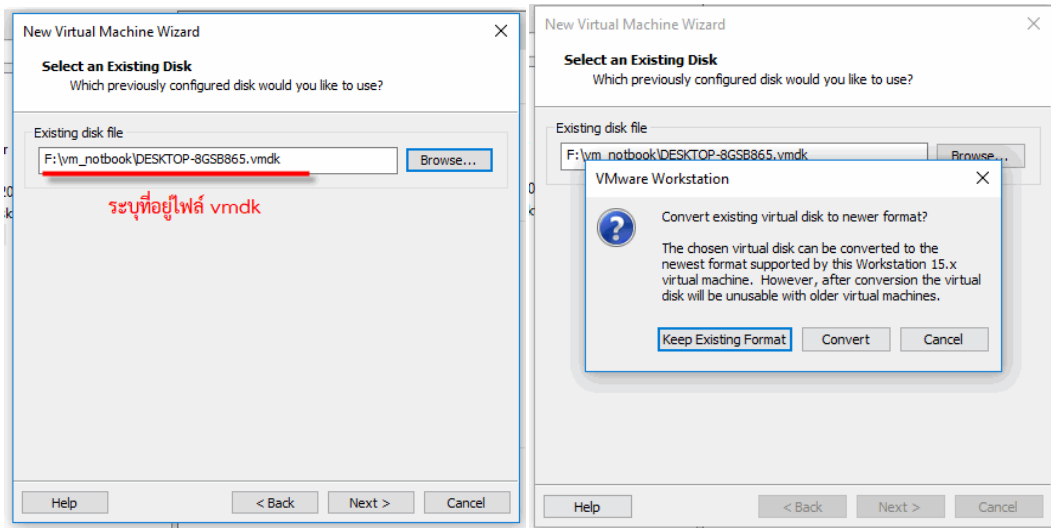
ภาพที่ ๑๐๔ โปรแกรม StarWind V2V Converter 15



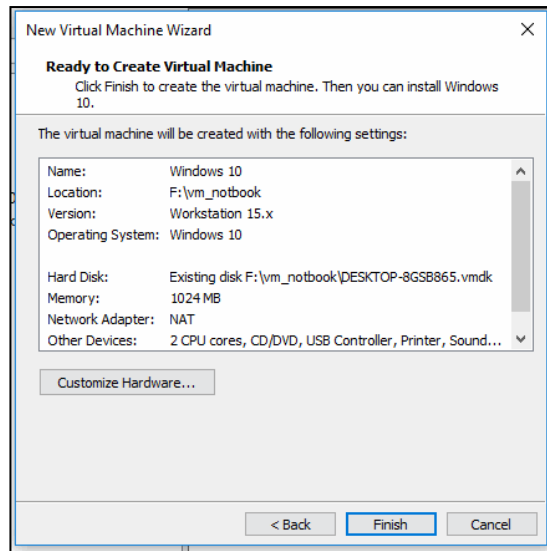
ภาพที่ ๑๐๕ โปรแกรม StarWind V2V Converter 16



ภาพที่ ๑๐๖ โปรแกรม StarWind V2V Converter 17

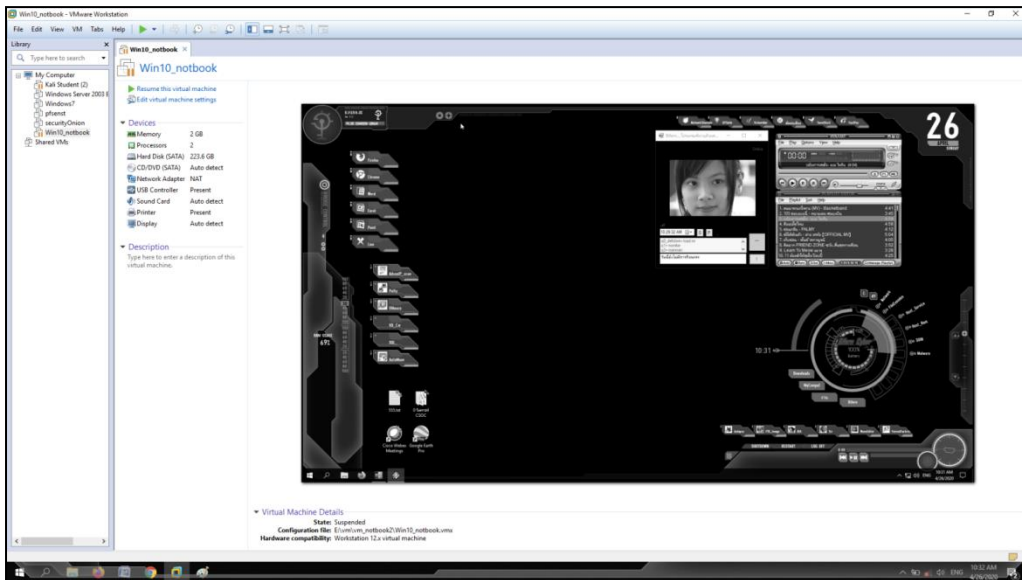


ภาพที่ ๑๐๗ โปรแกรม StarWind V2V Converter 18



ภาพที่ ๑๐๘ โปรแกรม StarWind V2V Converter 19

จากนั้นเมื่อเปิดโปรแกรม เราจะพบคอมพิวเตอร์อยู่ในระบบ VM-Ware ดังภาพที่ ๙๘



ภาพที่ ๑๐๙ โปรแกรม StarWind V2V Converter 20

๕.๓ กรณีที่ต้องทำ Sandbox

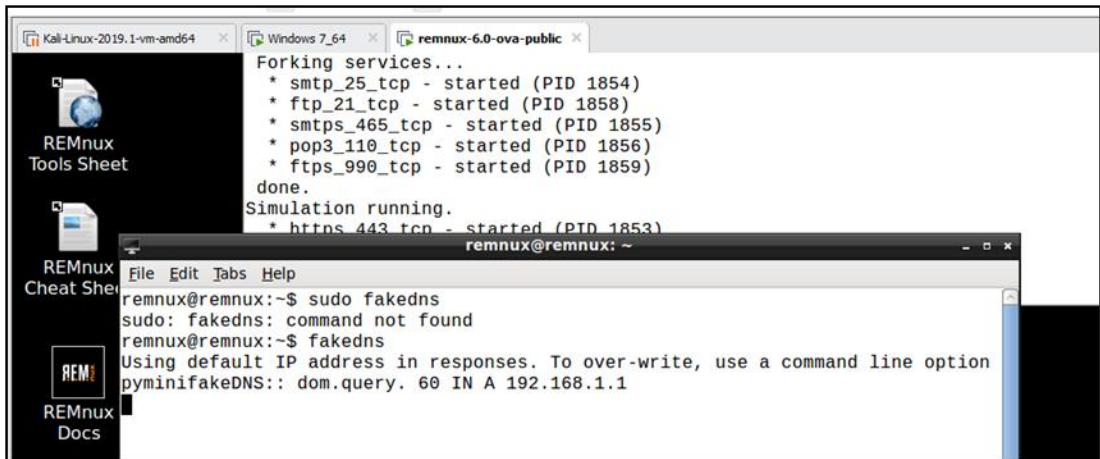
Sandbox เป็นการค้นหาไวรัสแบบ Static เราจะต้อง Snapshot VM-Ware ด้วยเสมอ โดยในที่นี่จะแบ่งเป็น ๒ ส่วนคือ Window 7 เป็นเครื่องที่จะติดมัลแวร์ และ Remnux จะเป็นเครื่องมอเนิเตอร์และสร้าง DNS ปลอม การทำ Sandbox มีความอันตรายต่อระบบต้องตั้งค่า VM ให้เป็น Host Only และตัดการเชื่อมต่อกับระบบภายนอก เบื้องต้นจะต้องเริ่มวางแผนด้วยการออกแบบ Network ก่อนว่าจะมีเครื่องในการทดสอบกี่เครื่อง โดยทั่วไปจะใช้ ๒ เครื่อง คือ เครื่องที่ติดไวรัส กับเครื่องที่ทำหน้าที่เป็นตัวเก็บ Logs และจำลองอินเทอร์เน็ตปลอม ปกติก็จะใช้ VM Ramnux โดย Set ให้คอมพิวเตอร์ทั้งสองเครื่องอยู่ในวง LAN เดียวกัน ทดสอบด้วยการ Ping หากัน และการทำ Sandbox ต้องขอข้อมูลความรู้เรื่องของการเตรียมการทดสอบหรือการจัดเตรียมสภาพแวดล้อมการทดลองก่อน เพื่อให้กระบวนการสอดคล้องและต่อเนื่องกัน ดังภาพ

การเชอระบบ	การทำ sanbox	set ip แบบ linux
vm win7	vm remnux	sudo ifconfig eth0 192.168.180.128 netmask 255.255.255.0 sudo route add default gw 192.168.180.1 eth0
ติดตั้งโปรแกรม ProcessMonitor	เปิด dns ปลอม	เปิดเว็บเซอวิส inetsim
ติดตั้งโปรแกรม processhacker	set ip แบบ linux	เปิด dns ปลอม fakedns
set ip แบบฟิก	เปิดโปรแกรม ราชด เพื่อแคปเจอร์เน็ตเวิร์ค	ให้ windows เปิด ip เครื่องของ Linux
ip 192.168.180.10	จากนั้นทำการ scapChort ไว้	อ้างอิง
subnet 255.255.255.0		https://www.youtube.com/watch?v=4LzCr9qf5_Q
dns 192.168.160.128	start dns ปลอม	
จากนั้นทำการ scapChort ไว้	เปิดราชด	
ทดสอบเข้าหน้าเว็บด้วย ip ของ remnux		
เปิดโปรแกรม processhacker และ ProcessMonitor ทำการเคย์ไปเซตโดยคลิกที่รูปข้างบนแล้วกดเริ่มมอเนิเตอร์ที่รูปบน		
ทำการโหลดมัลแวร์และรันมัลแวร์		
สังเกตโปรเซสของมัลแวร์ที่โปรแกรม ProcessHacker		
ทำการ kill โปรเซสของมัลแวร์ด้วยโปรแกรม ProcessHacker		
ที่โปรแกรม processMonitor กดรูปแว่นมิกคริ่งเพื่อหยุดการตรวจจับ		
ทำการ save เป็นไฟล์ csv	ปิดโปรแกรมราชดแล้ว Save ไฟล์ .pcap	
นำไฟล์ csv ไปเปิดกับโปรแกรม Don.... เพื่อดูความลึ้มพันธ์	ปิด DNS ปลอม	
	นำ .pcap ไปวิเคราะห์ได้	

ภาพที่ ๑๑๐ การทำ Sandbox

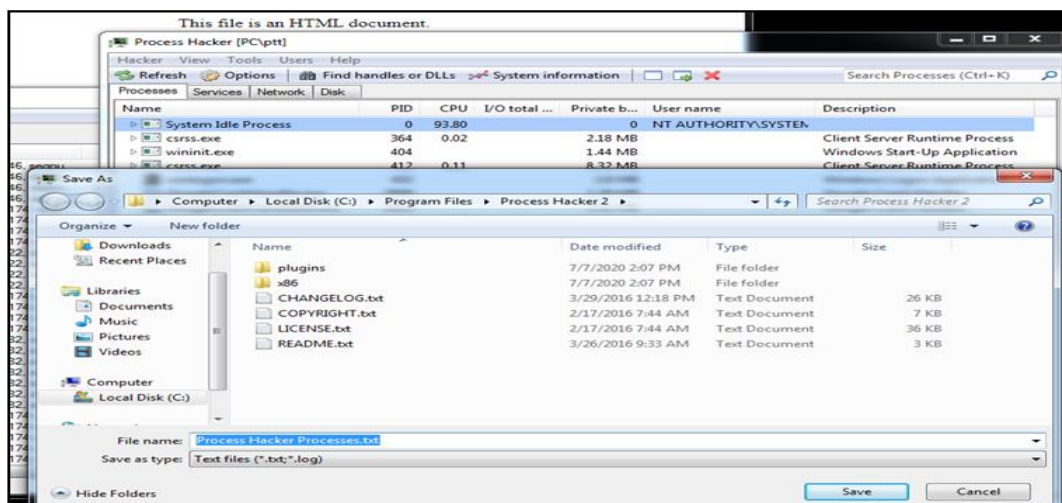
เมื่อเตรียมสภาพแวดล้อมของการทดสอบเสร็จเรียบร้อยแล้ว ขั้นตอนต่อไปคือการทำให้ Sandbox หรือการดำเนินการทดสอบ โดยมีรายละเอียดดังนี้

๕.๑.๒.๑ วิธีทำ Sandbox เริ่มจากเปิด VM-ware Remnux เพื่อทำการ Set ค่า IP ให้เป็น Network เดียวกันกับเครื่อง Win7 เพื่อให้สามารถตรวจจับแพ็กเก็ตและสร้างเป็น DNS ปลอมให้กับ Sandbox โดยเปิด Command Line แล้วพิมพ์คำสั่ง # sudo ifconfig eth0 192.168.75.101 netmask 255.255.255.0 และ # sudo route add default gw 192.168.75.1 eth0 จากนั้นก็ทำการตั้งค่า Network VM ของทั้งสองให้เป็น Host-only ทำการติดตั้งโปรแกรม Process Monitor และ Process Hacker บน Win7 กำหนดค่า IP Address โดยให้ Gateway เป็น IP ของ Remnux เปิดเซอวิสเว็บไซต์ของ ด้วยคำสั่ง #>sudo inetsim เปิด Terminal ขึ้นมาใหม่แล้วทำการสตาร์ท DNS จำลองของ Remnux ด้วยคำสั่ง #>sudo fakedns



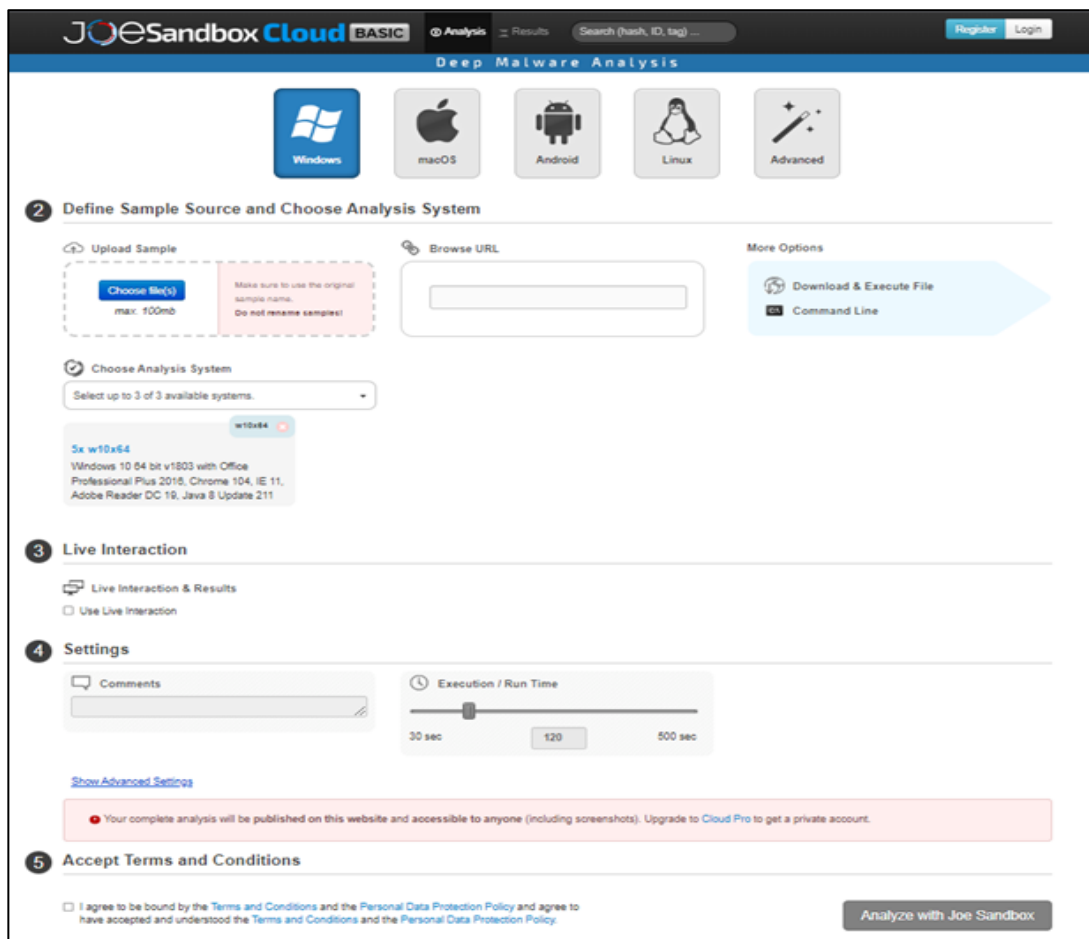
ภาพที่ ๑๑๑ คำสั่ง #> sudo fakedns

จากนั้นทำการ Snapshot เครื่องเหยื่อ Win7 แล้วพิมพ์หมายเลข IP Address ของเครื่อง Remnux ที่บราวเซอร์จะแสดงหน้าต่างการต้อนรับการใช้งานของโปรแกรม Remnux แสดงว่าระบบพร้อมใช้งานที่ VM ของ Remnux เปิดโปรแกรม Wireshark เพื่อทำการบันทึกภาพหน้าจอไฟล์ .pcap Network ของเหตุการณ์เปิดโปรแกรม Process Hacker และ Process Monitor ทำการเคลียร์โพรเซส ด้วยการคลิกที่รูปยางลบ แล้วกดเริ่มมอนิเตอร์ คลิกที่รูปแว่น และทางฝั่ง Remnux ให้ทำการเปิดการมอนิเตอร์ Network ทำการโหลดมัลแวร์และรันมัลแวร์ ที่ VM-Win7 ให้สังเกตโพรเซสของมัลแวร์ที่โปรแกรม Process Hacker โดยสามารถทำการ Kill โพรเซสของมัลแวร์ได้ด้วยโปรแกรม Process Hacker ที่โปรแกรม Process Monitor กดรูปแว่นขยายอีกครั้งเพื่อหยุดการตรวจจับ จากนั้น Save เป็นไฟล์ .csv ที่ VM Remnux ปิดโปรแกรม Wireshark แล้ว Save ไฟล์ .pcap และปิด fakedns ปลอม เมื่อทดลองเสร็จแล้วให้ทำการบันทึก logs จากโปรแกรม Process Hacker โดยจะได้ไฟล์เป็น .txt



ภาพที่ ๑๑๒ แสดงการ รันโปรแกรม Process Hacker

ส่วนโปรแกรม Process Monitor จะสามารถเลือกได้ว่าจะ save เป็นไฟล์ประเภทใด ถ้าเป็นไฟล์ PML จะสามารถเปิดกับโปรแกรมเดิมได้ หรือจะเลือกเป็นแบบ CSV หรือ XML จากนั้นจึงทำการ stop การทำงานของโปรแกรม Wireshark ในฝั่ง Ramnux พร้อมบันทึกไฟล์ .pcap และปิดการทำงานของ Terminal fakedns กับ inetsim เป็นอันเสร็จสิ้นการทำ Sandbox สำหรับการดึงไฟล์ .js ที่ซ่อนอยู่ในไฟล์ PDF ทำได้ด้วยคำสั่ง #>pdfextract -j ชื่อไฟล์.pdf แล้ว ls ชื่อไฟล์.dump /scripts/#>pdfwalder ชื่อไฟล์.pdf นอกจากนี้ ใน VMRamnux จะมีโปรแกรมที่สามารถวิเคราะห์ไฟล์เอกสาร Office ว่ามีมาโครไวรัสฝังอยู่หรือไม่ด้วยคำสั่ง #>OfficeMalScanner ชื่อไฟล์.doc info, #>OfficeMalScanner ชื่อไฟล์ .doc scan หรือ #>RTFScan ชื่อไฟล์.doc scan, #>RTFScan ชื่อไฟล์.rtf หรือ #>Malzilla จะเป็น GUI โดยคลิกที่แท็บ Decoder แล้วคลิกพื้นที่ว่างเลือก Load_from_file แล้วเลือกไฟล์ที่ต้องการ จากนั้นกดปุ่ม Run script จะแสดงรหัสและโค้ดออกมาให้ทำการคลิกอีกครั้ง จะปรากฏข้อความซึ่งอาจเป็นลิงค์ของมัลแวร์ นอกจากนี้ยังมีการทำ Sandbox แบบออนไลน์อีกด้วย ซึ่งวิธีการคือการนำไฟล์ที่ต้องสงสัยไปตรวจสอบที่เว็บไซต์ Joesandbox (<https://www.joesandbox.com/#windows>) ดังแสดง



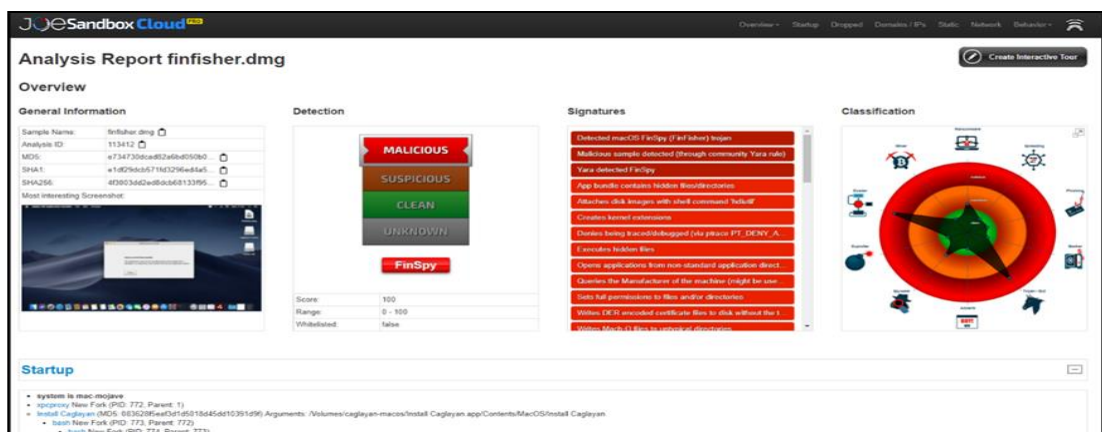
ภาพที่ ๑๑๓ เว็บไซต์ Joesandbox.com

บทที่ ๖ การวิเคราะห์ข้อมูล

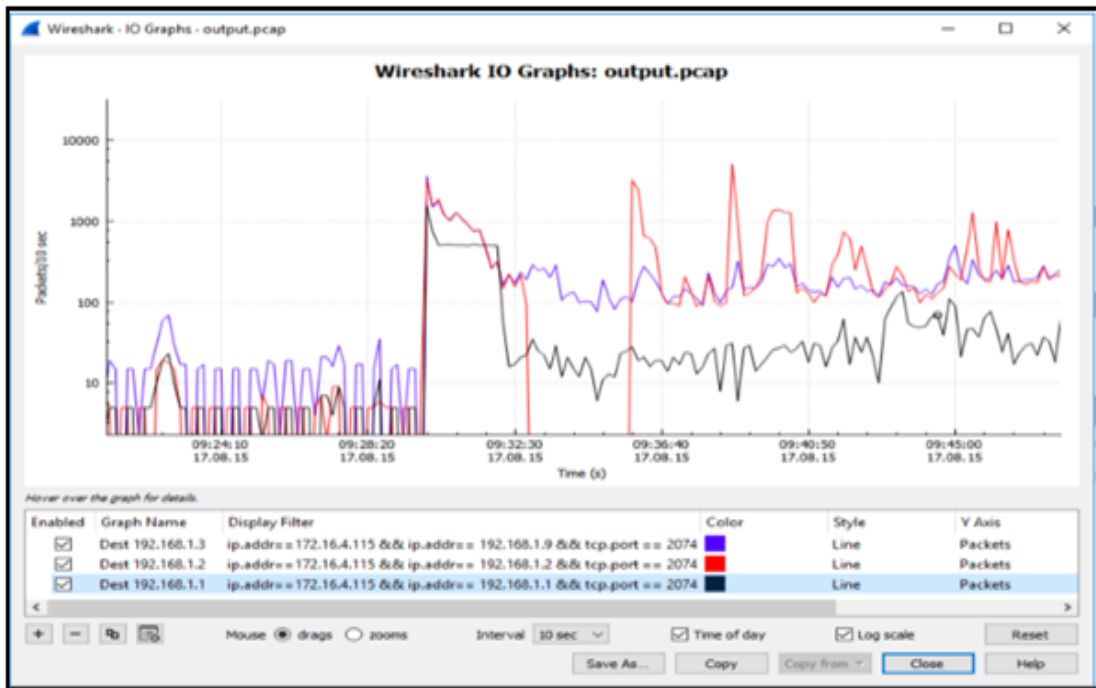
การวิเคราะห์ Network Forensic เราจะเริ่มจากค้นหาข้อมูลหมายเลข IP Address ต้นทาง ปลายทาง Port ที่ใช้รับส่งข้อมูลที่มีการรับส่งไฟล์ที่ถูกเรียกใช้ลิงก์เว็บที่อยู่ของไฟล์ http status อาจดูลึกไปถึงลักษณะการรับส่งข้อมูลว่าเป็นแบบ get/post/request ซึ่งหลายครั้งอาจเป็นการใช้คำสั่ง Command line หรือ Sql Command โจมตีเข้ามา หรืออาจมีการอำพรางด้วยการเข้ารหัสเป็น Base64, Sha1, Sha256 รวมถึงการส่ง Byte Code เข้ามาในระบบ เพื่อทำให้เกิดการปฏิเสธการให้บริการเว็บไซต์ หรือรบกวนการทำงานของระบบ สำหรับการวิเคราะห์ Network Forensics จะแบ่งย่อยตามโปรแกรมที่ทาง ทอ.ใช้งาน ประกอบด้วยโปรแกรม Wireshark, Imperva, Security Onion และ Deep Instinct โดยมีรายละเอียดการใช้งานและการวิเคราะห์ด้วยโปรแกรมทั้งหมด เช่น โปรแกรม Wireshark ใช้ในการวิเคราะห์ Network Forensic ชื่อโปรแกรมมีเครื่องมือหนึ่งที่ช่วยให้เรา เห็นกลุ่มของข้อมูลที่เกิดขึ้นว่ามีปริมาณเท่าไร โดยจะขอเริ่มจากการใช้งาน IO Graph เป็นการแสดงผลของข้อมูลแพ็กเก็ตที่เก็บมาได้นำมาแสดงผลในรูปแบบของกราฟ โดยที่สามารถทำการเลือกชุดของข้อมูลมาแสดงผลได้ตามที่ต้องการโดยต้องใช้งานร่วมกับ Filter Statement ซึ่งจะแตกต่างจาก TCP Flow Graph เป็นต้น

๖.๑ การแสดงผลโดยการใช้งาน IO Graph

- ๖.๑.๑ สามารถทำการซูมดูข้อมูลในแนวแกน x และแกน y ได้ (TCP Flow Graph ทำได้ไม่ดี)
 - ๖.๑.๒ สามารถกำหนดสีของกราฟในการแสดงผลข้อมูลได้
 - ๖.๑.๓ สามารถกำหนดรูปแบบของกราฟได้ เช่น กราฟเส้น impulse เป็นต้น
 - ๖.๑.๔ สามารถใส่สูตรทางคณิตศาสตร์เพื่อคำนวณผลที่ได้และแสดงผลที่กราฟได้
 - ๖.๑.๕ สามารถปรับแกน y ให้แสดงผลแบบ Logarithm เพื่อแสดงผลที่มีค่าแตกต่างกันมากได้
 - ๖.๑.๖ สามารถนำค่าต่าง ๆ ที่ต้องการมาทำการแสดงผลเพื่อเปรียบเทียบความสัมพันธ์กันได้ดี
- สูงสุด ๕ ชุดข้อมูล

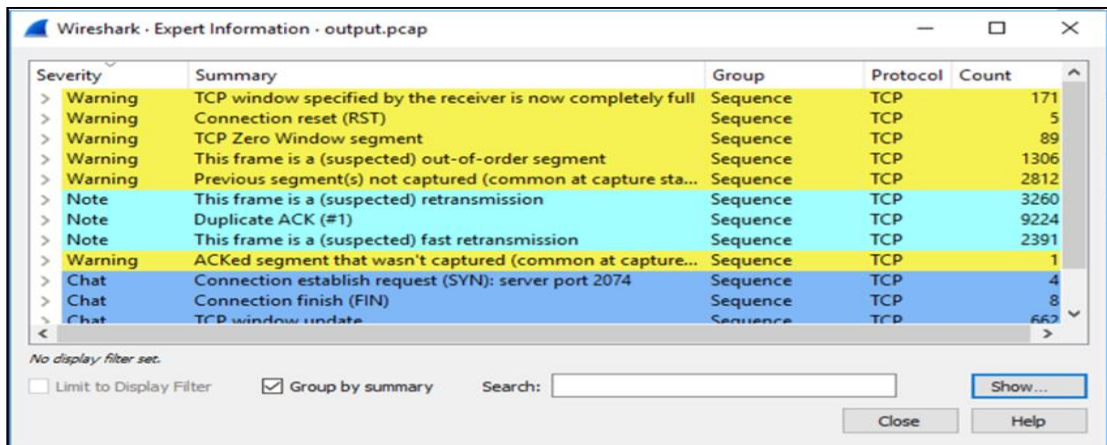


ภาพที่ ๑๑๔ วิเคราะห์กระบวนการทำงานของมัลแวร์



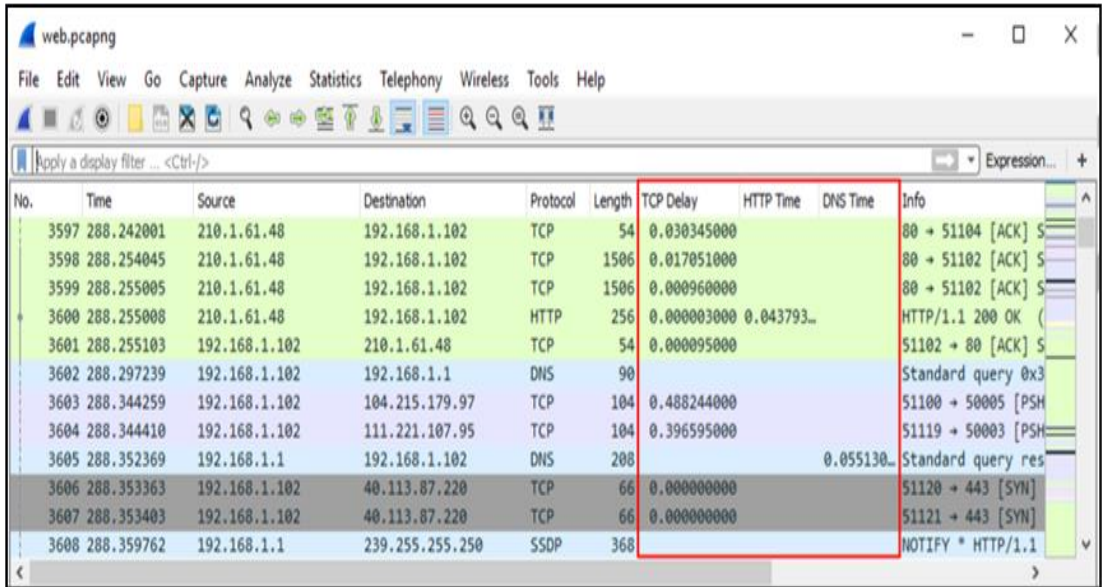
ภาพที่ ๑๑๕ การแสดงผลด้วย IO Graph

๖.๑.๗ การแสดงผลด้วย IO Graph การนำ IO Graph มาใช้แสดงผลข้อมูลจะได้ข้อมูลที่มีความละเอียดในการแสดงผลด้านเวลา และการนำชุดข้อมูลมาแสดงผลเพื่อเปรียบเทียบกัน ดังนั้นเมื่อเกิดความผิดพลาดระหว่างโปรแกรมที่ทำงานอยู่ใน ระบบ Network เดียวกัน หรือมี Source-Destination ที่เกี่ยวข้องกันก็จะสามารถนำชุดข้อมูลที่ได้จากการ Filter ขึ้นมาทำการแสดงผลเพื่อเปรียบเทียบการทำงานหรือความผิดปกติที่อาจจะเกิดขึ้นซึ่งส่งผลให้ระบบ Network ได้รับผลกระทบนั้นได้อย่างชัดเจนทั้งนี้ การใช้งานโปรแกรม Wireshark โดยปกติแล้วเมื่อเราต้องการหาข้อมูลบางอย่างเช่นการที่เครื่อง Client ต้องการเปิด Connection เพื่อเริ่มสื่อสารกับเครื่อง Server ตามเนื้อหาทางทฤษฎีเราจะเริ่มต้นทำการหา แพ็กเก็ต TCP SYN หรือในกรณีที่มีการปิด Connection จะต้องมีการส่งแพ็กเก็ต FIN เพื่อเริ่มการปิด Connection การสื่อสาร หรือกรณีที่เกิดความผิดพลาดอื่นเช่นการเกิดแพ็กเก็ต Re-transmission ในกรณีที่มี การร้องขอข้อมูลที่ขาดหายไป กรณีที่ไฟล์แพ็กเก็ตมีขนาดใหญ่มาก การที่จะหาแพ็กเก็ตดังกล่าวอาจจะทำได้ยาก เนื่องจากแพ็กเก็ต SYN/FIN จะมีการส่งออกมาเพียงแค่ครั้งเดียว ดังนั้นโปรแกรม Wireshark จึงมีเครื่องมือ สำหรับการทำสรุปเหตุการณ์ที่สำคัญที่เกิดขึ้นจากแพ็กเก็ตที่เปิดขึ้นมาในโปรแกรมไว้ให้ นั่นคือ Expert Information นั่นเอง โดยใน Expert Information จะทำการสรุปความผิดปกติของการสื่อสารและจะสรุปรวมเหตุการณ์ต่าง ๆ ที่พบอยู่ในแพ็กเก็ตที่กำลังเปิดใช้งานอยู่ไว้เป็นกลุ่มของเหตุการณ์ ดังนั้น การค้นหาความผิดปกติต่าง ๆ ที่เกิดขึ้นก็จะสามารถทำได้โดยง่ายจากการใช้งาน Expert Information สำหรับรูปตัวอย่างของข้อมูลที่ได้จาก Expert Information จะมีตามภาพที่ ๑๐๕

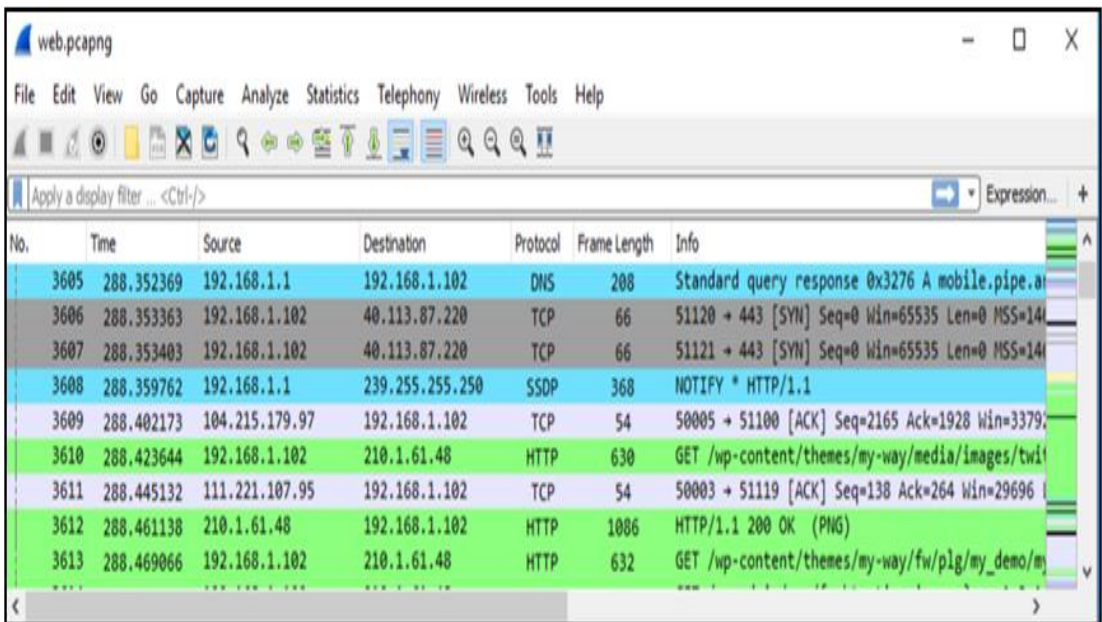


ภาพที่ ๑๑๖ แสดงข้อมูลสรุปที่ได้จาก Expert Information

การเพิ่ม Column เพื่อแสดงข้อมูลเพิ่มเติมโดยปกติแล้วโปรแกรม Wireshark จะมีการแสดงผลทางหน้าจอโปรแกรมเป็นค่ากลางของ โปรแกรมอยู่แล้วคือค่า Default เพื่อใช้แสดงผลแบบทั่วไปซึ่งเพียงพอต่อการใช้งานอยู่แล้ว แต่ในบางกรณี ผู้ใช้งานต้องการนำข้อมูลบางอย่างที่ตัวเองสนใจไปแสดงผลเพื่อให้สามารถตรวจสอบการทำงานของ Network ที่กำลังวิเคราะห์ ดังนั้นการเพิ่มชุดข้อมูลลงไปเพื่อนำไปแสดงผลเป็น Column ใหม่จึงเป็นทางเลือกที่ดีทำให้การวิเคราะห์สะดวกมากขึ้น โดยโปรแกรม Wireshark สนับสนุนความสามารถนี้ให้ผู้ใช้สามารถนำชุดข้อมูลมาแสดงผลได้ตามที่ต้องการ เช่น การแสดงผลของค่า TCP Time ซึ่งเป็นข้อมูลที่โปรแกรม Wireshark สามารถทำการคำนวณได้จากแพ็กเก็ตตามปกติ สามารถนำข้อมูลชุดนี้มาแสดงผลเป็น Column เพิ่มเติมได้เช่นเดียวกันตามภาพที่ ๑๐๖ การนำค่า TCP time มาแสดงผลเป็น Column เพิ่มบนโปรแกรม Wireshark การใช้งาน Profile ต่อเนื่องจากหัวข้อการเพิ่ม Column เมื่อเราต้องการข้อมูลขึ้นมาแสดงผลเพื่อให้เหมาะกับการใช้งานวิเคราะห์หรือศึกษาข้อมูลจากแพ็กเก็ตโดยการเพิ่มชุดข้อมูลต่าง ๆ เช่น Column ของ TCP delay หรือ HTTP Response เพื่อให้สามารถอ่านค่าได้ง่ายมากขึ้น แต่ในกรณีที่ไม่ต้องอ่านค่าดังกล่าวแล้ว การแสดงผล Column เหล่านั้นก็จะเป็นข้อมูลที่ไม่ได้ถูกใช้งาน และกลายเป็นสิ่งที่รบกวนการทำงาน เนื่องจากการรบกวนสายตา ดังนั้นโปรแกรม Wireshark จึงได้มีการจัดการโปรไฟล์ในการแสดงผลข้อมูลขึ้นมาเพื่อใช้แก้ไข เช่น ในกรณีที่ต้องการวิเคราะห์การทำงานของ HTTP ก็ให้ทำการจัดการแสดงผลให้เหมาะสมและทำการบันทึกเป็น HTTP Profile ต่อมาเมื่อต้องการวิเคราะห์ข้อมูลการใช้งานเกี่ยวกับ Database ก็ทำการสร้างการแสดงผลของ Database และบันทึกไว้ กรณีที่ต้องการใช้งานแบบปกติก็ทำการ เรียกค่า Default Profile มาใช้งาน ถ้าต้องการกลับไปวิเคราะห์การทำงานของ HTTPก็ทำการเรียก HTTP Profile กลับมาใช้งานได้ทันที การสลับการแสดงผลของ Profile แบบนี้ มีความยืดหยุ่นการใช้งาน มากกว่าการใช้งานแบบปกติ ซึ่งจะต้องมีการจัดการแสดงผลใหม่ทุกครั้งที่ต้องการใช้การแสดงผลข้อมูลในแบบเฉพาะเจาะจง



ภาพที่ ๑๑๗ การแสดงผลโดย Custom Profile



ภาพที่ ๑๑๘ การแสดงผลโดย Default Profile

๖.๑.๘ การทดลองตรวจสอบและดึงข้อมูลจากแพ็กเก็ต HTTP ให้ใช้โปรแกรม Wireshark จับแพ็กเก็ตระหว่างใช้งานอินเทอร์เน็ต ในระหว่างนั้นให้ทำการเข้าเว็บไซต์และเปิดไฟล์ชนิดต่าง ๆ เช่น รูปภาพและวิดีโอ เป็นต้น ทำการหยุดจับแพ็กเก็ต และบันทึกเพื่อทำการทดลองต่อไป สิ่งที่จะได้รับจากการทดลองสามารถทำการดึงข้อมูลชนิดต่าง ๆ ออกมาจากแพ็กเก็ต HTTP เพื่อทำการตรวจสอบการทำงานได้ (Forensics) ขั้นตอนการทดลองเตรียมความพร้อมด้วยการตรวจสอบการตั้งค่าของโปรแกรม Wireshark ก่อนทำการกดปุ่มที่ Edit Preferences ที่หน้าต่าง Wireshark Preferences ให้ทำการหาโปรโตคอล IPv4 และเลือก Reassemble Fragmented IPv4 Datagrams ที่หน้าต่าง Wireshark Preferences ให้ทำการหาโปรโตคอล TCP และเลือก Validate the TCP Checksum if Possible และ Allow Subdissector to Reassemble TCP Streams เมื่อตรวจสอบการตั้งค่าทั้งหมดถูกต้องแล้วให้ทำการเลือกที่เมนู File -> Export Objects -> HTTP โปรแกรม Wireshark จะทำการรวมแพ็กเก็ต HTTP ที่ได้กลับเป็นไฟล์ขึ้นมาให้ใหม่ที่หน้าต่าง HTTP Object List ให้ทำการเลือกไฟล์ขึ้นมาหนึ่งไฟล์และทำการ Save ลงที่เครื่องคอมพิวเตอร์ ด้วยการกดปุ่ม Save As ทำการเปิดไฟล์ที่บันทึกลงในเครื่องขึ้นมาดูว่าได้ไฟล์ที่สมบูรณ์หรือไม่ จากตัวอย่างจะเป็นไฟล์ Network Diagram ที่สร้างจาก UnetLab ให้ลองทำการหาไฟล์ประเภทอื่นที่ได้จากการ Export ของโปรแกรม Wireshark ทำการ Save และเปิดไฟล์

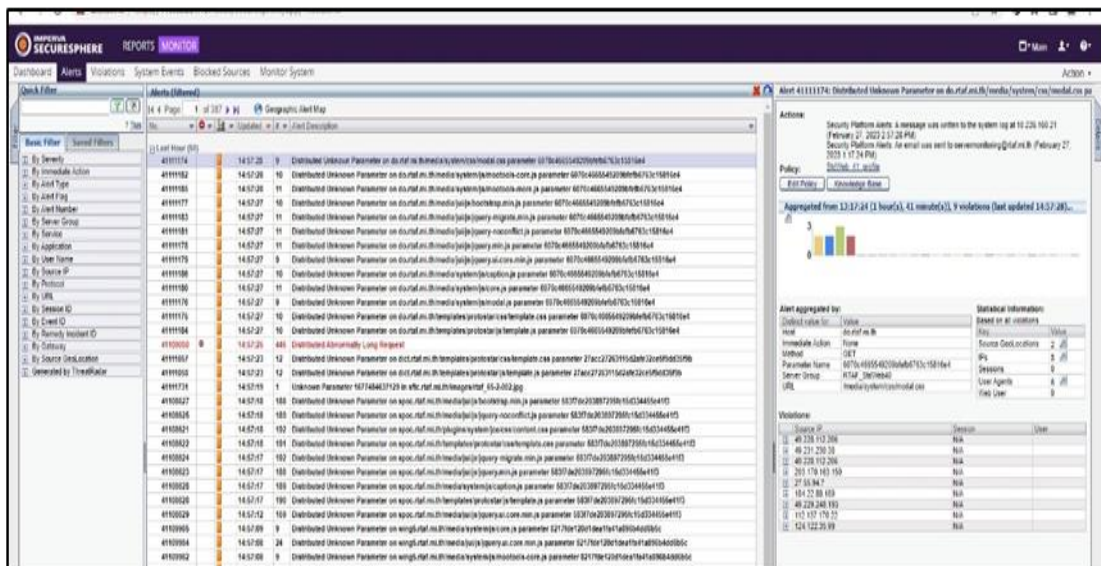
๖.๑.๙ การทดลองถอดรหัส HTTPS ก่อนที่จะเริ่มทำ Lab สามารถเลือกทำ Lab ด้วยตนเอง หรือจะใช้ไฟล์ที่ได้เตรียมไว้ให้ เนื่องจากทำ Lab ด้วยตนเองจะเสียเวลาในการ Restart Windows ก่อนเริ่มทำเนื้อหา Lab โดยปกติแล้วเราจะไม่สามารถดูข้อมูลที่ใช้งานโปรโตคอล HTTPS ได้ เนื่องจากข้อมูลจะมีการเข้ารหัสอยู่ แต่สามารถใช้เทคนิคบางอย่างในการทำให้โปรแกรม Wireshark สามารถทำการถอดรหัส SSL ได้ โดยเริ่มจาก ขั้นตอนที่ ๑ เพิ่มตัวแปร Environment ของ Windows เพื่อให้ Windows สามารถทำการ Export SSL Log เพื่อนำไปใช้ถอดรหัส SSL ด้วยขั้นตอนดังนี้ เข้าไปที่เมนู Control Panel -> System and Security -> System -> Advanced System Settings -> Advanced -> Environment Variables... จากนั้นขั้นตอนที่ ๒ ให้ทำการกด New เพื่อเพิ่มตัวแปรระบบให้ทำการตั้งชื่อตัวแปรระบบใหม่ชื่อ SSLKEYLOGFILE และทำการ Save ไว้ที่ตำแหน่งใดก็ได้ ทำการเก็บไว้ที่ C:\Users\demo\Desktop\sslkey.log เสร็จแล้วให้ทำการ Restart เครื่องที่ต้องการถอดรหัส SSL จากนั้นให้ทำการเปิดใช้งาน Web Browser ตามปกติ โดยให้เน้นทำการลองเข้าใช้งานเว็บไซต์ที่เป็น HTTPS เพื่อให้ Windows ทำการ Export SSL Log ให้กับเรา โดยให้ลอง Login ใช้งาน Web mail เช่น Gmail หรือ Outlook เป็นต้น เพื่อลองหา Username และ Password ในการ Login จากการถอดรหัส SSL ขั้นตอนที่ ๓ เปิดโปรแกรม Wireshark และทำการเพิ่ม SSL Log ที่ได้ทำการบันทึกไว้ก่อนหน้านี้ โดยเข้าไปที่เมนู Edit > Preferences เลือก Advanced -> Search Tls และใส่ Path ที่เก็บ Log File ไว้ จากขั้นตอนที่ ๒ เมื่อทำการเพิ่ม SSL log เรียบร้อยแล้ว โปรแกรม Wireshark จะทำการเพิ่มแถบข้อมูลด้านล่างเพื่อแสดงข้อมูล SSL ที่ถูกถอดรหัสเพิ่มที่ตำแหน่งของ Packet byte pane ให้ลองทำการ Filter ด้วย Filter string ดังนี้ "http.request.method== "POST" &&Tls" แล้ว Apply ดูผลลัพธ์ที่ Packet Detail Pane และค้นหาข้อมูลที่นำสนใจจาก Packet

๖.๑.๑๐ การวิเคราะห์จากโปรแกรม Imperva ซึ่งเป็น Web App Firewall โดยสามารถ Download Logs ผ่าน Dashboard



ภาพที่ ๑๑๙ โปรแกรม Imperva

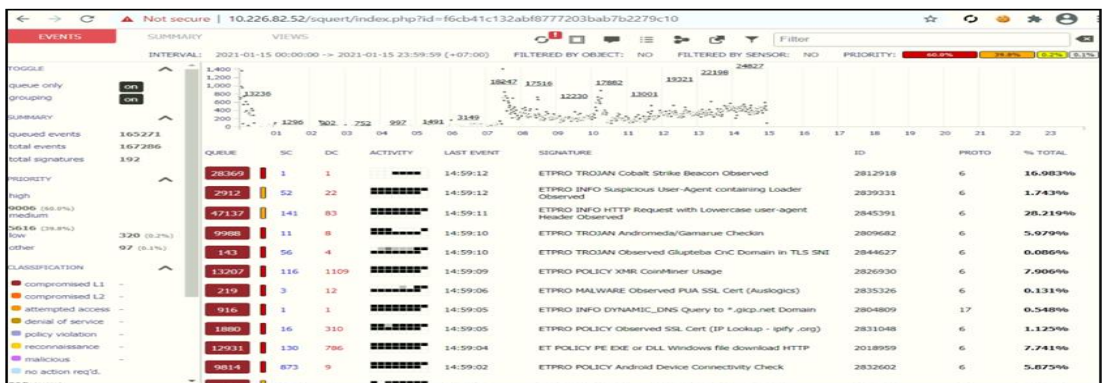
เข้าไปที่เมนู View Results> Manage Reports เลือก Group ของรายงานที่ต้องการ จากนั้นให้คลิกที่ Tab Data Scope >กำหนดวันที่เริ่มต้น และวันสิ้นสุด > กดบันทึกกลับมาที่ Tab General Details >กำหนดรูปแบบไฟล์ ในที่นี้แนะนำเป็น .CSV >คลิก Run Report และทำการดาวน์โหลดไฟล์ ทั้งนี้การใช้งานสามารถเปิดด้วยโปรแกรม Microsoft Excel โดยสามารถนำ Logs มาวิเคราะห์สถิติการโจมตีของแต่ละประเทศ รูปแบบการโจมตี ความสำเร็จของการโจมตี หมายเลข IP Address แล้วนำไปดำเนินการ Block โดยการวิเคราะห์จะนำหมายเลข IP Address ไปตรวจสอบกับเว็บไซต์ VirusTotal.com และ AbuseIP เพื่อหาความสัมพันธ์กับกลุ่มหรือหมายเลข IP Address ที่เป็นภัยคุกคาม



ภาพที่ ๑๒๐ การวิเคราะห์ลักษณะของ URL โดยโปรแกรม Imperva

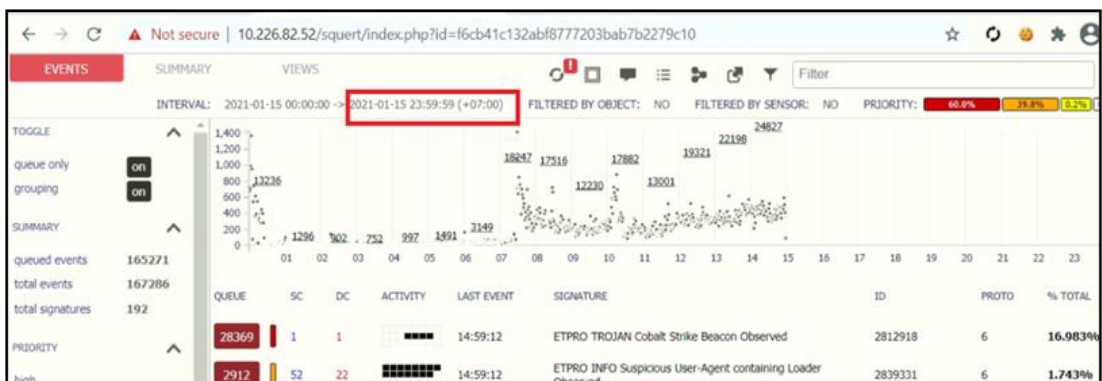
อีกส่วนหนึ่งก็คือการวิเคราะห์ลักษณะของ URL ที่เข้ามาว่าเป็นความพยายามทำอะไร มีการตอบกลับของ Server ผังเราหรือไม่ มีการ Block ของ Firewall หรือไม่ และส่งผลกระทบต่อเว็บไซต์ใดของกองทัพอากาศ เพื่อให้การวิเคราะห์มีความครบถ้วนสามารถสืบค้นเหตุการณ์ย้อนหลัง จึงต้องมีการนำเข้าสู่ข้อมูล และจัดเก็บในระบบฐานข้อมูล phpMySQL เพื่อใช้ในการทำรายงาน

๖.๑.๑๑ Security Onion เป็นโปรแกรมประเภทแจ้งเตือน และวิเคราะห์ Logs จากการเข้าถึงทางเครือข่ายสารสนเทศของกองทัพอากาศ ทำหน้าที่รวบรวม จัดเก็บแยกประเภทโปรโตคอลภัยคุกคาม และแจ้งเตือน (Alert) โดยรับ Logs จากอุปกรณ์เครือข่ายที่ทำหน้าที่เป็น Core Switch ดังนั้นหากเกิดการโจมตีจากภายนอกเครือข่ายหรือภายในเครือข่ายของ ทอ.จะสามารถตรวจสอบจากโปรแกรมนี้



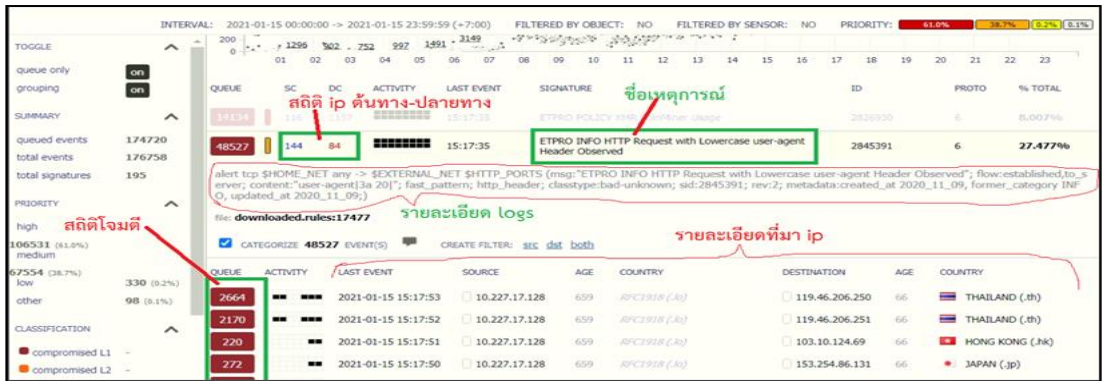
ภาพที่ ๑๒๑ Security Onion

ก่อนอื่นต้องทำการเซตค่าวันเวลาของ Logs ให้เป็นเวลาประเทศไทยเสียก่อน เพื่อป้องกันความสับสนกับเวลาจริง (Time Zone) เมื่อเกิดการโจมตี โดยนำมาส์ไปคลิกที่เวลาดังภาพที่ ๑๑๑



ภาพที่ ๑๒๒ Set ค่าวันเวลาของ Logs

คลิกเครื่องหมายถูกออกแล้วกด  เพื่อให้ระบบโหลดข้อมูลใหม่

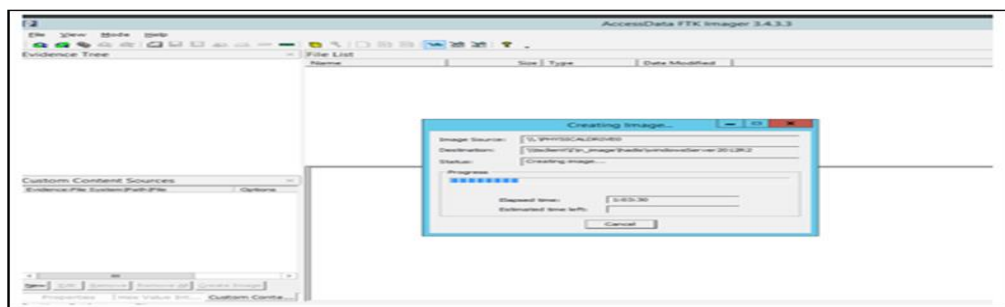


ภาพที่ ๑๒๓ สถิติที่ทำการโจมตี

สำหรับข้อมูลที่เราจะได้จาก Security Onion นั้นจะมีหลายส่วน โดยหลัก ๆ ก็คือ สถิติที่ทำการโจมตีเข้ามาทำให้เราทราบว่า ณ ปัจจุบันมีความพยายามโจมตีระบบด้วยเทคนิคประเภทใดมีเป้าหมายไปยังที่ไหน ทั้งนี้ยังสามารถใส่ IP Address เพื่อค้นหาเครื่องผู้ใช้งานในระบบ พร้อมทั้งมี Tab Summary เพื่อสรุปและแสดงกลุ่มข้อมูลลำดับ ๑ - ๑๐ ของการโจมตี และแผนที่แสดงการโจมตีจากทั่วโลกอีกด้วย

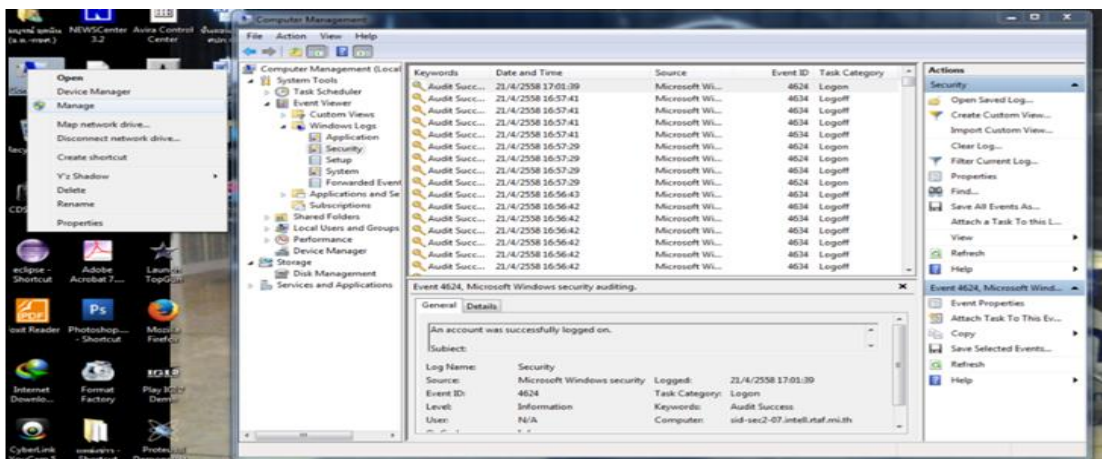
๖.๒ การวิเคราะห์ Host Forensic

การเตรียมหลักฐานก่อนการวิเคราะห์ (Master and Slab) ไม่ว่าจะป็นฮาร์ดดิสก์หรือ RAM ก็ต้องทำค่า Hash เสมอ ซึ่งกระบวนการโคลนดิสก์หรือแคปเชอร์ RAM ด้วยโปรแกรม FTK โปรแกรม จะทำการสร้าง Hash ให้อัตโนมัติเมื่อได้ทำการโคลนเสร็จ โดยผู้ทำการเตรียมหลักฐานก่อนการวิเคราะห์ต้องทำการบันทึกข้อมูลหรือถ่ายภาพไว้ด้วยเสมอและจะต้องเตรียมฮาร์ดดิสก์ไว้ ๒ ลูก โดยฮาร์ดดิสก์ลูกแรกเราจะใช้ทดสอบจริงบนเครื่อง PC จริงๆ เพื่อหาข้อมูลที่มีอยู่ ณ ขณะนั้น เช่น ไฟล์ที่ต้องสงสัย วันเดือนปี ที่สร้างหรือแก้ไขไฟล์ Startup การตั้งค่าที่ผิดปกติใน Registry ไฟล์โฮส ประวัติ Web Browser, Windows Logs, Web Server Logs และ DB Logs เป็นต้น อาจเรียกว่าเป็นการวิเคราะห์ด้วยคน ฮาร์ดดิสก์ที่สองใช้ทำอิมเมจไฟล์ สำหรับหาข้อมูลที่อาจถูกลบไปประวัติการใช้ไฟล์ต่าง ๆ อาจเรียกว่าเป็นการวิเคราะห์ด้วยโปรแกรมอัตโนมัติ



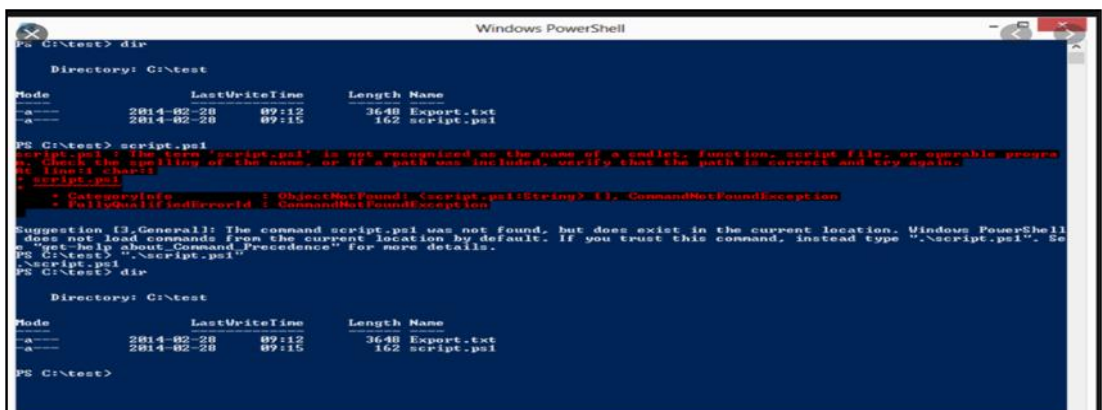
ภาพที่ ๑๒๔ โปรแกรม FTK Imager

๖.๒.๑ การวิเคราะห์ Disk Image ในที่นี้จะกล่าว การวิเคราะห์ด้วยคน ซึ่งเป็นการอ่าน และวิเคราะห์ Logs ด้วยตัวเองหรือผ่านโปรแกรมช่วยเหลือในการค้นหาบ้างเล็กน้อย ข้อดีคือทำให้ได้ ข้อมูลเชิงลึก แต่ก็ใช้เวลาในการวิเคราะห์นานด้วย สำหรับสิ่งที่จะทำการค้นหาและวิเคราะห์ ได้แก่ ประวัติการใช้งานเว็บไซต์ หรือ History ของเว็บนั้นเอง มีประโยชน์ในการช่วยยืนยันว่าผู้ใช้งานมีการ เข้าเว็บไซต์ที่เป็นอันตรายหรือไม่ ในที่นี้จะขอกกล่าวแค่ Web Browser เช่น Chrome, Firefox และ IE Logs เป็นต้น ซึ่ง Logs จะมีอยู่ด้วยกัน ๒ ส่วนใหญ่ ๆ คือ Logs Web และ Logs ของเครื่อง โดย Logs ของระบบปฏิบัติการ Linux จะถูกเก็บไว้ที่ #> nm /var/log/message หรือ #> cat /dev/null > file_log.txt สำหรับระบบปฏิบัติการ Windows จะเรียกว่า Even Logs และจะถูกเก็บไว้ ดังภาพที่ ๑๑๔



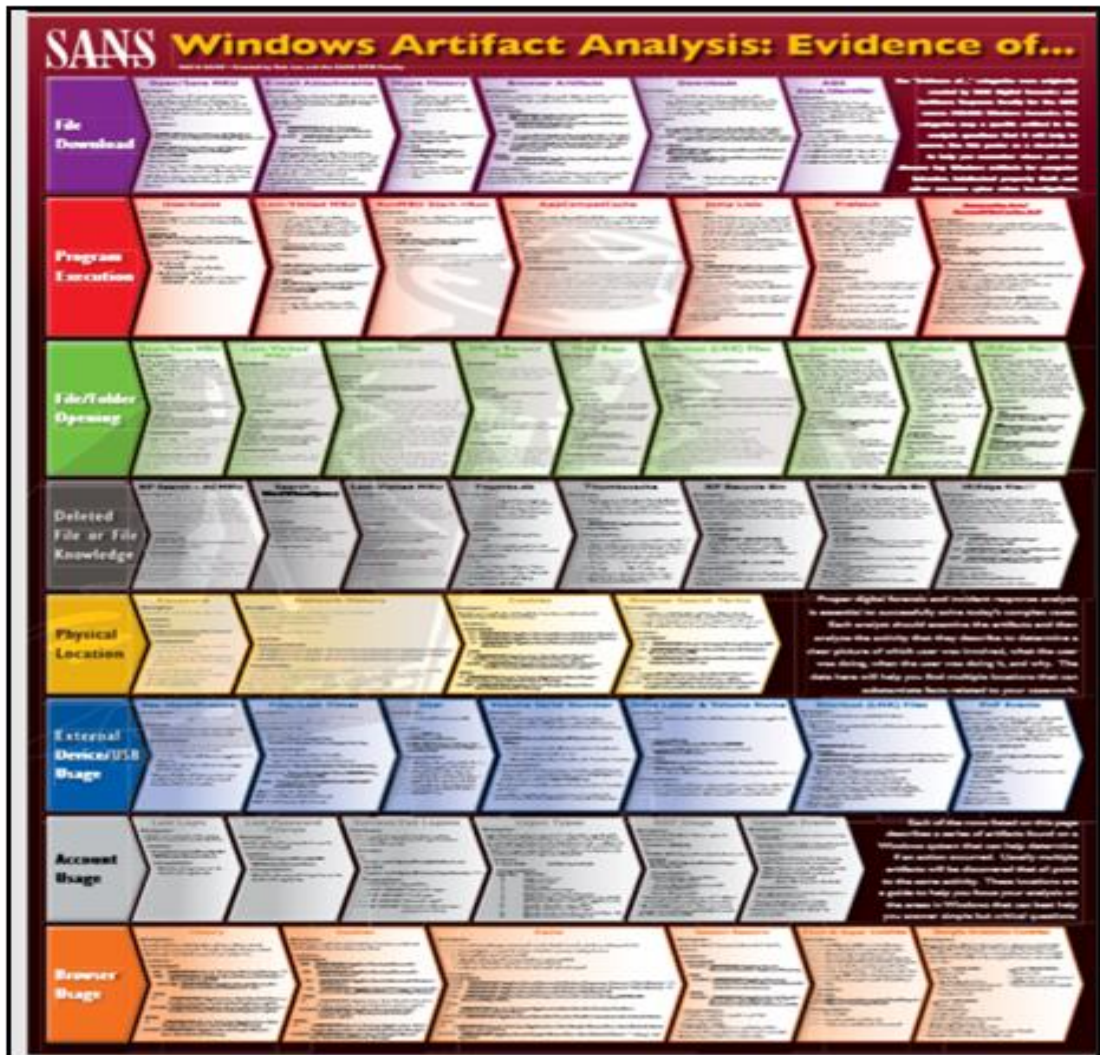
ภาพที่ ๑๒๕ การวิเคราะห์ Disk Image

นอกจากนี้ Windows ยังเก็บ Log ไว้ในตำแหน่ง C:\WINDOWS\system32\logFiles Logs Web จะขึ้นอยู่โปรแกรม Web Server ที่ได้ติดตั้งไว้ เช่น Joomla จะเก็บไฟล์หน้าเว็บไว้ที่ Windows Server 2003 Services เป็นต้น ให้เข้าไปภาพที่ ๑๑๕ แล้วเปิดไฟล์ที่ชื่อ Event log ดังภาพที่ ๑๑๕ ด้วยการรันคำสั่งผ่าน Windows PowerShell เป็นการตรวจสอบว่ามีการใช้งานหรือไม่



ภาพที่ ๑๒๖ ประวัติการใช้งาน Word Error หรือข้อความแจ้งเตือนของ Microsoft Office

๖.๒.๒ วงจรชีวิตของไฟล์ (File Evident การลบ ย้าย คัดลอก) จะเป็นเรื่องของการหาข้อมูลจากการเปลี่ยนแปลงของไฟล์เมื่อผู้ใช้งานมีการใช้งานไฟล์ ทำให้ทราบได้ว่าใครเป็นผู้รันไฟล์ และไฟล์เกิดจากที่ใดเป็นครั้งแรก มีการแพร่กระจายไปที่ใดบ้าง เนื้อหาส่วนนี้มีรายละเอียดเพิ่มเติม แนะนำให้ศึกษาจากเอกสารของ SANS ดังภาพที่ ๑๑๖



ภาพที่ ๑๑๖ วงจรชีวิตของไฟล์

๖.๒.๓ โพรเซสพื้นฐานในระบบ Windows นักวิเคราะห์ควรรู้ว่าพื้นฐานของ Host Windows ที่จะช่วยลดกระบวนการค้นหาแม่ลแแวร์ที่เกิดขึ้นได้อย่างรวดเร็ว โดยสามารถใช้ข้อมูลตัวอย่างการวิเคราะห์โพรเซส เป็นข้อมูลอ้างอิงเพื่อให้ทราบว่าในสถานะการใช้งานปกติมี Service อะไรบ้างในระบบ Windows หากเกิดความผิดปกติจะช่วยให้การวิเคราะห์มีความถูกต้องมากขึ้น ดังแสดง

๖.๒.๓.๑ Service system> Parent Process : Default Part = ไม่สามารถสร้างได้จาก image, Number of Instances : Parent Process = 1 , User Account : User Login = Local System, Start Time : เวลาเริ่มต้น = At boot time (ขึ้นอยู่กับเวลาในการบูต), Description : System จะทำการประมวลผลและรับผิดชอบในโหมดการทำงานนี้ มอดูลที่ทำงานภายใต้ System.exe จะเป็น Child Process ได้แก่ .sys แต่ยังมี .dll อีกหลายตัวที่ทำงานตาม Kernel ของระบบปฏิบัติการนั้น เช่น ntoskrnl.exe เป็นต้น

๖.๒.๓.๒ Service smss.exe> Parent Process: Default Part ปกติจะต้องอยู่ใน System\root\System32\smss.exe, Parent Process : ระดับสิทธิ์ = System Number of Instances : Parent Process จะมี Instructions Process , User Account : User Login = Local System, Start Time : เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสต์ของระบบไม่กึ่งวินาที, Description : มีหน้าที่ในการสร้าง Session และ Instructions ซึ่ง Instructions จะสร้าง Child Instructions โดยกระบวนการจะเริ่มต้นที่ระบบย่อยของ windows (csrss.exe & womomot.exe) โดยมี Service wininit.exe มี Session = 0 และ Service winlogon.exe มี Session = 1 หรือสูงกว่า

๖.๒.๓.๓ Service wininit.exe> Parent Process : Default Part = ปกติจะต้องอยู่ใน SystemRoot\System32\wininit.exe, Parent Process : สร้างโดย Instance ของ smss.exe ดังนั้นเครื่องมือมักจะไม่ได้รับบุชื่อกระบวนการหลัก, Number of Instances : Parent Process = 1 , User Account : User Login = Local System, Start Time: เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสต์ของระบบไม่กึ่งวินาที, Description : จะเริ่มต้นโดยจะเป็น Key ของ Background ภายใต้ Session 0 และจะ Start Service อีก ๓ ตัวคือ Control Manager (services .exe) ,Local Session Manager (lsm.exe) และ Local Session Manager (lsm.exe)

๖.๒.๓.๔ Service taskhost.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\taskhost.exe, Parent Process : ระดับสิทธิ์ = services.exe, Number of Instance : Parent Process = 1 หรือมากกว่า, User Account : User ล็อกอิน = Local System, Start Time : เวลาเริ่มต้นไม่แน่นอนและมีความแตกต่างกันอย่างมาก, Description : เป็นกระบวนการประมวลผลโพรเซสทั่ว ๆ ไปของ Windows Tasks Manager โดยจะมี Universal Background Process Manager (UBPM) ทำงานอยู่เบื้องหลัง เช่น User login, Start System , เวลาของ CPU, Windows log event, เครื่อง Lock หรือเครื่อง Unlock เป็นต้น มีงานมากกว่า ๗๐ รายการที่กำหนดค่าไว้ล่วงหน้าในการติดตั้งเป็นค่าเริ่มต้นของ Windows 7 Enterprise (แม้ว่าหลาย

ง
๑
น
จะถูกปิดใช้งาน) เช่น defrag.exe ถูกกำหนดเวลาให้มีการทำงานในทุกวันพุธ ช่วงเวลา ๐๑๐๐ และมีการสำรองข้อมูลไฟล์ กลุ่ม Registry หลักทุก ๆ ๑๐ วัน เป็นต้น ไฟล์ปฏิบัติการทั้งหมด (DLLS & EXE) ที่ใช้งานเป็นค่าเริ่มต้น และใช้ในการกำหนดเวลา Windows 7 และ Windows 8 จะได้รับรองโดย Microsoft

๖.๒.๓.๕ Service lsass.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\lsass.exe, Parent Process : ระดับสิทธิ์ = winint.exe Number of Instances : Parent Process = 1 , User Account : User Login = Local System Start Time : เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสท์ของระบบไม่ว่าวันที่ Description : = lsass.exe หรือชื่อเต็มคือ Local Security Authentication Subsystem Server process รับผิดชอบในการตรวจสอบผู้ใช้ โดยการเรียกผู้ให้บริการความปลอดภัยของแพ็คเกจที่ เหมาะสม (SSP) การรับรองความถูกต้องที่ระบุใน Registry HKLM\SYSTEM\CurrentControlSet\Control\Lsa โดยทั่วไปจะเป็น Kerberos SSP ใช้สำหรับบัญชีโดเมน หรือ MSV1_0 SSP ใช้สำหรับ local accounts เมื่อผู้ใช้ได้รับการรับรองความถูกต้อง lsass.exe จะสร้างโทเค็นการเข้าถึงสำหรับผู้ใช้ที่ระบุสิทธิ์ และข้อจำกัดด้านความปลอดภัยสำหรับผู้ใช้ และกระบวนการอื่นของผู้ใช้เท่านั้น ซึ่งเป็นกระบวนการหนึ่งของกระบวนการที่ควรเกิดขึ้น และไม่ควรมีโปรเซสลูก

๖.๒.๓.๖ Service winlogon.exe>, Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\winlogon.exe, Parent Process : ระบุสิทธิ์ สร้างโดยกระบวนการของ smss.exe ดังนั้นเครื่องมือวิเคราะห์มักจะไม่ได้ระบุชื่อกระบวนการหลัก, Number of Instances : Parent Process = 1 หรือมากกว่า, User Account : User Login = Local System, Start Time : เวลาเริ่มต้น ภายในไม่ว่าวันที่ของเวลาบูสท์สำหรับกระบวนการแรก (สำหรับเซสชัน ๑) เวลาเริ่มต้นสำหรับกระบวนการเพิ่มเติมเกิดขึ้นเมื่อมีการสร้างเซสชันใหม่โดยทั่วไปผ่านทาง Remote Desktop หรือการเข้าสู่ระบบการสลับผู้ใช้อย่างรวดเร็ว Description : เป็นระบบตอบโต้ผู้ใช้เวลา login หรือ logoff ถูกเปิดใช้งานโดย Service LogonUI.exe ซึ่งจะรับชื่อผู้ใช้และรหัส ผ่านหน้าจอเข้าสู่ระบบและส่งผ่านข้อมูลรับรองไปยัง lsass.exe เพื่อตรวจสอบข้อมูลรับรองเมื่อผู้ใช้ได้รับการรับรองความถูกต้องแล้ว Winlogon.exe จะโหลด NTUSER.DAT ของผู้ใช้ลงใน Registry HKCU และเริ่มต้นเชลล์ของผู้ใช้ (explorer.exe) ผ่าน Userinit.exe

๖.๒.๓.๗ Service iexplore.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน System\Program Files\Internet Explorer\iexplore.exe หรือ \Program Files (x86) \Internet Explorer\iexplore.exe, Parent Process : ระดับสิทธิ์ = explorer.exe, Number of Instances : Parent Process = 0 หรือมากกว่า, User Account : User Login ขึ้นอยู่กับว่าใครเป็นผู้ login เข้ามา, Start Time : เวลาเริ่มต้น โดยทั่วไปเมื่อผู้ใช้เริ่ม Internet Explorer อย่างไรก็ตาม กระบวนการดังกล่าวสามารถเริ่มต้นได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า การโต้ตอบของผู้ใช้ผ่านสวิตช์ “-embedding” (ในกรณีนี้ Parent Process อาจไม่ใช่ explorer.exe) Description : = Internet Explorer (IE) เป็นแอปพลิเคชัน Desktop ทั่วไปที่เปิดโดยผู้ใช้แอปพลิเคชัน และเป็นส่วนย่อยของ explorer.exe IE เวอร์ชันใหม่จะมีกระบวนการย่อยสำหรับแต่ละแท็บที่เปิดอยู่ ด้วยเหตุผลหลายประการ รวมถึงความปลอดภัยที่เพิ่มขึ้นเมื่อเข้าสู่เว็บไซต์อินเทอร์เน็ต IE จะเรียกใช้กระบวนการแท็บด้วยความน่าเชื่อถือที่ต่ำซึ่งจะเป็นความยากสำหรับผู้โจมตีที่จะทำการแก้ไขพื้นที่อ่อนไหวของ Registry หรือระบบไฟล์หากพวกเขาสามารถควบคุม Child Process ของ IE ผู้โจมตีมักจะตั้งชื่อไฟล์ iexplore.exe และวางไว้ในไดเรกทอรีสำรอง (misspell Explore.exe) ให้เป็น iexplorer.exe

๖.๒.๓.๘ Service explorer.exe> Parent Process: Default Part = ปกติจะต้องอยู่ใน SystemRoot\explorer.exe, Parent Process : ระดับสิทธิ์ ถูกสร้างโดยกระบวนการของ userinit.exe ดังนั้นเครื่องมือวิเคราะห์มักจะไม่ได้ระบุชื่อกระบวนการหลัก, Number of Instances : รายการต่อผู้ใช้ที่ Logon แบบโต้ตอบ, User Account : User Login ขึ้นอยู่กับว่าใครเป็นผู้ Login เข้ามา Start Time : เวลาเริ่มต้น = เริ่มเมื่อการเข้าสู่ระบบแบบโต้ตอบ Description : Service explorer.exe เป็นหัวใจหลักของ Explorer ช่วยให้ผู้ใช้สามารถเข้าถึงไฟล์ โดยทำหน้าที่เป็นทั้งไฟล์เบราร์เซอร์ผ่าน Windows Explorer (แต่ยังคง explorer.exe) และอินเตอร์เฟซของผู้ใช้ เช่น เดสก์ท็อป และเมนูเริ่มแถบงานของแผงควบคุม เป็นต้น แอปพลิเคชันที่เปิดใช้งานผ่านการเชื่อมโยงผ่านส่วนขยายไฟล์ และ Shortcut ควรมีเพียงหนึ่งกระบวนการของ explorer.exe ที่ทำงานอยู่ การเข้าสู่ระบบแบบโต้ตอบโดยไม่คำนึงถึงหน้าต่าง Windows Explorer ที่เปิดโดยผู้ใช้ให้สังเกตว่า explorer.exe ที่ถูกต้องนั้นอยู่ใน SystemRoot ถ้ามีใดเรกทอรีมากกว่า SystemRoot\System32 มักจะเป็นผู้โจมตี โดยจะตั้งชื่อมัลแวร์ของพวกเขาว่า explorer.exe และวางไว้ใน System32 หรือ misspell explorer.exe บางครั้งจะเป็น expl.exe

๖.๒.๓.๙ Service lsm.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\lsm.exe, Parent Process : ระดับสิทธิ์ = winint.exe, Number of Instances : Parent Process = 1 , User Account : User Login = Local System Start Time : เวลาเริ่มต้นเกิดขึ้นภายหลังการบูตของระบบไม่ว่าวันชาติ Description : เป็นการจัดการบริการ Terminal รวมถึงเซสชัน Remote Desktop รวมถึง local sessions เพิ่มเติมผ่านการสลับผู้ใช้ผ่านการสื่อสารกับ smss.exe เพื่อเริ่มเซสชันใหม่ โดย smss.exe สร้าง csrss.exe และ winlogon.exe เพิ่มเติมเพื่อสนับสนุนเซสชันใหม่ เท่านั้น ซึ่งเป็นกระบวนการหนึ่งของกระบวนการที่ควรเกิดขึ้น และไม่ควรมี Child Process

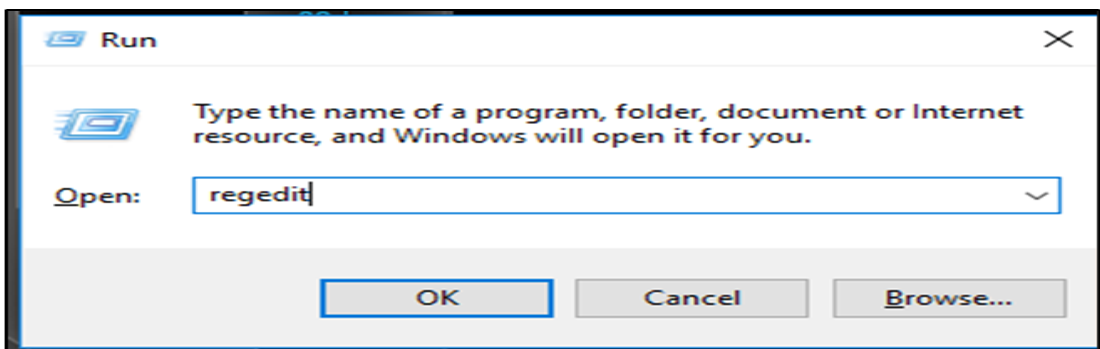
๖.๒.๓.๑๐ Service svchost.exe> Parent Process : Default Part ปกติจะอยู่ใน SystemRoot\System32\smss.exe, Parent Process : ระดับสิทธิ์ = System Number of Instances : Parent Process = 5 และ Child Process User Account : User Login จะแตกต่างกันไปขึ้นอยู่กับกระบวนการ svchost.exe แม้ว่าโดยทั่วไปจะเป็นบัญชี Local System, Network Service หรือ Local Service กระบวนการที่ทำงานภายใต้บัญชีอื่นใดควรได้รับการตรวจสอบ Start Time : เวลาโดยทั่วไปภายในไม่กี่วินาทีของเวลาเริ่มต้นทำงาน อย่างไรก็ตามสามารถเริ่ม Service ได้แล้ว อาจส่งผลให้เกิดกระบวนการใหม่ของ svchost.exe หลังจากเวลา Description : กระบวนการโฮสต์ทั่วไปสำหรับ Windows Services มันถูกใช้สำหรับการเรียกใช้บริการ DLLs Windows จะเรียกใช้ svchost.exe หลายกระบวนการ แต่ละตัวใช้พารามิเตอร์ “-k” ที่ไม่ซ้ำกันสำหรับการจัดกลุ่มบริการที่คล้ายกัน พารามิเตอร์ “-k” ทั่วไปรวมถึง BTsvcs, DcomLaunch, RPCSS, Local Service Network Restricted, Netsvcs, Local Service Network Service, Local Service No Network, Secsvcs และ Local Service And Nolmpersonation ผู้เขียนมัลแวร์

จะใช้ประโยชน์จาก svchost.exe ทั้งโดยตรงหรือโดยอ้อมเพื่อซ่อนมัลแวร์ โดยตรงจะติดตั้งมัลแวร์เป็นบริการในกระบวนการที่ถูกต้องของ svchost.exe และโดยอ้อมจะผสมผสานกับกรณีที่ต้องการของ svchost.exe โดยสะกดชื่อผิดพลาดเล็กน้อย (scvhost.exe) หรือสะกดถูกต้องแต่วางไว้ใน Directory อื่นที่ไม่ใช่ System32 svchost.exe ที่ถูกต้องควรเรียกใช้จากตำแหน่ง SystemRoot \System32 และควรมี services.exe เป็นพาเรนต์ รวมถึงการติดตั้งค่าเริ่มต้นของ Windows 7 ทั้งหมดและบริการที่ดำเนินการด้วย . DLL ซึ่งรับรองโดย Microsoft

๖.๒.๓.๑๑ services.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot \System32\services.exe, Parent Process : ระดับสิทธิ์ = wininit.exe, Number of Instances : Parent Process = 1 , User Account : User Account : User Login = Local System, Start Time : เวลาเริ่มต้นเกิดขึ้นภายหลังการบูสต์ของระบบไม่กึ่งวินาที Description : = Unified Background Process Manager (UBPM) ซึ่งรับผิดชอบกิจกรรมพื้นหลัง เช่น บริการและงานที่กำหนด Services.exe ใช้ Service Control Manager (SCM) จัดการบริการโหลด และอุปกรณ์ไดรเวอร์ที่ทำเครื่องหมายสำหรับการเริ่มอัตโนมัติโดยเฉพาะ นอกจากนี้เมื่อผู้ใช้เข้าสู่ระบบแบบโต้ตอบได้สำเร็จ SCM (services.exe) พิจารณาว่าการบูสต์สำเร็จแล้ว และตั้งค่าชุดควบคุม Last Known Good (HKLM\SYSTEM \ Select>LastKnownGood) ให้เป็นค่าของ CurrentControlSet

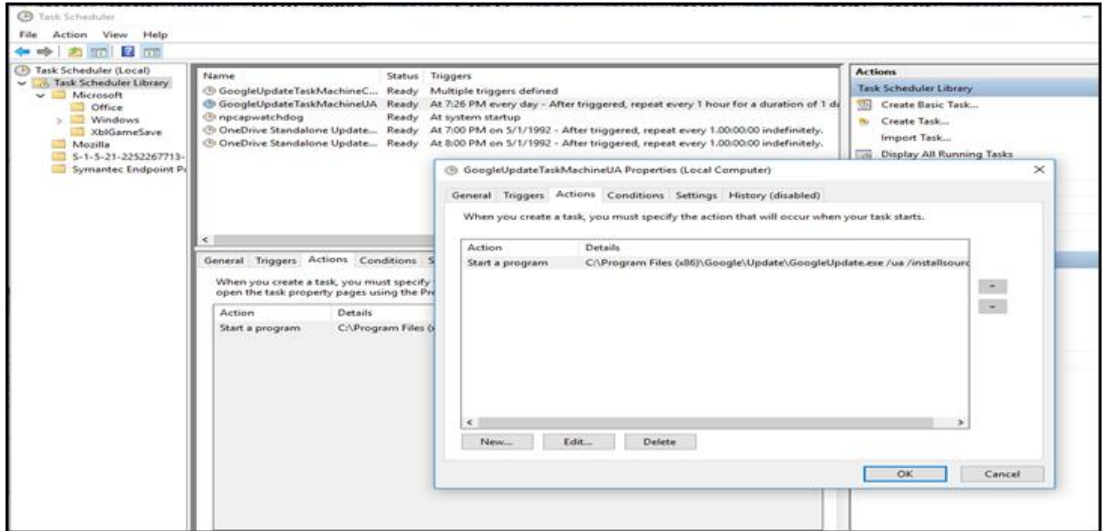
๖.๒.๓.๑๒ Service csrss.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\csrss.exe, Parent Process : ระดับสิทธิ์ สร้างโดยกระบวนการของ smss.exe ดังนั้นเครื่องมือวิเคราะห์มักจะไม่ได้ระบุชื่อกระบวนการหลัก, Number of Instances : Parent Process = 2 หรือมากกว่า, User Account : User Login = Local System, Start Time : เวลาเริ่มต้นภายในไม่กี่วินาทีของเวลาบูสต์สำหรับ ๒ กระบวนการแรก (สำหรับเซสชัน ๐ และ ๑) เวลาเริ่มต้นสำหรับกระบวนการจะเพิ่มขึ้นเหมือนใหม่ และเซสชันจะถูกสร้างขึ้นบ่อยครั้ง แม้ว่าจะสร้างเฉพาะเซสชัน ๐ และ ๑ เท่านั้น

๖.๒.๔ Registry และการหาประวัติการใช้งาน usb คลิกปุ่ม Run หรือใช้คีย์ลัด Window + R พิมพ์ regedit แล้วกด Enter แล้วกดเลือกเข้าเมนูตามนี้ HKEY_ LOCAL_ MACHINE \SYSTEM\CurrentControlSet\Enum\USBSTOR การหาด้วยโปรแกรม USB Forensic Tracker v1.1.3 ทำการแตกไฟล์ก่อน และกดปุ่ม Run เพื่อให้ระบบทำงาน



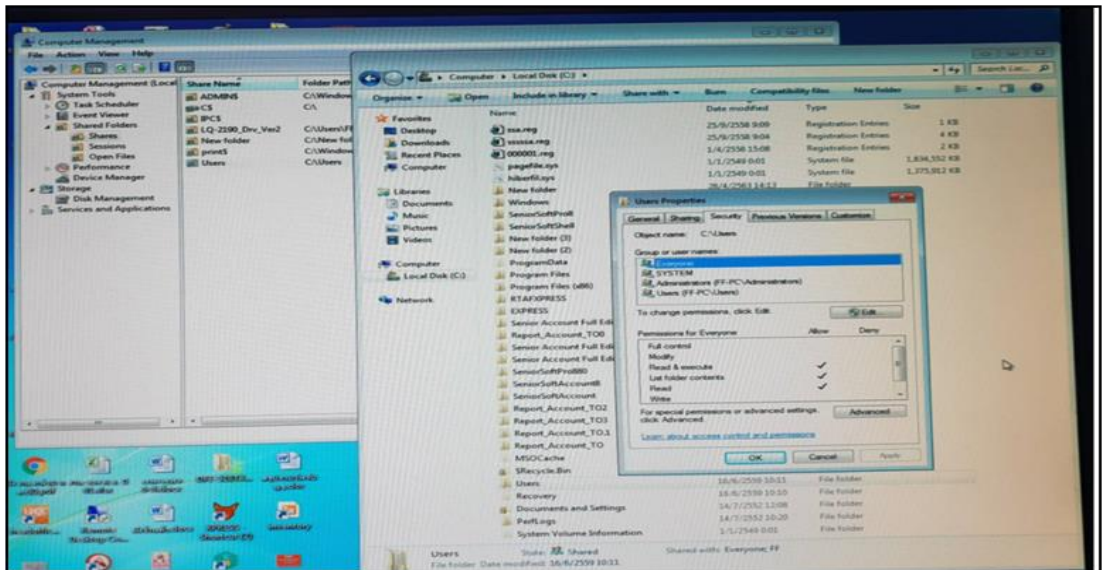
ภาพที่ ๑๒๘ Regedit

๖.๒.๔.๑ โปรแกรมตั้งเวลาทำงานอัตโนมัติ (Task Scheduler)



ภาพที่ ๑๒๙ โปรแกรมตั้งเวลาทำงานอัตโนมัติ

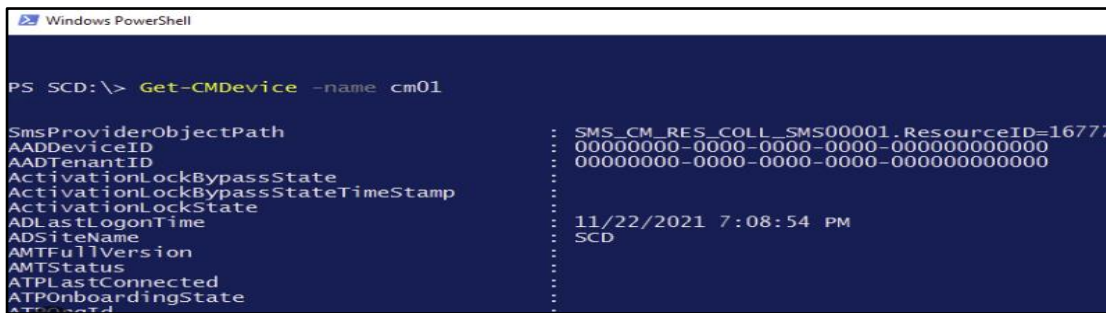
๖.๒.๔.๒ การตั้งค่า Firewall เพื่อเปิด - ปิด Port



ภาพที่ ๑๓๐ การตั้งค่า Firewall เพื่อเปิด - ปิด Port

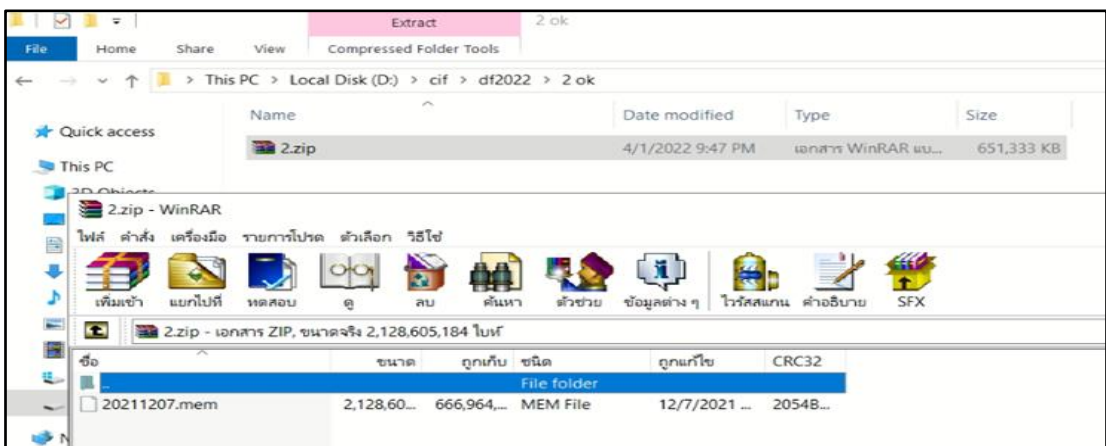
๖.๓ การวิเคราะห์ Malware Analysis

แบ่งออกเป็น ๓ ส่วน คือ การพิสูจน์ไฟล์, การรันไฟล์ และการวิเคราะห์เชิงลึกระดับฟังก์ชันของไฟล์ สำหรับการพิสูจน์ไฟล์สามารถทำได้หลายวิธี มัลแวร์เองก็มีที่มาจากหลายแหล่ง ในที่นี้ขอยกตัวอย่าง มัลแวร์ที่มีการซ่อนตัวอยู่ใน Ram ซึ่งไม่สามารถตรวจหรือค้นหาจากเครื่องคอมพิวเตอร์ได้ เนื่องจากไม่มีการสร้างไฟล์ใด ๆ ไว้ในระบบ ซึ่งส่วนมากจะอาศัยสคริปต์ของโปรแกรม Powershell ในการรันตัวเอง สำหรับกระบวนการวิเคราะห์จะเริ่มจากนำไฟล์ Ram ที่เก็บมาได้มาทำการแตก Zip ออกก่อน ดังภาพที่ ๑๒๑



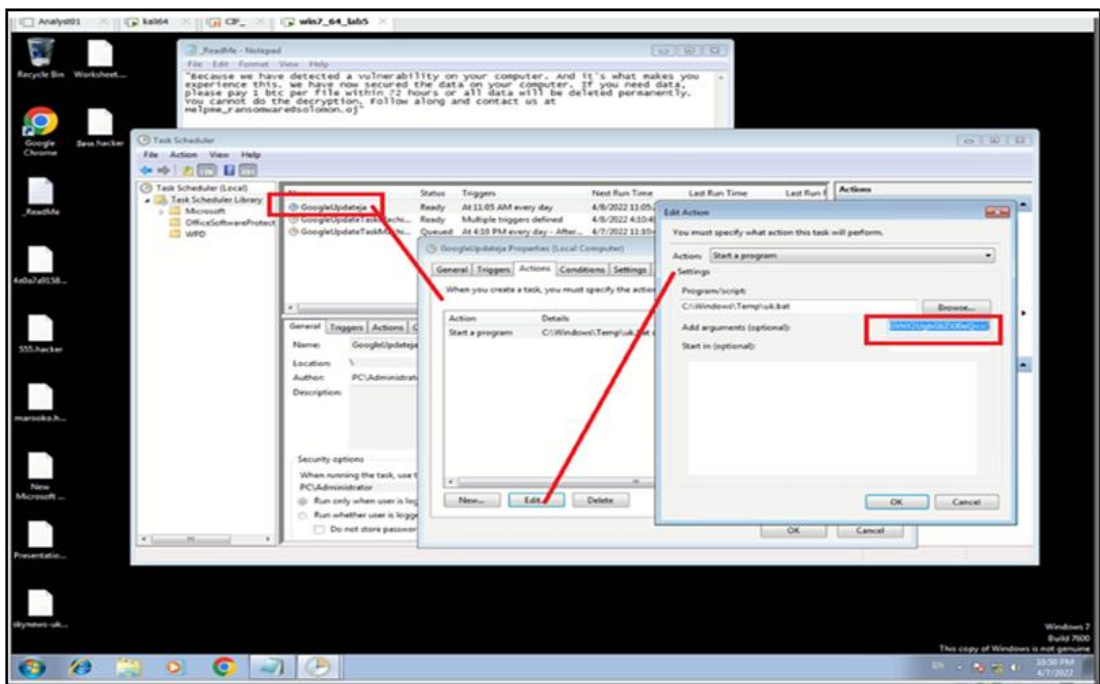
ภาพที่ ๑๓๑ โปรแกรม Powershell

ทำการอัปโหลดไฟล์ 20211207.mem เข้า Kali เพื่อใช้โปรแกรม Volatility ในการวิเคราะห์ ซึ่งมีอยู่ในระบบปฏิบัติการ Kali Linux เปิด Terminal จากนั้นพิมพ์คำสั่ง imageinfo เพื่อเตรียมพร้อมระบบ ก่อนทำการวิเคราะห์ข้อมูล จากนั้นใช้คำสั่ง #>volatility-f 20211207.mem - profile=Win7SP1x86 เพื่อค้นหาว่ามีการรันไฟล์อะไรต้องสงสัยผ่าน โพรเซสใด ๆ ในระบบหรือไม่ แล้วเราจะพบว่า โพรเซส powershell.exe หมายเลข PID 2848 มีการดาวน์โหลดไฟล์บางอย่างที่น่าสงสัยจากเว็บไซต์ภายนอก เมื่อกดคลิ๊กเข้าไปเราจะสามารถ ดาวน์โหลดไฟล์บางอย่างมาได้ โดยมีลักษณะเป็นไฟล์รูปภาพที่ชื่อ d.png ดังภาพที่ ๑๒๑



ภาพที่ ๑๓๒ โปรแกรม Volatility

จากนั้นทำการตรวจสอบไฟล์มัลแวร์เบื้องต้นด้วยเว็บไซต์ Virustotal.com อีกตัวอย่างหนึ่งคือ การวิเคราะห์มัลแวร์เรียกค่าไถ่ โดยผู้ใช้งานแจ้งมาว่าไฟล์ต่าง ๆ ที่เก็บไว้ที่หน้าจอของเครื่องถูกเปลี่ยนนามสกุล และจะสังเกตได้ว่าไฟล์ต่าง ๆ ที่หน้าจอถูกเปลี่ยนนามสกุลเป็น .hacker ทั้งหมด พร้อมกับมีไฟล์เรียกค่าไถ่ที่ชื่อ ReadMe.txt ถ้าเราเปลี่ยนเป็นนามสกุลอื่น ๆ อีกประมาณ ๕ นาที มันก็จะกลับมาเป็นเหมือนเดิมอีก แสดงว่าต้องมีโปรแกรมบางอย่างที่คอยเปลี่ยนนามสกุลของไฟล์เหล่านี้ อย่างมีช่วงเวลา ซึ่งใน Windows จะมีโปรแกรมหนึ่งที่ทำหน้าที่ตั้งเวลาการรันโปรแกรมได้ และมักถูกใช้ตั้งเวลาโจมตี นั่นคือโปรแกรม Task Scheduler ซึ่งจะต้องไปตรวจสอบ และพบว่า มีชื่อของคำสั่งหนึ่งที่ผิดปกติ คือ GoogleUpdateja จากการตรวจสอบรายละเอียด จะพบว่าโปรแกรมถูกรันไฟล์มัลแวร์ที่ชื่อ uk.bat ทุก ๆ ๕ นาที ดังภาพที่ ๑๒๒

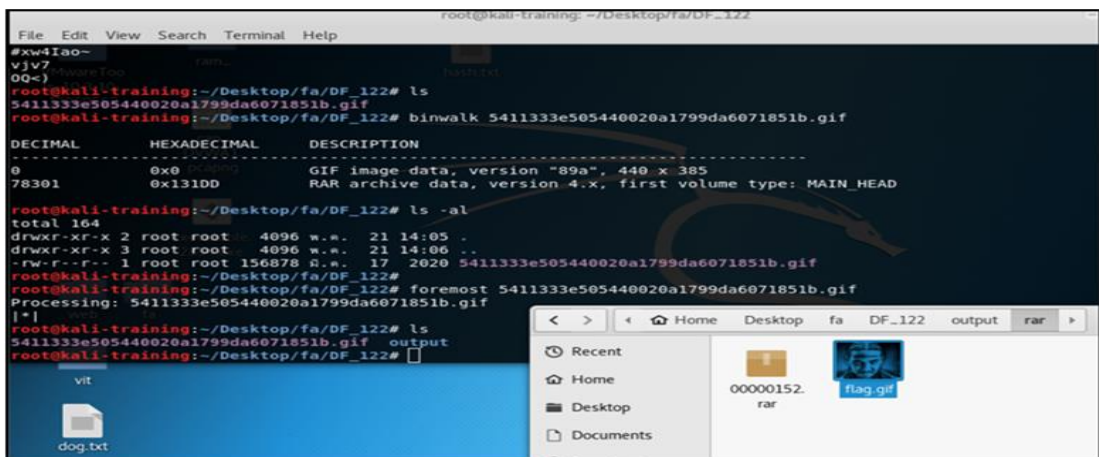


ภาพที่ ๑๒๓ การตรวจสอบไฟล์มัลแวร์เบื้องต้น

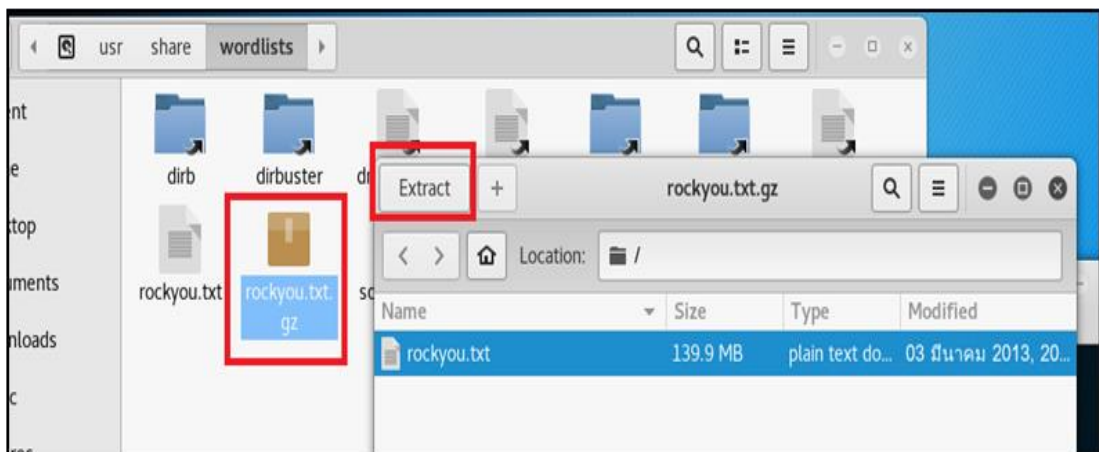
๖.๓.๑ การวิเคราะห์ผ่านโปรแกรม Deep Instinct ซึ่งเป็นโปรแกรมแอนตี้ไวรัสด้วยปัญญาประดิษฐ์ มีความสามารถในการวิเคราะห์ และให้ค่าความน่าจะเป็นของภัยคุกคามที่ตรวจพบทาง ทอ.ได้ดำเนินการติดตั้งโปรแกรมดังกล่าวบนเครื่องคอมพิวเตอร์เพื่อป้องกันมัลแวร์จากอินเทอร์เน็ต และยังถูกใช้เป็นส่วนหนึ่งของระบบตรวจสอบและรายงานผลมายังส่วนกลางเพื่อใช้วิเคราะห์ภัยคุกคามบนเครื่องผู้ใช้งาน เมื่อนำมาใช้ในงาน Forensic โปรแกรม Deep Instinct จะสามารถให้ข้อมูลของไฟล์ที่มีการติดมัลแวร์ และพฤติกรรมอำพรางตัวด้วยการเปลี่ยนแปลงตัวเองตลอดเวลาสำหรับผู้ดูแลระบบ สามารถสั่ง Scan ไวรัส สั่ง Block ไฟล์ที่เป็นอันตราย ตัดการเชื่อมต่ออินเทอร์เน็ต รวมถึงทราบหมายเลข IP Address ของเครื่องได้ ทั้งนี้ในองค์กรขนาดใหญ่จะใช้ระบบจ่ายหมายเลข

๖.๓.๓ การระบุรูปแบบไฟล์ เราอาจคิดว่าทำไมต้องระบุในเมื่อเห็นอยู่แล้วว่าเป็นไฟล์นามสกุลอะไร แต่อย่าลืมว่าไฟล์เครื่องคอมพิวเตอร์สามารถถูกเปลี่ยนแปลงหรือแก้ไขได้ และ แฮกเกอร์ก็มักจะเลือกใช้วิธีดังกล่าว เพื่อจะซ่อนไฟล์หรือบายพาสระบบเพื่อให้สามารถผ่านฟังก์ชันการตรวจสอบนามสกุลไฟล์เมื่อดาวนโหลดไฟล์เข้ามาในระบบ ดังนั้นการทำ Forensics เพื่อหาว่ารูปแบบไฟล์เดิมนั้นเป็นอะไร จึงมีความจำเป็น และในการแข่งขัน CTF ส่วนมากนิยมใช้คำสั่งเหล่านี้ในการหาคำตอบซึ่งก็รวดเร็วมาก เช่น คำสั่ง mdls ใน MacOS หรือ libmagic ในระบบ UNIX และถ้าเป็นใน Linux เราก็จะใช้คำสั่งว่า File เป็นต้น

๖.๓.๔ การแตกไฟล์เชิงลึก เป็นกระบวนการเพื่อแยกส่วนประกอบของไฟล์ออกมา คล้ายกับการ Unzip แต่จะแตกต่างกันตรงที่สามารถถอดรหัสไฟล์ที่ไม่ทราบมาก่อนได้ด้วย (ส่วนใหญ่) และสามารถหาข้อมูลที่ถูกซ่อนอยู่ในไฟล์ได้อีกด้วย โดยมีอยู่ ๒ คำสั่งที่นิยมใช้ คือ binwalk -e แล้วตามด้วยชื่อไฟล์ เพื่อหาข้อมูลเบื้องต้นเกี่ยวกับไฟล์รูปภาพ และ คำสั่ง foremost เป็นคำสั่งที่ใช้สำหรับแตกไฟล์ที่ซ่อนอยู่ออกมา

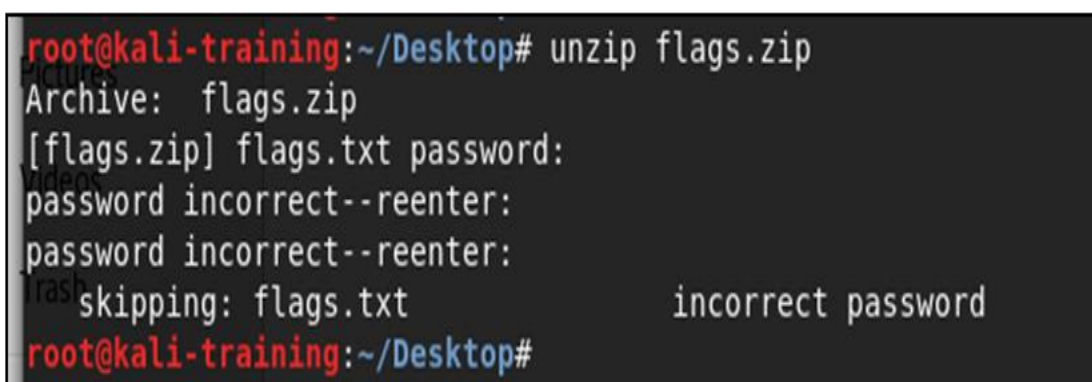


ภาพที่ ๑๓๖ คำสั่ง foremost & binwork



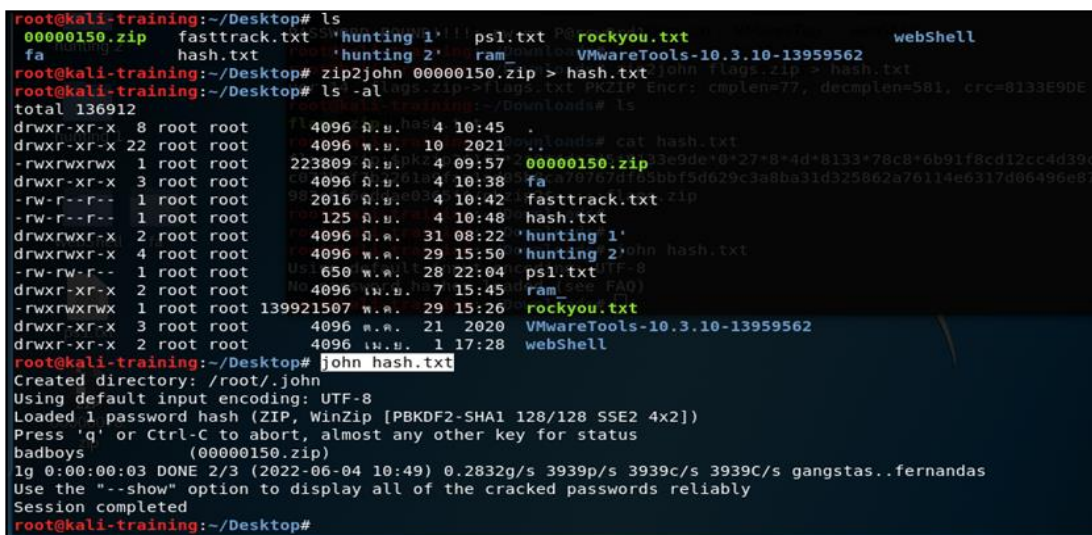
ภาพที่ ๑๓๗ คำสั่งเกี่ยวกับไฟล์ zip

Unzip เปิดไฟล์ หรือคลายไฟล์ กรณี .gz ให้ใช้คำสั่ง `gzip -d` ตามด้วยชื่อไฟล์ Details -v จะให้ข้อมูลเชิงลึกเกี่ยวกับค่าที่มีอยู่ในฟิลด์ต่าง ๆ ของรูปแบบข้อมูล zipinfo แสดงรายการข้อมูลเกี่ยวกับเนื้อหาของไฟล์ zip โดยไม่ต้องแตกไฟล์ `zip -F input.zip --out output.zip` และ `zip -FF input.zip --out output.zip` พยายามซ่อมแซมไฟล์ zip ที่เสียหาย `fcrackzip brute-force` สุ่มเดาหัดผ่าน zip (สำหรับรหัสผ่านที่ไม่เกิน ๗ อักขระ) ก่อนอื่นต้องติดตั้งโปรแกรมประเภท Dictionary สำหรับการทำให้ Brute-Force ในโปรแกรมทดสอบความปลอดภัยระบบ เช่น Kali Linux จะเก็บไฟล์สำหรับใช้ Brute-Force ไว้ที่ `/usr/share/wordlists/` ไฟล์ชื่อว่า `rockyou.txt.gz` ซึ่งต้องทำการแตกไฟล์ออกมา ก่อน ด้วยการดับเบิลคลิกที่ไฟล์ แล้วเลือก Extract ดังภาพที่ ๒๓๗



ภาพที่ ๑๓๘ rockyou.txt.gz

จากนั้นก็ทำการคัดลอกไฟล์มาวางไว้กับไฟล์ที่จะทำการ Brute-Force แล้วใช้คำสั่ง `#> facrackzip -u -D -p /ที่อยู่ของไฟล์/rockyou.txt` ชื่อไฟล์ที่ต้องการ Brute-Force.zip หรือจะใช้คำสั่ง `zip2john` ก็ได้ เช่น `#> zip2john abc.zip > hash.txt, #> john hash.txt` เป็นต้น



ภาพที่ ๑๓๙ Brute-Force

บทที่ ๗ การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน

ในการวิเคราะห์หลักฐานทางดิจิทัล บางครั้งทีมงานที่ทำการวิเคราะห์ก็อาจจะไม่สามารถทำการวิเคราะห์ได้เนื่องจากขาดประสบการณ์ จึงต้องมีการส่งมอบหลักฐานให้กับหน่วยงานหรือองค์กรที่มีศักยภาพสูงขึ้นถัดไปในการดำเนินการ สำหรับ ศชบ.ทอ. หากไม่สามารถดำเนินการได้ จะทำการส่งมอบหลักฐานให้กับ บก.ทท.ต่อไป โดยในกระบวนการถ่ายโอนหลักฐานจะต้องมีการทำเอกสารตาม “แบบฟอร์มควบคุมหลักฐาน” ที่มีการกำหนดอย่างชัดเจนว่าหลักฐานถูกส่งมอบโดยใคร เมื่อไหร่ ดังภาพที่ ๑๒๙ - ๑๓๐

ส่วนพิสูจน์หลักฐาน สทฐ.ภรช.ศชบ.ทอ.

แบบฟอร์มควบคุมหลักฐาน

หมายเลขเหตุการณ์ : _____ รูปแบบการโจมตี : _____
 เจ้าหน้าที่ตรวจพิสูจน์หลักฐาน : (ชื่อ-สกุล / รหัสประจำตัว) _____
 ชื่อผู้เสียหาย : _____ User: _____ Password: _____
 ชื่อผู้ต้องสงสัย : _____ User: _____ Password: _____
 วันที่/เวลา เก็บหลักฐาน : _____ สถานที่เกิดเหตุ : _____
 เก็บหลักฐานทั่วไป เก็บหลักฐานมืออาหาล

รายละเอียดของพยานหลักฐาน		
ลำดับที่	จำนวน	คำอธิบาย (รุ่น, หมายเลขเครื่อง, สภาพ, รอยขีดข่วน)

แบบฟอร์มการรับ - จัดเก็บหลักฐาน				
ลำดับที่	วันที่ / เวลา	ผู้นำเข้าหลักฐาน (ลายมือชื่อ & รหัสประจำตัว)	ผู้นำเข้าหลักฐาน (ลายมือชื่อ & รหัสประจำตัว)	หมายเหตุ / สถานที่เก็บ

|
หน้า 1 ใน ๒ หน้า

ภาพที่ ๑๔๐ แบบฟอร์มควบคุมหลักฐาน

ส่วนพิสูจน์หลักฐาน ผพฐ.กรจ.คชบ.ทอ.

แบบฟอร์มควบคุมหลักฐาน

แบบฟอร์มการรับ - ส่งหลักฐาน				
ลำดับที่	วันที่ / เวลา	ผู้นำเข้าหลักฐาน (ลายมือชื่อ & รหัสประจำตัว)	ผู้นำเข้าหลักฐาน (ลายมือชื่อ & รหัสประจำตัว)	หมายเหตุ / สถานที่ส่ง

แบบฟอร์มการส่งคืน - ทำลายหลักฐาน

แบบฟอร์มการส่งคืนหลักฐาน
ลำดับที่ #: _____ เป็นเอกสารที่มีความเกี่ยวข้องกับ (ผู้ต้องสงสัย):
หลักฐานชิ้นนี้เป็นหลักฐานที่ดำเนินคดีเสร็จสิ้นแล้ว ต้องการที่จะ ส่งคืนเจ้าของ ทำลายทั้ง
ชื่อ & รหัสประจำตัว # ของเจ้าของหลักฐาน : _____ ลายมือชื่อ : _____
วันที่ : _____

แบบฟอร์มการทำลายหลักฐาน
ลำดับที่ #: _____ เป็นหลักฐานที่ต้องทำลายโดย (เจ้าหน้าที่ทำลายหลักฐาน) _____
หมายเลขประจำตัว #: _____ วันที่ : _____
ชื่อ-นามสกุล & หมายเลขประจำตัว # ของผู้สังเกตการณ์ : _____ ลายมือชื่อ : _____
วันที่ : _____

หน้า 2 ใน 2 หน้า

ภาพที่ ๑๔๑ แบบฟอร์มการรับ - ส่งหลักฐาน

๗.๑ กระบวนการจัดเก็บหลักฐาน

นอกจากจะต้องมีการบันทึกเป็นเอกสารดังที่ได้กล่าวมาแล้ว หลักฐานที่ยังไม่ได้รับการส่งมอบให้เจ้าของ หรืออยู่ระหว่างดำเนินการวิเคราะห์จะต้องถูกเก็บให้ปลอดภัย เพื่อป้องกันไม่ให้อาณาหลักฐานเกิดความเสียหายระหว่างดำเนินการจัดเก็บ และในกรณีที่มีหลักฐานจำนวนมาก ก็จะสามารถค้นหาและบริหารจัดการหลักฐานให้เป็นระเบียบได้อีกด้วย ดังนั้นการมีห้องสำหรับเก็บหลักฐานที่สามารถมองเห็นได้จากภายนอก มีระบบกล้องวงจรปิดเพื่อแสดงให้เห็นถึงกระบวนการจัดเก็บที่ชัดเจน เมื่อมีการดำเนินคดีในชั้นศาล ทางที่วิเคราะห์หลักฐานก็จะสามารถใช้เป็นหลักฐานยืนยันความบริสุทธิ์ของตนเอง



ภาพที่ ๑๔๒ ตัวอย่างห้องเก็บพยานหลักฐาน

๗.๒ การเก็บรักษา การถ่ายโอน และการส่งมอบหลักฐาน

การควบคุมพยานหลักฐาน เป็นกระบวนการที่ต้องควบคุมหลักฐานไม่ให้ถูกแก้ไขหรือเปลี่ยนแปลง รวมทั้งเป็นการยืนยันว่าการได้มาซึ่งหลักฐานนั้น ผู้ทำการวิเคราะห์ไม่ได้ทำการเปลี่ยนแปลงหรือทำให้ทรัพย์สินอันเป็นหลักฐานนั้นเสียหายจากการพิสูจน์หลักฐาน ทั้งจะมีประโยชน์ในการสร้างความน่าเชื่อถือในชั้นศาลด้วย โดยกระบวนการจะใช้เอกสารในการควบคุมและกำกับการทำงาน เช่น มีการบันทึกการรับมอบหลักฐาน ระบุวันเวลา ชื่อผู้ส่ง ชื่อผู้รับ วัสดุที่ใช้ในการเก็บ ต้องไม่ทำให้หลักฐานเสียหายหรือถูกเปลี่ยนแปลง สถานที่เก็บต้องถูกควบคุม ไม่เป็นที่อัปชื้น หรือร้อนเกินไป มีกล่องวงจรปิดเพื่อตรวจสอบการเข้าออก มีระบบรักษาความปลอดภัยที่เหมาะสมและมีถึงดับเพลิง รวมทั้งมีแผนเผชิญเหตุที่สามารถเคลื่อนย้ายพยานหลักฐานได้เมื่อเกิดเหตุจำเป็นที่ต้องเคลื่อนย้าย

๗.๓ กระบวนการส่งคืนหลักฐาน

หลังจากที่ทีมงานวิเคราะห์ดำเนินการวิเคราะห์หลักฐานเสร็จแล้ว จะต้องนำหลักฐานส่งคืนให้กับเจ้าของ เพื่อใช้เป็นหลักฐานและจะต้องมีการเซ็นรับหลักฐาน หรือมีการถ่ายภาพเอาไว้ด้วย เพื่อป้องกันกรณีบุคคลแอบอ้างมารับหลักฐานไป ทั้งนี้หลักฐานที่จะส่งคืนจะต้องไม่เสียหายด้วยเหตุจากกระบวนการวิเคราะห์หลักฐาน ซึ่งกระบวนการวิเคราะห์หลักฐานจะไม่ยุ่งเกี่ยวกับหลักฐานจริง แต่จะใช้สำเนาของพยานหลักฐาน ในการวิเคราะห์แทน โดยแทนค่าความเที่ยงตรงของข้อมูลด้วยการทำ Hash ไฟล์หลักฐาน

บทที่ ๘ การออกรายงานผลการวิเคราะห์

รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์ คือ รายละเอียดของข้อมูลบน Complete Forensic Investigation Process ซึ่งสามารถเตรียมการโดยการตรวจพิสูจน์นิติคอมพิวเตอร์ การตรวจพิสูจน์นิติคอมพิวเตอร์ได้มีการเก็บข้อมูลที่เกี่ยวข้องกับเหตุการณ์ การสืบสวนสอบสวน และเตรียมการสำหรับรายงานฉบับสมบูรณ์ โดยสามารถเปิดเผยผลการตรวจพิสูจน์นิติคอมพิวเตอร์ ซึ่งไม่ใช่แค่การนำเสนอข้อเท็จจริง แต่เป็นการสื่อสารความคิดเห็นของผู้เชี่ยวชาญด้วยคุณลักษณะของรายงานที่ดี

๘.๑ รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์

คุณสมบัติของรายงานที่ดี มีดังนี้

๘.๑.๑ การกำหนดรายละเอียดของเหตุการณ์อย่างถูกต้อง

๘.๑.๒ ชัดเจนและเข้าใจง่ายในการตัดสินใจ

๘.๑.๓ สามารถใช้ในทางกฎหมายได้

๘.๑.๔ ไม่เกิดความซับซ้อน

๘.๑.๕ สามารถใช้ในการอ้างอิงได้

๘.๑.๖ สรุปข้อมูลเพื่อนำมาจัดทำเป็นรายงาน


๘.๑.๗ สามารถจัดทำได้ตามเวลาที่กำหนดไว้

๘.๑.๘ การจัดทำเอกสารรายงานการตรวจพิสูจน์

๘.๑.๙ การเก็บบันทึกและให้ข้อมูล เพื่อนำไปใช้ในการจัดทำเอกสาร รายงาน จำเป็นต้องมีรายละเอียด เช่น วันที่และเวลาของหลักฐาน, วันที่และเวลาปัจจุบัน, เวลาที่วิเคราะห์เสร็จสิ้น สิ่งที่พบจากการสอบสวน, เทคนิคพิเศษนอกเหนือจากกระบวนการปกติ, แหล่งข้อมูลภายนอกที่ช่วยในการค้นหาหลักฐาน และได้รับการอบรมหลักสูตร Computer Crime Investigators และแนวปฏิบัติที่ดีสำหรับผู้ตรวจพิสูจน์ เป็นต้น ผู้มีส่วนเกี่ยวข้องท่านใหม่สามารถเข้าใจในเนื้อหาของรายงานได้ ตรวจสอบให้แน่ใจ ว่ารายงานมีความสอดคล้องกับคำสั่งที่ได้รับ ขณะมีการแก้ไขรายงาน ต้องมั่นใจว่าหลักฐานไม่มีความซับซ้อน และนำเสนออย่างถูกต้องและเหมาะสม ทบทวนรายงานอีกครั้งก่อนดำเนินการส่งรายงาน กล่าวคือ การจัดทำรายงานการตรวจพิสูจน์นิติคอมพิวเตอร์นั้น ต้องมีรายละเอียดที่ครบถ้วนและสมบูรณ์ รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์ที่ดีควรมีความเข้าใจง่าย ชัดเจน สามารถนำไปใช้ในทางกฎหมายได้ ไม่มีความซับซ้อน อ้างอิงแหล่งที่มาได้ และจัดส่งได้ตามเวลาที่กำหนด

๘.๑.๑๐ สำหรับการออกรายงานของ ศชบ.ทอ. จะประกอบด้วย ๒ ส่วนใหญ่ ๆ คือ เอกสารหลัก และเอกสารแนบ โดยเอกสารหลักจะเป็นแบบฟอร์มหนังสือราชการ ที่จะกล่าวถึงสาเหตุที่มาของเหตุการณ์ที่จะต้องดำเนินการ Forensic รวมถึงรายละเอียดโดยย่อของเหตุการณ์

และผลการวิเคราะห์ที่ได้ พร้อมสรุปแนวทางแก้ไขโดยย่อ นำเรียน ผู้บังคับบัญชาเพื่อพิจารณา ดำเนินการต่อไป ดังภาพที่ ๑๓๒



สำเนาฉบับ บันทึกข้อความ

ส่วนราชการ ศทบ.ทอ.(กรมโทรคมนาคม)

ที่ กท ๑๒๕๐๑๗ **วันที่** ๓๐.๑๒.๒๕๖๒

เรื่อง รายงานผลการตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

เลขที่ ศทบ.ทอ.

๑. ศทบ.ทอ. ได้ตรวจพบกิจกรรมซึ่งเกินอันตรายจากโปรแกรม Security Onion ว่าเครื่องคอมพิวเตอร์หมายเลข IP: 10.235.232.44 ของ ผกท.ศทก.ทอ. มีการเชื่อมต่อไปยังระบบคอมพิวเตอร์ภายนอกเครือข่าย ทอ. ที่มีความอันตราย เมื่อ ๒๖๗ ๕.๓.๖๕ นั้น

๒. ศทบ.ทอ. ตรวจสอบแล้วมีข้อมูล ดังนี้

๒.๑. เก็บหลักฐานที่ ผกท.ศทก.ทอ. เก็บไฟล์ข้อมูลทั้งหมดของเครื่องคอมพิวเตอร์ ที่เกิดเหตุเพื่อทำการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics : DF) โดยมีผลการตรวจพบ ดังนี้ (ตามแนบ)

๒.๑.๑ พบการมีตัวขูดค่าสปีดในโปรแกรมตั้งค่าเวลาของเครื่องคอมพิวเตอร์

๒.๑.๒ พบไฟล์ที่ชื่อสงสัยชื่อ offload

๒.๒ จากการตรวจสอบเป็นการโจมตีผ่านช่องโหว่ของระบบปฏิบัติการ Windows 7 โดยพบการส่งไฟล์ชื่อ offload เข้ามาภายในเครื่องคอมพิวเตอร์ ซึ่งเก็บไฟล์จากเว็บไซต์ที่มีความเกี่ยวข้องกับ Trojan Andromeda และพบการตั้งขูดค่าสปีดทำงานทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มกระบวนการทำงาน โดยเก็บไฟล์ขูดค่าสปีดของ Trojan.Lennon Duck ส่งผลให้มีการเชื่อมต่อไปยังเว็บไซต์อันตรายภายนอก ศทบ.ทอ. ได้ดำเนินการลบขูดค่าสปีดดังกล่าวออกจากระบบคอมพิวเตอร์เรียบร้อยแล้ว

๓. ศทบ.ทอ. พิจารณาแล้ว เพื่อเป็นการป้องกันการแพร่กระจายจากการโจมตีไปยังเครื่องคอมพิวเตอร์ภายใน ศทบ.ทอ. และเกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศของ ทอ. เห็นควรให้ผู้รับผิดชอบและผู้ใช้งานดำเนินการในส่วนที่เกี่ยวข้อง ดังนี้

๓.๑. ดำเนินการตรวจสอบและคำขอข้อมูลของเครื่องคอมพิวเตอร์อื่น ๆ ภายในที่กตทท

๓.๒. ดำเนินการติดตั้งระบบปฏิบัติการเวอร์ชันล่าสุด และถูกต้องตามลิขสิทธิ์

๓.๓. ติดตั้งโปรแกรมป้องกันไวรัส Deep insight โดยสามารถประสานการติดตั้งและการใช้งานได้จาก ศทบ.ทอ. หากมีข้อสงสัยสามารถติดต่อ ศทบ.ทอ. โทร.๒๖๗๕๐๐๐

จึงเรียนมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต.
ธอ.ศทบ.ทอ.

3.ท. 3.ท.
 3.ท. 3.ท.
 3.ท. 3.ท.
 3.ท. 3.ท.

ภาพที่ ๑๔๓ ตัวอย่างรายงานผลการตรวจพิสูจน์หลักฐานทางดิจิทัล

๘.๒ ข้อมูลเบื้องต้น

ข้อมูลเบื้องต้น เป็นการกล่าวถึงรายละเอียดที่ได้รวบรวมหรือไปเก็บหลักฐานแล้วเอามาบรรยายถึงพฤติกรรมและสาเหตุที่ทำให้เกิดปัญหา พร้อมทั้งมีแผนภาพแสดงพฤติกรรมการโจมตีให้ด้วย โดยอาจมีหัวข้อย่อย ๆ ภายในเพื่ออธิบายรายละเอียดของเหตุการณ์อื่น ๆ ที่มีมากกว่า ๑ เหตุการณ์ และอีกส่วนหนึ่งคือ เอกสารแนบจะเป็นรายงานที่ลงรายละเอียดรวมถึงแสดงกระบวนการวิเคราะห์ โดยมีหัวข้อเนื้อหาหลัก ๆ ทั้งหมด ๔ ข้อ ประกอบด้วย

๘.๒.๑ ตรวจสอบหลักฐานและความเสียหาย เป็นการอธิบายกระบวนการทำงานตาม Chain of Custody และเครื่องมือที่ใช้ในการวิเคราะห์หลักฐาน

๘.๒.๒ ช่องทางการโจมตี จะเป็นการกล่าวถึงช่องทางต่าง ๆ ที่ได้ตรวจพบจากข้อมูล Logs หรือข้อมูลผลการวิเคราะห์ด้านอื่น ๆ อันจะเป็นการอธิบายให้ทราบถึงสาเหตุของการเกิดเหตุการณ์โจมตีทางไซเบอร์

๘.๒.๓ การแพร่กระจาย เป็นการรายงานเกี่ยวกับพฤติกรรมการแพร่กระจายของมัลแวร์ หรือภัยคุกคามที่ได้ทำการวิเคราะห์ผล ซึ่งจะช่วยให้ผู้รับรายงานสามารถจำกัดขอบเขตความเสียหายได้ พร้อมทั้งเตรียมแผนรับมือหากเกิดเหตุการณ์โจมตีขึ้นอีก

๘.๒.๔ สรุปและข้อเสนอแนะ เป็นการกล่าวถึงเนื้อหาทั้งหมดโดยสรุปอีกครั้งพร้อมแนะนำแนวทางแก้ไขให้กับหน่วยงานที่เกิดเหตุ โดยอาจแนะนำวิธีการหรือช่องทางในการดำเนินการแก้ไขให้บรรเทาได้ ทั้งนี้เป็นหน้าที่ของเจ้าของระบบที่จะดำเนินการแก้ไข โดย ศชบ.ทอ.จะสนับสนุนด้านบุคลากรและเทคนิคในการแก้ไขปัญหา พร้อมแนบเบอร์ติดต่อกรณีที่มีข้อสงสัยต้องการซักถามและลงชื่อผู้ทำการวิเคราะห์ไว้ด้วย

นิยามคำศัพท์ที่เกี่ยวข้องกับงานด้าน Forensic Computer

Computer Forensic คือ การค้นหา และเก็บหลักฐานทางดิจิทัลที่อยู่ในอุปกรณ์คอมพิวเตอร์ เช่น ไฟล์ที่อยู่ใน พีซี โน้ตบุ๊ก หรือพีดีเอ เป็นต้น หรือหลักฐานดิจิทัลที่ถูกสร้างจากระบบคอมพิวเตอร์ เช่น บันทึกการใช้งานโทรศัพท์ และข้อมูลของการใช้อินเทอร์เน็ต เป็นต้น ซึ่งหลักฐานทั้งหมดนี้จะถูกนำมาวิเคราะห์ว่าหลักฐานนี้เกิดขึ้นเมื่อไหร่ เกิดจากอะไร ตอนนี้อยู่ทำอะไร และถูกใช้โดยใคร และการทำ Computer Forensic จะประกอบไปด้วย การเก็บหลักฐาน การพิสูจน์ความถูกต้องของหลักฐาน และการวิเคราะห์หลักฐานเพื่อนำเสนอในชั้นศาล แล้วแต่กรณี ซึ่งจะมีคำนิยามศัพท์ที่เกี่ยวข้องพอสังเขปเรียงตามลำดับอักษรภาษาอังกฤษ ดังนี้

(A)

analysis	การวิเคราะห์
authentication systems	ระบบการยืนยันบุคคลตัวจริง
authenticity verification	ความเป็นเจ้าของ
admissibility of Evidence	การรับฟังพยานหลักฐาน
automated fingerprint	ลายพิมพ์นิ้วมืออัตโนมัติ
authentication of Evidence	การยืนยันว่าเป็นพยานหลักฐานที่แท้จริง หรือการพิสูจน์ความถูกต้องของหลักฐาน
anti-Static Bag	ถุงป้องกันไฟฟ้าสถิต

(B)

backdoor	ในทางความมั่นคงของระบบคอมพิวเตอร์ช่องโหว่ของระบบรักษาความมั่นคง ที่ผู้ออกแบบหรือผู้ดูแลตั้งใจไว้โดยเป็นกลไกลับทางซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคง แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้
----------	---

(C)

case studies.	กรณีศึกษา
certificate Authority or CA	ผู้ประกอบการรับรองใบรับรองดิจิทัล คือ บุคคลที่สามที่น่าเชื่อถือ (Trusted third Party) ทำหน้าที่ออกใบรับรองดิจิทัล และทำหน้าที่ เจ้าหน้าที่ Passport ซึ่งมีหน้าที่ทวนสอบ (verifies) รูปพรรณ (identity) ของผู้ถือใบรับรอง (Certificate's Holder) ใบรับรองดิจิทัลทนต่อการถูกรบกวน (Tamper-Proof) และไม่สามารถทำปลอมได้
characteristics	ลักษณะ
civil law	กฎหมายแพ่ง
civil procedure law	กฎหมายวิธีพิจารณาความแพ่ง
collection	การเก็บรวบรวม

commission of a crime	การประกอบอาชญากรรม
comparative automated fingerprint	การตรวจเปรียบเทียบลายพิมพ์นิ้วมืออัตโนมัติ
compare evidence	เปรียบเทียบพยานหลักฐาน
computer fraud	การฉ้อโกงทางคอมพิวเตอร์
computer network systems	ระบบเครือข่ายคอมพิวเตอร์
computer security system	ระบบความปลอดภัยคอมพิวเตอร์
conclusion	การสรุปผล
connections	การควบคุมหน่วยงานในกระบวนการยุติธรรม
conviction	การลงโทษ
court	ศาล
crime	อาชญากรรม
crime analysis	การวิเคราะห์อาชญากรรม
crime patterns	รูปแบบอาชญากรรม
crime scene analysis	การวิเคราะห์ในสถานที่เกิดเหตุ
crime scene investigation	การตรวจสถานที่เกิดเหตุ
crime scene photography	การถ่ายภาพในสถานที่เกิดเหตุ
crime scene protection	การรักษาสถานที่เกิดเหตุ
crime scene reconstruction	การประมวลเหตุการณ์ในสถานที่เกิดเหตุ
crime scene search	การค้นหาในสถานที่เกิดเหตุ
criminal law	กฎหมายอาญา
criminal justice administration	การบริหารงานยุติธรรมทางอาญา
criminal procedures	กระบวนการทางอาญา
criminal procedure law	กฎหมายวิธีพิจารณาความอาญา
criminalistics	การพิสูจน์หลักฐาน
cryptographic system	ระบบการเข้ารหัส
compliance	การปฏิบัติตามกฎระเบียบข้อบังคับ และกฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความ ปลอดภัยขององค์กรอย่างถูกต้อง ได้ตามมาตรฐาน เช่น การปฏิบัติตามประกาศมาตรฐานการรักษาความปลอดภัย ในการประกอบธุรกรรมอิเล็กทรอนิกส์ โดยคณะกรรมการ ธุรกรรมอิเล็กทรอนิกส์และการจัดทำแผน เพื่อรองรับ พรบ. และพรฎ. ด้านความปลอดภัยทางอิเล็กทรอนิกส์ เป็นต้น
cloud	เซิร์ฟเวอร์ของผู้ให้บริการบนอินเทอร์เน็ต ซึ่งกระจายอยู่ ตามที่ต่าง ๆ ทั่วโลก จะให้พื้นที่กับผู้ใช้เพื่อเก็บข้อมูลต่าง ๆ ไว้บนเน็ต แล้วดึงมาใช้งานได้ในทุกอุปกรณ์และทุกเวลา

cybercrime อาชญากรรมทางไซเบอร์ คือ การกระทำผิดใด ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลายเปลี่ยนแปลง หรือขโมยข้อมูลต่าง ๆ รวมถึงระบบเครือข่ายที่ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต เพื่อแสวงหาผลประโยชน์อย่างผิดกฎหมายโดยทางตรงและทางอ้อม เป็นต้น

(D)

data mining	เหมืองข้อมูล
database system	ระบบฐานข้อมูล
data warehouse	คลังข้อมูล
deciphering indent	การอ่านรอยกดเขียน
detecting	สืบหา
determination	การตรวจหา
diagnosis	การวินิจฉัย
digital image processing	การประมวลผลภาพดิจิทัล
digital photography system	ระบบการถ่ายภาพดิจิทัล
dimensions	มิติ
document processing	การประมวลผลเอกสาร
data Forensic	การพิสูจน์หลักฐานข้อมูลซึ่งมักใช้แทนกันได้กับการพิสูจน์หลักฐานทางคอมพิวเตอร์เป็นการศึกษาข้อมูลดิจิทัลและวิธีการสร้างและใช้งานเพื่อการสอบสวน

(E)

electric circuits	วงจรไฟฟ้า
electromagnetic waves	คลื่นแม่เหล็กไฟฟ้า
electron microscope	กล้องจุลทรรศน์อิเล็กตรอน
emphasized	เน้น
erasure	การขูดลบ
estimation	การประมาณค่า
ethical	จริยธรรม
ethics	จริยธรรม
evaluation	การประเมิน
events	เหตุการณ์
events surrounding	เหตุการณ์แวดล้อม
evidence	หลักฐาน
evidence identification	พยานหลักฐาน

evidence, documentary	พยานเอกสาร
evidence Collection Form	บันทึกการยึดหลักฐาน
evidence preservation	การสงวนและรักษาวัตถุพยาน
evidence, Criminal	พยานหลักฐานในคดีอาญา
evidence, Expert	พยานหลักฐานจากผู้เชี่ยวชาญ
evidence in rebuttal	พยานหลักฐานเพื่อหักล้าง
examination of handwriting	การตรวจพิสูจน์ลายมือ
expert witness	พยานผู้ชำนาญการ
expert witness in court	พยานผู้ชำนาญการในชั้นศาล
exploratory	เชิงการตรวจสอบ
exploratory data analysis	การวิเคราะห์ข้อมูลเชิงการตรวจสอบ
	(F)
financial fraud	การทุจริตทางการบัญชี
fingerprint	ลายพิมพ์นิ้วมือ
fingerprint	ลายนิ้วมือ
forecasting of crime patterns	การพยากรณ์รูปแบบอาชญากรรม
forensic accounting	การบัญชีทางนิติวิทยาศาสตร์
forensic finance	การเงินทางนิติวิทยาศาสตร์
forensic science	นิติวิทยาศาสตร์
forensic science history	ประวัตินิติวิทยาศาสตร์
forensic scientists	นักนิติวิทยาศาสตร์
forgery	การปลอมแปลงเอกสาร
forgery detection	การตรวจการปลอมแปลง
foundations	กระบวนการ
fraud	การฉ้อโกง
fraud examination techniques	เทคนิคการตรวจสอบการทุจริต
fundamental biometric systems	ระบบไบโอเมตริกซ์เบื้องต้น
fundamentals of fingerprint	ความรู้พื้นฐานของลายพิมพ์นิ้วมือ
forensic Duplicator	ชุดทำสำเนาข้อมูล
faraday Bag	ถุงป้องกันคลื่นแม่เหล็กไฟฟ้า
forensic Artifact	ข้อมูลใด ๆ ที่อยู่ในสื่อบันทึก หรือร่องรอยทางกายภาพใด ๆ ที่เกิดจากการปฏิสัมพันธ์ระหว่างสิ่งสองสิ่งและสามารถ ใช้ในการประกอบการทำนิติวิทยาศาสตร์เพื่อพิสูจน์ ข้อเท็จจริงหรือหาความกระจ่างให้กับเรื่องที่กำลังสนใจอยู่ได้

(G)

gather รวบรวม

(H)

handwriting ลายมือเขียนข้อความ

hot spots พื้นที่เสี่ยงภัย

hypotheses สมมติฐาน

hypotheses testing การทดสอบสมมติฐาน

(I)

identification การตรวจพิสูจน์

identification of individual การพิสูจน์เอกลักษณ์บุคคล

image attribute การใช้ภาพอ้างอิง

image capture devices อุปกรณ์ในการจับภาพ

image enhancements การทำภาพให้ชัดเจน

indented impressions การตรวจอ่านรอยกดบนกระดาษ

indexing การทำดรรชนี

individual project โครงการศึกษารายบุคคล

information systems ระบบสารสนเทศ

information technology เทคโนโลยีสารสนเทศ

information technology security ความปลอดภัยของเทคโนโลยีสารสนเทศ

information technology security laws กฎหมายเกี่ยวกับความปลอดภัยของเทคโนโลยีสารสนเทศ

integrity ความเป็นหนึ่งเดียว

internet อินเทอร์เน็ต

internet Crime อาชญากรรมทางอินเทอร์เน็ต

interpretation of results การแปลผล

investigation การสืบสวน

investigation techniques เทคนิคการสืบสวน

(L)

laboratory ห้องปฏิบัติการ

latent fingerprint from evidence การเก็บลายพิมพ์นิ้วมือแฝงจากพยานหลักฐาน

laws กฎหมาย

legal เชิงนิติศาสตร์

linking the suspect document การเชื่อมโยงเอกสารพิรุธ

(M)

management การจัดการ

manners พฤติการณ์

mapping crime investigation การทำแผนที่ในการสืบสวนทางอาชญากรรม

method	วิธี
models	แบบจำลอง
motion	การเคลื่อนที่
memory Dump Tool	เครื่องมือทำสำเนาหน่วยความจำ
mobile Phone Forensics Tool	เครื่องมือตรวจวิเคราะห์โทรศัพท์เคลื่อนที่
malware (malicious software)	ไวรัส หนอนอินเทอร์เน็ต และโทรจันที่มีพฤติกรรม รบกวนและสร้างความเสียหายแก่ระบบเครื่องคอมพิวเตอร์
(N)	
network Security Officer	เจ้าหน้าที่รักษาความปลอดภัยเครือข่าย ผู้ซึ่งได้รับ มอบหมาย อย่างเป็นทางการจากผู้ซึ่งมีอำนาจหน้าที่ให้มีการปฏิบัติ อย่างถูกต้องในเรื่องที่เกี่ยวข้องภายในระบบข้อมูลอัตโนมัติ เป็นภัยคุกคามที่ใช้เล่ห์กลต่าง ๆ เพื่อให้เราเปิดเผยข้อมูล
nontechnical attack social engineering	
network systems	ระบบเครือข่าย
network security	ความปลอดภัยของเครือข่าย
Net	(เน็ต) มาจากคำว่า อินเทอร์เน็ต (Internet) คือ ระบบเครือข่าย ขนาดใหญ่ที่เชื่อมโยงกันทั่วโลก เมื่ออุปกรณ์ต่าง ๆ เชื่อมต่อ เข้ามาใน ระบบเครือข่ายอินเทอร์เน็ตก็จะสามารถสื่อสาร กันได้จากทุกมุมโลก ผ่านโปรแกรมหรือแอปพลิเคชันต่าง ๆ
(O)	
obliterations	การลบล้าง
observation	การสังเกตการณ์
obstacles	อุปสรรค
open Security	สิ่งแวดล้อมที่ไม่ได้มีการรับรองที่เพียงพอว่าอุปกรณ์และ แอปพลิเคชัน ต่าง ๆ ได้รับการปกป้องจากความเจตนาร้าย ทั้งก่อนและระหว่างการปฏิบัติงานของระบบ
open Systems Security	การรักษาความปลอดภัยในระบบเปิดหรือเครื่องมือต่าง ๆ ที่ใช้สำหรับทำให้การเชื่อมต่อของเครือข่ายของระบบเปิด (Open Systems) ต่าง ๆ มีความปลอดภัย
operational Data Security	การรักษาความปลอดภัยของข้อมูลการปฏิบัติการ การปกป้องข้อมูลการเปลี่ยนแปลง, การทำลาย, หรือ การเปิดเผยโดยไม่ได้รับอนุญาตทั้งโดยอุบัติเหตุและโดย เจตนาในระหว่างการ Input, Processing และ Output

operations Security (OPSEC)	ปฏิบัติการความปลอดภัย กระบวนการพิสูจน์ทราบข้อมูลสำคัญและการวิเคราะห์การกระทำของฝ่ายเราที่เกี่ยวข้องกับปฏิบัติการทางทหารและกิจกรรมอื่น ๆ
	(P)
performance	ประสิทธิภาพ
perpetrator of a crime	ผู้ประกอบอาชญากรรม
person identification	การพิสูจน์บุคคล
photograph	ภาพถ่าย
physical evidence	พยานหลักฐานทางกายภาพ
preparation	การเตรียม
preservation of evidence	การรักษาพยานหลักฐาน
printing	ลายพิมพ์
print out	สิ่งพิมพ์ออก
privacy	ความเป็นส่วนตัว
procedures research	วิธีการวิจัย
processes	กระบวนการ
processing algorithms	อัลกอริทึมของการประมวลผล
protection	การป้องกัน
professional	หลักวิชาชีพ
proof	การพิสูจน์
print out	สิ่งพิมพ์ออก
public safety	ความปลอดภัยของสาธารณะ
phishing	การปลอมแปลง E-mail หรือ Web Site รูปแบบหนึ่ง โดยส่วนใหญ่จะมีวัตถุประสงค์ที่ต้องการข้อมูลข่าวสารต่าง ๆ โดยส่วนมากข่าวสารที่คนส่ง Phishing ต้องการมากคือ User, Password และหมายเลขบัตรเครดิต โดย Phishing ส่วนมากจะอ้างว่ามาจากบริษัทที่มีความน่าเชื่อถือว่ามาจากบริษัทที่เหยื่อเป็นสมาชิกอยู่เป็น eBay.com, Pay Pal.com และ Online Banks ต่าง ๆ เป็นต้น
	(R)
research design	การออกแบบการวิจัย
research hypothesis	การตั้งสมมติฐานการวิจัย
research methodology	ระเบียบวิธีวิจัย
response	การตอบสนอง
retrieval	การสืบค้น

retrieving	การค้นคืน
rules of evidence	กฎของพยานหลักฐาน
rules of evidence relating to fraud	กฎของพยานหลักฐาน

(S)

sample	ตัวอย่าง
searching	การค้นหา
security	ความปลอดภัย
seminar	สัมมนา
secure socket layer: SSL	<p>มาตรฐานของ Protocol การสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุด Protocol โดย SSL ถูกออกแบบและกำหนดรายละเอียดโดยบริษัท Netscape เมื่อ ค.ศ. ๑๙๙๔ เพื่อบริการความปลอดภัยแก่ข้อมูลในระหว่างชั้น Protocol ระดับแอปพลิเคชัน (เช่น HTTP, Telnet, NNTP, หรือ FTP) กับ Protocol TCP /IP และเป็นมาตรฐานความปลอดภัยสำหรับโปรแกรม Web Browsers และเครื่อง Servers บนเครือข่าย Internet โดย SSL ทำให้เกิดการสื่อสารอย่างปลอดภัยระหว่างไคลเอนต์และเซิร์ฟเวอร์ โดยการอนุญาตให้มีกระบวนการพิสูจน์ตัวตนร่วมกับการใช้งานลายเซ็นดิจิทัล สำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูล (Data Encryption) เพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูล ทั้งนี้ Web ที่ใช้ SSL จะมีรูปกุญแจอยู่ในมุมล่างของ Web Browser และ Web Address จะขึ้นต้นด้วยคำว่า Https</p>
seminar in Forensic science	สัมมนานิติวิทยาศาสตร์
signatures	ลายมือชื่อ
source determination	การกำหนดแหล่งที่มา
specific methods	วิธีการตรวจพิเศษ
storage	การจัดเก็บ
storing	การจัดเก็บ
spam mail	การส่งข้อความที่ไม่เป็นที่ต้องการให้กับคนจำนวนมาก ๆ จากแหล่งที่ผู้รับไม่เคยรู้จักหรือติดต่อมาก่อน โดยมากอยู่ในรูปของ E-mail ทำให้ผู้รับรำคาญใจและเสียเวลาในการลบข้อความเหล่านั้นโดย Spam Mail ทำให้ประสิทธิภาพการขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย

Social Network

สังคมออนไลน์ที่ผู้คนมารวมตัวกันบนอินเทอร์เน็ตผ่านโปรแกรมหรือแอปพลิเคชันต่าง ๆ เช่น Facebook, Twitter และ Instagram เป็นต้น

(T)

techniques used to detect
testimony examination

เทคนิคที่ใช้สืบค้นตรวจพิสูจน์

techniques

เทคนิคการสอบปากคำ

technical attack

ภัยคุกคามจากผู้มีความรู้ด้าน System and Software

testing

การทดสอบ

training in court

การฝึกในชั้นศาล

(U)

undercover

การจารกรรม

unique

เป็นหนึ่งเดียว

(R)

recognition concepts

แนวคิดทางการรับรู้จัดจำรูปแบบ

(V)

virtual Private Network

เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN – Wide Area Network) เป็นระบบเครือข่ายภายในองค์กร ซึ่งเชื่อมเครือข่ายในแต่ละสาขาเข้าด้วยกันโดยอาศัย Internet เป็นตัวกลาง มีการทำ Tunneling หรือการสร้างอุโมงค์เสมือนไว้รับส่งข้อมูล มีระบบเข้ารหัสป้องกันการลักลอบใช้ข้อมูล เหมาะสำหรับองค์กรขนาดใหญ่ ซึ่งต้องการความคล่องตัวในการติดต่อรับส่งข้อมูลเครือข่ายเสมือนที่ยอมให้กลุ่มของ Site สามารถสื่อสารกันได้ นโยบายในการใช้งานใน VPN ถูกกำหนดโดยชุดของ Admin Policies ที่จัดทำขึ้นโดยสมาชิกในกลุ่มนั้น หรือถูกกำหนดอย่างเบ็ดเสร็จโดย Service Provider (SP) site ดังกล่าวนั้นอยู่ภายในองค์กรเดียวกันหรือต่างองค์กรก็ได้ หรือ VPN อาจเป็น Intranet หรือ Extranet Site ดังกล่าวอาจอยู่ในมากกว่าหนึ่ง VPN ก็ได้หรือ VPN อาจทับกัน, ทุก Site ไม่จำเป็นต้องอยู่ภายใต้ SP เดียวกัน, VPN อาจกระจายอยู่หลาย SP

อ้างอิง

- Cloudnine. (2023, 12). *How to Create an Image Using FTK Imager – eDiscovery Best Practices*. Abstract retrieved from <https://cloudnine.com/ediscoverydaily/electronic-discovery/how-to-create-an-image-using-ftk-imager-ediscovery-best-practices/>
- Crowdstrike. (2023, 1). *Real Time Threat Visibility - Start Your Free Trial Today*. Abstract retrieved from <https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-redline.pdf>
- Desdelinux. (2565, 10). *Maltego : เครื่องมือชุดข้อมูล – การติดตั้งบน GNU/Linux*. Abstract retrieved from <https://blog.desdelinux.net/th/maltego-herramienta-mineria-datos-instalacion-linux/>
- Dforensic.com (2023, 3). *Digital Forensics Examiner*. Abstract retrieved from <https://www.dforensic.blogspot.com/>
- ETDA สพรธ. (2559, 9). *ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน version 1.0*. Abstract retrieved from <https://ictlawcenter.etda.or.th/files/files/Feedback-Device-Management-standard-in-digital-forensic-evidence.pdf>
- Exploit Database. (2022, 4). *Google Hacking Database*. Abstract retrieved from <https://www.exploit-db.com/google-hacking-database>
- Jennifer Marsh. (2016, 3). *How to Detect and Analyze DDoS Attacks Using Log Analysis*. Abstract retrieved from <https://www.loggly.com/blog/how-to-detect-and-analyze-ddos-attacks-using-log-analysis/>
- Joe Marshall and Jon Munshaw. (2020, 9). *The Art and Science of Detecting Cobalt Strike : by Nick Mavis*. Abstract retrieved from <https://www.scribd.com/document/477576770/Talos-Cobalt-Strike-pdf>
- Justin Nordine. (2022, 11). *OSINT Framework*. Abstract retrieved from <https://www.osintframework.com>
- Lucideus. (2018, 10). *Introduction to Event Log Analysis Part 1 — Windows Forensics Manual 2018*. Abstract retrieved from <https://medium.com/@lucideus/introduction-to-event-log-analysis-part-1-windows-forensics-manual-2018-b936a1a35d8a>
- Michael Elkan. (2561, 12). *Maltego*. Abstract retrieved from <http://www.b-maltego.blogspot.com/2018/12/maltego.html>

- Raj Chandel's Blog. (2023, 1). *Hacking Articles*. Abstract retrieved from <https://www.hackingarticles.in>
- Rashi_garg. (2022, 7). *Windows Forensic Analysis*. Abstract retrieved from <https://www.geeksforgeeks.org/windows-forensic-analysis/>
- Ritesh G. Menezes and Francis N. Monteiro. (2022, 9). *Forensic Autopsy*. Abstract
retrieved from <https://www.ncbi.nlm.nih.gov/books/NBK539901/>
- Semi Yulianto. (2021, 4). *Tutorial : Wazuh SIEM - Installation and Configuration (Complete Steps)*. Abstract retrieved from <https://www.youtube.com/watch?v=kd5THDYTarM>
- StrWind Hyperconvergence. (2023, 1). *StarWind V2V Converter Help : Concept*. Abstract retrieved from <https://www.starwindsoftware.com/v2v-help/Concept.html>
- TechTalkthai.com (2561, 7). *จะรู้ได้อย่างไร ว่าเรากำลังถูกโจมตีแบบ DDoS*. Abstract retrieved from <https://www.techtalkthai.com/how-to-know-you-are-under-ddos-attack/>
- The Sleuth Kit. (2023, 1). *Autopsy*. Abstract retrieved from <https://www.sleuthkit.org/autopsy/>