

การพิสูจน์หลักฐานทางดิจิทัล

พ.ศ.๒๕๖๖

โดย กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ



บันทึกข้อความ

NN 0500.m/ 9008	วันที่	99 n.U.55	
-----------------	--------	-----------	--

เสนอ ศชบ.ทอ.

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

๒. ทสส.ทอ.จึงขอส่งคู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ เพื่อใช้ในการฝึก ความชำนาญของจำพวกทหารไซเบอร์ รายละเอียดตามแนบ

จึงเสนอมาเพื่อดำเนินการต่อไป

FEE พล.อ.ต.

ผอ.สนผ.ทสส.ทอ.ทำการแทน จก.ทสส.ทอ.



บันทึกข้อความ

	۷	สส.ท	alar al	
เลขรับ, อันที่	9 1	n.v.	9632	
1363		چ و	واو !	

ส่วนราชการ สนผ.ทสส.ทอ.(กนผ.โทร.๒-๑๐๕๖)

ที่ กห obod.m(b)/ bom

วันที่ 9 10 ก.ย.ออ

เรื่อง ขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ จำพวกทหารไขเบอร์

เรียน จก.ทสส.ทอ.

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

สนผ.ทสส.ทอ.ตรวจสอบแล้ว มีข้อมูล ดังนี้

๒.๑ ระเบียบ ทอ.ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓ และฉบับแก้ไขเพิ่มเติม ข้อ ๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่า ทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๙ แนบท้ายระเบียบนี้ (แนบ ๑)

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

๒.๒.๑ วิชา การป้องปรามทางไซเบอร์

๒.๒.๒ วิชา การป้องกันทางไซเบอร์

๒.๒.๓ วิชา การข่าวกรองทางไซเบอร์

๒.๒.๔ วิชา การพิสูจน์หลักฐานทางติจิทัล

๒.๒.๕ วิชา ความรู้พื้นฐานสำหรับปฏิบัติการทางไขเบอร์

 ๓. สนผ.ฯ พิจารณาแล้ว เพื่อให้การดำเนินการฝึกงานในหน้าที่ของสายวิทยาการไซเบอร์ เป็นไปด้วยความเรียบร้อย จึงขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึก ความขำนาญของจำพวกทหารไซเบอร์ต่อไป

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

, Wa.a.a 😪

ผอ.สนผ.ทสส.ทอ.

- อนุมัติดามข้อ ๓

wa.a.n.

จก.ทสส.ทอ. 🎐 ก.ย.๖๖

42	74 - CA 26	÷.	1 20 20		5 3	1875U EECO
	1		¥	- 	2004	200 d oc
چو چو	มราชการ ๙๙	ณ.ทอ.(นกพ.ๆ ไ	บนท า (ของอย่-ยะก	กขอคา	1) 	
สว	Ha I UII I a MU					
. สว ที่	NH 0500.0/	en 125	÷	วันที่	W 61.9.55	เลขรับ
สว ที่ เรีย	กห ออ๕อ.ด/ ()ง ขอให้พิจารณ	6ฟ&5 มาตำราของหลัก	สูตรสายวิทยาเ		UG1.9.55	เลขรับไขทางๆ วันที่

271.00-5 Ambor 6 d a.a. 6866

๑. ตามหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๑๐๘๙ ลง ๙ ส.ค.๖๖ ให้ ศขบ.ทอ.ปรับปรุง เนื้อหาคำราของหลักสูตรสายวิทยาการไขเบอร์จำนวน ๕ วิชา นั้น

๒. ศชบ.ทอ.ตรวจสอบและพิจารณาแก้ไขเนื้อหา รายละเอียดตามความเหมาะสม ร่วมกับ
 ร.อ.หญิง สุธิดา บทสันเทียะ นมฐ.ผมทส.กนผ.สนผ.ทสส.ทอ.แล้วเมื่อวันที่ ๒๓ ส.ค.๖๖ ดังมี รายละเอียดตามแนบ/

จึงเสนอมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต

ผอ.ศชบ.ทอ.

	กนผ.สนผ.ทสส.พอ.
เลขรั	ບ
วันที่	6d J.a. 55
เวลา	992EV

หราบแล้ว

- รอง ผอ.ถนม.สนุย.ทสส.ทอ.ทราบ -พศต. - อำเนิ เรทรโนส่วนเกี่ยงไร น.อ. ผูอ.ถนน สนน.ทสส.ทอ.

ทราบแล้ว

น.อ. 201-รอง พอ.กษศ.สนม.ทสส.ทอ. 6 (ส.ศ. 55

ทราบแล้ว

น.ฮ. รอง ผอ.อน์ผ.สนผ.ทสส.ทอ. 2.61



ระเบียบกองทัพอากาศ ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงแก้ไขแนวทางปฏิบัติเกี่ยวกับการฝึกงานในหน้าที่ของ กองทัพอากาศ ให้เป็นไปด้วยความเรียบร้อย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๕๔

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งชัดหรือแย้งกับ ระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

๔.๑ "การฝึกงานในหน้าที่" หมายความว่า การให้นายทหารประทวนเข้ารับ การฝึกงานตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย เพื่อเพิ่มพูนความรู้ ความสามารถ และความขำนาญ ให้สูงขึ้น ตามลักษณะความขำนาญทหารอากาศของเหล่าทหารหรือจำพวกทหาร โดยใช้ตามมาตรฐานการฝึก ความชำนาญ และหนังสือคู่มือการฝึกงานในหน้าที่เป็นแนวทางการฝึก

<. ๒ "การฝึก" หมายความว่า การฝึกงานในหน้าที่

๔.๓ "นายทหารผึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร ที่แต่งตั้งขึ้น ให้มีหน้าที่รับผิดชอบ และดำเนินการ ควบคุม กำกับ ดูแล เกี่ยวกับการฝึกงานในหน้าที่ของหน่วยขึ้นตรง กองทัพอากาศ ให้ใช้คำย่อว่า "นฝน."

๔.๔ "ผู้ช่วยนายทหารผึกงานในหน้าที่" 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"...

ถด.ดส.๒.๒ ระดับ ๕๐ จำนวนชั่วโมงรวมของการเรียน

การสอนของภาคปฏิบัติและภาคบรรยาย ไม่เกินร้อยละ ๘๐ ของจำนวนชั่วโมงรวมในระดับ ๗๐ ๓๑.๑๘.๒.๓ ระดับ ๗๐ จำนวนชั่วโมงรวมของการเรียนการสอน

ของภาคปฏิบัติและภาคบรรยาย ตรงกับความมุ่งหมายเฉพาะและวัตถุประสงค์การเรียนรู้ในระดับ do ๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและ

วิธีปฏิบัติงานของเหล่าทหารหรือจำพวกท[ั]หารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ ประกอบการฝึกงานในหน้าที่ตามระดับความขำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชา ในมาตรฐานการฝึกความขำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้าย ระเบียบนี้

หมวด ๖

การควบคุมกำกับดูแล

ข้อ ๗๒ หน่วยฝึกจะต้องดำเนินการฝึกตามระยะเวลาที่กำหนดไว้ในวงรอบการฝึก

ข้อ ๓๓ ผู้รับการฝึก จะต้องทำการฝึกครบทุกหัวข้อวิชา หรือหมวดวิชาที่เป็นวิชาหลักของ จำพวกทหารตามที่กำหนดในมาตรฐานการฝึกความขำนาญ

ข้อ ๓๔ เมื่อผู้รับการฝึกย้ายสังกัด ในระหว่างการฝึกภาคปฏิบัติ หรือรอการทดสอบภาควิชาการ ให้ส่วนราชการต้นสังกัดเดิมแจ้งให้ส่วนราชการต้นสังกัดใหม่ทราบถึงสถานภาพการฝึกที่ผ่านมา และเรื่องที่ จะต้องดำเนินการต่อไป พร้อมกับส่งประวัติการฝึก กับมาตรฐานการฝึกความชำนาญไปยังส่วนราชการ ต้นสังกัดใหม่ โดยส่วนราชการต้นสังกัดใหม่จะต้องแต่งตั้งผู้รับผิดชอบในขั้นตอนที่ยังเหลืออยู่ เพื่อดำเนินการ ฝึกต่อไปให้ครบตามหัวข้อที่กำหนดไว้ หากจะให้ทำการฝึกที่ส่วนราชการเดิมต่อไป ให้ประสานตกลงกัน แล้วแจ้งการเปลี่ยนแปลงให้ กรมกำลังพลทหารอากาศทราบ เพื่อแก้ไขเปลี่ยนแปลงหลักฐานการควบคุม การฝึกงานในหน้าที่ให้ถูกต้อง

ข้อ ๓๕ ผู้ที่ไม่สามารถทำการฝึกได้ครบตามที่กำหนด และอยู่ในกรณีที่จะต้องพ้นจากการฝึก ให้ส่วนราชการต้นสังกัดรายงานพร้อมหลักฐานประกอบให้กรมกำลังพลทหารอากาศ ดำเนินการนำเรียนขออนุมัติ ผู้บัญชาการทหารอากาศ หากจะเข้ารับการฝึกในปีต่อไปจะต้องเริ่มดำเนินการใหม่ ซึ่งการพ้นจากการฝึก จะต้องอยู่ในกรณี 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

ตช.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาลปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอับสมควร

ข้อ ๓๖ การลา ...

ผนวก 🖬 ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ. ๒๕๖๓



หนังสือคู่มือการฝึกงานในหน้าที



คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

ີສຑຐ**Ͽ.**๒໔໑ຓ໐ ຨຑຐ**Ͽ.**๒໔໑໕໐ ຨຑຐຉ.๒໔໑๗໐

กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ คู่มือการฝึกงานในหน้าที่วิชาการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) จัดทำขึ้น เพื่อประกอบการฝึกความชำนาญ ตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ เนื้อหาความรู้ของคู่มือเล่มนี้กล่าวถึงนิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) มาตรฐานงาน Digital Forensics การค้นหาข้อมูลทางโซเซียล และเครือข่าย การเก็บหลักฐาน การเตรียมหลักฐาน การวิเคราะห์ข้อมูล การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน และการออกรายงานผลการวิเคราะห์ เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่มีความรู้ความเข้าใจ เสริมสร้าง ทักษะในการนำไปปฏิบัติงานในสายวิทยาการไซเบอร์ เพื่อให้เกิดความปลอดภัยสูงสุด ต่อผู้ปฏิบัติงาน ระบบคอมพิวเตอร์ และระบบสารสนเทศของกองทัพอากาศ

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณ เจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

> กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ ๒๘ สิงหาคม ๒๕๖๖

สารบัญ

	หน้า
คำนำ	ก
สารบัญ	ข
สารบัญตาราง	ঀ
สารบัญภาพ	ຈ
บทที่ ๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)	୭
๑.๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)	୭
๑.๒ Chain of Custody หรือ "ห่วงโซ่การคุ้มครองพยานหลักฐาน"	តា
บทที่ ๒ มาตรฐานงาน Digital Forensics	୶
๒.๑ มาตรฐาน SANS Institue	b
๒.๒ คู่มืองาน Forensic จากกระทรวงดิจิทัล ๆ	୭୦
บทที่ ๓ การค้นหาข้อมูลทางโซเชียลและเครือข่าย	මේ
ຓ.໑ OSINT Framework	මම
๓.๒ การค้นหาข้อมูลทางโซเชียล (Maltego, Shodan, Google Hacking)	ଭଣ
๓.๓ พื้นฐานการใช้งาน WireShark	୭୯
บทที่ ๔ การเก็บหลักฐาน	ඳූබ
๔.๑ การเตรียมการ	දූල
๔.๒ การเข้าพื้นที่	දූල
๔.๓ การจำกัดการแพร่กระจาย	ඳූම
๔.๔ การจัดลำดับการเก็บหลักฐาน	ඳූම
๔.๕ การเก็บหลักฐานเครือข่าย	ඳූම
<.b การเก็บหลักฐานเครื่องโฮส	ଝଁଳ
๔.๗ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)	60
๔.๘ การจำกัดพื้นที่เครื่องเกิดเหตุ	60
บทที่ ๕ การเตรียมหลักฐาน	ර්
๕.๑ การสร้างไฟล์เพื่อทำการเก็บหลักฐานไฟล์ Image ด้วย Mandiant Redline	ර්ම
๕.๒ การโคลนฮาร์ดดิสเป็น Master และ Slab	ಶಿಡ
บทที่ ๖ การวิเคราะห์ข้อมูล	പ്പ
๖.๑ การแสดงผลโดยการใช้งาน IO Graph	ಡಠಿ
๖.๒ การวิเคราะห์ Host Forensic	ಡನ
๖.๓ การวิเคราะห์ Malware Analysis	ଝଣ

สารบัญ (ต่อ)

	หน้า
บทที่ ๗ การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน	രാല
๗.๑ กระบวนการจัดเก็บหลักฐาน	୦୦๔
๗.๒ การเก็บรักษา การถ่ายโอน และการส่งมอบหลักฐาน	୦୦୯
๗.๓ กระบวนการส่งคืนหลักฐาน	୦୦୯
บทที่ ๘ การออกรายงานผลการวิเคราะห์	රෙම
๘.๑ รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์	රෙ
๘.๒ ข้อมูลเบื้องต้น	ಂಡ
นิยามคำศัพท์ที่เกี่ยวข้องกับงานด้าน Forensic Computer	೦೦ನ
อ้างอิง	୭୭୯

สารบัญตาราง

		หน้า
ตารางที่ ๑	คุณสมบัติของ Input Filter	ണൽ
ตารางที่ ๒	การใช้งาน Filter	୩ଟ
ตารางที่ ๓	Logical Operator	କଟ

สารบัญภาพ

ภาพที่	١	หน้า
ภาพที่ ๑ ชื่	ข้อมูลในเอกสาร Chain of Custody	តា
ภาพที่ ๒ /	Association of Chief Police Officers	ଝ
ภาพที่ ๓	เว็บไซต์ของ National Institute of Justice (NIJ)	ፈ
ภาพที่ ๔	Logo ของหลักสูตรต่าง ๆ ของ SANS Institue	р
ภาพที่ ๕ [Digital Forensics	Ъ
ภาพที่ ๖ เ	เผ่น Poster เรื่อง Network Forensic	ಜ
ภาพที่ ๗ เ	เผ่น Poster เรื่อง Network Forensic Toolbox	ಜ
ภาพที่ ๘ เ	เผ่น Poster เรื่องกระบวนการวิเคราะห์ Malware Forensic	ನ
ภาพที่ ๙ ข้	<i>เ</i> ้อเสนอแนะมาตรฐาน	ၜ၀
ภาพที่ ๑๐	คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติฯ	୭୭
ภาพที่ ๑๑	OSINT Framework	୭๒
ภาพที่ ๑๒	Network Fingerprinting	ଭள
ภาพที่ ๑๓	ขั้นตอนที่ ๑ เลือกจุดหมายปลายทางและค้นพบเว็บไซต์	໑ຓ
ภาพที่ ๑๙	ตัวอย่างการกำหนดเว็บไซต์เป้าหมาย	୶
ภาพที่ ๑๕	ขั้นตอนที่ ๒ ค้นหาไซต์อื่น ๆ	୶ଝ
ภาพที่ ๑๖	ขั้นตอนที่ ๓ การเปิดเผยชื่อ & MX Server เซิร์ฟเวอร์ NS และ MX	୶ଝ
ภาพที่ ๑๗	To DNS Name – NS (Name Server)	වෙ
ภาพที่ ๑๘	ขั้นตอนที่ ๔ หากต้องการเรียกใช้กลุ่มข้อมูล	වෙ
ภาพที่ ๑๙	ขั้นตอนที่ ๕ ค้นหาที่อยู่ IP	ଚ୍ଚା
ภาพที่ ๒๐	ขั้นตอนที่ ๖ ค้นหาบล็อกเครือข่าย IP	୶୶
ภาพที่ ๒๑	Logo ของเว็บไซต์ Shodan	୶๙
ภาพที่ ๒๒	Shodan ค้นหาข้อมูลของอุปกรณ์	രി
ภาพที่ ๒๓	หน้าจอแสดงผลของ IP Camera	ଜା
ภาพที่ ๒๔	การใช้คำค้นหากับเว็บไซต์ Google	ല്പല
ภาพที่ ๒๕	Site domain	මම
ภาพที่ ๒๖	Filetype	២៣
ภาพที่ ๒๗	Case Study	ഇല
ภาพที่ ๒๘	Intitle	២៣
ภาพที่ ๒๙	โครงสร้างของ OSI 7 Layer เปรียบเทียบกับ TCP Model ในโปรแกรม Wireshark	ഉപ്പ
ภาพที่ ๓๐	กระบวนการส่งข้อมูล จากบนลงล่าง จากซ้ายไปขวา	ഉേ
ภาพที่ ๓๑	การเชื่อมต่อ Topology ในโปรแกรม EVE-NG เพื่อศึกษาการทำงานของ ARP	പര
ภาพที่ ๓๒	แพ็กเก็ตของ ARP ที่โปรแกรม Wireshark ได้รับเข้ามา	പര
ภาพที่ ๓๓	Client, Network, Server	ഉപ്പ
ภาพที่ ๓๔	รูปแสดงเครือข่ายบนคอมพิวเตอร์ที่โปรแกรม Wireshark ตรวจจับได้	ഉപ്പ

ภาพที่		หน้า
ภาพที่ ๓	🛿 การแสดงรายละเอียดของแพ็กเก็ตที่โปรแกรม Wireshark	මය
ภาพที่ ๓	แสดงผลการใช้งาน TCPDump เพื่ออ่านข้อมูลแพ็กเก็ตที่ได้บันทึกเก็บไว้	ຄ໐
ภาพที่ ๓	ฟ โปรแกรม Microsoft Network Monitor	ຄ໑
ภาพที่ ๓	🗧 ตัวอย่างการใช้งาน Microsoft netsh เพื่อเก็บข้อมูลในระบบเครือข่าย	ຓ໑
ภาพที่ ๓	🛪 การเก็บข้อมูลด้วยการทำ Remote Capture (Wireshark+TCPDump)	ബില
ภาพที่ ๔	> Network TAP	៣៣
ภาพที่ ๔	การสื่อสารระหว่างอุปกรณ์เมื่อสวิทช์ทำงานตามปกติ	ഩ൪
ภาพที่ ๔	การทำงานของสวิทซ์เมื่อมีการตั้งค่าให้ทำการทำงานในรูปแบบ SPAN	ഩ൪
ภาพที่ ๔	n ตัวอย่างการทำงานของ RSPAN	ഩൔ഻
ภาพที่ ๔	🛫 ตัวอย่างการทำงานของ ARP Spoofing	ຕາຍ
ภาพที่ ๔	🛿 MAC table บนเครื่อง PC ก่อนการทำ ARP Spoofing	ຄອ
ภาพที่ ๔	 ผลที่เกิดจากการทำ ARP Spoofing บนเครื่องที่ต้องการเก็บข้อมูล 	ഩൕ
ภาพที่ ๔	ฟ โปรแกรม Wireshark	ഩ๘
ภาพที่ ๔	< การแยกกลุ่มของ Input Filter	೯೦
ภาพที่ ๔	⊀ Display Filter	೯೦
ภาพที่ ๕	o Coloring Rule	ଝ୭
ภาพที่ ๕	o Conversation	ഭില
ภาพที่ ๕	 แสดงข้อมูลการ Login เข้าเราท์เตอร์ด้วย Telnet 	ଙ୍କ
ภาพที่ ๕	n แสดงข้อมูลในการสื่อสารของ HTTP	ଝଝ
ภาพที่ ๕	🛫 แสดงค่า Round - Trip Time ของเครือข่าย	୯୯
ภาพที่ ๕	🗶 แสดงค่า Time/Sequence (Steven's – Style)	୯୯
ภาพที่ ๕	 แสดงค่า Time/Sequence (tcptrace – Style) 	៤ ୭
ภาพที่ ๕	ฟ แสดงค่า TCP Packet	ଝ ରା
ภาพที่ ๕	< ตัวอย่างขนาดของแพ็กเก็ตไฟล์ที่นำมาใช้วิเคราะห์ปัญหา	೯
ภาพที่ ๕	๙ ตัวอย่างการกำหนดขอบเขตเพื่อจำกัดการเก็บข้อมูลเพื่อแก้ปัญหาของบริษัท A	೯
ภาพที่ ๖	ตัวอย่างการกำหนดขอบเขตเพื่อจำกัดการเก็บข้อมูลเพื่อแก้ปัญหาของบริษัท B	ଝଟ
ภาพที่ ๖	การเก็บข้อมูลและมองปัญหาจากจุดต่าง ๆ ใน Network	డం
ภาพที่ ๖	ฏ ภาพรวมการให้บริการ Internet โดยใช้ PPPOE	ඳීම
ภาพที่ ๖	n การเก็บหลักฐานด้าน Network ภายนอก	ഭ്ണ
ภาพที่ ๖	๙ การเก็บหลักฐานด้านเครือข่าย ภายใน	ഭ്ണ
ภาพที่ ๖	ะ การเก็บหลักฐาน RAM	ଝଝ
ภาพที่ ๖	การเก็บหลักฐาน RAM	ኖ ፈ
ภาพที่ ๖	การเก็บหลักฐาน RAM	ଝଝ
ภาพที่ ๖	ิ่< การเก็บหลักฐาน RAM	¢ರಿ
ภาพที่ ๖	๙ การเก็บหลักฐาน RAM	៥៦

ภาพที่	หน้า
ภาพที่ ๗๐ การเก็บหลักฐาน RAM	ଝ ଶ
ภาพที่ ๗๑ การเก็บหลักฐาน RAM	ଝ ରା
ภาพที่ ๗๒ การเก็บหลักฐาน RAM	విప
ภาพที่ ๗๓ การเก็บหลักฐาน RAM	ଝ୍ଟ
ภาพที่ ๗๔ การเก็บหลักฐาน RAM	
ภาพที่ ๗๕ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)	oď
ภาพที่ ๗๖ การจำกัดพื้นที่เครื่องเกิดเหตุ	oď
ภาพที่ ๗๗ โปรแกรม Mandiant Redline	මේ
ภาพที่ ๗๘ รันไฟล์โปรแกรม Mandiant RedLine 2	ඔර
ภาพที่ ๗๙ โปรแกรม Mandiant RedLine 3	່ວຄ
ภาพที่ ๘๐ โปรแกรม Mandiant RedLine 4	່ວຄ
ภาพที่ ๘๑ โปรแกรม Mandiant RedLine 5	ಶಿಷ
ภาพที่ ๘๒ โปรแกรม Mandiant RedLine 6	ಶಿಷ
ภาพที่ ๘๓ โปรแกรม Mandiant RedLine 7	ಶಿ
ภาพที่ ๘๔ โปรแกรม Mandiant RedLine 8	ಶಿಜೆ
ภาพที่ ๘๕ โปรแกรม Mandiant RedLine 9	66
ภาพที่ ๘๖ โปรแกรม Mandiant RedLine 10	66
ภาพที่ ๘๗ โปรแกรม Mandiant RedLine 11	් ක
ภาพที่ ๘๘ การโคลนฮาร์ดดิสก์เป็น Master และ Slab	ಶಿಡ
ภาพที่ ๘๙ โปรแกรม StarWind V2V Converter	ಸಿರ
ภาพที่ ๙๐ โปรแกรม StarWind V2V Converter 1	ಶಿನ
ภาพที่ ๙๑ โปรแกรม StarWind V2V Converter 2	ଜାଠ
ภาพที่ ๙๒ โปรแกรม StarWind V2V Converter 3	ଜାଠ
ภาพที่ ๙๓ โปรแกรม StarWind V2V Converter 4	ຕ /໑
ภาพที่ ๙๙ โปรแกรม StarWind V2V Converter 5	ମ୍ବ
ภาพที่ ๙๕ โปรแกรม StarWind V2V Converter 6	ର୍ଣାଣ
ภาพที่ ๙๖ โปรแกรม StarWind V2V Converter 7	ର୍ଣାଣ
ภาพที่ ๙๗ โปรแกรม StarWind V2V Converter 8	ର୍ଣ୍ଣକ
ภาพที่ ๙๘ โปรแกรม StarWind V2V Converter 9	ର୍ଣ୍ଣକ
ภาพที่ ๙๙ โปรแกรม StarWind V2V Converter 10	ର୍ଣ୍ଣକ
ภาพที่ ๑๐๐ โปรแกรม StarWind V2V Converter 11	ଶାଙ୍କ
ภาพที่ ๑๐๑ โปรแกรม StarWind V2V Converter 12	ଶାଙ୍କ
ภาพที่ ๑๐๒ โปรแกรม StarWind V2V Converter 13	୶ଝ
ภาพที่ ๑๐๓ โปรแกรม StarWind V2V Converter 14	୶ୡ
ภาพที่ ๑๐๔ โปรแกรม StarWind V2V Converter 15	୶୲ୄୄୄୄୄ

ภาพที่		หน้า
ภาพที่ ๑๐๕	โปรแกรม StarWind V2V Converter 16	ຝາວ
ภาพที่ ๑๐๖	โปรแกรม StarWind V2V Converter 17	ଚ୍ଚାର
ภาพที่ ๑๐๗	โปรแกรม StarWind V2V Converter 18	ଚ୍ଚାର
ภาพที่ ๑๐๘	โปรแกรม StarWind V2V Converter 19	୶୶
ภาพที่ ๑๐๙	โปรแกรม StarWind V2V Converter 20	୶୶
ภาพที่ ๑๑๐	การทำ Sandbox	୶୶
ภาพที่ ๑๑๑	คำสั่ง #> sudo fakedns	೯೦
ภาพที่ ๑๑๒	แสดงการ รันโปรแกรม Process Hacker	೯೦
ภาพที่ ๑๑๓	เว็บไซต์ Joesanbolbox.com	ເຈ
ภาพที่ ๑๑๔	วิเคราะห์กระบวนการทำงานของมัลแวร์	പ്പ
ภาพที่ ๑๑๕	การแสดงผลด้วย IO Graph	៨៣
ภาพที่ ๑๑๖	แสดงข้อมูลสรุปที่ได้จาก Expert Information	ಗಗ
ภาพที่ ๑๑๗	การแสดงผลโดย Custom Profile	ಗಳ
ภาพที่ ๑๑๘	การแสดงผลโดย Default Profile	ಗಳ
ภาพที่ ๑๑๙	โปรแกรม Imperva	ଜ ଣ
ภาพที่ ๑๒๐	การวิเคราะห์ลักษณะของ URL โดยโปรแกรม Imperva	ଜ ଣ
ภาพที่ ๑๒๑	Security Onion	ಷಷ
ภาพที่ ๑๒๒	Set ค่าวันเวลาของ Logs	ಷನ
ภาพที่ ๑๒๓	สถิติที่ทำการโจมตี	ನನ
ภาพที่ ๑๒๔	โปรแกรม FTK Imager	ನನ
ภาพที่ ๑๒๕	การวิเคราะห์ Disk Image	ನಂ
ภาพที่ ๑๒๖	ประวัติการใช้งาน Word Error หรือข้อความแจ้งเตือนของ Microsoft Office	ನಂ
ภาพที่ ๑๒๗	วงจรชีวิตของไฟล์	๙๏
ภาพที่ ๑๒๘	Regedit	ನ೬
ภาพที่ ๑๒๙	โปรแกรมตั้งเวลาทำงานอัตโนมัติ *	ನರಿ
ภาพที่ ๑๓๐	การตั้งค่า Firewall เพื่อเปิด - ปิด Port	ನರಿ
ภาพที่ ด๓๑	โปรแกรม Powershell	ଟ୍ଟଣ୍
ภาพที่ ๑๓๒ เ	โปรแกรม Volatility	ଟ୍ଟଣ୍ୟ
ภาพที่ ๑๓๓ เ	การตรวจสอบไฟล์มัลแวร์เบื้องต้น	ನನ
ภาพที่ ๑๓๔	แสดง Dashboard ของโปรแกรม Deep Instinct	ನನ
ภาพที่ ๑๓๕	การทดสอบรั้นไฟล์มัลแวร์บนสถาพแวดล้อมจำลอง	ನನ
ภาพที ๑๓๖	คำสัง foremost & binwork	ၜ၀၀
ภาพที ๑๓๗ ่	ค้าสังเกี่ยวกับไฟล์ zip	ၜ၀၀
ภาพที่ ๑๓๘	rockyou.txt.gz	୦୦୦
ภาพที่ ๑๓๙	Brute-Force	୦୦୭

	o	
ภาพที่		หน้า
ภาพที่ ๑๔๐	แบบฟอร์มควบคุมหลักฐาน	ෙම
ภาพที่ ๑๔๑	แบบฟอร์มการรับ – ส่งหลักฐาน	୭୦୩
ภาพที่ ๑๔๒	ตัวอย่างห้องเก็บพยานหลักฐาน	೦೦೯
ภาพที่ ๑๔๓	ตัวอย่างรายงานผลการตรวจพิสูจน์หลักฐานทางดิจิทัล	୭୦୩

บทที่ ๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

Digital Forensics หรือ นิติวิทยาดิจิทัลเป็นกระบวนการที่ใช้สำหรับหาตัวผู้กระทำความผิด หรือใช้สำหรับเก็บรวมรวบ ข้อมูล หลักฐานต่าง ๆ ที่อาจเกี่ยวข้องกับคดีความต่าง ๆ ที่เกิดขึ้นและ การค้นหาข้อมูลมีอยู่หลายวิธีการ เช่น ติดตามจาก ที่อยู่ หมายเลขไอพี (IP Address) ตามพิกัด (GPS) การดูคลิปกล้องวงจรปิด การสืบหาผู้กระทำความผิดจากข้อมูลอัตลักษณ์บุคคล (Biometric Data) ต่าง ๆ หรือการเจาะข้อมูลเข้าไปในเครื่องเซิร์ฟเวอร์ (Server) เป็นต้น เพื่อระบุตัวผู้กระทำความผิด ซึ่ง Digital Forensics นั้นมีความละเอียดและซับซ้อน

๑.๑ นิติวิทยาดิจิทัล และห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

เป็นหนึ่งในศาสตร์ของนิติวิทยาที่ใช้เครื่องมืออิเล็กทรอนิกส์เข้ามาช่วยเหลือการวิเคราะห์ พิจารณา และตรวจพิสูจน์หลักฐานทางดิจิทัล เพื่อนำเอาข้อมูลและหลักฐานต่าง ๆ เหล่านั้นมาประกอบรูปคดี จนสามารถเชื่อมโยงไปถึงตัวคนร้าย หรือผู้ที่อยู่เบื้องหลังการก่อเหตุอาชญากรรมเพื่อดำเนินการจับกุม ต่อไปได้ โดย Digital Forensics จะแบ่งออกเป็น ๓ ประเภท คือ

๑.๑.๑ นิติวิทยาเครือข่าย (Network Forensics) เป็นการเฝ้าติดตาม ตรวจสอบ เก็บรวบรวม และวิเคราะห์การเคลื่อนไหวบนเครือข่ายดิจิทัลต่าง ๆ เช่น ประวัติการเข้าใช้งานเว็บไซต์ ระยะเวลา ที่ใช้ในการอยู่หน้าเว็บไซต์ การรับ-ส่งข้อมูล เป็นต้น หรือการเคลื่อนไหวบนเครือข่ายดิจิทัลที่นำไปสู่ การโจมตีทางไซเบอร์ ทั้งในเรื่องของความปลอดภัยของข้อมูล การเจาะเข้าระบบความปลอดภัย การปล่อยไวรัส และการใช้งานเครือข่ายที่ผิดไปจากวิสัยที่ควรจะเป็น

๑.๑.๒ นิติวิทยาไวรัสคอมพิวเตอร์ (Malware Analysis) เป็นการวิเคราะห์และเฝ้าดู พฤติกรรมการทำงานของไวรัสคอมพิวเตอร์ ตั้งแต่การยืนยันไฟล์ว่าเป็นภัยคุกคาม การจำลอง การทำงานบนสภาพแวดล้อมสมมุติ (Sandbox) และการวิเคราะห์ฟังก์ชันการทำงาน เพื่อค้นหา พฤติกรรมที่ซ่อนเร้น หรือนำมาซึ่งความเสียหายต่อระบบ ทั้งนี้จำเป็นต้องใช้ความรู้และประสบการณ์ ในการทำงานสูงมากในการทำงานด้าน Digital Forensics หรือการพิสูจน์หลักฐานทางดิจิทัล ของกองทัพอากาศ จะเน้นไปที่การเก็บหลักฐานให้ถูกต้องตามหลักของ Forensic และการวิเคราะห์ข้อมูล ภัยคุกคาม โดยกระบวนการเหล่านี้ได้นำเอามาตรฐานหลายตัวในระดับโลกมาใช้เป็นหลักเกณฑ์ ในการปฏิบัติงาน แต่เนื่องด้วยงานของกองทัพอากาศไม่ได้เน้นพิสูจน์หลักฐานแล้วนำไปสู่ การดำเนินคดี แต่เป็นการให้ความสำคัญไปที่การค้นหาและพิสูจน์ช่องทางที่ถูกโจมตีด้วยเทคนิคขั้นสูงต่าง ๆ เพื่อเสนอผู้บังคับบัญชาในการออกมาตรการป้องกันหรือเพื่อค้นหาช่องโหว่ที่ถูกใช้งาน รวมทั้งดำเนินการ ปิดช่องโหว่ดังกล่าวเป็นหลัก

๑.๑.๓ หลักฐานดิจิทัล หมายถึง พยานหลักฐานที่อยู่ในรูปแบบข้อมูลที่คอมพิวเตอร์สามารถ จัดเก็บและจัดการได้ โดยปัจจุบันพยานหลักฐานดิจิทัลเกิดขึ้นโดยทั่วไปจากสภาพสังคมในปัจจุบัน ที่คนในสังคมใช้คอมพิวเตอร์ในชีวิตประจำวันเป็นปกติ เมื่อเกิดอาชญากรรมขึ้น พยานหลักฐาน ในรูปแบบดิจิทัลจึงเข้ามามีบทบาทในกระบวนการยุติธรรมเพิ่มมากขึ้นตามความเจริญของสังคม ดังนั้นในการรวบรวมพยานหลักฐานและการพิจารณาคดี หากทุกฝ่ายที่เกี่ยวข้องกับกระบวนการยุติธรรม มีความรู้ ความเข้าใจเกี่ยวกับพยานหลักฐานดิจิทัล ก็จะทำให้เกิดความยุติธรรมขึ้นอย่างแท้จริง เพราะพยานหลักฐานดิจิทัลสามารถพิสูจน์ได้ว่าบุคคลที่ถูกดำเนินคดีกระทำความผิด ทำให้ศาล สามารถมั่นใจได้มากยิ่งขึ้นว่าผลการตัดสินคดีนั้นถูกต้อง ทั้งเพื่อให้สามารถใช้นำเสนอเป็นหลักฐานใน ชั้นศาล หรือเพื่อรับฟังเป็นพยานหลักฐานในชั้นศาลตามขอบเขตอำนาจได้ และเพื่อให้มีมาตรฐานใน การนำไปใช้กับผู้ใช้งานที่ไม่ได้เป็นผู้เชี่ยวชาญ ผลการวิเคราะห์หลักฐานอาจจะหลีกเลี่ยงการใช้ คำศัพท์เฉพาะได้ โดยต้องเป็นไปตามขอบเขตอำนาจศาล และจะไม่ครอบคลุมการวิเคราะห์หลักฐาน ดิจิทัลหรือการยอมรับหรือการซั่งน้ำหนักพยานหลักฐาน รวมถึงความเกี่ยวข้องอันเป็นการพิจารณา ของศาล นอกจากนี้ยังไม่มีการกำหนดให้ใช้เครื่องมือหรือวิธีการเฉพาะอันอาจทำให้ได้มาซึ่งหลักฐาน มัดตัวผู้กระทำความผิด โดยทั่วไปจะมีหลักการสำคัญเกี่ยวกับการจัดการหลักฐานทางดิจิทัล อยู่ ๔ รูปแบบ คือ

๑.๑.๓.๑ Identification Process กระบวนการระบุข้อมูล IP วันเวลาที่มีการบันทึก พฤติกรรมของการกระทำต่าง ๆ การแจ้งเตือนของระบบหรือข้อความที่ใช้ในการสนทนาระหว่างกัน ต้องมีครบถ้วนและสามารถสืบย้อนหลังได้

๑.๑.๓.๒ Collection Process กระบวนการรวบรวมข้อมูลหรือกระบวนการของข้อมูล ที่มีความอ่อนไหวต่อการเปลี่ยนแปลงได้ 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 ไม่ว่าจะเป็น ทางกายภาพหรือทางตรรกะ (Logic) จะต้องไม่ก่อให้เกิดผลกระทบกับพยานหลักฐานจากหลักการ ที่ได้กล่าวมา เพื่อให้กระบวนการบริหารจัดการหลักฐานเป็นไปในแนวทางเดียวกัน และเป็นการคุ้มครอง พยานหลักฐาน จึงได้มีการกำหนดกระบวนการคุ้มครองพยานหลักฐานหรือ Chain of Custody เพื่อให้สามารถแสดงถึงกระบวนการแก้ไขเปลี่ยนแปลงใด ๆ กับหลักฐานแล้ว สามารถยืนยัน ความถูกต้องของกระบวนการและไม่ก่อให้เกิดความคลาดเคลื่อนของผลการวิเคราะห์ได้ ซึ่งเป็นลักษณะ ของการมีเอกสารกำกับทุกเหตุการณ์หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจาก หลักฐานที่พบนั้นสามารถนำไปใช้ในยืนยันในชั้นศาลได้ หลักฐานเกล่านี้จึงจะต้องได้รับการจัดการ อย่างระมัดระวัง และรอบคอบ เพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา ในการบันทึก จะไม่บันทึกเพียงแค่ว่าหลักฐานคือหลักฐานอะไรเท่านั้น แต่เรายังต้องบันทึกข้อมูลอื่น ๆ ด้วย เช่น ใครเป็นคนเก็บหลักฐาน เวลาที่เก็บหลักฐาน และรายละเอียดอื่น ๆ ที่เราพบขณะเก็บหลักฐาน กล่าวโดยสรุป คือ เอกสาร Chain of Custody จะประกอบด้วยข้อมูลที่เกี่ยวข้องกับการรวบรวมหลักฐาน การขนย้ายหลักฐาน การจัดเก็บหลักฐาน และการจัดการกับหลักฐานทางอิเล็กทรอนิกส์

๑.๒ Chain of Custody หรือ "หวงโซการคุมครองพยานหลักฐาน"

เอกสารแสดงลำดับการเกิดเหตุการณ หรือเอกสารแสดงทุกขั้นตอน ตั้งแตการยึดเครื่อง คอมพิวเตอร การดูแลรักษา การควบคุม การวิเคราะห และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส เนื่องจากหลักฐานที่พบสามารถนำไปใชในยืนยันไดในชั้นศาล หลักฐานเหลานี้จึงจะตองไดรับการ ้จัดการอยางระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงขอกลาวหาวาเปนหลักฐานที่ปลอมหรือทำขึ้นมา



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

มาตรฐานที่นำมาใช้ในงานด้าน Digital Forensics แต่ละประเทศจะใช้ไม่เหมือนกัน แต่โดยรวม แล้วก็จะเหมือนกันขึ้นอยู่กับลักษณะกฎหมายและความเหมาะสมของแต่ละประเทศ เช่น สหรัฐอเมริกา และยุโรป เป็นต้น จะใช้มาตรฐานของ SAN Institute ซึ่งเป็นบริษัทด้านการรักษาความปลอดภัย ทางไซเบอร์ชั้นนำของสหรัฐ ๆ ร่วมกับ International Organization for Standardization (ISO) ซึ่งเป็น มาตรฐาน การวัดคุณภาพองค์กร เป็นการรับรองระบบการบริหารและการดำเนินงานขององค์กรในแต่ละ ประเทศ เพื่อให้เป็นมาตรฐานเดียวกันทั่วโลก ซึ่งกระบวนการเหลานี้ไดนำมาตรฐานหลายตัวในระดับโลก มาใชเป็นหลักเกณฑในการปฏิบัติงาน ในบางครั้งหลักฐานที่นำมาวิเคราะหเพื่อนำไปสู่การ ดำเนินคดีความจะมีการให้ความละเอียดรอบคอบเปนพิเศษ ได้แก่ มาตรฐานระดับโลกที่นิยมนำมาใช้ เป็นมาตรฐานการปฏิบัติงานด้านการพิสูจน์หลักฐานทางดิจิทัล ดังภาพ



ภาพที่ ๒ Association of Chief Police Officers

องค์กร Association of Chief Police Officers หรือ ACPO เป็นองค์กรด้านกระบวนการ สืบสวนทางดิจิทัลของสมาคมตำรวจของสหราชอาณาจักร ซึ่งสามารถนำมาใช้เป็นแนวทาง ในงานตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

Scientific Working Group on Digital Evidence (SWGDE) เป็นคณะทำงานทางวิทยาศาสตร์ เกี่ยวกับหลักฐานดิจิทัล ของสหรัฐ ๆ ที่รวบรวมองค์ความรู้เกี่ยวกับการบังคับใช้กฎหมายด้านนิติ ดิจิทัล เพื่อพัฒนาแนวทางและมาตรฐานของงานการกู้คืน การเก็บรักษา และการตรวจสอบหลักฐาน ดิจิทัล โดยได้รับการสนับสนุนจากสำนักงานสืบสวนกลางสหรัฐอเมริกา โดยมีเอกสารแนะนำแนวทาง งานพิสูจน์หลักฐานทางดิจิทัลและยังสนับสนุนให้มีการใช้เอกสารเผยแพร่จำนวนมากในการสร้าง มาตรฐานระดับชาติและระดับสากลสำหรับงานด้านพิสูจน์หลักฐานและมัลติมิเดีย ISO/IEC 27037 เปนแนวทางในการจัดการหลักฐานดิจิทัล ซึ่งครอบคลุมในเรื่องของ การระบุ การรวบรวม การได้มา และการเก็บรักษาหลักฐานดิจิทัล ตามมาตรฐานของ ISO ที่จะเน้นไปในเรื่อง ของกระบวนการทำงานเป็นหลัก

สถาบันมาตรฐานและเทคโนโลยีแหงชาติ (The National Institute of Standards and Technology: NIST) เปนหนวยงานรัฐบาลกลางที่ดำเนินงานโดยกระทรวงพาณิชยของสหรัฐอเมริกา เป็นเอกสารที่ใหขอมูลโดยละเอียดเกี่ยวกับวิธีที่องคกรจะสามารถสร้างความสามารถทางนิติวิทยาศาสตร พัฒนานโยบายและขั้นตอนพื้นฐานที่จำเปน โดยมีจุดเด่นในเรื่องของการชวยให้องคกรสามารถใชเทคนิค ทางนิติวิทยาศาสตรเพื่อชวยในการตรวจสอบเหตุการณดานความปลอดภัยของคอมพิวเตอรและ ในการแก่ไขปญหาดานการปฏิบัติงานดานเทคโนโลยีสารสนเทศ

National Institute of Justice (NIJ) เป็นแนวทางการตรวจพิสูจนพยานหลักฐานดิจิทัลสำหรับ หนวยงานบังคับใชกฎหมายและสำนักงานอัยการ โดยจะมีเนื้อหาเกี่ยวกับการจัดการกับหลักฐาน ดิจิทัลใหอยู่ในกระบวนการสอบสวนที่สมบูรณ โดยในส่วนของกองทัพอากาศ จะใช้มาตรฐาน ของสถาบัน System Administration, Networking and Security (SANS) และ ISO/IEC 27037 : 2012 เป็นหลัก โดยจะมีเอกสาร "ข้อเสนอแนะมาตรฐาน การจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์ พยานหลักฐาน" เป็นคู่มือประกอบการดำเนินการใด ๆ ทาง Digital Forensics ของกองทัพอากาศ โดยมีรายละเอียด ดังนี้



ภาพที่ ๓ เว็บไซต์ของ National Institute of Justice (NIJ)

๒.๑ มาตรฐาน SANS Institue

SANS Institue เป็นองค์กรที่ทำงานเกี่ยวกับการออกใบรับรองความสามารถด้านไซเบอร์และ ยังเป็นผู้พัฒนาเครื่องมือที่จำเป็นทั้งหมดบนระบบปฏิบัติการ Linux Ubuntu ที่เรารู้จักกันในชื่อ Sift เพื่อใช้เป็นเครื่องมือในการตรวจสอบทาง Forensic รวมถึงระบบการตอบสนองต่อเหตุการณ์แบบ ดิจิทัล ทั้งนี้ SANS Institue ไม่ได้ดำเนินการเฉพาะในส่วนของ Forensic เท่านั้น แต่ยังออกใบรับรอง ความสามารถทางไซเบอร์ในด้านอื่น ๆ อีกด้วย โดยในส่วนของ Forensic จะแบ่งออกเป็นหลายหลักสูตร ซึ่งจะมี Logo ของแต่ละหลักสูตร ดังภาพ



ภาพที่ ๔ Logo ของหลักสูตรต่าง ๆ ของ SANS Institue

สาเหตุที่นำ SANS Institue มากล่าวเพราะเป็นมาตรฐานที่ได้รับการยอมรับจากทั่วโลก และเป็นกลุ่มนักพัฒนาเครื่องมือที่เปิดให้ใช้งานโดยไม่มีค่าใช้จ่าย ทั้งนี้ยังมีมาตรฐานระดับโลกอีกมาก ที่สามารถนำมาใช้เป็นมาตรฐานในการปฏิบัติงานได้ เช่น ISO และ NIST เป็นต้น ซึ่งขึ้นอยู่กับความ ต้องการและความเหมาะสมของแต่ละองค์กร โดยในที่นี้จะไม่แยกย่อยตามหลักสูตรของ SANS Institue แต่จะแสดงให้เห็นเป็นภาพกว้าง ๆ และจะกล่าวถึงรายละเอียดการปฏิบัติที่สามารถนำมาใช้งานได้จริง โดยมีกระบวนการปฏิบัติงานดังภาพ



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)

๒.๒.๑.๘ รายงานผล (Evidence Presentation)

นอกจากนี้ในเอกสาร Poster เกี่ยวกับงานด้าน Forensics ของ SANS Institute ซึ่งกล่าวถึงคำสั่งต่าง ๆ ที่มักจะต้องใช้ในการสืบค้นข้อมูล รวมถึงคำแนะนำกระบวนการทำงานและ โปรแกรมที่จะใช้ในการวิเคราะห์ ซึ่งสามารถนำมาเป็นมาตรฐานในการปฏิบัติงานได้เช่นกัน ทั้งนี้สำหรับ รายละเอียดเนื้อหาจะกล่าวในหัวข้อการวิเคราะห์ข้อมูล

๒.๑.๒ รายละเอียดของแผ่นโปสเตอร์ (Poster) ที่นำมาใช้เป็นมาตฐานงาน Forensic มีดังนี้
 ๒.๑.๒.๑ ด้าน Network Forensic จะเป็นการแนะนำเครื่องมือและแนวทางในการ
 ค้นหาหลักฐานทาง Network Forensic โดยจะแบ่งออกเป็น ๓ ส่วนใหญ่ ๆ คือ P หมายถึง ไฟล์ข้อมูล
 การจราจรใน Network (Packet Capture : pcap), F หมายถึงแผนผังเครือข่าย (Flow-Based or
 network diagram) และ L หมายถึง ล็อกไฟล์ (Logs File) โดยใช้อักษรย่อว่า PFL โดยมีรายละเอียด
 ความหมาย ดังนี้

๒.๑.๒.๑ (๑) Р หมายถึง ไฟล์ข้อมูลการจราจรใน Network (Packet Capture: pcap) เป็นส่วนสำคัญที่สุดเพราะจะทำให้ทราบว่าใครคุยกับใครในระบบ มีการรับส่งข้อมูล อะไรบ้างระหว่างกัน ปัจจุบันเครื่องมือที่ทำการวิเคราะห์ไฟล์ pcap ที่ดีที่สุดคือโปรแกรม WireShark
 ๒.๑.๒.๑ (๒) F หมายถึง แผนผังเน็ตเวิร์ค (Flow-Based or Network Diagram) เพื่อให้ทราบว่าอุปกรณ์แต่ละส่วนมีการชื่อมต่ออย่างไร

๒.๑.๒.๑ (๓) L หมายถึง ล็อกไฟล์ (Logs File) จัดเป็นข้อมูลที่มีความสำคัญ อีกตัวหนึ่ง ซึ่งสามารถบอกได้ว่าใครทำอะไรกับระบบบ้าง โดยจะมีรายละเอียดที่ค่อนข้างแปลผลได้ง่าย เนื่องจากเป็นข้อความธรรมดา ทั้งยังมีรายละเอียดของวันเวลาซึ่งนำไปสร้างเป็นไทม์ไลน์ของเหตุการณ์ ทั้งนี้ยังมีรายละเอียดอีกมาก ซึ่งจะสรุปในรูปแบบของแผ่น Poster โดยจะกล่าวเป็นด้าน ๆ ในหัวข้ออื่น ต่อไป



ภาพที่ ๖ แผ่น Poster เรื่อง Network Forensic



ภาพที่ ๗ แผ่น Poster เรื่อง Network Forensic Toolbox

๒.๑.๒.๒ ด้าน Host Forensic จะเป็นการศึกษาและทำความเข้าใจเกี่ยวกับการ เปลี่ยนแปลงของเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นในส่วนของฮาร์ดแวร์หรือซอฟต์แวร์ โดยในที่นี้จะ เน้นไปที่เรื่องของซอฟต์แวร์เป็นหลัก เนื่องจากการโจมตีทางไซเบอร์จะส่งผลกระทบต่อ ระบบปฏิบัติการ ไฟล์ ระบบเก็บ Logs และระบบเซอร์วิสที่ให้บริการ นอกจากนี้ยังมีส่วนที่เป็นฮาร์ดแวร์ ที่สามารถใช้เป็นหลักฐานทาง Forensic ได้ เช่น RAM, Hard Disk และ USB เป็นต้น โดยจะมุ่งไปที่ การค้นหาหลักฐานในระบบเมื่อมีการสร้างหรือรันไฟล์ใด ๆ ขึ้นมาใช้งาน จะก่อให้เกิด Logs หรือ การเปลี่ยนแปลงของข้อมูลบางอย่างของไฟล์ ทั้งนี้ยังรวมไปถึงการเปิดใช้งานไฟล์ การแก้ไข การคัดลอก การใช้คำสั่งคัดไฟล์ และการลบไฟล์ทิ้งด้วย สำหรับการหาข้อมูลประวัติการใช้งานบราวเซอร์ จะเป็นการสำรวจพฤติกรรมผู้ใช้งานว่ามีการท่องเว็บไซต์ที่เป็นอันตรายหรือไม่

๒.๑.๒.๓ ด้าน Malware Forensic จะมุ่งเน้นไปในเรื่องของการหาความผิดปกติหรือ ไฟล์ที่ต้องสงสัยว่าเป็นไฟล์มัลแวร์หรือไม่ โดยการหาจากร่องรอยการเปลี่ยนแปลงของไฟล์หรือ โพรเซส (Process) ที่มีพฤติกรรมการรับส่งข้อมูลหรือมีการเรียกใช้งาน Port ที่ผิดปกติ จนถึงการ ทดลองรันไฟล์ที่ต้องสงสัยเพื่อหาพฤติกรรมแอบแฝง ทั้งนี้ กระบวนการที่นำมาใช้จะเป็นดังรูป



ภาพที่ ๘ แผ่น Poster เรื่องกระบวนการวิเคราะห์ Malware Forensic

๒.๒ คู่มืองาน Forensic จากกระทรวงดิจิทัล ๆ

เป็นเอกสารอ้างอิงที่ใช้เป็นมาตรฐานในการวิเคราะห์ข้อมูล โดยเนื้อหาจะกล่าวถึงหลักการ เกี่ยวกับงานพิสูจน์หลักฐานและพยานหลักฐานดิจิทัล การปฏิบัติงานในสถานที่เกิดเหตุ เครื่องมือที่ใช้ การประเมินและวางแผนการเก็บรวบรวมหลักฐานในสถานที่เกิดเหตุ การบรรจุ การเคลื่อนย้าย การปฏิบัติงานในห้องปฏิบัติการ การบันทึกข้อมูล การทำรายงาน รวมไปถึงคุณสมบัติเบื้องต้นของ ผู้ทำการวิเคราะห์หลักฐาน ทั้งนี้รายละเอียดสามารถศึกษาเพิ่มเติมจากเอกสารดังภาพแสดง



ภาพที่ ๙ ข้อเสนอแนะมาตรฐาน

คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล		
ผู้ตรวจแก้ร่างข้อเสนอแนะ		
นางสุรางคณา วายุภาพ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
นางสาวพืชญลักษณ์ คำทองสุก	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
ที่ปรึกษา		
พลตำรวจโท วิสนุ ปราสาททองโอสถ	สำนักงานตำรวจแห่งชาติ	
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
ประธาน		
นายธงชัย แสงศิริ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
ผู้ทำงาน		
พันตำรวจเอก นิเวศน์ อาภาวศิน	สำนักงานตำรวจแห่งชาติ	
พันตำรวจโท หญิง จีรบูรณ์ บำเพ็ญนรกิจ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
พันตำรวจโท นันทวุฒิ รอดมณี	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับ	
	อาชญากรรมทางเทคโนโลยี	
นายปกรณ์ ธรรมโรจน์	สำนักงานอัยการสูงสุด	
นางสาวอมรรัตน์ เล็กวิชัย	สถาบันนิติวิทยาศาสตร์	
นางสาวธนิสสรา ลิ่นสุวรรณ	สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี	
	สารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการ	
	สื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร	
นายโสฬส พานิชปรีชา	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	
นายธันวา วาทหงษ์	บริษัท ไพร้ชวอเตอร์เฮาส์คูเปอร์ส คอนซัลดิ้ง (ประเทศไทย) จำกัด	
เลขานุการ		
นางสาวกรรณิกา ภัทรวิศิษฏ์สัณธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	

ภาพที่ ๑๐ คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติฯ

ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน Version 1.0 จัดทำโดย คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล

ศูนย์ดิจิทัลฟอเรนสิกส์ 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 เพื่อหาความสัมพันธ์ ของเหตุการณ์ นำไปสู่การดำเนินการสืบสวนสอบสวนเพื่อหาบุคคลผู้กระทำความผิด

ຓ.໑ OSINT Framework

เป็นเครื่องมือที่ใช้ในการค้นหาข้อมูล โดยมีการรวบรวมลิงก์เว็บไซต์ของเครื่องมือที่ต้องการและ จัดเป็นหมวดหมู่ ทำให้สามารถไล่ลำดับการค้นหาได้ง่าย การใช้งาน เช่น ถ้ามีข้อมูล IP หากต้องการ หาต่อว่าจะสามารถนำไปใช้ประโยชน์ในการค้นหาข้อมูลประเภท อื่น ๆ ได้อย่างไร เราก็จะสามารถ คลิกหัวข้อ IP Address ได้เลย โดย OSINT Framework จะทำการเชื่อมโยงข้อมูลอื่น ๆ ที่เกี่ยวข้อง เป็นลักษณะกราฟเส้น แสดงความสัมพันธ์เป็นชื่อเครื่องมือ ดังภาพ



ภาพที่ ๑๑ OSINT Framework

๓.๒ การค้นหาข้อมูลทางโซเซียล (Maltego, Shodan และGoogle Hacking)

โดยโครงสร้างของเว็บไซต์หรือโดเมนมีส่วนช่วยให้การค้นหาข้อมูลและโครงสร้างเว็บเป้าหมาย ทำได้ง่ายและเป็นระบบมากขึ้น ทั้งนี้เครื่องมือที่ได้รับความนิยมในลำดับต้น ๆ สำหรับการวิเคราะห์ ข้อมูลและมีขั้นตอนการใช้งาน ดังนี้

๓.๒.๑ Maltego เป็นเครื่องมือที่นิยมสำหรับการวิเคราะห์เครือข่ายที่ไม่ซับซ้อน โดยใส่ชื่อโดเมน หรือเว็บไซต์ที่ต้องการค้นหาข้อมูล ระบบจะดึงเอาข้อมูลความสัมพันธ์ต่าง ๆ และเชื่อมโยง เป็นโครงสร้างแสดงเป็นภาพรวม ทำให้ทราบความเชื่อมโยงของเว็บไซต์ ทั้งนี้ เครื่องมือดังกล่าวเป็น โปรแกรมฟรีแวร์ ไม่มีค่าใช้จ่าย โดยมีเงื่อนไขต้องเป็นสมาชิกของเว็บไซต์เท่านั้น โดยมีขั้นตอนในการใช้งาน ดังนี้



ภาพที่ ๑๒ Network Fingerprinting

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

	B = + * + * * B	Maltego Classic Eval 4.1.9
New Open Store	Recent Documents SpaceX Enrichment.mgl Beginning SpaceX Enrichment.mtgl New Graph (1).mgl ScientOrgTrace.mtgl	New Collaboration Import (Depart) Windows elect All β_k Add Parents γ_k Add Parents γ_k Add Parents γ_k Select Rookinarised γ_k Reverse Links γ_k elect All β_k Add Parents γ_k Add Parents γ_k Select Rookinarised γ_k Reverse Links γ_k elect None γ_k Add Colleber γ_k Select Rookinarised γ_k Select None γ_k vert Selection γ_k Add Similar Skings β_k Select Parents β_k Select Linkers γ_k
-Save All		Transform Hub
Save As Import Export	:	ATERVA CTAS andraf Parva Transforms UE INSTALLED FACTOR FROM CaseFile Entities Patersa Patersa Patersa Patersa Patersa Patersa Patersa Patersa Patersa Patersa
Tools	•	appressive Lab appressive Lab urry Kasperssy Units urry Kasperssy Threat Intelligence Data Feeds. Note that Dat. JRCNASS DESPENANTELY Control Connect Platform Set Platform Set P
Options Cicense Manager		hodan ndreugParerva uery Shodan data from within Maltegor titE INSTALLED FOR Skink Intelligence (BRI) from the Deep and DarkWith PARCHASED SERARATELY INSTALLED
More about Malteg		rowdStrike Intel rowdStrike Intel rowdStrike Intel rowdStrike Intel rowdStrike Inteligence API Transforms rowdStrike Inteligence API Transforms This set of transforms are based on the Hybrid Analysis 0 "Unclusional Strike Inteligence Interior Inteligence Int
VirusTotal Malformity Lat Query the Virus	Public API Is Total Public API	Control Media Investigative Instaligence Tool

ภาพที่ ๑๓ ขั้นตอนที่ ๑ เลือกจุดหมายปลายทางและค้นพบเว็บไซต์

จากตัวอย่างจะทำการค้นหาโดยใช้ชื่อโดเมนชื่อเดียวซึ่งระบบจะแสดงหน้า ว่างเปล่าขึ้นมา โดยสามารถเพิ่มเอนทิตี (Entity) แรกได้ โดยสามารถดู Entity Palette ทางด้านซ้าย และพิมพ์ "domain" ในแถบค้นหาเพื่อเรียกใช้เอนทิตีของโดเมน เมื่อขึ้นภาพสัญลักษณ์ให้ทำการลาก และวางลงบนหน้าจอเพื่อเริ่มการตรวจสอบได้



ภาพที่ ๑๔ ตัวอย่างการกำหนดเว็บไซต์เป้าหมาย

๓.๒.๑.๒ ขั้นตอนที่ ๒ ค้นหาเว็บไซต์อื่น ๆ ด้วยรหัสติดตาม (Tracking Code) สิ่งแรก ที่ต้องตรวจสอบคือรหัสติดตามที่องค์กรใช้ ด้วยการจัดเตรียมการวิเคราะห์สำหรับโดเมนเว็บไซต์ บ่อยครั้ง ที่สามารถเชื่อมโยงโดเมนต่าง ๆ เข้าด้วยกันได้เนื่องจากใช้รหัสติดตามร่วมกัน รหัสติดตามสามารถ แตกต่างกันไปตามรหัส Google Analytics ของ Amazon Affiliates codes และสามารถใช้เพื่อ ระบุข้อมูลการสร้างรายได้หรือต้องการค้นหารหัสติดตามที่เชื่อมโยงกับเว็บไซต์ ในขั้นต้นต้อง ้ดำเนินการแปลงเป็นโดเมนเว็บก่อน ทำได้โดยการคลิกขวาที่ Public Domain และพิมพ์ "ชื่อเว็บไซต์" ในแถบค้นหาเพื่อดูโดเมนทั้งหมดที่เชื่อมไปยังความละเอียดของเว็บไซต์ โดย "Quick Lookup" ที่ Ę ٤١ ۹١ ٤١ ้จะทำงานได้ดี และควรแก้ไขโดเมนของเราไปยังเว็บไซต์จากที่นี่เราสามารถคลิกขวาและป้อน "To Tracking Codes" เพื่อดำเนินการแปลงรหัสติดตาม จากตัวอย่างไม่ได้ส่งผลใด ๆ แต่มีการส่ง ข้อมลต่อไปยังเว็บไซต์ของ เทสลา (tesla.com) ด้านล่างเราจะเห็นผลลัพธ์ของการแปลงของโดเมน ที่เกี่ยวข้องอีกสองโดเมน หากต้องการค้นหาโดเมนเหล่านี้ต่อ สามารถคลิกขวาที่โค้ดติดตาม จากนั้น ้คลิกที่ "ไซต์อื่น ๆ ที่มีรหัสเดียวกัน" เพื่อค้นหาไซต์อื่น ๆ ที่มีรหัสติดตามเดียวกัน



ภาพที่ ๑๕ ขั้นตอนที่ ๒ ค้นหาไซต์อื่น ๆ

การเชื่อมโยงเหล่านี้สามารถใช้ประโยชน์ได้ในการค้นหาโดเมนอื่น ๆ ของ บุคคลเดียวกัน แต่ในบางกรณีโดเมนที่ได้อาจไม่ได้รับการยอมรับอย่างเป็นทางการ ทำให้ผู้โจมตีสามารถ ค้นพบส่วนที่เชื่อมโยงกันขององค์กรได้ การติดตามว่าองค์กรเหล่านั้นติดตามผู้ใช้อย่างไร องค์กรส่วน

 ใหญ่จะใช้รหัสติดตามเหมือนกันเพื่อช่วยในการวิเคราะห์โครงสร้างความสัมพันธ์ในองค์กรให้ง่ายขึ้น ๓.๒.๑.๓ ขั้นตอนที่ ๓ การเปิดเผยชื่อ DNS ที่เป็น Mail Server (MX) ของโดเมน สามารถแจ้งเตือนเกี่ยวกับบริการ E-mail ที่องค์กรใช้และบริการของโฮสต์ได้ โดยบางองค์กร จะมีโฮสต์เซิร์ฟเวอร์เหล่านี้อยู่ภายใน ซึ่งส่วนใหญ่ไม่ได้ใช้บริการของบุคคลที่สาม(เซิร์ฟเวอร์ E-mail ที่ไม่ใช่ขององค์กร) ข้อมูลนี้เป็นประโยชน์สำหรับแฮกเกอร์เนื่องจากสามารถนำข้อมูลไปใช้ ในเชิงลึกได้ เช่น การโทรหาบริษัท จากผู้ให้บริการเฉพาะรายที่ใช้อินเทอร์เน็ตหรือเว็บโฮสติ้ง การค้นหาข้อมูลนี้สามารถทำได้โดย คลิกขวาที่โดเมนที่เราสร้างขึ้นก่อนหน้านี้และพิมพ์ "mx" (ตัวแปรแทนชื่อของ Server E-mail) ในแถบค้นหาเพื่อดู Conversion ที่จะแก้ไขเซิร์ฟเวอร์ MX จากนั้นคลิกที่ปุ่มสัญลักษณ์ 🏜 เพื่อแสดงข้อมูล MX ซึ่งมักระบุว่าผู้ให้บริการรายใดใช้



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

หากต้องการดูระเบียน NS ของไซต์เราสามารถคลิกขวาที่โดเมนและพิมพ์ "ns" เพื่อดูการแปลงที่เกิดกับเซิร์ฟเวอร์ เลือก "To DNS – NS (Name Server)" เพื่อรับข้อมูลเซิร์ฟเวอร์ โดยสามารถให้ข้อมูลเกี่ยวกับองค์กรว่ากำลังใช้บริการของบุคคลที่สามเพื่อโฮสต์โดเมนของตนหรือไม่ หากต้องการดูระเบียน NS ของไซต์เราสามารถคลิกขวาที่โดเมนและพิมพ์ "ns" เพื่อดูการแปลง ที่เกิดกับเซิร์ฟเวอร์ แล้วเลือก "To DNS Name – NS (Name Server)" เพื่อรับข้อมูลเซิร์ฟเวอร์ โดยสามารถให้ข้อมูลเกี่ยวกับองค์กรว่ากำลังใช้บริการของบุคคลที่สามเพื่อโฮสต์โดเมนของตนหรือไม่



ภาพที่ ๑๗ To DNS Name – NS (Name Server)

๓.๒.๑.๔ ขั้นตอนที่ ๔ หากต้องการเรียกใช้กลุ่มข้อมูลทั้งหมดให้คลิกขวา ที่หน่วยโดเมนที่เราเพิ่มไว้ก่อนหน้านี้ แล้วเลือก "PATERVA CTAS" เพื่อเรียกใช้การแสดงกลุ่ม การเปลี่ยนแปลงต่าง ๆ คุณสามารถเลือกไอคอน "All Transforms" ถัดจากการแปลง "DNS from Domain" ที่กำหนดให้ดำเนินการแปลงทั้งหมดที่มีอยู่



ภาพที่ ๑๘ ขั้นตอนที่ ๔ หากต้องการเรียกใช้กลุ่มข้อมูล

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

๓.๒.๑.๕ ขั้นตอนที่ ๕ ค้นหาที่อยู่ IP หลังจากที่เรามีชุดระเบียน DNS เราจะสามารถ นำข้อมูลเหล่านี้ไปใช้ในการค้นหาไปยังที่อยู่ IP เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับ Service ที่องค์กรขนาด ใหญ่หลายแห่งจะเป็นเจ้าของเครือข่ายในการให้บริการของตนเองและเป็นโอกาสในการหาข้อมูลเพิ่มเติม ซึ่งสามารถเริ่มต้นค้นหาได้ว่าเป็นโฮสต์ภายในหรือภายนอก ต่อมาคือวิธีใช้ Maltego เพื่อจับภาพเครือข่าย ทั้งหมดโดยใช้ชื่อโดเมนเดียว สามารถทำได้โดยการเลือกระเบียน DNS ที่พบจากนั้นคลิกขวาที่ไฟล์ เหล่านั้นเพื่อรับแพ็กเกจการแปลง ซึ่งจะมีการเปลี่ยนแปลงเพียงอย่างเดียว ดังนั้นจึงสามารถเลือก "เรียกใช้ทั้งหมด" เพื่อเชื่อมโยงระเบียน DNS ที่อยู่ของ IP โดยจะมีข้อมูลมากมายเกี่ยวกับเครือข่าย ขนาดใหญ่ที่ประกอบขึ้นด้วยโครงสร้างพื้นฐานที่เชื่อมต่อ



ภาพที่ ๑๙ ขั้นตอนที่ ๕ ค้นหาที่อยู่ IP

๓.๒.๑.๖ ขั้นตอนที่ ๖ ค้นหาบล็อกเครือข่าย IP บล็อกเครือข่ายเป็นกลุ่มที่อยู่ของ IP ขนาดใหญ่ ซึ่งโดยปกติจะถูกกำหนดให้กับเอนทิตีตัวเดียวเมื่อสามารถระบุ Netblock ที่เป็น ขององค์กรเป้าหมายสามารถทำทุกอย่างได้ การสแกนที่อยู่ IP ภายในช่วงเพื่อค้นหาบริการ ที่ยังไม่ได้ค้นพบ หากต้องการค้นพบ Netblocks ที่องค์กรเป้าหมายสามารถเป็นเจ้าของได้ สามารถ เลือกที่อยู่ IP ที่ได้ค้นพบก่อนหน้านี้และคลิกขวาเพื่อเลือกการแปลง Maltego หนึ่งในสามเพื่อค้นหา Netblock ได้ด้วยการพิมพ์ "netblocks" ในแถบค้นหา เมื่อ Maltegro พบ Netblock จะสามารถ ขยายการค้นหาของ 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) เมื่อมีกลุ่มที่เป็นสมาชิก ขององค์กรเป้าหมายแล้ว หมายเลข AS จะถูกใช้อ้างอิงองค์กรขนาดใหญ่ ซึ่งมักเป็นผู้ให้บริการ อินเทอร์เน็ต ทั้งนี้เราต้องการระบุพื้นที่บล็อกเครือข่ายที่มีโพรโตคอลใช้งานเส้นทางเดียวกัน ถ้าสามารถระบุหมายเลข AS ของเป้าหมายได้ เราก็จะสามารถหาบล็อคเครือข่ายทั้งหมดได้เช่นกัน จากนั้นจะค้นพบชื่อ DNS ทั้งหมดที่อยู่ในแต่ละบล็อคเครือข่ายเหล่านั้น และเพื่อให้สามารถแก้ไขชื่อ DNS เหล่านั้นลงในที่อยู่ IP ของบริการเป้าหมายอื่น ๆ ได้ จึงจำเป็นต้องระบุหมายเลข AS ในขั้นตอน สุดท้ายนี้ด้วย





ภาพที่ ๒๑ Logo ของเว็บไซต์ Shodan

๓.๒.๒ Shodan คือเว็บไซต์ Search Engine ที่ทำหน้าที่เหมือน Google แต่คนละ Concept โดย Shodan Concept คือสามารถทำการค้นหาอุปกรณ์ที่เชื่อมต่อ Internet หรือมีการ n n ้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 คำค้นเบื้องต้น Country - จำกัดประเทศ, City - จำกัดชื่อจังหวัด, OS - จำกัดระบบปฏิบัติการ, Port - จำกัดเลข Port ซึ่ง Shodan จะนำ ข้อมูลมาตรวจสอบ ช่องโหว่ในระบบความปลอดภัยของอุปกรณ์หรือระบบนั้น ๆ เพื่อเป็นแนวทาง ในการปรับปรุงแก้ไข ป้องกันการถูกเจาะระบบความปลอดภัยของอุปกรณ์เบื้องต้น หรือ คือผู้ใช้งาน ้สามารถสวมบทบาทเป็น Hacker จำเป็น เพื่อไปทดสอบระบบหรืออุปกรณ์ของผู้อื่นได้ อีกทั้งยังเปิด ให้สามารถนำ API ไปใช้เพื่อตรวจสอบความปลอดภัยของระบบได้ซึ่งผู้ไม่หวังดีอ[้]าจใช้ความสามารถ ของ Shodan ในการโจรกรรม ข้อมูล (Hack) ได้ เนื่องจากทุกวันนี้อุปกรณ์ภายในองค์กรมีการ เชื่อมต่อ Internet หรือเป็น Always Online เช่น กล้องวงจรปิด หรือ CCTV เป็นต้น จึงกลายเป็น ภัยใกล้ตัวที่มักถูกมองข้ามไป
ทั้งนี้ความอันตรายอันดับต้น ๆ เมื่อทุกสิ่งเชื่อมต่อเข้ากับ Internet เนื่องจาก Shodan สามารถค้นหาข้อมูลของอุปกรณ์และระบบต่าง ๆ ที่เชื่อมต่อ Internet จากทั่วโลกได้นั้น ทำให้เกิด เป็นความอันตรายลำดับที่ ๑

🔏 Ѕнор	AN count	try:"TH" city:"Ban	gkok*	Q # E	xplore Downloads	Reports	Pricing	Enterprise Access		📥 My Account
🐴 Exploits	🔩 Maps	🐔 Images	Share Search	A Download Results	Lal Create Report					
TOTAL RESULT	5		New Ser	vice: Keep track of what	you have connected to t	he Internet. C	heck out <mark>Sh</mark>	nodan Monitor		
645,071			G1-91-183-210 True Internet Added on 2022 Thalland, HTTP/1 charse	abdicasianet.co.9 kol-14 04:09:09 GMT Bangkok 0 501 Not Implemented\r c=150-8859-1\r\n\r\n@fTM	- \nDate: Tue, 14 Jan 2020 L>⊂HEAD>⊂TITLE>501 Not I	03:11:17 GMT\/ mplemented <td>∿nServer: B ILE>≺/HEAD>\</td> <td>Boa/0.94.14rc21\r\nAccept-Ranges: b InrdBODY>-H1>S01 Not Implemented<td>sytes\r\nConnection: close\r\nConten }\nPOST to non</td><td>t-Type: text/html;</td></td>	∿nServer: B ILE>≺/HEAD>\	Boa/0.94.14rc21\r\nAccept-Ranges: b InrdBODY>-H1>S01 Not Implemented <td>sytes\r\nConnection: close\r\nConten }\nPOST to non</td> <td>t-Type: text/html;</td>	sytes\r\nConnection: close\r\nConten }\nPOST to non	t-Type: text/html;
Thailand TOP CITIES Bangkok Bangkok Noi	<i></i>	645,071 644,960 102	ppp-115-87-34 True Internet Added on 2020 Thailand,	5-117.rsvip4.asianet.co.th -01-14 04:09:15 GMT Bangkok						
TOP SERVICES			http/1 charse	.0 501 Not Implemented\r t=ISO-8859-1\r\n\r\n <htm< td=""><td>\nDate: Tue, 14 Jan 2020 L><head><title>501 Not In</title></head></td><td>03:12:03 GMT\ nplemented<td><pre>`\nServer: B ILE>\</pre></td><td>8oa/0.94.14rc21\r\nAccept-Ranges: t \n<80DY><h1>501 Not Implemented<td>oytes\r\nConnection: close\r\nConten I>\nPOST to non</td><td>t-Type: text/html;</td></h1></td></td></htm<>	\nDate: Tue, 14 Jan 2020 L> <head><title>501 Not In</title></head>	03:12:03 GMT\ nplemented <td><pre>`\nServer: B ILE>\</pre></td> <td>8oa/0.94.14rc21\r\nAccept-Ranges: t \n<80DY><h1>501 Not Implemented<td>oytes\r\nConnection: close\r\nConten I>\nPOST to non</td><td>t-Type: text/html;</td></h1></td>	<pre>`\nServer: B ILE>\</pre>	8oa/0.94.14rc21\r\nAccept-Ranges: t \n<80DY> <h1>501 Not Implemented<td>oytes\r\nConnection: close\r\nConten I>\nPOST to non</td><td>t-Type: text/html;</td></h1>	oytes\r\nConnection: close\r\nConten I>\nPOST to non	t-Type: text/html;
Modern Web Int	erface	85,288								
HTTP (81) HTTPS SSH TOP ORGANIZJ	ATIONS	41,763 29,581 12,541	45-64-188-26- Bangmod Ent Added on 2020 Thailand,	tatic bangmod-ldc.com erprise Co. I-01-14 04:09:08 GMT Bangkok	SSH-2.0-OpenS Key type: ssh Key: AAAAB3N2 NyfiSZSq3Pk13 dBGXh1YYD+XS	SH_7.4 i-rsa iaClyc2EAAAADAG Uloh79pYwrP9Mr ivXgAsh4nC05h+8	ABAAABAQDqr1 P9k4fZnzQy8i CLK06/RSLu81	T709iFYVg5NC79kUHepMLRiwsDw40VV2to ImuYgTQk7UnSA4GvV2zYXoS8GPjE/VJmLDL tMSSAJCTY6G5GeK60eFFmHt/hizaJ+0000m	I3rg3TX6a MgBz UDh2	
True Internet		189,287			Dc+yqgRDUDe20	r51NH1jbZI				
3BB Broadband	r.	142,175		_						
AIS Fibre CAT Telecom pu	ublic company Ltd	23,424	184-82-199-0.3 AIS Fibre Added on 2020	4. public. sila1-bcr01. myaisfibre.c	om RFB 003.008					
TOP OPERATIN	IG SYSTEMS		Thailand,	Bangkok						

ภาพที่ ๒๒ Shodan ค้นหาข้อมูลของอุปกรณ์

ผู้ใช้งานทั่วไปสามารถมีความเสี่ยงถูกผู้ไม่ประสงค์ดีเข้าถึงความเป็นส่วนตัวโดยที่ ไม่รู้ตัว ซึ่ง Shodan สามารถสร้างความอันตรายได้มากกว่าที่คิด จากภาพที่จะเห็นได้ว่ามีอุปกรณ์หรือ ระบบที่ทำการเชื่อมต่อ Internet และพบช่องโหว่ทางด้านความปลอดภัย มากถึง ๖๔๕,๐๗๑ 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 ซึ่งสามารถจำกัด ให้แคบลงได้มากกว่าเดิม เพียงคลิกเข้าไปที่หัวข้อทางด้านซ้าย เช่น ต้องการดูเฉพาะ Devices ที่ใช้ บริการ Internet ของ True เมื่อกดเลือกก็จะ Scope เหลือเพียง ๑๒ ชิ้น ตามตัวเลขด้านหลัง จากนั้นทำการเลือกมา ๑ ตัว เพื่อมาทดสอบความปลอดภัย โดยสามารถใช้ในการส่องกล้องวงจรปิด ของผู้อื่นได้ โดยมีขั้นตอนในการปฏิบัติข้ามต้น 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 แม้ว่าหน้าเว็บนั้นจะไม่มีลิงก์ไปจากเว็บไหน 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 ด้วยการใช้ Request หลากหลายรูปแบบที่ถูกออกแบบมาเพื่อตรวจสอบ Server แต่ละเครื่องว่าเป็น C&C Server หรือไม่นั่นเอง ซึ่ง Request เหล่าแท้จริงแล้วก็คือ 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 พร้อม กับข้อมูลประกอบว่าเป็น C&C Server ของ Remote Access Trojan (RAT) ตระกูลใด เช่น Dark Comet, njRAT, Poison Ivy, Ghost RAT และอื่น ๆ เป็นต้น ปัจจุบัน Malware Hunter นี้ตรวจ พบ C&C Server เกินกว่า ๕,๗๐๐ เครื่องไปเป็นที่เรียบร้อยแล้ว

๓.๒.๓ Google Hacking เป็นการใช้คำค้นหากับเว็บไซต์ Google ที่ลงลึกในรายละเอียดได้ และยังสามารถช่วยให้เราตีกรอบข้อมูลจำเพาะในสิ่งที่เราสนใจได้ มีประโยชน์ช่วยในการค้นหาข้อมูล ให้รวดเร็วและเจาะจงได้ดีขึ้น ตัวอย่างเช่น intitle, inurl, intext, site, link, cach และ filetype เป็นต้น



ภาพที่ ๒๔ การใช้คำค้นหากับเว็บไซต์ Google



ภาพที่ ๒๕ Site domain



ภาพที่ ๒๖ Filetype



ภาพที่ ๒๗ Case Study

ogle	intitle "cisco"		\$ C
	Web Images Maps News	Videos More - Search tools	
	About 26,900,000 results (0.38 seconds)		
	Cisco Systems, inc www.cisco.com/ ~ Cisco (NASDAQ: CSCO) is the worldwide lea opportunities of tomorrow by proving that ama	der in 17 that helps companies seize the izing things can happen	C
	Results from cisco.com	٩	Cisc mult
	ชิส โก้ ประเทศไทย ประเทศไทย (ปลีอน) ล็อกสิน ปลูชิ ลง ทะเบิณ เกี่ยวกับซิสไก่ ชิสไก่	Cisco.com Login Page Your login was unsuccessful for one of the following reasons	beac desi equi Desi
	Products & Services Products & Services. shriftouter- 369x215. Provide New Services	Cisco Networking Academy The Networking Academy program Disco Advanced	CEC Stor
	Routers Gisco routers and routing products can transform your network and	Training & Events Explore a variety of Cisco training courses, certifications, and events.	Four
	Cisco Networking Academy https://www.netacad.com/ •		Pro

ภาพที่ ๒๘ Intitle

ทั้งนี้การใช้ประโยชน์จาก Google Hacking ก็จะคล้าย ๆ กับตัว Shodan โดยกล่าว ได้ว่าเป็นวิธีการใช้งานทั่วไปแบบที่ใช้กันในการค้นหาข้อมูลจากเว็บไซต์ Google แต่อีกหนึ่งสิ่งที่ Google ทำได้ก็คือ "การค้นหาข้อมูลแห่งช่องโหว่เพื่อใช้เป็นเครื่องมือในการแฮกข้อมูล" การใช้งาน Google แบบเดิม ๆ จึงเปลี่ยนไปเป็น "เครื่องมือชั้นยอดของเหล่าแฮกเกอร์ในการสุ่มหาเป้าหมายและค้นหา เครื่องมือโจมตีนั้นเอง

๓.๓ พื้นฐานการใช้งาน WireShark

WireShark เป็นเครื่องมือที่ใช้สำหรับตรวจจับแพ็กเก็ตและวิเคราะห์ แพ็กเก็ตไปในตัวโดยจะมีผลต่อ การวิเคราะห์ที่เมื่อเปรียบเทียบกับสถาปัตยกรรม 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 จนสิ้นสุด ที่ Physical จากนั้น Physical ก็จะทำการส่งผ่านสาย LAN หรือระบบ Wifi แล้วแต่กรณี เพื่อให้อีก ฝั่งหนึ่งรับข้อมูล 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, เร้าเตอร์ และ Switch เป็นต้น

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

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

๓.๓.๑.๔ Layer 4 (Transport Layer) หากต้องการความแม่นยำใช้ TCP หาก ต้องการความรวดเร็วใช้ UDP

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

๓.๓.๑.๖ Layer 6 (Presentation Layer) เป็นการระบุชนิดของข้อมูลที่สื่อสาร ออกไปว่าเป็นชนิดใด เช่น ในการเปิดเว็บเพจหนึ่งหน้าจะมีส่วนประกอบอื่น ๆ เพื่อให้เว็บเพ็จทำงาน อยู่หลายตัว เช่น HTML, Java Script และ Video Streaming เป็นต้น สิ่งเหล่านี้นั้นเองเราเรียกว่า Presentation

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

๓.๓.๒ โพรโทคอล ARP

เป็นโพรโทคอลที่มีการทำงานอยู่ใน Layer 2 ของแบบจำลอง OSI โดยทั่วไปแล้ว องค์กรส่วนใหญ่ ที่มีการใช้งานระบบเครือข่ายจะมีการเชื่อมต่ออุปกรณ์ในระบบเครือข่ายเข้าด้วยกัน โดยใช้มาตรฐาน Ethernet ดังนั้น ข้อมูลที่อยู่ใน Layer 2 ของ Ethernet ก็คือ MAC Address ใน Layer 2 ของแบบจำลอง OSI จะเป็นการเชื่อมต่อกันในลักษณะ "จุดต่อจุด" ซึ่งจะมองการเชื่อมต่อ เพื่อส่งข้อมูลกันในระยะสั้น ๆ คือจาก MAC Address บนการ์ด LAN บนเครื่องคอมพิวเตอร์ไปยัง MAC Address บนเครือข่ายของสวิทช์ที่เชื่อมต่ออยู่กับการ์ด LAN นั้น ๆ เป็นอันสิ้นสุดการสื่อสารใน Layer 2 ของ แบบจำลอง OSI ในกรณีที่ต้องการส่งข้อมูลต่อไปที่จุดอื่น ใน Layer 2 ของแบบจำลอง OSI จะเป็นหน้าที่ของ สวิทช์ซึ่งจะต้องทำการมองหา MAC Address ของอุปกรณ์ปลายทางที่เครื่อง คอมพิวเตอร์นั้นต้องการที่จะติดต่อด้วยว่าต้องทำการส่งข้อมูลไปที่ปลายทางที่การเชื่อมต่อใดของ สวิทช์ โดยการมองหา MAC Address ของสวิทช์นั้นจะต้องมีกระบวนการ "จับคู่" ข้อมูลของ MAC Address ใน Layer 2 และ IP Address ใน Layer 3 ของแบบจำลอง OSI ซึ่งกระบวนการทำงาน ในการจับคู่ระหว่าง MAC Address และ IP Address เข้าด้วยกันนี้ จะมีการทำงานผ่านโปรโตคอล ARP โดยการทำงานของโปรโตคอล ARP จะมีอยู่ ๒ ขั้นตอนคือ ARP request และ ARP reply โดย ARP จะเกิดขึ้นก็ต่อเมื่ออุปกรณ์นั้นไม่ทราบ MAC Address ของอุปกรณ์ในเครือข่ายเดียวกัน ที่ต้องการที่จะติดต่อด้วย ขั้นตอนนี้จะมีการส่ง IP Address ที่ต้องการทราบออกไปพร้อมกับ Broadcast Destination MAC Address กระจายออกไปในเครือข่าย ด้วย MAC Address ปลายทางคือ FFF.FFF.FFFF พร้อมกับส่ง MAC/IP Address ของเครื่องต้น ทางออกไปด้วย เมื่อเครื่องปลายทางที่มี IP Address ตรงกับเครื่องต้นทางประกาศหาก็จะตอบกลับ ด้วย ARP reply แพ็กเก็ตซึ่งจะมีข้อมูล IP/MAC Address ของเครื่องปลายทางกลับไปให้เครื่องต้นทาง ในกรณีที่ต้องการเห็นการทำงานของโพรโทคอล ARP ให้ได้ชัดเจนนั้นจะต้องนำโปรแกรม Wireshark หรือ TCPDump มาช่วยในการจับแพ็คเก็ตขึ้นมาแสดงผล ในกรณีตัวอย่างเราสามารถนำโปรแกรม EVE-NG มาประยุกต์ใช้งานในการเรียนรู้การทำงานของโพรโทคอลต่างๆได้อย่างง่ายดาย รวมทั้ง ในกรณีนี้ที่เป็น โปรโตคอล ARP ก็เช่นกัน จากในรูปที่ ๓๑ เราจะทำการต่อ Topology โดยมี PC ทั้งหมด ๔ เครื่อง เชื่อมต่อกันผ่านสวิทซ์ ให้ทำการจับแพ็คเก็ตที่เครือข่ายใดเครือข่ายหนึ่งของสวิทซ์ เพื่อสังเกตการทำงาน ในบางครั้งเราอาจจะไม่เห็นโพรโทคอล ARP อยู่ในส่วนของแพ็คเก็ต ที่แสดงผลในโปรแกรม Wireshark จะต้องทำการเคลียร์ ARP บนอุปกรณ์เพื่อให้อุปกรณ์ทำการสร้าง ARP Request ก่อน



ภาพที่ ๓๑ การเชื่อมต่อ Topology ในโปรแกรม EVE-NG เพื่อศึกษาการทำงานของ ARP

เมื่อโพรโทคอล ARP แสดงผลที่โปรแกรม Wireshark แล้วจะลองมาทำการเปรียบผลที่ได้ จากโปรแกรม Wireshark กับทฤษฎีก่อนหน้านี้ที่ว่าในกระบวนการส่ง ARP Request นั้น ต้องมีการส่ง IP/MAC Address ของเครื่องต้นทางอออกไป พร้อมกับ Broadcast Destination Address ที่เป็น MAC Address FFF.FFF.FFF.FFF เมื่อลองดูแพ็กเก็ตที่โปรแกรม Wireshark แสดงผลในรูป พบว่าในโปรโตคอล ARP แพ็คเก็ตแรกจะมีการส่งข้อมูลตามที่ได้กล่าวไว้ในทฤษฎีจริงตามผล

Source	Destination	Protocol	Frame Lengt	Info
00:00:00:00:00:01	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 ในส่วนนี้จะกล่าวถึงการทำงานของโปรแกรมที่ ต้องการใช้งานอยู่บนโพรโทคอล TCP ซึ่งเป็นโปรแกรม ประเภทที่ต้องการความถูกต้องของข้อมูล ในการสื่อสารบนระบบเครือข่าย โดยทั่วไปแล้วการสื่อสารโดยใช้ โพรโทคอล TCP จะเป็นการสื่อสาร แบบ Client-Server การสื่อสารกันจะต้องเริ่มต้นด้วยการส่งคำขอใช้งาน จากเครื่อง Client ไปที่ ้เครื่อง Server ซึ่งการเริ่มต้นการสื่อสารนี้จะต้องเริ่มต้นด้วยการส่งแพ็กเก็ต Syn จาก เครื่อง Client ้ไปหาเครื่อง Server หลังจากนั้นเครื่อง Server จะทำการตอบรับแพ็กเก็ต Syn กลับไปที่เครื่อง Client เป็นแพ็กเก็ต Syn/ACK เมื่อเครื่อง Client ได้รับการตอบรับจากเครื่อง Server ก็จะทำการส่ง แพ็กเก็ต ACK กลับไปที่เครื่อง Server เพื่อเป็นการยืนยันและเริ่มต้นการส่งข้อมูลต่อไป สำหรับ ขั้นตอนการส่งแพ็กเก็ต Syn – Sync/ACK – ACK ที่มีลำดับขั้นตอนแบบนี้ จะถูกเรียกว่ากระบวนการ Three Way Handshaking ของโพรโทคอล TCP นั่นเอง เมื่อสิ้นสุดกระบวนการ Three Way Handshaking แล้ว เครื่อง Client ที่ต้องการรับข้อมูลจะส่งแพ็กเก็ต REQ ไปแจ้งให้ Server ส่งข้อมูล ึกลับมาให้ เมื่อเครื่อง Server ได้รับ REQ แล้วเครื่อง Server ก็จะเริ่มส่งข้อมูลมายังเครื่อง Client โดยในขั้นตอนนี้จะมีการแจ้งขนาดของ Window Size ที่ใช้ในการรับส่งข้อมูลระหว่างกันด้วย เป็น การกำหนดขนาดของการส่งข้อมูลให้มีความสัมพันธ์กันกับข้อมูลที่ถูกรับและส่ง โดยกระบวนการนี้จะ ้อยู่ในส่วนของ Data Transfer และ ขั้นตอนสุดท้าย เมื่อเครื่อง Server ส่งข้อมูลให้กับเครื่อง Client ้จนครบแล้ว เครื่อง Server จะทำการส่งแพ็กเก็ต FIN ไปแจ้งให้เครื่อง Client ทราบว่าสิ้นสุดการส่ง ้ข้อมูลแล้ว หลังจากนั้นเครื่อง Client จะทำการตอบกลับมาด้วยแพ็กเก็ต FIN/ACK เพื่อตอบรับ การปิดการสื่อสาร เมื่อเครื่อง Server ได้ รับแพ็กเก็ตแล้วก็จะส่งแพ็กเก็ต ACK ตอบกลับ เพื่อทำการ ้ปิดการสื่อสารเช่นกัน เป็นอันจบกระบวนการสื่อสารในแบบ TCP กระบวนการนี้จะอยู่ในส่วน ของ Close Connection สำหรับกระบวนการทั้งหมดจะแสดงดังภาพที่ ๓๓

จากคำอธิบายข้างต้นเมื่อนำมาประยุกต์ใช้ในการแก้ไขปัญหาที่เกี่ยวข้องกับระบบเครือข่าย สรุปเป็นข้อ ๆ จะได้ดังต่อไปนี้

๓.๓.๓.๑ ถ้าไม่พบแพ็กเก็ต SYN จากเครื่อง Client ไปที่เครื่อง Server จะทำให้พบ ปัญหาที่เกี่ยวกับการเชื่อมต่อ คือเครื่อง Client ไม่สามารถเชื่อมต่อกับ Server ได้

๓.๓.๓.๒ ถ้าเครื่อง Client ไม่ส่งแพ็กเก็ต ACK กลับไปที่ Server ก็จะไม่สามารถ ติดต่อกับ 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 ตัวอย่างการสื่อสารโดยใช้โพรโทคอล TCP เนื้อหาที่กล่าวมาเป็นเพียงตัวอย่าง การสรุปข้อมูลเบื้องต้นที่ได้จากรูปแบบการสื่อสารโดยใช้โพรโตทคอล TCP เท่านั้น ไม่ใช่ข้อมูลทั้งหมด การจะแสดงให้เห็นตัวอย่างคร่าว ๆ ในการสรุปปัญหาที่อาจจะเกิดขึ้นในระบบเครือข่ายเมื่อมีการใช้ งานจริงนั้นยังคงเป็นเรื่องที่ต้องทำความเข้าใจและทดลองต่อ ๆ ไป โดยบางหน่วยงานอาจจะพบ รูปแบบของแพ็กเก็ตที่แตกต่างจากที่ได้กล่าวไปในเบื้องต้นก็ได้ ซึ่งหากเรามีความเข้าใจถึงรูปแบบของ การสื่อสารได้แล้ว การวิเคราะห์และแก้ปัญหาที่เกิดขึ้นก็จะอาศัยหลักการจากพื้นฐานการสื่อสารที่เรา ได้เรียนรู้กันมานั่นเอง ทั้งนี้ การเก็บข้อมูลในระบบเครือข่ายจะนิยมใช้โปรแกรม Wireshark โดยทั่วไปแล้วข้อมูลจะอยู่ในรูปแบบของไฟล์นามสกุล .pcap หรือ .pcapng ทั้งที่ได้จากตัวโปรแกรม Wireshark หรือจากโปรแกรม TCPDump บนระบบปฏิบัติการ Linux แต่ตัวโปรแกรม Wireshark ก็ยังสนับสนุนการอ่านข้อมูลจากไฟล์ชนิดอื่น ๆ ได้ด้วย เช่น .cap เป็นต้น

จากภาพที่ ๓๓ จะเห็นได้ว่าเราสามารถทำการเลือกระบบเครือข่ายที่ถูกแสดงอยู่ได้ใน โปรแกรม Wireshark โดยโปรแกรมจะแสดงข้อมูลมาให้ทุกเครือข่ายที่มีการเชื่อมต่ออยู่กับ คอมพิวเตอร์ เมื่อเราทำการเลือกแล้ว โปรแกรม Wireshark ก็จะเริ่มทำการเก็บข้อมูล จากเครือข่าย ที่เราเลือกมาทั้งหมด สำหรับเครือข่ายที่สามารถใช้งานได้จะแสดงดังภาพที่ ๓๔

Interface	Traffic	Link-layer Header	Promit	
> VirtualBox Host-Only Ne	etwork	Ethernet		
> Local Area Connection* Local Area Connection*	13 10	Ethernet		1
Local Area Connection*	9	Ethernet		
> VMware Network Adapt Local Area Connection*	11	Ethernet	NN	1
> VMware Network Adapt > Bluetooth Network Con	nection 2	Ethernet		1
> VMware Network Adapt	er VMnet0 A	Ethernet		
< .			>	F
	o all interfaces	Manapa	e Interfac	

ภาพที่ ๓๔ รูปแสดงเครือข่ายบนคอมพิวเตอร์ที่โปรแกรม Wireshark ตรวจจับได้

เมื่อโปรแกรม Wireshark เริ่มทำการเก็บข้อมูลจากเครือข่ายที่ได้เลือกไว้แล้ว Wireshark จะแสดงผลข้อมูลออกมาด้วยหน้าโปรแกรมดังภาพที่ ๓๕

No.	Т	ime		S	surce		De	stinat	ion		Protocol	Frame Le	ength	Info
	55	25.007	311	1	11.22	1.77_	19	2.16	8.1.	102	TCP	5	4	40018 → 50808 [ACK] Seq=19 Ack=7 Win=83 Len=0
	56	25.110	814	1	52.12	5.17.	19	2.16	8.1.	102	TLSv1.	2 38	8	Application Data
	57	25.118	831	1	92.16	8.1	16	2.12	5.17	.3	TLSv1.	2 49	3	Application Data
	58	25.234	470	1	92.16	8.16_	19	2.16	8.16	0.2	NBNS	11	0	Refresh NB LENOVO-E130<20>
	59	25.480	144	1	92.16	8.1	15	7.55	.235	.1_	UDP	18	3	64930 + 40018 Len=141
	60	25.495	295	1	92.16	8.1	16	2.12	5.17	.3	TCP	49	3	[TCP Retransmission] 50793 + 443 [PSH, ACK] Seq=1 Ack=33
	61	25.509	785	1	52.12	5.17.	19	2.16	8.1.	102	TCP	5	4	443 + 50793 [ACK] Seq=335 Ack=440 Win=83 Len=0
	62	25.788	741	1	57.55	.235.	19	2.16	8.1.	102	UDP	6	3	40018 → 64930 Len=21
	63	25.802	813	1	52.12	5.17_	19	2.16	8.1.	102	TCP	6	6	[TCP Dup ACK 61#1] 443 + 50793 [ACK] Seq=335 Ack=440 Win
¢								• • • •						3
> Fr	ame 1:	66 byt	es c	n wi	re (5	28 b	its)	, 66	byt	tes d	apture	d (528 b	its)	on interface 0
> Et	hernet	II, Sr	CI 6	58:17	12914	7:03	:77,	Dst	ti fi	3:d1:	11:96:	90:c2		
> In	ternet	Protoc	01 1	/ersi	on 4,	Snc	: 19	2.16	8.1.	. 102,	, Dst:	119.235.	235.8	4
> Tr	ansmis	sion Co	ntro	1 Pr	otoco	1, S	rc P	ort	507	736,	Dst Po	rt: 443,	Seq:	1, Ack: 1, Len: 12
> Tr	anspor	t Layer	Sec	urit	У									
0000	f8 d	1 11 96	90	c2 6	8 17	29 4	7 c	3 77	68	00 4	5 00	· · · · · h	·)6·	w · · E ·
0010	00 34	4 74 02	40	00 8	0 06	61 7	3 c	0 a8	01	66	7 eb	-4t ·@··	· as ·	· · fu ·
0020	eb 5	c6 30	01	bb d	a 88	08 b	7 0	9 01	cd	ce 5	0 18	-1-0		· · · P ·
0030	00 fe	86 fb	60	00 8	0 02	00 0	6 0	0 00	00	04 0	0 00	******		4.9.7.4.8
0040	00 7	1										· 0		

ภาพที่ ๓๕ การแสดงรายละเอียดของแพ็กเก็ตที่โปรแกรม Wireshark

เมื่อทำการเก็บข้อมูลเพื่อนำไปใช้งานได้ตามที่ต้องการแล้วให้ทำการบันทึกเป็นข้อมูลเพื่อนำไป วิเคราะห์ผลที่ได้ภายหลัง โดย Wireshark สามารถทำการบันทึกข้อมูลเก็บไว้ได้ในหลากหลายรูปแบบ ไฟล์ชนิดต่าง ๆ ที่โปรแกรม Wireshark สามารถจัดเก็บได้

การเก็บข้อมูลด้วย TCPDump โดยปกติแล้วระบบปฏิบัติการตระกูล Unix/Linux จะมีแพ็กเก็ต โปรแกรมพื้นฐานสำหรับการเก็บข้อมูลแพ็กเก็ตมาให้เป็นพื้นฐานเป็นปกติอยู่แล้วไม่จำเป็นต้องติดตั้ง เพิ่มนั่นคือ TCPDump โดย TCPDump สามารถทำการเก็บข้อมูลแพ็กเก็ตได้เหมือนกับโปรแกรม Wireshark สำหรับการใช้งาน TCPDump นั้น จะมีการทำงานในลักษณะ Command Line ซึ่งจะต้องมี การระบุคำสั่ง เช่น โพรโทคอล เครือข่าย และขนาดของข้อมูลที่ต้องการจัดเก็บ เป็นต้น

๓.๓.๘ รูปแบบคำสั่งในการใช้งาน TCPDump จะมีโครงสร้าง ดังนี้

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

root@localhost:~		- 0	- ×	
<pre>win 260, length 0 21:51:39.024194 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla :63500, ack 601, win 292, length 300</pre>	gə [P.],	seq	63192	^
21:51:39.827811 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Fla 65, ack 62088, win 260, length 84	gs [P.],	seq	681:7	
21:51:39.831533 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Fla 17. ack 62088, win 260, length 52	gs [P.],	aed	765:8	
21:51:39.831561 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla	gs [.], a	ick 8	17, w	
21:51:39.869038 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Fla win 256, length 0	ga [.], a	ick 6	3192,	
21:51:39.869050 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla	gs [P.],	seq	63500	
21:51:39.869762 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla	gs [P.],	seq	64220	
21:51:39.870759 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla	gs [P.],	seq	64480	
21:51:39.937682 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Fla win 256, options (nop.nop.sack 1 (63500:64220)), length 0	g≊ [.], 4	ick 6	3192,	
21:51:39,937693 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fia	g≋ [₽.],	seq	64644	
21:51:39.941158 IP 10.200.200.21.61230 > 10.100.70.20.ssh: Fla win 256, options [nop.nop.sack 1 (63500:64680]], length 0	gs [.], a	ick 6	3192,	
21:51:39.941170 IP 10.100.70.20.ssh > 10.200.200.21.61230: Fla	gs [P.],	seq.	64808	v

ภาพที่ ๓๖ แสดงผลการใช้งาน TCPDump เพื่ออ่านข้อมูลแพ็กเก็ตที่ได้บันทึกเก็บไว้

๓.๓.๙ การเก็บข้อมูลด้วย Microsoft Network Monitor (GUI) สำหรับบางองค์กรที่มี กฏระเบียบเคร่งครัดในการจัดการโปรแกรมต่าง ๆ ที่ติดตั้งลงในเครื่อง เช่น มีข้อกำหนดให้ใช้ โปรแกรมที่ต้องได้รับรองความถูกต้องปลอดภัยจาก Microsoft เท่านั้น ในกรณีที่ไม่ได้รับอนุญาตจะ ไม่สามารถติดตั้งโปรแกรมได้ ในกรณีที่ Microsoft Network Monitor จะเป็นตัวช่วยในการ แก้ปัญหาในส่วนของการเก็บข้อมูลเครือข่ายจากเครื่องที่ต้องการได้เช่นเดียวกัน สำหรับการทำงาน ของ Microsoft Network Monitor ก็จะมีหลักการเดียวกันกับโปรแกรม Wireshark แต่สามารถ แยกแยะข้อมูลที่มี อยู่ออกมาได้ตามโปรแกรมที่มีการใช้งานอยู่

10	Microsoft Network Monitor 3.4 -	×
File Edit View Frames	Capture Filter Experts Tools Help	
New Capture Open C Capture1 😤 Start Page	apture 🙀 Save As 🌾 Capture Settings 🕨 Stint 🔳 Pause 📑 Stop	-
Network Conversa X	Display Filter	×
A Traffic My Traffic Cutaroant> B C drone.exc (45 C drone.exc (45 C drone.exc (9 C drone	🔀 Apply 🐇 Remove 🛛 🖓 History + 🏹 Load Filter + 🖓 Save Filter 🥥 Clea	e Test
	Frame Summary	×
	🖏 Find 👻 🕹 🕇 📪 Autoscroll 🗱 Color Rules 🎊 Aliases 👻 Ecolu	mns +
	Frame Number Time Date Local Adjusted Time Offset Process Name Source Destination Protocol Name D	* 04M
	Image: Constraint of the	, 22225F
	Frame Details X Hex Details	×
	- Trame: Humber = 1, Captured Frame Lengt - Trame: Humber = 1, Captured Frame Lengt - NetmonFilter: Updated Capture Filter: 3 0000 00 01 00 00 00 00 00 01 0000 00 03 00 04 09 22 0000 00 00 43 00 32 00C.: 0012 5C 00 57 00 72 00P.r. 0018 6F 00 67 07 72 00P.r.	Fra ^
< >	> 001E 61 00 6D 00 20 00 m.m.	~1
Parsed: 88	Displayed: 89 Dropped: 0 Ceptured: 89 Pending: 0 Focused: 1 Selected: 1	1.4

ภาพที่ ๓๗ โปรแกรม Microsoft Network Monitor

การเก็บข้อมูลด้วย Microsoft "netsh" (Command Line) กรณีนี้เป็นการใช้งาน โปรแกรมที่มากับ Microsoft Windows เช่นเดียวกันกับ Network Monitor แต่จะมีข้อได้เปรียบ มากกว่า Microsoft Network Monitor ตรงที่ netsh เป็นคำสั่งที่ถูกติดตั้งมาพร้อมกับ Windows เลยตั้งแต่ตอนติดตั้งไม่จำเป็นต้องดาวน์โหลดและติดตั้งโปรแกรมเพิ่มเติมอีก สำหรับการใช้งาน netsh จะเป็นในลักษณะ Command Line เท่านั้น ซึ่งอาจจะไม่สะดวกสำหรับท่านที่มีความคุ้นเคยกับการใช้งาน โปรแกรมในลักษณะของ GUI สำหรับตัวอย่างการใช้งานโปรแกรม Microsoft netsh จะเป็นดังภาพที่ ๓๘

<pre>^ ^ C:\Windows\system32>netsh trace start persistent=yes capture=yes tracefile=d:\ne ttrace.pcap Trace configuration: Status: Running Trace File: D:\nettrace.pcap Append: Off Gircular: On Max Size: 250 MB Report: Off C:\Windows\system32>netsh trace stop Correlating traces done Merging traces done Merging traces done The trace file and additional troubleshooting information have been compiled as "d:\nettrace.cab". File location = d:\nettrace.pcap Tracing session was successfully stopped.</pre>	23	Administrator: Command Prompt		×					
Trace configuration: Status: Running Trace File: D:\nettrace.pcap Append: Off Circular: On Max Size: 250 MB Report: Off C:\Windows\system32>netsh trace stop Correlating traces done Merging traces done Merging traces done The trace file and additional troubleshooting information have been compiled as "d:\nettrace.cab". File location = d:\nettrace.pcap Tracing session was successfully stopped.	C:\Windows\syste ttrace.pcap	m32>netsh trace start persistent=yes capture=yes trace	file=	1:\ne ^					
Status: Running Trace File: D:\nettrace.pcap Append: Off Circular: On Max Size: 250 MB Report: Off C:\Windows\system32>netsh trace stop Correlating traces done Merging traces done Generating data collection done The trace file and additional troubleshooting information have been compiled as "d:\nettrace.cab". File location = d:\nettrace.pcap Tracing session was successfully stopped.	Trace configuration:								
C:\Windows\system32>netsh trace stop Correlating traces done Merging traces done Generating data collection done The trace file and additional troubleshooting information have been compiled as "d:\nettrace.cab". File location = d:\nettrace.pcap Tracing session was successfully stopped.	Status: Trace File: Append: Circular: Max Size: Report:	Running D:\nettrace.pcap Off On 250 MB Off							
	C:\Windows\syste Correlating trac Merging traces . Generating data The trace file a "d:\nettrace.cab File location = Tracing session	m32>netsh trace stop es done done collection done nd additional troubleshooting information have been co " d:\nettrace.pcap was successfully stopped.	mpiled	1 as					

ภาพที่ ๓๘ ตัวอย่างการใช้งาน Microsoft netsh เพื่อเก็บข้อมูลในระบบเครือข่าย

๓.๓.๑๐ การเก็บข้อมูลด้วยการทำ Remote capture (Wireshark+ TCPDump) สำหรับ การใช้งานในรูปแบบ 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 คือสามารถทำการมอนิเตอร์ข้อมูลที่เกิดบน เครื่อง Linux เครื่องใดก็ได้ที่สามารถเข้าถึงได้ และนำข้อมูลที่ได้มาแสดงผลที่ Wireshark บน Windows ได้ในทันทีเพื่อแก้ปัญหาในกรณีที่ต้องการวิเคราะห์ปัญหาที่เกิดขึ้นในลักษณะ Real Time แต่การทำงานในลักษณะนี้ก็จะมีข้อเสียด้วยเช่นกัน คือ ในกรณีข้อมูลที่ได้มาจากการใช้งาน TCPDump มีมากเกินไปอาจจะทำให้เกิดการรบกวนการทำงานของอุปกรณ์อื่น ๆ ในระบบ ซึ่งจะทำ ให้การใช้งานเครือข่ายโดยรวมซ้าลงได้ สำหรับสคริปต์เพื่อการใช้งาน Remote Capture ดังภาพที่ ๓๙ จะเห็นได้ว่าในคำสั่งตัวอย่าง Script เพื่อให้สามารถ Remote Capture ได้ จะต้องมีการใช้งาน โปรแกรม plink โดยโปรแกรมจะต้องติดตั้งอยู่ที่ C:\Telnet\plink.exe -ssh -pw [password] root@[P 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 นั่นเอง การเก็บข้อมูลด้วยวิธีการพิเศษ การเก็บข้อมูลด้วย Network TAP การเก็บข้อมูลด้วย Network TAP เป็นวิธีการที่อาศัยการทำงานพื้นฐานคือการเชื่อมต่อกันของ วงจรไฟฟ้า เริ่มตั้งแต่การต่อสายแลนเข้า หากันแบบง่าย ๆ ไปจนถึงการออกแบบเป็นฮาร์ดแวร์เพื่อการใช้งาน เพื่อใช้งานเฉพาะทาง เช่น Network TAP แบบสาย UTP CAT5/6 และแบบสาย Fiber Optic เป็นต้น โดยทั่วไป Network TAP จะถูกนำมาใช้งานในบางสถานการณ์ ได้แก่ นำมาใช้ในการวิเคราะห์ ปัญหาทางด้านระบบเครือข่ายที่ ต้องการตัดประเด็นการทำงานที่ผิดพลาดของอุปกรณ์ออกไปอย่างชัดเจน เช่น ไม่แน่ใจว่าการที่ระบบ เครือข่ายมีปัญหานั้นเกิดจากการที่สวิทช์ทำงานผิดปกติหรือไม่ เป็นต้น การใช้งาน Network TAP จึง เป็นทางออกที่น่าสนใจสำหรับกรณีนี้ หรือการนำ Network TAP ไปใช้งานกับการ Audit PCI-DSS ของเครื่อง POS ที่ไม่สามารถทำการติดตั้งโปรแกรมต่าง ๆ เพิ่มเติมได้และอุปกรณ์ POS เองก์ไม่ รองรับการทำงานในการเก็บข้อมูลเครือข่าย



ภาพที่ ๔๐ Network TAP

๓.๓.๑๒ การสื่อสารระหว่างอุปกรณ์เมื่อสวิทช์ทำงานตามปกติ อุปกรณ์ Network Tap ก็มีข้อเสียในการใช้งานด้วยเช่นกันคือ กรณีใดก็ตามที่มีการใช้งาน Network TAP แบบ Passive หรือ Network TAP ที่ไม่มีการออกแบบที่ดีพอ ตัว Network TAP เองก็จะเป็นอุปกรณ์ที่ทำให้เกิดปัญหา ู้ขึ้นเสียเอง เนื่องจาก Network TAP จะทำให้สัญญาณที่ใช้ในการสื่อสารในระบบ LAN อ่อนลง ซึ่งจะทำให้รับข้อมูลผิดพลาดได้ อีกประเด็นหนึ่งคือ เมื่อต้องการนำ Network TAP มาใช้งาน ้จะต้องทำการถอดสายแลนของเครื่องที่ต้องการตรวจสอบออกและนำ Network TAP เข้ามาเชื่อมต่อ แทน ดังนั้นในกรณีนี้จะทำให้เกิด Downtime ขึ้นกับอุปกรณ์ การเก็บข้อมูลด้วยการใช้งาน SPAN และ RSPAN โดยปกติแล้วสวิทช์จะทำการเชื่อมต่อสื่อสารระหว่างเครื่องสองเครื่องที่มีการสื่อสารกัน โดยตรงไม่ได้การกระจายการสื่อสารนั้นออกไปทุกเครือข่าย (Broadcast) แบบเดียวกับฮับ (Hub) ซึ่งวิธีการนี้ทำให้การสื่อสารระหว่างคอมพิวเตอร์สองเครื่องที่เชื่อมต่อกันผ่านสวิทช์มีประสิทธิภาพสูง กว่าการใช้งานฮับ และยังเป็นการป้องกันการดักเก็บข้อมูลกลางทางระหว่างการสื่อสารของ ้คอมพิวเตอร์สองเครื่องได้ด้วยเช่นเดียวกัน แต่ในมุมมองของการแก้ปัญหาทางเครือข่ายโดยใช้งาน ้โปรแกรม Wireshark นั้นจะพบว่าเมื่อมีการใช้งานสวิทช์จะไม่สามารถนำข้อมูลของเครื่องที่มีปัญหา มาวิเคราะห์การทำงานได้ แต่หากต้องการข้อมูลจากสวิทช์โดยตรงมาใช้ในการวิเคราะห์ จะต้องใช้ ้ ฟังก์ชัน SPAN (Switch Port Analyzer) ซึ่งการใช้งาน SPAN หรือในอีกชื่อหนึ่งคือ Port Mirror เป็นเทคนิคในการสั่งให้สวิทช์ทำการคัดลอกข้อมูลจากเครือข่ายหนึ่งไปยังเครือข่ายอื่นที่ไม่ใช่ ปลายทางที่แท้จริงของอุปกรณ์นั้น การทำงานแบบนี้



มีลักษณะการทำงานคล้ายกับการทำงานของฮับ แต่จะเป็นการทำงานแบบเฉพาะเจาะจงบนเครื่อข่าย ที่ต้องการเท่านั้น

ภาพที่ ๔๑ การสื่อสารระหว่างอุปกรณ์เมื่อสวิทช์ทำงานตามปกติ



ภาพที่ d การทำงานของสวิทช์เมื่อมีการตั้งค่าให้ทำการทำงานในรูปแบบ SPAN

๓.๓.๑๓ คำสั่ง SPAN เป็นการนำข้อมูลเครือข่ายที่มีปัญหามาวิเคราะห์บนระบบเครือข่าย ขนาดใหญ่ ซึ่งในกรณีที่มีการเชื่อมต่อของสวิทช์หลาย ๆ ตัวเข้าไว้ด้วยกันมักจะทำได้ยาก เนื่องจาก การใช้งาน SPAN นั้น จะต้องทำการเชื่อมต่อเครื่องที่ติดตั้งโปรแกรม Wireshark เพื่อทำการวิเคราะห์ ปัญหาไปอยู่บนสวิทช์ตัวเดียวกันกับสวิทช์ของอุปกรณ์ที่ต้องการตรวจสอบข้อมูลบนระบบเครือข่ายใน กรณีที่มีปัญหา ซึ่งในกรณีนี้อาจจะทำได้ยากหรือมีความไม่สะดวก เช่น สวิทช์อยู่คนละอาคาร หรืออยู่ ในห้องศูนย์ข้อมูลซึ่งต้องมีการกำหนดเวลาในการเข้าออก ไม่อาจจะทำให้การวิเคราะห์หรือแก้ไข ปัญหาได้ ดังนั้นจึงมีวิธีการพัฒนาฟังก์ชันการทำงานแบบ Remote Switch Port Analysis : (RSPAN) เพื่อแก้ไขปัญหาดังกล่าว การทำงานของ RSPAN จะต้องทำการเพิ่ม VLAN พิเศษขึ้นมาอีกหนึ่ง VLAN เพื่อนำ VLAN ที่เพิ่มมาใช้งานเป็น Remote VLAN สำหรับการส่งข้อมูล SPAN ไปที่สวิทช์อื่น ตัวอย่างการทำงานของ RSPAN ดังภาพที่ ๔๓



ภาพที่ ๔๓ ตัวอย่างการทำงานของ RSPAN

จากภาพที่ ๔๓ เครื่องที่ทำการติดตั้งโปรแกรม Wireshark เพื่อทำการวิเคราะห์ข้อมูล คือ PC-Z ติดตั้งอยู่ที่ Switch A และเครื่อง PC-B เป็นเครื่องที่มีปัญหาเกิดขึ้น ผู้ดูแลระบบต้องการ ที่จะทำการ ส่งข้อมูลการ SPAN ของ Switch B กลับไปที่ Switch A ดังนั้นเมื่อการเชื่อมต่อไม่ได้อยู่ บนสวิทช์ตัวเดียวกัน จึงต้องใช้ฟังก์ชั่น RSPAN แทน SPAN ตามปกติ โดยสิ่งที่เพิ่มขึ้นมาคือการตั้งค่า Remote VLAN ตามที่ได้กล่าวไว้ข้างต้น และอนุญาตให้มีการส่งข้อมูลออกไปที่ Trunk ที่เชื่อมต่อกับ สวิทช์ทั้งสองตัว

๓.๓.๑๔ การเก็บข้อมูลด้วยการใช้ Hacking Technique การเก็บข้อมูลเครือข่ายแบบนี้เป็น วิธีที่ไม่แนะนำให้นำไปใช้งานในระบบจริง เนื่องจากเป็นการกระทำ ที่เข้าข่ายในการทำผิดกฏหมาย อาญารูปแบบหนึ่ง การแนะนำการทำงานของวิธีนี้จะใช้ตัวอย่างของเทคนิคที่ เรียกว่า ARP Spoofing ซึ่งถือเป็นรูปแบบหนึ่งของการทำ Man In The Middle (MITD) ยกตัวอย่างการทดลองในระบบปิด โดยใช้การจำลองการทำงานผ่านโปรแกรมจะลองระบบเครือข่าย คือ EVE-NG โดยใช้การทำงาน ร่วมกับโปรแกรม VirtualBox เพื่อให้เห็นการทำงานที่สมบูรณ์มากขึ้น สำหรับ การทำงานโดยละเอียด จะมีการกล่าวถึงในส่วนของการทำการทดลองต่อไป การเก็บข้อมูลในระบบเครือข่ายโดยการใช้งาน ARP Spoofing นี้จะเป็นการหลอกให้อุปกรณ์ PC-A ส่งข้อมูลการสื่อสารไปที่ PC-B ที่มีการทำ ARP Spoofing ไว้เพื่อทำการเก็บข้อมูลการเชื่อมต่อไปที่ภายนอกเครือข่ายที่โดยปกติจะต้องมีการส่งข้อมูล ไปที่เราท์เตอร์เมื่อมีการหลอกให้ PC-A ทำการส่งข้อมูล การสื่อสารไปที่ PC-B แทนดังนั้น PC-B จึงสามารถทำการบันทึกข้อมูลการสื่อสารของ PC-A ได้ ดังภาพที่ ๔๔



ภาพที่ ๔๔ ตัวอย่างการทำงานของ ARP Spoofing

C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?> C:\Users\VS-Vin ?>arp	.ece		
Interface: 10 1 1 2 - Internet Address 10.1.1.1 10.1.1.4 10.1.1.255 224.0.0.222 224.0.0.252 239.255.255.250 255.255.255.255	0xh Physical Address ca-01-24-5e-00-00 08-00-27-7b-01-99 11-11-11-11-11-11 01-00-5e-00-00-16 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa ff-ff-ff-ff-ff-ff	Type dynamic static static static static static 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 ๔๕ MAC table บนเครื่อง PC ก่อนการทำ ARP Spoofing

๓.๓.๑๕ ผลที่เกิดจากการทำ ARP Spoofing นั้นสามารถดูได้จากภาพที่ ๔๕ โดยปกติแล้ว PC-A จะมีตาราง ARP ของการเชื่อมต่อกับเราท์เตอร์ดังในรูป แต่เมื่อใดก็ตามที่ PC-A ถูกทำการดัก เก็บข้อมูลไปโดยการใช้งาน ARP Spoofing ในระบบเครือข่ายตาราง ARP ของเครื่อง PC-A จะเปลี่ยนไปดังในภาพที่ ๔๖ ซึ่งจะทำให้ PC-A ส่ง ข้อมูลการใช้งานระบบเครือข่ายไปที่ PC-B ที่กำลัง ทำ ARP Spoofing อยู่นั่นเอง หากสังเกตุ MAC Address ของรูปจะเห็นได้ว่าผลของการทำ ARP Spoofing จะทำให้ MAC Address ของ Router เปลี่ยนไปเป็น MAC Address ของ PC-B แทน

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		*
Internet Address 10.1.1.1 10.1.1.4	0xb Physical Address ca-01-24-9c-00-1c 08-00-27-7b-01-99	Type dynamic dynamic	
10.1.1.255 224.0.0.22 224.0.0.252 239.255.255.250 255.255.255.255	11-11-11-11-11-11 01-00-5e-00-00-16 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa ff-ff-ff-ff-ff-ff-ff	static static static static static 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 เป็นเมนูของเครื่องมือหลักเมื่อต้องการใช้งาน โปรแกรม 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 เพื่อนำมาแสดงผลและวิเคราะห์การ ทำงานในลำดับต่อไป

๓.๓.๑๖.๓ Packet List Pane เป็นส่วนที่ใช้แสดงรายละเอียดของแพ็กเก็ตที่เก็บ ข้อมูลมาได้ โดยจะแสดงรายละเอียดเบื้องต้นทั้ง IP Address โพรโทคอลและรายละเอียดเบื้องต้น ของแพ็กเก็ตนั้น ๆ

๓.๓.๑๖.๔ Packet Detail Pane เป็นส่วนที่ใช้แสดงรายละเอียดต่าง ๆ ของ แต่ละแพ็กเก็ตโดยละเอียด โดยจะแสดงข้อมูลในรายละเอียดไล่ขึ้นมาตั้งแต่ระดับเฟรมไปจนถึงข้อมูล ที่อยู่ใน Layer Application ๓.๓.๑๖.๕ Packet Byte Pane จะเป็นการแสดงข้อมูลของแพ็กเก็ตนั้นในรูปแบบ ของข้อมูลฐานสิบหกและตัวอักษร ASCII โดยในกรณีที่ข้อมูลไม่มีการเข้ารหัสจะสามารถทำการอ่าน ข้อมูลในส่วนนี้ออกมาได้ทันที สำหรับตำแหน่งของเมนูต่าง ๆ ของโปรแกรม Wireshark สามารถดู ได้ ดังภาพที่ ๔๗



ภาพที่ ๔๗ โปรแกรม Wireshark

๓.๓.๑๗ การสร้างและนำ Filter ไปใช้งานในโปรแกรม Wireshark เมื่อเราทำการเก็บข้อมูล ในระบบเครือข่ายขึ้นมาแล้ว ในขั้นตอนต่อไปเราจะต้องนำข้อมูลที่ได้มาศึกษาการทำงานหรือ วิเคราะห์หาการทำงานที่ผิดปกติ แต่โดยทั่วไปแล้วในขั้นตอนการเก็บข้อมูลส่วนใหญ่มักจะทำการเก็บ ข้อมูลมาในลักษณะให้ "เยอะที่สุดเอาไว้ก่อน" เพื่อในกรณีที่ไม่สามารถที่จะทำการเก็บข้อมูลซ้ำได้ บ่อย ๆ โดยอาจจะมีสาเหตุมาจากการต้องทำการขอ Change Request ตามขั้นตอน ซึ่งอาศัย ระยะเวลาและขั้นตอนในการดำเนินการที่นาน หรือเหตุที่เกิดขึ้นนั้นอาจจะไม่สามารถสร้าง สถานการณ์แบบเดียวกันได้อีก (Re - Produce) หรือเป็นเหตุการณ์ที่ต้องออกมาเก็บข้อมูลนอก สถานที่ซึ่งไม่สามารถออกมาได้บ่อย ๆ ดังนั้น เมื่อข้อมูลที่จัดเก็บมาได้มีขนาดใหญ่และมีความซับซ้อนสูง การใช้งาน Filter ในโปรแกรม Wireshark จึงเป็นเรื่องสำคัญ โดยเป็นขั้นตอนที่จะสามารถทำให้เรา ระบุขอบเขตของข้อมูลที่ต้องการได้ละเอียดและลึกขึ้นจากข้อมูลพื้นฐานที่มีขนาดใหญ่ โดยทั่วไปแล้ว การใช้งาน 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
โพรโทคอล	ใช้ระบุโปรโทคอลที่มีการใช้งานแบบเฉพาะเจาะจง	Ether, IP, UDP, HTTP

ตารางที่ ๑ คุณสมบัติของ Input Filter

๓.๓.๑๘ โดยในการใช้งาน Filter จะมี Input Filter อยู่เพียงแค่หนึ่งหรือทั้งสามก็ได้ 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 เลือกโพรโทคอล TCP Port 80 มาแสดงผล เป็นต้น

จากตัวอย่างที่ยกมาให้ดูทั้งสามแบบ จะเห็นได้ว่ามีการใช้งานเครื่องหมาย "==" 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
>=	มีค่ามากว่าหรือเท่ากับ
<=	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 โดยการใช้งานร่วมกับ การใช้เครื่องหมาย "()" เพื่อใช้ในการแยกกลุ่มของ Input Filter ให้ชัดเจนขึ้นได้ด้วยดังตัวอย่าง ต่อไปนี้

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 อะไรก็ได้ ที่ ไม่ใช่ 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 แทนได้ หรือไม่สามารถจำ Input Filter หรือ Operator แบบต่าง ๆ ได้ ตัวโปรแกรม Wireshark ก็จะมีตัว ช่วยอำนวยความสะดวกในการใช้งาน Filter ให้ โดยทำการคลิกที่ Filter บนเมนู ดังภาพที่ ๔๘



ภาพที่ ๔๘ การแยกกลุ่มของ Input Filter

ണ.ണ. ഇറ Display Filter

ในกรณีที่ต้องการเพิ่ม Operator เข้ามาใช้งาน ให้ทำการกด Filter แล้วจะมี หน้าต่างใหม่ถูกเปิดขึ้นมา ให้เราสามารถเลือกเป็น Display Filter แล้วทำการกด Expression เพื่อ เพิ่ม Option ก็จะพบคำสั่งต่าง ๆ สำหรับการใช้งาน Operator ดังภาพที่ ๔๙

The shore bisplay the s		
Name	Filter	^
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp	
No ARP and no DNS	not arp and !(udp.port == 53)	
нттр	http	
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80	
Non-DNS	!(udp.port == 53 tcp.port == 5	
UDP only	udp	
TCP only	tcp	
IPX only	ipx	
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1	
IPv6 only	ір∨б	
IPv4 address isn't 192.0.2.1 (don't use != for this!) !(ip.addr == 192.0.2.1)	
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1	~
<	>	
+ – Pa <u>C: Users Panya jAppData</u>	Roaming shark profiles Classic dfilt	e
OK	Cancel Help	

ภาพที่ ๔๙ Display Filter

๓.๓.๒๑ การใช้งาน Coloring Rules

Coloring Rules เป็นการให้สีกับข้อมูลตัวอักษรและ Background ที่แสดงขึ้นมาใน ช่องของ 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 กำกับอยู่ ด้วยเพื่อใช้ในการจับคู่สีของ Filter String ให้เข้ากับสีของ Coloring Rule แต่ละตัวนั่นเอง และใน กรณีที่จำค่าของ Filter ที่ต้องการใช้งานไม่ได้ ก็สามารถเข้ามาที่เมนู Coloring Rule และทำการนำ Filter String ไปใช้งานเป็นต้นแบบในการทำ Filter ได้ด้วยเช่นกัน



ภาพที่ ๕๐ Coloring Rule

ണ.ണ.യാ Coloring Rule

เนื่องจากโปรแกรม Wireshark มีการแสดงผลที่ซับซ้อนและ Coloring Rule ที่ได้ สร้างมาให้อาจจะไม่เพียงพอต่อการใช้งานของผู้ใช้ ดังนั้นโปรแกรม Wireshark จึงอนุญาตให้ผู้ใช้งาน สามารถสร้าง Coloring Rule เองได้ด้วยการกดปุ่ม New ใน Coloring Rule โดยเมื่อกดแล้วจะมี หน้าต่างขึ้นมาทำการตั้ง Coloring Rule ตัวใหม่ตามที่เราต้องการได้ โดยจะต้องทำการตั้งชื่อและ Filter ไว้ด้วย นอกจากนี้ยังสามารถทำการแก้ไขสีของ Foreground และ Background ได้ตามที่ ต้องการจากเมนูนี้ด้วย

๓.๓.๒๓ Statistics Conversations ในการใช้งาน Wireshark

โดยปกติแล้วจะมีแพ็กเก็ตที่เราทำการเก็บข้อมูลเข้ามาเป็นจำนวนมาก แต่ในการ ระบุปัญหาหรือการตรวจสอบการทำงานระหว่างเครื่อง Client และ Server จะมีการติดต่อกันเพียง สองเครื่อง เป็นการจับคู่การสื่อสาร ในกรณีที่เราต้องการหาคู่ระหว่าง Client และ Server สามารถดู ได้จากช่อง Packet List Pane ดังนั้น Wireshark จึงมีการเตรียมเมนูที่มีการแสดงผลการการสื่อสาร ระหว่างเครื่อง Client และ Server เอาไว้ให้ เพื่ออำนวยความสะดวกในการใช้งาน สำหรับการใช้งาน เมนูนี้สามารถเข้าไปที่เมนู Statistics -> Conversations โดยโปรแกรม Wireshark จะเปิดหน้าต่าง Conversations ขึ้นมาใหม่อีกหนึ่งอัน โดยจะแสดงรายละเอียดของการสื่อสารระหว่างเครื่องเป็นคู่ ๆ ไว้ให้ โดยสามารถทำการเลือกดูค่า Conversation ระหว่างเครื่องต่าง ๆ ตามโปรโทคอลที่ใช้งานได้ ดังภาพที่ ๕๑

Ethernet · 5	IPv4 · 122 1	Pv6 · 2	TCP · 16	7 UDP - 25						
Address A	Address B	Packets	Bytes	Packets A - B	Bytes A - B	Packets B - A	Bytes B - A	Rel Start	Duration	Bits/s A -
.218.118.65	192.168.43.197	8	5048	4	2694	4	2354	5.178709	32.2001	
3.32.43.102	192.168.43.197	2	109	1	54	1	55	23.333636	0.0231	1
3.35.19.7	192.168.43.197	6	355	3	193	3	162	4.173667	0.8088	1
3.57.172.231	192.168.43.197	42	15 k	24	8571	18	6784	4.781203	32.5313	2
3.59.135.168	192.168.43.197	8	510	5	347	3	163	18.494092	15.1152	
3.114.139.82	192.168.43.197	18	3116	10	2062	8	1054	4.967427	32.2481	
3.125.159.139	192.168.43.197	7	452	3	224	4	228	7.967177	0.2431	7
3.250.197.153	192.168.43.197	7	410	3	193	4	217	21.400058	17.1194	
3.251.254.220	192.168.43.197	7	410	3	193	4	217	18.094446	18.8631	
4.95.92.78	192.168.43.197	2	109	1	54	1	55	21.440974	0.0289	1
4.96.111.110	192.168.43.197	2	109	1	54	1	55	18.583251	0.0531	8
4 100 221 100	107 160 47 107	21	1220	0	\$70	17	651	10 41 4050	10 6600	
										,
Name resolutio	·	mit to disola	v filter	Abso	ute start time				Conver	sation Type

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 โดยจะเป็นการแสดงรายละเอียด ของข้อมูลที่อยู่ใน TCP Stream โดยทั่วไปแล้วการสื่อสารระหว่าง Client – Server จะมีการส่ง ข้ อ มู ล

ที่มากกว่าหนึ่งชุดข้อมูลระหว่างกัน โดยเมื่อมีการส่งข้อมูลหนึ่งชุดจบไปแล้ว จะมีการหยุดส่งข้อมูล ก่อน แต่กระบวนการของ TCP Connection จะยังไม่มีการตัดการเชื่อมต่อ โดยในโปรแกรม Wireshark จะเรียกการนับชุดข้อมูลที่มีการส่งในหนึ่งชุดนี้ว่า "Stream index" เพื่อใช้ในการอ้างอิง ชุดข้อมูล 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 จะเป็นการแสดงผลที่ได้จากการ เก็บข้อมูลการใช้งาน Telnet ของอุปกรณ์เครือข่าย โดยปกติแล้ว Telnet เป็นการสื่อสารในแบบที่ ไม่ได้ทำการเข้ารหัส การสื่อสาร ดังนั้น เราจะสามารถใช้ Follow TCP Stream เพื่อดูข้อมูลการ ใช้งาน Telnet ในการติดต่อ สื่อสารระหว่างเครื่องคอมพิวเตอร์ได้ ดังภาพที่ ๕๒

🚄 Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet.pcapng	-		×
User Access Verification			^
Username:Y			
Password: cisco			
R1#			
55 client ohte. 52 server ohte. 97 turne.			*
Entire conversation (836 bytes) V Show and save data as ASCII	~	Stream [0 🗘
Find:		Find Ne	ext
Filter Out This Stream Print Save as Back Ck	ose	Help	

ภาพที่ ๕๒ แสดงข้อมูลการ Login เข้าเราท์เตอร์ด้วย Telnet

๓.๓.๒๕ การใช้ Follow TCP Steam กับ SSH

เพื่อดูข้อมูลของโพรโทคอล SSH จากตัวอย่างการใช้งาน Telnet จะเห็นได้ว่าข้อมูล ที่ถูกส่งอยู่ในระบบเครือข่ายจะไม่ถูกเข้ารหัส ทำให้สามารถเห็นข้อมูลทั้งหมดได้ ดังนั้น SSH จึงถูก พัฒนาขึ้นมาเพื่อแก้ไขปัญหาดังกล่าว เช่น ข้อมูลถูกส่งเข้าไปที่อุปกรณ์เดียวกันแต่เมื่อมีการใช้งาน SSH จะทำให้ไม่สามารถเห็นข้อมูลที่ใช้ในการสื่อสารกันได้ แต่ยังคงใช้งานผ่าน Feature Follow TCP Steam เป็นต้น

๓.๓.๒๖ การใช้ Follow TCP Steam กับ HTTP

เพื่อดูข้อมูลของโปรโทคอล HTTP เช่นเดียวกันกับ Telnet และ SSH โปรโทคอล HTTP จะมีการสื่อสารผ่านโพรโทคอล TCP เราจึงสามารถใช้ Follow TCP Stream ได้ โดยจะเห็น ได้ว่าโปรโทคอล HTTP ไม่มีการเข้ารหัสในการสื่อสารเช่นเดียวกัน ดังนั้นข้อมูล HTML ในหน้าจอของ Follow TCP Stream ก็จะสามารถสังเกตได้เช่นเดียวกันกับ 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 ที่แฝงอยู่ในแพ็กเก็ตข้อมูล ที่ได้มาให้อยู่ในรูปแบบบของกราฟ ซึ่งจะทำให้เราสามารถนำความสัมพันธ์ของกราฟที่ได้มาใช้ในการ วิเคราะห์การทำงานหรือค้นหาปัญหาที่อาจจะเกิดขึ้นได้อย่างสะดวกแม่นยำ 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 ที่แพ็คเก็ตเดินทางในระบบเครือข่าย หลักการสังเกตุง่าย ๆ ในการนำ Round – Trip Time มาใช้ กล่าวคือ กราฟจะมีความหนาแน่นใกล้กับแกน X มากที่สุด หรือก็คือแพ็คเก็ตสามารถเดินทางใน เครือข่ายได้รวดเร็วนั่นเอง โดยแต่ละจุดในกราฟคือแพ็คเก็ตแต่ละชิ้นส่วน และจากกราฟแสดงให้เห็น ว่าค่า Round-Trip Time ของแพ็คเก็ตชุดนี้อยู่ในระดับที่ต่ำ เนื่องจากค่าเฉลี่ยของ RTT จะอยู่ ใกล้เคียงกับเวลา ๐.๑ วินาทีนั่นเอง



ภาพที่ ๕๔ แสดงค่า Round - Trip Time ของเครือข่าย

๓.๓.๒๗.๒ กราฟ Throughput เป็นกราฟที่ใช้แสดงค่า Throughput จาก Source -> Destination ในทิศทางเดียว ดังนั้นกรณีที่ต้องการดูค่า Throughput แล้วในกราฟไม่ แสดงค่าใด ๆ ขึ้นมา ให้ลองทำการสลับค่า Source <-> Destination ดูก่อนทุกครั้ง การใช้งานกราฟ Throughput โดยทั่วไปแล้วจะใช้สังเกตแนวโน้มของข้อมูลที่ผ่านเข้าออกในระบบเครือข่าย หรือ นำไปใช้ในการสังเกตการลดค่าหรือ Throughput Drop ในกรณีที่การสื่อสารมีปัญหา



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 เช่นเดียวกัน กับแบบ Steven แต่มีความพิเศษตรงที่กราฟแบบ Tcptrace จะแสดงค่า Window size และ ค่า 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 โดยแต่ละจดจะเป็นการแสดงขนาดของ Window size ในช่วงเวลานั้น ๆ การใช้งานกราฟนี้สามารถเห็นความเปลี่ยนแปลงได้อย่างชัดเจนของค่า Window Scaling แต่ข้อเสียของการใช้งาน TCP Stream Graph คือ กราฟที่แสดงผลนั้นในส่วนของ ้แกน x จะเป็นส่วนที่ใช้สำหรับการแสดงค่าเวลาที่เริ่มนับจาก "๐" กล่าวคือ เวลาที่เริ่มต้นในการเก็บ แพ็กเก็ตนั้นจะมีการนับต่อไปเรื่อย ๆ ซึ่งไม่ได้มีการแสดงค่าเวลาที่แท้จริงในขณะที่เริ่มทำการเก็บแพ็กเก็ต เช่น เราเริ่มทำการเก็บแพ็กเก็ตเพื่อนำมาวิเคราะห์การทำงานของโปรแกรมหนึ่งที่เวลา ๑๓๔๐ แต่การแสดง ้ค่าเวลาของ TCP Stream Graph จะทำการแสดงผลเริ่มต้นที่เวลาเท่ากับ "o" และเพิ่มขึ้นไปเรื่อย ๆ ไม่ได้แสดงค่าเวลาเป็น ๑๓๔๐ ตามเวลาจริงที่เราเริ่มทำการเก็บข้อมูล เป็นต้น ส่วนต่อมาก็คือการแสดงผลของ TCP Stream Graph นั้น จะเป็นการแสดงผลรวมทั้งหมดที่เกิดจากแพ็กเก็ตที่เราเก็บข้อมูลมาได้แล้ว ทำการบีบอัดการแสดงผลให้พอดีอย่ในหน้าเดียว ดังนั้นการแสดงผลจะไม่มีความละเอียดมากพอ เช่น กรณีที่เราทำการเก็บข้อมูลแพ็คเก็ตในระยะเวลา ๕ นาที และนำมาแสดงผลที่ TCP Stream Graph จะมีการแสดงผลในแกน x เท่ากับข้อมูลแพ็กเก็ตที่ใช้ระยะเวลาในการเก็บเป็นระยะเวลา ๒ หรือ ๔ ชั่วโมงก็ได้ ดังนั้นต้องระมัดระวังในการนำ TCP Stream Graph ไปใช้งานในส่วนนี้ด้วย การจัดการไฟล์ .pcapng ในหลายสถานการณ์เรามีความจำเป็นที่จะต้องมีการลองดึงข้อมูลที่ต้องการ ้วิเคราะห์ปัญหาออกมาจากอุปกรณ์ Network เป็นระยะเวลานานแบบต่อเนื่อง เพื่อให้ได้ข้อมูลที่มาก พอ หรือเพื่อให้ครอบคลุมช่วงเวลาที่เกิดปัญหาเพื่อที่จะนำข้อมูลที่ได้มาใช้งานต่อไป ถึงแม้ในบางครั้ง ข้อมูลที่เราอยากได้นั้นอาจจะมีจำนวนแค่หลักสิบหรือหลักร้อยแพ็กเก็ต (Packet) ไม่สามารถคาดเดา ้ได้ว่าปัญหาที่เกิดขึ้นนั้นจะเกิดขึ้นในช่วงใดได้บ้าง ทำให้เราอาจต้องเก็บข้อมูลค้างไว้นานหลายชั่วโมง หรืออาจจะต้องเก็บข้อมูลกันข้ามวันเลยทีเดียว

จากภาพที่ ๕๘ เป็นข้อมูลตัวอย่างจากการเก็บข้อมูลเพื่อนำไปวิเคราะห์การปัญหาที่ เกิดขึ้นในช่วง เวลาประมาณไม่เกินสามชั่วโมง จะเห็นได้ว่าไฟล์มีขนาดใหญ่ถึง 3.7GB

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

a		ا ل	ಷ	ка и ,	6 9 0	9 20	୧୧
ภาพท่	ھھ	ตวอยางขนาดขอ	งแพตเ	กตเฟ	ลท่น้ำม	าโชว์เค	ราะหปุ่อเหา
••••••	~				0		

ดังภาพที่ ๕๘ ถ้าจะนำไฟล์มาใช้งานจะเกิดเหตุการณ์อะไรบ้าง ทั้งในระหว่างการเก็บข้อมูล เพื่อให้ได้ไฟล์มา หากจะสรุปเหตุการณ์ที่เป็นไปได้ จะสามารถเขียนออกมาได้ ดังนี้

(๑.) ระหว่างเก็บข้อมูลของไฟล์ a. ถ้า Disk ที่ใช้เก็บข้อมูลมีขนาดไม่พอเนื่องจากประเมินไม่ได้ ว่าจะต้องเก็บไฟล์ขนาดไหนจะเป็นอย่างไร กรณี Disk IO ที่ใช้รองรับการเขียนไฟล์จะพอหรือไม่ ถ้าไม่พอก็ได้ข้อมูลไม่ครบตามต้องการ หรือเมื่อเก็บข้อมูลเสร็จแล้วจะทำการ Save ข้อมูลเพื่อนำไป ใช้งานต่อจะสามารถดำเนินการได้หรือไม่

(๒.) ระหว่างนำไฟล์ไปใช้ เครื่องที่นำไฟล์นี้ไปเปิดใช้งานจะสามารถเปิดไฟล์นี้ได้หรือไม่ ในการประมวลผลจากไฟล์นี้จะต้องใช้เครื่องที่มีประสิทธิภาพขนาดไหน ในการกรองหาข้อมูล ที่ต้องการและนำมาแสดงผล จะสามารถแสดงผลได้หรือไม่ ราวกับว่าไม่อาจนำข้อมูลไปใช้งานต่อได้ ดังนั้น เพื่อให้สามารถนำข้อมูลที่ได้ไปใช้งานต่อได้อย่างมีประสิทธิภาพ สิ่งที่สำคัญที่สุดก่อนการเริ่ม เก็บข้อมูลคือ การวางแผนและเตรียมการให้เหมาะสมทั้งก่อนและหลังการเก็บข้อมูล เช่น บริษัท A มีปัญหาการใช้งาน Application ของฝ่ายบัญชีตัวหนึ่งในช่วงเวลาประมาณ ๑๖๓๐ ของทุกวัน เป็นระยะเวลาติดต่อกันมานานกว่า ๓ เดือน โดยไม่ทราบสาเหตุ โดยอาการคือในช่วงเวลา ๑๖๓๐ - ๑๗๓๐ ฝ่ายบัญชีจะไม่สามารถดึงข้อมูลจาก Database ได้ หรือถ้าดึงข้อมูลได้ก็จะใช้เวลานานกว่าปกติมาก เป็นต้น



ภาพที่ ๕๙ ตัวอย่างการกำหนดขอบเขตเพื่อจำกัดการเก็บข้อมูลเพื่อแก้ปัญหาของบริษัท A

แนวทางในการแก้ไขปัญหา เพื่อที่จะได้เห็นการเปลี่ยนแปลงทั้งก่อนและหลัง ช่วงเวลาที่เกิดปัญหา เราอาจจะต้องเก็บข้อมูลในระหว่างเวลา ๑๖๐๐ - ๑๘๐๐ ก่อนที่ปัญหา จะเกิดขึ้น โดยอาจเลือกเก็บข้อมูลแค่ฝ่ายบัญชีก็ได้ แต่ในการเก็บข้อมูลที่ต้องการวิเคราะห์ ควรจะมี แค่การใช้งานในส่วนของ Datacenter และฝ่ายบัญชีเท่านั้น การใช้งาน Internet ไม่ควรเก็บมาด้วย ทั้งนี้การเก็บข้อมูลต่อเนื่องยาวนาน ๒ ชั่วโมงอาจจะทำให้ได้ไฟล์ขนาดที่ใหญ่มาก 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 แต่ก็จะเห็นได้ว่าปัญหาที่เกิดขึ้นมีเฉพาะเวลาแบบเจาะจงและเกิดขึ้นเฉพาะตอน 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 เป็น

ต้น

๓.๓.๒๘.๓ แบ่งโดยใช้ระยะเวลา เช่น ให้แบ่งไฟล์ใหม่ทุก ๆ ๕ นาที เป็นต้น

ทั้งนี้ การแบ่ง่ไฟล์โดยกำหนดจากขนาดของ่ไฟล์จะสะดวกมากที่สุด เนื่องจากในการทำงานจริง ส่วนมากปัญหาที่พบจะไม่สามารถกำหนดระยะเวลาที่แน่นอนได้ ทำให้บางครั้งอาจจะใช้เวลามากกว่า ๑๒ ชั่วโมง และข้อมูลในแต่ละช่วงเวลาก็มีขนาดไม่เท่ากัน เช่น ถ้าเก็บข้อมูลในช่วงเช้า พนักงานทุกคนจะใช้ ระบบ Network เป็นจำนวนมาก เนื่องจากต้องเข้าใช้งานระบบพร้อม ๆ กัน และจะเริ่มลดปริมาณ การใช้งานลงหลังจากนั้นอีกประมาณ ๒ ชั่วโมง และเริ่มมีการใช้งานมากอีกครั้งหลังจากช่วงพัก กลางวัน หรือกรณีของ ISP ที่ให้บริการ FTTH จะมีปริมาณการใช้งานมากเป็นพิเศษในช่วงเย็นไป จนถึงเวลาประมาณเที่ยงคืนหรือถึงตีสาม และจะลดลงในช่วงเวลากลางวัน ทั้งนี้การแบ่งข้อมูล ออกเป็นส่วน ๆ ตามขนาดของข้อมูลที่ได้จึงเหมาะสมในกรณีแบบนี้ โดยขนาดของไฟล์ที่เหมาะสมจะ อยู่ที่ประมาณ 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 ถ้าหากเราไม่สามารถ เห็นภาพรวมของระบบ เป็นต้น ทำให้ในหลายครั้งการตัดสินใจแก้ปัญหาอาจจะทำไปโดยไม่มีข้อสรุป ที่ชัดเจน เช่น จากภาพที่ ๖๑ เราไม่พบว่าเกิดการ Authentication ที่จุดที่ ๒ ซึ่งบางครั้งผู้วิเคราะห์ ระบบอาจจะตีความไปว่าอุปกรณ์ Gateway มีปัญหา เพราะไม่ส่ง Authentication Message ออกมาทั้ง ๆ ที่อาจจะเป็นที่อุปกรณ์ Access หรือ PPPoE Client ไม่มีการส่ง Message ออกมาก็ เป็นได้ ทั้งนี้การมาเปิด Session ก่อนแล้วจึงจะเกิด Authentication Message จาก Gateway ไปที่ AAA นั้นก็สามารถเกิดขึ้นได้เช่นกัน เป็นต้น



ภาพที่ ๖๑ การเก็บข้อมูลและมองปัญหาจากจุดต่าง ๆ ใน Network

ดังภาพที่ ๖๑ จะเห็นได้ว่าถ้าพบปัญหาเพียงจุดเดียวเราอาจจะวิเคราะห์ปัญหา ผิดพลาดได้ ดังนั้น การเก็บข้อมูลให้ครบถ้วนจากจุดต่าง ๆ ในระบบ Network เป็นเรื่องที่ต้อง ทำ เพื่อให้สามารถเห็น แพ็กเก็ต ในภาพรวมได้อย่างถูกต้องครบถ้วน แต่การเก็บ แพ็กเก็ต เข้ามาจาก จุดต่าง ๆ ใน ระบบ Network โดยทั่วไปแล้วจะเก็บมาจากอุปกรณ์ต่างชนิดกัน กรณีที่ต้องการเก็บ ข้อมูลจาก Network ในจุดที่ ๑ - ๓ อาจจะต้องใช้ Server ถึง ๓ ตัวแยกกันในการเก็บข้อมูล เมื่อได้ ข้อมูลที่ต้องการแล้ว โดยทั่วไปจะทำการเปิดไฟล์แต่ละชุดแล้วจึงตรวจสอบใหม่ ซึ่งอาจจะพอมองเห็น ปัญหาได้ครอบคลุมได้ ทั้งนี้เราต้องใช้วิธีการรวมไฟล์ชุดต่าง ๆ เข้าด้วยกันก่อนแล้วจึงค่อยตรวจสอบ สิ่งที่เกิดขึ้นจากภาพรวม เพื่อที่จะสรุปปัญหาออกมาเป็นจุดต่าง ๆ ได้แม่นยำขึ้น



ภาพที่ ๖๒ ภาพรวมการให้บริการ Internet โดยใช้ PPPOE

เมื่อลองเปรียบเทียบการทำงานโดยใช้ Application Flow Diagram จะเห็นได้ว่าปัญหา ที่เจอเป็นการที่ Gateway ไม่ส่ง Authentication Message ไปหา AAA ทำให้ทราบว่าก่อนที่จะมี การส่ง Authentication Message (Access-Request) จะต้องเกิด Message จาก PPPoE Client กล่าวคือ กลุ่มของ PPPoE Discovery และ PPPoE Session ประเภท LCP/PAP จะมีการรับส่ง ข้อมูลไปมาหากันให้ครบก่อนที่ Gateway จะมีการส่ง Authentication Message (Access-Request) ออกไปที่ AAA ดังนั้น ปัญหาอาจจะเกิดจากการที่ Client มีการส่ง Message ไม่เป็นไปตามขั้นตอน การทำงาน จากภาพที่ ๖๒ ทำให้เห็นถึงปัญหาในภาพรวมผ่าน Application Flow Diagram โดยมีขั้นตอนโดยสรุป ดังนี้

(๑) ใช้โปแกรม Wireshark รวมไฟล์ที่กำหนดให้เพื่อให้เป็นแพ็กเก็ตทั้งหมดในภาพรวมก่อน

(๒) ใช้งาน Filter Command เพื่อแยกเฉพาะข้อมูลที่สนใจออกมาจากแพ็กเก็ตทั้งหมด

(๓) ใช้งาน Flow Graph เพื่อสร้าง Protocol/Application Flow ออกมาจากส่วนที่ทำงาน ถูกต้อง มาใช้เป็นข้อมูลในการอ้างอิงการทำงาน เพราะเมื่อใดก็ตามที่มีการทำงานที่ผิดปกติ เราก็จะ สามารถใช้ Protocol/Application Flow ในการอ้างอิงได้ และยังเป็นการช่วยให้เราหาจุดที่ทำงาน ผิดพลาดได้รวดเร็วมากขึ้นอีก

(๔) เมื่อได้ Protocol/Application Flow จาก Wireshark แล้วก็ให้ลองสร้าง Protocol/ Application Flow ออกมาด้วยตนเอง โดยให้วาดลงกระดาษใช้โปรแกรมต่าง ๆ ช่วยก็ได้ โดยมี หลักการคือพยายามจัด Packet ให้เป็นกลุ่มก่อน และใช้ลูกศรแสดงทิศทางการทำงานของ Protocol/Application ด้วย เพียงเท่านี้ก็จะทำให้เราสามารถวิเคราะห์ปัญหาทางเครือข่ายผ่าน เครื่องมือของ Wireshark ได้อย่างมีประสิทธิภาพ

บทที่ ๔ การเก็บหลักฐาน

การเก็บหลักฐาน ในขั้นตอนแรกจะต้องดำเนินการตรวจสอบคำร้องก่อนว่าต้องการให้ ดำเนินการเก็บหลักฐานแบบฟ้องศาลหรือไม่ หากต้องนำไปฟ้องศาลจำเป็นต้องปฏิบัติตาม "ข้อเสนอแนะมาตฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน" แต่ถ้าไม่ก็ให้ ตรวจสอบดูก่อนว่าเครื่องได้ทำการปิดอยู่หรือไม่ (แนะนำให้เปิดอยู่ดีที่สุด) กรณีที่เครื่องเปิดอยู่ควรให้ ผู้รับผิดชอบหรือเจ้าของเครื่องทำการ Login เข้าสู่ระบบพร้อมทั้งรวบรวมข้อมูล User และ Password ของเจ้าของระบบมาด้วย จากนั้นจึงทำการถ่ายภาพหน้าจอ หมายเลขเครื่อง Port หรือจุด ที่มีการเชื่อมต่อ รวมถึงบริเวณโดยรอบด้วย จากนั้นจึงดำเนินการเก็บหลักฐาน RAM เป็นอันดับแรก ด้วยโปรแกรมใดโปรแกรมหนึ่ง โดยลำดับขั้นตอนการดำเนินการเก็บหลักฐานจะมีรายละเอียด ดังนี้

๔.๑ การเตรียมการ

ต้องทราบขนาดของฮาร์ดดิสก์เครื่องเกิดเหตุมีขนาดเท่าใด เพื่อที่จะสามารถจัดเตรียมฮาร์ดดิสก์ ของเราให้เพียงพอกับขนาดข้อมูลที่จะดำเนินการเก็บหลักฐาน และควรทราบประเภทคอมพิวเตอร์ที่ จะดำเนินการเก็บหลักฐานว่าเป็นเครื่อง Server, VMware, PC หรือ Notebook เพื่อจะได้เตรียม เครื่องมือสำหรับจัดเก็บหลักฐานได้ถูกต้อง

๔.๒ การเข้าพื้นที่

ต้องขออนุญาตเจ้าของพื้นที่และควรให้เจ้าของพื้นที่เป็นผู้นำทางไปพร้อมสอบถามอาการ เบื้องต้นเพื่อประเมินการเก็บหลักฐาน

<.m การจำกัดการแพร่กระจาย

ในกรณีที่เป็นพวกมัลแวร์จำเป็นต้องทำการตัดการเชื่อมต่อระบบ Network โดยรอบก่อนเพื่อ ป้องกันการแพร่กระจายของมัลแวร์

๙.๙ การจัดลำดับการเก็บหลักฐาน

ให้เริ่มจากการสำรวจจุดเชื่อมต่อทาง Network จากนั้นจึงไล่เรียงเส้นทางมายังเครื่องที่เกิดเหตุ โดยจะต้องสังเกตุว่าเครื่องคอมพิวเตอร์ ณ เวลาที่เข้าไปดำเนินการเก็บหลักฐานมีการเปิดใช้งานอยู่ หรือไม่ ถ้าเป็นเครื่องมีการเปิดใช้งานอยู่ ก็ต้องทำการเก็บ RAM ของระบบเป็นอันดับแรก ตามด้วย ฮาร์ดดิสก์ และข้อมูลอื่น ๆ ของเครื่อง รวมถึงช่วงเวลาในการใช้งานของระบบ

๙.๕ การเก็บหลักฐานเครือข่าย

๔.๕.๑ เครือข่ายภายนอก หรือกายภาพเครือข่าย เช่น อุปกรณ์ Switch มีการเชื่อมต่อไปยัง หน่วยงานใด ได้รับ IP วงไหน มีการกระจาย Wifi ในหน่วยงานหรือไม่ มีการแบ่งระบบ VLAN ในระบบหรือไม่ มีการกำหนด Gateway ไปยังที่ใด ทั้งนี้หากได้แผนผังระบบเครือข่าย ของหน่วยงาน ที่เกิดเหตุมาได้ก็จะช่วยให้สามารถวิเคราะห์ปัญหาได้รวดเร็วยิ่งขึ้น



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 ที่มีการ ดักจับแพ็กเก็ตเอาไว้



ภาพที่ ๖๔ การเก็บหลักฐานด้านเครือข่าย ภายใน

๙.๖ การเก็บหลักฐานเครื่องโฮส

๔.๖.๑ ข้อมูลโฮสพื้นฐาน เป็นการรวบรวมข้อมูลระบบปฏิบัติการที่ใช้ รุ่น เวอร์ชัน Password เข้าสู่ระบบ (เก็บเป็นความลับใช้แค่ใน lab เท่านั้น ห้ามพิมพ์ลงเอกสารรายงาน ให้ใช้ สัญญาลักษณ์ #### แทน) และซอฟต์แวร์ที่ต้องสงสัยภายใน ข้อมูลช่องเสียบอุปกรณ์มีอะไรบ้าง ต่อ ใช้งานหรือไม่ เชื่อมต่อกับอะไร ใครมีสิทธิใช้งานได้บ้าง 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 มีความจุ รวมเท่าไหร่ ที่สำคัญคือ เราจะสามารถเก็บข้อมูล RAM ได้ก็ต่อเมื่อเหตุการณ์เกิดขึ้นแล้วเครื่อง คอมพิวเตอร์ยังคงเปิดใช้งานอยู่ และห้ามทำการปิดเครื่องคอมพิวเตอร์ เพราะจะทำให้บางโปรแกรม ลบตัวเองหลังจาก 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





ให้เสียบ USB ที่มีโปรแกรม MagnetRAMCapture.exe จากนั้นทำการรัน โปรแกรม โดยโปรแกรมจะให้เราเลือกตำแหน่งในการจัดเก็บไฟล์ โดยในที่นี้จะสร้างไฟล์ไว้ที่หน้าจอ จากนั้นทำการตั้งชื่อไฟล์ โดยจะต้องมีนามสกุลเป็น .raw กรณีที่ไม่สามารถคัดลอกไฟล์ได้อาจมีสาเหตุ มาจาก RAM มีเนื้อที่ทำงานไม่เพียงพอ ให้ทำการ .zip/.rar ไฟล์ก่อนแล้วค่อยคัดลอกไฟล์ .zip มา ๔.๖.๒.๓ โปรแกรม RamCapturer

0	msvcr110 dll	10/22/2018 10:11	Application extens	830 KI
		10/22/2010 10:11	Application extens	50 KI
8	The second secon	10/22/2018 10:11	Application	58 KI
	RamCaptureDriver64.sys	10/22/2018 10:11	System file	34 KI
	Belkasoft Live RAM Capturer		- 0	×
	Select output folder path:			
	E:\1 งานกอง\0 forensic\1 โปรแกรม forens	sic\x64		
	Loading device driver Physical Memory Page Size = 4096 Total Physical Memory Size = 33536 MB			^
				~

ภาพที่ ๖๗ การเก็บหลักฐาน RAM

โปรแกรม RAMCapture.exe มีข้อดีตรงที่ไม่ต้องติดตั้งโปรแกรมลงในเครื่อง เพียง Run โปรแกรมก็สามารถทำการคัดลอก RAM ได้ทันที ทั้งนี้หลังจากเก็บข้อมูล RAM และควรทำ การ Hash ไฟล์ด้วย เพื่อใช้เป็นหลักฐานเวลานำไปวิเคราะห์สามารถใช้เปรียบเทียบเพื่อยืนยันความ เที่ยงตรงว่าไม่เกิดการเปลี่ยนแปลงไประหว่างการคัดลอกข้อมูล 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

Select	Source X	
l r	Please Select the Source Evidence Type	
	Physical Drive	
	C Logical Drive	
	O Image File	
	 Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.) 	-
	C Femico Device (multiple CD/DVD)	
	< Back Next > Cancel Help	

ภาพที่ ๖๙ การเก็บหลักฐาน RAM

จากนั้นทำการเลือกฮาร์ดดิสก์ที่จะทำการสร้าง Image

Selec	t Drive	×
	Source Drive Selection Please select from the following available drives: \\.\PHYSICALDRIVE0 - HGST HUC101860CSS204 SCSI Disk [\\.\PHYSICALDRIVE0 - HGST HUC101860CSS204 SCSI Disk Devit \\.\PHYSICALDRIVE1 - HGST HUC101860CSS204 SCSI Disk Devit \\.\PHYSICALDRIVE3 - WD My Passport 25E1 USB Device [1000G	
	< Back Finish Cancel Help	

ภาพที่ ๗๐ การเก็บหลักฐาน RAM

ตามด้วยการกดปุ่ม Add

	Starting Evidence Number:	1
- Image Destination(s)		
Add	Edit,	Remove
	Add Overflow Location	

ภาพที่ ๗๑ การเก็บหลักฐาน RAM

	Create Ir	nage Evidence Item Informat	ion	×
Select Image Type ×	\\.V	Case Number:	tast_Evdein	
Please Select the Destination Image Type	Imag	Evidence Number:	620703	
C Raw (dd)		Unique Description:		
C SMART		Examiner:		
€01		Notes:		
C AFF				
	✓ Ver		< Back Next > Cancel Help	
< Back Next > Cancel Help		Sta	rt Cancel	

ภาพที่ ๗๒ การเก็บหลักฐาน RAM

เลือกที่แหล่งที่จะเก็บไฟล์ Image

Create Ima	ge	×	Browse For Folder	×
	lect Image Destination	×	Select the destination folder for the image	
Imag	Image Destination Folder E:Neb_520703 Image Flemame (Excluding Externation) Faet_620703	Browse	> Recovery Image (D:) DATADRIVE1 (E:) 00 หน้าจอ 0 tast_HTML5 > 1 งามกอง	^
	Image Fragment Size (MB) 1500 For Raw, E01, and AFF formats: 0 = do not fragment Compression (0=None, 1=Fastest,, 9=Smallest) 6 Use AD Encryption	4	> 2 1#2 jRaja_Home_Edition lab_620703 > n_image USS	~
Ver	< Back Finish Cancel	Help	Folder: New folder Make New Folder OK Cancel	

ภาพที่ ๗๓ การเก็บหลักฐาน RAM

٦

จากนั้นก็กดปุ่ม start ได้เลย ซึ่งกระบวนการจะใช้เวลาค่อนข้างนานหลายชั่วโมงขึ้นอยู่กับปริมาณ ข้อมูลในฮาร์ดดิสก์

-		
Image Source		
\\.\PHYSICALDRIVE0		
	Starting Evidence Number: 1	
Image Destination(s) —		
E:\ab_620703\tast_620	0703 [E01]	
	1	
Add	Edit,,, Remove	
Add	Edit,,, Remove	
Add	Edit,,, Remove Add Overflow Location	
Add	Edit,,, Remove	
Add	Edit, Remove Add Overflow Location ey are created Progress Stati	stics
Add Verify images after the Create directory listing	Edit Remove Add Overflow Location ey are created Progress Stati s of all files in the image after they are created	stics
Add Verify images after the Create directory listing	Edit Remove Add Overflow Location Add Overflow Location ey are created Precalculate Progress Station s of all files in the image after they are created Image after they are created	stics
Add Verify images after the Create directory listing	Edit Remove Add Overflow Location	stics

ภาพที่ ๗๔ การเก็บหลักฐาน RAM

<.๗ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)

จะมีความแตกต่างจากกรณีที่แล้วมา เนื่องจากเป็นหลักฐานที่สามารถทำให้เกิดความเสียหาย ทั้งต่อเครื่องมือในการเก็บและข้อมูลที่กำลังจะเก็บด้วย ส่วนใหญ่จะใช้อุปกรณ์พิเศษในการจัดเก็บนั้น คือ Blue Box หรือเครื่องป้องกันการเขียนข้อมูลย้อนกลับ



ภาพที่ ๗๕ การเก็บหลักฐานที่เป็นมัลแวร์ (Malware)

๙.๘ การจำกัดพื้นที่เครื่องเกิดเหตุ

ในการเข้าพื้นที่เกิดเหตุ เรามีความจำเป็นต้องทำการควบคุมพื้นที่เกิดเหตุเพื่อป้องกันไม่ให้ หลักฐานทางกายภาพเสียหาย โดยทั่วไปจะมีการกางเทปกั้น เพื่อควบคุมพื้นที่ ดังภาพที่ ๖๕



ภาพที่ ๗๖ การจำกัดพื้นที่เครื่องเกิดเหตุ

บทที่ ๕ การเตรียมหลักฐาน

กระบวนการเตรียมหลักฐานมีความสำคัญอย่างยิ่งสำหรับงาน Forensics นอกจากจะทำให้ ทำงานได้รวดเร็วขึ้นแล้ว ยังช่วยให้กระบวนการทดสอบมีความแม่นยำเพิ่มขึ้นอีกด้วย ทั้งนี้การเตรียม หลักฐานจะเน้นไปที่การจัดสภาพความพร้อมของข้อมูลที่จะทำการวิเคราะห์เป็นหลัก โดยงานหลัก ๆ จะเป็นการทำให้ข้อมูลอยู่ในสภาพที่พร้อมจะทำการวิเคราะห์ ซึ่งโดยธรรมชาติของหลักฐานทางดิจิทัล เมื่อเป็นข้อมูลที่มีปริมาณมาก และไม่อยู่ในรูปแบบที่จะทำการวิเคราะห์ผลได้ทันที หรือแม้แต่ อยู่ในหลักฐานของจริงซึ่งไม่สามารถทำการวิเคราะห์ได้ทันที จำเป็นต้องมีการทำสำเนาออกมาก่อน โดยจะค่อนข้างใช้ระยะเวลาพอสมควร ดังนั้นหากกระบวนการเตรียมหลักฐานสามารถทำได้รวดเร็ว การวิเคราะห์หลักฐานทางดิจิทัลก็จะสามารถได้ผลลัพธ์รวดเร็วด้วยเช่นกัน ทั้งนี้ยังรวมไปถึงการ เตรียมไฟล์สำหรับใช้เก็บหลักฐานด้วย โดยในที่นี้จะขอเริ่มจากหลักฐานที่เป็น RAM ก่อน ซึ่งมี โปรแกรม Mandiant Redline ในการทำหน้าที่วิเคราะห์ Process ของระบบปฏิบัติการ Windowds ให้เบื้องต้นก่อน หากต้องใช้คนวิเคราะห์จะใช้เวลานานเนื่องจาก Process ในระบบคอมพิวเตอร์ มีปริมาณมากมาย



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

ท็ LL ป 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 แล้วจะเกิดหน้า cmd ขึ้น เมื่อทำงานเสร็จหน้า 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 จากนั้นใช้โปรแกรมดั้มโพรเซสที่ชื่อ Mandiant Redline ผ่าน USB ทำการดั้มโพรเซสของเครื่องออกมาแล้ว Re Snapshort 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, เซอร์วิส ของระบบ, เครือข่าย และรายการเพิ่มเติมอื่น ๆ เป็นต้น ตามด้วยทำการสร้างโฟลเดอร์ปลายทาง สำหรับใช้เก็บข้อมูล แนะนำให้เป็น USB ที่ Format เป็น USB ที่ไม่มีข้อมูล และกด OK

			Styles	
Redline	-			
	Select Target Platform	View and Edit Your Script for Windows	×	×
	Collector can be created on	Memory Disk System Network Other	Show Advanced Parameter	5
Collect Data Create a Standard Collector > Create a Comprehensive Collector > Create an IOC Search Collector >	Windows Review Script Configurat You have chosen to cree The comprehensive colle crept below. Edit your script Acquire Memory Image Checking this option	Process Listing PID Process Name Shortest Matched String Content Reper Hendles Getions Gimports MDS Stu2256	Specifies the Process ID (PIO) of the process to analyze The first 15 characters of the process name. Calved be- a Only return processes with particular content. Place each entry on a new line.] V Ports V Strings V Verify Digital Signatures SHA1 SHA1 SHA1 SHA1 SHA1	y choosing to edit the
Open Previous Analysis >	Specify Collector Location 1. Your Collector package 2. On the Windows mach you configured it, and say etc.) is created. 3. When the collection is	Use Raw File Access Orivers Exampration Shortest Matched String Deports Deports MacSo MacSo MacSo MacSo Detection Ut7 It7 It7 It7 It7 It7 It7 It7 It7 It7 I	B ♥ Verify Digital Signatures SHA 3 ■ Use Raw File Access ♥ SSDT Indee	will run the Collector, as sssion2, AnalysisSession3, iSession folder.
	A copy of these instruction	Soft Thine Work Dights Signatures Acquire Keenory Image Acquire mage of memory that can be use Restine	IV Drivers d to accurately acquire process memory and drivers during analysis in OK	Browse
	Cancel			ок

ภาพที่ ๘๒ โปรแกรม Mandiant RedLine 6

จากนั้นจะมีกล่องข้อความแจ้งเตือน (ต้องปิดแอนตี้ไวรัสในเครื่องคอมพิวเตอร์) เพื่อบอกขั้นตอน การนำไฟล์ไปใช้งานสามารถกดปิดได้



ภาพที่ ๘๓ โปรแกรม Mandiant RedLine 7

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

								3
💼 🔜 I 🖂 🔜 🛨 I	Application Tools Cap_Ram				- 🗆	\times	CDu	AABBCCDE
File Home Share	View Manage					~ 🕜	Q	Subtle Ref 🤤
	C . L I Did (C) Il	Landa a Cara Dava			Court Court	-		
$\leftarrow \rightarrow \uparrow \uparrow \square \rightarrow ThisPC$	C > Local Disk (C:) > Users > User > Downi	loads > Cap_Kam		~ 0	Search Cap_	K)	1.1	· · · 6 · 🛆
^	Name	Date modified	Туре	Size				
🖈 Quick access	x64	1/30/2021 4:25 PM	File folder					
Desktop 🖈	×86	1/30/2021 4:25 PM	File folder					
🔶 Downloads 🛛 🖈	elevate.cmd	4/27/2020 11:58 AM	Windows Comma	2 KB				
😭 Documents 🛛 🖈	elevate.vbs	4/27/2020 11:58 AM	VBScript Script File	4 KB				
Pictures 🖈	finishAnalysis.js	4/27/2020 11:58 AM	JavaScript File	2 KB				
CarDaine Demonst	getNextSessionFolder.js	4/27/2020 11:57 AM	JavaScript File	1 KB				
Chebrive - Personal	📓 getPath.js	4/27/2020 11:56 AM	JavaScript File	3 KB				
💻 This PC	Helper.bat	4/27/2020 11:56 AM	Windows Batch File	3 KB				
3D Objects	MemoryzeAuditScript.xml	1/30/2021 4:25 PM	XML Document	21 KB				
Desktop	Readme.txt	4/27/2020 11:57 AM	Text Document	1 KB				
Documents	RunRedlineAudit.bat	4/27/2020 11:56 AM	Windows Batch File	1 KB				
- Downloads								
Readme.txt - Notepad						-		J X
File Edit Format View Help								
On the Windows	machine you want to	audit nun	the 'Pup	Podlin	oAudit	hat	1	~
	liachine you want to			Veditii	CAUUIC	·Dat		
script, prefera	bly from removable n	nedia (e.g.	a USB Ha	rd Dri	ve). T	he s	cr	lpt
will run the Co	llector, as you conf	figured it,	and save	the r	esults	to	a	
folder named 'S	Sessions	sion1'. Eve	rv time v	ou run	the s	crin	+	a
						- \		
new Analysisses	sion tolder (Analysi	issession2,	Analysis	Sessio	ns, et	с.)	15	•
created.								
When the coller	tion is finished to	appefon the	posulte	hack t		202	1.00	ic
			i esurts		U your		Туз	13
machine, then d	louble-click Analysi	isSession.m	ans tile	locat	ed ins	ıde	τηε	
AnalysisSes <u>sio</u> r	i folder.							

ภาพที่ ๘๔ โปรแกรม Mandiant RedLine 8

C:\WINDOWS\System32\cmd.exe			- [) X	A
UEnsuring the proper working directory .\x64\xagt.exe* -o *C:\Users\User\Downloads\Cap_	Ram\\Sessions\AnalysisSessior	nl∖Audits" -f "Memoryz	seAuditScript.xm	n1"	
_ ⊇ _ =	Application Tools Cap_Ram				- 0
File Home Share	View Manage				
$\leftarrow \rightarrow \checkmark \uparrow$ 📙 > This P	C > Local Disk (C:) > Users > User >	Downloads → Cap_Ram		√ Ö	Search Cap_R.
^	Name	Date modified	Туре	Size	
A Quick access	Sessions	1/30/2021 4:34 PM	File folder		
Desktop 🖈	x64	1/30/2021 4:25 PM	File folder		
N Downloads 🖈	x86	1/30/2021 4:25 PM	File folder		
🗄 Documents 🖈	levate.cmd	4/27/2020 11:58 AM	Windows Comma	2 KB	
📰 Pictures 🛷	📓 elevate.vbs	4/27/2020 11:58 AM	VBScript Script File	4 KB	
OpeDrive - Personal	🌋 finishAnalysis.js	4/27/2020 11:58 AM	JavaScript File	2 KB	
	getNextSessionFolder.js	4/27/2020 11:57 AM	JavaScript File	1 KB	
This PC	🧭 getPath.js	4/27/2020 11:56 AM	JavaScript File	3 KB	
🧊 3D Objects	lelper.bat	4/27/2020 11:56 AM	Windows Batch File	3 KB	
Desktop	MemoryzeAuditScript.xml	1/30/2021 4:25 PM	XML Document	21 KB	
🗄 Documents	Readme.txt	4/27/2020 11:57 AM	Text Document	1 KB	
	RunRedlineAudit.bat	4/27/2020 11:56 AM	Windows Batch File	1 KB	

ภาพที่ ๘๕ โปรแกรม Mandiant RedLine 9

หลังจาก cmd ปิดไปแล้วเราจะได้ไฟล์ ดังนี้



ภาพที่ ๘๖ โปรแกรม Mandiant RedLine 10

เมื่อเปิดใช้งานสามารถเข้าไปที่ Analyze data > From a Saved Memory File หรือ สามารถเปิดจากไฟล์ที่มีนามสกุล .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 StarWindoconverter กรณีที่เครื่องคอมพิวเตอร์ที่เกิดเหตุเป็นเครื่อง Notebook หรือเครื่องที่ไม่สามารถแกะเอาฮาร์ดดิสก์ออกมาได้ให้ใช้วิธีการทำ Image ให้เป็น ไฟล์ .vmdk



ภาพที่ ๘๙ โปรแกรม StarWind V2V Converter

? \times ÷ StarWind V2V Converter Select location of image to convert P2V Convert physical machine or disk 🔾 Local file File on the local machine Remote VMware ESXi Server Virtual Disk or Virtual Machine on remote ESXi Server (version 5.5 and later versions) O Microsoft Hyper-V Server Virtual Disk or Virtual Machine on remote Hyper-V hypervisor Microsoft Azure OAWS Amazon Web Services Next > Cancel

เมื่อทำการ Run โปรแกรมขึ้นมาแล้วให้ทำการเลือก P2V และกด Next

ภาพที่ ๙๐ โปรแกรม StarWind V2V Converter 1

เลือก Physical Disk และกด Next

	?	\times
← 🔿 StarWind V2V Converter		
Select physical data to convert		
◯ Disk Volume		
Convert single disk volume to virtual disk file		
Physical Disk		
Convert physical disk to virtual disk file. Volume structure is preserved. It is possible select a set of disk volumes for copying to virtual disk file	e to	
Entire machine		
Migrate this physical machine to new virtual machine		
Next >	Car	ncel

ภาพที่ ๙๑ โปรแกรม StarWind V2V Converter 2

? \times StarWind V2V Converter Select physical disk to convert Select disk SanDisk SDSSDA240G \sim Volume Label Size Free Space Required C:\
()?\Volume{a... 223 GB 69.0 GB 154 GB 901 MB 403 MB 498 MB Next > Cancel

เลือก Disk ที่เก็บข้อมูลของระบบที่ต้องการจะทำ VM-Ware

ภาพที่ ๙๒ โปรแกรม StarWind V2V Converter 3

เลือก Local File และกด Next

		?	×
← O s	arWind V2V Converter		
C - 1	and a section of deadle attack to a sec		
Sele	ect location of destination image		
(Docal file		
	File on the local machine		
0	Bemote VMware ESXi Server		
	Virtual Disk or Virtual Machine on remote ESXi Server (version 5.5 and later versions)		
(Microsoft Hyper-V Server		
	Virtual Disk or Virtual Machine on remote Hyper-V hypervisor		
(Azure		
	Microsoft Azure		
	ANG		
,	Amazon Web Services		
	Next >	Cane	cel

ภาพที่ ๙๓ โปรแกรม StarWind V2V Converter 4

เลือก VMDK และกด Next

		?	\times
~	StarWind V2V Converter		
	Select destination image format		
	VMDK VMware Virtual Machine Disk		
	O VHD /VHDX Microsoft Virtual Hard Disk		
	QCOW2 QEMU qcow2 disk image		
	IM6/RAW Raw disk image (img). This image format is suitable for StarWind. Disk space for this is allocated at the creation time and does not change over time	image	
	Next >	Canc	el

ภาพที่ ๙๔ โปรแกรม StarWind V2V Converter 5

เลือก VMware Workstation growable image และกด Next

?	×
← 🔿 StarWind V2V Converter	
Select option for VMDK image format	
Wware Workstation growable image Disk space for this image is allocated on demand, so disk size of this image grows over time. WARNING! This format is not compatible with ESXi vmdk format!	
VMware Workstation pre-allocated image Disk space for this image is allocated at the creation time and does not change over time. WARNING! This format is not compatible with ESXI vmdk format!	
Stream-optimized image Monolithic sparse format compressed for streaming. Suites for using with OVF packages	
C ESXi Server image Select type ESX image	
Additional options	
Next > Ca	ncel

ภาพที่ ๙๕ โปรแกรม StarWind V2V Converter 6

ทำการสร้างโฟลเดอร์สำหรับเก็บไฟล์ VM-ware

		_			
? >	<		~ (?		
Г	O Save As				×
	Save in:	👝 Cyber-training	g-03 (E:) ~	G 🌶 📂 🖽 -	
	Quick access Desktop Libraries This PC	Name 630419_cif Automatic CyberWar FA-18 Oper ip va program spack vm squfinsadu squfinsadu squfinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stuffinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu stufinsadu	^ Mouse and Keyboard ation Desert Storm จาโก62 ร้าโก63 M DESKTOP-8GS8865.vmdk	Date modified 4/19/2020 9:31 PM 2/15/2020 11:50 AM 12/9/2019 11:25 AM 2/15/2020 11:59 AM 2/17/2020 11:159 AM 2/17/2020 5:20 PM 1/17/2020 7:15 PM 3/25/2020 6:13 AM 3/6/2020 8:28 PM 2/28/2020 7:53 AM 4/23/2020 11:18 AM	Type * File fol File fol Fol Fol Fol Fol
Cancel				⊙> Malware	
	?)	? × Save As Save n: Uuick access Desktop Libraries Libraries Network	? × Save As Save in: ■ Cybertramm Cuick access Cuick access Desktop Desktop Desktop This PC Network Fie name: Save as type:	? X Save As Save in: Cybertraining-03 (E) Save in: Cybertraining-03 (E) X Rest in the initial of t	? X Save As Image: Cybertraining-03 (E) Save in: Cybertraining-03 (E) Quick access Date modified Quick access Cybertraining-03 (E) Desterop Date modified Quick access Cybertraining-03 (E) Desterop Date modified Quick access Cybertraining-03 (E) Desterop System Program 2/15/2020 11:50 AM System System Speck 1/17/2020 11:50 AM System System Cybertraining-02 (System System System System System System System S

ภาพที่ ๙๖ โปรแกรม StarWind V2V Converter 7

– ៧ണ –

เมื่อกระบวนการเสร็จสิ้นและกด Finish

← 🔇 9 % - StarW	find V2V Converter	?	×	← ○ Finished -	StarWind V2V Converter	?	×
Converting	9 %			Converting	9 100%		
Burning Log:				Burning Log:			
Time 11:18:51 11:18:56 11:18:56 11:18:56 11:18:57 11:18:57	Information Started Taking inapphots Taking inapphot of volume C:\- success Success Creating output image file Success: Created file E:\vm_notbook\pESkTCP-8G58865.vmdk Converting			Time 11:18:51 11:18:56 11:18:56 11:18:57 11:18:57 11:18:57 11:18:57 11:18:57 11:18:57	Information Started Taking snapshots Taking snapshots for Yolume C: \-success Success Creating output image file Success: Created Re: Lym_notbook/DESKTOP-8GS8865.vmdk Converting Success Converted successfully!		
	Finish	Canc	el		Convert another image	Fir	nish

ภาพที่ ๙๗ โปรแกรม StarWind V2V Converter 8

ไฟล์ .vmdk ดังรูป ไม่สามารถเปิดกับโปรแกรม VMware Workstation ได้ ต้องทำการนำเข้า ไฟล์ก่อน

tbook								
are View								
This PC > Cyber-training-03 (E:) > vm_notbook								
	Name	Date modified	Туре	Size				
	🛋 15.png	4/23/2020 11:44 AM	PNG File	310 KB				
*	🐣 DESKTOP-8GSB865.vmdk	4/24/2020 10:25 AM	VMware virtual dis	147,224,64				
7 7 7								

ภาพที่ ๙๘ โปรแกรม StarWind V2V Converter 9

จากนั้นให้ทำการนำเข้าไฟล์ vmdk โดยไปที่เมนู File > New Virual Machine Wizrd..

SIFT-Workstation - VMwa	are Workstation		– – ×
File Edit View VM T	abs Help 🕨 🗕 🚽	🐢 🛥 I 🔲 🗖 🔁 💌	
Library	New Virtual Machine Wizard	×	
My Computer WebDeveloper Prsenst Web for pentester		Welcome to the New Virtual Machine Wizard	
Windows 7		What type of configuration do you want?	
Ubuntu 16.04 Desi SIFT-Workstation Shared VMs	PRO"	 Typical (recommended) Create a Workstation 15.x virtual machine in a few easy steps. 	
		Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual 64k type and compatibility with older vieware products.	
	Help	< Back Next > Cancel	
			Virtual Machine Details State: Powerd off Configuration file: Configuration (SIFT-Workstation.vmx Hard To an and the state of the s

ภาพที่ ๙๙ โปรแกรม StarWind V2V Converter 10

SIFT-Workstation - VMwa	are Workstation	– 🗆 X
File Edit View VM Ta	Tabs Help 🕨 🖛 🚭 😰 🕰 🛄 🗖 🖾 🔀 🖂 🖉 👻	
Library Type here to search My Computer WebDeveloper Drientst Windows 7 Windows 7 Windows 8 rever 20 Ubuntu 16.04 Desk SIFT-Workstation Shared VMs	New Virtual Machine Wizard X Choose the Virtual Machine Hardware Compatibility Which hardware compatibility X Virtual machine hardware compatibility Wirtual machine hardware compatibility Hardware compatibility Workstation 15.x Compatible products: ESX Server Pusion 11.x Imitations: 64 GB memory 10 processors 10 Table size 3 GB shared graphics memory	
	 ✓ Virtual Machine Details State: Powered off Configuration file: C:Virtual Machines/SIFT-W Hardware compatibility: Workstation 14x virtual machines Primary IP address: Network information is not a 	orkstation\SIFT-Workstation.vmx hine available

ภาพที่ ๑๐๐ โปรแกรม StarWind V2V Converter 11

Edit View VM T	abs Help 🕨 🗸 🖧 🖓 🔑 🕰 🔲 🗖 🖓	>_
Type here to search My Computer G WebDeveloper G pfsenst Web for pentester Windows 7 Windows Server 20 Ubuntu 16.04 Desk SIFT-Workstation Shared VMs	New Virtual Machine Wizard X Guest Operating System Installation A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: Installer disc: CD Drive (G:) CD Drive (G:) F:\Programs\Windows 10\Windows 1809.iso Browse Install the operating system later. The virtual machine will be created with a blank hard disk.	
		1

ภาพที่ ๑๐๑ โปรแกรม StarWind V2V Converter 12

Та	bs Help ▶ ▼ 母 ₽ ₽ ₽ 🔲 🗆 🛱 🕅 ►	M Ta	ibs Help ▶ ▼ 母 ♀ ♀ ♀ 🔲 🗆 [], 汉 ▷ [
1 2r	New Virtual Machine Wizard X Select a Guest Operating System Which operating system will be installed on this virtual machine?	ch per	New Virtual Machine Wizard X Name the Virtual Machine What name would you like to use for this virtual machine?
ester ver 20 Desk tion	Guest operating system Microsoft Windows Linux Apple Mac OS X VMware ESX Version		Virtual machine name: Windows 10 Location: F:\vm_notbook The default location can be changed at Edit > Preferences.
	Windows 10 V		กำหนดโฟลเดอร์ที่จะจัดเก็บ VM ควรเป็นที่เดียวกับไฟล์ vmdk
	Help < Back Next > Cancel		< Back Next > Cancel

ภาพที่ ๑๐๒ โปรแกรม StarWind V2V Converter 13

	New Virtual Machine Wizard X	New Virtual Machine Wizard	×
	Name the Virtual Machine What name would you like to use for this virtual machine?	Firmware Type What kind of boot device should this virtual machine have?	
er	Virtual machine name: Windows 10	Firmware type	
20	Locat VMware Workstation X		
<u></u> 5К	Five The specified location appears to contain an existing virtual machine. Having two virtual machines installed in the same location can cause problems, including loss of data if the two virtual machines have the same name. Would you like to continue with this location?		
Ļ	< Back Next > Cancel	< Back Next > Cancel	

ภาพที่ ๑๐๓ โปรแกรม StarWind V2V Converter 14

New Virtual Machine Wizard	×	New Virtual Machine Wizard X
Processor Configuration Specify the number of processors for this virtual machine.		Memory for the Virtual Machine How much memory would you like to use for this virtual machine?
Processors Number of processors: Number of processors: 1 Number of cores per processor: 2 Total processor cores: 2		Specify the amount of memory allocated to this virtual machine. The memory size multiple of 4 MB. 0 32 GB 13 GB Memory for this virtual machine: 16 GB Memory for this virtual machine: 2 GB Memory for this virtual machine: 16 GB Memory for this virtual machine: 2 GB Memory for this virtual machine: 16 GB Memory for this virtual machine: 2 GB Memory for this virtual machine: 16 GB Memory for this virtual machine: 128 MB Is Recommended memory: 128 MB Guest OS recommended minimum: 128 MB IGB 16 MB IGB 8 MB IGB 8 MB IGB
Help < Back Next > Can	cel	Help < Back Next > Cancel

ภาพที่ ๑๐๔ โปรแกรม StarWind V2V Converter 15



ภาพที่ ๑๐๕ โปรแกรม StarWind V2V Converter 16

	New Virtual Machine Wizard Select a Disk Type What kind of disk do you want to create?	×	Image: Signature of the state of the s
r !0 .k	Virtual disk type OIDE OSCSI (Recommended) © SATA ONMe Ision SATA ให้ตรงกับประเภท Disk ของเครื่อง	ด้นฉบับ	Wew Virtual Machine Wizard X Image: Market of Search New Virtual Machine Wizard X Image: Market of Search Select a Disk Weh disk do you want to use? Image: Market of Search With disk do you want to use? Select a Disk Image: Market of Search Other Other Other Image: Market other Other Other Other Image: Market other Other Other Other Other Image: Market other Other Other Other Other Other Image: Market other Other Other Other Other Other Other Image: Market other
	Help < Back Next > Cancel		Help < Back Next > Cancel

ภาพที่ ๑๐๖ โปรแกรม StarWind V2V Converter 17

	New Virtual Machine Wizard X	I	New Virtual Machine Wizard $ imes$
-	Select an Existing Disk Which previously configured disk would you like to use?		Select an Existing Disk Which previously configured disk would you like to use?
r !0 k	Existing disk file F:\vm_notbook\pESKTOP-8GSB865.vmdk ระบุที่อยู่ใฟล์ vmdk	D	Existing disk file F: Jvm.notbook/DESKTOP-8GSB865.vmdk Rrowse VMware Workstation Convert existing virtual disk to newer format? The chosen virtual disk can be converted to the newest format supported by this Workstation 15.x virtual machine. However, after conversion the virtual disk will be unusable with older virtual machines. Keep Existing Format Convert Cancel
	Help < Back Next > Cancel		Help < Back Next > Cancel

ภาพที่ ๑๐๗ โปรแกรม StarWind V2V Converter 18

The virtual machine v	vill be created with the following settings:	
Name:	Film pathock	^
Version:	Workstation 15 x	
Operating System:	Windows 10	
Hard Disk:	Evisting disk E. Jum nothook/DESKTOP-8698865 umdk	
Memory:	1024 MB	
Network Adapter:	NAT	
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Printer, Sound	¥
Customize Hardwa	are	

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 เป็นการค้นหามัลแวร์แบบ Static เราจะต้อง Snapshot VM-Ware ด้วยเสมอ โดยใน ที่นี้จะแบ่งเป็น ๒ ส่วนคือ Window 7 เป็นเครื่องที่จะติดมัลแวร์ และ Remnux จะเป็นเครื่อง มอนิเตอร์และสร้าง DNS ปลอม การทำ Sandbox มีความอันตรายต่อระบบต้องตั้งค่า VM ให้เป็น Host Only และตัดการเชื่อมต่อกับระบบภายนอก เบื้องต้นจะต้องเริ่มวางแผนด้วยการออกแบบ Network ก่อนว่าจะมีเครื่องในการทดสอบกี่เครื่อง โดยทั่วไปจะใช้ ๒ เครื่อง คือ เครื่องที่ติดไวรัส กับ เครื่องที่ทำหน้าที่เป็นตัวเก็บ Logs และจำลองอินเทอร์เน็ตปลอม ปกติก็จะใช้ VM Ramnux โดย Set ให้คอมพิวเตอร์ทั้งสองเครื่องอยู่ในวง LAN เดียวกัน ทดสอบด้วยการ Ping หากัน และการทำ Sandbox ต้องขอย้อนความรู้เรื่องของการเตรียมการทดสอบหรือการจัดเตรียมสภาพแวดล้อมการ ทดลองก่อน เพื่อให้กระบวนการสอดคล้องและต่อเนื่องกัน ดังภาพ

การเชคระบบ		set ip ແນນ linux	sudo ifconfig eth0 192.168.180.128 netmask 255.255.255.0
การทำ	i sanbox		sudo route add default gw 192.168.180.1 eth0
vm win7	vm remunx	เปิดเว็บเซอร์วิส	inetsim
ดิดตั้งโปรแกรม ProcessMonitor	เปิด dns ปลอม	เปิด dns ปลอม	fakedns
ดิดตั้งโปรแกรม processhacker	set ip ແນນ linux		ให้ windows เปิด ip เครือ่งของ Linux
set ip แบบฟิก	เปิดโปรแกรม วาชาด เพื่อแค็บเจอร์เน็ตเวิด		
ip 192.168.180.10	จากนั้นทำการ scapChort ไว้		ລ້າงอึง
subnet 255.255.255.0			https://www.youtube.com/watch?v=4LzCr9qf5_Q
dns 192.168.160.128	start dns ปลอม		
จากนั้นทำการ scapChort ไว้	เปิดวาชาด		
ทดสอบเข้าหน้าเว็บด้วย ip ของ remunx			
เปิดโปรแกรม processhacker และ			
ProcessMonitor ทำการเคลียโปรเชตโดย			
คลิกที่รูปขางลบแล้วกดเริ่มมอนิเตอร์ที่รูปแ	ว่น		
ทำการโหลดมัลแวร์และรันมัลแวร์			
สังเกตโปรเซต์ของมัลแวร์ที่โปรแกรม Proc	essHacker		
ทำการ kill โปรเชตของมัลแวร์ด้วยโปรแกร	N ProcessHacker		
ที่โปรกแกรม processMoniter กตรูปแว่นอี	กครั้งเพื่อหยุดการตรวจจับ		
ทำการ save เป็นไฟล์ csv	ปิดโปรแกรมวาชาคแล้ว Save ไฟล์ .pcap		
	ปิด DNS ปลอม		
น่าไฟล์ csv ไปเปิดกับโปรแกรม Don เพื่อ	งดูดวามสัมพันธ์		
	นำ .pcap ไปวิเคราะห์ได้		

ภาพที่ ๑๑๐ การทำ Sandbox

เมื่อเตรียมสภาพแวดล้อมของการทดสอบเสร็จเรียบร้อยแล้ว ขั้นตอนต่อไปคือการทำ 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 เปิดเซอร์วิสเว็บไซต์ของ ด้วยคำสั่ง #>sudo inetsim เปิด Terminal ขึ้นมาใหม่แล้ว ทำการสตาร์ท DNS จำลองของ Remnux ด้วยคำสั่ง #>sudo fakedns



ภาพที่ ๑๑๑ คำสั่ง #> sudo fakedns

จากนั้นทำการ Snapshot เครื่องเหยื่อ Win7 แล้วพิมพ์หมายเลข IP Address ของ เครื่อง Remnux ที่บราวเซอร์จะแสดงหน้าต่างการต้อนรับการใช้งานของโปรแกรม Remunx แสดง ว่าระบบพร้อมใช้งานที่ VM ของ Remnux เปิดโปรแกรม Wireshark เพื่อทำการบันทึกภาพหน้าจอ ไฟล์ .pcap Network ของเหตุการณ์เปิดโปรแกรม Process Hacker และ Process Monitor ทำการเคลียร์โพรเซส ด้วยการคลิกที่รูปยางลบ แล้วกดเริ่มมอนิเตอร์ คลิกที่รูปแว่น และทางฝั่ง Remnux ให้ทำการเปิดการมอนิเตอร์ Network ทำการโหลดมัลแวร์และรันมัลแวร์ ที่ VM-Win7 ให้สังเกตุโพรเซสของมัลแวร์ที่โปรแกรม Process Hacker โดยสามารถทำการ Kill โพรเซส ของมัลแวร์ได้ด้วยโปรแกรม Process Hacker ที่โปรแกรม Process Monitor กดรูปแว่นขยายอีกครั้ง เพื่อหยุดการตรวจจับ จากนั้น Save เป็นไฟล์ .csv ที่ VM Remnux ปิดโปรแกรม Wireshark แล้ว Save ไฟล์ .pcap และปิด fakedns ปลอม เมื่อทดลองเสร็จแล้วให้ทำการบันทึก logs จากโปรแกรม Process Hacker โดยจะได้ไฟล์เป็น .txt

Process I	lacker [PC\ptt]								a x
Hacker Vi	ew To	ols Users Help								
Processes	Op Services	Network Disk	indles or	DLLs >	• ⁴ System inf	ormation		×	Search Processes (Ctrl-	+ K)
Name			PID	CPU	I/O total	Private b	User nan	ne	Description	
> Syst	em Idle	Process	0	93.80		0	NT AUT	HORITYLSYSTEN		
	exe nit.exe		364 404 412	0.02		2.18 MB 1.44 MB 8.32 MB			Client Server Runtime Pro- Windows Start-Up Applica	cess ition
Save As		-	-			a trans				- 23-
				-						
, , , ,	nputer	Local Disk (C:)	 Progra 	am Files	 Process F 	lacker 2 P		• • • •	Search Process Hacker 2	,
Organize - Nev	vfolder									
Downloads	-	Name	^			Date modifi	ed	Туре	Size	
Secent Places		alugins				7/7/2020 2-0	07 PM	File folder		
	111	₩ x86				7/7/2020 2:0	7 PM	File folder		
Libraries		CHANGELOG.	tot			3/29/2016 1	2:18 PM	Text Document	26 KB	
Documents		COPYRIGHT.b	et.			2/17/2016 7	44 AM	Text Document	7 KB	
J Music	10.1	LICENSE.txt				2/17/2016 7	44 AM	Text Document	36 KB	
Videos		README.txt				3/26/2016 9	MA 55:	Text Document	3 КВ	
Computer										
Local Disk (C:)										
-	-									
	Process	s Hacker Processes.t	xt.							
File name:	and the second se									

ภาพที่ ๑๑๒ แสดงการ รันโปรแกรม Process Hacker

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

JOOSandbox Cloud	SIC OAnalysis _ Results (Search (hash, ID, tag) Deep Malware Analysis	Register Login
Define Sample Source and Choose Anal	vis System	*/: Advanced
Upfoad Sample Choose Br(5) max: f00mb	Browse URL	More Options
Choose Analysis System Select up to 3 of 3 available systems.		
Use Dive Interaction & Results Use Dive Interaction Settings Comments	() Execution / Run Time	
Show Advanced Settings	30 sec 120 500 sec	
Your complete analysis will be published on this website Accept Terms and Conditions	e and accessible to anyone (including screenshots). Upgrade to (Doud Pro to get a private account.
I agree to be bound by the Terms and Conditions and the Pers have accepted and understood the Terms and Conditions and the have accepted and understood the Terms and Conditions and the	onal Data Protection Policy and agree to the Personal Data Protection Policy.	Analyze with Joe Sandbox

ภาพที่ ๑๑๓ เว็บไซต์ Joesanbolbox.com

บทที่ ๖ การวิเคราะห์ข้อมูล

การวิเคราะห์ Network Forensic เราจะเริ่มจากค้นหาข้อมูลหมายเลข IP Address ต้นทาง ปลายทาง Port ที่ใช้รับส่งข้อมูลที่มีการรับส่งไฟล์ที่ถูกเรียกใช้ลิงก์เว็บที่อยู่ของไฟล์ http status อาจดูลึกไปถึงลักษณะการรับส่งข้อมูลว่าเป็นแบบ get/post/request ซึ่งหลายครั้งอาจเป็นการใช้ คำสั่ง Command line หรือ Sql Command โจมตีเข้ามา หรืออาจมีการอำพรางด้วยการเข้ารหัส เป็น Base64, Sha1, Sha256 รวมถึงการส่ง Byte Code เข้ามาในระบบ เพื่อทำให้เกิดการปฏิเสธ การให้บริการเว็บไซต์ หรือรบกวนการทำงานของระบบ สำหรับการวิเคราะห์ Network Forensics จะแบ่งย่อยตามโปรแกรมที่ทาง ทอ.ใช้งาน ประกอบด้วยโปรแกรม Wireshark, Imperva, Security Onion และ Deep Instinct โดยมีรายละเอียดการใช้งานและการวิเคราะห์ด้วยโปรแกรมทั้งหมด เช่น โปรแกรม Wireshark ใช้ในการวิเคราะห์ Network Forensic ชื่อโปรแกรมมีเครื่องมือหนึ่งที่ช่วย ให้เรา เห็นกลุ่มของข้อมูลที่เกิดขึ้นว่ามีปริมาณเท่าไหร่ โดยจะขอเริ่มจากการใช้งาน IO Graph เป็น การทำผลของข้อมูลแพ็กเก็ตที่เก็บมาได้นำมาแสดงผลในรูปแบบของกราฟ โดยที่สามารถทำการเลือก ชุดของข้อมูลมาแสดงผลได้ตามที่ต้องการโดยต้องใช้งานร่วมกับ Filter Statement ซึ่งจะแตกต่าง จาก TCP Flow Graph เป็นต้น

๖.๑ การแสดงผลโดยการใช้งาน IO Graph

- ๖.๑.๑ สามารถทำการซูมดูข้อมูลในแนวแกน x และแกน y ได้ (TCP Flow Graph ทำได้ไม่ดี)
- ๖.๑.๒ สามารถกำหนดสีของกราฟในการแสดงข้อมูลได้
- ๖.๑.๓ สามารถกำหนดรูปแบบของกราฟได้ เช่น กราฟเส้น impulse เป็นต้น
- ๖.๑.๔ สามารถใส่สูตรทางคณิตศาสตร์เพื่อคำนวนผลที่ได้และแสดงผลที่กราฟได้
- ๖.๑.๕ สามารถปรับแกน y ให้แสดงผลแบบ Logarithm เพื่อแสดงผลที่มีค่าแตกต่างกันมากได้

๖.๑.๖ สามารถนำค่าต่าง ๆ ที่ต้องการมาทำการแสดงผลเพื่อเปรียบเทียบความสัมพันธ์กันได้ สูงสุด ๕ ชุดข้อมูล



ภาพที่ ๑๑๔ วิเคราะห์กระบวนการทำงานของมัลแวร์



ภาพที่ ๑๑๕ การแสดงผลด้วย IO Graph

๖.๑.๗ การแสดงผลด้วย IO Graph การนำ IO Graph มาใช้แสดงผลข้อมูลจะได้ข้อมูลที่มี ้ความละเอียดในการแสดงผลด้านเวลา และ การนำชดข้อมลมาแสดงผลเพื่อเปรียบเทียบกัน ้ดังนั้นเมื่อเกิดความผิดพลาดระหว่างโปรแกรมที่ทำงานอย่ใน ระบบ Network เดียวกัน หรือมี Source-Destination ที่เกี่ยวข้องกันก็จะสามารถนำชุดข้อมูลที่ได้จากการ Filter ขึ้นมาทำการ แสดงผลเพื่อเปรียบเทียบการทำงานหรือความผิดปกติที่อาจจะเกิดขึ้นซึ่งส่งผลให้ระบบ Network ้ได้รับผลกระทบนั้นได้อย่างชัดเจนทั้งนี้ การใช้งานโปรแกรม Wireshark โดยปกติแล้วเมื่อเราต้องการ หาข้อมูลบางอย่างเช่นการที่เครื่อง Client ต้องการเปิด Connection เพื่อเริ่มสื่อกสารกับเครื่อง Server ตามเนื้อหาทางทฤษฎีเราจะเริ่มต้นทำการหา แพ็กเก็ต TCP SYN หรือในกรณีที่มีการปิด Connection จะต้องมีการส่งแพ็กเก็ต FIN เพื่อเริ่มการปิด Connection การสื่อสาร หรือกรณีที่เกิด ้ความผิดพลาดอื่นเช่นการเกิดแพ็กเก็ต Re-transmission ในกรณีที่มี การร้องขอข้อมูลที่ขาดหายไป กรณีที่ไฟล์แพ็กเก็ตมีขนาดใหญ่มาก การที่จะหาแพ็กเก็ตดังกล่าวอาจจะทำได้ยาก เนื่องจากแพ็กเก็ต SYN/FIN จะมีการส่งออกมาเพี้ยงแค่ครั้งเดียว ดังนั้นโปรแกรม Wireshark จึงมีเครื่องมือ สำหรับการ ทำสรุปเหตุการณ์ที่สำคัญที่เกิดขึ้นจากแพ็กเก็ตที่เปิดขึ้นมาในโปรแกรมไว้ให้นั้นคือ Expert Information นั่นเอง โดยใน Expert Information จะทำการสรุปความผิดปกติของการสื่อสารและ ้จะสรุปรวมเหตุการณ์ต่าง ๆ ที่พบอยู่ในแพ็กเก็ตที่กำลังเปิดใช้งานอยู่ไว้เป็นกลุ่มของเหตุการณ์ ดังนั้น การค้นหาความผิดปกติต่าง ๆ ที่เกิดขึ้นก็จะสามารถทำได้โดยง่ายจากการใช้งาน Expert Infotrintion สำหรับรูปตัวอย่างของข้อมูลที่ได้จาก Expert Information จะมีตามภาพที่ ๑๐๕

eve	erity	Summary	Group	Protocol	Count
-	Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	171
- 1	Warning	Connection reset (RST)	Sequence	TCP	5
- 1	Warning	TCP Zero Window segment	Sequence	TCP	89
	Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1306
	Warning	Previous segment(s) not captured (common at capture sta	Sequence	TCP	2812
	Note	This frame is a (suspected) retransmission	Sequence	TCP	3260
	Note	Duplicate ACK (#1)	Sequence	TCP	9224
4	Note	This frame is a (suspected) fast retransmission	Sequence	TCP	2391
	Warning	ACKed segment that wasn't captured (common at capture	Sequence	TCP	1
	Chat	Connection establish request (SYN): server port 2074	Sequence	TCP	4
	Chat	Connection finish (FIN)	Sequence	TCP	8
	Chat	TCP window undate	Sequence	тср	662
dis	splay filter set.				

ภาพที่ ๑๑๖ แสดงข้อมูลสรุปที่ได้จาก Expert Information

การเพิ่ม Column เพื่อแสดงข้อมูลเพิ่มเติมโดยปกติแล้วโปรแกรม Wireshark ้จะมีการแสดงผลทางหน้าจอโปรแกรมเป็นค่ากลางของ โปรแกรมอยู่แล้วคือค่า Default เพื่อใช้แสดงผล แบบทั่วไปซึ่งเพียงพอต่อการใช้งานอยู่แล้ว แต่ในบางกรณี ผู้ใช้งานต้องการนำข้อมูลบางอย่างที่ตัวเอง สนใจไปแสดงผลเพื่อให้สามารถตรวจสอบการทำงานของ Network ที่กำลังวิเคราะห์ ดังนั้นการเพิ่ม ชุดข้อมูลลงไปเพื่อนำไปแสดงผลเป็น Column ใหม่จึงเป็นทางเลือกที่ดีทำให้การวิเคราะห์สะดวกมากขึ้น โดยโปรแกรม Wireshark สนับสนุนความสามารถนี้ให้ผู้ใช้งานสามารถนำชุดข้อมูลมาแสดงผลได้ ตามที่ต้องการ เช่น การแสดงผลของค่า TCP Time ซึ่งเป็นข้อมูลที่โปรแกรม Wireshark สามารถทำ การคำนวนได้จากแพ็กเก็ตตามปกติ สามารถนำข้อมูลชุดนี้มาแสดงผลเป็น Column เพิ่มเติมได้ เช่นเดียวกันตามภาพที่ ๑๐๖ การนำค่า TCP time มาแสดงผลเป็น Column เพิ่มบนโปรแกรม Wireshark การใช้งาน Profile ต่อเนื่องจากหัวข้อการเพิ่ม Column เมื่อเราต้องการข้อมูลขึ้นมา ้แสดงผลเพื่อให้เหมาะกับการใช้งานวิเคราะห์หรือศึกษาข้อมลจากแพ็กเก็ตโดยการเพิ่มชดข้อมลต่าง ๆ เช่น Column ของ TCP delay หรือ HTTP Response เพื่อให้สามารถอ่านค่าได้ง่ายมากขึ้น แต่ในกรณี ู้ที่ไม่ต้องการอ่านค่าดังกล่าวแล้ว การแสดงผล Column เหล่านั้นก็จะกลายเป็นข้อมูลที่ไม่ได้ถูกใช้งาน และกลายเป็นสิ่งที่รบกวนการทำงาน เนื่องจากเป็นการรบกวนสายตา ดังนั้นโปรแกรม Wireshark ้จึงได้มีการจัดการโปรไฟล์ในการแสดงผลข้อมูลขึ้นมาเพื่อใช้แก้ไข เช่น ในกรณีที่ต้องการวิเคราะห์ การทำงานของ HTTP ก็ให้ทำการจัดการแสดงผลให้เหมาะสมและทำการบันทึกเป็น HTTP Profile ้ต่อมาเมื่อต้องการวิเคราะห์ข้อมูลการใช้งานเกี่ยวกับ Database ก็ทำการสร้างการแสดงผลของ Database และบันทึกไว้ กรณีที่ต้องการใช้งานแบบปกติก็ทำการ เรียกค่า Default Profile มาใช้งาน ถ้าต้องการกลับไปวิเคราะห์การทำงานของ HTTPก็ทำการเรียก HTTP Profile กลับมาใช้งานได้ทันที การสลับการแสดงผลของ Profile แบบนี้ มีความยืดหยุ่นการการใช้งาน มากกว่าการใช้งานแบบปกติ ซึ่งจะต้องมีการจัดการแสดงผลใหม่ทุกครั้งที่ต้องการใช้การแสดงผลข้อมูลในแบบเฉพาะเจาะจง

Fil	web.po e Edit	capng View Go	Capture Analyze Stat	istics Telephony Wireles	s Tools H	Help				-	۵	×	
4	10	0	X C 9 0 0 1	T 🛓 📜 🔍 Q	Q. 🎚					100.0	European		
No.	вррку а	Time	Source	Destination	Protocol	Length	TCP Delay	HTTP Time	DNS Time	Info	Expressi	on	^
1	3597	288.242001	210.1.61.48	192.168.1.102	TCP	54	0.030345000			80 - 51104	[ACK]	s=	
	3598	288.254045	210.1.61.48	192.168.1.102	TCP	1506	0.017051000			80 - 51102	[ACK]	s	
	3599	288.255005	210.1.61.48	192.168.1.102	TCP	1506	0.000960000			80 - 51102	[ACK]	s=	
	3600	288.255008	210.1.61.48	192.168.1.102	HTTP	256	0.000003000	0.043793		HTTP/1.1 2	00 OK	(
	3601	288.255103	192.168.1.102	210.1.61.48	TCP	54	0.000095000			51102 → 80	[ACK]	s	
1	3602	288.297239	192.168.1.102	192.168.1.1	DNS	90				Standard q	uery 0	3	
	3603	288.344259	192.168.1.102	104.215.179.97	TCP	104	0.488244000			51100 → 50	005 [PS	SH	
1	3604	288.344410	192.168.1.102	111.221.107.95	TCP	104	0.396595000			51119 → 50	003 [PS	5H===	
	3605	288.352369	192.168.1.1	192.168.1.102	DNS	208			0.055130_	Standard q	uery re	25	
	3606	288.353363	192.168.1.102	40.113.87.220	TCP	66	0.00000000			51120 - 44	3 [SYN]		
	3607	288.353403	192.168.1.102	40.113.87.220	TCP	66	0.000000000			51121 → 44	3 [SYN]		
	3608	288.359762	192.168.1.1	239.255.255.250	SSDP	368				NOTIFY * H	TTP/1.1		Y
<												>	

ภาพที่ ๑๑๗ การแสดงผลโดย Custom Profile

4	web.pca	png					- 🗆 X	
File	Edit	View Go Ca	pture Analyze Statistic	s Telephony Wireles	s Tools	Help		
A	1	0 📙 🗄 🗙	C 9 * * * 7	1 🔄 🗐 Q Q	Q II			
	ipply a di	splay filter <ctrl-< td=""><td> ></td><td></td><td></td><td></td><td>📑 🔹 Expression</td><td>ŀ</td></ctrl-<>	>				📑 🔹 Expression	ŀ
No.		Time	Source	Destination	Protocol	Frame Length	Info	^
	3605	288.352369	192.168.1.1	192.168.1.102	DNS	208	Standard query response 0x3276 A mobile.pipe.ar	
3	3606	288.353363	192.168.1.102	40.113.87.220	TCP	66	51120 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=144	
ţ.	3607	288.353403	192.168.1.102	40.113.87.220	TCP	66	51121 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=14	
	3608	288.359762	192.168.1.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1	
	3609	288.402173	104.215.179.97	192.168.1.102	TCP	54	50005 → 51100 [ACK] Seq=2165 Ack=1928 Win=33792	
	3610	288.423644	192.168.1.102	210.1.61.48	HTTP	630	GET /wp-content/themes/my-way/media/images/twit	
	3611	288.445132	111.221.107.95	192.168.1.102	TCP	54	50003 → 51119 [ACK] Seq=138 Ack=264 Win=29696 (
	3612	288.461138	210.1.61.48	192.168.1.102	HTTP	1086	HTTP/1.1 200 OK (PNG)	
<	3613	288.469066	192.168.1.102	210.1.61.48	HTTP	632	GET /wp-content/themes/my-way/fw/plg/my_demo/my_	v

ภาพที่ ๑๑๘ การแสดงผลโดย Default Profile

๖.๑.๘ การทดลองตรวจสอบและดึงข้อมูลจากแพ็กเก็ต HTTP ให้ใช้โปรแกรม Wireshark จับแพ็กเก็ตระหว่างใช้งานอินเทอร์เน็ต ในระหว่างนั้นให้ทำการเข้าเว็บไซต์และเปิดไฟล์ชนิดต่าง ๆ เช่น รูปภาพและวิดีโอ เป็นต้น ทำการหยุดจับแพ็กเก็ต และบันทึกเพื่อทำการทดลองต่อไป สิ่งที่จะ ได้รับจากการทดลองสามารถทำการดึงข้อมูลชนิดต่าง ๆ ออกมาจากแพ็กเก็ต HTTP เพื่อทำการ ตรวจสอบการทำงานได้ (Forensics) ขั้นตอนการทดลองเตรียมความพร้อมด้วยการตรวจสอบการตั้งค่า ของโปรแกรม Wireshark ก่อนทำการกดปุ่มที่ Edit Preferences ที่หน้าต่าง Wireshark Preferences ให้ทำการหาโปรโตคอล IPv4 และเลือก Reassamble Fragmented IPv4 Datagrams ที่หน้าต่าง Wireshark Preferences ให้ทำการหาโปรโทคอล 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 ด้วยการกด ปุ่ม Save As ทำการเปิดไฟล์ที่บันทึกลงในเครื่องขึ้นมาดูว่าได้ไฟล์ที่สมบูรณ์หรือไม่ จากตัวอย่างจะ เป็นไฟล์ 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 เพื่อทำให้ 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 ไว้ที่ ตำแหน่งใดก็ได้ ทำการเก็บไว้ที่ C;\Users\demo\Desktop\sslkey.log เสร็จแล้วให้ทำการ Restart ้เครื่องที่ต้องการถอดรหัส SSL จากนั้นให้ทำการเปิดใช้งาน Web Browser ตามปกติ โดยให้เน้นทำ การลองเข้าใช้งานเว็บไซต์ที่เป็น HTTPS เพื่อให้ Windows ทำการ Export SSL Log ให้กับเรา โดยให้ลอง Login เข้าใช้งาน Web mail เช่น Gmail หรือ Outlook เป็นต้น เพื่อลองหา Username และ Password ในการ Login จากการถอดรหัส SSL ขั้นตอนที่ ๓ เปิดโปรแกรม Wireshark และทำการ เพิ่ม 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 และค้นหาข้อมูลที่น่าสนใจจาก Packet

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

A pioneer and leader of a new category of data security solutions for high-value business data in the data center.	User: Password: Login
Show License Status ↔	
Show Copyright Information 🛛 🗧	

ภาพที่ ๑๑๙ โปรแกรม Imperva

เข้าไปที่เมนู View Resuilts> Manage Reports เลือก Group ของรายงานที่ ต้องการ จากนั้นให้คลิกที่ Tab Data Scope >กำหนดวันที่เริ่มต้น และวันสิ้นสุด > กดบันทึก กลับมาที่ Tab General Details >กำหนดรูปแบบไฟล์ ในที่นี้แนะนำเป็น .CSV > คลิก Run Report และทำการดาวน์โหลดไฟล์ ทั้งนี้การใช้งานสามารถเปิดด้วยโปรแกรม Microsoft Excel โดยสามารถ นำ Logs มาวิเคราะห์สถิติการโจมตีของแต่ละประเทศ รูปแบบการโจมตี ความสำเร็จของการโจมตี หมายเลข IP Address แล้วนำไปดำเนินการ Block โดยการวิเคราะห์จะนำหมายเลข IP Address ไปตรวจสอบกับเว็บไซต์ VirusTotal.com และ AbuseIP เพื่อหาความสัมพันธ์กับกลุ่มหรือหมายเลข IP Address ที่เป็นภัยคุกคาม

SECURESPHERE REP	ORTS MONITO	1							D-Min 2-
ushboard Alerts Violations 1	lystem Events	Bocked	Sources M	onitor 3	/55#/11				Ad
Quick Filter	Alerta Hillers	0				Alert 4111117	: Distributed Unknown Parameter on d	o.rtaf.mi.th/media/w	pitem/coa/modal.
(7)	Luci Dave	1.000			(bills				And a construction
CADEN	a presentation		11 10	100	prest may	Actional		17.251	
12	8 94 1	0	· Updated	* 8.9	al Designo •		Security Pattorn werk: a message was one February 27, 2025 2 57 26 PM	out to the system roll be	10.226 190.21
Bese, filter Secol Filters	List and Hour D	1					Security Phillom Alerts: An email was sent to	s servermonitering Qriat	Inith (February 27,
I fy bereity	41111114		1417.25		Introdec Unknown Parameter on do ital ini thimedia kystemicos modal cas parameter (UTBC402554220504tbL*C2c15515a4	1000	2023 1 17 24 PM)		
1) By inmediate Action	41111182		14:57:28	10	Intributed Unknown Parameter on do stall m. thimedia system (almostocia-core ja parameter 4070;44080412090/mb4763;c1581164	Policy	Income_SI_MIGH		
E By And Type	4111155		14157.00		Jacoburod Unknown Parameter on doural as phinedia system balmonous wore ja parameter 6010x4665432090x4667551101644	Estreity	Kavadedge Base		
E DI ANNER	41111177		14:57:57	40	Jastribuited Unknown Parameter on dourbal.mi.ithinedia jurija hootskingumin ja parameter 6070c466584120984rfb6763c1581664	Annalated	IN THE SECTION AND A STREET AND	Wandstown (Red and	And 12 TO 19
T by wet hunder	41111183		14:17:27		Netburkd Unknown Parameter on dourtal multimedia bally bowry angests win je parameter 60%r 4665643598ch/b4243ch581664	- And the second	an that is it manual at any other	a competer liner of	and stor any-
a by serve wrote	4101181		14.57.07	41	Net/Ibuitod Unknown Parameter on doursal mi. Brinadia Sailja Sowere nocenflict ja parameter 857bc4665546501064/b6763c1581464	. 3			
 By Application 	4101178		14.57.07		Natributed Unknown Parameter on dourtal multimedia baile basers min ja parameter 4070s 44655450004/h8745c15516c4				
T By User Name	41111175		14.57:37		Autobarted University Parameter on dourted an drived a faile loser a success minute parameter #170x488554809864654745c15516e4	0			-
1 By Starte IP	41011586		14.57.97	10	Autobalad Unincean Parameter on dourbal as Brinedia's unternitaic spotential parameter 6070c456564020804/b6763c1581864				
g By Petron	41011150		14:57:37	**	Autobacked Unitscenni Parameter on discted an University weeternian one a parameter 607(c4866548208)/e866762c16216e4				
E Ry LPR	41111176		14.57.27		Autobacked University Parameter on dourbal on thimself a fundeminationada (a parameter 0070c4665648206blefbd705c16616e4				
C By Session ID	A1011176		1457.07	10	Astributed Unknown Parameter on duutal w. D.hemplates protostarius template cas parameter 00700.00056102904eb6703c16416et	Aiert apprepaie	i ilyi	Stateboar bit	WARD
C Dy Drett D	4111154		14:52:27	10	Astrobuted Unknown Parameter on dourtal an ith terrolates protostaria terrolate a parameter 6076x460054800105456760c1581464	Codent rate 1	Ville As def as B	Deses or at o	Volum.
 By Second another of 	#1808080		141226	441	Applicated Abstractive Long Respect	Immediate Activ	n Time	Seutes Geol.	scations 2 A
Ev Severa Gask scatter	41111057		1412-21	12	Instributed Unknown Parameter on their staf mith templates beste staf i sa have been star 27 acr 27 20111543/attr 22 relified (2019)	Method	OFT	PL .	2.0
T Geveraled by Threadkalar	4101015		14(27(2))		Settladed Descence Parameter on dot dad as to benolate technicate to benolate to benolate a benerity 27ao 27203/1624/0204020100	Paramater Nam	 6070c468554020004b6763;15816e4 8714 	Sessors	0
	41011738		1412/15	1	Inknown Parometer 1677484619125 in offer rist militanaonaintef 45.3.012 jao	URL STORE	Impdial pythemic psimodal cas	User Agente	8.75
	4110827		1412/10	100	Intelligibility of the same that any start and the intelligibility to compare the startments (\$15776/2018)(759)(10)(10)(10)(10)(10)(10)(10)(10)(10)(10	1.10		Vieb User	
	41408626		14:57:18	485	Instituted University Personney on ance staf with Instituted Information According to accompting to accompting the INVESTIGATION ACCORDING ACCORD.	Volder			
	41853621		14.62-68	152	Intelligiated Distances Parameter on sport dation Protocing system because content and parameter \$557 to \$555172681 (545)4656417	Searce P.		Section	User
	41103622		14.57/18	101	Natilbuled University Parameter on ecce. dof mith benefative protector transfermings are parameter 601706/01007266/c16c134466-410	49 228 113	Mé	NA	Lane.
	41103824		1412-17	402	Indefinited Unknown Parameter on approxidation Informativability Security microla with to parameter 8337/ds3058872950-551334855-610	49 231 230	31	80.	
	41100623		14.62.07	100	National University Parameter on apport dat multimediative Insurance in a parameter \$2577.0x2010572681 (5613)/468e/115	201.170.14	cene 1 150	NA	
	41458628		14.62.47	486	Intributed Between Parameter on some dat nichtendiskovlandskrauten is aarander 6000 (2007)00-56/3480a140	1 27 55 34 7		NA	
	41150620		14.62.67	190	Satisfacted Universe Parameter on soon dat to th temptote instantia is provide to parameter (307 (a)(31))/(a)(31))/(a)(31))/(a)(31))/(a)(31))/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/(a)(31)/	18 101 22 88	63	16.0	
	4110020		1812-12	114	tatebulard University Research on according to the Antipational According to the Antipational State	49 229 240	199	No.	
	4180965		1612/05		Introduced University Parameter on according to Dimension on a compared CDT Net 2011 Section 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	124 122 30	W .	hit	
	Analysis		1812-08	N	table of the second measure of a second real of the second				
	410000		141210	1	Satisfied Disaster Partners as word, dot as it leads where is mariners done is assessed Diffue Conferential Addition				
	ALCONG.	1	1107.00	1					

ภาพที่ ๑๒๐ การวิเคราะห์ลักษณะของ URL โดยโปรแกรม Imperva

อีกส่วนหนึ่งก็คือการวิเคราะห์ลักษณะของ URL ที่เข้ามาว่าเป็นความพยายามทำอะไร มีการตอบกลับของ Server ฝั่งเราหรือไม่ มีการ Block ของ Firewall หรือไม่ และส่งผลกระทบ ต่อเว็บไซต์ใดของกองทัพอากาศ เพื่อให้การวิเคราะห์มีความครบถ้วนสามารถสืบค้นเหตุการณ์ ย้อนหลัง จึงต้องมีการนำเข้าข้อมูล และจัดเก็บในระบบฐานข้อมูล phpMySQL เพื่อใช้ในการทำรายงาน

๖.๑.๑๑ Security Onion เป็นโปรแกรมประเภทแจ้งเตือน และวิเคราะห์ Logs จากการ เข้าถึงทางเครือข่ายสารสนเทศของกองทัพอากาศ ทำหน้าที่รวบรวม จัดเก็บแยกประเภทโปรโทคอล ภัยคุกคาม และแจ้งเตือน (Alert) โดยรับ Logs จากอุปกรณ์เครือข่ายที่ทำหน้าที่เป็น Core Switch ดังนั้นหากเกิดการโจมตีจากภายนอกเครือข่ายหรือภายในเครือข่ายของ ทอ.จะสามารถตรวจสอบจาก โปรแกรมนี้

← → C	 Not secu 	re 10.22	6.82.52/	squert/in	ndex.php?id	l=f6cb41c1	32abf8777203bab7b	2279c10					\$	0	* 😁	
EVENTS	SUMMAR	X	VIEWS				o ⁰ 🗆 🗭		6	T Fi	tor					-
	INTERVAL	: 2021-01-1	15 00:00:0	0 -> 2021	-01-15 23:59:5	\$9 (+07:00)	FILTERED BY OBJECT:	NO FI	LTERED BY	SENSOR:	NO	PRIORITY:	60	ons 📃 💳	0.2%	0.376
OGGLE	^	1,400							22198 24	4827						
queue only	on	1,000				18	247 17516 17882	1922								
prouping	on	800 132 600 1	36				12230	13001	See	ie-si						
AUMINARY .	^	200	, 1296	502 . 71	997 15	91 . 3149	"Tensorgenete" 30	State Stat	10000	-2024						
queued events	165271	0 1	01 0	2 03	04 05	06 07	08 09 10 1	11 12	17 14	3.5	16	17 18	19	20 21	22 23	20
total events	167286	-	-									1000		-	-	1
total signatures	192	QUEUE	Sec	or .	ACTIVITY	CAST EVENT	SEGRETORE					10		Picoro	The TOTAL	
PRIORITY	~	28369	3	I		14:59:12	ETPRO TROJAN C	obalt Strike E	Beacon Obse	beved		2812918	5	6	16.983%	é .
high		2912	52	22		14:59:12	ETPRO INFO Susp Observed	icious User-A	Agent contai	ning Load	er	2839331		6	1.743%	
9006 (60.0%) medium		47137	141	83		14:59:11	ETPRO INFO HTT Header Observed	P Request will	th Lowercas	e user-ag	ent	2845391		6	28.219%	i.
5616 (29.8%) low	320 (0.2%)	9968	11	8		14:59:10	ETPRO TROJAN A	ndromeda/Gi	amarue Che	ckan		2809682		6	5.979%	
other	97 (0.1%)	143	56	4		14:59:10	ETPRO TROJAN O	bserved Glup	steba CnC D	omain in 1	ILS SNI	2844627		6	0.086%	
CLASSIFICATION	~	13207	116	1109		14:59:09	ETPRO POLICY X	4R CoinMiner	Usage			2826930	ē.	6	7.906%	
compromised L1		-									20			1000	10,000,000,000	
compromised L2	-	219	3	12		14:59:06	ETPRO MALWARE	Observed PL	UA SSL Cert	(Ausiogic	-5	2835326		0	0.131%	
attempted access		916	1	1		14:59:05	ETPRO INFO DYN	AMIC_DNS Q	wery to *.gi	cp.net Do	main	280-4809	6	17	0.548%	
denial of service		Concession in the local division in the loca														
policy violation		1880	16	310		14:59:05	ETPRO POLICY OF	bserved SSL 0	Cert (IP Loo	kup - ipify	.019)	2831048		0	1.125%	
reconnaissance		12931	130	786		14:59:04	ET POLICY PE EX	or DLL Wirk	dows file do	which H	TTP	2018959	6	6	7.741%	
malicious	-	-	-													
no action reg'd.		9814	8/3	9		14:59:02	ETPRO POLICY A	saroid Device	Connectivit	y cneck		2832602		0	5.675%	

ภาพที่ ๑๒๑ Security Onion

ก่อนอื่นต้องทำการเซ็ตค่าวันเวลาของ Logs ให้เป็นเวลาประเทศไทยเสียก่อน เพื่อป้องกันความสับสนกับเวลาจริง (Time Zone) เมื่อเกิดการโจมตี โดยนำเมาส์ไปคลิกที่เวลา ดังภาพที่ ๑๑๑

EVENTS	SUMMAR	Y VIEWS O ^M 🔲 🗭 🗄 🏲 Filter			
	INTERVA	: 2021-01-15 00:00:00 -> 2021-01-15 23:59:59 (+07:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO	PRIORITY:	60.0%	0.2%
TOGGLE	_ ^ i	1400			
queue only	on	1,000 3 33331 1/202			
grouping	on	600 122230 122230 600			
SUMMARY	^	400 200 , 1296 302, 752 997 1661 3149			
queued events	165271	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	17 18 19	20 21	22 23
total events	167286		100	-	
total signatures	192	QUEUE SC DC ACTIVITY LAST EVENT SIGNATURE	10	PROTO	% TOTAL
RIORITY	~	28369 1 1 1 ETPRO TROJAN Cobalt Strike Beacon Observed	2812918	6	16.9839
		2912 52 22 14:59:12 ETPRO INFO Suspicious User-Agent containing Loader	2839331	6	1.743%

คลิกเครื่องหมายถูกออกแล้วกด 🌮 เพื่อให้ระบบโหลดข้อมูลใหม่

TOGGLE	^	0	, 1295 S	03 04 05	06 07 08	09 10	11 12 13	14 15	16 17 1	19	20 21	22 23
queue only	on											
grouping	on	QUEUE	ระ สถิติ	oc ACTIVITY อ ต้นทาง-ปล	LAST EVENT S	IGNATURE	ชื่อเหตุการเ	ณ์	ID		PROTO	% TOTAL
SUMMARY	^		115	Tes BUILDERE	15:17:33		v x348, schloer Usa					8.007%
queued events	174720	48527	144 4	34	15:17:35	TPRO INFO	HTTP Request with Lo	wercase user-a	ent 2845	391	6	27.477%
total events	176758					leader Obser	ved					
PRIORITY	^	erver; cor O, update	tent:"user-a d_at 2020_1	gent[3a 20]"; fast_p 1_09;)	attern; http_header;	classtype:b	ad-unknown; sid:28	45391; rev:2;	metadata:create	i_at 2020	_11_09, form	ser_category INF
PRIORITY high สถิติโจ 106531 (61.0%) medium	มดี	file: down	tent:"user-a d_at 2020_1 oaded.rules	gent[3a 20]"; fast_p 1_09;) :17477 5つじる 7 EVENT(5) 単	attern; http_header; อะเอียด logs create filter: ระร	dat both	ad-unknown; sid:28 รายส	45391; rev:2; กะเอียดที่ม	n ip	1_at 2020	_11_09, form	ser_category INF
PRIORITY high สถิติโจ 06531 (61.0%) medium 57554 (38.7%) low	330 (0.2%)	erver; cor O, update file: down	tent: "user-a d_at 2020_1 oaded.rules contze 4852	gent[3a 20]"; fast_p 1_09;) \$12477 \$188 7 EVENT(5) LAST EVENT	attern; http_header; อะเอียด logs create filter: ระร source	dat both	ad-unknown; sid:28	45391; rev:2; 1ะเอียดที่ม	In ip	1_at 2020 AGE	COUNTRY	ser_category INF
PRIORITY high สถิติโจ 06531 (61.0%) medium 7554 (31.7%) low other	330 (0.2%) 98 (0.1%)	erver; cor O, update file: downi Catter QUEUE	tent: "user-a d_at 2020_1 oaded.rules contze 4852	gent[3a 20]7; fast_p 1_09;) 117477 \$788 7 EVENT(S) 1LAST EVENT 2021-01-15 15:17:53	attern; http_header; อะเอียด logs cREATE FILTER: <u>stc</u> source 10.227.17.128	dat both AGE 659	ad-unknown; sid:28 รายธ country <i>คระเรเธ (Ja)</i>	45391; rev:2; 1ะเอียดที่ม	In ip RESTINATION	AGE 66	COUNTRY	AND (.th)
PRIORITY high สถิติโจ 06531 (61.0%) medium 7554 (31.7%) low other	330 (0.2%) 98 (0.1%)	erver; cor O, update file: down CATEG 2664 2170	tent:"user-a d_at 2020_1 oaded.rules contze 4852	gent[3a 20]7; fast_p 1_09;) 117477 \$7186 7 EVENT(5) LAST EVENT 2021-01-15 15:17:53 2021-01-15 15:17:53	attern; http_header; มะเอียด logs cREATE FILTER: มะ source 10.227.17.128	das both AGE 659	ad-unknown; sid:28 ว่ายะ country คระเรเล (4a) คระเรเล (4a)	45391; rev:2; 1ะเอียดที่ง 	In ip RESTINATION 119.46.206.250	AGE 66 66	COUNTRY	AND (.th) AND (.th)
PRIORITY high SDDI (6531 (61.0%) medium (7554 (38.7%) low cther classification	330 (0.2%) 98 (0.1%)	erver; cor O, update Re: down Carter 2664 2170 220	tent: "user-a d_at 2020_1 oaded.rules contze 4852 ACTIVITY	cont13a 20[7; fast_pl.09;) cl.09;) cl.09; cl.01; cl.01;	attern; http_header; สะเอียด logs cREATE FILTER: มระ SOURCE 10.227.17.128 10.227.17.128 10.227.17.128	dat both AGE 659 659	COUNTRY RFC1918 (.kt) RFC1918 (.kt) RFC1918 (.kt) RFC1918 (.kt)	45391; rev:2; าะเอียดที่ม	In ip RESTINATION 119.46.206.250 119.46.206.251 103.10.124.69	AGE 66 66	COUNTRY	AND (.th) AND (.th) KONG (.hk)

ภาพที่ ๑๒๓ สถิติที่ทำการโจมตี

สำหรับข้อมูลที่เราจะได้จาก Security Onion นั้นจะมีหลายส่วน โดยหลัก ๆ ก็คือ สถิติที่ทำการโจมตีเข้ามาทำให้เราทราบว่า ณ ปัจจุบันมีความพยายามโจมตีระบบด้วยเทคนิคประเภท ใดมีเป้าหมายไปยังที่ไหน ทั้งนี้ยังสามารถใส่ IP Address เพื่อค้นหาเครื่องผู้ใช้งานในระบบ พร้อมทั้ง มี Tab Summary เพื่อสรุปและแสดงกลุ่มข้อมูลลำดับ ๑ – ๑๐ ของการโจมตี และแผนที่แสดงการ โจมตีจากทั่วโลกอีกด้วย

๖.๒ การวิเคราะห์ Host Forensic

การเตรียมหลักฐานก่อนการวิเคราะห์ (Master and Slab) ไม่ว่าจะเป็นฮาร์ดดิสก์หรือ RAM ก็ต้องทำค่า Hash เสมอ ซึ่งกระบวนการโคลนดิสก์หรือแคปเซอร์ RAM ด้วยโปรแกรม FTK โปรแกรม จะทำการสร้าง Hash ให้อัตโนมัติเมื่อได้ทำการโคลนเสร็จ โดยผู้ทำการเตรียมหลักฐานก่อนการ วิเคราะห์ต้องทำการบันทึกข้อมูลหรือถ่ายภาพไว้ด้วยเสมอและจะต้องเตรียมฮาร์ดดิสก์ไว้ 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 ฮาร์ดดิสลูกที่สองใช้ทำอิมเมจไฟล์ สำหรับหาข้อมูลที่อาจถูกลบ ไปประวัติการใช้ไฟล์ต่าง ๆ อาจเรียกว่าเป็นการวิเคราะห์ด้วยโปรแกรมอัตโนมัติ

64		AccessData FTK Imager 3.4.3.3						
the New Hote Sep-		-						
the set of								
	Printerna		Size Type Date Ma	diat				
			Constinue Images					
			Figure states and states and					
		Construction:	[the best of the second secon	Carrier 201282				
		The law	Creating mage					
	1	a magness						
Custom Content Sources								
Enderus Pie Isolen Patri Pie Optore		2	mand time. [1-03-30					
			Cancat					
al m	1.4.1							
Properties mex Value 2-1. Custom Cont	Read II.							

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 ในที่นี้จะขอกล่าวแค่ 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 #> rm /var/log/message หรือ #> cat /dev/null > file_log.txt สำหรับระบบปฏิบัติการ Windows จะเรียกว่า Even Logs และจะถูกเก็บไว้ ดังภาพที่ ๑๑๔

Open	Computer Management (Local	Keywords	Date and Time	Source .	Event ID	Task Category		Actions
Device Manager	> (7) Task Scheduler	Audit Succ	21/4/2558 17:01:39	Microsoft Wi	4624	Logon	1	Security
Manana	A Bill Event Viewer	Aude Succ	21/4/2558 16:57:41	Microsoft Wi-	4634	Logoff		Open Saved Log
	> Custom Views	Audit Succ	21/4/2558 16:57:41	Microsoft Wi	4634	Logoff		Y Create Custom View
Map network drive	a 💊 Windows Logs	Audit Succ	21/4/2558 10:57:41	Microsoft Wi	4634	Logoff		Import Custom View
Disconnect network drive	Application	Aude Succ	21/4/2558 16:57:41	Microsoft Wi	45.34	Logoff		
	Security	Aude Succ	21/4/2558 16:57:29	Microsoft Wi	4624	Logon		Clear Log
Create shortcut	E Setup	Audit Succ	21/4/2558 16:57:29	Microsoft Wi	4624	Logon		Filter Current Log
V'z Shadow	• Ja System	Aude Succ	21/4/2558 16:57:29	Microsoft Wi	40.34	Logott		Properties
Delete	Forwarded Event	Audit Succ	21/4/2558 16:57:29	Microsoft Wi_	46.24	Logon		00 Find
Rename	Approximations and set	Audit Succ	21/4/208 1609 43	Microsoft Wi	40.14	Logon		
	Shared Folders	Audit Succ	21/4/2008 10:00:42	Microsoft WL.	40.04	Logon		hell Save All Events As
Properties	The Local Divers and Genues	Audt Succ	21/4/2538 10:56:42	Microsoft wi	40.54	Logon		Attach a Task To this
	Redormance	Audit Succ	21/4/2558 10:50:42	Microsoft Wi	40.94	Logott		View
	- Device Manager	Aude Succ	21/4/2558 10:50:42	Microsoft Wi	40.04	Logon		Coll Badance
	. Storage	C funda Surce	20.00/2008 10:00/42	Macrosoft W.	40.74	Logon		and the second
Adobe Launda	Disk Management	AUGE SUCC	21/4/2008 16:06/42	Microsoft Willia	40.14	Logon		Help
Acrossi 7	E Services and Applications	Event 4624, Micro	soft Windows security auditing.				×	Event 4624, Microsoft Win
	and and a	General Data						Event Properties
PS S		Large Large					101	Will Attach Tark To This E
er Photoshop Mooil	100 m	An account w	as successfully looped on.				100	and the second s
- Shortcut Forder								olici cobh
		ISubject:						he Save Selected Events_
		Loo Neme	Security				1	G Refresh
CLEAN COLOR	and the second se	Same	Microsoft Windows security	Loopert	21/4/2558 17:01-30			El Main
Format Play 1719		E	ACM	Tank Calencer	Longe			
Factory Dem	and the second sec	Event an	4024	Task Category	Logon			
	and the second se	Level	antormation	Keywords:	Audit Success			
	and the second se	User	N/A	Computer	sid-sec2-07.intell.rt	af.mi.th		

ภาพที่ ๑๒๕ การวิเคราะห์ Disk Image

นอกจากนี้ Windows ยังเก็บ Log ไว้ในตำแหน่ง C:\WINDOWS\system32\logFies 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) จะเป็นเรื่องของการหาข้อมูล จากการเปลี่ยนแปลงของไฟล์เมื่อผู้ใช้มีการใช้งานไฟล์ ทำให้ทราบได้ว่าใครเป็นผู้รันไฟล์ และไฟล์เกิด จากที่ใดเป็นครั้งแรก มีการแพร่กระจายไปที่ใดบ้าง เนื้อหาส่วนนี้มีรายละเอียดเพิ่มเติม แนะนำให้ ศึกษาจากเอกสารของ SANS ดังภาพที่ ๑๑๖



ภาพที่ ๑๒๗ วงจรชีวิตของไฟล์

๖.๒.๓ โพรเซสพื้นฐานในระบบ Windows นักวิเคราะห์ควรรู้ว่าพื้นฐานของ Host Windows ที่จะช่วยลดกระบวนการค้นหามัลแวร์ที่เกิดขึ้นได้อย่างรวดเร็ว โดยสามารถใช้ข้อมูลตัวอย่างการ วิเคราะห์โพรเซส เป็นข้อมูลอ้างอิงเพื่อให้ทราบว่าในสถานะการใช้งานปกติมี Service อะไรบ้างใน ระบบ Windows หากเกิดความผิดปกติจะช่วยให้การวิเคราะห์มีความถูกต้องมากขึ้น ดังแสดง
๖.๒.๓.๑ Service system> Parent Process : Default Part = ไม่สามารถสร้างได้ จาก 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 ของ ระบบปฏิบัติการนั้น เช่น ntoskrnl.exe เป็นต้น

๖.๒.๓.๒ Service smss.exe> Parent Process: Default Part ปกติจะต้องอยู่ใน System\root\System32\smss.exe, Parent Process : ระดับสิทธิ = System Number of Instances : Parent Process จะมี Instructions Process , User Account : User Login = Local System, Start Time : เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสต์ของระบบไม่กี่วินาที, Description : มีหน้าที่ในการสร้าง Session และInstructions 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 = ปกติจะต้อง อยู่ใน SystemRoot\System32\wininit.exe, Parent Process : สร้างโดย Instance ของ smss.exe ดังนั้นเครื่องมือมักจะไม่ได้ระบุชื่อกระบวนการหลัก, Number of Instances : Parent Process = 1, User Account : User Login = Local System, Start Time: เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสต์ ของระบบไม่กี่วินาที, 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 ปกติจะต้อง อยู่ใน SystemRoot\System32\taskhost.exe, Parent Process : ระดับสิทธิ = 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 1

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 Isass.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน SystemRoot\System32\Isass.exe, Parent Process : ระดับสิทธิ = winint.exe Number of Instances : Parent Process = 1 , User Account : User Login = Local System Start Time : เวลาเริ่มต้น เกิดขึ้นภายหลังการบูสต์ของระบบไม่กี่วินาที Description : = Isass.exe หรือชื่อเต็มคือ Local Security Authentication Subsystem Server process รับผิดชอบในการตรวจสอบผู้ใช้ โดยการเรียกผู้ให้บริการความปลอดภัยของแพ็กเก็ต ที่เหมาะสม (SSP) การรับรองความถูกต้องที่ระบุ ใน Rigistry HKLM\SYSTEM\CurrentControlSet\Control\Lsa โดยทั่วไปจะเป็น Kerberos SSP ใช้สำหรับบัญชีโดเมน หรือ MSV1_0 SSP ใช้สำหรับ local accounts เมื่อผู้ใช้ได้รับการรับรองความ ถูกต้อง Isass.exe จะสร้างโทเค็นการเข้าถึงสำหรับผู้ใช้ที่ระบุสิทธิ์ และข้อจำกัดด้านความปลอดภัย สำหรับผู้ใช้ และกระบวนการอย่างอื่นของผู้ใช้เท่านั้น ซึ่งเป็นกระบวนการหนึ่งของกระบวนการที่ควร เกิดขึ้น และไม่ควรมีโปรเซสลูก

๖.๒.๓.๖ Service winlogon.exe>, Parent Process : Default Part ปกติจะต้อง อยู่ใน 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 ภายในไม่กี่วินาทีของเวลาบูสต์สำหรับกระบวนการแรก (สำหรับเซสซัน ๑) เวลา เริ่มต้นสำหรับกระบวนการเพิ่มเติมเกิดขึ้นเมื่อมีการสร้างเซสชั่นใหม่โดยทั่วไปผ่านทาง Remote Desktop หรือการเข้าสู่ระบบการสลับผู้ใช้อย่างรวดเร็ว Description : เป็นระบบตอบโต้ผู้ใช้เวลา login หรือ logoff ถูกเปิดใช้งานโดย Service LogonUl.exe ซึ่งจะรับชื่อผู้ใช้และรหัส ผ่านหน้าจอ เข้าสู่ระบบและส่งผ่านข้อมูลรับรองไปยัง Isass.exe เพื่อตรวจสอบข้อมูลรับรองเมื่อผู้ใช้ได้รับการ รับรองความถูกต้องแล้ว Winlogon.exe จะโหลด NTUSER.DAT ของผู้ใช้ลงใน Registry HKCU และเริ่มต้นเซลล์ของผู้ใช้ (explorer.exe) ผ่าน Userinit.exe

๖.๒.๓.๗ Service iexplore.exe> Parent Process : Default Part ปกติจะต้องอยู่ใน System\Program Files\Internet Explorer\iexplore.exe ห รื อ \Program Files (x86) \Internet Explorer\iexplore.exe, Parent Process : ระดับสิทธิ = 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 ด้วยเหตุผลหลาย ประการ รวมถึงความปลอดภัยที่เพิ่มขึ้นเมื่อเข้าสู่เว็บไซต์อินเทอร์เน็ต IE จะเรียกใช้กระบวนการแท็บ ด้วยความน่าเชื่อถือที่ต่ำซึ่งจะเป็นความยากสำหรับผู้โจมตีที่จะทำการแก้ไขพื้นที่อ่อนไหวของ Registry หรือระบบไฟล์หากพวกเขาสามารถควบคุม Child Process ของ IE ผู้โจมตีมักจะตั้ง ชื่อมัลแวร์ 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 : ระดับสิทธิ ถูกสร้างโดยกระบวนการของ userinit.exe ดังนั้นเครื่องมือวิเคราะห์มักจะไม่ได้ระบุชื่อกระบวนการหลัก, Number of Instances : รายการต่อผู้ใช้ที่ Logon แบบโต้ตอบ, User Account : User Login ขึ้นอยู่กับว่าใคร เป็นผู้ Login เข้ามา Start Time : เวลาเริ่มต้น = เริ่มเมื่อการเข้าสู่ระบบแบบโต้ตอบ Description : Service explorer.exe เป็นหัวใจหลักของ Explorer ช่วยให้ผู้ใช้สามารถเข้าถึงไฟล์ โดยทำหน้าที่ เป็นทั้งไฟล์เบราว์เซอร์ผ่าน Windows Explorer (แต่ยังคง explorer.exe) และอินเตอร์เฟสของผู้ใช้ เช่น เดสก์ท็อป และเมนูเริ่มแถบงานของแผงควบคุม เป็นต้น แอปพลิเคชันที่เปิดใช้งานผ่านการเชื่อมโยง ผ่านส่วนขยายไฟล์ และ Shortcut ควรมีเพียงหนึ่งกระบวนการของ explorer.exe ที่ทำงานอยู่ การเข้าสู่ระบบแบบโต้ตอบโดยไม่คำนึงถึงหน้าต่าง Windows Explorer ที่เปิดโดยผู้ใช้ให้สังเกตว่า explorer.exe ที่ถูกต้องนั้นอยู่ใน SystemRoot ถ้ามีไดเรกทอรีมากกว่า 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 : ระดับสิทธิ = winint.exe, Number of Instances : Parent Process = 1 , User Account : User Login = Local System Start Time : เวลาเริ่มต้นเกิดขึ้นภายหลังการบูตของระบบไม่กี่วินาที Description : เป็นการจัดการบริการ Terminal รวมถึงเซสชัน Remote Desktop รวมถึง local sessions เพิ่มเติมผ่านการสลับผู้ใช้ผ่าน การสื่อสารกับ smss.exe เพื่อเริ่มเซสชันใหม่ โดย smss.exe สร้าง csrss.exe และ winlogon.exe เพิ่มเติมเพื่อสนับสนุนเซสชันใหม่ เท่านั้น ซึ่งเป็นกระบวนการหนึ่งของกระบวนการที่ควรจะเกิดขึ้น และไม่ควรมี Child Process

๖.๒.๓.๑๐ Service svchost.exe> Parent Process : Default Part ปกติจะอยู่ใน SystemRoot\System32\smss.exe, Parent Process : ระดับสิทธิ = System Number of Instances : Parent Process = 5 และ Child Process User Account : User Login จะแตกต่างกันไปขึ้นอยู่ กับกระบวนการ svchost.exe แม้ว่าโดยทั่วไปจะเป็นบัญชี Local System, Network Service หรือ Local Service กระบวนการที่ทำงานภายใต้บัญชีอื่นใดควรได้รับการตรวจสอบ Start Time : เวลา โดยทั่วไปภายในไม่กี่วินาทีของเวลาเริ่มต้นทำงาน อย่างไรก็ตามสามารถเริ่ม Service ได้แล้ว อาจส่งผลให้เกิดกระบวนการใหม่ของ svchost.exe หลังจากเวลา Description : กระบวนการโฮสต์ ทั่วไปสำหรับ Windows Services มันถูกใช้สำหรับการเรียกใช้บริการ DLLs Windows จะเรียกใช้ svchost.exe หลายกระบวนการ แต่ละตัวใช้พารามิเตอร์ "-k" ที่ไม่ซ้ำกันสำหรับการจัดกลุ่มบริการ ที่คล้ายกัน พารามิเตอร์ "-k" ทั่วไปรวมถึง BTsvcs, DcomLaunch, RPCSS, Local Service Network Restricted, Netsvcs, Local Service Network Service, Local Service No Network, Secsvcs และ Local Service And NoImpersonation ผู้เขียนมัลแวร์ จะใช้ประโยชน์จาก svchost.exe ทั้งโดยตรงหรือโดยอ้อมเพื่อซ่อนมัลแวร์ โดยตรงจะติดตั้งมัลแวร์ เป็นบริการในกระบวนการที่ถูกต้องของ svchost.exe และโดยอ้อมจะผสมผสานกับกรณีที่ถูกต้อง ของ 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 : ระดับสิทธิ = wininit.exe, Number of Instances : Parent Process = 1 , User Account : User Account : User Login = Local System, Start Time : เวลาเริ่มต้นเกิดขึ้นภายหลังการบูสต์ของระบบไม่กี่วินาที Description : = Unified Background Process Manager (UBPM) ซึ่งรับผิดชอบกิจกรรมพื้นหลัง เช่น บริการและ งานที่กำหนด Services.exe ใช้ Service Control Manager (SCM) จัดการบริการโหลด และ อุปกรณ์ไดรเวอร์ที่ทำเครื่องหมายสำหรับการเริ่มอัตโนมัติโดยเฉพาะ นอกจากนี้เมื่อผู้ใช้เข้าสู่ระบบ แบบโต้ตอบได้สำเร็จ 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 ปกติจะต้องอยู่ ใน SystemRoot\System32\csrss.exe, Parent Process : ระดับสิทธิ 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

🖅 Run	×
	Type the name of a program, folder, document or Internet resource, and Windows will open it for you.
Open:	regedit ~
	OK Cancel <u>B</u> rowse

ภาพที่ ๑๒๘ Regedit

Task Scheduler (Local) Task Scheduler (Local) Task Scheduler Library Microsoft Office Microsoft XbtGameSave Mozilia	Name Status Ti © GoogleUpdateTaskMachineC Ready A © GoogleUpdateTaskMachineJA. Ready A © OneDrive Standalone Update Ready A © OneDrive Standalone Update Ready A	liggers Untiple triggers defined 8.726 PM every day - After triggered, repeat every 1 hour for a duration of 1 dk 8 system startup 4.700 PM on 5/1/1992 - After triggered, repeat every 1.00.0000 indefinitely. 8.00 PM on 5/1/1992 - After triggered, repeat every 1.00.0000 indefinitely.	Actions Task Scheduler Library Create Basic Task Front Task Import Task Distance All Running Tasks
Symantec Endpoint Pr	K General Triggers Actions Conditions S When you create a task, you must specify open the task property pages using the Pro Action Details Start a program C:\Program Files 0	GoogleUpdateTasiMachineUA Properties (Local Computer) General Triggers Actions Conditions Settings History (disabled) When you create a task, you must specify the action that will occur when Action Details Start a program C(\Program Files (x86)\Google\Update\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdate\GoogleUpdat	your task starts. fate.exe /us /installsourx * * *

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 และการวิเคราะห์เชิงลึกระดับฟังก์ชัน ของไฟล์ สำหรับการพิสูจน์ไฟล์สามารถทำได้หลายวิธี มัลแวร์เองก็มีที่มาจากหลายแหล่ง ในที่นี้ ขอยกตัวอย่าง มัลแวร์ที่มีการซ่อนตัวอยู่ใน Ram ซึ่งไม่สามารถตรวจหรือค้นหาจากเครื่อง คอมพิวเตอร์ได้ เนื่องจากไม่มีการสร้างไฟล์ใด ๆ ไว้ในระบบ ซึ่งส่วนมากจะอาศัยสคริปต์ของโปรแกรม Powershell ในการรันตัวเอง สำหรับกระบวนการวิเคราะห์จะเริ่มจากนำไฟล์ Ram ที่เก็บมาได้มาทำ การแตก 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 มีการดาวน์โหลดไฟล์บางอย่างที่น่า สงสัยจากเว็บไซต์ภายนอก เมื่อกดลิ้งเข้าไปเราจะสามารถ ดาวน์โหลดไฟล์บางอย่างมาได้ โดยมี ลักษณะเป็นไฟล์รูปภาพที่ชื่อ d.png ดังภาพที่ ๑๒๑

Home Share	e View	Compressed Fo	der Tools					
-> ~ ↑ 📕 > 1	This PC > Lo	cal Disk (D:) >	cif > df202	2 > 2 ok				
	Name	~			Date modif	lied	Туре	Size
Quick access	2.zip	2			4/1/2022 9:	47 PM	เอกสาร WinRAR แบ	651,333 KB
This PC								
2D.Objecte								
🔚 2.zip - WinRA	R							
 2.zip - WinRA ไฟล์ คำสั่ง เครื่องม่ 	งR มือ รายการโปร	เด ตัวเลือก วิธีใ	้อ้					
 2.zip - WinRA ไฟล์ ดำสั่ง เครื่อง: ไฟล์ ดำสั่ง เครื่อง: 	เR มือ รายการโปร วิ โ 🌅	เด ตัวเลือก วิธีโ OO				<u>A</u> .	1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	
2.zip - WinRA ปฟล์ ดำสั่ง เครื่อง: (พี่มเข้า แยกไป	งR มือ รายการโปร 🎽 🏹 ที่ หตุสอบ	เด ตัวเลือก วิธีไ ดู ลบ	ร์ช มี คัณหา	เรียงย่าย สาวช่วย	ข้อมูลต่าง ๆ	โวรัสสมวน	ต่าออิบาย SFX	
 2.zip - WinRA ไฟล์ ค่าสั่ง เครื่อง เพิ่มเข้า แขกไป เพิ่มเข้า แขกไป โร่ อายาาย 	เR มือ รายการโปร ไที่ หตุสอบ เอกสาร ZIP, ชุย	หด ตัวเลือก วิธีโ	สีช) คันหา 5,184 ใบห์	ເຈັ້າຫ່າຍ	ข้อมูลต่าง ๆ	โ วรัสสแกน	ร้างอิบาย SFX	
2.zip - WinRA	ห มือ รายการโปร ได้ หดสอบ เอกสาร ZIP, ขะ	รด ตัวเลือก วิธีไ อุ มาตจริง 2,128,603 ชนาต	ไซ่ ภัณหา 5,184 ใบท์	ตัวช่วย ชนิด	ข้อมูลต่าง ๆ ถูกแก้ไร	โวร์สสแกน 15 สสแกน	ແລ2	
2.zip - WinRA	เR มือ รายการโปร ได้ หดสอบ เอกสาร ZIP, ชะ	รด ตัวเลือก วิธีไ ดู ละ นาดจริง 2,128,603 ชนาด	ไซ่ ม คั่นหา 5,184 ใบห์ ถูกเก็บ ร	รนิด Tile folder	ข้อมูลต่าง ๆ ถูกแก้ไข	ไวรัสสแกน 1วรัสสแกน	 มีคาอธิบาย SFX 	

ภาพที่ ๑๓๒ โปรแกรม Volatility

จากนั้นทำการตรวจสอบไฟล์มัลแวร์เบื้องต้นด้วยเว็บไซต์ Virustotal.com อีกตัวอย่างหนึ่งคือ การวิเคราะห์มัลแวร์เรียกค่าไถ่ โดยผู้ใช้งานแจ้งมาว่าไฟล์ต่าง ๆ ที่เก็บไว้ที่หน้าจอของเครื่องถูก เปลี่ยนนามสกุล และจะสังเกตได้ว่าไฟล์ต่าง ๆ ที่หน้าจอถูกเปลี่ยนนามสกุลเป็น .hacker ทั้งหมด พร้อมกับมีไฟล์เรียกค่าไถ่ที่ชื่อ ReadMe.txt ถ้าเราเปลี่ยนเป็นนามสกุล อื่น ๆ อีกประมาณ ๕ นาที มันก็จะกลับมาเป็นเหมือนเดิมอีก แสดงว่าต้องมีโปรแกรมบางอย่างที่คอยเปลี่ยนนามสกุลของไฟล์ เหล่านี้อย่างมีช่วงเวลา ซึ่งใน Windows จะมีโปรแกรมหนึ่งที่ทำหน้าที่ตั้งเวลาการรันโปรแกรมได้ และมักถูกใช้ตั้งเวลาโจมตี นั้นคือโปรแกรม Task Scheduler ซึ่งจะต้องไปตรวจสอบ และพบว่ามีชื่อ ของคำสั่งหนึ่งที่ผิดปกติ คือ GoogleUpdateja จากการตรวจสอบรายละเอียด จะพบว่าโปรแกรมถูก สั่ ง ใ ห้ รันไฟล์มัลแวร์ที่ชื่อ uk.bat ทก ๆ ๕ นาที ดังภาพที่ ๑๒๒



ภาพที่ ๑๓๓ การตรวจสอบไฟล์มัลแวร์เบื้องต้น

๖.๓.๑ การวิเคราะห์ผ่านโปรแกรม Deep Instinct ซึ่งเป็นโปรแกรมแอนตี้ไวรัสด้วย ปัญญาประดิษฐ์ มีความสามารถในการวิเคราะห์ และให้ค่าความน่าจะเป็นของภัยคุกคามที่ตรวจพบ ทาง ทอ.ได้ดำเนินการติดตั้งโปรแกรมดังกล่าวบนเครื่องคอมพิวเตอร์เพื่อป้องกันมัลแวร์จาก อินเทอร์เน็ต และยังถูกใช้เป็นเซนเซอร์สำหรับตรวจจับและรายงานผลมายังส่วนกลางเพื่อใช้วิเคราะห์ ภัยคุกคามบนเครื่องผู้ใช้งาน เมื่อนำมาใช้ในงาน Forensic โปรแกรม Deep Instinct จะสามารถให้ ข้อมูลของไฟล์ที่มีการติดมัลแวร์ และพฤติกรรมอำพรางตัวด้วยการเปลี่ยนแปลงตัวเองตลอดเวลา สำหรับผู้ดูแลระบบ สามารถสั่ง Scan ไวรัส สั่ง Block ไฟล์ที่เป็นอันตราย ตัดการเชื่อมต่ออินเทอร์เน็ต รวมถึงทราบหมายเลข IP Address ของเครื่องได้ ทั้งนี้ในองค์กรขนาดใหญ่จะใช้ระบบจ่ายหมายเลข



IP Address แบบอัตโนมัติทำให้เครื่องคอมพิวเตอร์มีการเปลี่ยนแปลง หมายเลขIP Address

ภาพที่ ๑๓๔ แสดง Dashboard ของโปรแกรม Deep Instinct

๖.๓.๒ การรันไฟล์ เป็นการทดสอบรันไฟล์มัลแวร์บนสถาพแวดล้อมจำลองเพื่อวิเคราะห์ พฤติกรรมของมัลแวร์ เพื่อค้นหาแนวทางแก้ไข โดยจะต้องทำบนระบบจำลองที่เรียกว่า Sandbox การวิเคราะห์เชิงลึกระดับฟังก์ชันของไฟล์ เป็นการทำความเข้าใจฟังก์ชันการทำงานของมัลแวร์ เพื่อค้นหาพฤติกรรมที่อาจซ่อนอยู่ หรือการถูกแทรกการทำงานของโปรแกรมในสภาวะปกติ เช่น การที่โปรแกรมเครื่องคิดเลขถูกเรียกขึ้นมาทำงานเองแบบอัตโนมัติ หรือการที่เราติดตั้งโปรแกรม Crack ที่มีมัลแวร์ เป็นต้น โดยส่วนมากจะใช้โปรแกรม IDA Pro ในการวิเคราะห์ ซึ่งผู้ใช้จะต้องมีความรู้ใน เรื่องของภาษาภาษาแอสเซมบลี (Assembly Language) ซึ่งเป็นภาษาเครื่อง นอกจากนี้ยังมีการซ่อนไฟล์ มัลแวร์มากับไฟล์รูปภาพ ไฟล์วิดีโอ หรือไฟล์เอกสารต่าง ๆ ได้อีกด้วย ซึ่งการจะวิเคราะห์จะต้องสามารถ ดึงไฟล์ดังกล่าวออกมาก่อน เช่น การอ่านไฟล์ข้อมูลเชิงลึก เราจะใช้คำสั่งดังภาพที่ ๑๒๔ เป็นต้น



ภาพที่ ๑๓๕ การทดสอบรันไฟล์มัลแวร์บนสถาพแวดล้อมจำลอง

๖.๓.๓ การระบุรูปแบบไฟล์ เราอาจคิดว่าทำไมต้องระบุในเมื่อเห็นอยู่แล้วว่าเป็นไฟล์นามสกุล อะไร แต่อย่าลืมว่าไฟล์เครื่องคอมพิวเตอร์สามารถถูกเปลี่ยนแปลงหรือแก้ไขได้ และ แฮกเกอร์ก็มักจะ เลือกใช้วิธีดังกล่าว เพื่อจะซ่อนไฟล์หรือบายพาสระบบเพื่อให้สามารถผ่านฟังก์ชันการตรวจสอบ นามสกุลไฟล์เมื่อดาวน์โหลดไฟล์เข้ามาในระบบ ดังนั้นการทำ Forensics เพื่อหาว่ารูปแบบไฟล์เดิม นั้นเป็นอะไร จึงมีความจำเป็น และในการแข่งขัน CTF ส่วนมากนิยมใช้คำสั่งเหล่านี้ในการหาคำตอบ ซึ่งก็รวดเร็วมาก เช่น คำสั่ง mdls ใน MacOS หรือ libmagic ในระบบ UNIX และถ้าเป็นใน Linux เราก็จะใช้คำสั่งว่า File เป็นต้น

๖.๓.๔ การแตกไฟล์เซิงลึก เป็นกระบวนการเพื่อแยกส่วนประกอบของไฟล์ออกมา คล้ายกับ การ Unzip แต่จะแตกต่างกันตรงที่สามารถถอดรหัสไฟล์ที่ไม่ทราบมาก่อนได้ด้วย (ส่วนใหญ่) และ สามารถหาข้อมูลที่ถูกซ่อนอยู่ในไฟล์ได้อีกด้วย โดยมีอยู่ ๒ คำสั่งที่นิยมใช้ คือ binwalk -e แล้วตาม ด้วยชื่อไฟล์ เพื่อหาข้อมูลเบื้องต้นเกี่ยวกับไฟล์รูปภาพ และ คำสั่ง foremost เป็นคำสั่งที่ใช้สำหรับ แตกไฟล์ที่ซ่อนอยู่ออกมา

File Fele M	in Court Torontal	root@kali-training: ~/Desktop/fa/DF_122
#xw4Iao~ vjv7 00<) root@kali-t 5411333e505 root@kali-t	raining:-/Desktoj training:-/Desktoj	http://fa/DF_122# ls 1851b.gif p/fa/DF_122# binwalk 5411333e505440020a1799da6071851b.gif
DECIMAL	HEXADECIMAL	DESCRIPTION
0 78301	0×0 0×131DD	GIF image data, version "89a", 440 x 385 RAR archive data, version 4.x, first volume type: MAIN_HEAD
total 164 drwxr-xr-x drwxr-xr-x -rw-r-r- root@kali-t Processing: * root@kali-t	2 root root 40 3 root root 1568 raining:-/Deskto raining:-/Deskto 5411333e5054400 raining:-/Deskto	06 w.s. 21 14:05 . 06 w.s. 21 14:06 . 78 K.s. 17 2020 5411333e505440020a1799da6071851b.gif p/fa/0F_122# p/fa/0F_122# p/fa/0F_122# 1s < > < ☆ Home Desktop fa DF_122 output rar >
s411333e50s root(kali-t vit dog.txt	5440020a1799da607 raining:-/Deskto	1551b.gif output 0 Recent 1 Image: Constraint of the second secon

ภาพที่ ด๓๖ คำสั่ง foremost & binwork



ภาพที่ ๑๓๗ คำสั่งเกี่ยวกับไฟล์ zip

Unzip เปิดไฟล์ หรือคลายไฟล์ กรณี .gz ให้ใช้คำสั่ง gzip -d ตามด้วยชื่อไฟล์ Details -v จะให้ข้อมูลเชิงลึกเกี่ยวกับค่าที่มีอยู่ในฟิลด์ต่าง ๆ ของรูปแบบข้อมูล zipinfo แสดง รายการข้อมูลเกี่ยวกับเนื้อหาของไฟล์ zip โดยไม่ต้องแตกไฟล์ zip -F input.zip --out output.zip และ zip -FF input.zip --out output.zip พยายามซ่อมแซมไฟล์ zip ที่เสียหาย fcrackzip bruteforce สุ่มเดารหัสผ่าน zip (สำหรับรหัสผ่านที่ไม่เกิน ๗ อักขระ) ก่อนอื่นต้องติดตั้งโปรแกรมประเภท Dictionary สำหรับการทำ Brute-Force ในโปรแกรมทดสอบความปลอดภัยระบบ เช่น Kali Linux จะเก็บไฟล์สำหรับใช้ Brute-Force ไว้ที่ /usr/share/wordlists/ ไฟล์ชื่อว่า rockyou.txt.gz ซึ่งต้อง ทำการแตกไฟล์ออกมาก่อน 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 หรือจะใช้ คำสั่ง zip2john ก็ได้ เช่น #> zip2john abc.zip > hash.txt, #> john hash.txt เป็นต้น

<pre>root@kali-training:~/Desktop# ls</pre>	
00000150.zip fasttrack.txt hunting 1	psl.txt rockyou.txt webShell
fa hash.txt hunting 2'	ramVMwareTools-10.3.10-13959562
root@kali-training:~/Desktop# zip2john 0000	150.zip > hash.txt210hn flags.zip > hash.txt
root@kali-training:~/Desktop# ls -al ags 21	
total 136912	
drwxr-xr-x 8 root root 4096 A.s.	0:45 .
drwxr-xr-x 22 root root 4096 w.s. 10	2021 ounloads# cat hash.txt
-rwxrwxrwx 1 root root 223809 1.9. 4	9:57 200000150.zip3e9de+0+27+8+4d+8133+78c8+6b9118cd12cc4d39c
drwxr-xr-x 3 root root 4096 A.u. 4	0:38 ¹⁵ fa ^c a79767df65bbf5d629c3a8ba31d325862a76114e6317d86496e87
-rw-rr 1 root root 2016 1.8. 4	0:42 fasttrack.txt
-rw-rr 1 root root 125 มิ.ย. 4	0:48 hash.txt
drwxrwxr-x 2 root root 4096 มิ.ค. 31	8:22 'hunting 1'
drwxrwxr-x 4 root root 4096 w.e. 29	5:50 'hunting'2'ohn hash.txt
-rw-rw-r 1 root root 650 w.e. 28	2:04 psl.txt
drwxr-xr-x 2 root root 4096 in.u. 7	5:45 ¹⁰ ram(see FAD)
-rwxrwxrwx 1 root root 139921507 w.e. 29	5:26 rockyou.txt
drwxr-xr-x 3 root root 4096 m.m. 21	2020 VMwareTools-10.3.10-13959562
drwxr-xr-x 2 root root 4096 เพ.ย. 1	7:28 webShell
root@kali-training:~/Desktop# john hash.txt	
Created directory: /root/.john	
Using default input encoding: UTF-8	
Loaded 1 password hash (ZIP, WinZip [PBKDF2	SHA1 128/128 SSE2 4x2])
Press 'q' or Ctrl-C to abort, almost any ot	er key for status
badboys (00000150.zip)	
1g 0:00:00:03 DONE 2/3 (2022-06-04 10:49) 0	2832g/s 3939p/s 3939c/s 3939C/s gangstasfernandas
Use the "show" option to display all of t	e cracked passwords reliably
Session completed	
root@kali-training:~/Desktop#	

ภาพที่ ๑๓๙ Brute-Force

บทที่ ๗ การถ่ายโอนหลักฐาน การจัดเก็บหลักฐานและการส่งคืนหลักฐาน

ในการวิเคราะห์หลักฐานทางดิจิทัล บางครั้งทีมงานที่ทำการวิเคราะห์ก็อาจจะไม่สามารถ ทำการวิเคราะห์ได้เนื่องจากขาดประสบการณ์ จึงต้องมีการส่งมอบหลักฐานให้กับหน่วยงาน หรือองค์กรที่มีศักภาพสูงขึ้นถัดไปในการดำเนินการ สำหรับ ศซบ.ทอ. หากไม่สามารถดำเนินการได้ จะทำการส่งมอบหลักฐานให้กับ บก.ทท.ต่อไป โดยในกระบวนการถ่ายโอนหลักฐานจะต้องมี การทำเอกสารตาม "แบบฟอร์มควบคุมหลักฐาน" ที่มีการกำหนดอย่างชัดเจนว่าหลักฐานถูกส่งมอบ โดยใคร เมื่อไหร่ ดังภาพที่ ๑๒๙ - ๑๓๐

		แบบฟอร์มค	วบคุมหลักฐาน	
หมายเลข	เหตุการณ์ :	รป	แบบการโจมดี :	
เจ้าหน้าที่	ตรวจพิสูจน์หลั	กฐาน : (ชื่อ-สกุล / รหัสประจำตั)	
ชื่อผู้เสียห	าย :	User:	Pa	issword:
ชื่อผู้ต้องส	งสัย :	User:	Pa	issword:
วันที่/เวลา	า เก็บหลักฐาน	: <u></u> ao	านที่เกิดเหตุ :	
🗖 ເກົ່ນ	หลักฐานทั่วไป	🗖 เก็บหลักฐานฝ้องศาล		
		รายละเอียดขอ	องพยานหลักฐาน	
ລຳດັບที่	จำนวน	คำอธิบาย (ร	ุ่น, หมายเลขเครื่อง, สภาพ, รอย	ขัดช่วน)
			y	
สำลับเพื่	วันนี้ (เวลา	แบบพอรมการรง ถังใจเข้าหลักราบ	ป – จดเกบหลกฐาน เข้าเข้าหลักราบ	มาวยเมต / สถาบที่เกี
et MON	7477 (2411	(ลายมือชื่อ & รหัสประจำตัว)	(ลายมือชื่อ & รหัสประจำตัว)	กล เองกุ / สถานกลา
				1

ภาพที่ ๑๔๐ แบบฟอร์มควบคุมหลักฐาน

				ส่วนพิสูจน์	หลักฐาน ผพฐ.กรช.ศชบ.ทอ.	
			แบบฟอร์มค	วบคุมหลักฐาน		
			แบบฟอร์มการ	รับ - ส่งหลักฐาน		
ลำ	เด้บที่	วันที่ / เวลา	ผู้นำเข้าหลักฐาน	ผู้นำเข้าหลักฐาน	หมายเหตุ / สถานที่ส่ง	
\vdash			(ลายมอชอ & รหสประจาตว)	(ลายมอชอ & รหสประจาตว)		
\vdash						
\vdash						
\vdash						
T						
			แบบฟอร์มการส่งคื	่น - ทำลายหลักฐาน		
ແບ	บฟอร์ สาส่ เ	มการส่งคืนหลัก	ฐาน เข็มแอกสวรที่มีความเกี่ยวข้องกับ	(ຍັຫ້ວາຜາຂັບ).		
หลั	ักฐานข	' ขั้นนี้เป็นหลักฐา	นที่ดำเนินคดีเสร็จสิ้นแล้ว ต้องกา	เพ็มองถงถอง. รที่จะ : ส่งคืนเจ้าของ	ทำลายทิ้ง	
ชื่อ	& รหั	สประจำตัว # ข	องเจ้าของหลักฐาน :	ลายมีอชื่อ	:	
วัน	ที: <u></u> มษอร์	บการทำลายหลั	0501			
ลำต่	แบบพอรมการทาสายหลุกฐาน ลำดับที่ #: เป็นหลักจานที่ต้องทำลายโดย (เจ้าที่ทำลายหลักจาน)					
หม	หมายเลขประจำตัว #:วันที่ :					
ชื่อ วัน	-นามส ส่.	กุล & หมายเลา	ขประจำตัว # ของผู้สังเกตุการณ์	:ลายมือซีส		
414	<u></u>					
					หน้า 2 ใน 2 หน้า	

ภาพที่ ๑๔๑ แบบฟอร์มการรับ - ส่งหลักฐาน

๗.๑ กระบวนการจัดเก็บหลักฐาน

นอกจากจะต้องมีการบันทึ๊กเป็นเอกสารดังที่ได้กล่าวมาแล้ว หลักฐานที่ยังไม่ได้รับการส่งมอบ ให้เจ้าของ หรืออยู่ระหว่างดำเนินการวิเคราะห์จะต้องถูกเก็บให้ปลอดภัย เพื่อป้องกันไม่ให้หลักฐาน เกิดความเสียหายระหว่างดำเนินการจัดเก็บ และในกรณีที่มีหลักฐานจำนวนมาก ก็จะสามารถค้นหา และบริหารจัดการหลักฐานให้เป็นระเบียบได้อีกด้วย ดังนั้นการมีห้องสำหรับเก็บหลักฐานที่สามารถ มองเห็นได้จากภายนอก มีกระบบกล้องวงจรปิดเพื่อแสดงให้เห็นถึงกระบวนการจัดเก็บที่ชัดเจน เมื่อมีการดำเนินคดีในชั้นศาล ทางทีมวิเคราะห์หลักฐานก็จะสามารถใช้เป็นหลักฐานยืนยัน ความบริสุทธิ์ของตนเอง



ภาพที่ ๑๔๒ ตัวอย่างห้องเก็บพยานหลักฐาน

๗.๒ การเก็บรักษา การถ่ายโอน และการส่งมอบหลักฐาน

การควบคุมพยานหลักฐาน เป็นกระบวนการที่ต้องควบคุมหลักฐานไม่ให้ถูกแก้ไขหรือ เปลี่ยนแปลง รวมทั้งเป็นการยืนยันว่าการได้มาซึ่งหลักฐานนั้น ผู้ทำการวิเคราะห์ไม่ได้ทำการ เปลี่ยนแปลงหรือทำให้ทรัพย์สินอันเป็นหลักฐานนั้นเสียหายจากการพิสูจน์หลักฐาน ทั้งจะมีประโยชน์ ในการสร้างความน่าเชื่อถือในชั้นศาลด้วย โดยกระบวนการจะใช้เอกสารในการควบคุมและกำกับ การทำงาน เช่น มีการบันทึกการรับมอบหลักฐาน ระบุวันเวลา ชื่อผู้ส่ง ชื่อผู้รับ วัสดุที่ใช้ในการเก็บ ต้องไม่ทำให้หลักฐานเสียหายหรือถูกเปลี่ยนแปลง สถานที่เก็บต้องถูกควบคุม ไม่เป็นที่อับชื้น หรือ ร้อนเกินไป มีกล้องวงจรปิดเพื่อตรวจสอบการเข้าออก มีระบบรักษาความปลอดภัยที่เหมาะสมและมี ถังดับเพลิง รวมทั้งมีแผนเผชิญเหตุที่สามารถเคลื่อนย้ายพยานหลักฐานได้เมื่อเกิดเหตุจำเป็นที่ต้อง เคลื่อนย้าย

๗.๓ กระบวนการส่งคืนหลักฐาน

หลังจากทีมงานวิเคราะห์ดำเนินการวิเคราะห์หลักฐานเสร็จแล้ว จะต้องนำหลักฐานส่งคืนให้กับ เจ้าของ เพื่อใช้เป็นหลักฐานและจะต้องมีการเซ็นต์รับหลักฐาน หรือมีการถ่ายภาพเอาไว้ด้วย เพื่อป้องกันกรณีบุคคลแอบอ้างมารับหลักฐานไป ทั้งนี้หลักฐานที่จะส่งคืนจะต้องไม่เสียหายด้วยเหตุ จากกระบวนการวิเคราะห์หลักฐาน ซึ่งกระบวนการวิเคราะห์หลักฐานจะไม่ยุ่งเกี่ยวกับหลักฐานจริง แต่จะใช้สำเนาของพยานหลักฐาน ในการวิเคราะห์แทน โดยแทนค่าความเที่ยงตรงของข้อมูลด้วยการ ทำ Hash ไฟล์หลักฐาน

บทที่ ๘ การออกรายงานผลการวิเคราะห์

รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์ คือ รายละเอียดของข้อมูลบน Complete Forensic Investigation Process ซึ่งสามารถเตรียมการโดยการตรวจพิสูจน์นิติคอมพิวเตอร์ การตรวจพิสูจน์ นิติคอมพิวเตอร์ได้มีการเก็บข้อมูลที่เกี่ยวกับเหตุการณ์ การสืบสวนสอบสวน และเตรียมการสำหรับ รายงานฉบับสมบูรณ์ โดยสามารถเปิดเผยผลการตรวจพิสูจน์นิติคอมพิวเตอร์ ซึ่งไม่ใช่แค่การนำเสนอ ข้อเท็จจริง 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 จำเป็นต้องมี รายละเอียด เช่น วันที่และเวลาของหลักฐาน, วันที่และเวลาปัจจุบัน, เวลาที่วิเคราะห์เสร็จสิ้น สิ่งที่ พบจากการสอบสวน, เทคนิคพิเศษนอกเหนือจากกระบวนการปกติ, แหล่งข้อมูลภายนอกที่ช่วยใน การค้นหาหลักฐาน และได้รับการอบรมหลักสูตร Computer Crime Investigators และแนวปฏิบัติ ที่ดีสำหรับผู้ตรวจพิสูจน์ เป็นต้น ผู้มีส่วนเกี่ยวข้องท่านใหม่สามารถเข้าใจในเนื้อหาของรายงานได้ ตรวจสอบให้แน่ใจ ว่ารายงานมีความสอดคล้องกับคำสั่งที่ได้รับ ขณะมีการแก้ไขรายงาน ต้องมั่นใจว่า หลักฐานไม่มีความซ้ำซ้อน และนำเสนออย่างถูกต้องและเหมาะสม ทบทวนรายงานอีกครั้งก่อน ดำเนินการส่งรายงาน กล่าวคือ การจัดทำรายงานการตรวจพิสูจน์นิติคอมพิวเตอร์นั้น ต้องมี รายละเอียดที่ครบถ้วนและสมบูรณ์ รายงานการตรวจพิสูจน์นิติคอมพิวเตอร์ที่ดีควรมีความเข้าใจง่าย ชัดเจน สามารถนำไปใช้ในทางกฎหมายได้ ไม่มีความซับซ้อน อ้างอิงแหล่งที่มาได้ และจัดส่งได้ ตามเวลาที่กำหนด

๘.๑.๑๐ สำหรับการออกรายงานของ ศซบ.ทอ. จะประกอบด้วย ๒ ส่วนใหญ่ ๆ คือ เอกสาร หลัก และเอกสารแนบ โดยเอกสารหลักจะเป็นแบบฟอร์มหนังสือราชการ ที่จะกล่าวถึงสาเหตุ ที่มาของเหตุการณ์ที่จะต้องดำเนินการ Forensic รวมถึงรายละเอียดโดยย่อของเหตุการณ์ และผลการวิเคราะห์ที่ได้ พร้อมสรุปแนวทางแก้ไขโดยย่อ นำเรียน ผู้บังคับบัญชาเพื่อพิจารณา ดำเนินการต่อไป ดังภาพที่ ๑๓๒



ภาพที่ ๑๔๓ ตัวอย่างรายงานผลการตรวจพิสูจน์หลักฐานทางดิจิทัล

๘.๒ ข้อมูลเบื้องต้น

ข้อมูลเบื้องต้น เป็นการกล่าวถึงรายละเอียดที่ได้รวบรวมหรือไปเก็บหลักฐานแล้วเอามา บรรยายถึงพฤติกรรมและสาเหตุที่ทำให้เกิดปัญหา พร้อมทั้งมีแผนภาพแสดงพฤติกรรมการโจมตี ให้ด้วย โดยอาจมีหัวข้อย่อย ๆ ภายในเพื่ออธิบายรายละเอียดของเหตุการณ์อื่น ๆ ที่มีมากกว่า ๑ เหตุการณ์ และอีกส่วนหนึ่งคือ เอกสารแนบจะเป็นรายงานที่ลงรายละเอียดรวมถึงแสดง กระบวนการวิเคราะห์ 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 อันจะเป็นการอธิบายให้ทราบถึงสาเหตุของการเกิดเหตุการณ์ โจมตีทางไซเบอร์

๘.๒.๓ การแพร่กระจาย เป็นการรายงานเกี่ยวกับพฤติกรรมการแพร่กระจายของมัลแวร์ หรือภัยคุกคามที่ได้ทำการวิเคราะห์ผล ซึ่งจะช่วยให้ผู้รับรายงานสามารถจำกัดขอบเขตความเสียหายได้ พร้อมทั้งเตรียมแผนรับมือหากเกิดเหตุการณ์โจมตีขึ้นอีก

๘.๒.๔ สรุปและข้อเสนอแนะ เป็นการกล่าวถึงเนื้อหาทั้งหมดโดยสรุปอีกครั้งพร้อมแนะนำ แนวทางแก้ไขให้กับหน่วยงานที่เกิดเหตุ โดยอาจแนะนำวิธีการหรือช่องทางในการดำเนินการแก้ไขให้ บรรเทาได้ ทั้งนี้เป็นหน้าที่ของเจ้าของระบบที่จะดำเนินการแก้ไข โดย ศซบ.ทอ.จะสนับสนุนด้าน บุคลากรและเทคนิคในการแก้ไขปัญหา พร้อมแนบเบอร์ติดต่อกรณีที่มีข้อสงสัยต้องการซักถามและลง ชื่อผู้ทำการวิเคราะห์ไว้ด้วย

นิยามคำศัพท์ที่เกี่ยวข้องกับงานด้าน Forensic Computer

Computer Forensic คือ การค้นหา และเก็บหลักฐานทางดิจิทัลที่อยู่ในอุปกรณ์ คอมพิวเตอร์ เช่น ไฟล์ที่อยู่ใน พีซี โน้ตบุ๊ก หรือพีดีเอ เป็นต้น หรือหลักฐานดิจิทัลที่ถูกสร้างจากระบบ คอมพิวเตอร์ เช่น บันทึกการใช้งานโทรศัพท์ และข้อมูลของการใช้อินเทอร์เน็ต เป็นต้น ซึ่งหลักฐาน ทั้งหมดนี้จะถูกนำมาวิเคราะห์ว่าหลักฐานนี้เกิดขึ้นเมื่อไหร่ เกิดจากอะไร ตอนนี้ใช้ทำอะไร และถูกใช้ โดยใคร และการทำ Computer Forensic จะประกอบไปด้วย การเก็บหลักฐาน การพิสูจน์ความ ถูกต้องของหลักฐาน และการวิเคราะห์หลักฐานเพื่อนำเสนอในชั้นศาล แล้วแต่กรณี ซึ่งจะมีคำนิยาม ศัพท์ที่เกี่ยวข้องพอสังเขปเรียงตามลำดับอักษรภาษาอังกฤษ 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	ในทางความมั่นคงของระบบคอมพิวเตอร์ช่องโหว่ของระบบ
	รักษาความมั่นคง ที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้
	โดยเป็นกลไกลลับทางซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้ข้าม
	ผ่านการควบคุมความมั่นคง แต่อาจเปิดทางให้ผู้ไม่ดีสามารถ
	เข้ามาในระบบและก่อความเสียหายได้
	(C)
case studies.	กรณีศึกษา
certificate Authority or CA	ผู้ประกอบการรับรองใบรับรองดิจิทัล คือ บุคคลที่สาม
	ที่น่าเชื่อถือ (Trusted third Party) ทำหน้าที่ออกใบรับรอง
	ดิจิทัล และทำหน้าที่ เจ้าหน้าที่ Passport ซึ่งมีหน้า
	ที่ทวนสอบ (verifies) รูปพรรณ (identity) ของผู้ถือใบรับรอง
	(Certificate's Holder) ใบรับรองดิจิทัลทนต่อการถูก
	รบกวน (Tamper-Proof) และไม่สามารถทำปลอมได้
characteristics	้ลักษณะ
civil law	กฎหมายแพ่ง
civil procedure law	 กฎหมายวิธีพิจารณาความแพ่ง
collection	~ การเก็บรวบรวม

commission of a crime comparative automated fingerprint compare evidence computer fraud computer network systems computer security system conclusion connections conviction court crime crime analysis crime patterns crime scene analysis crime scene investigation crime scene photography crime scene protection crime scene reconstruction crime scene search criminal law criminal justice administration criminal procedures criminal procedure law criminalistics cryptographic system compliance

การประกอบอาชญากรรม การตรวจเปรียบเทียบลายพิมพ์นิ้วมืออัตโนมัติ เปรียบเทียบพยานหลักฐาน การฉ้อโกงทางคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบความปลอดภัยคอมพิวเตอร์ การสรุปผล การควบคุมหน่วยงานในกระบวนการยุติธรรม การลงโทษ ศาล อาชญากรรม การวิเคราะห์อาชญากรรม รูปแบบอาชญากรรม การวิเคราะห์ในสถานที่เกิดเหตุ การตรวจสถานที่เกิดเหตุ การถ่ายภาพในสถานที่เกิดเหตุ การรักษาสถานที่เกิดเหตุ การประมวลเหตุการณ์ในสถานที่เกิดเหตุ การค้นหาในสถานที่เกิดเหตุ กฎหมายอาญา การบริหารงานยุติธรรมทางอาญา กระบวนการทางอาญา กฎหมายวิธีพิจารณาความอาญา การพิสูจน์หลักฐาน ระบบการเข้ารหัส การปฏิบัติตามกฎระเบียบข้อบังคับ และกฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความ ปลอดภัยขององค์กรอย่างถูกต้อง ได้ตามมาตรฐาน เช่น การปฏิบัติตามประกาศมาตรฐานการรักษาความปลอดภัย ในการประกอบธุรกรรมอิเล็กทรอนิกส์ โดยคณะกรรมการ ธุรกรรมอิเล็กทรอนิกส์และการจัดทำแผน เพื่อรองรับ พรบ. และพรฎ. ด้านความปลอดภัยทางอิเล็กทรอนิกส์ เป็นต้น เซิร์ฟเวอร์ของผู้ให้บริการบนอินเทอร์เน็ต ซึ่งกระจายอยู่

ตามที่ต่าง ๆ ทั่วโลก จะให้พื้นที่กับผู้ใช้เพื่อเก็บข้อมูลต่าง ๆ ไว้บนเน็ต แล้วดึงมาใช้งานได้ในทุกอุปกรณ์และทุกเวลา

cloud

cybercrime

อาชญากรรมทางไซเบอร์ คือ การกระทำผิดใด ๆ ที่เกี่ยวข้อง กับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ หรือการใช้ คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่าง ๆ รวมถึงระบบเครือข่าย ที่ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต เพื่อแสวงหาผลประโยชน์อย่างผิดกฎหมายโดยทางตรง และทางอ้อม เป็นต้น

data mining database system data warehouse deciphering indent detecting determination diagnosis digital image processing digital photography system dimensions document processing data Forensic

คลังข้อมูล การอ่านรอยกดเขียน สืบหา การตรวจหา การวินิจฉัย การประมวลผลภาพดิจิทัล ระบบการถ่ายภาพดิจิทัล มิติ การประมวลผลเอกสาร การพิสูจน์หลักฐานข้อมูลซึ่งมักใช้แทนกันได้กับการพิสูจน์ หลักฐานทางคอมพิวเตอร์เป็นการศึกษาข้อมูลดิจิทัลและ

วิธีการสร้างและใช้งานเพื่อการสอบสวน

(E)

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

(D)

เหมืองข้อมูล

ระบบฐานข้อมูล

evidence, documentary evidence Collection Form evidence preservation evidence, Criminal evidence, Expert evidence in rebuttal examination of handwriting expert witness expert witness in court exploratory exploratory data analysis

financial fraud fingerprint fingerprint forecasting of crime patterns forensic accounting forensic finance forensic science forensic science history forensic scientists forgery forgery detection foundations fraud fraud examination techniques fundamental biometric systems fundamentals of fingerprint forensic Duplicator faraday Bag forensic Artifact

พยานเอกสาร บันทึกการยึดหลักฐาน การสงวนและรักษาวัตถุพยาน พยานหลักฐานในคดีอาญา พยานหลักฐานจากผู้เชี่ยวชาญ พยานหลักฐานเพื่อหักล้าง การตรวจพิสูจน์ลายมือ พยานผู้ชำนาญการ พยานผู้ชำนาญการในชั้นศาล เชิงการตรวจสอบ การวิเคราะห์ข้อมูลเชิงการตรวจสอบ (F) การทุจริตทางการบัญชี ลายพิมพ์นิ้วมือ ลายนิ้วมือ การพยากรณ์รูปแบบอาชญากรรม การบัญชีทางนิติวิทยาศาสตร์ การเงินทางนิติวิทยาศาสตร์ นิติวิทยาศาสตร์ ประวัตินิติวิทยาศาสตร์ นักนิติวิทยาศาสตร์ การปลอมแปลงเอกสาร การตรวจการปลอมแปลง กระบวนการ การฉ้อโกง เทคนิคการตรวจสอบการทุจริต ระบบไบโอเมทริกซ์เบื้องต้น ความรู้พื้นฐานของลายพิมพ์นิ้วมือ ชุดทำสำเนาข้อมูล ถุงป้องกันคลื่นแม่เหล็กไฟฟ้า ข้อมูลใด ๆ ที่อยู่ในสื่อบันทึก หรือร่องรอยทางกายภาพ ใด ๆ ที่เกิดจากการปฏิสัมพันธ์ระหว่างสิ่งสองสิ่งและสามารถ

ใช้ในการประกอบการทำนิติวิทยาศาสตร์เพื่อพิสูจน์ ข้อเท็จจริงหรือหาความกระจ่างให้กับเรื่องที่กำลังสนใจอยู่ได้

	(G)
gather	ຽວບຽວມ
	(H)
handwriting	ลายมือเขียนข้อความ
hot spots	พื้นที่เสี่ยงภัย
hypotheses	สมมติฐาน
hypotheses testing	การทดสอบสมมติฐาน
	(1)
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	รกฎหมายเกี่ยวกับความปลอดภัยของเทคโนโลยีสารสนเทศ
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	្និច			
models	แบบจำลอง			
motion	การเคลื่อนที่			
memory Dump Tool	เครื่องมือทำสำเนาหน่วยความจำ			
mobile Phone Forensics Tool	เครื่องมือตรวจวิเคราะห์โทรศัพท์เคลื่อนที่			
malware (malicious software)	ไวรัส หนอนอินเทอร์เน็ต และโทรจันที่มีพฤติกร			
	รบกวนและสร้างความเสียหายแก่ระบบเครื่องคอมพิวเตอร์			
	(N)			
network Security Officer	เจ้าหน้าที่รักษาความปลอดภัยเครือข่าย ผู้ซึ่งได้รับ			
	มอบหมาย			
	อย่างเป็นทางการจากผู้ซึ่งมีอำนาจหน้าที่ให้มีการปฏิบัติ			
	อย่างถูกต้องในเรื่องที่เกี่ยวข้องภายในระบบข้อมูลอัตโนมัติ			
nontechnical attack social	เป็นภัยคุกคามที่ใช้เล่ห์กลต่าง ๆ เพื่อให้เราเปิดเผยข้อมูล			
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			
	การเปดเผยโดยไม่ได้รับอนุญาตทั้งโดยอุบัติเหตุและโดย			
	เจตนาในระหว่างการ Input, Processing และ Output			

ปฏิบัติการความปลอดภัย กระบวนการพิสูจน์ทราบข้อมูล สำคัญและการวิเคราะห์การกระทำของฝ่ายเราที่เกี่ยวข้อง กับปฏิบัติการทางทหารและกิจกรรมอื่น 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 โดยส่วนใหญ่จะมีวัตถุประสงค์ที่จะต้องการข้อมูลข่าวสาร ต่าง ๆ โดยส่วนมากข่าวสารที่คนส่ง Phishing ต้องการมาก คือ User, Password และหมายเลขบัตรเครดิต โดย Phishing ส่วนมากจะอ้างว่ามาจากบริษัทที่มีความ น่าเชื่อถือว่ามาจากบริษัทที่เหยื่อเป็นสมาชิกอยู่เป็น eBay.com, Pay Pal.com และOnline Banks ต่าง ๆ เป็นต้น
research design	งา น การออกแบบการวิจัย

researc research hypothesis research methodology response retrieval

การตั้งสมมติฐานการวิจัย ระเบียบวิธีวิจัย การตอบสนอง 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	มาตรฐานของ Protocol การสื่อสารที่มีกระบวนการ พิสูจน์ตัวตนรวมอยู่ในชุด Protocol โดย SSL ถูกออกแบบ และกำหนดรายละเอียดโดยบริษัท Netscape เมื่อ ค.ศ. ๑๙๙๔ เพื่อบริการความปลอดภัยแก่ข้อมูลในระหว่างชั้น Protocol ระดับแอปพลิเคชัน (เช่น HTTP, Telnet, NNTP,หรือ FTP) กับ Protocol TCP /IP และเป็นมาตรฐานความปลอดภัย สำหรับโปรแกรมWeb Browsers และเครื่อง Servers บนเครือข่าย Internet โดย SSL ทำให้เกิดการสื่อสาร อย่างปลอดภัยระหว่างไคลเอนต์และเซิร์ฟเวอร์ โดยการ อนุญาตให้มีกระบวนการพิสูจน์ตัวตนร่วมกับการใช้งาน ลายเซ็นดิจิทัล สำหรับการรักษาความถูกต้องของข้อมูลและ การเข้ารหัสข้อมูล (Data Encryption) เพื่อป้องกันความเป็นส่วนตัวระหว่าง การสื่อสารข้อมูล ทั้งนี้ Web ที่ใช้ SSL จะมีรูปกุญแจอยู่ ในมุมล่างของ Web Browser และ Web Address จะขึ้นต้นด้วยคำว่า Https
seminar in Forensic science	สัมมนานิติวิทยาศาสตร์
signatures	ลายมือชื่อ
ource determination	การกำหนดแหล่งที่มา
specific methods	วิธีการตรวจพิเศษ
storage	การจัดเก็บ
storing	การจัดเก็บ
spam mail	การส่งข้อความที่ไม่เป็นที่ต้องการให้กับคนจำนวนมาก ๆ จากแหล่งที่ผู้รับไม่เคยรู้จักหรือติดต่อมาก่อน โดยมาก อยู่ในรูปของ E-mail ทำให้ผู้รับรำคาญใจและเสียเวลาใน การลบข้อความเหล่านั้นโดย Spam Mail ทำให้ประสิทธิภาพ การขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย

techniques used to detect

testimony examination

techniques

testing

technical attack

training in court

recognition concepts

virtual Private Network

undercover

unique

สังคมออนไลน์ที่ผู้คนมารวมตัวกันบนอินเทอร์เน็ตผ่าน โปรแกรมหรือแอปพลิเคชันต่าง ๆ เช่น Facebook, Twitter และ Instragram เป็นต้น

(T) เทคนิคที่ใช้สืบค้นตรวจพิสูจน์

เทคนิคการสอบปากคำ ภัยคุกคามจากผู้มีความรู้ด้าน System and Software การทดสอบ การฝึกในชั้นศาล (U) การจารกรรม เป็นหนึ่งเดียว (R) แนวคิดทางการรับรู้จดจำรูปแบบ (V) เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN – Wide Area Network) เป็นระบบเครือข่าย

(WAN – Wide Area Network) เป็นระบบเครือข่าย ภายในองค์กร ซึ่งเชื่อมเครือข่ายในแต่ละสาขาเข้าด้วยกัน โดยอาศัย Internet เป็นตัวกลาง มีการทำ Tunneling หรือการสร้างอุโมงค์เสมือนไว้รับส่งข้อมูล มีระบบเข้ารหัส ป้องกันการลักลอบใช้ข้อมูล เหมาะสำหรับองค์กรขนาดใหญ่ ซึ่งต้องการความคล่องตัวในการติดต่อรับส่งข้อมูลเครือข่าย เสมือนที่ยอมให้กลุ่มของ Site สามารถสื่อสารกันได้ นโยบาย ในการใช้งานใน VPN ถูกกำหนดโดยชุดของ Admin Policies ที่จุดทำขึ้นโดยสมาชิกในกลุ่มนั้น หรือถูกกำหนดอย่าง เบ็ดเสร็จโดย Service Provider (SP) site ดังกล่าวนั้น อยู่ภายในองค์กรเดียวกันหรือต่างองค์กรก์ได้ หรือ VPN อาจเป็น Intranet หรือ Extranet Site ดังกล่าวอาจอยู่ ในมากกว่าหนึ่ง VPN ก็ได้หรือ VPN อาจทับกัน, ทุก Site ไม่ จำเป็นต้องอยู่ภายใต้ 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/electronicdiscovery/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 : เครื่องมือขุดข้อมูล 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 สพธอ. (2559, 9). ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยาน หลักฐาน 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-2018b936a1a35d8a
- 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-areunder-

ddos-attack/

The Sleuth Kit. (2023, 1). *Autopsy*. Abstract retrieved from https://www.sleuthkit.org/ autopsy/