คุณลักษณะเฉพาะ

ชุดโปรแกรมสำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์

๑. วัตถุประสงค์การใช้งาน

สำหรับใช้ตรวจพิสูจน์หลักฐานข้อมูลคอมพิวเตอร์ วิเคราะห์ข้อมูลที่บันทึกอยู่ในสื่อบันทึกข้อมูลดิจิทัลชนิดต่างๆ เช่น ฮาร์ดดิสก์ที่ติดตั้งในเครื่องคอมพิวเตอร์ หน่วยความจำของโทรศัพท์เคลื่อนที่

๒. ลักษณะทั่วไป

เป็นชุดโปรแกรมสำเร็จรูปพื้นฐานที่จำเป็นสำหรับการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ ประกอบด้วยโปรแกรมดังนี้

๒.๑ โปรแกรม Encase สำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๒.๒ โปรแกรม Internet Evidence Finder (IEF) ที่ใช้ในการสืบค้นและตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๒.๓ โปรแกรม VMware WorkStation ที่ใช้ในการจำลองระบบคอมพิวเตอร์สำหรับการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๒.๔ โปรแกรม TeamViewer ที่ใช้ในการควบคุมคอมพิวเตอร์ผ่านระบบเครือข่ายสำหรับการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๓. คุณลักษณะเฉพาะทางวิชาการ

ผ๑.๑.๑

๓.๑ โปรแกรม Encase สำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๓.๑.๑ สามารถใช้งานบนระบบปฏิบัติการ Microsoft Windows ทั้งในรูปแบบ 32Bit และ 64Bit ได้เป็นอย่างน้อย

๓.๑.๒ รองรับการสืบค้นระบบในไฟล์ซิสเต็มดังต่อไปนี้ Windows FAT12 (Floppy), FAT16, FAT32, NTFS, Macintosh HFS, HFS+, HFSX, Sun Solaris UFS, Linux EXT2, EXT3, EXT4, BSD FFS, FreeBSD FFS2/UFS2, IBM AIX JFS, CDFS, Joliet, DVD, UDF, ISO 9660, Palm และ HP-UX (vxfs) ได้เป็นอย่างน้อย

๓.๑.๓ สามารถจัดสร้างอิมเมจไฟล์โดยทำในรูปแบบของ Bit-Stream Image หรือ Bit-by-Bit Copy ซึ่งสามารถจัดเก็บได้ทั้งในแบบ Physical และ Logical Drive ได้เป็นอย่างน้อย

พ.ต.ท. ประธาน	ร.ต.อ. กรรมการ	ร.ต.ท. กรรมการ/เลขานุการ
(นิติ อินทุลักษณ์)	(วุฒิชัย โกญจนาท)	(ธัญญสิทธิ์ เกิดโภคทรัพย์)
นักวิทยาศาสตร์(สบ๒)	นักวิทยาศาสตร์(สบ๑)	นักวิทยาศาสตร์(สบ๑)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจทางเคมี ฟิสิกส์ ปฏิบัติหน้าที่ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

๓.๑.๔ รองรับการทำงานกับสำเนาหลักฐานในรูปแบบ E01, EX01, L01, LX01 และ DD ได้เป็นอย่างน้อย

๓.๑.๕ การจัดเก็บของอิมเมจต้องสามารถตรวจสอบความสมบูรณ์และถูกต้องโดยใช้ MD5 และ SHA-1 ได้เป็นอย่างน้อย

๓.๑.๖ สามารถตรวจสอบข้อมูลจดหมายอิเล็กทรอนิกส์ได้หลายรูปแบบ เช่น Outlook PST, Outlook Express DBX, Microsoft Exchange EDB, Lotus Notes NSF และ AOL ได้เป็นอย่างน้อย

๓.๑.๗ สามารถตรวจสอบข้อมูลจดหมายอิเล็กทรอนิกส์ทางเว็บ (Web-based email) ได้ เช่น Yahoo, Hotmail, Netscape mail ได้เป็นอย่างน้อย

๓.๑.๘ สามารถแสดงประวัติการใช้งานอินเทอร์เน็ต (Web-Browsing History) และหน้าเว็บเพจที่ถูกเก็บไว้ (HTML Cached) ของโปรแกรม Internet Explorer, Mozilla Firefox และ Apple Safari ได้เป็นอย่างน้อย

๓.๑.๙ สามารถวิเคราะห์ระบบอิมเมจไฟล์ของ VMWARE, Microsoft Virtual PC และ SafeBack v2 ได้เป็นอย่างน้อย

๓.๑.๑๐ สามารถค้นหาไฟล์ที่ถูกลบ และต้องรองรับภาษาไทยได้เป็นอย่างน้อย

๓.๑.๑๑ สามารถสร้างดัชนีข้อมูล (Indexing) พร้อมทำการค้นหาแบบ Live Search ได้เป็นอย่างน้อย

มอ.๑.๑

๓.๑.๑๒ สามารถค้นหาข้อมูลตามคำที่สนใจ (Keyword) ได้เป็นอย่างน้อย

๓.๑.๑๓ สามารถสร้างระบบจำลองไฟล์เสมือน (Virtual File System) โดยสร้างไดร์ฟเสมือนจากไฟล์หลักฐานได้

๓.๑.๑๔ สามารถสร้างระบบจำลองดิสก์เสมือนจริง (Physical Disk Emulator) โดยการสร้างระบบดิสก์เสมือนจริงขึ้นมาจากไฟล์หลักฐานได้

๓.๑.๑๕ รองรับถอดรหัสไฟล์ Encrypting File System (EFS), SafeGuard Easy, PGP WDE, SecureDoc Full Disk Encryption และ McAfee SafeBoot ได้เป็นอย่างน้อย

พ.ต.ท. ประธาน	ร.ต.อ. กรรมการ	ร.ต.ท. กรรมการ/เลขานุการ
(นิติ อินทุลักษณ์)	(วุฒิชัย โกญจนาท)	(ธัญญสิทธิ์ เกิดโภคทรัพย์)
นักวิทยาศาสตร์(สบ๒)	นักวิทยาศาสตร์(สบ๑)	นักวิทยาศาสตร์(สบ๑)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจทางเคมี ฟิสิกส์ ปฏิบัติหน้าที่ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

๓.๑.๑๖ สามารถสร้างระบบป้องกันการเขียนทับข้อมูลแบบซอร์ฟแวร์ (Software Writeblocker) ได้

๓.๑.๑๗ สามารถตรวจวิเคราะห์ข้อมูลจากโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการ iOS, Nokia , Windows Mobile และ Android ได้เป็นอย่างน้อย

๓.๑.๑๘ สามารถสร้างรายงานในรูปแบบ TEXT, RTF, XML, HTML และ PDF ได้ และผู้ใช้สามารถปรับเปลี่ยนรูปแบบรายงานได้ตามต้องการ

๓.๒ โปรแกรม Internet Evidence Finder (IEF) ที่ใช้ในการสืบค้นและตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๓.๒.๑ เป็นโปรแกรมที่ใช้ในการสืบค้นและตรวจพิสูจน์หลักฐานคอมพิวเตอร์ที่เกี่ยวกับประวัติการใช้งานอินเทอร์เน็ตในระบบคอมพิวเตอร์

๓.๒.๒ สามารถใช้งานบนระบบปฏิบัติการ Microsoft Windows 2000, XP, Vista และ 7 ทั้งในรูปแบบ 32Bit และ 64Bit ได้เป็นอย่างน้อย

๓.๒.๓ รองรับการทำงานกับสำเนาหลักฐานในรูปแบบ E01, EX01, L01, LX01 และ DD ได้เป็นอย่างน้อย

๓.๒.๔ สามารถวิเคราะห์และค้นหาข้อมูลในหน่วยความจำ (Search Live Memory) ได้

๓.๒.๕ สามารถค้นหาข้อมูลในหน่วยจัดเก็บข้อมูลทั้งแบบ LogicalDrive และ Physical Drive ได้

๓.๒.๖ รองรับการทำงานใน ๓ รูปแบบได้แก่ Full Search, Quick Search และ Unallocated Search ได้เป็นอย่างน้อย

ผ.ต.ต

๓.๒.๗ รองรับการการวิเคราะห์หลักฐาน Pictures, Videos, Instant Messaging Chat History, Web Browser History, Browser Activity, Social Networking Sites, Webmail, P2P File sharing applications, Cloud based services, และ Google Maps ได้เป็นอย่างน้อย

๓.๒.๘ สามารถออกรายงานในรูปแบบ PDF, Excel และ HTML ได้

๓.๒.๙ เป็นโปรแกรมที่ผ่านการทดสอบจาก US Defense Cyber Crime Institute (DC3)

พ.ต.ท.	ประธาน	ร.ต.อ.	กรรมการ	ร.ต.ท.	กรรมการ/เลขานุการ
(นิติ อินทุลักษณ์)		(วุฒิชัย โกญจนาท)		(ธัญญสิทธิ์ เกิดโภคทรัพย์)	
นักวิทยาศาสตร์(สบ๒)		นักวิทยาศาสตร์(สบ๑)		นักวิทยาศาสตร์(สบ๑)	
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์		กลุ่มงานตรวจทางเคมี ฟิสิกส์ ปฏิบัติหน้าที่ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์		กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	

๓.๓ โปรแกรม VMwareWorkStation ที่ใช้ในการจำลองระบบคอมพิวเตอร์สำหรับการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๓.๓.๑ เป็นโปรแกรมสำหรับจำลองระบบคอมพิวเตอร์เสมือน (Virtual Machine)

๓.๓.๒ สามารถรองรับหน่วยประมวลผลกลางเสมือนได้อย่างน้อย ๑๖ ตัว

๓.๓.๓ สามารถรองรับหน่วยความจำเสมือนได้อย่างน้อย ๘ เทระไบต์

๓.๓.๔ สามารถรองรับระบบเครือข่ายเสมือนได้อย่างน้อย ๒๐ ระบบ มอ.๓.๓

๓.๓.๕ สามารถรองรับการประมวลผลแบบ Hyper-V support

๓.๓.๖ สามารถติดตั้งได้บนระบบปฏิบัติการ Windows 7 หรือ Window 10 ได้เป็นอย่างน้อย

๓.๓.๗ รองรับหน่วยความจำของการ์ดแสดงผลขนาด ๒ จิกะไบต์

๓.๓.๘ รองรับการบูตแบบ Boot virtual machines with EFI support ได้เป็นอย่างน้อย

๓.๓.๙ สามารถนำออกข้อมูลของโปรแกรมไปเป็นระบบ OVF ได้

๓.๔ โปรแกรม TeamViewer ที่ใช้ในการควบคุมคอมพิวเตอร์ผ่านระบบเครือข่ายสำหรับการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รุ่นปัจจุบัน

๓.๔.๑ เป็นโปรแกรมสำหรับใช้ควบคุมระบบคอมพิวเตอร์ผ่านระบบเครือข่ายอินเทอร์เน็ต (Remote)

๓.๔.๒ สามารถรองรับการทำงานของระบบปฏิบัติการ Windows, Mac, Linux, iOS, Android, Windows Phone 8 ได้เป็นอย่างน้อย

๓.๔.๓ มีความสามารถเปลี่ยนเมนูการใช้งานภาษาไทยและภาษาอังกฤษ

๔. <u>ส่วนประกอบและอุปกรณ์อะไหล่</u>

๔.๑ ชุดโปรแกรมสำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ทั้งหมด ต้องมีชื่อผู้ใช้งาน และรหัสผ่านสำหรับเข้าใช้บริการเว็ปไซต์ของผู้ผลิตเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ

๔.๒ ชุดโปรแกรมสำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ทั้งหมด ต้องสามารถอัพเกรดชุดโปรแกรมเมื่อบริษัทผู้ผลิตมีการออกรุ่นใหม่ได้ในระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ

๔.๓ มีกล่องใส่อุปกรณ์ และคู่มือการใช้งานโปรแกรมครบชุด

พ.ต.ท. ประธาน	ร.ต.อ. กรรมการ	ร.ต.ท. กรรมการ/เลขานุการ
(นิติ อินทุลักษณ์)	(วุฒิชัย โกญจนาท)	(ธัญญสิทธิ์ เกิดโภคทรัพย์)
นักวิทยาศาสตร์(สบ๒)	นักวิทยาศาสตร์(สบ๑)	นักวิทยาศาสตร์(สบ๑)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจทางเคมี ฟิสิกส์ ปฏิบัติหน้าที่ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

๕. **การทดสอบและผล**

๕.๑ ตรวจพินิจความเรียบร้อยตามข้อ ๒, ๓ และ ๔

๕.๒ ทำการทดสอบการทำงานของโปรแกรมจนสามารถใช้งานได้ดี

๖. **ข้อกำหนดอื่นๆ**

มอ.๓.๑

๖.๑ ชุดโปรแกรมต้องติดตั้งให้พร้อมใช้งาน

๖.๒ รับประกันคุณภาพพร้อมทั้งบริการแก้ไขปัญหาขัดข้องในการใช้งานโปรแกรมในกรณีต่างๆ ไม่น้อยกว่า ๓ ปี นับจากวันรับมอบ

๖.๓ โปรแกรมตามข้อ ๒.๑ ถึง ๒.๔ มีการฝึกอบรมใช้งานโปรแกรมให้กับเจ้าหน้าที่ไม่เกิน ๑๐ นาย ระยะเวลารวมไม่น้อยกว่า ๒๐ ชั่วโมง

พ.ต.ท. ประธานกรรมการ
(นิติ อินทุลักษณ์)
นักวิทยาศาสตร์ (สบ๒) กลุ่มงานตรวจพิสูจน์
อาชญากรรมคอมพิวเตอร์

ร.ต.อ. กรรมการ
(วุฒิชัย โกญจนาท)
นักวิทยาศาสตร์ (สบ๑) กลุ่มงานตรวจทางเคมี ฟิสิกส์
ปฏิบัติหน้าที่กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

ร.ต.ท. กรรมการ/เลขานุการ
(ธัญญสิทธิ์ เกิดโภคทรัพย์)
นักวิทยาศาสตร์ (สบ๑) กลุ่มงานตรวจพิสูจน์
อาชญากรรมคอมพิวเตอร์

–อนุมัติ

พล.ต.ท.
(มนู เมฆหมอก)
ผบช.สพฐ.ตร.
คณะกรรมการพิจารณาคุณลักษณะเฉพาะของพัสดุ และขอบเขตโดยละเอียดของงาน (TOR) เครื่องมือวิทยาศาสตร์และอุปกรณ์เครื่องมือเครื่องใช้เกี่ยวกับการตรวจพิสูจน์ สำนักงานพิสูจน์หลักฐานตำรวจ ได้มีมติเห็นชอบให้ใช้ ในการประชุม ครั้งที่ ๕ / ๒๕๕๙
วันที่ ๑๖ พ.ค ๒๕๕๙

พล.ต.ต.
(เสถียร คูวิบูลย์ศิลป์)
ผบก.สฝจ./เลขานุการ
๑๐ ส.ค. ๒๕๕๙