คุณลักษณะเฉพาะ

ชุดอุปกรณ์เครื่องมือและชุดโปรแกรมในการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์

๑. วัตถุประสงค์การใช้งาน

ใช้สำหรับตรวจพิสูจน์หลักฐานและวิเคราะห์ข้อมูลที่บันทึกในวัตถุพยานชนิดต่างๆ เช่น คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ หน่วยความจำของอุปกรณ์พกพา เป็นต้น

๒. ลักษณะทั่วไป

เป็นชุดเครื่องมือและอุปกรณ์ที่ใช้วิเคราะห์ข้อมูลระบบปฏิบัติการ หรือประวัติการใช้งานโปรแกรมต่างๆ ของผู้ใช้งานที่ติดตั้งอยู่ เช่น ประวัติการโทรศัพท์ การรับส่งข้อความสั้น (SMS) โปรแกรมสนทนาระบบโซเชียลเน็ตเวิร์ค การเข้าถึงระบบอินเทอร์เน็ต หรือแฟ้มข้อมูลอื่นๆ เป็นต้น โดย ๑ ชุด ประกอบด้วย

๒.๑ ชุดโปรแกรมตรวจพิสูจน์หลักฐานคอมพิวเตอร์ EnCase จำนวน ๒ ชุด

๒.๒ ชุดโปรแกรมตรวจพิสูจน์ข้อมูลระบบโซเชียลเน็ตเวิร์ค จำนวน ๑ ชุด

๒.๓ ชุดตรวจพิสูจน์โทรศัพท์เคลื่อนที่ Cellebrite จำนวน ๑ ชุด

พ.ต.อ.หญิง สุเทพา โสรมย์

๓. คุณลักษณะเฉพาะทางวิชาการ

๓.๑ ชุดโปรแกรมตรวจพิสูจน์หลักฐานคอมพิวเตอร์ EnCase

๓.๑.๑ เป็นโปรแกรมรุ่นสำหรับหน่วยงานบังคับใช้กฎหมาย ที่สามารถติดตั้งใช้งานบนระบบปฏิบัติการ Microsoft Windows 10 แบบ 64Bit ได้เป็นอย่างน้อย

๓.๑.๒ รองรับการสืบค้นระบบในระบบไฟล์ดังต่อไปนี้ FAT12/16/32, NTFS, EXT2/3/4, UFS/UFS2, LVM8, FFS/FFS2, Palm, HFS, HFS+, HFSX, CDFS, Joliet, ISO 9660, UDF, DVD และ HP-UX ได้เป็นอย่างน้อย

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

๓.๑.๔ รองรับการทำงานกับข้อมูลสำเนาหลักฐานในรูปแบบ 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

พ.ต.อ. ประธาน	พ.ต.ต.หญิง กรรมการ	ว่าที่ ร.ต.อ.หญิง กรรมการ/เลขานุการ
(วิวัฒน์ สิทธิสรเดช)	(สมร ดีแสง)	(วันทนีย์ ตุลยเสวี)
นวท.(สบ ๔) กคพ.พฐก.	นวท.(สบ ๒) กคพ.พฐก.	นวท.(สบ ๑) กคพ.ศพฐ.๓ ปฏิบัติราชการ กคพ.พฐก.

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 ในพื้นที่ Unallocated หรือ File Slack ได้เป็นอย่างน้อย

๓.๑.๑๑ สามารถสร้างดัชนีข้อมูล (Indexing) พร้อมทำการค้นหาแบบ Live Search ได้เป็นอย่างน้อย

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

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

พ.ต.อ.หญิง

พ.ต.อ. ประธาน
(วิวัฒน์ สิทธิสรเดช)
นวท.(สบ ๔) กคพ.พฐก.

พ.ต.ต.หญิง กรรมการ
(สมร ดีแสง)
นวท.(สบ ๒) กคพ.พฐก.

ว่าที่ ร.ต.อ.หญิง กรรมการ/เลขานุการ
(วันทนีย์ ตุลยเสวี)
นวท.(สบ ๑) กคพ.ศพฐ.๓
ปฏิบัติราชการ กคพ.พฐก.

ชุด1

๓.๒ ชุดโปรแกรมตรวจพิสูจน์ข้อมูลระบบโซเชียลเน็ตเวิร์ค

๓.๒.๑ เป็นโปรแกรมที่ใช้ในการตรวจพิสูจน์ สืบค้นและวิเคราะห์ข้อมูลหลักฐานทางคอมพิวเตอร์ที่เกี่ยวกับประวัติการใช้งานอินเทอร์เน็ตในระบบคอมพิวเตอร์

๓.๒.๒ สามารถใช้งานบนระบบปฏิบัติการ Microsoft Windows 10 แบบ 64Bit ได้เป็นอย่างน้อย

๓.๒.๓ รองรับการทำงานกับสำเนาหลักฐานในรูปแบบ (Evidence Image Formats) E01, EX01, L01, LX01, AD1, DD, RAW, BIN, IMG, DMG, FLP, VFD, BIF, VMDK, VHD, VDI, XVA, ZIP และ TAR ได้เป็นอย่างน้อย

๓.๒.๔ รองรับการวิเคราะห์และสืบค้นข้อมูลของระบบการจัดเก็บข้อมูล (File System) NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT และ YAFFS2 ได้เป็นอย่างน้อย

พ.ต.อ.หญิง

๓.๒.๕ รองรับข้อมูลนำเข้า (Search Input Source) แบบ Drives, Files/Folders, Images, JTAG/ Chip Off Images, Network Shares, Live RAM Captures, Physical/ Logical Mobile Images, Volume Shadow Copies และ Volumes/ Partitions ได้เป็นอย่างน้อย

๓.๒.๖ สามารถวิเคราะห์และสืบค้นข้อมูลในหน่วยความจำ (live RAM captures) ได้

๓.๒.๗ สามารถวิเคราะห์และสืบค้นข้อมูลจากโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการ iOS, Android, Kindle Fire และ Windows 10

๓.๒.๘ สามารถค้นหาข้อมูลในหน่วยจัดเก็บข้อมูลทั้งแบบ LogicalDrive และ Physical Drive ได้

๓.๒.๙ รองรับการวิเคราะห์ข้อมูล unallocated cluster และ unpartitioned space

๓.๒.๑๐ รองรับการวิเคราะห์ข้อมูล Social Media แบบ Bebo, Facebook, Google+, Instagram, LINE, LinkedIn, MySpace, Twitter, Sina Weibo และ VK ได้เป็นอย่างน้อย

๓.๒.๑๑ รองรับการวิเคราะห์ข้อมูล Web Mail แบบ Gmail, GMX, Hotmail, Hushmail, Mailinator, MBOX, Outlook.com และ Yahoo ได้เป็นอย่างน้อย

๓.๒.๑๒ รองรับการวิเคราะห์ข้อมูล Chat แบบ Adium, AIM, Chatroulette, GoogleTalk, iChat, iMessage, Mail.ru, MSN Messenger, MSN Plus!, ICQ, Mail.ru, mIRC, Omegle, ooVoo, Paltalk, Pidgin, QQ Chat, Second Life, Skype, TorChat,

๓.๒.๑๓ รองรับการการวิเคราะห์หลักฐาน Pictures, Videos, Web Browser History, Browser Activity, P2P File sharing applications และ Google Maps ได้เป็นอย่างน้อย

๓.๒.๑๔ รองรับการวิเคราะห์ข้อมูล Cloud Services แบบ Carbonite, Dropbox (including Dropbox database decryption) , Google docs, Google Drive, Flickr, Sharepoint และ SkyDrive/OneDrive ได้เป็นอย่างน้อย

๓.๒.๑๕ สามารถออกรายงานในรูปแบบ TRUE VIEW EXPORTS

๓.๓ ชุดตรวจพิสูจน์โทรศัพท์เคลื่อนที่ Cellebrite

๓.๓.๑ มีสิทธิ์การใช้งานโปรแกรม UFED4PC, UFED Physical Analyzer, UFED Phone Detective และ UFED Reader ได้เป็นอย่างน้อย

๓.๓.๒ สามารถทำสำเนาข้อมูลใน SIM Card (SIM Card Clone) ได้

๓.๓.๓ สามารถสืบค้นข้อมูลในเครื่องโทรศัพท์ได้แก่ Call History, SMS, Phonebook, Contacts, Audio, Video, Picture, Email, Calendar และ IMEI ได้เป็นอย่างน้อย

๓.๓.๔ สามารถตรวจสอบข้อมูลการใช้งานระบบเครือข่าย (Network Information) ได้เป็นอย่างน้อย

๓.๓.๕ สามารถตรวจสอบข้อมูลประวัติการใช้งานอินเทอร์เน็ต (Web History) ได้เป็นอย่างน้อย

๓.๓.๖ รองรับการวิเคราะห์ข้อมูลโทรศัพท์เคลื่อนที่ และอุปกรณ์ที่ใช้ระบบปฏิบัติการ Android และ iOS ได้เป็นอย่างน้อย

๓.๓.๗ สามารถกรองข้อมูลที่สนใจเป็นพิเศษ (Watch List)

๓.๓.๘ สามารถวิเคราะห์ข้อมูลประวัติการใช้งานแบบ Timeline

๓.๓.๙ สามารถวิเคราะห์ข้อมูลในระดับเลขฐาน ๑๖ (Hex Viewer) พ.ต.อ.หญิง

๓.๓.๑๐ สามารถสืบค้นประวัติการใช้งานโปรแกรม Conversation/Chat

๓.๓.๑๑ สามารถแสดงรายการไฟล์ (Document) ที่มีอยู่ในระบบโทรศัพท์เคลื่อนที่

๓.๓.๑๒ สามารถอ่านแฟ้มข้อมูล SQLite Database ได้

๓.๓.๑๓ สามารถออกรายงานในรูปแบบ PDF, HTML, XML และ Excel ได้

๓.๓.๑๔ สามารถทำงานร่วมกับ Python Script ได้

พ.ต.อ. ประธาน	พ.ต.ต.หญิง กรรมการ	ว่าที่ ร.ต.อ.หญิง กรรมการ/เลขานุการ
(วิวัฒน์ สิทธิสรเดช)	(สมร ดีแสง)	(วันทนีย์ ตุลยเสวี)
นวท.(สบ ๔) กคพ.พฐก.	นวท.(สบ ๒) กคพ.พฐก.	นวท.(สบ ๑) กคพ.ศพฐ.๓
		ปฏิบัติราชการ กคพ.พฐก.

๔. ส่วนประกอบและอุปกรณ์อะไหล่

๔.๑ อุปกรณ์ตามข้อ ๓.๓ ชุดตรวจพิสูจน์โทรศัพท์เคลื่อนที่ Cellebrite มีกระเป๋าหรือกล่องใส่อุปกรณ์แบบครบชุด พร้อมสายเชื่อมต่อกับวัตถุพยานชนิดต่างๆ ครบตามจำนวนที่บริษัทผู้ผลิตกำหนด

๔.๒ อุปกรณ์ตามข้อ ๓.๓ ชุดตรวจพิสูจน์โทรศัพท์เคลื่อนที่ Cellebrite ได้รับอุปกรณ์หรือสายเชื่อมต่อกับวัตถุพยานชนิดต่างๆ เมื่อบริษัทผู้ผลิตมีการออกรุ่นใหม่ ครบตามจำนวนที่บริษัทผู้ผลิตกำหนด เป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบโดยไม่มีค่าใช้จ่าย

๔.๓ โปรแกรมและอุปกรณ์ตามข้อ ๓.๑-๓.๓ มีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้บริการเว็บไซต์ของผู้ผลิตโปรแกรมเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ

๔.๔ มีคู่มือการใช้งานของโปรแกรมและอุปกรณ์ต่างๆ ครบชุด

๕. การทดสอบและผล

๕.๑ ตรวจพินิจความเรียบร้อยตามข้อ ๒, ๓ และ ๔

๕.๒ ทำการทดสอบการทำงานจนสามารถใช้งานได้ดี พ.ต.อ.หญิง

๖. ข้อกำหนดอื่นๆ

๖.๑ ชุดโปรแกรมมีการติดตั้งลงบนเครื่องตรวจพิสูจน์หลักฐานคอมพิวเตอร์ พร้อมทดลองเพื่อให้พร้อมใช้งาน

๖.๒ สามารถปรับปรุงรุ่นโปรแกรมเมื่อบริษัทผู้ผลิตมีการออกโปรแกรมรุ่นใหม่ได้ในระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ โดยไม่เรียกร้องค่าใช้จ่ายเพิ่มเติม

๖.๓ มีหนังสือรับรองการจัดจำหน่ายผลิตภัณฑ์จากบริษัทผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทยอย่างเป็นทางการ

๖.๔ รับประกันคุณภาพพร้อมทั้งความชำรุดเสียหายตามสภาพการใช้งานปกติ และสามารถให้การสนับสนุนบริการหลังการขายได้ตลอดระยะเวลารับประกัน พร้อมทั้งบริการแก้ไขปัญหาขัดข้องในการใช้งานโปรแกรมในกรณีต่างๆ ไม่น้อยกว่า ๓ ปี นับจากวันรับมอบ

พ.ต.อ. ประธาน	พ.ต.ต.หญิง กรรมการ	ว่าที่ ร.ต.อ.หญิง กรรมการ/เลขานุการ
(วิวัฒน์ สิทธิสรเดช)	(สมร ดีแสง)	(วันทนีย์ ตุลยเสวี)
นวท.(สบ ๔) กคพ.พฐก.	นวท.(สบ ๒) กคพ.พฐก.	นวท.(สบ ๑) กคพ.ศพฐ.๓
		ปฏิบัติราชการ กคพ.พฐก.

๖.๕ จัดให้มีการฝึกอบรมโดยวิทยากรที่ผ่านการรับรองความรู้ความสามารถในด้าน Computer Forensic Examiner ได้แก่ Certified Forensic Computer Examiner (CFCE) ของสถาบัน iACIS หรือ Certified Computer Forensic Technician (CCFT) ของสถาบัน HTCN ให้กับเจ้าหน้าที่ไม่เกิน ๑๐ นาย เป็นระยะเวลา ไม่น้อยกว่า ๑๘ ชั่วโมง

๖.๖ ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายในส่วนของสถานที่ ค่าอาหาร ค่าอาหารว่าง ค่าใช้จ่ายในการเดินทางไปราชการ ค่าพาหนะ ค่าที่พัก และเบี้ยเลี้ยงของผู้เข้ารับการฝึกอบรมทั้งหมด อัตราเบิกจ่ายไม่ต่ำกว่าระเบียบทางราชการกำหนด

พ.ต.อ. ประธานกรรมการ
(วิวัฒน์ สิทธิสรเดช)
นักวิทยาศาสตร์ (สบ ๔)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์
กองพิสูจน์หลักฐานกลาง

พ.ต.ต.หญิง กรรมการ
(สมร ดีแสง)
นักวิทยาศาสตร์ (สบ ๒)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์
กองพิสูจน์หลักฐานกลาง

ว่าที่ ร.ต.อ.หญิง กรรมการ/เลขานุการ
(วันทนีย์ ตุลยเสวี)
นักวิทยาศาสตร์ (สบ ๑)
กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์
ศูนย์พิสูจน์หลักฐาน ๓
ปฏิบัติราชการ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์
กองพิสูจน์หลักฐานกลาง

- อนุมัติตามเสนอ

พล.ต.ท.
(พงษ์วุฒิ พงษ์ศรี)
ผบช.สพฐ.ตร.
๒๐ ก.ค. ๖๑

คณะกรรมการพิจารณาคุณลักษณะเฉพาะของพัสดุและขอบเขตโดยละเอียดของงาน (Terms of Reference) เครื่องมือวิทยาศาสตร์และอุปกรณ์เครื่องมือเครื่องใช้เกี่ยวกับการตรวจพิสูจน์ สำนักงานพิสูจน์หลักฐานตำรวจ ได้มีมติเห็นชอบให้ใช้ในการประชุมครั้งที่ ๔/๒๕๖๑ เมื่อวันที่ ๕ กรกฎาคม ๒๕๖๑

พ.ต.อ.หญิง
(สุเจตนา โสตถิพันธุ์)
นวท.(สบ ๕)ฯ รรท. ผบก.สฝจ./เลขานุการ