

คุณลักษณะเฉพาะ

โปรแกรมตรวจพิสูจน์หลักฐานคอมพิวเตอร์ แบบที่ ๑



๑. วัตถุประสงค์การใช้งาน


ใช้สำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ และสื่อบันทึกข้อมูลดิจิทัล เช่น ฮาร์ดดิสก์ หน่วยความจำ แฟลช แผ่นซีดีชนิดต่างๆ เป็นต้น

๒. ลักษณะทั่วไป

เป็นชุดโปรแกรมตรวจพิสูจน์ Encase สำหรับติดตั้งในเครื่องตรวจพิสูจน์หลักฐาน มีความสามารถเข้าถึงระบบไฟล์ (File system) ชนิดต่างๆ ของสื่อบันทึกข้อมูลดิจิทัล สามารถทำสำเนาข้อมูล ตรวจสอบ และวิเคราะห์ ตรวจหาร่องรอยการกระทำผิด และการกู้คืนข้อมูลดิจิทัล


๓. คุณลักษณะเฉพาะทางวิชาการ

- ๓.๑ เป็นโปรแกรมรุ่นสำหรับหน่วยงานบังคับใช้กฎหมาย ที่สามารถติดตั้งใช้งานบนระบบปฏิบัติการ Microsoft Windows 8 แบบ 64Bit ได้เป็นอย่างน้อย
- ๓.๒ 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
- ๓.๓ สามารถจัดสร้างอิมเมจไฟล์โดยทำในรูปแบบของ Bit Stream Image หรือ Bit-by-Bit Copy ซึ่งสามารถจัดเก็บได้ทั้งในแบบ Physical และ Logical Drive ได้เป็นอย่างน้อย
- ๓.๔ รองรับการทำงานกับข้อมูลสำเนาหลักฐานในรูปแบบ E01, EX01, L01, LX01 และ DD ได้เป็นอย่างน้อย
- ๓.๕ การจัดเก็บของอิมเมจต้องสามารถตรวจสอบความสมบูรณ์และถูกต้องโดยใช้ MD5 และ SHA-1 ได้เป็นอย่างน้อย
- ๓.๖ สามารถตรวจสอบข้อมูลจดหมายอิเล็กทรอนิกส์ได้หลายรูปแบบ เช่น Outlook PST, Outlook Express DBX, Microsoft Exchange EDB, Lotus Notes NSF และ AOL ได้เป็นอย่างน้อย
- ๓.๗ สามารถตรวจสอบข้อมูลจดหมายอิเล็กทรอนิกส์ทางเว็บ (Web-based email) ได้ เช่น Yahoo, Hotmail, Netscape mail ได้เป็นอย่างน้อย
- ๓.๘ สามารถแสดงประวัติการใช้งานอินเทอร์เน็ต (Web-Browsing History) และหน้าเว็บเพจที่ถูกเก็บไว้ (HTML Cached) ของโปรแกรม Internet Explorer, Mozilla Firefox และ Apple Safari ได้เป็นอย่างน้อย


พ.ต.ท. 
(นิตี อินทุลักษณ์)
นวท.(สบ๓) กคพ.พฐก.

ประธาน

ร.ต.อ.


กรรมการ
(รัญญสิทธิ์ เกิดโคตรทรัพย์)
นวท.(สบ๑) กคพ.พฐก.

ร.ต.ท.


กรรมการ/เลขานุการ
(ไทภาน วงศ์บุญรอด)
นวท.(สบ๑) กคพ.พฐก.

- ๓.๙ สามารถวิเคราะห์ระบบอิมเมจไฟล์ของ VMware, Microsoft Virtual PC และ SafeBack v2 ได้ เป็นอย่างน้อย
- ๓.๑๐ สามารถค้นหาไฟล์ที่ถูกลบ ในพื้นที่ Unallocated หรือ File Slack ได้เป็นอย่างน้อย
- ๓.๑๑ สามารถสร้างดัชนีข้อมูล (Indexing) พร้อมทำการค้นหาแบบ Live Search ได้เป็นอย่างน้อย
- ๓.๑๒ สามารถค้นหาข้อมูลตามคำที่สนใจ (Keyword) ได้เป็นอย่างน้อย
- ๓.๑๓ สามารถสร้างระบบจำลองไฟล์เสมือน (Virtual File System) โดยสร้างไดรฟ์เสมือนจากไฟล์ หลักฐานได้
- ๓.๑๔ สามารถสร้างระบบจำลองดิสก์เสมือนจริง (Physical Disk Emulator) โดยการสร้างระบบดิสก์ เสมือนจริงขึ้นมาจากไฟล์หลักฐานได้
- ๓.๑๕ รองรับถอดรหัสไฟล์ Encrypting File System (EFS), SafeGuard Easy, PGP, WDE, SecureDoc Full Disk Encryption และ McAfee SafeBoot ได้เป็นอย่างน้อย
- ๓.๑๖ สามารถสร้างระบบป้องกันการเขียนทับข้อมูลแบบซอฟต์แวร์ (Software Writeblocker) ได้
- ๓.๑๗ สามารถตรวจวิเคราะห์ข้อมูลจากโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการ iOS, Nokia, Windows Mobile และ Android ได้เป็นอย่างน้อย
- ๓.๑๘ สามารถสร้างรายงานในรูปแบบ TEXT, RTF, XML, HTML และ PDF ได้ และผู้ใช้สามารถ ปรับเปลี่ยนรูปแบบรายงานได้ตามต้องการ


๔. ส่วนประกอบและอุปกรณ์อะไหล่

- ๔.๑ มีกล่องใส่อุปกรณ์ครบชุด
- ๔.๒ มีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้บริการเว็บไซต์ของผู้ผลิตโปรแกรมเป็นระยะเวลาไม่น้อย กว่า ๑ ปี นับตั้งแต่วันรับมอบ
- ๔.๓ มีคู่มือการใช้งานครบชุด

๕. การทดสอบและผล

- ๕.๑ ตรวจพินิจความเรียบร้อยตามข้อ ๒, ๓ และ ๔
- ๕.๒ ทำการทดสอบการทำงานของโปรแกรมจนสามารถใช้งานได้ดี



พ.ต.ท. 
(นิติ อินทุลักษณะ)
นวท.(สบ๓) กคพ.พฐก.

ประธาน

ร.ต.อ. 

กรรมการ

(ธีัญญสิทธิ เกิดโคตรทรัพย์)

นวท.(สบ๑) กคพ.พฐก.

ร.ต.ท. 

กรรมการ/เลขานุการ


(โศภณ วงศ์บุญรอด)

นวท.(สบ๑) กคพ.พฐก.

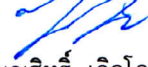
๖. ข้อกำหนดอื่นๆ


- ๖.๑ ชุดโปรแกรมมีการติดตั้งลงบนเครื่องตรวจพิสูจน์หลักฐานคอมพิวเตอร์ พร้อมทดลองเพื่อให้พร้อมใช้งาน
- ๖.๒ สามารถปรับปรุงรุ่นโปรแกรมเมื่อบริษัทผู้ผลิตมีการออกโปรแกรมรุ่นใหม่ได้ในระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ โดยผู้ขายไม่เรียกร้อยค่าใช้จ่ายเพิ่มเติม
- ๖.๓ มีหนังสือรับรองการจัดจำหน่ายผลิตภัณฑ์จากบริษัทผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทยอย่างเป็นทางการ
- ๖.๔ รับประกันคุณภาพพร้อมทั้งความชำรุดเสียหายตามสภาพการใช้งานปกติ และสามารถให้การสนับสนุนบริการหลังการขายได้ตลอดระยะเวลารับประกัน พร้อมทั้งบริการแก้ไขปัญหาขัดข้องในการใช้งานโปรแกรมในกรณีต่างๆ ไม่น้อยกว่า ๓ ปี นับจากวันรับมอบ
- 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 ๓๐ ชั่วโมง



พ.ต.ท. 
(นิติ อินทุลักษณะ)
นาวท.(สบ๓) กคพ.พฐก.

ประธาน

ร.ต.อ.  กรรมการ
(รัญญสิทธิ เกิดโภคทรัพย์)
นาวท.(สบ๑) กคพ.พฐก.

ร.ต.ท.  กรรมการ/เลขานุการ
(โศภณ วงศ์บุญรอด)
นาวท.(สบ๑) กคพ.พฐก.

๖.๖ ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายในส่วนของสถานที่ ค่าอาหาร ค่าอาหารว่าง ค่าใช้จ่ายในการเดินทางไปราชการ ค่าพาหนะ ค่าที่พัก และเบี้ยเลี้ยงของผู้เข้ารับการฝึกอบรมทั้งหมด อัตราเบิกจ่ายไม่ต่ำกว่าระเบียบทางราชการกำหนด



พ.ต.ท.  ประธานกรรมการ

(นิต อินทุลักษณ์)

นักวิทยาศาสตร์ (สบ๓)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

ร.ต.อ.  กรรมการ

(ธิญญสิทธิ์ เกิดโคกทรัพย์)

นักวิทยาศาสตร์ (สบ๑)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

คณะกรรมการพิจารณาคุณลักษณะเฉพาะของพัสดุเครื่องมือวิทยาศาสตร์และอุปกรณ์เครื่องมือเครื่องใช้ที่เกี่ยวข้องกับการตรวจพิสูจน์ สำนักงานพิสูจน์หลักฐาน ตำรวจ ได้มีมติเห็นชอบให้ใช้ในการประชุมครั้งที่ ๒/๒๕๖๒ วันที่ ๒๕ เมษายน ๒๕๖๒

พล.ต.ต. 

(นิต บัณฑวงศ์)

ผบก.สฝจ./เลขานุการ

ร.ต.ท.  กรรมการ/เลขานุการ

(ไศภน วงศ์บุญรอด)

นักวิทยาศาสตร์ (สบ๑)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

- อนุมัติ

พล.ต.ท. 

(พนมพร อธิธิประเสริฐ)

ผบช.สพฐ.ตร.

๒ พ.ค. ๖๒