

## คุณลักษณะเฉพาะ

### ชุดโปรแกรมตรวจพิสูจน์หลักฐานคอมพิวเตอร์ FTK

#### ๑. วัตถุประสงค์การใช้งาน

ใช้สำหรับตรวจพิสูจน์หลักฐานคอมพิวเตอร์ และสื่อบันทึกข้อมูลดิจิทัล เช่น ฮาร์ดดิสก์ หน่วยความจำ แฟลช เป็นต้น ในด้านการถอดรหัสที่มีการป้องกันการเข้าถึงข้อมูล

#### ๒. ลักษณะทั่วไป

เป็นชุดโปรแกรมตรวจพิสูจน์ FTK สำหรับติดตั้งในเครื่องคอมพิวเตอร์ที่ใช้ตรวจพิสูจน์หลักฐาน มีความสามารถค้นหา และวิเคราะห์ข้อมูลร่องรอยการกระทำผิดต่างๆ เช่น ข้อมูลจดหมายอิเล็กทรอนิกส์ ระบบปริ๊นเตอร์ของระบบปฏิบัติการ รวมถึงสามารถกู้คืนข้อมูลรหัสผ่านของโปรแกรมประยุกต์ที่มีใช้งานอย่างแพร่หลายในปัจจุบัน

#### ๓. คุณลักษณะเฉพาะทางวิชาการ

- ๓.๑ โปรแกรมสามารถติดตั้งใช้งานบนระบบปฏิบัติการ Microsoft Windows 7, 8 หรือ 10 แบบ 32 หรือ 64Bit ได้เป็นอย่างดี
- ๓.๒ สนับสนุนการทำงานแบบใช้หน่วยประมวลผลกลางหลายแกน (Multi-Thread/Multi-Core)
- ๓.๓ มีความสามารถบริหารจัดการเรื่องตรวจพิสูจน์โดยอาศัยฐานข้อมูลกลาง มีความสะดวกในการเข้าใช้งาน ลดกระบวนการทำงานที่ซับซ้อน
- ๓.๔ รองรับการค้นหาข้อมูลโดยวิธีการทำดัชนีข้อมูล (Indexing) และการกรองข้อมูล (Filtering)
- ๓.๕ รองรับการวิเคราะห์ข้อมูลในระบบไฟล์ดังต่อไปนี้ FAT12, FAT16, FAT32, NTFS, HFS, HFS+, EXT2/3/4 ได้เป็นอย่างดี
- ๓.๖ รองรับการนำเข้าไฟล์วัตถุพยานในรูปแบบ DMG, AD1, UFD, BIN, TAR, ZIP, E01, EX01, L01, LX01, ISO, VHD, VHDX, DD, VMDK, CTR ได้เป็นอย่างดี
- ๓.๗ มีความสามารถวิเคราะห์ข้อมูลแบบ Volatile Data ได้เป็นอย่างดี
- ๓.๘ สามารถยืนยันความสมบูรณ์และความถูกต้องของวัตถุพยานโดยวิธีการตรวจสอบค่า HASH แบบ MD5 และ SHA-1 ได้เป็นอย่างดี
- ๓.๙ รองรับการวิเคราะห์แฟ้มข้อมูลจดหมายอิเล็กทรอนิกส์ชนิดต่างๆ เช่น Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, Netscape และ AOL ได้เป็นอย่างดี
- ๓.๑๐ สามารถถอดรหัสฐานข้อมูลประเภท PLIST, SQLite ได้เป็นอย่างดี

พ.ต.ท.

( นิติ อินทุลักษณะ )

นวท.(สบ๓) กคพ.พฐก.

ประธาน

ร.ต.อ.

( ธีรยุทธสิทธิ์ เกิดโภคทรัพย์ )

นวท.(สบ๑) กคพ.พฐก.

กรรมการ

ร.ต.ท.

( ไศภณ วงศ์บุญรอด )

นวท.(สบ๑) กคพ.พฐก.

พ.ต.อ. หวิง

กรรมการ/เลขานุการ



- ๓.๑๑ รองรับการอ่านระบบไฟล์ที่มีการเข้ารหัสแบบ Bitlocker และ FileVault ได้เป็นอย่างดีน้อย
- ๓.๑๒ รองรับการค้นหาข้อมูลร่องรอยที่เกิดจากการใช้งาน (Artifacts) เช่น Browsers, Chat, Operating System, Facebook, Line, Skype, Viber, WeChat, WhatsApp, Calendar, Call, Contacts, GPS Cache, SMS, Wifi Networks, Chrome, IE, Firefox และ Safari ได้เป็นอย่างดีน้อย
- ๓.๑๓ มีระบบฐานข้อมูลห้องสมุดเก็บค่า Hash ของไฟล์ต่างๆ จำนวนไม่น้อยกว่า ๔๕ ล้านไฟล์
- ๓.๑๔ ได้รับสิทธิ์การใช้งานโปรแกรมส่วนเสริมเพื่อถอดรหัสแฟ้มข้อมูล Password Recovery Toolkit (PRTK) และ Distributed Network Attack (DNA)


#### ๔. ส่วนประกอบและอุปกรณ์อะไหล่


- ๔.๑ มีกล่องใส่อุปกรณ์ และคู่มือการใช้งานโปรแกรมครบชุด
- ๔.๒ มีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้บริการเว็บไซต์ของผู้ผลิตโปรแกรมเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ


#### ๕. การทดสอบและผล

- ๕.๑ ตรวจสอบพินิจความเรียบร้อยตามข้อ ๒, ๓ และ ๔
- ๕.๒ ทำการทดสอบการทำงานของโปรแกรมจนสามารถใช้งานได้ดี



พ.ต.ท.  ประธาน  
( นิตี อินทุลักษณะ )  
นาวท.(สบ๓) กคพ.พฐก.

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

ร.ต.ท.  กรรมการ/เลขาธิการ  
( โสภณ วงศ์บุญรอด )  
นาวท.(สบ๑) กคพ.พฐก.

## ๖. ข้อกำหนดอื่นๆ

- ๖.๑ ชุดโปรแกรมมีการติดตั้งลงบนเครื่องตรวจพิสูจน์หลักฐานคอมพิวเตอร์ พร้อมทดลองเพื่อให้พร้อมใช้งาน
- ๖.๒ สามารถปรับปรุงรุ่นโปรแกรมเมื่อบริษัทผู้ผลิตมีการออกโปรแกรมรุ่นใหม่ได้ในระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันรับมอบ โดยไม่เรียกวงค่าใช้จ่ายเพิ่มเติม
- ๖.๓ รับประกันคุณภาพพร้อมทั้งความชำรุดเสียหายตามสภาพการใช้งานปกติ และสามารถให้การสนับสนุนบริการหลังการขายได้ตลอดระยะเวลารับประกัน พร้อมทั้งบริการแก้ไขปัญหาขัดข้องในการใช้งานโปรแกรมในกรณีต่างๆ ไม่น้อยกว่า ๓ ปี นับจากวันรับมอบ
- ๖.๔ 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
- ๖.๕ ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายในส่วนของสถานที่ ค่าอาหาร ค่าอาหารว่าง ค่าใช้จ่ายในการเดินทางไปราชการ ค่าพาหนะ ค่าที่พัก และเบี้ยเลี้ยงของผู้เข้ารับการฝึกอบรมทั้งหมด อัตราเบิกจ่ายไม่ต่ำกว่าระเบียบทางราชการกำหนด

- อนุมัติตามเสนอ

พล.ต.ท.

(พงษ์วุฒิ พงษ์ศรี)

ผบช.สพฐ.ตร.

๒๐ ก.ค. ๖๑

คณะกรรมการพิจารณาคุณลักษณะเฉพาะของพัสดุ และขอบเขตโดยละเอียดของงาน (Terms of Reference) เครื่องมือวิทยาศาสตร์และอุปกรณ์ เครื่องมือเครื่องใช้เกี่ยวกับการตรวจพิสูจน์ สำนักงานพิสูจน์หลักฐานตำรวจ ได้มีมติเห็นชอบให้ใช้ในการประชุมครั้งที่ ๔/๒๕๖๑ เมื่อวันที่ ๕ กรกฎาคม ๒๕๖๑

พ.ต.อ.หญิง

สุเจตนา โสทธิพันธุ์

(สุเจตนา โสทธิพันธุ์)

นวท.(สบ ๕)ฯ รรท. ผบก.สฝจ./เลขานุการ

พ.ต.ท.

( นิติ อินทลักษณ์ )

นักวิทยาศาสตร์ (สบ๓)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

ร.ต.อ.

( ธีัญญุสิทธิ์ เกิดโภคทรัพย์ )

นักวิทยาศาสตร์ (สบ๑)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

ร.ต.ท.

( โสภณ วงศ์บุญรอด )

นักวิทยาศาสตร์ (สบ๑)

กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

กองพิสูจน์หลักฐานกลาง

