# เครื่องมือ ตรวจพิสูจน์พยานหลักฐานดิจิทัล

**นายวิษณุ เรืองวิทยานนท์**
**สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย**
**35 หมู่ที่ 3 เทคโนธานี ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี 12120**

ปัจจุบันเครื่องมือในการพิสูจน์พยานหลักฐานดิจิทัลมีอยู่เป็นจำนวนมาก และการเลือกเครื่องมือที่ถูกต้องจะสามารถเพิ่มประสิทธิภาพในการดำเนินการ อย่างไรก็ตาม การเลือกเครื่องมือดังกล่าวก็ขึ้นอยู่กับสถานที่และความต้องการ ดังนั้นในบทความนี้จึงเป็นการแนะนำการเลือกใช้เครื่องมือตรวจพิสูจน์พยานหลักฐานด้านดิจิทัล ซึ่งสามารถแยกได้ดังนี้

| เครื่องมือ | คำอธิบาย |
|---|---|
| • Database forensics | - การพิสูจน์พยานหลักฐานในเรื่องฐานข้อมูล |
| • Email analysis | - การวิเคราะห์จดหมายอิเล็กทรอนิกส์หรืออีเมล |
| • Audio/video forensics | - การพิสูจน์พยานหลักฐานในเรื่องของสื่อที่เป็นไฟล์เสียงหรือภาพเคลื่อนไหว |
| • Internet browsing analysis | - การพิสูจน์พยานหลักฐานในเรื่องการเข้าถึงอินเทอร์เน็ต |
| • Network forensics | - การพิสูจน์พยานหลักฐานที่เกี่ยวข้องกับระบบเครือข่าย |
| • Memory forensics | - การพิสูจน์พยานหลักฐานข้อมูลในหน่วยความจำหลัก |
| • File analysis | - การพิสูจน์พยานหลักฐานที่เกี่ยวกับไฟล์ต่างๆ |
| • Disk and data capture | - การพิสูจน์พยานหลักฐานในสื่อบันทึกข้อมูลต่างๆ และการจับข้อมูลทางดิจิทัล |
| • Computer forensics | - การพิสูจน์พยานหลักฐานของเครื่องคอมพิวเตอร์ |
| • Digital image forensics | - การพิสูจน์พยานหลักฐานที่เป็นข้อมูลรูปภาพ |

การเลือกใช้เครื่องมือตรวจพิสูจน์พยานหลักฐานด้านดิจิทัลขึ้นอยู่กับเงื่อนไขของการตรวจพิสูจน์ เช่น กฎหมายที่เกี่ยวข้อง ทักษะของพนักงาน ดังเช่น แท็บเล็ตที่ไม่สามารถใส่ SIM Card ได้อาจถูกพิจารณาว่าเป็นเครื่องคอมพิวเตอร์จึงต้องใช้เครื่องมือพิสูจน์พยานหลักฐานของเครื่องคอมพิวเตอร์ในการตรวจสอบ ไม่ใช่พิสูจน์พยานหลักฐานของอุปกรณ์เคลื่อนที่

## 5 แนวทาง ในการเลือกเครื่องมือตรวจพิสูจน์พยานหลักฐานด้านดิจิทัลให้เหมาะสม

การเลือกเครื่องมือที่ถูกต้อง ตรงความต้องการ ไม่ง่ายเสมอไป เพราะปัจจุบันมีเครื่องมือให้เลือกมากมาย ต่อไปนี้ เป็นแง่มุมสำหรับการพิจารณาตัดสินใจเลือก

### 1. ระดับของทักษะ

เครื่องมือบางชนิดต้องการเพียงทักษะขั้นพื้นฐาน ในขณะที่เครื่องมือบางชนิดอาจต้องการความเข้าใจขั้นสูง สิ่งสำคัญคือต้องประเมินความรู้ของผู้ใช้งานกับเครื่องมือให้เหมาะสม จึงจะได้เครื่องมือที่มีประสิทธิภาพตรงกับความสามารถในการดำเนินงาน

### 2. ผลลัพธ์

บางครั้งเครื่องมือที่เหมือนกัน อาจให้ผลลัพธ์ที่แตกต่างกัน ในบางกรณีเครื่องมืออาจให้ผลลัพธ์ในรูปของข้อมูลดิบ ในขณะที่บางเครื่องมือสามารถแสดงรายงานผลออกมาได้อย่างสมบูรณ์จนพนักงานที่ไม่มีความรู้ก็สามารถเอาไปอ่านทำความเข้าใจได้ ในทางกลับกัน ในผลลัพธ์ที่เป็นข้อมูลดิบเพียงอย่างเดียวก็อาจเพียงพอสำหรับการนำไปใช้ประโยชน์กับพนักงานที่เชี่ยวชาญบางคนได้

### 3. งบประมาณที่ใช้

การพิจารณาโดยใช้เกณฑ์ราคาเพียงอย่างเดียว อาจไม่เหมาะสมเสมอไป ดังนั้นในระหว่างการตัดสินใจ ควรพิจารณาความเหมาะสมระหว่างงบประมาณและคุณสมบัติต่างๆ ประกอบกันด้วย ทั้งนี้เนื่องจากเครื่องมือที่มีราคาถูกหรือฟรีนั้น อาจไม่ได้ให้คุณลักษณะพิเศษอย่างที่ต้องการ เนื่องจากทีมพัฒนาเครื่องมือเหล่านั้นคงต้องจัดทำเครื่องมือให้มีต้นทุนที่ถูกที่สุดเท่าที่จะเป็นไปได้

### 4. เน้นใช้งานเฉพาะด้าน

เนื่องจากการใช้งานเครื่องมือแต่ละชนิดก็ย่อมมีหน้าที่แตกต่างกัน ดังนั้นจึงขึ้นอยู่กับความต้องการใช้งานเป็นหลัก เช่น เครื่องมือที่ใช้ตรวจสอบฐานข้อมูล ก็จะแตกต่างจากเครื่องมือที่ใช้ทดสอบระบบเครือข่าย แนวทางปฏิบัติที่ดีที่สุด คือ เขียนรายการคุณสมบัติพิเศษที่ต้องการให้ครบถ้วนก่อนการเลือกซื้อ และพิจารณาเลือกเครื่องมือที่ครอบคลุมการทำงานหลายหน้าที่ครบตามคุณสมบัติที่ต้องการ ซึ่งอาจเป็นวิธีที่ดีกว่าการหาเครื่องมือแยกกันสำหรับแต่ละงาน

### 5. อุปกรณ์หรือส่วนเสริมอื่นๆ

เครื่องมือบางอย่างอาจต้องการอุปกรณ์เสริมเพิ่มเติม เพื่อให้สามารถทำงานได้ เช่น การพิสูจน์หลักฐานที่เกี่ยวข้องกับระบบเครือข่าย อาจต้องใช้อุปกรณ์เฉพาะทาง หรือการใช้สื่อบันทึกที่สามารถรีสตาร์ทระบบได้ ดังนั้นต้องตรวจสอบว่าต้องใช้อุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์อะไรบ้างที่จำเป็นในการใช้งานร่วมกัน

## ซอฟต์แวร์สำหรับการพิสูจน์พยานหลักฐานดิจิทัล

มีซอฟต์แวร์สำหรับการพิสูจน์พยานหลักฐานดิจิทัล ให้ใช้งานฟรี แนะนำ 5 ซอฟต์แวร์ด้วยกัน ที่จะมาช่วยในการตรวจสอบทางนิติวิทยาศาสตร์ดิจิทัล อาทิ กรณีของทรัพยากรบุคคลภายในองค์กร การตรวจสอบการเข้าถึงเครื่องแม่ข่ายโดยไม่ได้รับอนุญาต ชุดโปรแกรมและยูทิลิตี้เหล่านี้จะช่วยพิสูจน์พยานหลักฐานข้อมูลในหน่วยความจำหลัก การพิสูจน์พยานหลักฐานในสื่อบันทึกข้อมูล การพิสูจน์พยานหลักฐานที่เป็นข้อมูลรูปภาพ และอุปกรณ์เคลื่อนที่เหล่านี้จะสามารถนำข้อมูลเชิงลึกที่ถูกซ่อนอยู่กลับมาได้

หมายเหตุ รายการข้างล่างนี้ อาจไม่ครอบคลุมในทุกเรื่องที่ต้องการตรวจสอบ อาจจำเป็นต้องใช้โปรแกรมอื่นๆ มาเสริม เช่น โปรแกรมดูข้อมูลในไฟล์ โปรแกรมสร้าง hash และโปรแกรมแก้ไขไฟล์ข้อความ เป็นต้น

### 1 SANS SIFT

The SANS Investigative Forensic Toolkit (SIFT) ทำงานบนระบบปฏิบัติการ Ubuntu ผ่านรูปแบบ Live CD (การบูตและทำงานบนแผ่น CD) ซึ่งรวบรวมเครื่องมือที่จำเป็นในการตรวจพิสูจน์หรือหาร่องรอยเชิงลึก SIFT รองรับการวิเคราะห์ในรูปแบบ Expert Witness Format (E01) (สำหรับไฟล์), Advanced Forensic Format (AFF) (สำหรับ Disk Image) และ รูปแบบ RAW (dd) Evidence SIFT ได้รวมเครื่องมือ เช่น log2timeline ในการสร้าง Timeline สำหรับบันทึกการทำงานของระบบ Scalpel สำหรับการแกะรอยข้อมูล, Fifiuti สำหรับตรวจหาร่องรอยในถังขยะหรือ Recycle bin และอีกมากมาย


ที่มา: SANS Community (2019)

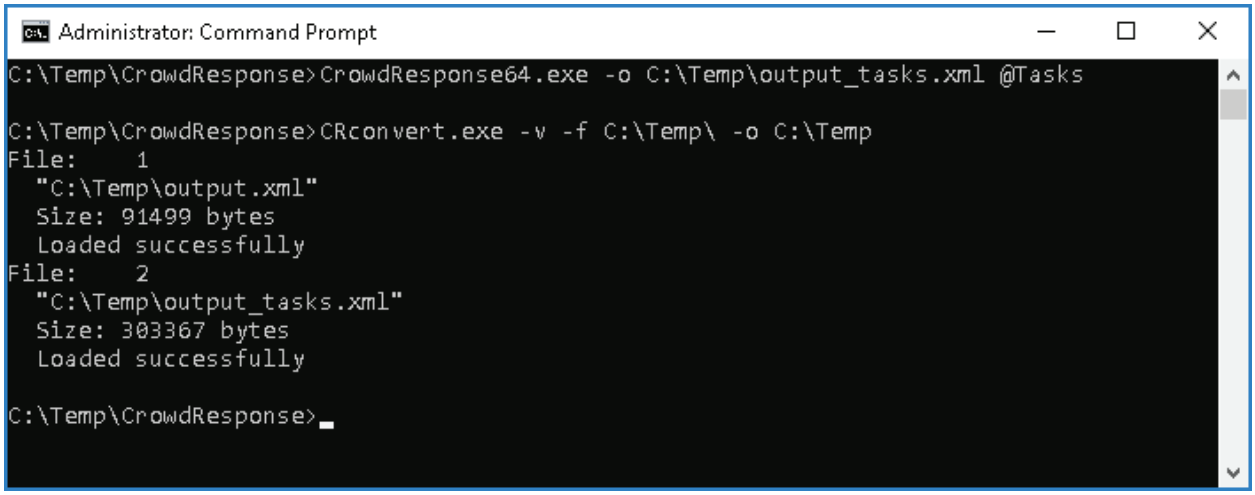
ครั้งแรกที่เปิดเครื่องและเข้าระบบได้ แนะนำให้อ่านเอกสารที่แสดงไว้บน Desktop ก่อน เพื่อให้คุ้นเคยกับเครื่องมือต่างๆ และวิธีการใช้งาน ซึ่งเอกสารเหล่านี้อธิบายได้ดีในการหาหลักฐานในระบบ ใช้เมนูบาร์ด้านบนเพื่อเข้าถึงเครื่องมือ หรือเรียกใช้ผ่าน Terminal Windows ก็ได้

**คุณสมบัติเด่น**

- ทำงานบนระบบปฏิบัติการ 64 บิต
- Update package ที่จำเป็นโดยอัตโนมัติ หรือ เลือกได้ว่าต้องการตัวไหน
- ทำงานระหว่าง Linux และ Windows ได้
- รองรับระบบไฟล์แบบขยายได้
- สามารถทำงานแบบ Live CD หรือติดตั้งลงเครื่องก็ได้

## 2 CrowdStrike CrowdResponse

CrowdResponse คือ แอปพลิเคชันคอนโซลที่มีขนาดเล็ก และสามารถใช้งานเป็นส่วนหนึ่งของสถานการณ์การเผชิญเหตุ เพื่อรวบรวมข้อมูลตามบริบท เช่น ลำดับของกระบวนการทำงาน ตารางเวลาการทำงาน หรือ Shim Cache มีการใช้ลายเซ็น YARA ฝังเข้าไปด้วย จึงสามารถค้นหา Host ที่มี Malware และรายงานกลับถ้าพบว่าติด Malware




ที่มา: GFI Software's blog (2019)

การสั่ง CrowdsResponse ทำงาน ให้ขยายไฟล์ Zip และเรียกใช้ผ่าน Command prompt ด้วยสิทธิ์ระดับ Administrator ให้เข้าสู่ Folder ที่เก็บไฟล์นี้ และพิมพ์คำสั่งให้ทำงาน โดยกำหนดว่าจะให้ผลลัพธ์ไปเก็บใน Folder ไหน และจะใช้เครื่องมืออะไรในการเก็บข้อมูล หากต้องการดู Parameter อื่นๆ ก็สามารถพิมพ์ CrowdResponse64.exe เพื่อดูเครื่องมือ (tools) ที่รองรับและวิธีการใช้งานได้

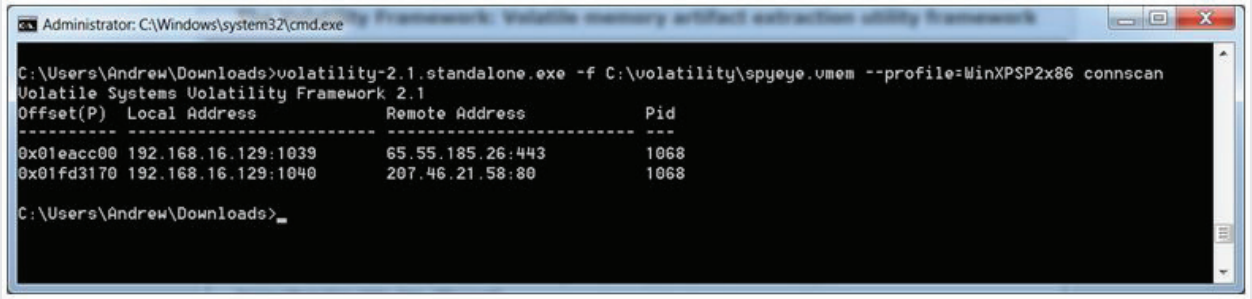
CrowdsResponse ยังมีเครื่องมือสำหรับแปลงข้อมูลจาก xml ไปเป็น csv หรือ html ชื่อ CRConvert.exe ซึ่งเอาข้อมูลที่ส่งออกมา แปลงเป็นรูปแบบที่ต้องการ

**คุณสมบัติเด่น**

- มาพร้อมกับ 3 โมดูล - แสดงรายการไดเรกทอรี โมดูลที่ทำงานอยู่ และโมดูลการประมวลผล YARA
- แสดงข้อมูลทรัพยากรแอปพลิเคชัน
- ตรวจสอบลายเซ็นดิจิทัลของกระบวนการที่กำลังทำงานอยู่
- สแกนหน่วยความจำ รวมถึงไฟล์โมดูลที่โหลดอยู่ และไฟล์บนดิสก์ของกระบวนการที่กำลังทำงานอยู่ทั้งหมด

## 3 Volatility

Volatility เป็นกรอบการทำงานในการตรวจพิสูจน์พยานหลักฐานในหน่วยความจำหลักของคอมพิวเตอร์ ใช้สำหรับการตอบสนองต่อเหตุฉุกเฉินและการวิเคราะห์ Malware ต่างๆ โดยจะทำการแยกข้อมูลดิจิทัลที่สร้างขึ้นออกจากข้อมูลดิบในหน่วยความจำหลัก Volatility เราสามารถแยกข้อมูลเกี่ยวกับงานที่กำลังทำ แยกหมายเลข Socket ของระบบเครือข่ายที่เปิดใช้งานอยู่ และสามารถเชื่อมต่อผ่านระบบเครือข่าย แยก DLL ที่เกี่ยวกับแต่ละงานที่ทำอยู่ แยกกลุ่ม Registry cache และหมายเลขของงานที่กำลังทำ และอื่นๆ




ที่มา: GFI Software's blog (2019)

ถ้าเรียกใช้งานแบบ Standalone ให้ Copy ไปวางใน Folder ใดๆ และเรียกใช้งานผ่าน Command prompt และพิมพ์คำสั่ง ดังนี้

volatility-2.x.standalone.exe –f <FILENAME> –profile=<PROFILENAME> <PLUGINNAME>

<FILENAME> หมายถึง ชื่อของไฟล์ที่ต้องการจะนำมาวิเคราะห์
<PROFILENAME> หมายถึง โปรไฟล์ของเครื่องที่ไปดึงข้อมูลมาเพื่อวิเคราะห์
<PLUGINNAME> หมายถึง ชื่อของ Plugin เสริมที่ต้องการนำมาใช้เพื่อแยกข้อมูลออกมา

หมายเหตุ ตัวอย่างข้างต้น มีการเรียกใช้ Plugin ชื่อ Connscan ในการหาข้อมูลการเชื่อมต่อด้วย TCP จากหน่วยความจำหลัก

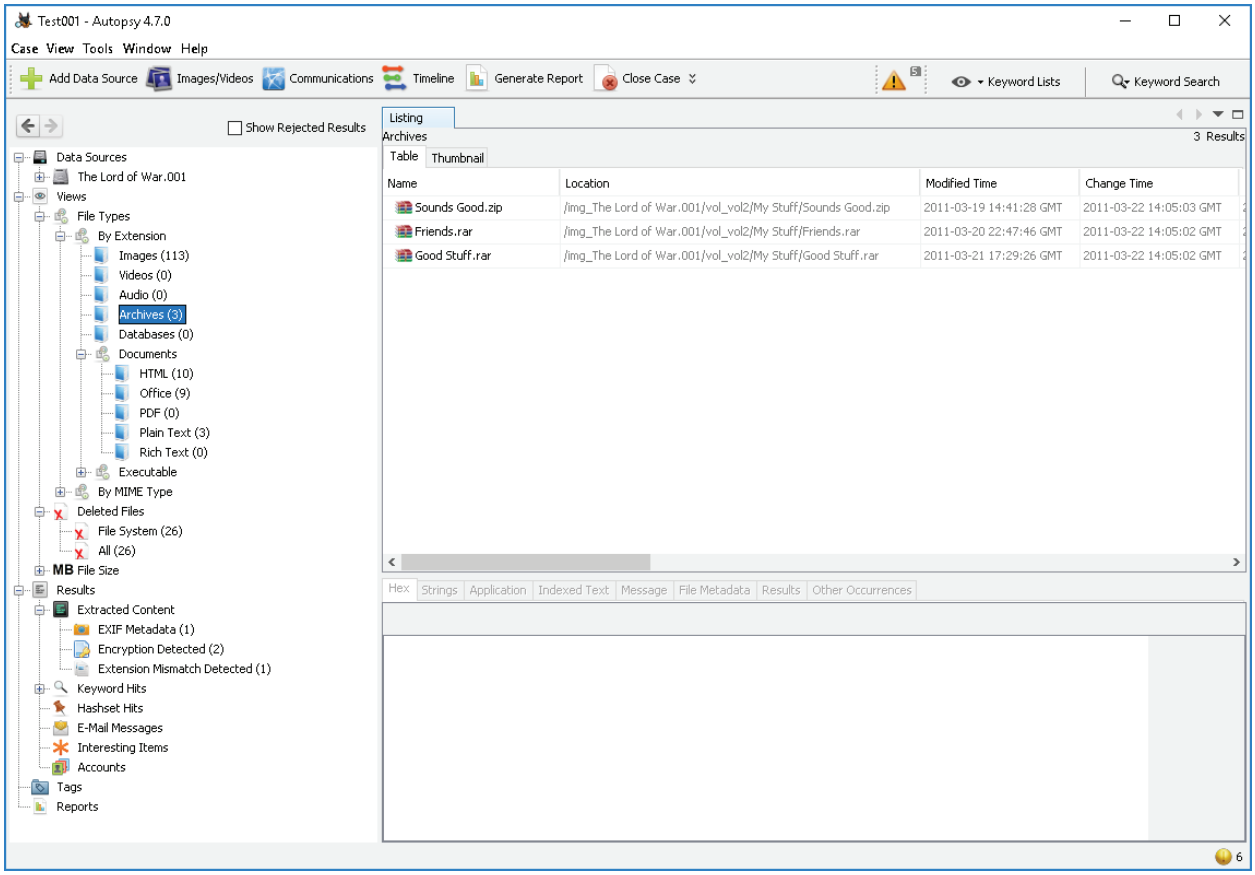
**คุณสมบัติเด่น**

- รองรับข้อมูลได้หลายรูปแบบ
- ทำงานบน Windows, Linux และ MAC
- มาพร้อมกับอัลกอริทึมที่ทำงานได้รวดเร็วและมีประสิทธิภาพ ในการวิเคราะห์ข้อมูลในหน่วยความจำจากระบบที่มีขนาดใหญ่
- API สามารถเพิ่มขยายความสามารถและเขียนเป็น Script ในการเชื่อมต่อเพื่อสร้างเป็นส่วนขยายอื่นๆ ในอนาคตได้

## 4 The Sleuth Kit (+Autopsy)

The Sleuth Kit เป็นเครื่องมือสำหรับตรวจพิสูจน์พยานหลักฐานดิจิทัลที่เปิดเผยรหัสโปรแกรม (Source Code) ที่สามารถใช้เพื่อวิเคราะห์เชิงลึกได้กับไฟล์ระบบได้หลายหลายประเภท Autopsy ทำงานเป็น GUI ให้กับ Sleuth Kit ในส่วนที่จำเป็นสำหรับการทำงาน มาพร้อมกับคุณสมบัติพิเศษ เช่น การวิเคราะห์ตามลำดับเวลา (time serial) การกรอง Hash การวิเคราะห์ไฟล์ระบบ และความสามารถในการค้นหาข้อมูลด้วยคำสำคัญ และยังสามารถเพิ่มโมดูลอื่นเพื่อให้สามารถใช้งานได้กว้างมากขึ้นได้อีกด้วย

หมายเหตุ: การใช้งาน Sleuth Kit ทำได้บน Linux ส่วน Autopsy ทำงานบน Windows




ที่มา: GFI Software's blog (2019)

เมื่อเรียกใช้ Autopsy ให้เลือกสร้าง Case ใหม่หรือเปิดจากที่มีอยู่แล้วก็ได้ ถ้าเลือกที่จะสร้างใหม่ ก็จำเป็นต้องเปิด image ไฟล์ที่ต้องการจะตรวจพิสูจน์ หรือดูบน disk ได้เลย เพื่อเพิ่มการตรวจวิเคราะห์ เมื่อการวิเคราะห์เสร็จสิ้นลง ให้เลือกว่าจะแสดงผลลัพธ์อย่างไร โดยเลือกที่หัวข้อที่แสดงอยู่ด้านซ้ายมือของหน้าจอโปรแกรม

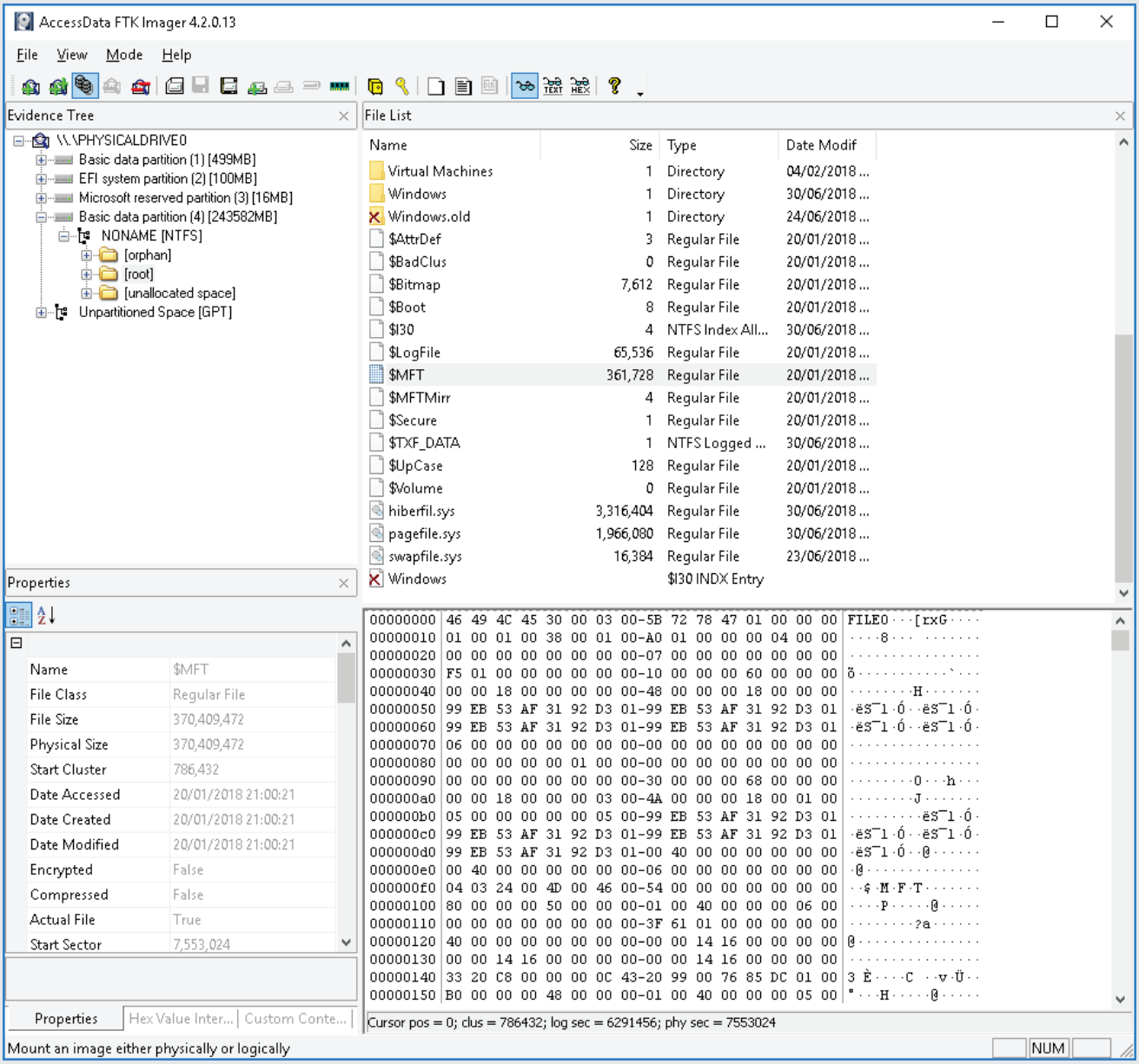
**คุณสมบัติเด่น**

- แสดงเหตุการณ์ที่เกิดขึ้นกับระบบผ่านหน้าจอที่เป็น GUI
- มีตัวเลือกการวิเคราะห์ Registry ไฟล์ LNK และอีเมล
- สนับสนุนไฟล์หลายรูปแบบ
- แยกข้อมูลออกจาก SMS บันทึกการโทร บันทึกหมายเลขติดต่อ โปรแกรม Tango และคำพูดจากเพื่อนมาวิเคราะห์ได้เหมือนกัน

## 5 FTK Imager

เป็นเครื่องมือในการดูข้อมูลรูปภาพ ที่ผู้ปฏิบัติสามารถตรวจสอบไฟล์และ Folder ในฮาร์ดดิสก์ หน่วยเก็บข้อมูลผ่านระบบเครือข่าย ข้อมูลในแผ่น CD/DVD และดูเนื้อหาในรูปภาพหรือหน่วยความจำหลัก เพื่อการพิสูจน์พยานหลักฐานที่เป็นข้อมูลรูปภาพ

หมายเหตุ: FTK มี Version ที่สามารถทำงานบน USB ไดร์ฟได้ด้วย




ที่มา: GFI Software's blog (2019)

เมื่อเรียกใช้ FTK Imager ไปที่เมนู File -> Add Evidence item.. เพื่อเปิดไฟล์หลักฐานที่จะนำมาดู ในการสร้างภาพถ่ายทางนิติวิทยาศาสตร์ ไปที่เมนู File -> Create Disk Image...' และเลือกแหล่งของ Image ที่ต้องการจะตรวจพิสูจน์

**คุณสมบัติเด่น**

- มาพร้อมกับความสามารถในการอ่านไฟล์เพื่อใช้ดูไฟล์หรือโฟลเดอร์ และข้อมูลที่อยู่ภายในไฟล์
- รองรับการเปิดไฟล์ที่เป็นลักษณะ Image
- ทำงานโดยใช้ประสิทธิภาพของ CPU ในเครื่องอย่างเต็มที่ในการทำงานแบบคู่ขนานกัน
- เข้าถึงฐานข้อมูลเคสที่ใช้ร่วมกันดังนั้นฐานข้อมูลกลางเดียวก็เพียงพอสำหรับเคสเดียว

## เอกสารอ้างอิง


GFI Software's blog, 2019. Top 20 Free Digital Forensic Investigation Tools for SysAdmins – 2019 update. [online]. Available at: https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/?fbclid=IwAR0ahSDcRyPO6tLn1E8ifuJ8z_zXE9-ljlIW2VMQGJ3aH3qewcBgh21BAWE, [accessed 11 Febuary 2020].

SANS Community, 2019. Investigate and fight cyberattacks with SIFT Workstation. [online]. Available at: https://www.sans.org/blog/investigate-and-fight-cyberattacks-with-sift-workstation, [accessed 11 Febuary 2020].