Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110 .Tel:02-714-3801-3.Fax :02-714-3804

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

Computer Forensics (การพิสูจน์หลักฐานทางคอมพิวเตอร์) คืออะไร?

January 2012

Date: 09-01-2012

Author: Andrew Smith

ในการค้นหาหลักฐานทุกครั้งนั้นผู้เชี่ยวชาญด้าน Computer Forensics จะทำการตรวจสอบข้อมูลทางอิเล็กทรอนิกส์ ที่เก็บไว้ในคอมพิวเตอร์ และ อุปกรณ์จัดเก็บข้อมูลทางดิจิตอลสำหรับหลักฐานที่ใช้แนวทางของการทำ computer Forensics ในการค้นหาหลักฐาน

ซึ่งขั้นตอนต่างๆ มีความจำเป็นที่ขั้นตอนนี้ต้องมีความชัดเจนในการในการอธิบายหลักฐานในแนวทางของ Computer Forensics

แนวทางการทำ computer Forensics เป็นวิธีการที่ไม่มีการเปลี่ยนแปลงแหล่งที่มาของหลักฐาน หรืออาจมีการเปลี่ยนแปลงน้อยที่สุดเพื่อให้ได้หลักฐานที่ต้องการ วิธีการได้มาของหลักฐานจะถูกบันทึกเป็นเอกสารและสามารถพิสูจน์ได้

การทำ Computer Forensics สามารถแบ่งออกเป็น 5 ขั้นตอนที่สำคัญดังนี้

การเก็บรักษาหลักฐาน – เมื่อมีการจัดการกับข้อมูลทาง digital ผู้ตรวจสอบจะต้องทำทุกอย่างเพื่อรักษาข้อมูล การรักษาข้อมูลนี้จะต้องทำในลักษณะที่จะไม่มีการเปลี่ยนแปลงข้อมูลที่พบ การกระทำในลักษณะนี้จะเกี่ยวข้องกับการทำ Forensics Images หรือ การโคลนนิ่งฮาร์ดดีสก์ ข้อมูลทาง Digital อาจเก็บไว้ใน ฮาร์ดดีสก์, CD/DVD, Floppy disks, pen drives, โทรศัพท์มือถือ , เครื่องเล่นเพลง และเทปสำรองข้อมูล

การระบุหลักฐาน - ในแต่ละปีความจุของฮารดดีสก์จะเพิ่มขึ้นเรื่อยๆ ส่งผลถึงการตรวจสอบข้อมูลอาจต้องเกี่ยวข้องกับข้อมูลจำนวนมากกว่าหนึ่งร้อยกิ๊กกะไบต์ เพื่อที่จะระบุหลักฐานที่มีคุณภาพผู้เชี่ยวชาญจะใช้เทคนิค เช่น การระบุคำในการค้นหา (keyword), แยกไฟล์ที่ต้องการค้นหา เช่น ไฟล์เอกสาร, ไฟล์รูปภาพ หรือไฟล์ประวัติการใช้งานอินเตอร์เนต

การแบ่งข้อมูล - เมื่อมีการพบหลักฐาน และจำเป็นที่จะต้องนำข้อมูลออกจาก forensic image การแสดงผลขึ้นอยู่กับปริมาณข้อมูล อาจใช้การปรินท์ออกมา แต่กรณีที่ข้อมูลมีจำนวนมาก เช่น ประวัติการใช้งานอินเตอร์เนต ซึ่งอาจมีข้อมูลมากถึง 100 หน้า ดังนั้นบางครั้งจึงต้องแสดงผลในรูปแบบของสื่ออิเล็กทรอนิกส์

การระบุหลักฐาน – การระบุถึงหลักฐานและการนำมาแสดงถือเป็นหน้าที่สำคัญของผู้ทำ Computer forensic การนำข้อมูลที่ถูกต้องมาแสดงถือเป็นเรื่องสำคัญมาก ผู้ทำจะต้องไม่เชื่อในผลของเครื่องมือแต่เพียงอย่างเดียวแต่จำเป็นจะต้องสามารถตรวจสอบข้อมูลที่ได้จากซอฟท์แวร์ computer forensic นั้นด้วย

หลักฐานที่ได้ - สิ่งที่สำคัญในการทำ Computer Forensics คือ การจดบันทึกการทำงานที่เกี่ยวข้องกับสื่อดิจิตอลทุกขั้นตอนตลอดการค้นหาข้อมูล บันทึกจะต้องมีข้อมูลที่เพียงพอที่จะให้บุคคลที่สามสามารถเข้าใจได้ หลักฐานสำคัญที่ได้มาจะไม่มีประโยชน์เลยถ้าไม่สามารถเขียนรายงานให้เข้าใจได้ สิ่งที่จำเป็นคือการหลีกเลี่ยงคำที่กำกวมเมื่อจำเป็นจะต้องใช้ศัพท์ทางเทคนิคซึ่งจะต้องมีการอธิบายให้เข้าใจ

หลักการสำคัญในการได้มาซึ่งหลักฐานทาง Computer Forensics

หลักการที่ 1: จะต้องไม่มีการกระทำโดยหน่วยงานด้านกฎหมายหรือตัวแทนบริษัทกฎหมายที่จะทำให้เกิดการเปลี่ยนแปลงข้อมูลที่ตรวจพบในเครื่องคอมพิวเตอร์หรือสื่อจัดเก็บข้อมูลระหว่างการนำหลักฐานไปนำเสนอต่อศาล

หลักการที่ 2: ในกรณีที่บุคคลใดมีความจำเป็นที่จะมีการเข้าถึงข้อมูลในคอมพิวเตอร์หรือสื่อบันทึกข้อมูลซึ่งเป็นหลักฐาน บุคคลนั้นจะต้องอธิบายถึงความเกี่ยวข้องกับข้อมูลและผลกระทบจากการกระทำนั้น

หลักการที่ 3: จะต้องมีการตรวจสอบและบันทึกการดำเนินงานที่เกี่ยวข้องกับหลักฐาน ซึ่งถ้ามีบุคคลภายนอกมาเกี่ยวข้องจะต้องมีการบันทึกไว้เช่นกัน

หลักการที่ **4:** บุคคลที่รับผิดชอบในการดำเนินงาน(เจ้าหน้าดูแลกรณีนั้นโดยตรง) จะต้องรับผิดชอบต่อการกระทำเพื่อให้มั่นใจว่าจะปฏิบัติตามกฎหมายและหลักการแ Computer Forensics

หลักการของ Computer Forensics 4 ข้อ ที่นำเสนอ สามารถนำไปใช้ในคดีต่างๆ ไม่ว่าจะเป็นคดีอาญา, คดีแพ่ง หรือการสืบสวนภายในองค์กร การนำหลักการนี้จะช่วยให้ไม่เกิดคำถามในเรื่องความสมบูรณ์ของหลักฐานดิจิตอล