

นำเสนอโดย: กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์

หัวข้อที่ 2

กู้...อย่างไรให้ผ่าน (Data Recovery)

นางสาวดวงสมร ชูดีจันทร์ ตำแหน่งช่างภาพการแพทย์ชำนาญการ
นางสาวภัทรรัตน์ หอมกระจำง ตำแหน่งนักนิติวิทยาศาสตร์ชำนาญการ
นางสาวกรรณิการ์ สุทรพจนารักษ์ ตำแหน่งนักนิติวิทยาศาสตร์ชำนาญการ
นางสาวอมรรรัตน์ เล็กวิชัย ตำแหน่งนักนิติวิทยาศาสตร์ชำนาญการพิเศษ

หลักการกู้ข้อมูล คือการนำกลับคืนมา หรือ การคืนสภาพ ซึ่งมีข้อควรตระหนักอยู่ 3 สิ่ง ดังนี้

1. สาเหตุ และ เงื่อนไขที่ต้องพิจารณาในการกู้คืนข้อมูล

1.1 สาเหตุที่เกิดจากกิจกรรม:

- ผู้ใช้งานเป็นเหตุให้ข้อมูลสูญหาย อาทิ การลบข้อมูล (Deleted, Empty Recycle Bin, Format), ติดไวรัส (Virus) เป็นต้น
- อุปกรณ์ หรือระบบเป็นเหตุให้ข้อมูลสูญหาย อาทิ Partition Loss, OS Crash, Bad Sector เป็นต้น

1.2 เงื่อนไขประเภทของอุปกรณ์: Hard Drive, RAID Array, USB Drive, Camera Card, Media Tape Backup, Mobile Devices

1.3 เงื่อนไขของระบบปฏิบัติการ: Windows OS, Apple OS, Linux OS, Android OS

1.4 เงื่อนไขของระบบการจัดเก็บ: Online, Offline

1.5 เงื่อนไขตำแหน่งในการจัดเก็บข้อมูล

1.6 เงื่อนไขเรื่ององค์ความรู้

1.7 เงื่อนไขงบประมาณ

1.8 เงื่อนไขการเลือกใช้วิธีที่เหมาะสมในการกู้ข้อมูลจากแต่ละสาเหตุ

2. การประเมินและข้อควรรู้ในการกู้คืนข้อมูล

2.1 ประเมินการกู้คืนข้อมูลโดยใช้ Software

- Non-Forensics Software: อาจเกิดการปนเปื้อนค่อนข้างมาก เพราะอาจเป็น SW ที่ไม่เคยผ่านการทดสอบ ว่าจะส่งผลกระทบต่อส่วนใดของระบบบ้าง
- Forensics Software: ก่อให้เกิดการปนเปื้อนน้อย หรืออาจไม่เกิดการปนเปื้อนต่อระบบ และ หากมีการปนเปื้อนก็สามารถอธิบายได้ว่าปนเปื้อนในส่วนใดบ้าง

2.2 ประเมินการกู้คืนข้อมูลโดยใช้ Hardware

- พิจารณาตามอาการที่แสดงออก อาทิ อะไหล่บางตัวเสีย (หัวอ่าน, จาน Disk, แผง PCB, แผงวงจรพัง)
- พิจารณาตามข้อจำกัด อาทิ เปลี่ยนอุปกรณ์นั้นๆ และต้องให้ตรงรุ่น, อะไหล่บางตัวมีราคาแพง, อะไหล่บางรุ่นอาจเลิกผลิตไปแล้ว, ควรทำในห้อง Clean Room อุปกรณ์บางตัวไม่สามารถเปลี่ยนอะไหล่ได้, ต้องมีองค์ความรู้และความเชี่ยวชาญ เป็นต้น

3. ข้อควรปฏิบัติ และ ข้อควรระวังในการกู้คืนข้อมูล (กฎ 3 ต.)

- ต้องหยุดทำกิจกรรม หรือเพิ่มข้อมูลใดๆ ต่อเมื่อทราบว่าข้อมูลสูญหาย เพื่อเป็นการป้องกันการเขียนทับข้อมูลที่ต้องการจะกู้คืนข้อมูล
- ต้องดำเนินการสำเนา Drive นั้นๆ ก่อนเสมอ แล้วส่งสำเนาไปดำเนินการกู้คืนข้อมูล หากจำเป็นต้องใช้เครื่องต่อ
- ต้องทำใจ เพราะการกู้คืนข้อมูลมีหลายเงื่อนไข บางเงื่อนไขอาจทำให้ไม่สามารถกู้ข้อมูลคืนได้