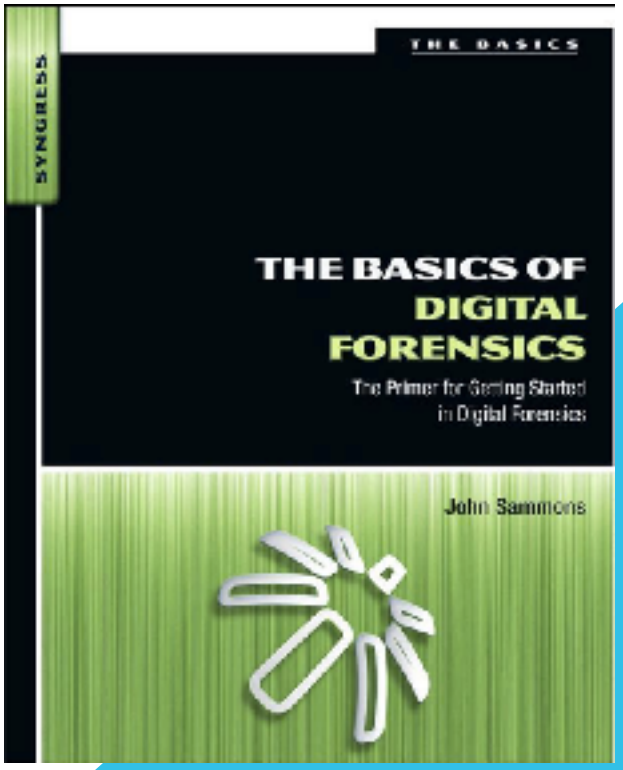

4. COLLECTING EVIDENCE

TOPICS

- Crime scenes (TKP)
- Documenting
- Chain of Custody
- Forensic cloning
- Live dan Dead Systems
- Hashing
- Final Report

CRIME SCENES AND COLLECTING EVIDENCE

PENGAMANAN TKP

- Orang yang tidak berkepentingan di larang mendekat
- Koneksi jaringan beresiko terhadap data
- Yang perlu dipastikan volatile data tidak akan hilang, cabut kabel jaringan
- Isolasi telephone yang disita dari jaringan
  - Image from crimescenecleanupdetroit.com

REMOVABLE MEDIA

- Memory cards bentuknya sangat kecil
- Bisa disembunyikan di buku, dompet, ikat kepala, dll.
- Bisa berupa DVD, hard disk eksternal, flash disk, memory cards
- Periksa buku dan manual untuk membantu menentukan level target
  - Apakah menggunakan enkripsi?

PONSEL

Bukti berharga

- SMS, email, call logs, contacts

Berinteraksi dengan phone bisa merubah data

- Aplikasi Apple "Find My iPhone" bisa digunakan untuk menghapus secara remote ponsel

ISOLASI PONSEL

Matikan ponsel

- Tapi kadang-kadang butuh password saat dinyalakan

Kontainer Pelindung

- Kaleng cat, Faraday bag

Power

- Sediakan baterai eksternal untuk memastikan ponsel tetap menyala
- Sita kabel power jika ponsel dalam keadaan, sehingga bisa di-charged untuk pemeriksaan

PERTANYAAN DI TKP

Setelah TKP diamankan, tanyakan

- Jenis perangkat apa saja yang ada?
- Berapa banyak perangkat?
- Apakah perangkatnya masih beroperasi?
- Tools apa saja dibutuhkan?
- Apakah dibutuhkan tenaga ahli?

URUTAN VOLATILITY

Kumpulkan barang bukti yang paling volatile

- CPU, cache dan register
- Routing table, ARP cache, proses
- RAM
- Temp files/swap space
- Hard disk
- logged data secara remote
- Archival media

DOCUMENTASI TKP

IF YOU DON'T WRITE IT DOWN, IT DIDN'T HAPPEN

JENIS DOKUMENTASI

- Foto
- Catatan tertulis
- Video
- Rekam secara detail
  - Jenis, buatan, model, serial number
  - Apakah perangkatnya menyala atau mati
  - Koneksi jaringan
  - Peripheral yang terkoneksi misalnya printers
  - Dokumentasikan dan beri label pada kabel

FOTO

- Kelilingi TKP untuk mencari perangkat dan apa saja yang dibutuhkan
- Foto keseluruhan TKP sebelum semuanya dirusak
- Ambil dari berbagai posisi, biarkan item barang bukti dalam posisi original Tambahkan mistar pada foto kedua untuk perspektif
- Foto tanpa melepaskan notes

NOTES

- Tidak ada standard
- Umumnya dalam bentuk Kronologis
- Catatan ini akan membantu nantinya di sidang
- Catatan bisa digunakan dan dilihat oleh pihak lain
  - Jangan menuliskan kesimpulan atau spekulasi

CHAIN OF CUSTODY

TANDAI BARANG BUKTI

- Initials, tanggal, nomor kasus
- Gunakan spidol permanent
- Bungkus dengan evidence anti-static bag
- Tamper-resistant evidence tape

FORENSIK KLONING

KLONING

- Kopi utuh hard drive, bit demi bit
- Termasuk di dalamnya unallocated space dan Master File Table
- Proses memakan waktu yang lama
- Biasanya dikerjakan di lab, bukan di TKP
- Pada kasus civil (perdata), bisa saja sulit untuk mendapatkan otoritas resmi untuk membawa komputer
  - Kloning dilakukan di TKP

TUJUAN KLONING

- Pemeriksaan dilakukan pada copy, bukan pada bukti original
  - Kecuali pada kasus darurat, misalnya penculikan anak
- Dengan kloning bisa melakukan recover jika terjadi kesalahan
- Forensik kloning yang sudah diautentikasi dianggap sama dengan yang asli di pengadilan

PROSES KLONING

- Kopi hard drive ke hard drive yang lain yang lebih besar
- Source drive biasanya dilepas dari komputer
- Penting untuk menggunakan write-blocker
  - Hardware atau software
- Pertama-tama lakukan clean secara Forensik untuk destination drive
- Buktikan hal tersebut sudah dilakukan pada case file

MEMBERSIHKAN MEDIA SECARA FORENSIK

- Bisa dibuktikan data benar-benar tidak ada → "Sterile"
- Overwrite keseluruhan drive dengan pola data tertentu
  - Misalnya 00000000

FORMAT IMAGE FORENSIK

Proprietary

- EnCase (.E01) – Biasa digunakan "Expert Witness"
- AccessData Custom Content Image (.AD1)

Open

- Advanced Forensics Format (AFF)
  - Open format, link Ch 4a: AFF - Forensics Wiki
- Raw (.dd atau .001)
  - Disk image langsung tanpa kompress

RESIKO DAN TANTANGAN

- Resiko terbesar: Writing to the evidence drive
- Bad sectors
- Rusak atau drive yang tidak berfungsi
- Corrupt boot sector
- Antiforensik (secara teoris, bukan resiko secara praktis)

EDISCOVERY

- Mengumpulkan dan menyajikan electronically stored information (ESI) untuk legal cases
- Dengan Kloning bisa menyajikan barang bukti secara baik
  - Bisa sangat mahal dan kurang bermanfaat
- du Pont v. Kolon
  - Kolon kalah dan didenda
  - $920 million judgement
  - 20 tahun larangan bersaing dengan du Pont
  - Links
    Ch 4b: DuPont v. Kolon: A Lesson In How To Avoid Sanctions For Spoliation Of Evidence
  - Ch 4c: DuPont v. Kolon: Judge Payne Issues Breathtaking 20-Year Worldwide Injunction barring Kolon from Making Body Armor Fiber for Theft of DuPont's

PERAMPASAN

Posted on September 6, 2011 by **Suzanne Herrmann Brock**

DuPont v. Kolon: A Lesson In How To Avoid Sanctions For Spoliation Of Evidence

Two recent decisions in the same case illustrate that, when it comes to imposing sanctions for spoliation of evidence, what matters is not simply whether you've intentionally deleted relevant evidence, but how you go about deleting it, and what the record reflects about your intentions. Although both the plaintiff and the defendant in E.I. du Pont De Nemours and Co. v. Kolon Industries, Inc., Civil Action No. 3:09cv58, demonstrated that the other intentionally destroyed relevant evidence, as is detailed below, the Court sanctioned only defendant Kolon Industries, Inc. ("Kolon") based on its manifest bad faith (read the decision here). As is discussed in an earlier post on Gibbons' E-Discovery Law Alert (which you can read here), plaintiff E.I. du Pont de Nemours and Company ("DuPont") escaped a similar fate based on its demonstrable good faith. In short, this case teaches that the intentional deletion of relevant evidence does not per se lead to sanctions. Rather, the parties' conduct — or misconduct, as the case may be — must be judged contextually.

Dupont filed a Complaint against Kolon on February 3, 2009, alleging trade secret misappropriation, theft of confidential business information, and conspiracy based on Kolon's efforts to recruit former DuPont employees and otherwise unlawfully obtain DuPont's proprietary information. When Kolon produced in discovery screenshots of key employees' computers taken after they had notice of the Complaint that appeared to show that they marked emails with instructions such as "Delete," "Need to Delete," "Remove All" and "Get Rid Of," DuPont moved for sanctions for spoliation of evidence.