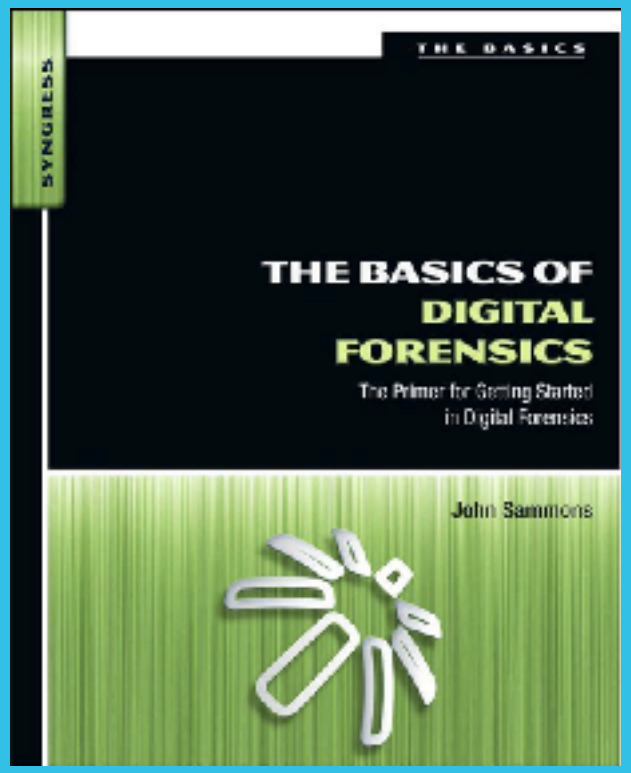
4. COLLECTING EVIDENCE PART 2



TOPIK

- Live and Dead Systems
- Hashing
- Final Report

LIVE AND DEAD SYSTEMS

AJARAN LAMA: CABUT KABEL

- Menghilangkan data RAM
- Dapat membuat file terenkripsi tidak tersedia
- Bisa mengakibatkan data corrupt di disk saat power goes off
- Bisa menghilangkan evidence yang tidak seluruhnya tersimpan di disk

SAAT INI: LIVE ACQUISITION

- Modern tools banyak di pasaran untuk tindakan awal
  - Orang Non-teknis
- Live acquisition penting jika data di RAM dibutuhkan
  - Malware -> RAM dibutuhkan
  - Kepemilikan pornografi anak -> RAM tidak dibutuhkan
- Pemeriksa perlu memiliki skills dan tools

PRINSIP LIVE COLLECTION

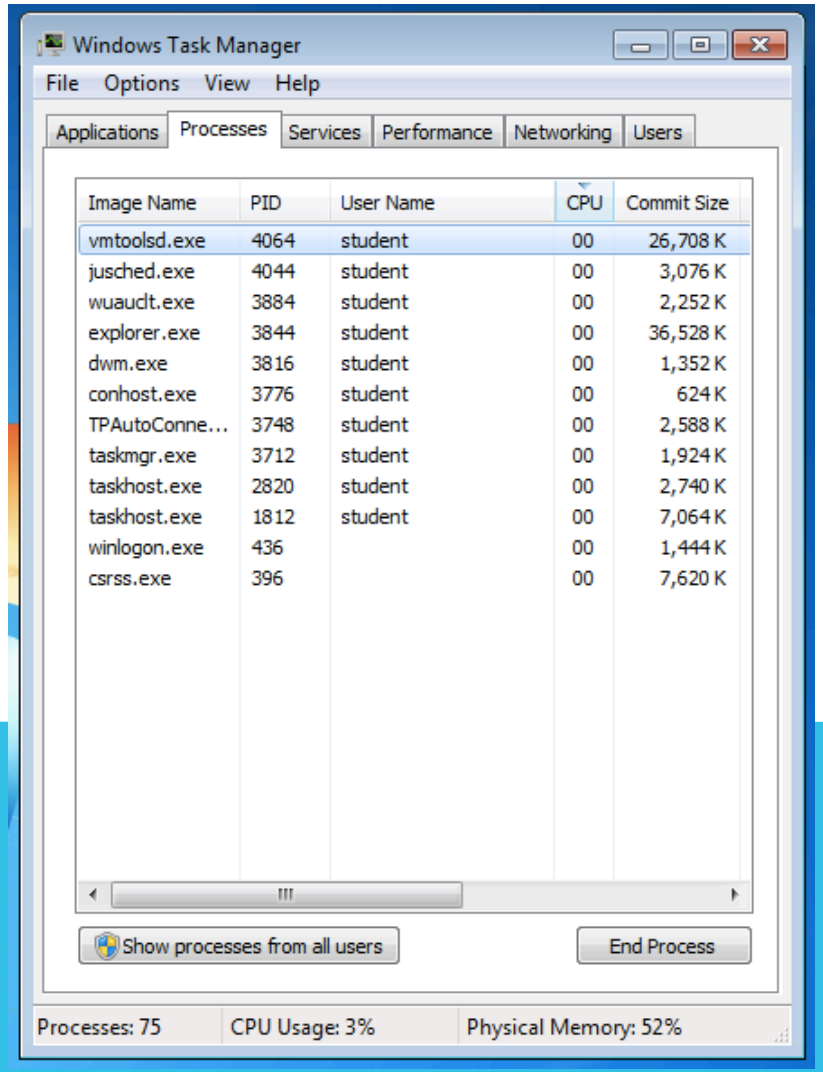
- Minimalkan Prosedur invasif sebisa mungkin
- RAM bisa berisi
  - Running processes (proses yang berjalan)
  - Executed console commands (perintah yang dijalankan di console)
  - Passwords dalam bentuk cleartext
  - Unencrypted data
  - Instant messages
  - IP Addresses
  - Trojans

MELAKUKAN DAN MENDOKUMENTASIKAN LIVE COLLECTION

- Bekerja tanpa interupsi
- Setiap interaksi dengan komputer harus dicatat
- Saya melakukan ini... komputer melakukan
- Buat desktop terlihat dengan menggerakkan mouse
  - Atau tekan key (dan lakukan record)
- Catat tanggal dan jam
- Catat icons dan tombol taskbar program berjalan
- Buka Task Manager & record processes
- Capture RAM dengan forensic RAM imager
- Melakukan shutdown yang tepat

TASK MANAGER

- Perlihatkan proses dari semua users
- Catat semua proses
- Pelakunya mungkin akan mengklaim malware yang telah melakukannya



ALGORITMA HASHING

- Walaupun hanya satu bit yang berubah pada file input akan merubah hash secara keseluruhan
- Jika nilai hash dari dua file sesuai, maka files bisa dikatakan sebagai indentik
- MD5 lebih umum
- SHA-1 lebih baik
- Dalam implementasi, keduanya digunakan
- Nilai Hash harus disertakan pada semua images barang bukti
  - Sehingga kopi image bisa diverifikasi

LAPORAN AKHIR

- Pertimbangkan audience
- Banyak reports yang terlampau teknis dan membingungkan
- Hindari jargon dan code
- Laporan yang di generate dengan menggunakan FTK atau EnCase termasuk di dalamnya, tapi agak sulit dimengerti jika digenerate otomatis
- Tambahkan narasi detail yang dilakukan oleh pemeriksa
- Tambahkan summary yang ditulis dalam plain English