

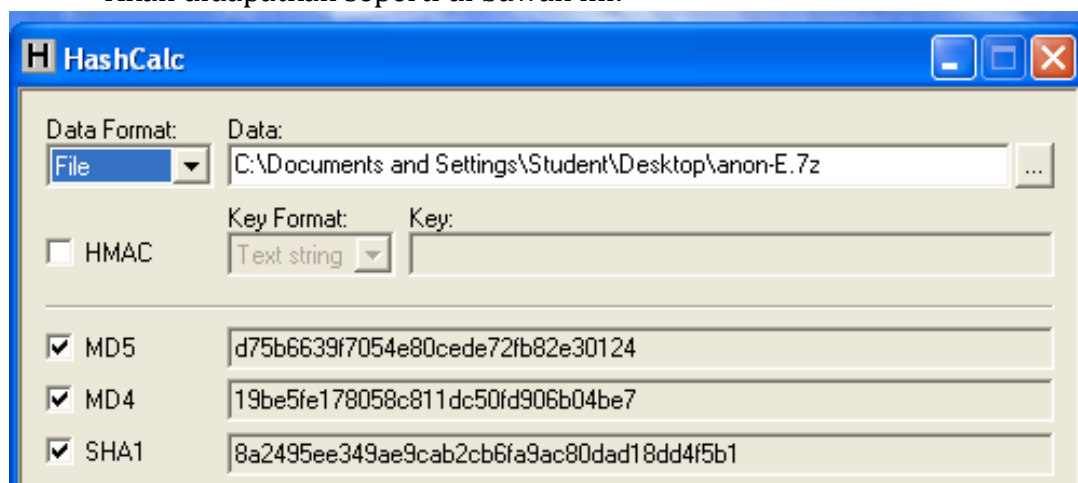
Project 20: Mencari Lebih Banyak Bukti di Kasus Anon (25 poin)

Kebutuhan Project

- Komputer Windows, dengan FTK yang sudah diinstal sebelumnya. Bisa real atau virtual. Di contoh ini menggunakan komputer Windows XP virtual machine.

Download File Evidence

1. Download the file below: anon-E.7z yang tersedia di elearning.
2. Gunakan Hashcalc untuk menghitung nilai hash file yang di download. Akan didapatkan seperti di bawah ini:



3. Unzip file dengan 7-Zip.

Tugas

4. Tugas saudara memeriksa kembali barang bukti untuk menemukan dan item bukti. Masing-masing bukti, cari dan screen capture gambar untuk membuktikannya.
5. Tulis dalam file word jawaban masing-masing item beserta gambar FULL-DESKTOP untuk membuktikannya.
6. Di sini tidak ada instruksi step-by-step, tapi sebelumnya kita telah mempelajari semua prosedur yang dibutuhkan pada project dan pelajaran sebelumnya.

Barang Bukti yang dicari (Masing-masing 5 point)

- a. Tentukan CurrentControlSet value
- b. Berapa banyak user accounts yang menggunakan sistem? Tulis semuanya.
- c. Siapa nama user yang terakhir logged-on?

- d. USB devices apa saja yang pernah terhubung ke komputer? Tulis semua, dengan “nama umum” dari USB tersebut, dan sertakan image(s) untuk membuktikannya.
- e. Berapa banyak URLs yang diketikan user di browser Internet Explorer baru-baru ini? Sertakan gambar daftar nya.

Simpan File

1. Simpan file dengan nama NamaKamu_Project20.doc, dengan format doc atau pdf.
2. Kirim melalui elearning.