PRAKTIKUM 1: PRA INVESTIGASI FORENSIKA DIGITAL

Pertemuan ke : 1

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-04	Mampu berpikir logis, kritis, sistematis dan inovatif, dan mampu mengambil keputusan secara tepat dibidang keahliannya
CPMK-01	Deskripsi dari CPMK tsb…

1.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan pra investigasi forensik digital evidence dengan tools windows
2. Mampu menganalisis sebelum dan sesudah menggunakan aplikasi writeblokers

1.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-04	CPMK-01	Mahasiswa memahami tahapan investigasi digital forensik

1.3. TEORI PENDUKUNG

Write Blockers adalah perangkat yang memungkinkan perolehan informasi pada drive tanpa membuat kemungkinan merusak konten drive secara tidak sengaja. Investigator melakukan ini dengan mengizinkan aplikasi investigator untuk lewat tetapi dengan memblokir commands pada sistem operasi yang digunakan oleh investigator.

Ada dua cara untuk membangun Write Blockers : pemblokir dapat memungkinkan semua perintah untuk lulus dari komputer ke drive kecuali untuk mereka yang ada di daftar tertentu. Atau, pemblokir dapat secara khusus memblokir perintah tulis dan membiarkan semuanya lewat.

Write Blockers juga dapat mencakup perlindungan drive yang akan membatasi kecepatan drive yang terpasang pada blocker. Drive yang berjalan pada kecepatan tinggi bekerja lebih keras. Perlindungan tambahan ini memungkinkan drive yang tidak dapat dibaca pada kecepatan tinggi (mode UDMA) untuk dibaca pada mode lebih lambat (PIO).

Gambar 1.1 Tableau Tools

Ada dua jenis blocker tulis, Asli dan Tailgate. Perangkat asli menggunakan antarmuka yang sama untuk masuk dan keluar, misalnya blok tulis IDE ke IDE. Perangkat Tailgate menggunakan satu antarmuka untuk satu sisi dan yang lain untuk yang lain, misalnya blok tulis Firewire ke SATA.

1.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. FTK Imager App.
3. Writeblocker
4. Flashdisk (Partisi Hardisk)

1.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

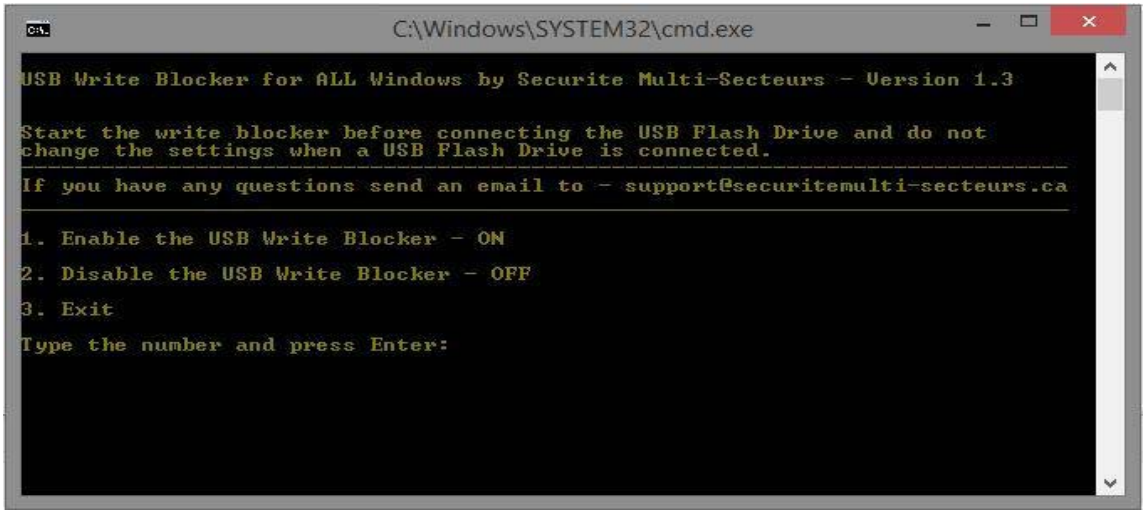
No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Apa alasan perlunya dilakukan tools pendukung seperti writeblock dan sejenisnya?	50
2.	CPL-04	CPMK-01	Bagaimana jika seorang investigator melakukan investigasi digital evidence tanpa menjalankan aplikasi writeblock terlebih dahulu?	50

1.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-04	CPMK-01	Selesaikan langkah praktikum berikut ini !	Screen Shot Hasil praktikum	100

Download dan Jalankan Aplikasi Writeblokers windows pada link tersedia :

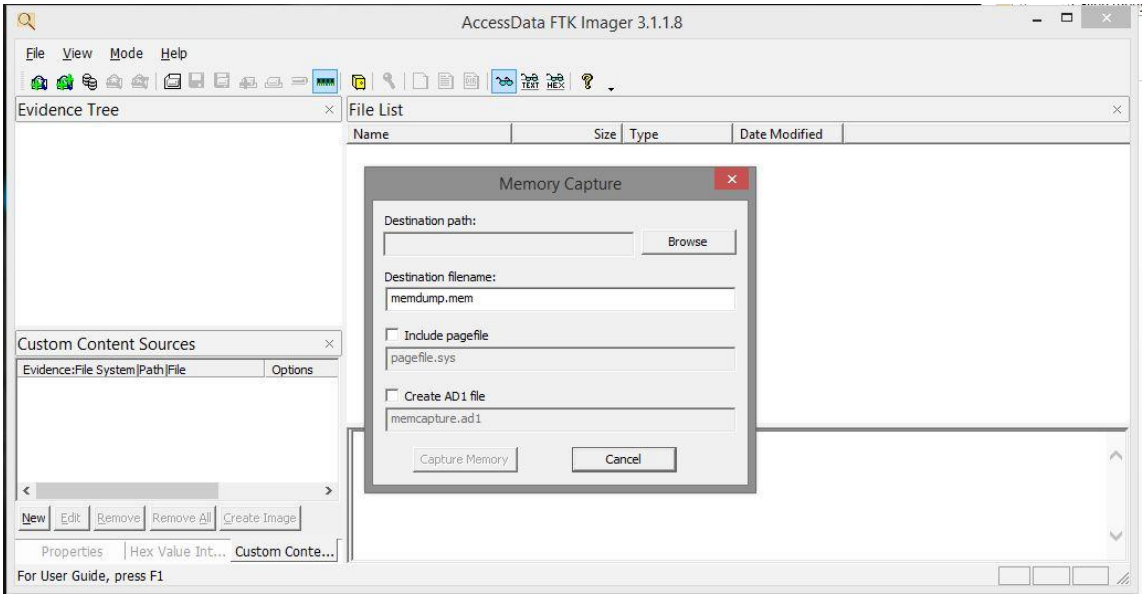


Gambar 1.2 Aplikasi Writeblokers.

Pilih Enable, maka aplikasi writebloker sudah berjalan pada komputer investigator, sehingga proses imaging tahap selanjutnya dapat dilakukan

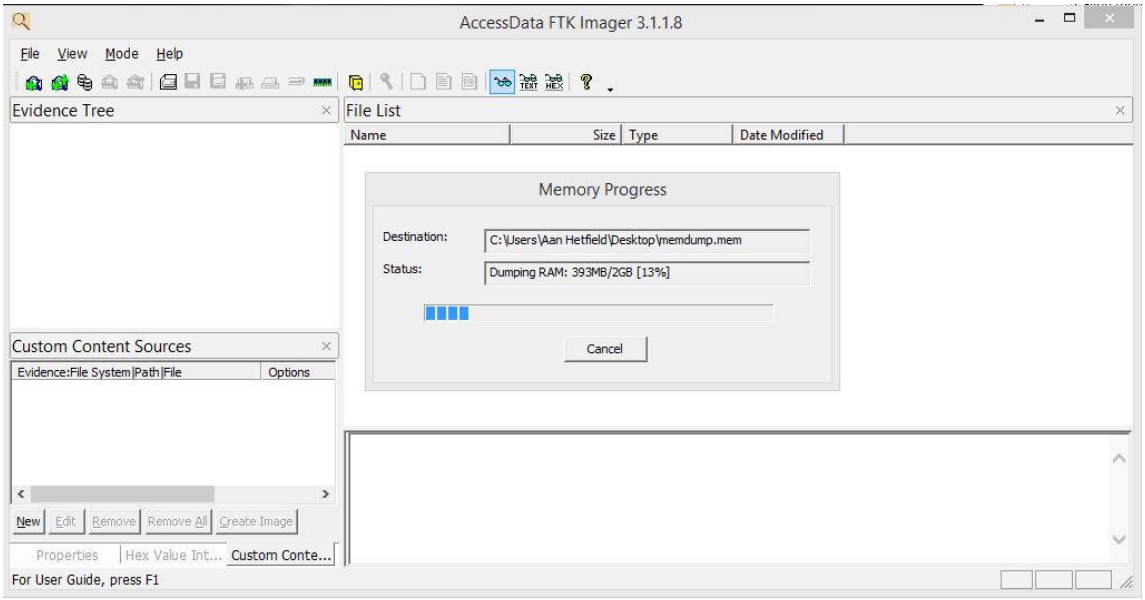
Buka Aplikasi FTK Imager untuk melakukan Imaging memori anda :

Menu File/Capture Momory



Gambar 1.3 Aplikasi FTK Imager.

Pilih destinasi file kemudian klik Capture Memory. Ceklist “pagefile.sys” yang merupakan file sistem Windows yang bertindak sebagai file swap untuk memori dapat berisi informasi memori yang sebagai bukti digital. Create AD1 file : Membuat file AD1 memungkinkan untuk membuat sebuah AD1 images dari isi memori



Gambar 1.4 Capture Memory.

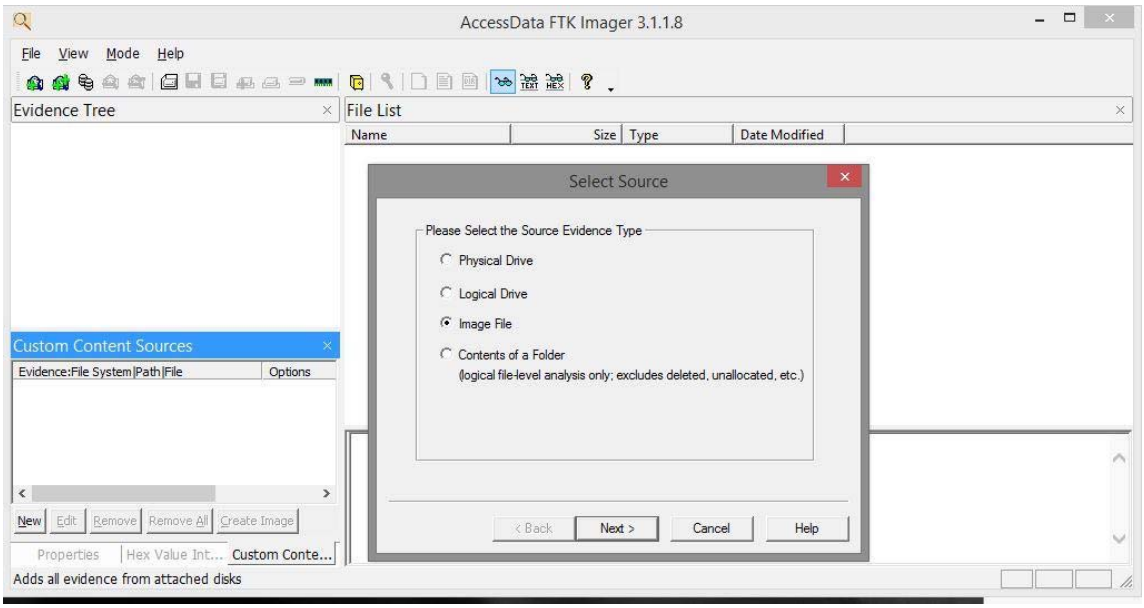
Tunggu sampai selesai proses capturing memory

Untuk membuka hasil capture memory dengan memilih menu

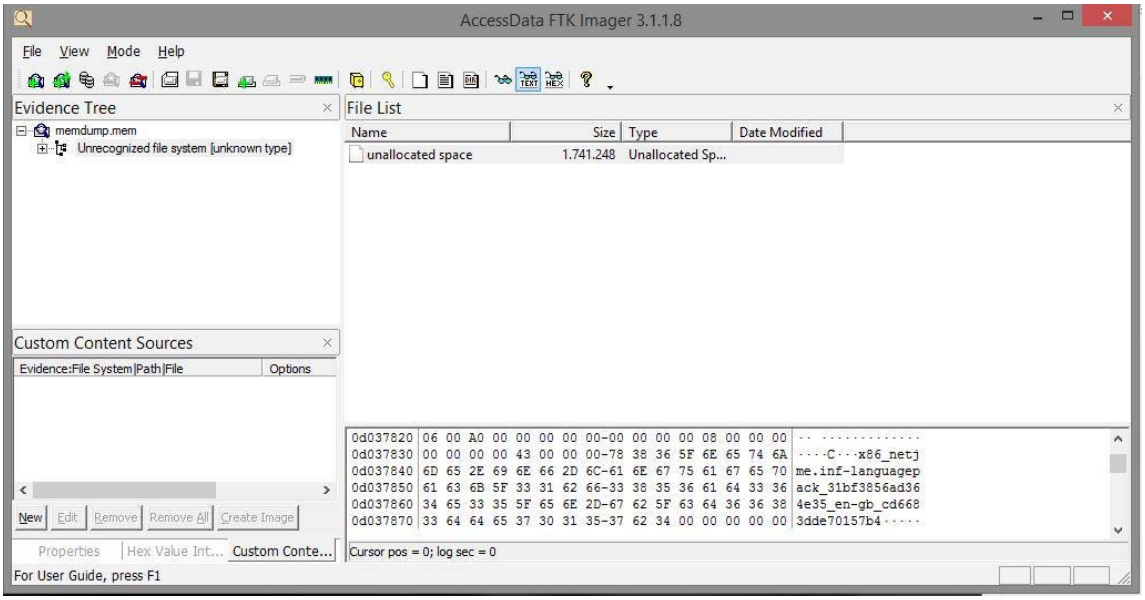
File/Add evidence itemGambar 5

Pilih Image File/Next

Cari file hasil capture memory ".mem"



Gambar 1.5 Add evidence.



Gambar 1.6 Hasil Capture Memory.

1.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Buat analisis hasil capture dumb masing masing memori, informasi apa saja yang ditemukan?	100

Lakukan proses capture momori anda dengan atau tanpa menjalankan aplikasi writeblokers, selanjutnya lakukan analisis perbedaannya (pastikan saat menjalankan writebloker restart komputer terlebih dahulu)

1.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-04	CPMK-01	20%		
2.	Praktik	CPL-04	CPMK-01	30%		
3.	Post-Test	CPL-04	CPMK-01	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**