PRAKTIKUM 7: EMAIL FORENSICS "TOOLS NETWORKMINER"

Pertemuan ke : 7

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-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu menganalisa digital evidence dan pengolahan bukti digital

7.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)

1. Praktikan mampu mengidentifikasi mail forensics
2. Praktikan mampu mengektraksi digital evidence dari email yang saling berinteraksi

7.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Kemampuan mahasiswa dalam Capture network masing-masing praktikan menggunakan networkminer dan Menentukan, mengklasifikasi jenis-jenis digital evidence email forensics

7.3. TEORI PENDUKUNG

Dengan email kita dapat berkomunikasi dengan orang manapun dan berada di belahan dunia manapun juga. Semakin maraknya orang mempublish email mereka , banyak juga saingan atau orang yang iri dengan cara melakukan tindakan pengrusakan email.

Dari sudut pandang forensik, e-mail dengan sistem client/server memudahkan dalam menemukan informasi (untuk kepentingan analisis) karena semua pesan di-download, dan disimpan dalam komputer lokal. Dengan mendapatkan akses ke komputer lokal, maka analisis terhadap e-mail akan jauh lebih mudah. Dua bagian e-mail yang dijadikan sumber pengamatan adalah header dan body. Yang paling umum dilihat dari sebuah header adalah From (nama dan alamat pengirim yang mudah untuk dipalsukan), To (tujuan yang juga dengan mudah disamarkan), Subject and Date (terekam dari komputer pengirim, namun menjadi tidak akurat jika tanggal dan jam pada komputer pengirim diubah). Untuk mendapatkan informasi yang lebih detail, header pada e-mail perlu diekstrak. Dari header tersebut bisa didapatkan informasi IP Lokal dari pengirim, ID unik yang diberikan oleh server e-mail, dan alamat server pengirim.

Umumnya, software e-mail client/server (seperti Ms.Outlook, Eudora, atau ThunderBird) telah menyediakan fasilitas untuk melihat header secara lengkap, namun

beberapa software forensik mampu membaca dan mengekstraksi header untuk keperluan analisis lebih lanjut seperti EnCase atau FTK. Dengan software forensik ini, analisis untuk melakukan pencarian, ekstrak header, pencetakan ke printer, dan pengelompokkan e-mail menjadi lebih mudah dilakukan.

Lalu, bagaimana dengan investigasi untuk web-based e-mail, seperti Yahoo! atau Gmail? E-mail yang pernah terbaca melalui web browser, tentunya tidak disimpan di komputer lokal seperti halnya e-mail dengan sistem client/server. Ketika e-mail dibaca pada sebah komputer, sistem operasi meng-cache isi website tersebut pada harddisk. Cara terbaik untuk melacak setiap e-mail yang pernah terbaca adalah melalui area temporary file seperti file swap atau file cache, atau jika temporary file telah terhapus, pelacakan dapat difokuskan pada area tempat lokasi file temporary sebelum dihapus.

Ektraksi untuk melakukan ini akan membutuhkan lebih banyak usaha dibandingkan ekstraksi dengan sistem client/server, karena penelusuran difokuskan untuk mencari file HTML di antara kumpulan ratusan atau mungkin ribuan halaman-halaman HTML. Software forensik seperti FTK atau EnCase dapat berguna untuk mempercepat pencarian. Misalkan mencari suatu pesan yang mengandung fadh325@situsku.com, maka teks tersebut dapat dimasukkan sebagai dasar pencarian pada sebuah software forensik, dan diatur agar pencarian dilakukan hanya untuk file HTML. Software forensik akan menjelajah isi harddisk, dan berusaha menemukan file (atau potongan file) dengan kriteria yang telah disediakan.

Macam-macam kejahatan pada E-mail:

- **E-mail spoofing,** adalah istilah yang digunakan untuk menjelaskan aktivitas e-mail (biasanya penipuan) di mana alamat pengirim dan bagian-bagian lain dari e-mail header yang diubah untuk muncul seolah-olah e-mail yang berasal dari sumber yang berbeda. E-mail spoofing adalah teknik yang biasa digunakan untuk e-mail spam dan phishing untuk menyembunyikan asal usul e-mail. Dengan mengubah sifat-sifat tertentu dari e-mail, seperti Dari, Return-Path dan Balas-Untuk bidang (yang dapat ditemukan dalam header pesan), pengguna yang bermaksud buruk dapat membuat e-mail yang tampak dari orang lain dari pengirim yang sebenarnya. Hasilnya adalah bahwa, meskipun e-mail yang tampaknya berasal dari alamat yang tercantum di bidang “Dari” (ditemukan dalam e-mail), itu sebenarnya berasal dari sumber lain.
- **Sniffing,** Definisi singkatnya adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer. Contohnya begini, Anda adalah pemakai komputer yang terhubung dengan suatu jaringan dikantor. Saat Anda mengirimkan email ke teman Anda yang berada diluar kota maka email tersebut akan dikirimkan dari komputer Anda trus melewati jaringan komputer kantor Anda (mungkin melewati server atau gateway internet), trus keluar dari kantor melalui jaringan internet, lalu sampe di inbox email teman Anda. Pada saat email tersebut melalui jaringan komputer kantor Anda itulah aktifitas SNIFFING bisa dilakukan. Oleh siapa ? Bisa oleh administrtor jaringan yang mengendalikan server atau oleh pemakai komputer lain yang terhubung pada jaringan komputer kantor Anda, bisa jadi teman sebelah Anda. Dengan aktifitas SNIFFING ini email Anda bisa di tangkap / dicapture sehingga isinya bisa dibaca oleh orang yang melakukan SNIFFING tadi. Sangat berbahaya bukan ?
- **SPAM**, adalah sebutan untuk kiriman email yang tidak dikehendaki penerimanya. Biasanya pengirim mendapatkan alamat email penerima dengan cara yang tidak wajar. Aktifitas spamming merugikan penerima karena menyebabkan Inbox cepat penuh (over quota), sehingga email lain yang mestinya masuk tidak bisa masuk

7.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer
2. Network Miner

7.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Apa perbedaan tools investigasi Wireshark dengan Networkminer?	50
2.	CPL-06	CPMK-03	Tools live forensics seperti network miner, wireshark dll Apakah dapat disebut sebagai penyadapan? Jelaskan menurun pendapat anda!,	50

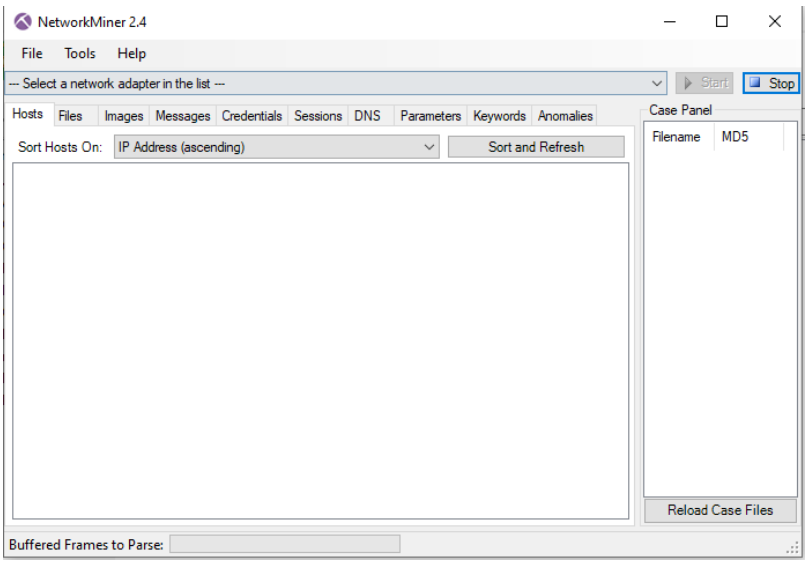
7.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut!	Screen shot Hasil praktikum	100

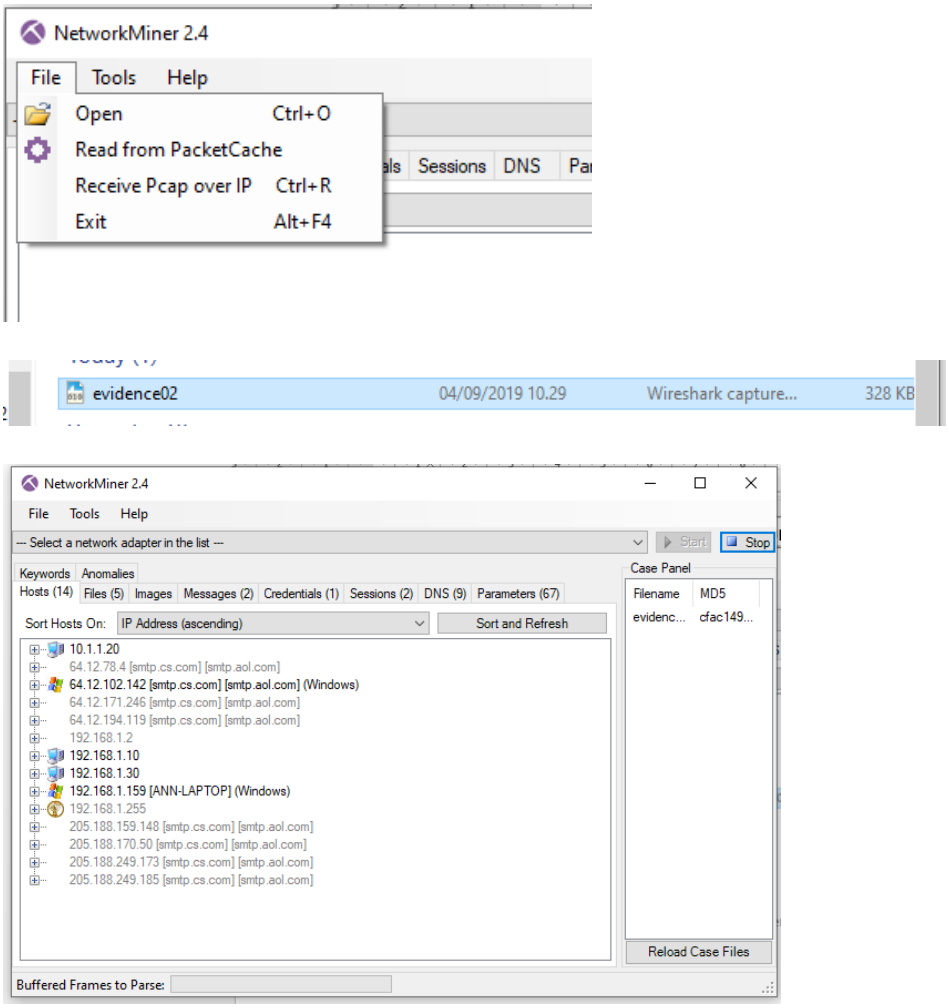
Langkah praktikum berisi tahapan secara rinci bagaimana praktikum dijalankan dan apa hasil yang harus dicapai dari setiap langkah.

1. Download aplikasi networkminer dan digital evidence
2. Buka aplikasi networkminer



Gambar 7.1 Interface Network Miner

3. Buka file yang didownload tadi (evidence02.pcap)



Gambar 7.2 Explore Network Miner

7.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Gunakan pertanyaan 5w + 1H untuk menjawab dari 8 daftar pertanyaan yang harus kita pecahkan. Keutamaan pertanyaan tersebut yaitu: 1. Apa alamat email Ann? 2. Apa kata sandi email Ann? 3. Apa alamat email kekasih rahasia Ann? 4. Dua item apa yang Ann beri tahu untuk dibawa oleh kekasih rahasianya? 5. Apa NAMA dari lampiran yang dikirimkan Ann kepada kekasih rahasianya? 6. Berapa MD5sum dari lampiran yang dikirimkan Ann kepada kekasih rahasianya? 7. Di CITY dan COUNTRY apa titik pertemuan mereka? 8. Apa MD5sum gambar yang tertanam dalam dokumen?	100

7.8. 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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 8: DATA CARVING

Pertemuan ke : 8

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-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu menganalisa digital evidence dan pengolahan bukti digital

8.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan;
1. Praktikan mampu mengekplorasi barang bukti digital dengan metode data carving
2. Praktikan dapat membuat skenario kasus dan mempraktekkannya

8.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa dalam menerapkan tools forensics Foremost (Linix/Windows) dan Ekplorasi digital evidence masing-masing flashdisk (storage)

8.3. TEORI PENDUKUNG

File Carving atau kadang hanya disebut dengan Carving, adalah praktek mencari masukan untuk file atau jenis lain dari objek berdasarkan pada isi, bukan pada metadata. File carving adalah alat yang ampuh untuk memulihkan file dan fragmen dari file saat entri direktori yang korup atau hilang, yang mungkin terjadi dengan file lama yang telah dihapus atau ketika melakukan analisis pada media yang rusak. Memory carving adalah alat yang berguna untuk menganalisis dump memori fisik dan virtual ketika struktur memori tidak diketahui atau telah ditimpa.

File Carvers paling banyak beroperasi dengan mencari header file dan / atau footer, dan kemudian "carving out" blok antara dua batas. Sematic carving melakukan carving berdasarkan analisa dari isi dari file yang diusulkan. File carving harus dilakukan pada sebuah disk image, bukan pada disk asli. Banyak program carving yang memiliki pilihan untuk hanya melihat dengan dekat batas-batas sektor mana header ditemukan. Namun, mencari masukan seluruh dapat menemukan file yang telah tertanam ke file lain, seperti JPEG yang tertanam ke dalam dokumen Microsoft Word. Hal ini dapat dianggap sebagai keuntungan atau kerugian, tergantung pada keadaan. Mayoritas program file carving hanya akan memulihkan file yang bersebelahan pada media (dalam file kata lain yang tidak terfragmentasi).

Fragmented File Recovery : Simson Garfinkel memperkirakan bahwa 58% upto pandangan, 17% dari JPEG dan 16% dari MS-Word file terfragmentasi dan, karenanya, muncul rusak atau hilang ke

pengguna menggunakan data tradisional ukiran. Set pertama dari file program ukiran yang dapat menangani file terfragmentasi secara otomatis memiliki akhirnya tiba. A. Pal, N. Memon. T. Sencar dan K. Shanmugasundaram telah memperkenalkan teknik yang disebut SmartCarving yang dapat memulihkan file terfragmentasi.

SmartCarving : Pal mengembangkan skema ukiran yang tidak terbatas pada file bifragmented. Teknik, yang dikenal sebagai SmartCarving, memanfaatkan heuristik mengenai perilaku fragmentasi filesystem yang dikenal. Algoritma ini memiliki tiga fase: preprocessing, pemeriksaan, dan reassembly. Pada tahap preprocessing, blok didekompresi dan / atau didekripsi jika diperlukan. Pada tahap pemeriksaan, blok diurutkan menurut tipe file mereka. Pada tahap reassembly, blok ditempatkan di urutan ke mereproduksi file yang dihapus. Algoritma SmartCarving adalah dasar untuk Forensik Foto gesit dan aplikasi Foto Pemulihan gesit dari Majelis Digital.

File Carving Taxonomy : Simson Garfinkel dan Joachim Metz telah mengusulkan taksonomi file carving sebagai berikut : Carving, Umum istilah untuk penggalian data (file) dari blok dibedakan (data mentah), seperti "carving" patung dari batu sabun.

Blok Berbasis Carving, Setiap metode carving (algoritma) yang menganalisis input di blok-per-blok dasar untuk menentukan apakah blok merupakan bagian dari file output yang mungkin. Metode ini mengasumsikan bahwa setiap blok hanya dapat menjadi bagian dari file tunggal (atau file tertanam).

Statistik Carving, Setiap metode carving (algoritma) yang menganalisis input pada karakteristik atau statistik misalnya, entropi untuk menentukan apakah input adalah bagian dari sebuah file output yang mungkin. Header / Footer Carving, Sebuah metode untuk carving file dari data mentah menggunakan sebuah header yang berbeda (mulai dari penanda file) dan footer (akhir penanda file).

Header / Maksimum (file) ukuran Carving, Sebuah metode untuk file carving dari data mentah menggunakan sebuah header yang berbeda (mulai dari penanda file) dan maksimum (file) ukuran. Pendekatan ini bekerja karena banyak format file (misalnya JPEG, MP3) tidak peduli jika sampah tambahan ditambahkan ke akhir file yang valid. Header / Carving Panjang Tertanam, Sebuah metode untuk file carving dari data mentah menggunakan sebuah header yang berbeda dan panjang file (ukuran) yang tertanam dalam format file

Struktur file berdasarkan Carving, Sebuah metode untuk file carving dari data mentah dengan menggunakan tingkat tertentu dari pengetahuan tentang struktur internal jenis file. Garfinkel yang disebut pendekatan " Semantic Carving" dalam penyerahan DFRWS2006 tantangan carving, sementara Metz dan Mora disebut pendekatan "Deep Carving."

Semantic Carving, Sebuah metode untuk file carving berdasarkan pada analisis linguistik isi file. Sebagai contoh, seorang semantic carver mungkin menyimpulkan bahwa enam blok dari perancis di tengah sebuah file HTML yang panjang ditulis dalam bahasa Inggris adalah fragmen kiri dari sebuah file dialokasikan sebelumnya, dan bukan dari file HTML berbahasa Inggris.

Carving dengan Validasi, Sebuah metode untuk file carving dari data mentah dimana file diukir divalidasi menggunakan jenis file validator tertentu.

Fragmen Pemulihan Carving, Sebuah metode carving di mana dua atau lebih fragmen dipasang kembali untuk membentuk file asli atau objek. Garfinkel sebelumnya disebut pendekatan "Split Carving."

Repackaging Carving, Sebuah metode carving yang mengubah data diekstraksi dengan menambahkan header baru, footer, atau informasi lainnya sehingga dapat dilihat dengan utilitas standar. Sebagai contoh, Garfinkel yang ZIP Carver mencari komponen individu dari sebuah file ZIP dan repackages mereka dengan Direktori Tengah baru sehingga mereka dapat dibuka dengan unzip utilitas standar.

8.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Foremost (Windows & Linux)

8.5. PRE-TEST

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

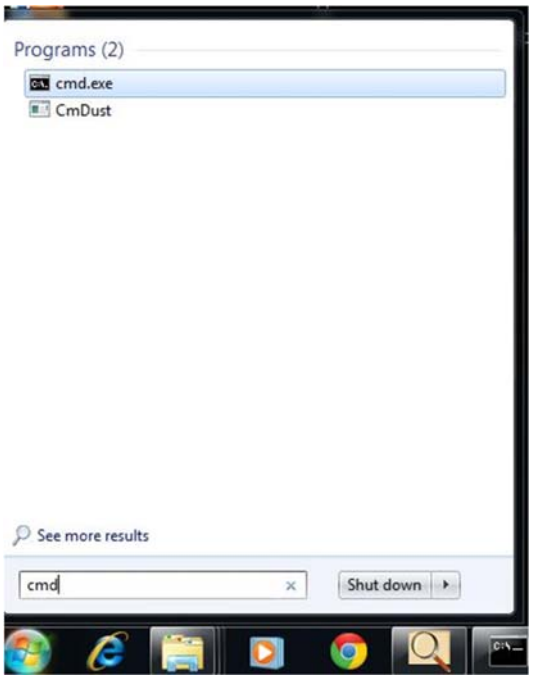
No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Apa yang dimaksud dengan File Carving?	50
2.	CPL-07	CPMK-03	Bolehkan seorang investigator melakukan File Recovery saat melakukan Data Carving, Jelaskan!	50

8.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

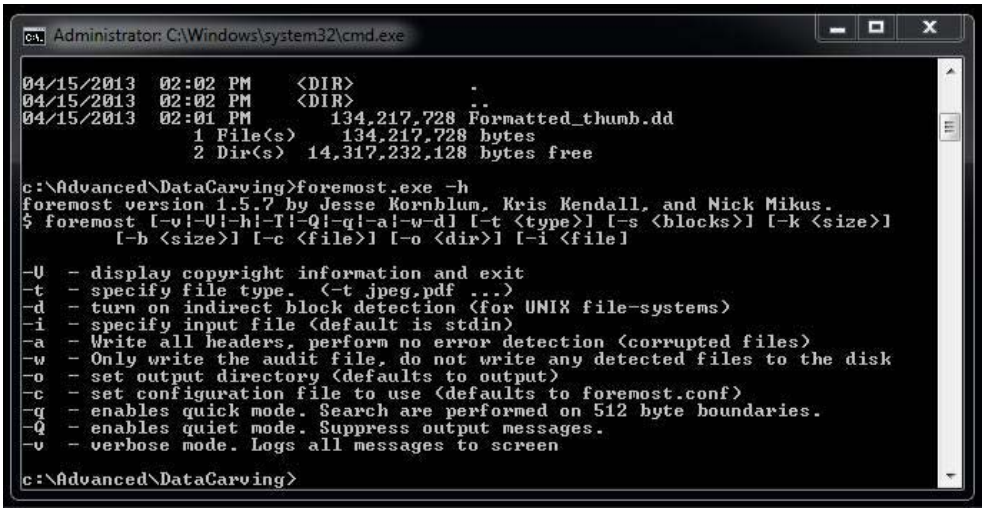
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum berikut!	Screen shot Hasil praktikum	100

1. Buka command prompt.
   a. Go to start menu. (Windows Icon bottom left)
   b. Ketik **cmd** dan enter.



Gambar 8.1 Open CMD.

2. Arahkan ke folder tempat Image yang akan kita gunakan
   a. Pada command prompt data carving folder by **cd c:\Advanced\DataCarving**.



Gambar 8.2 Open CMD Help

3. Gunakan foremost untuk mengekstak information dari image file.
   a. Untuk bantuan command ketik **foremost.exe –h**
   b. Cek PDF File **foremost.exe –t pdf –T –i Formatted_thumb.dd.**
      Eksekusi **foremost.exe**

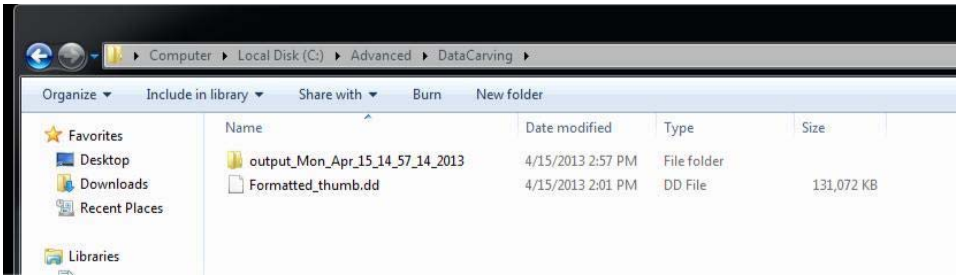
      File carving dengan perintah **–t** command.

      foremost.exe –T –i

      Formatted_thumb.dd.

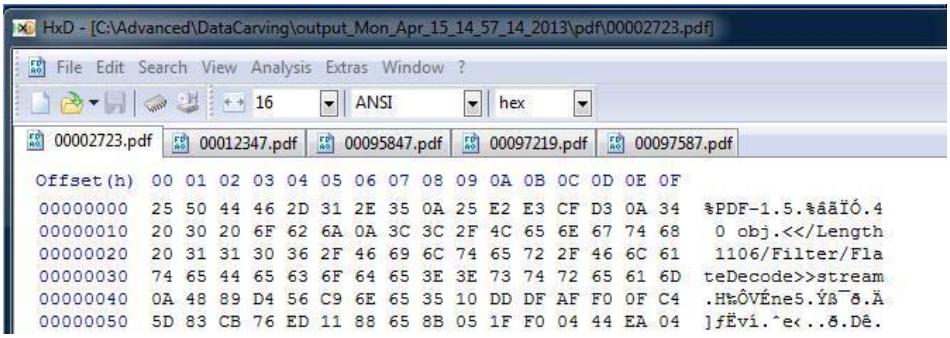
   c. Tunggu proses berjalan, tergantung besaran data yang akan dilakukan carving.

4. Arahkan ke folder data carving pada jendela windows dan perintah **–T** untuk menampilkan tanggal.



Gambar 8.3 Foremost Directory Carvimg

5. Ke dalam folder output dan kita akan melihat folder untuk setiap file yang kita cari. Dalam contoh ini disebut pdf. Cari di folder dan lihat pdf yang ditemukan
6. Buka HxD (the hex editor we use) untuk membuka file pdfs.
   Dengan melihat beberapa byte pertama kita dapat melihat header untuk file pdf. Ingat dari file konfigurasi yang terutama mencari tanda tangan byte yang memberi kita ascii **%PDF**.



Gambar 8.4 Foremost ASCII

8.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Lakukan hal yang sama dengan 3 tipe file yang berbeda selanjutnya buat analisisi file signature data carving!	100

8.8. 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-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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