PRAKTIKUM 9: FILE SIGNATURE

Pertemuan ke : 9

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

9.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan:
1. Praktikan mampu mengekplorasi barang bukti digital dengan mengidentifikasi file signature
2. Praktikan dapat membuat menganalisis perubahan file berdasarkan header file signature

9.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa dalam menerapkan Penggunaan tools winhex (Linux/Windows) dalam Ekplorasi file signature masing-masing praktikan

9.3. TEORI PENDUKUNG

File Signature adalah sebuah data yang berfungsi sebagai indentifikas atau memverifikasi suatu isi file. Dalam hal ini File Signature membantu dalam upaya mendeteksi manipulasi data. File-file sistem komputer diidentifikasi oleh 2 atribut: file extensions dan file signature. Suatu file extension adalah akhiran berupa nama pada file komputer yang teraplikasikan yang menunjukkan format dari file tersebut. sedangkan suatu file signature (dapat juga dikatan sebagai magic number) adalah satu set dari beberapa karakter yang tersimpan pada bagian awal dari file. Setiap jenis file / file type dapat dikenal dengan mudah melalui extension. Contohnya macam ‘exData01.jpg’, ‘exData.png’ atau ‘Surat.doc’. ‘.jpg’, ‘.png’ ‘.doc’ adalah extension file tersebut. Berbeda dengan extension ‘.txt’, file-file tersebut tidak dapat dilihat dengan kasat mata without decoding. Content file tersebut disimpan dan dibaca oleh computer dalam bentuk ‘Hex’ atau ‘Hexadecimal’. Computer akan membuka file dan membaca header atau permulaan file tersebut. Header ini dipanggil ‘File Signature’ atau ‘Magic Number’. Dia akan men-check file signature. File signature ini biasanya mengandungi format file, compression, file structure dan lain-lain. File yang dapat dilihat nilai Hex adalah ‘File Signature’ atau ‘Magic Number’.

Jika salah satu Staff mengganti format misal format file “Laporan.pdf” di ubah menjadi “Lukis.jpg” untuk menyembunyikan file tersebut. Dengan menggunakan tools maka magic number file ini akan terbaca :

jpg = FF D8 FF E0 ?? ?? 4A 46 49 46 00 (dan seterusnya adalah data image, compression, etc.)

png = 89 50 4E 47 0D 0A 1A 0A (dan seterusnya adalah data image, etc.)

ico = 00 00 01 00 (file icon, dan seterusnya adalah data image, etc.)

pdf = 25 50 44 46 (dan seterusnya adalah content pdf, etc.)

karene file “Lukis.jpg” adalah awalnya / asli nya dengan format pdf makan akan muncul karakter magic number 25 50 44 46 walau pun sudah di ubah jpg. Dengan begitu file yang disembunyikan tersebut akan terlihat.

9.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. WinHex (Windows & Linux)
3. Stegotools, OpenStego dll (Steganografi)

9.5. PRE-TEST

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

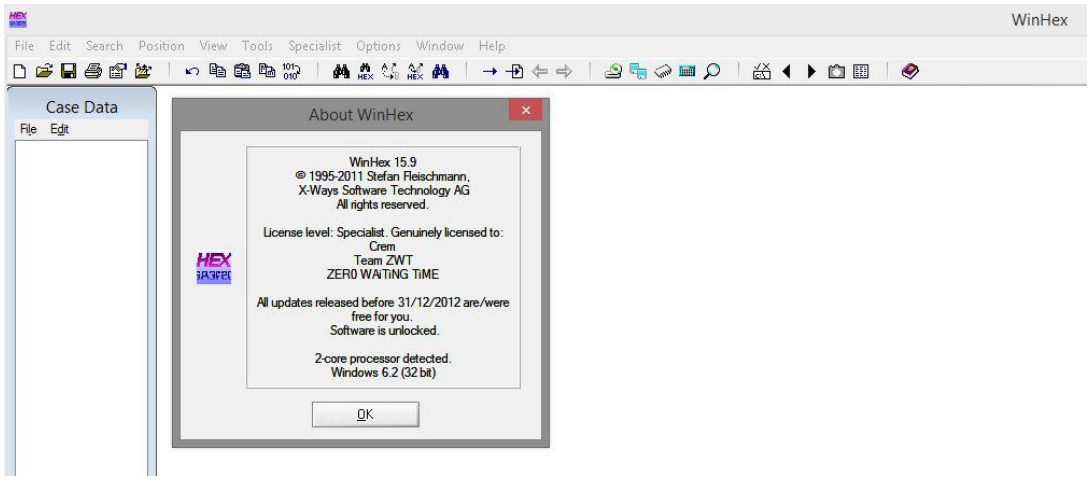
No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Apakah steganografi masuk kedalam ranah Anti Forensick, Jelaskan!	50
2.	CPL-07	CPMK-03	Jelaskan syarat-syarat terjadinya Anti Forensik!	50

9.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

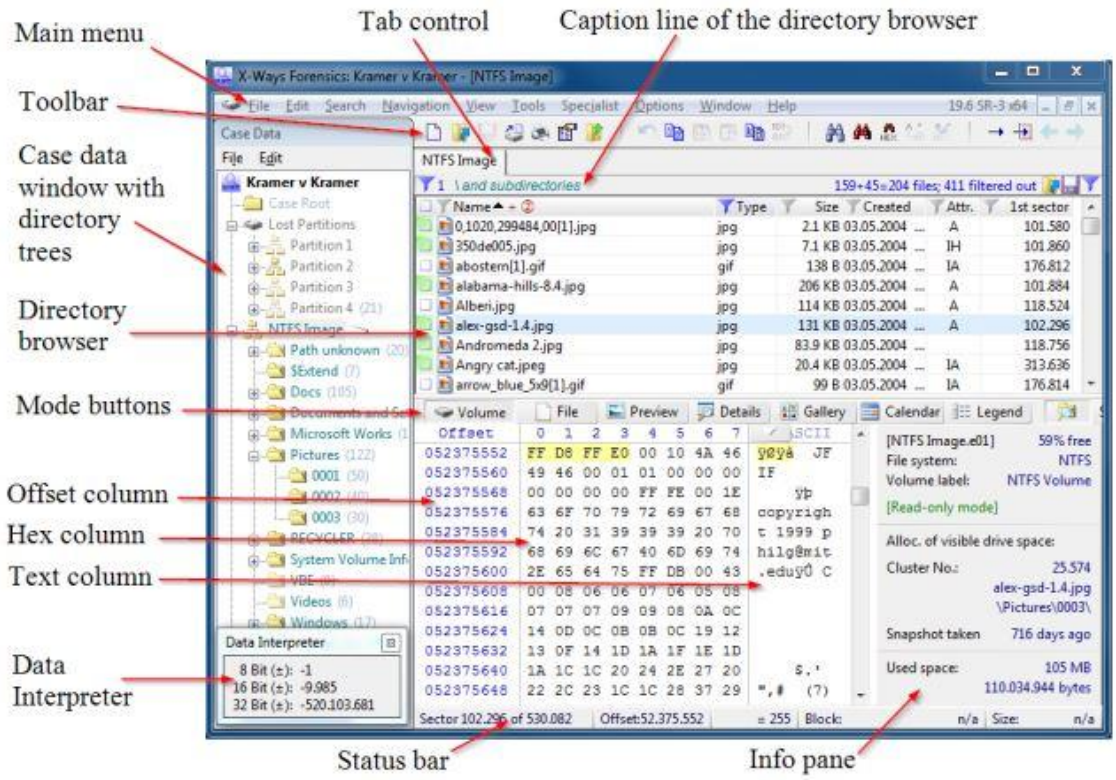
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum berikut!	Screen Shot Hasil praktikum	100

Jalankan Aplikasi Tools WinHex



Gambar 9.1 WinHex Explorer

- Buka Salah satu file ; JPEG/PDF/GIF dll
- Amati Header File Signature Pada Hex paling Atas



Gambar 9.2 WinHex Atributes.Buka StegoTools untuk memanipulasi file image

Gambar 9.3 Stego Aplikasi

Pilih Images/Steganografi dan tambahkan file anda yang akan disisipi data lain

Gambar 9.4 Stego Aplikasi Information Hidding

9.7. 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 menggunakan tools winhex dengan file signature sebelum dan sesudah dimanipulasi/penyisipan data!	100

9.8. 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:**