ANTI DIGITAL FORENSIC PADA PERANGKAT USB FLASHDISK

Faizal Achmad
Lembaga Sandi Negara
faizal.achmad@lemsaneg.go.id

ABSTRAK
Perangkat penyimpanan data sudah menjadi suatu kebutuhan yang penting pada era teknologi informasi saat ini. Salah satu perangkat penyimpanan data yang banyak digunakan adalah USB Flashdisk karena bentuknya yang kecil sehingga lebih mudah untuk dibawa. Namun dari kemudahan ini juga terdapat kerawanan keamanan informasi yang tersimpan didalam USB Flashdisk yaitu jika USB Flashdisk hilang atau diakses oleh pihak yang tidak berwenang walaupun data yang ada didalamnya sudah terhapus. Saat ini telah berkembang ilmu digital forensic yang mempelajari proses pengungkapan dan penafsiran data elektronik pada suatu perangkat, salah satu teknik yang dipelajari adalah pengungkapan data yang telah terhapus atau terformat pada USB Flashdisk. Penulisan ini menjelaskan dan mensimulasikan teknik-teknik yang dapat digunakan sebagai anti digital forensic pada perangkat USB Flashdisk, seperti File Encryption, Steganography, Disk Cleaning dan File Wiping, semua hal ini bertujuan untuk mengamankan data informasi yang terdapat didalam USB Flashdisk dari akses pihak yang tidak berwenang.

Kata Kunci : *Digital Forensic, Anti Digital Forensic, File Encryption, Steganography, Disk Cleaning, File Wiping, USB Flashdisk*

1. Pendahuluan

1.1 Latar Belakang Masalah

Seiring dengan semakin berkembangnya teknologi informasi dan perangkat pendukungnya, saat ini media penyimpanan informasi digital semakin beraneka ragam dengan kapasitas penyimpanan yang relatif besar dan harga terjangkau. Media penyimpanan informasi digital yang banyak digunakan adalah *Universal Serial Bus* (USB) *Flashdisk*, hal ini karena bentuknya yang kecil dan kompatibel dengan berbagai perangkat komputer. Namun ada beberapa kerawanan keamanan yang dapat terjadi pada suatu *USB Flashdisk* diantaranya adalah keamanan informasi yang tersimpan didalamnya jika *USB Flashdisk* hilang atau *USB Flashdisk* diberikan kepada orang lain ketika sudah tidak dibutuhkan lagi, walaupun data informasi yang ada didalamnya telah dihapus sebelumnya, hal ini tidak menjamin keamanan data informasi yang pernah tersimpan didalamnya, karena tidak menutup kemungkinan adanya pihak-pihak yang tidak berwenang melakukan proses pengungkapan kembali data informasi elektronik yang biasa disebut dengan *digital forensic*.

Untuk mengatasi hal tersebut maka pada penulisan ini akan dijelaskan metode dan teknik yang dapat digunakan sebagai *anti digital forensic* pada perangkat *USB Flashdisk*.

1.2 Tujuan Penulisan

Memberikan penjelasan dan simulasi metode serta teknik yang dapat digunakan sebagai anti digital forensic pada perangkat *USB Flashdisk.*

1.3 Perumusan Masalah

Dalam rangka pengamanan data informasi yang tersimpan dalam *USB Flashdisk* dari metode *Digital Forensic* maka perlu dirumuskan suatu solusi bagaimana metode dan teknik yang dapat digunakan sebagai *Anti Digital Forensic*.

2. Landasan Teori

2.1 Digital Forensic[1]

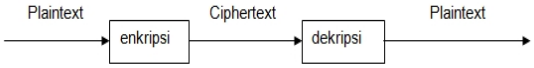
Digital Forensic adalah suatu proses mengungkap dan menafsirkan data elektronik yang akan digunakan pada pengadilan. Tujuan dari proses ini adalah untuk menjaga setiap barang bukti tetap dalam bentuk aslinya selama melakukan investigasi terstruktur dengan mengumpulkan , identifikasi, dan validasi informasi digital untuk tujuan rekonstruksi kejadian di masa lalu.

2.2 Anti Digital Forensic[2]

Anti Digital Forensic adalah suatu proses untuk memanipulasi, menghapus, atau mengaburkan data digital dengan tujuan untuk mempersulit pemeriksaan data digital, memperlama waktu atau bahkan membuat pemeriksaan data digital menjadi hampir mustahil untuk dilakukan. Beberapa metode yang digunakan dalam *Anti Digital Forensic* adalah :

- **Penyembunyian Data**
  Suatu data digital dapat disembunyikan dengan menggunakan teknik-teknik sebagai berikut :
  - **Kriptografi[3]**
    Kriptografi adalah suatu seni dan ilmu pengetahuan dalam menjaga kerahasiaan suatu pesan/informasi.
    Berikut merupakan istilah-istilah yang terdapat dalam kriptografi :

Enkripsi adalah proses menyamarkan suatu pesan sebagai cara untuk menyembunyikan isinya.
Plaintext (Teks Terang) adalah suatu pesan yang belum terenkripsi.
Ciphertext (Teks Sandi) adalah suatu pesan yang telah terenkripsi.
Dekripsi adalah suatu proses untuk mengembalikan Teks Sandi menjadi Teks Terang.



Gambar 1. Proses Enkripsi - Dekripsi

- **Steganografi**
  Steganografi adalah cabang dari ilmu keamanan informasi yang mencoba mengaburkan keberadaan suatu data melalui perangkat seperti tinta yang tidak terlihat.

- **Artifact Wiping**
  Artifact Wiping adalah metode yang digunakan untuk menghilangkan sebagian atau seluruh file sistem secara permanen. Hal ini dapat dilakukan menggunakan teknik sebagai berikut :
  - Disk cleaning
  - File wiping

2.3 USB Flashdisk[4]

USB Flashdisk adalah alat penyimpanan data memori flash tipe NAND yang memiliki alat penghubung USB yangterintegrasi. *Flashdisk* ini biasanya berukuran kecil, ringan, serta bisa dibaca dan ditulisi dengan mudah. Per November 2006, kapasitas yang tersedia untuk *USB Flashdisk* ada dari 128 megabyte sampai 64 gigabyte.

3. Metode Penelitian

Metode Penelitian yang dilakukan pada kegiatan penelitian ini adalah sebagai berikut :

- Melakukan studi literatur dan pengumpulan data dari berbagai sumber seperti buku dan internet mengenai metode dan teknik yang digunakan pada anti digital forensic.
- Melakukan simulasi metode dan teknik *anti digital forensic.*

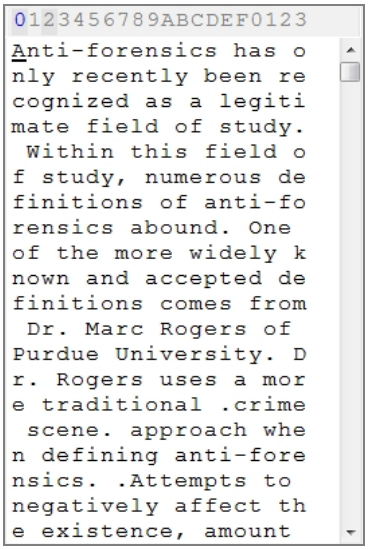
4. Pembahasan

Pada bagian ini akan dilakukan simulasi teknik-teknik yang dapat digunakan untuk mengamankan data informasi yang tersimpan dalam perangkat *USB Flashdisk* dari akses *Digital Forensic* pihak-pihak yang tidak berwenang.

4.1 Penyembunyian Data

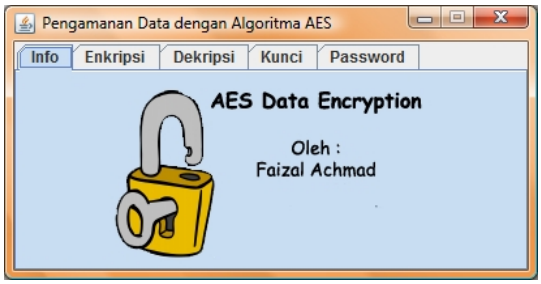
Teknik penyembunyian data biasanya digunakan untuk mengamankan data-data di dalam *USB Flashdisk* yang masih atau akan digunakan lagi kelak.

- ***File Encryption*** **(Enkripsi File)**
  Penyembunyian suatu data informasi berbentuk file dapat dilakukan dengan teknik enkripsi file, pada teknik ini digunakan suatu perhitungan algoritma kriptografi untuk menyamarkan informasi yang tersimpan pada file. Algoritma kriptografi yang dapat digunakan adalah "Algoritma Kriptografi Publik" yang merupakan algoritma kriptografi standar yang sudah dipublikasikan secara bebas dan "Algoritma Kriptografi Proprietary" yang merupakan algoritma kriptografi yang tidak dipublikasikan dan hanya digunakan oleh kalangan terbatas. Berikut merupakan simulasi enkripsi file pada *USB Flashdisk* dengan menggunakan "Algoritma Kriptografi Publik" dan "Algoritma Kriptografi Proprietary".
  Pada gambar.2 ditunjukkan sebuah file teks asli (Test File.txt) yang merupakan sebuah file biasa yang dapat langsung terbaca.



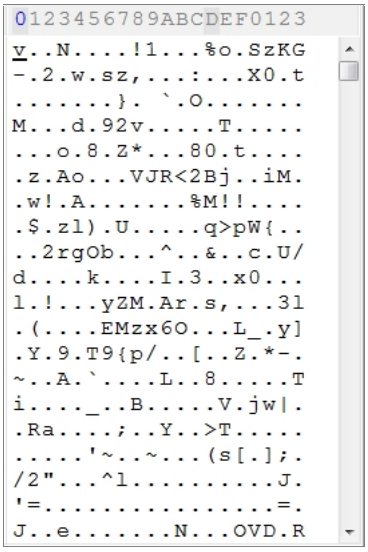
Gambar.2 "Test File.txt"

Informasi yang terdapat pada file "Test File.txt" akan disembunyikan dengan menggunakan enkripsi file. Aplikasi enkripsi file yang digunakan sebagai simulasi merupakan hasil buatan penulis sendiri menggunakan "Algoritma Kriptografi Publik" yaitu AES dengan kunci 256-bit dan "Algoritma Kriptografi Proprietary", seperti yang terlihat pada gambar.3.



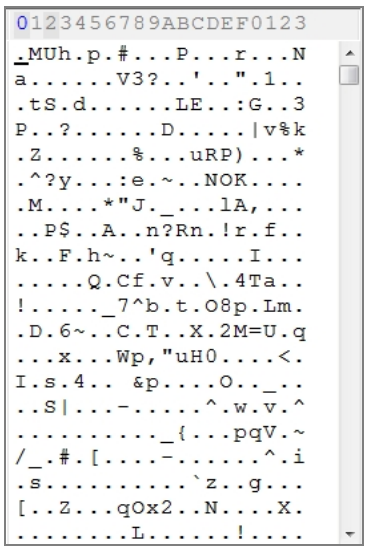
Gambar.3 Aplikasi Enkripsi File

Hasil dari enkripsi file "Test File.txt" dengan menggunakan "Algoritma Kriptografi Publik" seperti yang terlihat pada gambar.4



Gambar.4 Hasil enkripsi file menggunakan "Algoritma Kriptografi Publik"

Informasi yang terdapat dalam file hasil enkripsi tidak dapat terbaca secara langsung, diperlukan suatu teknik lebih lanjut untuk dapat menganalisanya. Sehingga akan mempersulit pihak-pihak yang akan melakukan investigasi.
Hasil dari enkripsi file "Test File.txt" dengan menggunakan "Algoritma Kriptografi Proprietary" seperti yang terlihat pada gambar.5



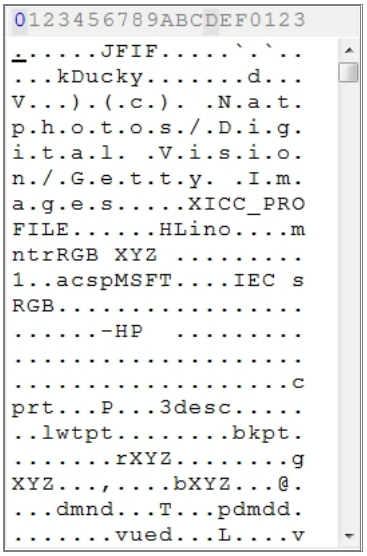
Gambar.5 Hasil enkripsi file menggunakan "Algoritma Kriptografi Proprietary"

Informasi yang terdapat dalam file hasil enkripsi tidak dapat terbaca secara langsung, diperlukan suatu teknik lebih lanjut untuk dapat menganalisanya. Sehingga akan mempersulit pihak-pihak yang akan melakukan investigasi.
Kelebihan dari teknik ini adalah enkripsi file dapat dilakukan baik untuk file dengan ukuran kecil maupun besar, kekurangan dari teknik ini adalah file hasil enkripsi dapat langsung terdeteksi sebagai file terenkripsi karena tidak dikenali oleh aplikasi yang umum digunakan.

- **Steganografi**
  Penyembunyian suatu data informasi dapat dilakukan dengan teknik steganografi, pada teknik ini data informasi disisipkan kedalam suatu file multimedia untuk menyamarkan informasi yang tersimpan di dalamnya. Contoh yang paling sederhana adalah menyisipkan suatu informasi singkat di dalam suatu file gambar seperti contoh berikut.

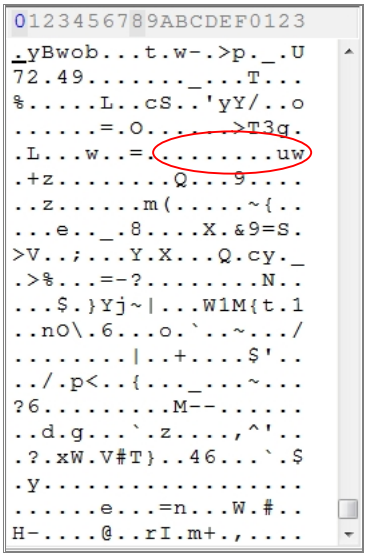

Gambar.6 Foto berjudul "Garden"

Pada gambar.6 terlihat suatu foto berjudul "Garden", jika dilihat menggunakan suatu aplikasi text editor *header file* atau bagian awal dari foto tersebut terlihat seperti pada gambar.7



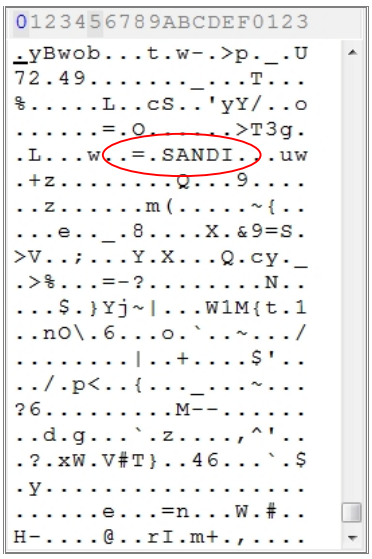
Gambar.7 Header dari foto "Garden"

Selanjutnya dari bagian akhir foto tersebut terdapat ruang kosong yang dapat digunakan untuk menyisipkan suatu informasi, seperti yang terlihat pada gambar.8



Gambar.8 Ruang kosong pada foto "Garden"

Dari ruang kosong yang terlihat pada gambar.8 akan disisipkan suatu informasi yaitu "SANDI" seperti pada gambar.9.



Gambar.9 Penyisipan kata "SANDI" pada foto berjudul "Garden"

Penampakann foto yang telah disisipkan dengan kata "SANDI" masih dapat terlihat dengan jelas pada gambar.10 dan secara kasat mata tidak ada perbedaan yang mencolok dibandingkan foto "Garden" asli yang terlihat pada gambar.6


Gambar.10 Foto "Garden" yang berisi kata "SANDI"

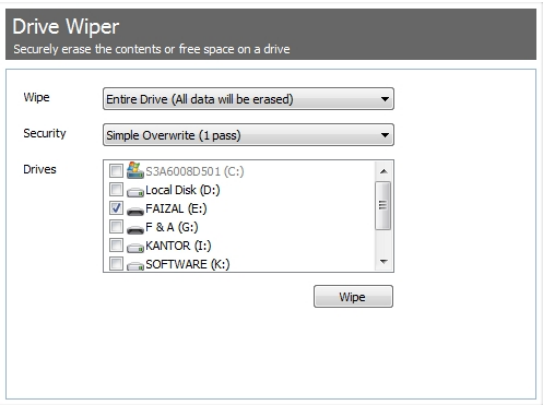
Kelebihan dari teknik ini adalah foto secara kasat mata tidak dapat langsung dideteksi mengandung suatu informasi, kekurangan dari teknik ini adalah besar ukuran informasi yang disisipkan bergantung pada file multimedia yang digunakan.
Untuk menambah kekuatan *steganography* informasi yang akan disisipkan dapat dienkripsi terlebih dahulu.

4.2 Artifact Wiping

Teknik *artifact wiping* biasanya digunakan untuk menghapus data-data di dalam *USB Flashdisk* yang sudah atau tidak akan digunakan lagi kelak.

- **Disk Cleaning**
  Pada proses *disk cleaning* semua data informasi yang tersimpan dalam suatu *USB Flashdisk* akan dihapus secara aman atau permanen dengan metode

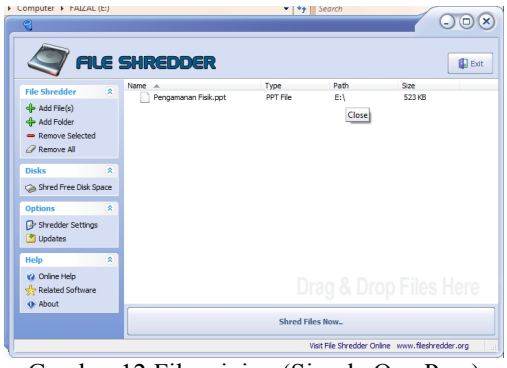
overwrite sehingga tidak dapat dikembalikan lagi. Pada simulasi digunakan aplikasi **CCleaner** untuk proses *disk cleaning*, *level security* yang digunakan pada simulasi adalah *simple overwrite* (1 *passes*) seperti yang terlihat pada gambar.11



Gambar.11 Simple Overwrite (1 Pass)

Level security simple overwrite (1 passes) merupakan *level* yang terendah, masih terdapat *level security* lainnya yang lebih tinggi tingkatannya, semakin tinggi *level security* yang digunakan pada proses *disk cleaning* maka waktu yang dibutuhkan akan semakin lama.

- **File Wiping**
  Pada proses *file wiping* berbeda dengan proses *disk cleaning*, pada proses *file wiping* tidak seluruh file dalam *USB Flashdisk* akan terhapus, tetapi dapat ditentukan file yang ingin dihapus dan *algoritma security* yang akan digunakan. Pada simulasi dilakukan proses *disk cleaning* dengan algoritma *security simple one pass* seperti yang terlihat pada gambar.12

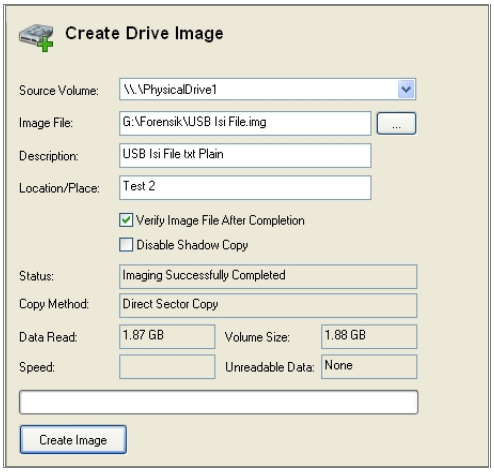


Gambar.12 File wiping (Simple One Pass)

Algoritma *security simple one pass* merupakan algoritma *security file wiping* dengan *level* yang paling rendah, masih terdapat algoritma security lainnya yang lebih tinggi tingkatannya, semakin tinggi level algoritma *security* yang digunakan pada proses *file wiping* maka waktu yang dibutuhkan akan semakin lama

4.3 Simulasi Digital Forensic

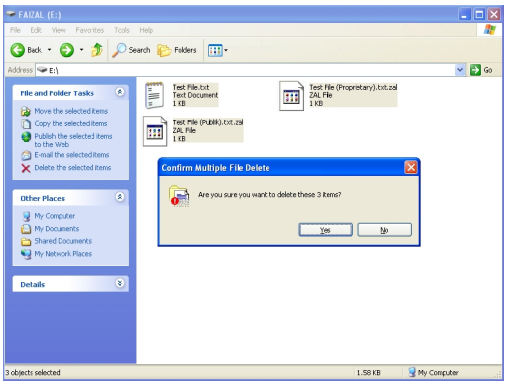
Proses *digital forensic* pada perangkat *USB Flashdisk* dimulai dengan proses *imaging* seperti yang terlihat pada gambar.13, hal ini dilakukan untuk mendapatkan image data sesuai dengan *USB Flashdisk* yang akan dilakukan *forensic*, hal ini bertujuan untuk menghindari kondisi *USB Flashdisk* berubah pada proses *digital forensic*.



Gambar.13 Proses imaging USB Flashdisk

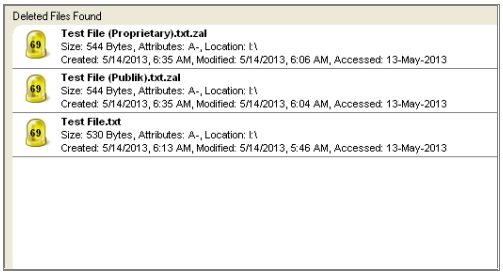
Dalam simulasi ini kondisi USB Flashdisk dibagi menjadi 3 kategori yaitu :

- **USB Flashdisk dengan kondisi file-file yang tersimpan didalamnya telah dihapus.**
  Pada simulasi ini kondisi awal *USB Flashdisk* telah terisi 3 buah file yang merupakan file *plain* (biasa), file hasil enkripsi dengan Algoritma Kriptografi Public dan Proprietary, kemudian semua file tersebut dihapus seperti pada gambar 14.



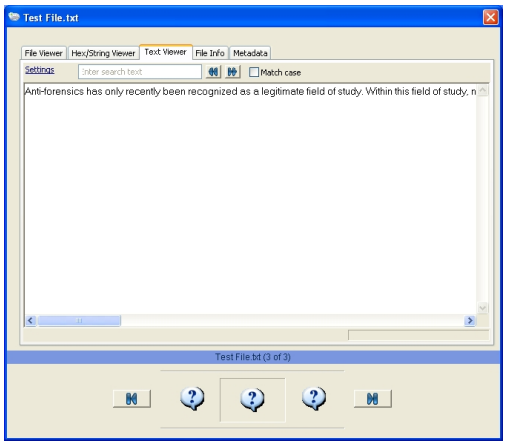
Gambar.14 Penghapusan file

USB Flashdisk yang telah dalam kondisi kosong tersebut kemudian dibuat menjadi *image* untuk dilakukan proses *forensic*. Pada proses *digital forensic* file-file yang telah terhapus tersebut ternyata masih dapat dimunculkan kembali menggunakan **OS Forensic** seperti yang terlihat pada gambar.15



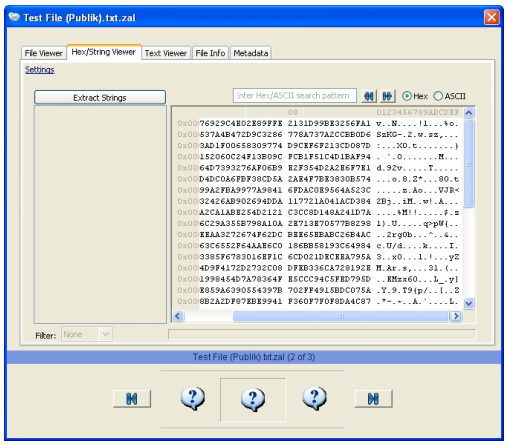
Gambar.15 Recover deleted file

Pertanyaan selanjutnya adalah apakah file-file yang dapat dimunculkan kembali tersebut masih dapat terbaca? Oleh karena itu masing-masing file tersebut akan dicoba untuk direview.
"Test File.txt" yang merupakan file plain (biasa) pada gambar.16, isinya terbaca sama persis dengan file tersebut saat belum terhapus pada gambar.2



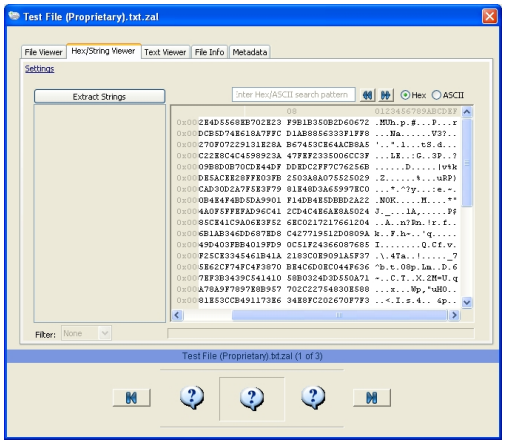
Gambar.16 Review file "Test File.txt" hasil recovery

"Test File (Public).txt.zal" yang merupakan file hasil enkripsi Algoritma Kriptografi Publik pada gambar.17, isinya terbaca sama persis dengan file tersebut saat belum terhapus pada gambar.4, file enkripsi seperti ini akan menyulitkan bagi seseorang yang akan melakukan investigasi terhadap informasi yang tersimpan pada file tersebut, karena walaupun algoritma kriptografinya sudah diketahui yaitu : AES dengan 256-bit kunci, tetapi ada 2^{256} kemungkinan kunci yang harus dicoba untuk membuka file enkripsi tersebut, sedangkan untuk mencoba semua kemungkinan kunci tersebut dibutukan sumber daya dan waktu yang lama.



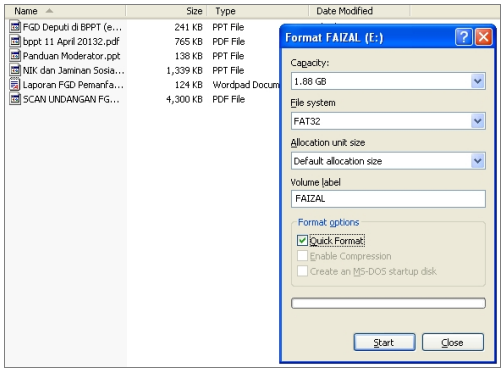
Gambar.17 Review file "Test File (Publik).txt.zal" hasil recovery

"Test File (Proprietary).txt.zal" yang merupakan file hasil enkripsi Algoritma Kriptografi Proprietary pada gambar.18, isinya terbaca sama persis dengan file tersebut saat belum terhapus pada gambar.5, file enkripsi seperti ini akan menyulitkan bagi seseorang yang akan melakukan investigasi terhadap informasi yang tersimpan pada file tersebut, karena algoritma kriptografi yang digunakan untuk enkripsi tidak diketahui dan berapa panjang bit kuncinya juga tidak diketahui, sehingga akan sangat sulit untuk memperkirakan ada berapa kemungkinan kunci yang harus dicoba untuk membuka file enkripsi tersebut.



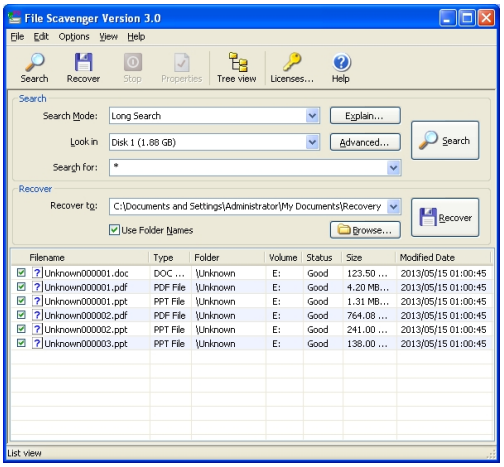
Gambar.18 Review file "Test File (Proprietary).txt.zal" hasil recovery

- **USB Flashdisk berisi file dan terformat**
  Pada simulasi ini kondisi awal *USB Flashdisk* telah terisi 6 buah file yang merupakan file plain (biasa), terdiri dari file dengan tipe *.doc, *.ppt, *.pdf. USB Flashdisk tersebut kemudian diformat sehingga semua file yang tersimpan didalamnya secara otomatis terhapus seperti pada gambar. 19



Gambar.19 Format USB Flashdisk

USB Flashdisk yang telah dalam kondisi kosong karena terformat tersebut kemudian dibuat menjadi *image* seperti yang telah dilakukan sebelumnya pada gambar.13 untuk dilakukan proses *forensic*. Pada proses *digital forensic* file-file yang telah terhapus karena proses *formatting* tersebut ternyata masih dapat dimunculkan kembali dengan menggunakan aplikasi **File Scavenger** seperti yang terlihat pada gambar.20

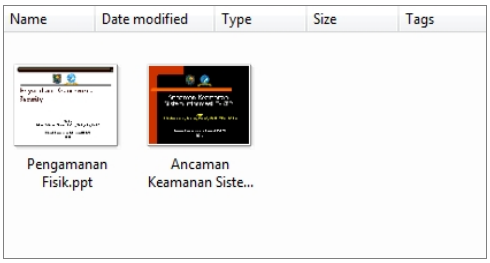


Gambar.20 Recovery formatted USB Flashdisk

Dari daftar file yang berhasil dilakukan *recovery* akan dicoba apakah file-file tersebut dapat terbaca, ternyata semua file tersebut dapat dibaca, salah satunya seperti yang terlihat pada gambar.21

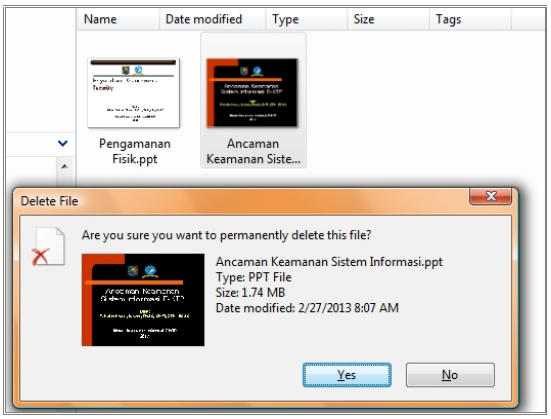
Gambar.21 Salah satu file hasil recovery

- **Manual delete file dan file wiping pada USB Flashdisk**
  Pada simulasi ini kondisi awal *USB Flashdisk* telah terisi 2 buah file yang merupakan file plain (biasa) seperti pada gambar.22.

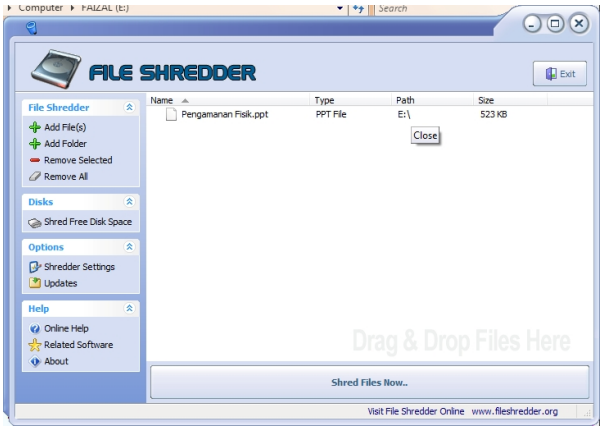


Gambar.22 Isi USB Flashdisk

Kemudian salah satu dari 2 file tersebut dihapus secara manual (gambar.23) dan satu file lainnya dihapus menggunakan metode *file wiping* (gambar.24)

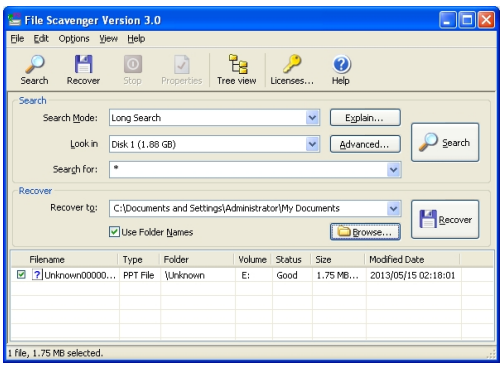


Gambar.23 Hapus file secara manual



Gambar.24 Hapus file dengan file wiping

USB Flashdisk yang telah dalam kondisi kosong karena tersebut kemudian dibuat menjadi *image* seperti yang telah dilakukan sebelumnya pada gambar.11 untuk dilakukan proses *forensic*. Pada proses *digital forensic* ternyata hanya 1 file saja yang masih dapat dimunculkan kembali seperti gambar.25



Gambar.25 USB Flashdisk recovery

File yang berhasil di*recovery* tersbut kemudian dibaca dan terlihat seperti pada gambar.26, ternyata file tersebut adalah file yang sebelumnya dihapus secara manual.

Gambar.26 File hasil recovery

Kesimpulan dari simulasi ini adalah file yang dihapus secara manual masih dapat dimunculkan kembali dengan proses *recovery*, sedangkan file yang dihapus dengan *file wiping* terhapus secara permanen, sehingga tidak dapat dimunculkan kembali.

5. Kesimpulan

Hasil kesimpulan dari penulisan ini adalah :

- *Digital Forensic* adalah suatu proses yang dilakukan untuk mengungkapkan dan menafsirkan data elektronik pada suatu perangkat.
- *Anti Digital Forensic* adalah suatu proses untuk memanipulasi, menghapus, atau mengaburkan data digital dengan tujuan untuk mempersulit proses *digital forensic.*
- Teknik yang digunakan untuk *Anti Digital Forensic* yaitu penyembunyian data dan *Artifact Wiping.*
- Teknik penyembunyian data pada perangkat *USB Flashdisk* digunakan untuk data-data yang masih atau akan digunakan kelak.
- Teknik *Artifact Wiping* pada perangkat USB digunakan untuk data-data yang sudah atau tidak akan digunakan lagi kelak.
- Perpaduan teknik penyembunyian data dan *artifact wiping* pada data-data yang tersimpan pada *USB Flashdisk* merupakan cara yang efektif untuk mencegah *digital forensic* terhadap perangkat *USB Flashdisk* dari pihak-pihak yang tidak berwenang.

Referensi

1. http://www.techopedia.com/definition/27805/digital-forensics, diakses 10 Mei 2013
2. http://www.forensicmag.com/article/anti-digital-forensics-next-challenge-part-1, diakses 10 Mei 2013
3. Bruce Schneier (1996). *Applied Cryptography, Second Edition*. John Wliey & Sons Inc
4. http://www.transiskom.com/2010/06/pengertian-usb-flash-disk.html, diakses 10 Mei 2013