APLIKASI PENERAPAN *DIGITAL FORENSICS* PADA SISTEM *FILE*

Resi Utami Putri

Jurusan Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia Yogyakarta

resiutami@yahoo.com

Abstrak

Forensik digital merupakan suatu cabang ilmu pengetahuan yang berguna untuk menelusuri jejak yang ditinggalkan serta merekonstruksinya. Saat ini kejahatan komputer sudah menjadi hal biasa di kalangan masyarakat, terutama menyangkut pencurian data baik secara terang-terangan maupun tersembunyi. Banyak penelitian yang telah dilakukan untuk melakukan pemulihan data yang telah dihilangkan pelaku yang memungkinkan membantu untuk penyelidikan oleh investigator forensik. Makalah ini mencoba untuk melihat tren forensik digital pada sistem file. Makalah ini menunjukkan beberapa tool yang berbeda yang digunakan oleh beberapa peneliti sebelumnya. Forensik sistem file kini sangat diperlukan karena untuk menganalisis data yang disembunyikan oleh pelaku kejahatan.

Kata kunci: forensik digital, sistem file, *tool* forensik, data.

1. Pendahuluan

Pada masa kini, perkembangan teknologi semakin pesat, komputer dan internet sudah banyak digunakan dalam kehidupan kita. Kejahatan dengan menggunakan teknologi komputer, menyimpan bukti kejahatan pada komputer maupun jaringan. Penyadapan dan menganalisis data yang disimpan dalam berbagai perangkat penyimpanan menjadi bagian yang penting dalam memperoleh barang bukti.

Tugas dari investigator forensik adalah mengumpulkan semua bukti yang tersedia untuk memahami dimana, bagaimana dan kapan serangan terjadi. Ketersediaan bukti memiliki dampak langsung terhadap kepastian kesimpulan yang diambil oleh investigator forensik mengenai modus dari penyerang. Seorang penyerang bisa menghapus atau mengaburkan bukti untuk menyembunyikan tindakan kejahatannya.

Proses pengumpulan bukti berfokus pada mengenali dan mengidentifikasi bukti berdasarkan karakteristik sistem *file*. Rekonstruksi peristiwa memeriksa bukti untuk mencari tahu mengapa sebuah objek memiliki karakteristik tertentu.

Pelaku kejahatan cenderung menyembunyikan atau mengenkripsi informasi sehingga ketika komputer mereka dikumpulkan oleh kepolisian, tidak ada bukti. Sebenarnya, ada banyak cara bagaimana data dapat bersembunyi. Cara yang paling terkenal adalah melakukan enkripsi data dan steganografi.

Menganalisis bukti digital adalah tantangan utama forensik digital saat ini. Seorang tersangka dapat menghapus bukti pada harddisk. Hanya ada beberapa alat yang memungkinkan untuk merekonstruksi hasil forensik.

2. Landasan Teori

Penggunaan teori diperlukan untuk mendefinisikan beberapa pengertian yang akan dibahas dalam makalah ini.

Setiap sistem operasi mempunyai sistem *file* yang berbeda. Pada sistem operasi Windows, jenis sistem *file*-nya adalah FAT 12/32 dan NTFS. Sistem operasi Linux mempunyai sistem *file* Ext2/Ext3/Ext4 dan Reiser. Sedangkan Mac mempunyai sistem *file* HFS dan HFS+/HFSX. Sistem *file* yang paling banyak digunakan adalah NTFS. NTFS juga banyak digunakan pada sistem operasi Windows dan sebagian UNIX.

Beberapa *tools* yang sering digunakan dalam forensik sistem *file* adalah Scalpel, Encase, FTK3, Foremost dan Revit. Dari beberapa *tools* tersebut yang paling banyak digunakan adalah Foremost.

Beberapa bagian dari suatu sistem *file* menurut Giampaolo (1999) adalah sebagai berikut:

a. Disk merupakan media penyimpanan dengan ukuran tertentu yang memiliki sektor atau ukuran blok. Ukuran blok adalah 512 *byte*.
b. Blok merupakan satuan terkecil yang ditulis oleh disk atau *file system*.
c. Partisi merupakan subset dari semua blok pada disk.
d. Volume merupakan nama yang diberikan pada kumpulan blok pada beberapa media penyimpanan seperti disk.
e. Superblok merupakan luas *volume* tempat *file system* menyimpan informasi.
f. Metadata merupakan istilah yang merujuk informasi tapi bukan merupakan bagiannya. Contohnya adalah ukuran *file*.
g. *Journal* adalah metode yang menunjukkan kebenaran metadata *file system*.
h. *i-node* merupakan tempat *file system* menyimpan semua metadata dari suatu file. *I-node* juga dikenal sebagai *File Control Block* (FCB)
i. *extend* (luas) merupakan nomor blok awal dan panjang blok yang berurutan pada disk.
j. Atribut adalah sebuah nama dan nilai yang terkait dengan nama (*text string*).

3. Tren forensik data saat ini

Bagian ini menjelaskan dan keterbatasan dari penelitian dan prosedur pengumpulan data.

3.1 Keterbatasan Penelitian

Pendekatan yang digunakan, kemungkinan belum mencakup gambaran yang sebenarnya dari garis besar forensik sistem *file*. Jumlah makalah juga belum terlalu signifikan membahas mengenai forensik digital terutama yang membahas sistem *file*. Akan tetapi dengan melihat beberapa penelitian sebelumnya sudah cukup untuk menunjukkan berbagai *tool* yang digunakan dalam forensik sistem *file*.

3.2 Prosedur Pengumpulan Data

Tahun 2002 merupakan awal dimulainya tren forensik digital karena maraknya kejahatan di bidang komputer hingga akhirnya dimulainya tren forensik digital di Indonesia yaitu pada tahun 2009. Penelitian ini mengambil dari beberapa jurnal maupun proseding yang dimulai dari tahun 2005 hingga tahun 2013. Tahun 2005 merupakan awal tahun dimulainya tren forensik sistem *file*. Dalam penelitian selama delapan tahun terakhir beberapa *tool* yang digunakan, ditunjukkan pada Tabel 1.

Tabel 1 *Tool* forensik yang digunakan

No.	Tahun	Peneliti	Tool yang digunakan
1	2005	Sarmoria	Monitor runtime
2	2005	Richard	Scalpel
3	2005	Sitaraman	Backtracker
4	2005	Wee	Runtime Disk Explorer for NTFS
5	2006	Roussev	Md5bloom
6	2009	Alazab	Chkdisk, Sleuth kit
7	2011	Thing	File carving – Adroit Photo Forensic
8	2012	Mahant	Mini-123
9	2012	Hand	Bin Carver
10	2013	Kalber	Py3xF
11	2013	Rousssev	Zsniff
12	2013	Vömel	Win32dd, WinPMEM, mdd

4. Diskusi dan Hasil Analisis

Beberapa Penelitian membahas tentang riset yang berhubungan dengan forensik sistem *file*. Hal yang menjadi perbandingan setiap penelitian adalah berdasarkan *tool* serta teknik yang digunakan dalam penelitian.

Penelitian yang dilakukan selama delapan tahun terakhir mengenai sistem *file*, telah membuat percabangan baru dari ilmu forensik digital. Pada awal penelitian, dimulai dengan masalah bagaimana menyembunyikan sebuah data dalam sistem *file* NTFS. Dalam Wee (2005) menerapkan teknik analisis yang biasa diterapkan dalam mendeteksi dan memulihkan data yang tersembunyi dengan dua tahap mengidentifikasi data yang tersembunyi dengan mencari anomali dan memulihkan data yang tersembunyi.

Selanjutnya Sitaraman & Venkatesan (2005) melakukan analisis forensik sistem *file* menggunakan teknik *backtracking* dengan penambahan parameter dari sistem *file*. Alat yang digunakan bernama Backtracker dapat mengidentifikasi dan mendapatkan akses masuk ke sistem.

Masih pada tahun 2005, masalah muncul bagaimana proses rekonstruksi sebuah sistem *file* yang bertujuan untuk membentuk rangkaian kejadian *file*. Proses rekonstruksi yang dilakukan dimulai dari titik deteksi, seperti isi *file* yang mencurigakan dan membentuk rantai dengan semua proses dan membangun kembali serangan suatu *file*. Sarmoria & Chapin (2005) menyajikan monitor *runtime* untuk membaca dan menulis operasi pada memori yang dipetakan. Konsepnya adalah untuk memantau penyisipan *page fault* dalam *kernel* manajemen memori. Sistem monitor *runtime* apabila diintegrasikan dengan Bactracker dan Forensix akan memberikan hasil pengurangan waktu pencarian, ruang pencarian dan dependensi palsu.

Pengertian *page fault* adalah merupakan kesalahan halaman pada memori utama yang harus diganti dengan halaman yang baru. *Page fault* terletak pada memori utama. Pergantian halaman dapat dilakukan dengan memindahkan *page* dari memori sekunder ke memori utama.

Pada tahun berikutnya, Richard III & Roussev (2005) melakukan penelitian untuk mengoptimalkan operasi *file carving* dengan Scalpel. Scalpel merupakan salah *tool* forensik. Scalpel dapat dengan cepat melakukan operasi *file carving* dengan ukuran yang besar tapi dengan sumber daya yang sederhana. *Recovery file* adalah mungkin, bahkan jika metadata *filesystem* telah hancur. Metadata merupakan peninggalan dari data yang telah dihapus.

Pada tahun berikutnya, Roussev, et al. (2006) melakukan penelitian untuk meningkatkan teknik *hashing* dalam meningkatkan efisiensi dan skalabilitas analisis forensik digital. Roussev, et al. menggunakan md5bloom yaitu alat memanipulasi filter *bloom* yang dapat dimasukkan ke dalam praktek forensik. Roussev juga menyediakan landasan teoritis dasar, yang mengkuantifikasi tingkat kesalahan terkait dengan berbagai filter *bloom* juga menyediakan kerangka probabilistik yang memungkinkan penafsiran langsung. Roussev membangun alat aliran berorientasi tujuan yang mendukung pengelolaan filter *bloom* yaitu md5bloom.

Pada tahun 2009, Alazab, et al. (2009) membahas teknik forensik digital dalam menganalisis *file system* NTFS yang merupakan *file system* paling standar dan banyak digunakan. Alazab, et al. mencoba menggali kerentanan *disk image* NTFS, mendeteksi data yang disembunyikan berdasarkan struktur internal dari sistem *file*. Akhirnya Alazab, et al. menemukan bahwa data tersembunyi di `$boot` tidak terdeteksi oleh alat forensik. Teknik yang digunakan adalah inspeksi manual gambar *file* NTFS juga dapat digunakan untuk sektor lain di sistem *file* NTFS. Alazab, et al. menggunakan *tool* Sleuth Kit (TSK) dan Autopsy forensik.

Thing, et al. (2011) mengembangkan rekonstruksi bukti dan sistem pemulihan dan melakukan percobaan untuk mengevaluasi kemampuan dalam mendeteksi dan memulihkan bukti yang dikaburkan. *File carving* bertujuan untuk mengatur *file* kembali ke bentuk aslinya dan memulihkan semua *file* dari data mentah. Tujuannya untuk mempercepat proses *carving* (ukiran). Hasilnya menunjukkan bahwa sistem mampu mencapai efisiensi dan akurasi yang lebih tinggi. Thing, et al. menggunakan *file carving* Adroit Photo Forensic.

Mahant & Meshram (2012) melakukan *recovery file* yang telah dihapus pada *file system* NTFS. Mahant membahas struktur operasi *file system* NTFS, penanganan terhadap *file* yang dihapus dan mengusulkan metode untuk memulihkan *file* yang telah dihapus pada disk. Perangkat yang digunakan untuk menggagalkan serangan adalah *skim block*. Mahant & Meshram melakukan penelitian menggunakan *tool* Mini 123.

Hand, et al. (2012) melakukan penelitian dengan *tool* bin carver dengan memanfaatkan *file header* dan *footer*. Hand, et al. berfokus pada *file* dokumen (pdf) dan gambar (jpeg). Bin carver merupakan *tool* yang dapat secara otomatis memulihkan *file executable* walaupun metadata dari suatu *file* telah rusak atau dihapus.

Penelitian tahun 2013, Kalber, et al. (2013) melakukan penelitian dengan merekonstruksi sistem file menggunakan pendekatan sidik jari (*fingerprinting*) dalam metadata. Membuat sistem yang secara otomatis dapat merekonstruksi tindakan yang dilakukan oleh berbagai aplikasi pada *file system* NTFS menggunakan *tool* Py3xF. Py3xF merupakan singkatan dari Python Forensic Fingerprinting Framework. Py3xF dapat secara otomatis memperoleh *fingerprinting* berdasarkan informasi *timestamp* disimpan dalam metadata.

Roussev & Quates (2013) mengembangkan suatu *tool* yaitu zsniff yang dapat mengklasifikasikan fragmen *file*. Zsniff merupakan alat yang secara otomatis dapat menemukan data yang dikompres dengan tabel kompresi Huffman. Roussev & Quates meneliti teks, gambar dan *executable* mempunyai *signature* yang berbeda.

Vömel & Stüttgen (2013) menyajikan *platform* evaluasi yang mampu mengukur faktor yang berbeda yang menentukan kualitas gambar yang dihasilkan memori yaitu masalah integritas. Dengan menggunakan aplikasi *open source* popular. Vömel & Stüttgen melakukan pengujian menggunakan beberapa *tool open souce* yaitu win32dd, winPMEM dan mdd.

5. Kesimpulan

Berdasarkan beberapa penelitian yang membahas forensik sistem *file*. Perkembangan mengenai teknik dan *tool* yang digunakan, semakin banyak dan beragam dari tahun ke tahun. Metode dan teknik yang digunakan juga semakin maju dan beragam, dilihat dari *tool* yang digunakan. Perkembangan *tool* juga menunjukkan hasil yang signifikan, dimana terdapat *tool* yang dapat mempercepat hasil pencarian data maupun *recovery* data, sehingga tidak perlu menunggu lama untuk memproses data yang ukurannya besar.

Tren forensik sistem *file* juga sudah mulai banyak yang meneliti dikarenakan bukti kejahatan biasanya dalam bentuk *file* dan *file* tersebut disembunyikan di dalam sebuah sistem *file*. Seorang investigator juga perlu mempelajari bagaimana sebuah *file* dibuat, bagaimana *file* diakses dan bagaimana *file* dimodifikasi melalui penyelidikan *timestamp* atau *MAC time* suatu *file*. Apabila *file* yang ditemukan telah dihapus oleh pelaku, seorang investigator perlu menyelidiki metadata dari suatu *file* yang dihapus dikarenakan metadata merupakan peninggalan dari *file* yang telah dihapus.

Sistem *file* juga dapat digunakan untuk menyimpan data yang tersembunyi oleh pelaku yang memungkinkan pelaku untuk menyimpan data

pada sektor *boot* (`$boot`) sehingga suatu *file* tidak bisa terdeteksi dan bahkan tidak merubah struktur sistem *file*. Besar *file* yang dapat disimpan pada `$boot` hingga 512 *byte*.

Pada penelitian yang akan datang diharapkan *tools* yang digunakan akan semakin berkembang sehingga dapat melakukan berbagai teknik forensik dalam satu *tool*. Diharapkan juga terdapat teknik baru bagaimana menemukan suatu *file* tersembunyi di tempat yang tersembunyi di sistem *file* dan bisa mengembalikan *file* yang telah dihapus.

Daftar Pustaka

Alazab, M., Venkatraman, S., Watters, P., 2009. Digital Forensic Techniques for Static Analysis of NTFS Images. Paper. *The 4th International Conference of Information Technology (ICIT 2009)*, AL-Zaytoonah University, Amman, Jordan.

Giampaolo, D., 1999. *Practical File System Design: with the Be File System*. San Francisco: Morgan Kaufmann Publishers, inc.

Hand, S., Lin, Z., Gu, G. & Thuraisingham, B., 2012. Bin Carver: Automatic Recovery of Binary Executable Files. *Digital Investigation*, 9, pp. S108-S117.

Kalber, S., Dewald, A. & Freiling, F.C., 2013. Forensic Application Fingerprinting based on File System Metadata. *The 7th International Conference on IT Security Incident Management and IT Forensics*, pp. 98-112.

Mahant, S.H. & Meshram, B.B., 2012. NTFS Deleted Files Recovery: Forensics View. *International Journal of Computer Science and Information Technology and Security (IJCSITS)*, 2(3), pp. 491-497.

Richard III, G.G. & Roussev, V., 2005. Scalpel: A Frugal, High Performance File Carver. *The 2005 Digital Forensic Research Workshop (DFRWS)*, New Orleans, LA.

Roussev, V., Chen, Y., Bourg, T. & Richard III, G.G., 2006. Md5bloom: Forensic Filesystem Hashing Revisited. *Digital Investigation*, 3S, pp. S82-S90.

Roussev V. & Quates, C., 2013. File Fragment Encoding Classification: An Empirical Approach. *Digital Investigation*, 10, pp. S69-S77.

Sarmoria, C.G. & Chapin, S.J., 2005. Monitoring Access to Shared Memory Mapped Files. *The 2005 Digital Forensic Research Workshop (DFRWS), New Orleans, LA.*

Sitaraman, S. & Venkatesan, S., 2005. Forensic Analysis of File System Intrusions using Improved Backtracking. Prosiding. *The 3rd IEEE International Workshop on Information Assurance (IWIA'05)*, pp. 154-163.

Thing, V.L.L., Chua, T.W., dan Cheong, M.L., 2011. Design of a Digital Forensics Evidence Reconstruction System for Complex and Obscure Fragmented File Carving. Prosiding. *The 7th International Conference on Computational Intelligence and Security (CIS 2011)*, pp. 793-797.

Wee, C.K., 2005. *Analysis of Hidden Data in NTFS File System*. [Online] Tersedia di: *http://www.iapsonline.com/sites/default/files/Analysis%20of%20Hidden%20Data%20in%20NTFS%20File%20System%20-%20By%20%20Cheong%20Kai%20Wee.pdf* [Diakses pada 1/10/2013].

Vömel, S. & Stüttgen, J., 2013. An Evaluation Platform for Forensic Memory Acquisition Software. *Digital Investigation*, 10, pp. S30-S40.