Analisis Algoritma Akuisisi Digital Forensik Terbaik: AFF, RAW, dan E01

by Sujatmiko Wikantiyoso

Submission date: 20-Nov-2019 08:45PM (UTC+0700)
Submission ID: 1216992798
File name: SUJATMIKO_W_PAPER_KUMPUL.doc (194K)
Word count: 1646
Character count: 10100

Analisis Algoritma Akuisisi Digital Forensik Terbaik: AFF, RAW, dan E01.

Abstract— **Proses akuisisi forensik memerlukan waktu yang lama. Ada beberapa faktor yang membuat proses akuisisi forensik menjadi lama. Diantaranya pemilihan format *image file* yang menjadi penyebabnya belum lagi jika diperlukan kompresi data nantinya. Setiap format memiliki algoritma yang berbeda yang berpengaruh pada hasil akhir pada proses akuisisi dikarenakan iinformasi yang diambil berbeda-beda. Faktor tersebut yang mungkin mempengaruhi kecepatan akuisisi disamping spesifikasi hardware ataupun storage yang digunakan. Pada paper ini akan dilakukan analisis terhadap beberapa format file akuisisi, yaitu AFF, E01, dan RAW yang berfokus hanya pada analisis algoritma pada masing-masing format untuk melihat informasi apa saja yang diambil pada saat proses akuisisi digital forensik tiap format.**

Keywords— Forensik Digital; Akuisisi forensik

I. PENDAHULUAN

Di era sekarang dimana sedang tinggi antusias pengguna internet juga memunculkan masalah baru. Penyebaran data yang semakin bebas dan meluas menjadi salah satu dampak tersendiri. Memang tidak bisa dihindari masuknya teknologi juga mempengaruhi bagaimana cara berperilaku di media sosial dan pengolahan data. Berbagai motif manipulasi data digital yang muncul, menjadikannya suatu kejahatan baru di era sekarang. Untuk mengatasi kejahatan digital (*cybercrime)* diperlukan penanganan khusus dalam memperoleh atau memperlakukan data.

Dalam memperoleh data digital, maka diperlukan proses akuisisi forensik dimana investigator melakukan pengkopian data dari media penyimpanan [1]. Dan data yang berhasil dikopi harus bersifat valid (benar) karena akan digunakan sebagai barang bukti di pengadilan. Proses akuisisi juga harus berdasarkan hukum yang berlaku, sebagai jaminan dilakukannya akuisi digital forensik sebagai hal yang legal dan diperbolehkan.

Namun proses akuisisi memerlukan waktu yang lama dan hal tersebut berbanding terbalik dengan jumlah kasus yang ditangani. Ada beberapa faktor yang mempengaruhi kecepatan proses akuisisi. Selain spesifikasi alat yang digunakan, pemilihan format hasil image juga menjadi faktor tersendiri.

Pemilihan format yang tepat akan mempengaruhi hasil analisis penanganan suatu kasus. Kualitas suatu data berdasarkan dari hasil informasi yang didapat, apakah sudah sesuai atau tidak. Kualitas data yang disalin berisi kelengkapan informasi seperti akses informasi, waktu dan pengguna. Kualitas data juga dipengaruhi oleh artefak (Registry Key, DLL)[2]. Registry merupakan data yang berisikan konfigurasi mengenai suatu perangkat lunak atau perangkat keras dan informasi tentang pengguna perangkat tersebut.

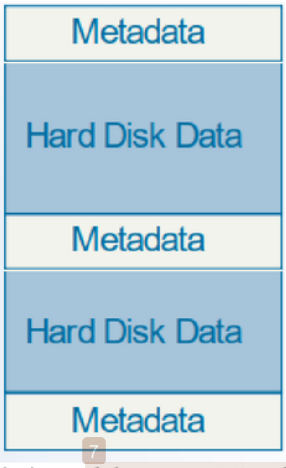
II. TINJAUAN PUSTAKA

A. Advanced Forensic Format (AFF)

AFF merupakan format *image* hasil akuisisi yang dikembangkan oleh Simson Garfinkel yang bersifat *opensource*. AFF dapat dikembangkan, misalnya dengan menambahkan fitur baru agar lebih kompatibel. Pengembangan tersebut memungkinkan untuk program lama agar dapat membaca file AFF yang dibuat oleh program yang lebih baru, dan memungkinkan program AFF yang lebih baru untuk membaca file AFF yang lama.

Gambar 1 Format penyimpanan AFF

AFF dapat menyimpan dengan hasil kompresi maupun tidak, bersama dengan metadata yang dapat tersimpan secara bersamaan atau terpisah pada disk. File AFF dipartisi



menjadi dua lapisan, *disk representation layer* dan *data-storage layer*. *Disk representation layer* menentukan nama segmen yang digunakan untuk menunjukkan semua informasi pada *disk image*. Tiap segmen AFF terdiri dari nama segmen, 32-bit *flag,* dan *payload* data. Nama dan *payload* data. Metadata menyimpan informasi mengenai *disk image*, dan segmen data, yang disebut *pages*.

Gambar 2 Struktur segmen AFF

Lapisan penyimpanan data pada AFF menyimpan segmen dalam bentuk biner (segmen disimpan berurutan dalam satu atau beberapa file. *Data pages* pada AFF dapat dikompres dengan zlib, ataupun tidak dikompresi sama sekali.

Format ini mendukung *internal sel-consistency checking* yang mana menjadi alat yang dapat memulihkan *image* jika bagian lain pada *image* rusak atau hilang. Format ini juka memiliki sertifikasi keaslian data dengan fungsi hash (MD5 dan SHA-1). Biasanya digunakan untuk analisis data.

Terdapat beberapa hal yang bisa didapat dengan menggunakan format AFF[3], yaitu:

- Kemampuan untuk menyimpan *disk image* dengan atau tanpa kompresi.
- Kemampuan untuk menyimpan berbagai ukuran *disk image*.
- Kemampuan untuk menyimpan meta data bersamaan dengan *disk images* atau terpisah.
- Kemampuan untuk meyimpan *image* pada *single file* atau dibagi menjadi beberapa file (*multiple file*).
- Bisa dikembangkan
- Lintas *platform*, *opensource*
- Kemampuan untuk pengecekan konsistensi *image*, sehingga bagian pada *image* bisa dipulihkan apabila terdapat bagian yang *corrupt* atau hilang.
- Kemempuan untuk menjamin keaslian file barang bukti dengan fungsi hash (MD5 dan SHA-1) dan tanda tangan digital.

B. RAW Images

Hanya mengandung data dari sumber *disk*. Tidak ada *header* atau metadata sehingga tidak menyimpan informasi tentang nomor serial pada drive, nama investigator, dan data dilakukannya akuisisi. Biasanya digunakan pada sistem operasi Linux. Merupakan sector-by-sector copy.

Gambar 3. File Raw hanya mengandung data. Meta data pada file terpisah[4]

Format RAW bisa dibuat dengan utility yang berbeda, biasanya menggunakan ekstensi **.dd .raw .img.** *RAW images* sering digunakan karena bisa diterapkan hampir pada semua tool akuisisi. Namun file *raw images* sendiri tidak dilakukan kompresi, sehingga sebagai hasilnya file tersebut bisa berukuran sangat besar, bahkan jika drive hanya mengandung sedikit data.

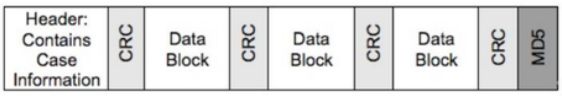
Format ini menunjukkan urutan byte yang tidak terstruktur yang diambil dari *physical* atau *logical volumes*[5].

Beberapa keuntungan menggunakan format RAW[6]:

- Cepat dalam transfer data
- Menghindari kesalahan kecil (*minor error*) ketika membaca driver yang diakuisisi.
- Bisa dibaca pada hampir setiap tool digital forensik

C. E01 Format

Merupakan *image file* yang dibuat oleh EnCase, aplikasi forensic dan tidak pengembangan format ini terbatas (*proprietary)*. Format ini dapat dibaca pada program lain yang mendukung format e01. E01 digunakan untuk menyimpan infromasi sensitif pada forensik digital.

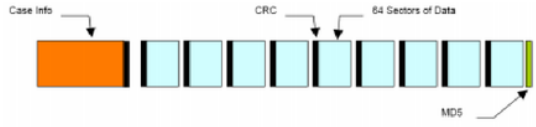


Gambar 4 Format pada Encase file[7]

E01 memiliki header dan footer yang menyimpan metadata suatu *image*. Metadata menyimpan informasi tentang tipe drive, versi EnCase yang digunakan untuk membuat *image*, sumber disk system operasi, dan waktu. Ketika file dibuat, informasi yang dibutuhkan oleh investigator tersimpan pada header. Tiap byte data dari tiap block pada file terverifikasi dengan 32-bit CRC (*Cylical Redudancy Check)*. CRC adalah suatu variasi dari checksum. Hard drive menyimpan satu CRC pada tiap sektornya. Ketika disk error saat dibaca, hal tersebut berarti nilai CRC pada sector tidak cocok dengan nilai CRC pada hard drive setelah dibaca.

Ukuran standar pada suatu block data adalah 64 sektor. EnCase akan mengidentifikasi block data dengan jumlah sector jika terjadi error. Dua block data ganjil yang berisi data berbeda dimana menghasilkn nilai CRC yang sama memiliki kemungkinan ¼ miliar[8]. Secara umum E01

melakukan kompresi pada block menggunakan kompresi zlib, sehingga setelah data block dibara, CRC akan dihitung dan ditambahkan pada blok.



Gambar 5 Format Encase forensics[5]

EnCase akan menghitung MD5 hash ketika melakukan akuisisi fisik atau logic. 128-bit hash biasa dikenal dengan "Acquisition Hash" yang menunjukkan nilai validasi pada suatu media orisinil dan terletak pada segmen paling akhir file barang bukti. Penggunakan MD5 bersifat opsional selama proses akuisisi. Namun melihat pentingnya penggunaan MD5 sebagai bentuk untuk menjaga orisinalitas data, maka metode ini sangat direkomendasikan pada proses akuisisi[8].

III. METODOLOGI PENELITIAN

3.1 Studi literatur

Penelitian dilakukan dengan melakukan riset pada dokumen literatur yang sudah ada. Sehingga data-data yang dikumpulkan merupakan data sekunder. Data nantinya akan dianalisis secara mendalam agar tercapai tujan dari penelitian.

3.2 Pembuatan diagram alur

Untuk mempermudah dalam mengetahui dan analisis proses akuisisi forensik, maka dibutuhkan diagram alur *(flowchart)* untuk mempermudah penelitian. Diagram alur adalah alat pemetaan sederhana yang menunjukkan urutan tindakan dalam proses dengan bentuk yang mudah dibaca dan dipahami [9].

3.3 Analisis Diagram Alur

Analisis dilakukan dengan melihat proses pada tiap format melalui diagram alur yang sudah dibuat. Masing-masing format memang memiliki kelebihan dan kekurangan masing-masing, olehkarena hal tersebut juga menjadi bahan pertimbangan ketika melakukan analisis. Sehingga memang pada tiap proses pada format didapat bagian apa saja yang diambil pada saat proses akuisisi terjadi. Dan selama proses analisis dimungkunkan untuk meninjau kembali apakah data riset yang didapat sudah cukup untuk membuatnya menjadi kesimpulan.

3.4 Kesimpulan

Untuk memberikan poin pada riset ini mengenai bagaimana hasil yang dicapai selama melakukan riset.

IV. HASIL DAN PEMBAHASAN

Setelah melakukan riset, dilakukan analisis dengan membandingkan masing-masing algoritma format *image*. Secara teoritis terlihat bahwa masing-masing format memiliki fungsi tersendiri. Namun jika dibandingkan apa yang membuat beda antara ketiga format *image* tersebut kita harus mengetahui urutan atau proses pada masing-masing format.

A. Perbandingan format

Format	Extensible	Proprietary	Compressed
AFF	v		v
RAW		v	
E01		v	v

Pada table tersebut terdapat beberapa variabel, diantaranya extensible (kemudahan untuk dikembangkan), proprietary (hak cipta), dan kompresi. Dari ketiga variabel tersebut menunjukkan perbedaan ketiga format secara sederhana.

B. Perbandingan Metadata

Format	Metadata
AFF	v
RAW	
E01	v

Berdasarkan table diatas, terlihat bahwa untuk format RAW tidak menyimpan metadata pada saat proses akuisisi. Namun disisi lain, dari ketiga format tersebut, RAW diyakini format yang lebih cepat dari yang lain, namun tetap saja pada RAW tidak menyimpan informasi tentang *disk image*.

V. KESIMPULAN

Setiap format memiliki kekurangan dan kelebihannya masing-masing. Namun berdasarkan hasil riset yang dilakukan AFF (*Advance Forensic Format)* lebih unggul dan mudah dikembangkan dari pada format yang lain. AFF sendiri kini sudah mengalami pengembangan untuk memperbaiki performa dan kompetabilitasnya dengan AFF4. Format AFF selain lebih lengkap dalam menyimpan informasi *disk image* saat akuisisi, juga sifatnya yang fleksibel untuk dikembangkan. AFF juga memiliki kemampuan untuk memvalidasi datanya. AFF juga bisa melakukan kompresi data.

VI. REFERENCES

[1] M. Kaur, N. Kaur, and S. Khurana, "A Literature review on Cyber Forensic and its Analysis tools," *Ijarcce*, vol. 5, no. 1, pp. 23–28, 2016.

[2] M. N. Faiz and W. A. Prabowo, "Comparison of Acquisition Software for Digital Forensics Purposes," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 1, p. 37, 2018.

[3] S. Garfinkel, D. Malan, K. Dubec, C. Stevens, and C. Pham, "Advanced forensic format: An open extensible format for disk imaging," *IFIP Int. Fed. Inf. Process.*, vol. 222, pp. 13–27, 2006.

[4] S. co. Scott D Smith, "Information Security Reading Room," 2019.

[5] S. Garfinkel, D. Malan, K. Dubec, C. Stevens, and C. Pham, "Disk Imaging with the Advanced Forensics Format, Library and Tools," *Proc. IFIP WG 11.9 Int. Conf. Digit. Forensics*, pp. 1–19, 2006.

[6] C. Forensic, "Storage Formats for Digital Evidence Evidence," 2015.

[7] J. L. Malone, "Fight crime. Unravel incidents ... one byte at a time.," *SANS Comput. Forensics*, p. 125, 2004.

[8] *EnCase Computer Forensics I*, I. Pasadena, California: Guidance Software, Inc., 2013.

[9] I. A. Ridlo, "Panduan pembuatan flowchart," p. 26, 2017.

Analisis Algoritma Akuisisi Digital Forensik Terbaik: AFF, RAW, dan E01

ORIGINALITY REPORT

8%	8%	7%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Muhammad Fajar Sidiq, Muhammad Nur Faiz. "Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital", Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2019 Publication	2%
2	Rusydi Umar, Anton Yudhana, Muhammad Nur Faiz. "Experimental Analysis of Web Browser Sessions Using Live Forensics Method", International Journal of Electrical and Computer Engineering (IJECE), 2018 Publication	2%
3	simson.net Internet Source	1%
4	Submitted to Liverpool John Moores University Student Paper	1%
5	Submitted to Universitas Jember Student Paper	1%

webeone.org

6	Internet Source	1%
7	pdfs.semanticscholar.org Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		