Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST

By ABDUL FADHIL

WORD COUNT 2488
TIME SUBMITTED 25-NOV-2019 12:57AM
PAPER ID 52366797

Available at https://jtsiskom.undip.ac.id (4 August 2019)
DOI: 10.14710/jtsiskom.7.3.2019.89-92

Jurnal Teknologi dan Sistem Komputer, 7(3), 2019, 89-92

Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST

Performance Comparison of Forensic Software for Carving Files using NIST Method

Doddy Teguh Yuwono[1)], Abdul Fadlil[*1,2)], Sunardi[1,2)]

[1)] *Magister Teknik Informatika, Universitas Ahmad Dahlan*
Jl. Prof. DR. Soepomo Sh, Warungboto, Umbulharjo, Yogyakarta, Daerah Istimewa Yogyakarta, Indonesia 55164

[2)] *Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan*
Jl. Prof. DR. Soepomo Sh, Warungboto, Umbulharjo, Yogyakarta, Daerah Istimewa Yogyakarta, Indonesia 55164

Cara sitasi: D. T. Yuwono, A. Fadlil, and S. Sunardi, "Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST," *Jurnal Teknologi dan Sistem Komputer*, vol. 7, no. 3, pp. 89-92, 2019. doi: 10.14710/jtsiskom.7.3.2019.89-92, [Online].

***Abstract** - Data lost due to the fast format or system crash will remain in the media sector of storage. Digital forensics needs proof and techniques for retrieving data lost in storage. This research studied the performance comparison of open-source forensic software for data retrieval, namely Scalpel, Foremost, and Autopsy, using the National Institute of Standards Technology (NIST) forensic method. The testing process was carried out using the file carving technique. The carving file results are analyzed based on the success rate (accuracy) of the forensic tools used in returning the data. Scalpel performed the highest accuracy for file carving of 100% success rate for 20 document files in pdf and Docx format, and 90% for 10 image files in png and jpeg format.*

***Keywords** - digital forensics; data retrieval tools; file carving; accuracy of forensic tools*

***Abstrak** - Data yang hilang karena format cepat atau sistem crash akan tetap ada di dalam sektor media penyimpanan. Forensik digital memerlukan bukti dan teknik pengembalian data yang tepat untuk mengembalikan data yang hilang dari media penyimpanan. Penelitian ini melakukan perbandingan performansi perangkat lunak forensik open source untuk mengembalikan data, yaitu Scalpel, Foremost dan Autopsy, menggunakan metode forensik National Institute of Standards Technology (NIST). Proses pengujian yang dilakukan menggunakan teknik file carving. Hasil file carving dianalisis dengan melihat tingkat keberhasilan (akurasi) alat forensik yang digunakan dalam pengembalian data. Scalpel menunjukkan akurasi file carving tertinggi dengan keberhasilan sebesar 100% untuk 20 file dokumen dalam format pdf dan Docx, dan 90% untuk file gambar dalam format png dan jpeg.*

***Kata Kunci** - forensik digital; perangkat lunak retrieval data; file carving; akurasi perangkat forensik*

[*)] Penulis korespondensi (Abdul Fadlil)
Email: fadlil@mti.uad.ac.id

I. PENDAHULUAN

Digital forensik digunakan untuk kepentingan memperoleh bukti hukum (*Pro Justice)*. Digital forensik menggunakan metode investigasi dan analisis data yang disimpan dan diambil dari perangkat penyimpanan untuk tujuan presentasi di pengadilan hukum, proses sipil atau administrasi. Digital forensik melibatkan suatu proses atau tahap mengumpulkan (koleksi), memeriksa (eksaminasi), menganalisa (analisa) dan mempresentasikan (*reporting*) bukti digital yang berkaitan dengan suatu kasus kejahatan digital menurut hukum yang berlaku [1].

Kejahatan *cyber* berupa aktivitas teknologi jaringan dijadikan alat atau media untuk melakukan kejahatan, seperti meretas jaringan, menghapus informasi, menyembunyikan informasi dan merusak informasi. Hasil kejahatan tersebut umumnya disembunyikan di media penyimpanan untuk dipergunakan dalam pencurian, pengintaian, *bullying*, terorisme, dan penipuan. Media penyimpanan data berfungsi sebagai alat atau media untuk menyimpan data atau program, dimana data atau program yang disimpan tersebut bisa dibuka, dibaca, diedit, dihapus, disembunyikan, dan diformat menggunakan komputer ataupun laptop. Penjahat *cyber* dalam menghilangkan jejaknya memilih menghapus, menyembunyikan dan memformat semua data-data yang dikumpulkan dalam tindak kejahatan yang dilakukannya [2].

Proses *delete*/menghapus suatu file tidak berarti menghapus data secara permanen dari media penyimpanan. Tetapi hanya memberitahukan kepada komputer bahwa ruang yang ditempati data tersebut tersedia untuk ditimpa/diisi oleh data yang lain. File ini dapat dengan mudah dikembalikan ke bentuk semula, bila belum tertimpa file lain [3]. Kapasitas penyimpanan yang semakin besar saat ini, memungkinkan orang

Submitted: 28 November 2018; Revised: 19 April 2019; Accepted: 22 July 2019; Published: 31 July 2019

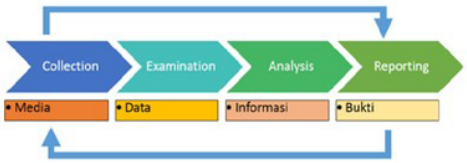
untuk menggunakan seluruh ruang harddisk, dan penimpaan hanya dilakukan ketika melakukan proses format. Sekalipun file dihapus, potongan-potongan file tersebut masih selamat dan tersimpan.

Jika sebuah dokumen berada pada *disk* dalam bentuk yang dikompres, maka dokumen tersebut tetap dalam bentuk ter-compress saat dihapus, dengan demikian pencarian di *disk* untuk sebuah kata kunci yang hanya ada di dalam file yang dihapus tidak akan membuahkan hasil. File yang sedikit terfragmentasi (terpecah-pecah) akan lebih mudah untuk dipulihkan. Penempatan file system yang baik memiliki lebih banyak manfaat, antara lain memungkinkan informasi yang terhapus dapat bertahan lebih lama daripada yang diduga [2], [4].

Suatu kasus kejahatan komputer dengan sistem operasi *proprietary* memunculkan permasalahan bagi penyidik dalam menemukan *file* dokumen, gambar, *history*, serta perubahan yang dilakukan oleh pelaku kejahatan pada suatu *drive* (media penyimpanan) [2], [5]. Suatu kasus kejahatan teknologi komputer yang terjadi akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas (*history*) yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti di media penyimpan utama yaitu berupa barang bukti elektronik dan barang bukti digital. Barang bukti elektronik dapat berupa bentuk fisik dari perangkat elektronik tersebut atau berupa media simpan (*storage device*), sedangkan barang bukti digital dapat berupa file dokumen, file gambar, *file* suara, *file* video, *history*, atau *file log* yang berisikan data-data terkait yang dapat dijadikan sebagai informasi pendukung dalam pengambil keputusan.

Pengangkatan barang bukti dapat dilakukan secara *dead forensic* dan *live forensic* [6]. Dead forensic membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan (harddisk). Live forensic menganalisis yang berjalan pada system atau data volatile yang tersimpan pada Random Access Memory (RAM) atau transit pada jaringan [7], [8]. Hasil analisa struktur dan isi folder serta aplikasi digunakan untuk mengungkap sebuah kasus kejahatan sesuai skenario percakapan yang telah dibuat pada bagian perancangan dan dilaksanakan pada bagian implementasi.

Metode yang digunakan beragam, di antaranya National Institute of Standards Technology (NIST) seperti halnya dalam [9]-[11] dan National Institute Of Justice (NIJ) dalam [12]. Belum banyak kajian yang membahas tentang kinerja perangkat lunak untuk pengembalian file yang terhapus, terformat dan tersembunyi untuk keperluan forensik digital seperti [13] yang membandingkan kinerja Scalpel dan Foremost. Penelitian ini berfokus pada analisis performansi perangkat lunak forensik Scalpel [14], Foremost dan Autopsy untuk mengembalikan *file carving* dalam mencari file dalam aliran data berdasarkan pengetahuan metadata format filenya dengan menggunakan metode NIST. Tipe file yang dikembalikan adalah tipe gambar JPG/JPEG dan PNG serta tipe dokumen Doc/Docx dan PDF.



Gambar 1. Alur kajian menggunakan NIST

Tabel 1. Tipe, format, dan jumlah file

Tipe File	Format File	Jumlah File	Ukuran (kB)
Gambar	JPG / JPEG	7 file	28 - 220
	PNG	3 file	270 - 2100
Dokumen	Doc / Docx	10 file	40 - 3200
	PDF	10 file	38 - 4900

II. Metode Penelitian

Analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital dalam kajian ini menggunakan metode NIST. Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, diekstrak data dari media dan diubah menjadi format yang bisa diproses oleh alat forensik. Data ditransformasikan menjadi informasi melalui analisis. Transformasi informasi menjadi bukti analogi dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan (Gambar 1).

Dalam tahap *collection*, dilakukan pelabelan, identifikasi, dan pengambilan data dari sumber data yang relevan. Proses ini menggunakan media penyimpanan flashdisk HP 8 GB. File sistem menggunakan FAT32. Tabel 1 menunjukkan tipe file, format file dan jumlah file dengan berbagai ukuran yang dimasukkan pada Flashdisk. Tipe file yang digunakan adalah file gambar PNG dan JPG/JPEG, file dokumen Doc / Docx dan file dokumen PDF berjumlah masing-masing 10 file.

Untuk menjalankan tahap berikutnya, dilakukan skenario penghapusan dan pemformatan file gambar, dokumen dan PDF. Ketika data dihapus, tidak ada satupun data yang didapat dan terlihat di aplikasi *file explorer*. Media penyimpan digandakan (*cloning*) dan hasil kloningan diujikan menggunakan perangkat lunak Scalpel, Foremost dan Autopsy. Tabel 2 menunjukkan alat dan bahan yang digunakan pada penelitian ini.

III. Hasil dan Pembahasan

Data-data yang telah dihapus dan diformat pada media penyimpanan diujikan dan dianalisis menggunakan perangkat lunak forensic Scalpel, Foremost dan Autopsy. Sebelum melakukan proses *cloning* media penyimpanan, dilakukan pengecekan posisi media penyimpanan yang telah terhapus tersebut. Proses ini merupakan tahapan untuk memastikan bahwa tidak adanya perubahan data terhadap file digital diakibatkan oleh aktifitas *recovery file carving*.

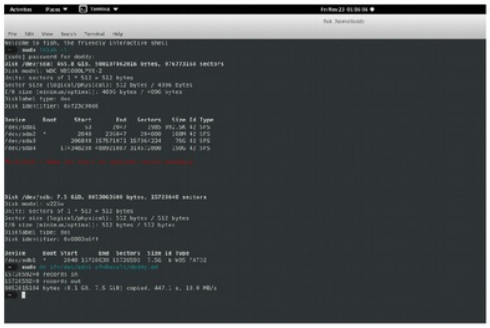
Tabel 2. Alat dan bahan penelitian

No	Nama	Spesifikasi	Keterangan
1	Laptop	Acer Aspire E 14	Hardware
2	Sistem Operasi	Arc-Linux	OS
3	USB FlashDisk	HP 8 Gb	Hardware
4	Scalpel	Aplikasi Forensic OpenSource	Software
5	Foremost	Aplikasi Forensic OpenSource	Software
6	Autopsy	Aplikasi Forensic OpenSource	Software

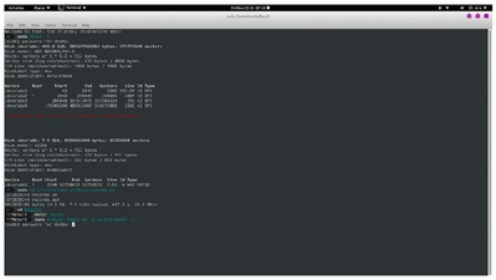
Cloning ini ditujukan untuk menjaga aspek *integrity* (keaslian data) pada data duplikasi akan identik dengan data yang asli. Dibandingkan jika dilakukan proses *logical backup*, bisa terjadi perubahan terhadap *timestamps* dokumen atau malah merubah keaslian dari data. Tahapan awal dalam proses *cloning* adalah pengecekan *directory* media penyimpanan. Flashdisk USB yang dialiaskan dengan /dev/sdb1 untuk dikloning . Informasi media diperoleh dengan perintah *fdisk -l* dan proses kloning dilakukan dengan perintah *dd if=/dev/sdb1 of=Result/doddy.dd* (Gambar 2). Hasil kloning diletakkan dalam folder *Result/doddy.dd* di media penyimpan lokal. Folder baru dibuat untuk menampung hasil dari *file carving recovery*.

Proses *recovery* dilakukan untuk mengembalikan file carving. File carving ini berisi kumpulan file-file yang telah dihapus, disembunyikan dan diformat sehingga file tidak utuh dan perlu disusun ulang secara terstruktur agar dapat kembali utuh seperti file awalnya yang bisa dibuka, dibaca, diedit dan digunakan sebagaimana mestinya [3]. Proses pengembalian *file carving* ini dilakukan dengan menggunakan Scalpel, Foremost dan Autospy. Proses pengembalian *file carving* menggunakan Scalpel ditunjukkan dalam Gambar 3. Pada proses analisis setelah pengembalian *file carving*, dalam folder output ditemukan folder baru yang merupakan folder utama yang berisi file-file yang berhasil dikembalikan sesuai dengan perangkat lunak forensik yang digunakan. *Autopsy* berhasil menemukan semua file pada *sector* penyimpanan, namun statusnya *corrupt*. *Autopsy* dapat dimaksimalkan dengan memodifikasinya menggunakan pemrograman *Phyton.*

Tingkat keberhasilan / akurasi proses *file carving* oleh tiap alat forensik, yaitu Scalpel, Foremost, dan Autopsy dinyatakan dalam Tabel 3 dan Tabel 4. Nilai Akurasi diukur dari sebelum dan sesudah proses forensik dilakukan. Scalpel memiliki performa yang lebih baik dibandingkan alat forensik lain untuk mengembalikan file gambar dan PDF. Hal ini selaras dengan yang dinyatakan dalam [13]. Dibandingkan Foremost dan Autospy yang hanya sekali, Scappel menelusuri tiap disk image (hasil kloning) dua kali secara berurutan [14]. Pada proses penelusuran pertama Scalpel akan membaca keseluruhan hasil kloning dalam potongan yang besar dengan nilai default sebesar 10MB. Setelah Scalpel memiliki indeks yang lengkap dari header dan footer, maka dengan header dan footer



Gambar 2. Proses penggalian informasi media dan proses kloning



Gambar 3. Proses pengembalian *file carving*

Tabel 3. Jumlah file yang berhasil dikembalikan

Tipe File	Format File	Pengembalian File		
		Scalpel	Foremost	Autopsy
Gambar	JPG / JPEG	7 file	6 file	7 file (corrupt)
	PNG	3 file	3 file	3 file (corrupt)
Dokumen	Doc / Docx	8 file	9 file	10 file (corrupt)
	PDF	10 file	10 file	10 file (corrupt)

Tabel 4. Akurasi proses pengembalian file carving

Tipe File	Format	Pengembalian File		
		Scalpel	Foremost	Autopsy
Gambar	JPG / JPEG	100%	86%	0
	PNG	100%	100%	0
Dokumen	Doc / Docx	80%	90%	0
	PDF	100%	100%	0

yang masih belum berhasil digabungkan untuk membentuk atau menghasilkan suatu file digunakan untuk mengisi satu set pekerjaan berurut yang mengendalikan operasi *file carving* selama penelusuran kedua. Foremost hanya melakukan pencarian berdasarkan potongan memori tanpa ada pengulangan

jika terdapat *header* dan *footer* yang berbeda potongan memorinya. Autopsy mengembalikan file sesuai dengan format file awal sebelum hilang karena terhapus ataupun terformat. Namun, Autopsy tidak memiliki kemampuan untuk memperbaiki file yang dikembalikan tadi jika file yang dikembalikan mengalami *corrupt*/rusak.

Pada ketiga perangkat lunak yang diuji tidak didapatkan laporan (*report*) secara otomatis sehingga investigator yang menggunakan perangkat lunak harus membuat laporan secara manual. Penggunaan perangkat lunak forensik Scalpel, Foremost dan Autopsy pada saat proses forensik digital memberikan laporan hasil audit yang menjelaskan semua tahapan dan proses dalam mendapatkan dan mengembalikan file yang telah dihapus, disembunyikan dan diformat. Hal ini dapat membantu para penegak hukum dalam menyajikan file-file yang berisi informasi kejahatan yang dikumpulkan oleh penjahat *cyber*, baik yang telah dihapus, disembunyikan dan diformat untuk mendapatkan bukti digital seperti dalam [1]-[6]. Pengembalian *file carving* ini dapat diterapkan pada media penyimpanan selain flash disk dalam berbagai format *filesystem*.

IV. KESIMPULAN

Dalam kerangka NIST untuk pengembalian *file carving*, alat bantu forensik *Scalpel* memiliki keunggulan dibandingkan *Foremost* dan *Autopsy* dalam pengembalian file-file yang terhapus, tersembunyi, dan terformat sehingga file-file tersebut dapat dipergunakan sebagaimana fungsinya.

DAFTAR PUSTAKA

[1] V. Rosalina, A. Suhendarsah, and M. Natsir, "Analisis Data Recovery Menggunakan Software Forensic : Winhex and X-Ways Forensic," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 3, no. 1, pp. 51-57, 2016.

[2] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (NIJ)," *ELINVO (Electronics, Informatics and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018.

[3] R. R. Oommen and P. Sulthan, "Recovering Deleted Files from NTFS," *International Journal of Science and Research*, vol. 5, no. 5, pp. 205-208, 2016.

[4] A. Chandsarkar and S. Patil, "Simplifying Data Recovery with Advance Techniques and Operations," *International Journal of Computer Science and Technology*, vol. 7, no. 4, pp. 217-221, 2016.

[5] F. Albanna and I. Riadi, "Forensic Analysis of Frozen Hard Drive using Static Forensics Method," *International Journal of Computer Science and Information Security*, vol. 15, no. 1, pp. 173-178, 2017.

[6] I. Riadi and E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *Jurnal Teknik Elektro*, vol. 10, no. 1, pp. 18-22, 2018.

[7] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *ILKOM Jurnal Ilmiah*, vol. 8, no. 3, pp. 242-247, 2016.

[8] S. Soni, Y. Prayudi, and B. Sugiantoro, "Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic," *Teknomatika*, vol. 9, no. 2, pp. 1-13, 2017.

[9] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *Information Technology Journal Research and Development*, vol. 3, no. 1, pp. 13-21, 2018.

[10] I. Riadi *et al.*, "Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute Of Standards And Technology (NIST)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 4, no. 2, pp. 161-166, 2017.

[11] I. Riadi, Sunardi, and A. Firdonsyah, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *International Journal of Cyber-Security and Digital Forensic*, vol. 16, no. 4, pp. 198-205, 2017.

[12] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *Jurnal Teknologi Informatika dan Sistem Informasi*, vol. 4, no. 2, pp. 219-227, 2018.

[13] R. Muttaqin, A. Arini, and F. Mintarsih, "Perbandingan Carving Tools Foremost dan Scalpel," *Jurnal Teknik Informatika*, vol. 8, no. 1, pp. 63-72, 2015.

[14] G. G. Richard and V. Roussev, "Scalpel: A Frugal, High Performance File Carver," in *2005 Digital Forensic Research Workshop (DFRWS)*, USA, New Orleans, 2005, pp. 1-10.

Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST

ORIGINALITY REPORT

20%

SIMILARITY INDEX

PRIMARY SOURCES

1	pt.scribd.com Internet	130 words — 5%
2	jtsiskom.undip.ac.id Internet	100 words — 4%
3	journal.uir.ac.id Internet	54 words — 2%
4	www.researchgate.net Internet	37 words — 1%
5	jurnal.uisu.ac.id Internet	31 words — 1%
6	kinetik.umm.ac.id Internet	25 words — 1%
7	Sunardi -, Imam Riadi, Andi Sugandi. "Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework", International Journal of Advanced Computer Science and Applications, 2019 Crossref	18 words — 1%
8	www.iaescore.com Internet	17 words — 1%
9	www.ejournal.org.cn Internet	12 words — < 1%
10	www.scmsgroup.org	

	Internet	11 words — < 1 %
11	d-nb.info Internet	11 words — < 1%
12	lppm.nusamandiri.ac.id Internet	11 words — < 1%
13	www.teknody.com Internet	11 words — < 1%
14	jurnal.mdp.ac.id Internet	10 words — < 1%
15	journal.uny.ac.id Internet	10 words — < 1%
16	journal.unnes.ac.id Internet	8 words — < 1%
17	kursorjournal.org Internet	8 words — < 1%
18	publikasiilmiah.unwahas.ac.id Internet	8 words — < 1%
19	budi.insan.co.id Internet	8 words — < 1%
20	Arif Hidayat, Sudarmaji ., Dharmawan ., Dedi Irawan, Lilik Joko Susanto, Mustika ., Hadi Pranoto. "Comparative Analysis Of Applications OSforensics, GetDataBack, Genius and Diskdigger On Digital Data Recovery in the Computer Device", International Journal of Engineering & Technology, 2018 Crossref	4 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		