ANALISIS *FILE CARVING PADA FILE SYSTEM DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)*

Doddy Teguh Yuwono[1], Siti Juhairiah[2], Sonedi[3]
Ilmu Komputer[1], PGSD[2], Pendidikan Ekonomi[3]
Universitas Muhammadiyah Palangkaraya [1,2,3]
doddy.zha09@gmail.com[1], sitijuhairiah.mpd@gmail.com[2] , sonedi.lilik@gmail.com[3]

ABSTRACT

Data recovery is the most important part of Digital Forensic. For investigators to produce evidence in court is very important, so that all types of data from Flash Memory or Hard Drive that are hidden, deleted and even formatted must be found. The basic principle of data, if it has ever been copied on a Flash Memory or Hard Drive, will never be permanently lost and even data that is lost due to deleted, formatted quickly or a system crash. So returning data is very possible. In this research, the tools used are FTK *Imager and Autopsy, which are Opensource Tools that can be used on Proprietary and Opensource operating systems. The method used is the National Institute of Standards Technology (NIST). NIST has an excellent work guide on policies and standards to ensure each Examiner follows the same workflow so that their work is documented and the results can be reviewed and can be maintained when reporting. The results of this study prove that* FTK *Imager and Autopsy tools can restore deleted, hidden and formatted data.*

Keywords: *Autopsy, Digital Forensic, Examiner,* FTK *Imager, NIST*

ABSTRAK

Pengembalian data adalah bagian terpenting dari Digital Forensic. Bagi penyidik untuk menghasilkan bukti di pengadilan adalah hal yang sangat penting, sehingga semua jenis data dari Flash Memory atau Hard Drive yang disembunyikan, dihapus bahkan diformat harus ditemukan. Prinsip dasar dari data jika sudah pernah dicopy pada Flash Memory atau Hard Drive tidak akan pernah hilang secara permanen dan bahkan data yang hilang karena dihapus, diformat cepat ataupun sistem crash. Sehingga pengembalian data sangat memungkinkan. Pada penelitian ini tool yang digunakan adalah FTK Imager dan Autopsy, yang merupakan Tools Opensource yang dapat digunakan pada system operasi Proprietary maupun Opensource. Metode yang digunakan yaitu *National Institute Of Standards Technology* (NIST). NIST memiliki panduan kerja yang sangat baik dalam kebijakan dan standar untuk menjamin setiap Examiner mengikuti alur kerja yang sama, sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di kaji ulang dan dapat dipertahankan ketika pelaporan. Hasil penelitian ini membuktikan tools FTK Imager dan Autopsy dapat mengembalikan data-data yeng telah terhapus, tersembunyi dan terformat..

Kata Kunci: *Autopsy, Digital Forensic, Examiner,* FTK *Imager,* NIST

PENDAHULUAN

Digital forensik adalah metode investigasi dan analisis data yang disimpan dan diambil dari perangkat penyimpanan untuk tujuan presentasi di pengadilan hukum, proses sipil atau administrasi. Digital forensik adalah disiplin gabungan dari ilmu pengetahuan dan perkembangan teknologi komputer untuk kepentingan memperoleh bukti hukum (*Pro Justice*). Digital forensik melibatkan suatu proses atau tahapan seperti mengumpulkan (*Collection*), memeriksa (*Examination*), menganalisa (*Analysis*) dan mempresentasikan (*Reporting*) sesuatu yang diperoleh secara digital sehingga dapat menjadi bukti digital yang berkaitan dengan suatu kasus kejahatan digital sesuai dengan hukum yang berlaku.(Albanna and Riadi, 2017)

Kejahatan *Cyber* adalah sebuah aktivitas yang menjadikan teknologi sebagai alat atau media untuk melakukan kejahatan, seperti meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi dan merusak informasi. Hasil kejahatan tersebut umumnya disembunyikan di media penyimpanan untuk dipergunakan dalam pencurian, pengintaian, bullying dan penipuan. Media Penyimpanan adalah perangkat atau alat yang memiliki fungsi untuk menyimpan data atau program, dimana data atau program yang disimpan tersebut tetap

bisa dibuka, dibaca, diedit, dihapus, disembunyikan, diformat menggunakan komputer ataupun laptop. Penjahat *Cyber* dalam menutupi ataupun menghilangkan jejaknya cenderung memilih untuk menghapus, menyembunyikan dan memformat semua data-data yang dikumpulkan dalam tindak kejahatan yang dilakukannya.(Rana *et al.*, 2017)

Pada proses delete/menghapus suatu file sebenarnya file tersebut tidak berarti data tersebut terhapus secara permanen dari media penyimpanan. Tetapi hanya memberitahukan kepada komputer bahwa ruang yang ditempati data tersebut tersedia untuk ditimpa/diisi/dioverwrite oleh data yang lain. Sehingga File tersebut dapat dikembalikan dengan mudah ke bentuk semula, dengan syarat belum ditimpa file yang lain. Kapasitas media penyimpanan yang terus berkembang memiliki kapasitas penyimpanan yang semakin besar pula, Hal tersebut memungkinkan penggunanya untuk menggunakan seluruh ruang penyimpanan yang tersedia, Sehingga proses *overwrite* cenderung hanya dilakukan pada proses format.(Putra, Fadlil and Riadi, 2017)

Hal tersebut menyebabkan file-file yang dihapus, menyisakan potongan-potongan file yang masih selamat dan tersimpan meskipun tidak utuh. Jika diibaratkan sebuah file yang dicompress berada pada media penyimpanan, file yang ter-compress saat dihapus tersebut akan tetap berada dalam bentuknya. Pencarian di media penyimpanan tidak akan memberikan hasil. Meskipun telah memasukkan sebuah kata kunci yang terdapat pada file yang dihapus tersebut. File yang mengalami sedikit *fragmentasi* (terpecah-pecah) cenderung akan lebih mudah untuk dipulihkan/ direcover (Yuwono, Fadlil and Sunardi, 2019). Penempatan *File System* yang baik memberikan lebih banyak manfaat, diantaranya informasi yang terhapus atau dihapus dapat bertahan lebih lama daripada yang yang diduga oleh penggunanya. (Yudhana, Riadi and Anshori, 2018)

File System atau lebih dikenal dengan sistem berkas merupakan penerapan dari struktur logika dalam mengendalikan akses-akses terhadap file-file yang ada pada media penyimpanan. Suatu *File System*, terdiri dari berbagai jenis dan setiap jenis menggunakan algoritma yang berbeda antara satu dengan yang lainnya. Semakin baru jenis dari *File System*, maka *File System* tersebut akan memiliki kualitas yang semakin bagus pula. Misalnya jenis FAT (*File Allocation Table*), Jenis partisi yang dijumpai pada OS (*Operating System*) Windows ini telah mengalami perubahan sampai pada Jenis FAT-32 dan diteruskan dengan jenis NTFS (*New Technology File System*).(Mahant and Meshram, 2012)

Umumnya media penyimpanan seperti USB Flashdisk, SD Card dan tipe memori external lainnya menggunakan Jenis *File System* ini untuk melakukan formating system. *File System* jenis FAT adalah salah satu jenis *File System* yang paling lama digunakan, sehingga penggunaanya sudah sangat umum mengetahuinya sejak masa komputer menggunakan OS DOS di tahun 80-an sampai tahun 90-an. *File System* FAT-32 merupakan jenis default dari *File System* ketika akan memformat flashdisk / microSD melalui komputer yang menggunakan OS Propietary. Hal ini dikarenakan *File System* FAT-32 cukup fleksibel sehingga dapat dibaca hampir di semua OS. (Oommen and Sugathan, 2016)

Microsoft, yang merupakan produsen dari OS Windows memperkenalkan NTFS. NTFS merupkan *File System* standar yang digunakan untuk media penyimpanan pada Hard Disk dan SSD di OS Windows. NTFS dipilih karena memiliki kecepatan proses transfer data yang baik dan tentunya dukungan dari Microsoft. Meski pada media penyimpanan Hard Disk secara standard menggunakan *File System* jenis NTFS, media penyimpanan lain seperti Flash disk juga dapat menerapkan NTFS. Penggunaan NTFS pada flashdisk umumnya dibutuhkan ketika akan membuat bootable media. Misalnya untuk membuat paket installasi OS.(Riadi, Sunardi; and Rauli, 2018)

Metode *Dead Forensic* dan *Live Forensic* adalah metode yang sudah tidak asing lagi dalam proses pengangkatan barang bukti digital. Metode *Dead forensic* adalah suatu teknik yang mengangkat atau mengambil data yang tersimpan secara permanen dalam media penyimpanan. Sedangkan Metode *Live forensic* adalah suatu teknik analisis yang berhubungan dengan data

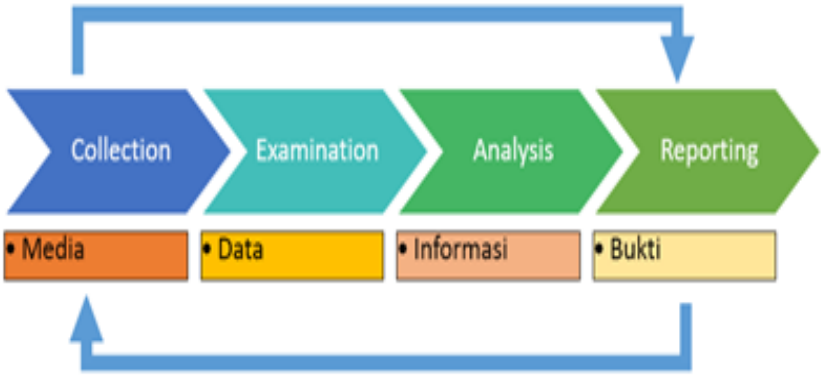
yang berjalan pada system maupun data volatile yang biasanya tersimpan pada *Random Access Memory* (RAM).(Nur Faiz, Umar and Yudhana, 2016)(Soni, Prayudi and Sugiantoro, 2017)

Hasil analisa struktur data, isi dari folder serta susunan dari aplikasi menjadi jawaban dalam mengungkap kasus kejahatan digital sesuai dengan skenario yang telah dibuat pada bagian perancangan, kemudian dilaksanakan pada bagian implementasi, serta di Analisa sehingga barang bukti digital yang meliputi pengumpulan data-data digital bersifat penting dapat disajikan dan dapat dilaporkan sebagai barang bukti digital (Riadi, Umar and Nasrulloh, 2018).

Berdasarkan latar belakang masalah yang dijabarkan, penelitian ini memfokuskan pada analisis *File Carving* yang merupakan proses mencari file dalam aliran data berdasarkan pengetahuan format filenya pada *File System* tertentu, daripada metadatanya dengan menggunakan metode NIST (*National Institute of Standards Technology*) (Riadi, Sunardi; and Firdonsyah, 2017; Riadi *et al.*, 2018). Penelitian yang dilakukan menggunakan *tool forensic* bernama FTK Imager dan Autopsy yang merupakan tool Opensource yang dapat digunakan pada OS *Propietary* ataupun *Opensource*.

METODE PENELITIAN

Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST. Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari Media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, 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.(Riadi, Sunardi; and Firdonsyah, 2017; Yudhana, Riadi and Anshori, 2018; Yuwono, Fadlil and Sunardi, 2019)



Gambar 2. Metode NIST

Berdasarkan gambar 1 hal ini dapat dijelaskan tahap selular Forensik Analisis sebagai berikut:

1. Collection adalah pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan dengan prosedur yang tepat agar tidak mengubah keaslian data dan untuk menjaga integritas data.
2. Examination adalah pengolahan data yang dikumpulkan, pada tahap ini adalah bagaimana penggunaan forensik kombinasi dari berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai kebutuhan penelitian sambil mempertahankan integritas data.
3. Analysis adalah tahapan dari pemeriksaan hasil dengan menggunakan metode teknis yang dibenarkan sesuai prosedur dan hukum.
4. Reporting adalah melaporkan hasil analisis yang meliputi persiapan, pengujian, penggambaran tindakan yang dilakukan, serta hasil yang diperoleh dari penelitian

HASIL DAN PEMBAHASAN

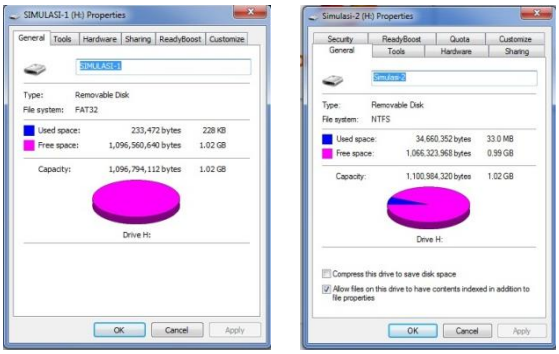
Dari penelitian yang dilakukan, dengan menggunakan tool forensic FTK Imager dan Autopsy diperoleh hasil berupa data-data yang telah dihapus maupun diformat pada media penyimpanan. Berikut adalah tabel 1 informasi tentang OS, hardware dan software yang diperlukan pada penelitian ini.

Tabel 1. Alat dan Bahan

No	Nama	Spesifikasi	Keterangan
1	Laptop	Acer Aspire E 14	Hardware
2	Sistem Operasi	Arc-Linux	OS
3	USB FlashDisk	Sandisk 1 Gb	Hardware
4	FTK Imager	Aplikasi Forensic OpenSource	Software
5	Autopsy	Aplikasi Forensic OpenSource	Software

A. *Collection*

Pada proses simulasi *collection* menggunakan media penyimpanan Flashdisk Sandisk yang diatur dengan kapasitas penyimpanan sebesar 1 Gb. *File system* digunakan untuk penelitian menggunakan FAT-32 dan NTFS.

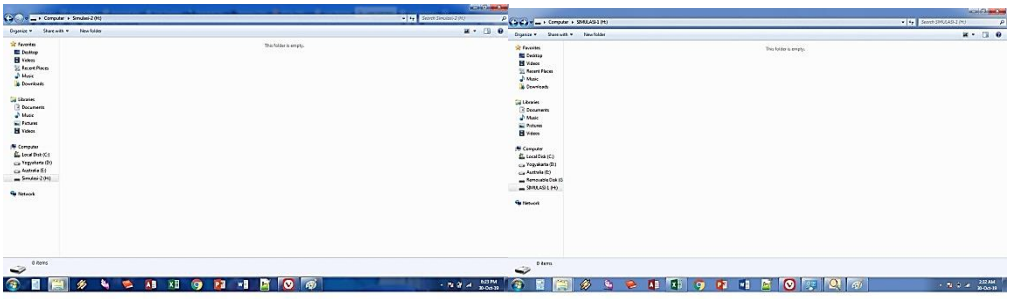


Gambar 3. Media Penyimpanan dengan *File system* FAT32 dan NTFS

Pada Gambar 2 merupakan properties tentang informasi Media penyimpanan Flashdisk 1 Gb dan file system yang digunakan adalah FAT32 dan NTFS yang digunakan dalam penelitian. Flashdisk yang digunakan telah diisi beberapa file gambar.

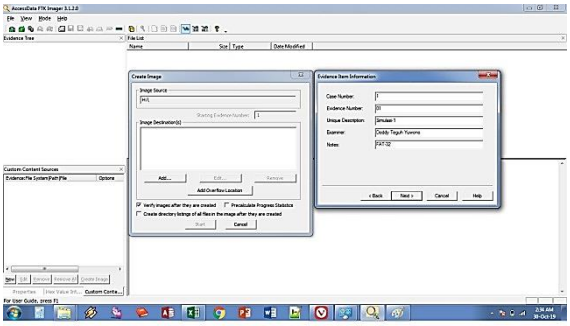
B. *Examination*

Pada proses examination merupakan pengujian pada Media penyimpanan Flashdisk dengan merk *Sandisk* yang memiliki kapasitas penyimpanan sebesar 1 Gb menggunakan tool *Autopsy*.



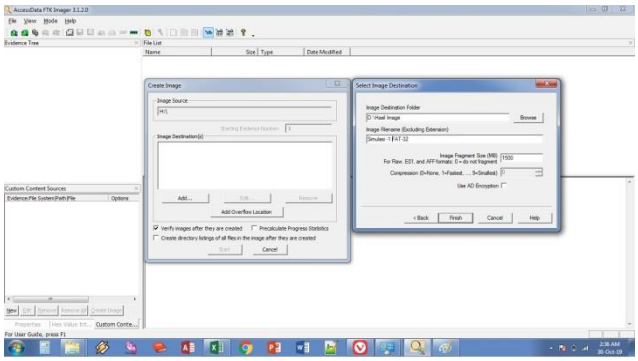
Gambar 3. Media Penyimpanan *Empty* pada *file system FAT32* dan *NTFS*

Pada gambar 3, merupakan tampilan dari isi media penyimpanan yang telah kosong karena dihapus file-file yang ada didalamnya dan diformat. Selanjutnya adalah proses *cloning* media penyimpanan, proses ini merupakan tahapan untuk memastikan bahwa tidak adanya perubahan data terhadap file digital diakibatkan oleh aktifitas *recovery file carving*. *Cloning* yang ditujukan untuk menjaga aspek *integrity* pada data duplikasi akan identik dengan data yang asli dengan menggunakan FTK *Imager*. Jika dilakukan proses *logical backup* ditakutkan akan terjadi perubahan terhadap *time stamps* dokumen atau malah merubah keaslian dari data. Tahapan awal dalam proses *cloning* adalah pengecekan *directory* media penyimpanan seperti pada gambar 4.



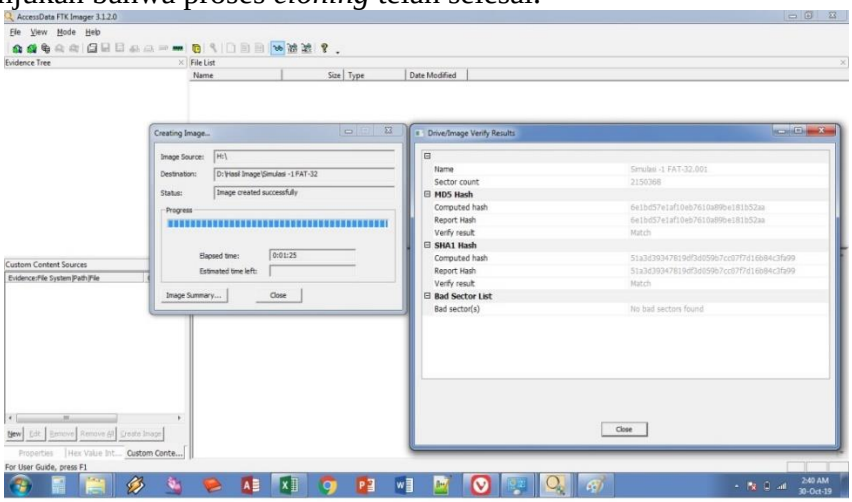
Gambar 4. Pengecekan *Directory* Media Penyimpanan

setelah mengetahui posisi directory media penyimpanan yang akan di *cloning*, tentukan folder yang menjadi tempat untuk meletakkan hasil *output* dari *cloning* media penyimpanan. seperti pada Gambar 5.



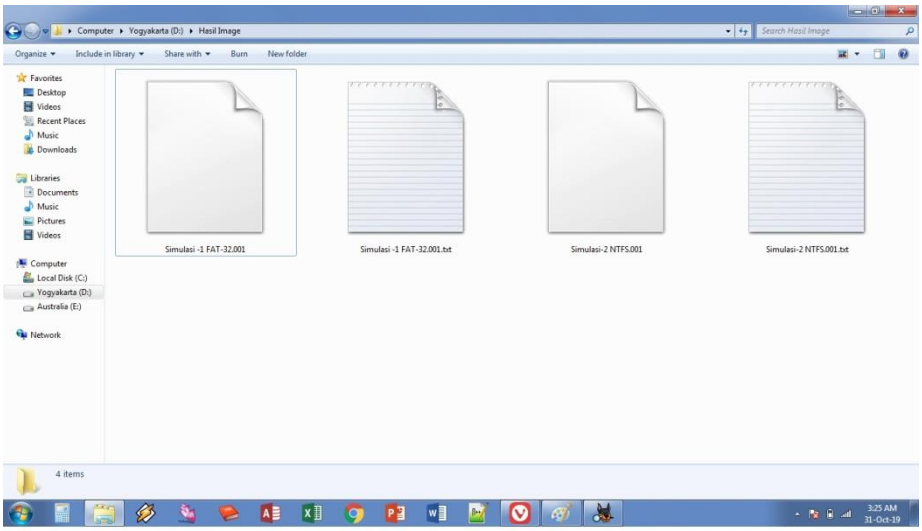
Gambar 5. Proses *Cloning* Media Penyimpanan

Gambar 6, menunjukan bahwa proses *cloning* telah selesai.



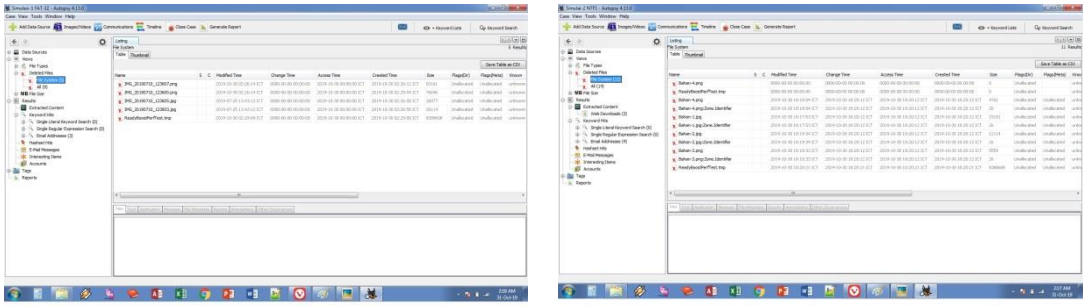
Gambar 6. *Proses* Cloning *telah selesai*

Pada Gambar 7, menunjukan hasil *cloning* dari media penyimpan .



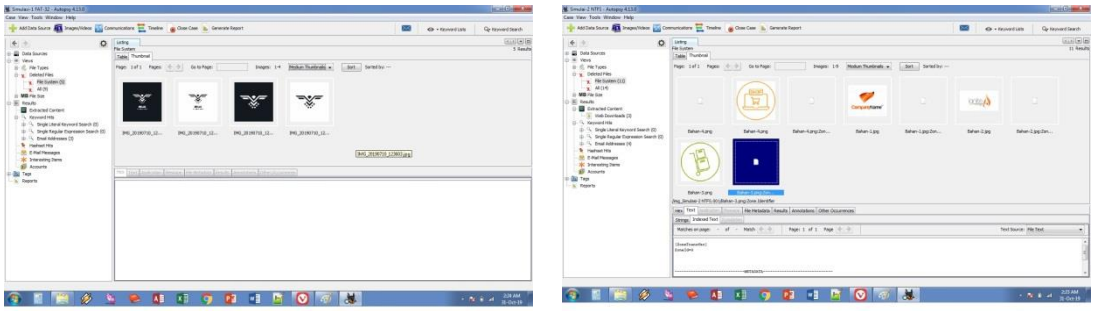
Gambar 7. *File* hasil *Cloning*

Pada gambar 8, proses pengembalian File Carving, *file carving* sendiri adalah 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.(Mahant and Meshram, 2012)



Gambar 8. Proses Pengembalian *File Carving* Pada FAT32 dan NTFS

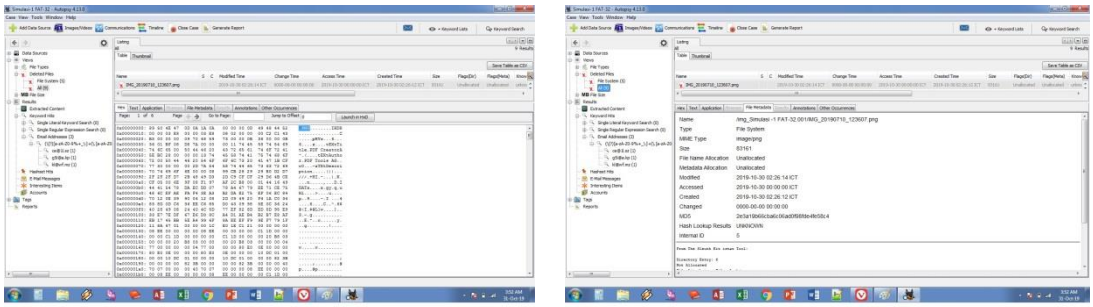
Pada gambar 9, *recovery file carving* menggunakan *Autopsy* diproses dan selesai mengembalikan semua file-file yang pernah di simpan menggunakan media penyimpanan yang diujikan.



Gambar 9. *Recovery File Carving* Selesai

C. *Analysis*

Pada proses *analysis* file-file yang telah dikembalikan dengan menggunakan tool *Autopsy* seperti pada gambar 9 akan dicek *Time stamps*-nya.



Gambar 9. Pengecekan *Time Stamps* Hasil *Recovery File Carving*

Pada gambar 9, terlihat beberapa Penjelasan seperti *Extensi* dari file, kemudian Metadanya serta *Hash* yang digunakan untuk mencocokan keutuhan dari file yang berhasil di *Recovery*.

D. *Reporting*

Pada tahap *reporting* merupakan hasil analisis yang telah dilakukan, berikut hasil yang telah ditemukan dari proses *Recovery File Carving* ini terdapat pada Tabel 2.

Tabel 2. Hasil tool *Autopsy*

No	Nama	Keterangan	
		FAT32	NTFS
1.	File Dihapus	Berhasil	Berhasil
2.	File Disembunyikan	Berhasil	Berhasil
3	File Diformat	Berhasil	Berhasil

Pada tahap ini telah dilakukan skenario yaitu beberapa file gambar, dihapus, disembunyikan dan diformat, ketika data dihapus dan diformat tidak ada satupun data yang didapat, setelah dikloning dengan FTK *Imager* dan menggunakan tool *Autopsy* dapat menampilkan file-file yang telah dihapus dan diformat. Kelebihan menggunakan *Autopsy* pada saat proses *forensic* media penyimpanan, *Autopsy* memberikan laporan hasil audit yang menjelaskan semua tahapan dan proses analisa dalam mendapatkan dan mengembalikan file yang telah dihapus, disembunyikan dan diformat.

KESIMPULAN

Penggunaan *software forensic* FTK *Imager* dan *Autopsy* memiliki keunggulan dalam pengembalian file-file yang terhapus, tersembunyi dan terformat, sehingga file-file tersebut dapat dipergunakan sebagaimana fungsinya. Software 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. Metode yang digunakan untuk melakukan analisis terhadap file carving atau tahapan untuk mendapatkan informasi dari file carving yaitu dengan metode *National Institute of Standards Technology* (NIST). Penelitian ini memberikan hasil berupa *file-file* yang dihapus, disembunyikan dan diformat pada dua jenis *File system* berhasil dikembalikan. Jika dibandingkan dengan *tools Forensics* sejenisnya FTK *imager* dan *Autopsy* memiliki kelebihan dari sisi tampilan dan kemudahan penggunaannya.

DAFTAR PUSTAKA

Albanna, F. and Riadi, I. (2017) 'Forensic Analysis of Frozen Hard Drive Using Static Forensics Method', *International Journal of Computer Science and Information Security*, 15(1), pp. 173–178.

Mahant, S. H. and Meshram, B. B. (2012) 'NTFS Deleted Files Recovery: Forensics View', *IRACST -International Journal of Computer Science and Information Technology & Security*, 2(3), pp. 491–497. Available at: http://ijcsits.org/papers/Vol2no32012/1vol2no3.pdf.

Nur Faiz, M., Umar, R. and Yudhana, A. (2016) 'Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary', *Jurnal Ilmiah ILKOM*, 8(3), pp. 242–247.

Oommen, R. R. and Sugathan, P. (2016) 'Recovering Deleted Files from NTFS', *International Journal of Science and Research (IJSR)*, 5(5), pp. 205–208. doi: 10.21275/v5i5.nov163235.

Putra, R. A., Fadlil, A. and Riadi, I. (2017) 'Forensik Mobile Pada Smartwach Berbasis Android', *Jurti*, pp. 41–47. doi: 25798790.

Rana, N. *et al.* (2017) 'Taxonomy of Digital Forensics : Investigation Tools and Challenges Department of Computer Science and Engineering Accendere Knowledge Management Services Pvt . Ltd ., India', *Computers and Society*. Available at: https://arxiv.org/ftp/arxiv/papers/1709/1709.06529.pdf.

Riadi, I. *et al.* (2018) 'Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method', 5(2), pp. 235–247.

Riadi, I., Sunardi; and Firdonsyah, A. (2017) 'Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework', *International Journal of Cyber-Security and Digital Forensics*, 16(4), pp. 198–205. doi: 10.17781/P002306.

Riadi, I., Sunardi; and Rauli, E. (2018) 'Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics', *Scientific Journal of Informatics (SJI) UNNES*, 10(1), pp. 18–22.

Riadi, I., Umar, R. and Nasrulloh, I. M. (2018) 'Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij)', 3(May), pp. 70–82. doi: 10.21831/elinvo.v3i1.19308.

Soni, Prayudi, Y. and Sugiantoro, B. (2017) 'Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic', *Teknomatika*, 9(2).

Yudhana, A., Riadi, I. and Anshori, I. (2018) 'Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist', 3(1), pp. 13–21.

Yuwono, D. T., Fadlil, A. and Sunardi (2019) 'Performance Comparison of Forensic Software for Carving Files using National Institute of Standards and Technology (NIST) Method', *Jurnal Teknologi dan Sistem Komputer*, 7(03). doi: 10.14710/jtsiskom.7.3.2019.%p.