**JUSTINDO**
**Jurnal Sistem dan Teknologi Informasi**
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO
E-ISSN: 25541-5735, P-ISSN: 2502-5724
*Volume 6, No. 2, Agustus 2021*

# Analisis Perbandingan Perangkat Lunak Forensik Digital untuk *File Carving* dalam Mengungkap Barang Bukti Digital

**Arvin Kynan Pratama[1], Carudin Carudin[2], Dadang Yusup[3]**

*Universitas Singaperbangsa Karawang*
*Email: [1]arvin.kynan17061@student.unsika.ac.id*

(Naskah masuk: 25 Mei 2021, diterima: 8 Juli 2021, diterbitkan: 30 Agutus 2021)

**ABSTRAK**

Kejahatan siber merupakan penyalahgunaan teknologi untuk dijadikan alat atau media dalam melakukan tindak kejahatan seperti meretas, mencuri, menghapus, menyembunyikan, dan merusak informasi. Pelaku kejahatan siber cenderung akan menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan untuk menghilangkan jejak barang bukti digital. Dalam ilmu forensik digital, kehilangan data dari media penyimpanan dapat diatasi dengan teknik *file carving*. Oleh karena itu penelitian ini bertujuan untuk mengetahui hasil proses *file carving* dalam mengungkap barang bukti digital dan mengevaluasi kinerja perangkat lunak forensik digital yang digunakan meliputi *Autopsy*, *PhotoRec*, *Scalpel*, dan *Foremost* berdasarkan 3 parameter penilaian dengan 3 skenario berbeda. Metodologi yang digunakan dalam proses analisis adalah *National Institute of Justice* (NIJ) yang terdiri dari 5 tahapan metode, yaitu *identification*, *collection*, *examination*, *analysis*, *reporting*. Hasil penelitian yang diperoleh menunjukkan pada skenario 1 *PhotoRec* dan *Autopsy* memiliki persentase kinerja dan kecepatan terbaik. Pada skenario 2 *PhotoRec* menjadi yang terbaik disusul dengan *Foremost* dan *Scalpel*, sedangkan *Autopsy* memiliki kinerja nihil. Pada skenario 3 *PhotoRec* dan *Autopsy* memiliki persentase kinerja yang terbaik, tetapi *Autopsy* memiliki kecepatan paling lambat dibandingkan ketiga perangkat lunak lainnya. Mengacu pada hasil penelitian, dapat disimpulkan hasil dari analisis *file carving* menunjukkan perangkat lunak *PhotoRec* mampu memenuhi semua skenario dan parameter penilaian dengan kinerja rata-rata pemulihan barang bukti digital sebesar 90,8%, sedangkan kinerja perangkat lunak lainnya adalah *Autopsy* sebesar 64,17%, *Foremost* 30%, dan *Scalpel* 0%.

**Kata kunci**: *Barang Bukti Digital, File Carving, Forensik Digital, Perangkat Lunak*

***ABSTRACT***

*Cybercrime is the misuse of technology to be used as a tool or media in committing crimes such as hacking, stealing, deleting, hiding, and destroying information. Cybercriminals tend to delete, hide, and format all collected data to eliminate traces of digital evidence. In digital forensics, data loss from storage media can be overcome by file carving techniques. Therefore, this study aims to determine the results of file carving process in uncovering digital evidence and evaluate the performance of digital forensics software used including Autopsy, PhotoRec, Scalpel, and Foremost based on 3 assessment parameters with 3 different scenarios. Methodology used in the analysis process is the National Institute of Justice (NIJ) which consists of 5 method stages, namely identification, collection, examination, analysis, reporting. The results of the research show that in scenario 1 PhotoRec and Autopsy have the best percentage of performance and speed. In scenario 2 PhotoRec is the best, followed by Foremost and Scalpel, while Autopsy has zero performance. In scenario 3 PhotoRec and Autopsy have the best percentage of performance, but Autopsy has the slowest speed compared to the other three software. Referring to the research results, it can be concluded that the results of file carving analysis show that the PhotoRec software is able to fulfill all scenarios and assessment*

*parameters with an average performance of recovering digital evidence of 90.8%, while the performance of other software is Autopsy of 64.17%, Foremost 30%, and Scalpel 0%.*

**Keywords**: *Digital Evidence, Digital Forensics, File Carving, Software*

## 1. PENDAHULUAN

Kejahatan Siber pada era digital sekarang ini diperlukan perhatian lebih dari lembaga dan penegak hukum terkait dalam menangani kasus tindak pidana siber. Menurut situs Direktorat Tindak Pidana Siber Bareskrim Polri (patrolisiber.id) dari bulan Januari 2020 sampai dengan Januari 2021 terdapat 2.259 total laporan yang diterima mengenai kejahatan siber (Direktorat Tindak Pidana Siber Bareskrim Polri, 2021). Kasus kejahatan siber yang paling banyak dilaporkan diantaranya adalah penyebaran konten provokatif sebanyak 1.048 kasus dan penipuan online sebanyak 649 kasus (Direktorat Tindak Pidana Siber Bareskrim Polri, 2021).

Kejahatan siber dengan memanfaatkan perangkat teknologi dapat dijadikan alat atau media dalam melakukan tindak kejahatan seperti meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi, dan merusak informasi (Rana, et al., 2017). Hasil dari kejahatan umumnya akan disembunyikan kedalam media penyimpanan agar dapat dipergunakan kembali selanjutnya, tetapi dalam menutupi dan menghilangkan jejaknya pelaku kejahatan siber cenderung akan menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan dalam melakukan tindak kejahatan (Putra, et al., 2017).

Terdapat suatu cara dalam *computer forensics* untuk mengatasi *file* yang hilang pada media penyimpanan dengan pendekatan *static forensics* yang disebut dengan teknik *file carving*. *File carving* merupakan aspek penting dari penerapan ilmu forensik digital karena dapat menambah fleksibilitas untuk mencari informasi yang tersimpan dari pokok struktur sistem *file* (Fikri, 2016). Alat *carving* yang paling sederhana bekerja dengan cara menemukan *header* dan *footer*, sedangkan paling canggih dapat melakukan validasi dan mengumpulkan kembali *file* yang terfragmentasi (Laurenson, 2013). Dalam melakukan uji performa pada setiap alat carving dapat diukur berdasarkan tiga parameter yang paling umum digunakan oleh analis forensik untuk menilai kinerja alat *carving*, diantaranya adalah kecepatan proses pemulihan *file*, kehandalan jumlah *file* yang berhasil dipulihkan, dan persentase kebenaran *file* yang dipulihkan (Laurenson, 2013).

Penelitian sebelumnya mengenai analisis forensik digital dalam melakukan *file carving* pernah dilakukan yaitu untuk melakukan analisis *file carving* pada *file* system dengan menggunakan *framework National Institute of Standards Technology* (NIST). Pada penelitian ini dilakukan analisis forensik dalam melakukan *file* carving menggunakan perangkat lunak *Autopsy* terhadap barang bukti elektronik berupa *flash disk*. Hasil dari penelitian ini menunjukkan bahwa perangkat lunak *Autopsy* memiliki keunggulan dalam pengembalian *file* yang terhapus, tersembunyi dan terformat berdasarkan sistem *file* FAT32 dan NTFS (Yuwono, et al., 2019). Selain itu penelitian lain mengenai *file carving* dalam melakukan analisis perbandingan *file carving* dengan metode NIST menghasilkan penelitian ini menunjukkan *Scalpel* dapat menghasilkan

pengembalian yang lebih baik dibandingkan *Foremost* (Yuwono & W, 2020). Sedangkan dalam penelitian lain mengenai perbandingan carving tools *Foremost* dan *Scalpel* menghasilkan *Foremost* memiliki kemampuan carving yang lebih cepat dengan tingkat validitas tinggi, dan jumlah *file* rusak yang kembali relatif rendah (Muttaqin, et al., 2015).

Penelitian mengenai masalah forensik digital sangat relevan dengan keadaan saat ini yang semakin serba digital. Sehingga penelitian ini akan lebih terfokus pada analisis kinerja perangkat lunak untuk *file carving* melalui pendekatan *static forensics* dalam mengungkap barang bukti digital menggunakan tahapan *framework National Institute of Justice* (NIJ). Tujuan dilakukannya penelitian ini adalah mengetahui hasil proses *file carving* dalam mengungkap barang bukti digital menggunakan perangkat lunak forensik digital seperti *Autopsy*, *PhotoRec*, *Scalpel*, dan *Foremost*. Selain itu penelitian ini juga bertujuan dalam melakukan evaluasi kinerja terhadap 4 perangkat lunak tersebut berdasarkan 3 parameter penilaian yaitu kecepatan proses pemulihan, jumlah *file* yang berhasil dipulihkan, dan kebenaran *file* yang dipulihkan. Sampel pengujian yang digunakan sebagai barang bukti digital terbagi menjadi 4 jenis *file* dengan 8 ekstensi berbeda yaitu gambar (jpg, png), video (mp4, avi), audio (mp3, wav), dan dokumen (docx, pdf). Selain itu skenario analisis *file carving* yang dibuat dalam penelitian ini terbagi menjadi 3 yaitu berdasarkan hasil *imaging FTK Imager* tanpa *BitLocker*, hasil *imaging FTK Imager* dengan *BitLocker*, dan secara langsung melalui *flash drive*.

Menurut situs resminya *Autopsy* merupakan *platform* forensik *open source* besutan *Basis Technology* yang cepat, mudah digunakan, dan mampu menganalisis semua jenis perangkat seluler dan media digital (Basis Technology, 2021). Sedangkan menurut situs resmi *CGSecurity*, *PhotoRec* menjadi perangkat lunak *multi-platform open source* yang dirancang untuk memulihkan *file* yang hilang pada berbagai macam sistem *file* dan membuat *disk* yang tidak dapat di-*boot* dapat di-*boot* kembali (CGSecurity, 2019). Selain itu terdapat juga *Scalpel* yang merupakan *file carver* besutan *Digital Forensics Solution* yang berjalan menggunakan *command* pada terminal Linux atau Windows, *Scalpel* cukup populer untuk investigasi forensik digital dan pemulihan *file* ( Computer Network Defence Limited, 2011). Berikutnya adalah *Foremost* yang merupakan perangkat lunak pemulihan *file* besutan *SourceForge* yang berjalan menggunakan *command* pada terminal Linux atau Windows. *Foremost* dikembangkan oleh Kantor Investigasi Khusus Angkatan Udara Amerika Serikat bersama Pusat Studi dan Penelitian Keamanan Sistem Informasi (SourceForge, 2021).

## 2. METODOLOGI

Metode yang digunakan dalam tahapan analisis forensik pada penelitian ini adalah *framework National Institute of Justice* (NIJ). Metode ini dikembangkan oleh badan penelitian, pengembangan, dan evaluasi dari Departemen Kehakiman Amerika Serikat yang berdedikasi dalam meningkatkan pengetahuan dan pemahaman tentang kejahatan dan masalah keadilan melalui sains (National Institute of Justice, 2019). *Framewrok* NIJ menjadi salah satu pilihan dalam melakukan analisis forensik digital, karena tahapan penelitian yang dilakukan dapat diketahui alurnya secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada .

Tahapan yang dikembangkan oleh NIJ sebagai pedoman dalam melakukan

proses investigasi barang bukti digital terdiri dari lima tahapan. Tahapan dari metode *framework National Institute of Justice* (NIJ) adalah *identification*, *collection*, *examination*, *analysis*, dan *reporting* (Riadi, et al., 2018) yang dapat dilihat pada Gambar 1, secara lengkap dijelaskan sebagai berikut.


Gambar 1. Tahapan *National Institute of Justice*

### 2.1 *Identification* (Identifikasi)

Tahap *Identification* (identifikasi) merupakan tahap penilaian awal terhadap kebutuhan proses analisis serta pemilahan barang bukti kejahatan yang digunakan dalam mendukung proses pencarian barang bukti digital (Riadi, et al., 2018). Tahap ini dilakukan identifikasi terhadap kebutuhan analisis dan skenario pelabelan serta perekaman barang bukti digital.

### 2.2 *Collection* (Pengumpulan)

Tahap *Collection* (pengumpulan) merupakan tahap pengumpulan barang bukti digital yang digunakan untuk mendukung proses penyidikan dalam pencarian barang bukti kejahatan digital (Riadi, et al., 2018). Tahap ini dilakukan proses pengambilan barang bukti digital dengan image agar tetap menjaga integritas bukti aslinya.

### 2.3 *Examination* (Pemeriksaan)

Tahap *Examination* (pemeriksaan) merupakan tahap pemeriksaan yang memastikan bahwa barang bukti digital yang dikumpulkan adalah *file* asli sesuai dengan yang didapat pada tempat kejadian kejahatan (Riadi, et al., 2018). Tahap ini merupakan proses validasi dengan melihat dan membandingkan nilai *hash*.

### 2.4 *Analysis* (Analisis)

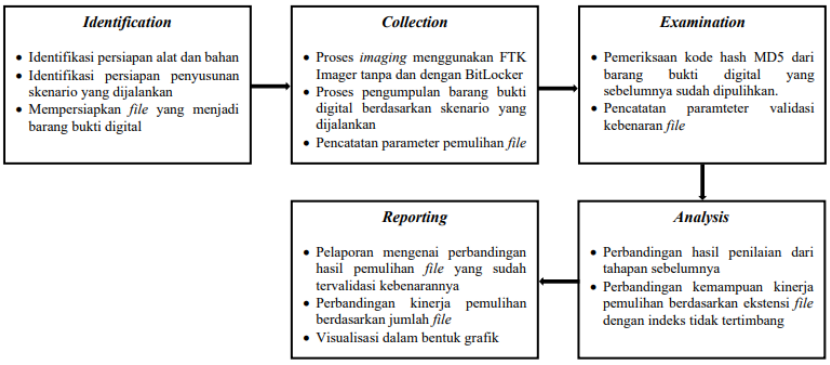
Tahap *Analysis* (analisis) merupakan tahap meneliti data yang sudah didapatkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail sesuai dengan teknik dan hukum untuk dapat membuktikan data tersebut (Riadi, et al., 2018). Tahap ini merupakan evaluasi terhadap hasil analisis agar barang bukti dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

### 2.5 *Reporting* (Pelaporan)

Tahap *Reporting* (pelaporan) merupakan tahap setelah memperoleh barang bukti digital dari proses pemeriksaan dan analisis (Riadi, et al., 2018). Tahap ini merupakan pelaporan hasil analisis meliputi seluruh penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan aspek pendukung lainnya pada proses tindakan forensik digital.

Perancangan penelitian yang dilakukan menggunakan metode *National Institute of Justice* (NIJ) penjelasannya dapat dilihat pada Gambar 2.


*p-ISSN : 2502-5724; e-ISSN : 2541-5735*




Gambar 2. Rancangan Penelitian

Berdasarkan penjelasan mengenai rancangan penelitian pada Gambar 2 dapat diketahui proses penelitian yang dilakukan pada tahap *identification* adalah mempersiapkan alat dan bahan penunjang, menyusun 3 skenario yang dijalankan, serta mempersiapkan sampel yang menjadi barang bukti digital. Pada tahap *collection* dilakukan proses *imaging* menggunakan perangkat lunak *FTK Imager* dengan *BitLocker* dan tanpa *BitLocker*, setelah itu dilakukan proses *carving* menggunakan 4 perangkat lunak berbeda sekaligus pencatatan barang bukti digital berdasarkan 3 skenario yang dibuat, sehingga pada tahap ini dapat diketahui parameter keberhasilan awal dan kecepatan pengembalian *file*. Pada tahap *examination* dilakukan pemeriksaan dan perbandingan barang bukti digital sebelum dan sesudah dilakukan *carving* dengan menggunakan nilai *hash* MD5 pada setiap skenario yang dijalankan, sehingga pada tahap ini dapat diketahui parameter keberhasilan pemulihan barang bukti digital yang telah tervalidasi kebenarannya. Selanjutnya pada tahap *analysis* dilakukan proses analisis perbandingan hasil dari tahapan pengumpulan dan pemeriksaan barang bukti digital pada setiap skenario yang sudah ditentukan. Hasil dari pencatatan kinerja perangkat lunak berdasarkan 3 parameter penilaian akan dibandingkan pada setiap skenarionya dengan membuat skema pada 4 jenis *file* yaitu gambar, video, audio, dan dokumen, sehingga hasil perbandingan akan dianalisis untuk mendapatkan hasil kinerja perangkat lunak pada setiap jenis *file* yang ada di setiap skenario. Selain itu pada tahap ini juga dilakukan perbandingan ekstensi *file* yang mampu dipulihkan oleh setiap perangkat lunak dan dihitung menggunakan rumus indeks tidak tertimbang, sehingga dapat menemukan persentase kinerja dari perangkat lunak terhadap ekstensi *file* tersebut. Pada tahap terakhir *reporting* dilakukan proses pelaporan mengenai perbandingan hasil pemulihan *file* yang sudah tervalidasi kebenarannya dan kecepatan proses dari setiap perangkat lunak pada skenario yang dijalankan. Hasil dari perbandingan akan divisualisasikan dan dihitung menggunakan rumus indeks tidak tertimbang untuk mengetahui kinerja terbaik dari perangkat lunak *file carving*.

## 3. HASIL DAN PEMBAHASAN

Hasil penelitian yang telah dilakukan dalam menganalisis kinerja perangkat lunak forensik digital untuk melakukan *file carving* dengan menggunakan *Autopsy*, *PhotoRec*, *Scalpel*, dan *Foremost* diperoleh representasi hasil evaluasi kinerja perangkat lunak dalam mengungkap barang bukti digital pada media penyimpanan permanen (*non-volatile*) berupa *flash drive* berkapasitas 16GB melalui pendekatan static forensics

dengan menggunakan *framework National Institute of Justice* (NIJ).

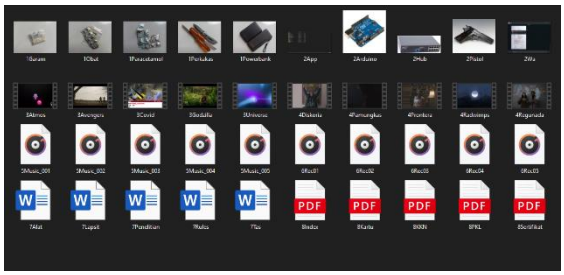
### 3.1 Tahap *Identification* (Identifikasi)

Persiapan yang pertama dilakukan adalah melakukan identifikasi kebutuhan analisis dan penyusunan skenario. Berikut pada Tabel 1 adalah alat dan bahan kebutuhan penunjang analisis.

Tabel 1. Alat dan Bahan Penunjang Analisis

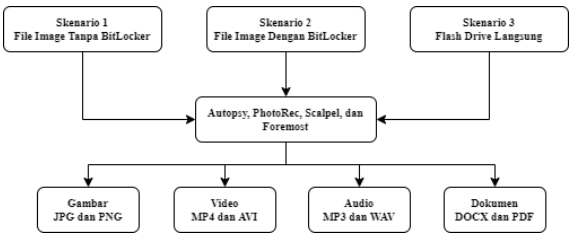
| No. | Nama | Keterangan |
|---|---|---|
| 1 | Laptop Acer Aspire 3 A315-41 | OS Windows 10 Pro 64-bit & OS Linux Ubuntu Focal Fossa |
| 2 | Flash Drive SanDisk CZ50 Cruzer Blade | USB 2.0, Kapasitas 16GB, FAT32 (*Default*) |
| 3 | *Autopsy* (Basis Technology) | Versi 4.18.0 64-bit, OS Windows |
| 4 | *PhotoRec* (CGSecurity) | Versi 7.2 64-bit, OS Windows |
| 5 | *Scalpel* (Digital Forensics Solution) | Versi 1.60 64-bit, OS Linux Ubuntu |
| 6 | *Foremost* (CGSecurity) | Versi 1.5 64-bit, OS Linux Ubuntu |
| 7 | *FTK Imager* (Access Data) | Versi 4.5.0 64-bit, OS Windows |
| 8 | *BitLocker* (Microsoft Corp.) | Versi 10.0.19041, OS Windows |

Selanjutnya penyusunan skenario pertama kali dilakukan adalah menentukan input yang digunakan dalam penelitian. Berdasarkan hasil yang diperoleh ketika memformulasikan masalah, dapat diketahui bahwa *file* yang paling sering hilang ataupun menjadi barang bukti digital yaitu foto, video, audio, dan dokumen. Oleh karena itu pada penelitian ini akan menentukan beberapa sampel *file* tersebut yang masing-masing memiliki ekstensi berbeda seperti pada Gambar 3.



Gambar 3. Sampel Barang Bukti Digital

Pada Gambar 3 penamaan *file* yang diawali dengan angka 1 adalah JPG, angka 2 adalah PNG, angka 3 adalah MP4, angka 4 adalah AVI, angka 5 adalah MP3, angka 6 adalah WAV, angka 7 adalah DOCX atau Microsoft Word, dan angka 8 adalah PDF. Sehingga pada setiap jenis *file* gambar, video, audio, dan dokumen terdapat 10 *file* dengan 2 ekstensi berbeda yang total keseluruhannya adalah 40 *file*. Setelah menentukan sampel barang bukti digital, selanjutnya adalah membentuk 3 skenario berbeda berdasarkan setiap kondisi analisis yang dilakukan. Skema yang dibentuk pada setiap skenario adalah berdasarkan 4 perangkat lunak yang sudah ditentukan sebelumnya. Skenario yang akan dijalankan pada penelitian ini alurnya seperti pada Gambar 4 berikut.




Gambar 4. Alur Skenario Pengumpulan Barang Bukti Digital

### 3.2 Tahap *Collection* (Pengumpulan)

Pada tahap pengumpulan target yang akan dipulihkan adalah *flash drive* berkapasitas 16GB yang didalamnya terdapat *file* yang menjadi barang bukti digital dan sudah dilakukan proses format. Dalam tahapan pengumpulan *file* yang hilang akan terbagi berdasarkan 3 skenario yang sudah ditentukan, 2 skenario diantaranya melalui *file image* dari hasil *imaging FTK Imager* tanpa *BitLocker* dan dengan *BitLocker*.

Setelah melakukan *imaging* tanpa *BitLocker* dan dengan *BitLocker* dihasilkan 2 *file image* berbeda yang selanjutnya dilakukan *file carving* menggunakan 4


*p-ISSN : 2502-5724; e-ISSN : 2541-5735*

perangkat lunak yang dibandingkan yaitu *Autopsy*, *PhotoRec*, *Scalpel*, dan *Foremost*. Dihasilkan seperti pada Tabel 2 skenario 1, Tabel 3 skenario 2, dan Tabel 4 skenario 3.

Tabel 2. Skenario 1 *File* Image Tanpa *BitLocker*

| Skenario 1 | Gambar | | Video | | Audio | | Dokumen | | Total | Kecepatan Proses |
|---|---|---|---|---|---|---|---|---|---|---|
| | JPG | PNG | MP4 | AVI | MP3 | WAV | DOCX | PDF | | |
| ***Autopsy*** | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 39 | 3 menit 6 detik |
| ***PhotoRec*** | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 39 | 2 menit 21 detik |
| ***Scalpel*** | 4 | 1 | 0 | 5 | 0 | 5 | 0 | 5 | 20 | 10 menit 34 detik |
| ***Foremost*** | 4 | 5 | 0 | 1 | 0 | 5 | 5 | 5 | 25 | 8 menit 7 detik |

Tabel 3. Skenario 2 *File* Image Dengan *BitLocker*

| Skenario 2 | Gambar | | Video | | Audio | | Dokumen | | Total | Kecepatan Proses |
|---|---|---|---|---|---|---|---|---|---|---|
| | JPG | PNG | MP4 | AVI | MP3 | WAV | DOCX | PDF | | |
| ***Autopsy*** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Error |
| ***PhotoRec*** | 3 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 33 | 2 menit 19 detik |
| ***Scalpel*** | 3 | 1 | 0 | 5 | 0 | 5 | 0 | 5 | 19 | 12 menit 40 detik |
| ***Foremost*** | 3 | 0 | 0 | 1 | 0 | 5 | 5 | 5 | 19 | 8 menit 6 detik |

Tabel 4. Skenario 3 Flash Drive Langsung

| Skenario 3 | Gambar | | Video | | Audio | | Dokumen | | Total | Kecepatan Proses |
|---|---|---|---|---|---|---|---|---|---|---|
| | JPG | PNG | MP4 | AVI | MP3 | WAV | DOCX | PDF | | |
| ***Autopsy*** | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 39 | 26 menit 31 detik |
| ***PhotoRec*** | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 39 | 7 menit 16 detik |
| ***Scalpel*** | 4 | 1 | 0 | 5 | 0 | 5 | 0 | 5 | 20 | 14 menit 27 detik |
| ***Foremost*** | 4 | 5 | 0 | 1 | 0 | 5 | 5 | 5 | 25 | 11 menit 55 detik |

### 3.3 Tahap *Examination* (Pemeriksaan)

Pada tahap ini dilakukan pemeriksaan barang bukti digital yang didapat setelah melakukan pengumpulan melalui proses *file carving* dengan tujuan mengetahui kebenaran *file* yang kembali sesuai dengan sebelum dilakukan format sehingga dapat terjamin keutuhannya (Al-Azhar, 2012). Pemeriksaan bukti digital dilakukan dengan melihat dan membandingkan nilai *hash* algoritme MD5 masing-masing *file* pada setiap skenario sehingga dapat diketahui persentase kebenaran *file* yang pulih. Pengukuran persentase kebenaran dilihat melalui perbandingan nilai *hash* pada setiap *file* yang pulih, sehingga poin persentase yang didapat menghasilkan seperti pada ketiga Tabel berikut.

Tabel 5. Skenario 1 *File* Image Tanpa *BitLocker*

| Skenario 1 | Gambar | Video | Audio | Dokumen | Total Pulih | Total Benar |
|---|---|---|---|---|---|---|
| ***Autopsy*** | 90% | 100% | 100% | 100% | 39 | 39 |
| ***PhotoRec*** | 90% | 100% | 100% | 100% | 39 | 39 |
| ***Scalpel*** | 0% | 0% | 0% | 0% | 20 | 0 |
| ***Foremost*** | 90% | 0% | 0% | 50% | 25 | 14 |

Tabel 6. Skenario 2 *File* Image Dengan *BitLocker*

| Skenario 2 | Gambar | Video | Audio | Dokumen | Total Pulih | Total Benar |
|---|---|---|---|---|---|---|
| ***Autopsy*** | - | - | - | - | 0 | 0 |
| ***PhotoRec*** | 30% | 90% | 100% | 100% | 33 | 32 |
| ***Scalpel*** | 0% | 0% | 0% | 0% | 19 | 0 |
| ***Foremost*** | 30% | 0% | 0% | 50% | 19 | 8 |

Tabel 7. Skenario 3 Flash Drive Langsung

| Skenario 3 | Gambar | Video | Audio | Dokumen | Total Pulih | Total Benar |
|---|---|---|---|---|---|---|
| ***Autopsy*** | 90% | 90% | 100% | 100% | 39 | 38 |
| ***PhotoRec*** | 90% | 90% | 100% | 100% | 39 | 38 |
| ***Scalpel*** | 0% | 0% | 0% | 0% | 20 | 0 |
| ***Foremost*** | 90% | 0% | 0% | 50% | 25 | 14 |

### 3.4 Tahap *Analysis* (Analisis)

Pada tahap ini dilakukan analisis melalui perbandingan hasil dari tahapan sebelumnya berdasarkan 3 parameter penilaian yang ditentukan. Hasil perbandingan skenario 1 *file image* tanpa *BitLocker* pada Tabel 1 dan Tabel 5 menunjukkan *PhotoRec* dan *Autopsy* unggul dalam melakukan pemulihan dengan tingkat kebenaran yang baik, akan tetapi *PhotoRec* sedikit lebih unggul dalam kecepatan pemulihan daripada *Autopsy*. Pada skenario 1 *Scalpel* memiliki performa tingkat kebenaran pemulihan paling rendah dengan kecepatan proses paling lama.

Hasil perbandingan skenario 2 *file image* dengan *BitLocker* pada Tabel 2 dan Tabel 6 menunjukkan *PhotoRec* jauh lebih unggul dalam melakukan pemulihan dengan tingkat kebenaran yang baik dan kecepatan proses tercepat dibandingkan 3 perangkat lunak lainnya. Sedangkan pada skenario 2 *Autopsy* mengalami error karena tidak dapat melakukan pemulihan hasil *imaging* yang terenkripsi dengan *BitLocker*, selain itu *Scalpel* memiliki performa tingkat kebenaran pemulihan terendah dibandingkan *PhotoRec* dan *Foremost* dengan kecepatan proses paling lama.

Hasil perbandingan skenario 3 yang dilakukan melalui flash drive langsung pada Tabel 3 dan Tabel 7 menunjukkan *PhotoRec* dan *Autopsy* unggul dalam melakukan pemulihan dengan tingkat kebenaran yang baik, akan tetapi *PhotoRec* jauh lebih unggul dalam kecepatan pemulihan daripada *Foremost*, *Scalpel*, dan *Autopsy*. Sedangkan pada skenario 3 *Autopsy* memiliki kecepatan proses paling lama dibandingkan perangkat lunak lainnya dan *Scalpel* seperti sebelumnya memiliki performa tingkat kebenaran pemulihan yang sangat rendah.

Dari hasil analisis yang dilakukan berdasarkan 3 skenario dengan 4 perangkat lunak dapat diketahui kinerja pemulihan berdasarkan 8 eksetensi *file* yang berbeda seperti pada Tabel 8. Hasil yang diperoleh dihitung menggunakan rumus metode indeks tidak tertimbang atau agregatif sederhana untuk mengukur persentase kinerja dari setiap perangkat lunak (Riadi, et al., 2020). Metode ini terbilang sangat sederhana dan mudah dihitung, karena tidak memerlukan faktor yang mempengaruhi naik turunnya angka indeks (Harianti, et al., 2011).

$$\text{Pon} = \frac{\sum \text{Pn}}{\sum \text{Po}} \text{ x } 100\% \quad (1)$$

Pada rumus persamaan (1) Pn adalah total pemulihan *file* yang didapat, Po adalah total jumlah seluruh ekstensi/jenis *file*, sedangkan Pon adalah hasil persentase kinerja (indeks tidak tertimbang atau agregatif sederhana).

Tabel 8. Kinerja Pemulihan Berdasarkan Ekstensi *File*

| Ekst. | *Autopsy* | *PhotoRec* | *Scalpel* | *Foremost* |
|---|---|---|---|---|
| **JPG** | ✓ | ✓ | ✓ | ✓ |
| **PNG** | ✓ | ✓ | × | ✓ |
| **MP4** | ✓ | ✓ | × | × |
| **AVI** | ✓ | ✓ | ✓ | ✓ |
| **MP3** | ✓ | ✓ | × | × |
| **WAV** | ✓ | ✓ | ✓ | ✓ |
| **DOCX** | ✓ | ✓ | × | ✓ |
| **PDF** | ✓ | ✓ | ✓ | ✓ |
| **Total** | 8 | 8 | 4 | 6 |

Berdasarkan Tabel 8 diketahui kemampuan perangkat lunak dalam melakukan pemulihan berdasarkan 8 ekstensi *file* berbeda yang kemudian dapat dihitung menggunakan rumus indeks tidak


*p-ISSN : 2502-5724; e-ISSN : 2541-5735*

tertimbang dan menunjukkan kinerja terbaik adalah perangkat lunak *Autopsy* serta *PhotoRec* dengan nilai indeks sebesar 100%, selain itu dibawahnya terdapat perangkat lunak *Foremost* dengan nilai indeks sebesar 75% dan perangkat lunak *Scalpel* dengan nilai indeks sebesar 50%.

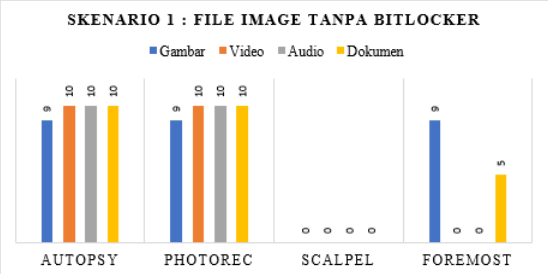
### 3.5 Tahap *Reporting* (Pelaporan)

Berdasarkan analisis yang telah dilakukan dapat dibentuk pelaporan mengenai pengetahuan yang diperoleh agar dapat lebih mudah dipahami. Pada skenario 1 *file image* tanpa *BitLocker* didapatkan hasil persentase kinerja perangkat lunak dalam melakukan pemulihan *file* dan sudah terbukti kebenarannya secara terurut dari yang terbaik menggunakan perhitungan indeks tidak tertimbang seperti pada Tabel 9.

Tabel 9. Persentase Kinerja Skenario 1

| No. | Nama | Persentase Kinerja | Kecepatan |
|---|---|---|---|
| 1 | *PhotoRec* | 97,5% | 2’ 21” |
| 2 | *Autopsy* | 97,5% | 3’ 6” |
| 3 | *Scalpel* | 35% | 8’ 7” |
| 4 | *Foremost* | 0% | 10’ 34” |

Pada Tabel 9 dapat diketahui perangkat lunak dengan kinerja terbaik adalah *PhotoRec* dan *Autopsy*, akan tetapi kecepatan *PhotoRec* sedikit lebih unggul dibandingkan *Autopsy*. Berikut adalah visualisasi grafik jumlah *file* yang berhasil dipulihkan dan sudah terbukti kebenarannya pada Gambar 5.



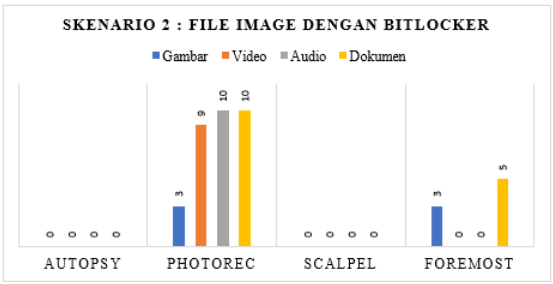

Gambar 5. Grafik Hasil Pemulihan Skenario 1

Pada skenario 2 *file image* dengan *BitLocker* didapatkan hasil persentase kinerja perangkat lunak dalam melakukan pemulihan *file* dan sudah terbukti kebenarannya secara terurut dari yang terbaik menggunakan perhitungan indeks tidak tertimbang seperti pada Tabel 10.

Tabel 10. Persentase Kinerja Skenario 2

| No. | Nama | Persentase Kinerja | Kecepatan |
|---|---|---|---|
| 1 | *PhotoRec* | 80% | 2’ 19” |
| 2 | *Foremost* | 20% | 8’ 6” |
| 3 | *Scalpel* | 35% | 12’ 40” |
| 4 | *Autopsy* | *Null* | *Error* |

Pada Tabel 10 dapat diketahui perangkat lunak dengan kinerja terbaik adalah *PhotoRec*, selain itu *Autopsy* tidak dapat melakukan pemulihan pada *file image* yang terenkripsi oleh *BitLocker*. Berikut adalah visualisasi grafik jumlah *file* yang berhasil dipulihkan dan sudah terbukti kebenarannya pada Gambar 6.




Gambar 6. Grafik Hasil Pemulihan Skenario 2

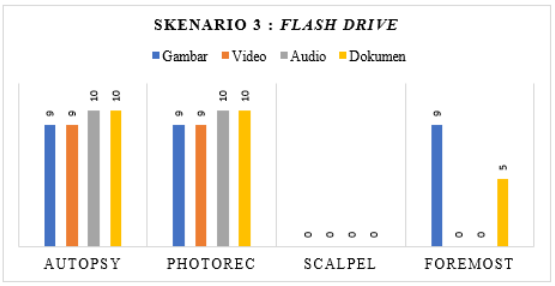
Pada skenario 3 dilakukan pemulihan melalui *flash drive* secara langsung dan didapatkan hasil persentase kinerja perangkat lunak dalam melakukan pemulihan *file* yang sudah terbukti kebenarannya secara terurut dari yang terbaik menggunakan perhitungan indeks tidak tertimbang seperti pada Tabel 11.

Tabel 11. Persentase Kinerja Skenario 3

| No. | Nama | Persentase Kinerja | Kecepatan |
|---|---|---|---|
| 1 | *PhotoRec* | 95% | 7’ 16” |

| | | | |
|---|---|---|---|
| 2 | *Autopsy* | 95% | 26’ 31” |
| 3 | *Scalpel* | 35% | 14’ 27” |
| 4 | *Foremost* | 0% | 11’ 55” |

Pada Tabel 11 dapat diketahui perangkat lunak dengan kinerja terbaik adalah *PhotoRec* dan *Autopsy*, tetapi *Autopsy* memakan kecepatan proses yang sangat lama dibandingkan 3 perangkat lunak lainnya. Berikut adalah visualisasi grafik jumlah *file* yang berhasil dipulihkan dan sudah terbukti kebenarannya pada Gambar 7.



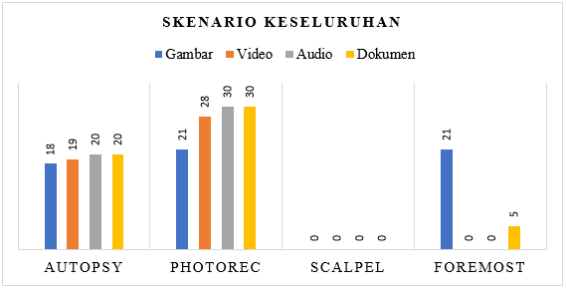

Gambar 7. Grafik Hasil Pemulihan Skenario 3

Dari hasil pemaparan diatas dapat diambil rata-rata secara keseluruhan persentase kinerja pemulihan dan kebenaran *file* setiap perangkat lunak seperti pada Tabel 12 berikut.

Tabel 12. Persentase Kinerja Keseluruhan

| No. | Nama | Persentase Kinerja |
|---|---|---|
| 1 | *PhotoRec* | 90,8% |
| 2 | *Autopsy* | 64,17% |
| 3 | *Scalpel* | 30% |
| 4 | *Foremost* | 0% |

Berdasarkan Tabel 12 dapat diketahui secara keseluruhan perangkat lunak *PhotoRec* memiliki hasil pemulihan dengan validasi kebenaran terbaik. Berikut adalah visualisasi secara keseluruhan berdasarkan 3 skenario yang dijalankan pada Gambar 8.




Gambar 8. Grafik Hasil Pemulihan Keseluruhan

Adapun hasil pengetahuan dari informasi yang sudah di dapat adalah sebagai berikut:

a. Pada Skenario 1 dan skenario 3 pemulihan dan persentase kebenaran *file* yang dihasilkan *PhotoRec* dan *Autopsy* dapat dilakukan dengan baik dari pada *Scalpel* dan *Foremost*. Tetapi parameter kecepatan proses *PhotoRec* pada 3 skenario sangat lebih unggul dari *Autopsy*, *Scalpel*, dan *Foremost*.
b. Pada Skenario 2 perangkat lunak *Autopsy* tidak dapat mengolah *file image* yang sudah dibuat dengan enkripsi *BitLocker*.
c. Pada skenario 3 perangkat lunak *Autopsy* memiliki kecepatan proses pemulihan paling lama dari pada *PhotoRec*, *Scalpel*, dan *Foremost*.
d. Secara keseluruhan perangkat lunak *Scalpel* selalu memiliki persentase kebenaran sebesar 0% karena *hash file* setelah melakukan pemulihan menunjukkan hasil yang berbeda dengan aslinya.
e. Secara keseluruhan perangkat lunak *Foremost* selalu memiliki persentase kebenaran 0% pada jenis *file* avi, wav, dan pdf.
f. Secara keseluruhan perangkat lunak *Scalpel* dan *Foremost* tidak mendukung pemulihan dengan eksetensi *file* mp3 dan mp4.
g. Secara keseluruhan perangkat lunak *Scalpel* tidak mendukung pemulihan dengan ekstensi *file* microsoft word


p-ISSN : 2502-5724; e-ISSN : 2541-5735

terbaru yaitu docx. Selain itu ekstensi *file* png yang dipulihkan *Scalpel* selalu rusak atau *corrupt*.

h. Secara keseluruhan perangkat lunak *Scalpel* lebih unggul dalam pemulihan *file* video dari pada *Foremost*, akan tetapi dengan tidak melihat kebenaran *file* video tersebut.
i. Dalam melakukan proses *file carving* baiknya dilakukan dengan menggunakan *file image* hasil *imaging*. Hal ini dikarenakan berdasarkan skenario 3, proses *file carving* menggunakan *flash drive* secara langsung memerlukan waktu yang cukup lama dari pada *file image*. Selain itu menggunakan *file image* jauh lebih aman dalam mengulang proses pemulihan karena tidak akan merusak meta data bukti digital didalam *flash drive*.
j. Perangkat lunak terbaik secara keseluruhan adalah *PhotoRec* karena mampu melewati 3 skenario dan memenuhi 3 parameter penilaian dengan sangat baik. Sedangkan perangkat lunak terbaik selanjutnya adalah *Autopsy* karena mampu memulihkan *file* dengan persentase kebenaran yang sama baiknya dengan *PhotoRec*. Selanjutnya apabila ingin melakukan *file carving* menggunakan terminal linux atau tanpa *user interface* penulis sarankan dapat menggunakan perangkat lunak *Foremost* karena jauh lebih baik dari *Scalpel*.

## 4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, maka didapatkan kesimpulan yaitu pada skenario 1 *Autopsy* mampu memulihkan 39 *file* dalam 3 menit 6 detik, *PhotoRec* 39 *file* dalam 2 menit 21 detik, *Scalpel* 0 *file* dalam 10 menit 34 detik, *Foremost* 14 *file* dalam 8 menit 7 detik. Selain itu pada skenario 2 *Autopsy* tidak mampu memulihkan *file* karena enkripsi *BitLocker*, *PhotoRec* 32 *file* dalam 2 menit 19 detik, *Scalpel* 0 *file* dalam 12 menit 40 detik, *Foremost* 8 *file* dalam 8 menit 6 detik. Kemudian pada skenario 3 *Autopsy* memulihkan 38 *file* dalam 26 menit 31 detik, *PhotoRec* 38 *file* dalam 7 menit 16 detik, *Scalpel* 0 *file* dalam 14 menit 27 detik, dan *Foremost* 14 *file* dalam 11 menit 55 detik.

Evaluasi terhadap kinerja perangkat lunak forensik digital dalam melakukan *file carving* menghasilkan *PhotoRec* memiliki rata-rata kinerja tertinggi yaitu sebesar 90,8%. Selain itu perangkat lunak terbaik selanjutnya adalah *Autopsy* dengan rata-rata kinerja 64,17% yang berhasil memenuhi parameter pemulihan dan kebenaran *file* menyaingi *PhotoRec* serta mampu menjalankan 2 skenario dengan baik. Setelah itu terdapat *Foremost* memiliki rata-rata kinerja 30% yang mampu melakukan pemulihan dengan persentase kebenaran *file* yang cukup baik, sedangkan terakhir adalah *Scalpel* karena setiap skenario yang dijalankan parameter pemulihan cukup mendapat hasil baik akan tetapi persentase kebenaran *file* tidak terpenuhi dengan baik, sehingga rata-rata kinerja *Scalpel* adalah 0%.

Penelitian mengenai *file carving* dapat dilakukan pengembangan lebih lanjut, dimana dalam penelitian berikutnya dapat menambahkan perbandingan perangkat lunak *file carving* lain seperti *Bulk Extractor* dan *MagicRescue*. Selain itu dapat dilakukan pengujian terhadap media penyimpanan *non-volatile* lainnya seperti *hard disk* (HDD), *solid state drive* (SSD), *hard disk external*, dan *secure digital card* (Kartu SD), serta dapat ditambahkan cakupan jenis dan ekstensi *file* berbeda lainnya seperti *file* program (exe, deb), *file* teks (txt) dan *file* kompres (rar, zip).

## DAFTAR PUSTAKA

Computer Network Defence Limited, 2011. *Scalpel.* [Online] Available at: https://www.securitywizardry.com/forensic-solutions/forensic-tools/scalpel [Diakses 28 June 2021].

Al-Azhar, M. N., 2012. *Digital Forensic Practical Guidelines for Computer Investigation.* Jakarta: Salemba Infotek.

Basis Technology, 2021. *Autopsy.* [Online] Available at: https://www.autopsy.com/about/ [Diakses 28 June 2021].

CGSecurity, 2019. *PhotoRec.* [Online] Available at: https://www.cgsecurity.org/wiki/PhotoRec [Diakses 28 June 2021].

Direktorat Tindak Pidana Siber Bareskrim Polri, 2021. *Statistik Jumlah Laporan Polisi yang dibuat Masyarakat.* [Online] Available at: https://patrolisiber.id/statistic [Diakses 23 Januari 2021].

Fikri, N., 2016. *Analisa Proses File Carving Menggunakan Photorec dan Foremost.* Jakarta: UIN Syarif Hidayatullah.

Harianti, A. et al., 2011. *Statistika I Edisi Revisi.* Yogyakarta: ANDI.

Laurenson, T., 2013. Performance Analysis of File Carving Tools. *28th Security and Privacy Protection in Information Processing Systems (SEC),* Juli.pp. 419-433.

Muttaqin, R., Arini & Mintarsih, F., 2015. Perbandingan Carving Tools Foremost dan Scalpel. *Jurnal Teknik Informatika,* April, VIII(1), pp. 63-72.

National Institute of Justice, 2019. *About NIJ.* [Online] Available at: https://nij.ojp.gov/about-nij [Diakses 23 January 2021].

Putra, R. A., Fadlil, A. & Riadi, I., 2017. Forensik Mobile Pada Smartwatch Berbasis Android. *Jurnal Rekayasa Teknologi Informasi,* Volume I, pp. 41-47.

Rana, N., Sansanwal, G., Khatter, K. & Singh, S., 2017. Taxonomy of Digital Forensics: Investigation Tools and Challenges. *Manav Rachna International University,* Agustus.

Riadi, I., Sunardi & Sahiruddin, 2020. Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK),* Februari, Volume VII, pp. 197-204.

Riadi, I., Umar, R. & Nasrulloh, I. M., 2018. Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIJ). *ELINVO (Electronics, Informatics, and Vocational Education),* Mei, I(3), pp. 70-82.

SourceForge, 2021. *Foremost.* [Online] Available at: http://foremost.sourceforge.net/ [Diakses 28 June 2021].

Yuwono, D. T., Juhairiah, S. & Sonedi, 2019. Analisis File Carving pada File System dengan Metode National Institute of Standards And Technology (NIST). *Prosiding SNRT (Seminar Nasional Riset Terapan),* November, VII(3), pp. 85-92.

Yuwono, D. T. & W, Y., 2020. Analisis Perbandingan File Carving dengan Metode NIST. *J-Sakti,* Mei, II(2), pp. 1-6.