INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 4 Tahun 2023 Page 2154-2165
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST

Jomanson Matondang[1✉], Iqbal Maulana[2], Carudin[3]
Informatika, Universitas Singaperbangsa Karawang
Email: jomanson.matondang17121@student.unsika.ac.id[1✉]

Abstrak

Kejahatan siber merupakan penyalahgunaan teknologi yang memiliki dampak negatif dari perkembangan teknologi pada era digital sekarang ini. Hasil dari kejahatan siber umumnya akan disembunyikan kedalam media penyimpanan, tetapi dalam menghilangkan jejak barang bukti digital pelaku kejahatan siber cenderung akan menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan. Kehilangan data dari media penyimpanan dapat diatasi dengan teknik file carving. File carving merupakan aspek penting dalam ilmu forensik digital untuk memulihkan file yang hilang dalam mengungkap barang bukti digital dengan menggunakan beberapa perangkat lunak file carving yang tersedia. Dalam penelitian ini dilakukan perbandingan evaluasi kinerja perangkat lunak forensik digital untuk file carving menggunakan metodologi National Institute of Standard and Technology(NIST) dari perangkat lunak Autopsy, PhotoRec, Scalpel, dan Foremost terhadap media penyimpanan flash drive dengan mengacu kepada tiga parameter penilaian yaitu kecepatan proses pemulihan, jumlah file yang berhasil dipulihkan, dan kebenaran file yang dipulihkan dengan membuat 3 skenario yaitu menggunakan file image tanpa BitLocker, file image dengan BitLocker, dan flash drive. 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 80%, sedangkan kinerja perangkat lunak lainnya adalah Autopsy sebesar 54.16%, Scalpel 15%, dan Foremost 10%.

Kata Kunci: *Barang bukti digital, Perangkat lunak forensik, Forensik digital, File carving*

Abstract

Cybercrime is an abuse of technology that can negatively affect the advancement of technology in this digital era. Evidences of cybercrime are commonly stored in storage medias, but in the effort of removing them, perpetrators usually sort to delete, hide, and format all collected data. Lost of data from storage devices can be solved using file carving. File carving is an important aspect in digital forensic to recover lost files using a number of file carving software. This research is a comparison of the software Autopsy, PhotoRec, Scalpel, and Foremost using the National Institute of Standard and Technologies (NIST) to file carve a flash drive storage media with three scenarios, which are image files without BitLocker, image files with BitLocker, and a flash drive with three comparing parameters, which are the speed of recovery, total recovered file, and the validity of the recovered files. The results show that in all scenarios and parameters, PhotoRec achieved 80% performance rate, the others include Autopsy with 54.16%, Scalpel with 15%, and Foremost with 10%.

Keyword: *Digital Evidences, Forensic Sotfware, Digital Forensic, File Carving*

PENDAHULUAN

Di era globalisasi seperti saat ini, setiap orang mudah untuk menyebarkan dan mendapatkan suatu informasi. Dengan berkembangnya teknologi gadget kini setiap orang bisa mengakses berita kapan saja dan di mana saja. Kemudahan teknologi juga membuat setiap orang dengan bebas menyebarkan informasi, dan berekspresi. Kemudahan setiap orang dalam memanfaatkan perkembangan teknologi dengan berbagai jenis perangkat yang sudah ada saat ini, memberikan banyak manfaat positif dan tentunya juga dampak negatif yang sama besarnya. Manfaat positif dari perkembangan teknologi salah satunya adalah memudahkan setiap orang dalam menunjang segala aktivitas pekerjaan sehingga dapat lebih efisien, selain itu dampak negatif yang dihasilkan adalah penyalahgunaan teknologi untuk tindak kejahatan digital yang dapat merugikan orang lain atau disebut dengan kejahatan siber.

Kejahatan siber dengan memanfaatkan perangkat teknologi dapat dijadikan alat atau media dalam melakukan kejahatan seperti meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi, dan merusak informasi. 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.

Terdapat suatu cara dalam computer forensics untuk mengatasi file yang hilang pada media penyimpanan dengan pendekatan static forensics yang disebut dengan teknik file carving. Teknik file carving memungkinkan pemulihan data yang hilang atau terhapus dengan mengidentifikasi tanda-tanda khusus dalam struktur data yang mengindikasikan keberadaan

file, sehingga memungkinkan penyelidik atau profesional forensik untuk memulihkan data tersebut. File carving merupakan aspek penting dari penerapan ilmu forensik digital karena dapat menambah fleksibilitas untuk mencari informasi yang tersimpan dari pokok struktur sistem file (Arvin, 2021). Alat carving yang paling sederhana bekerja dengan cara menemukan header dan footer, sedangkan paling canggih dapat melakukan validasi dan mengumpulkan kembali file yang terfragmentasi (Ali, 2018).

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. Penelitian 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 Justice (NIJ). Pada penelitian ini dilakukan analisis forensik dalam melakukan file carving menggunakan perangkat lunak FTK Imager dan Autopsy terhadap barang bukti elektronik berupa flash disk. Hasil dari penelitian ini menunjukkan bahwa perangkat lunak FTK Imager dan Autopsy memiliki keunggulan dalam pengembalian file yang terhapus, tersembunyi dan terformat berdasarkan sistem file FAT32 dan NTFS (Arvin, 2021).

Penelitian mengenai masalah forensik digital sangat relevan dengan keadaan saat ini yang semakin serba digital. Sehingga penelitian ini akan lebih terfokus pada analisis perbandingan perangkat lunak forensik digital untuk file carving dalam mengungkap barang bukti digital menggunakan framework National Institute of Standards Technology (NIST) dalam melakukan tahapan analisis forensik, selain itu penelitian ini akan mengevaluasi performa file carving (pemulihan file) pada 4 perangkat lunak berdasarkan 3 parameter pengujian terhadap 3 skenario kasus.

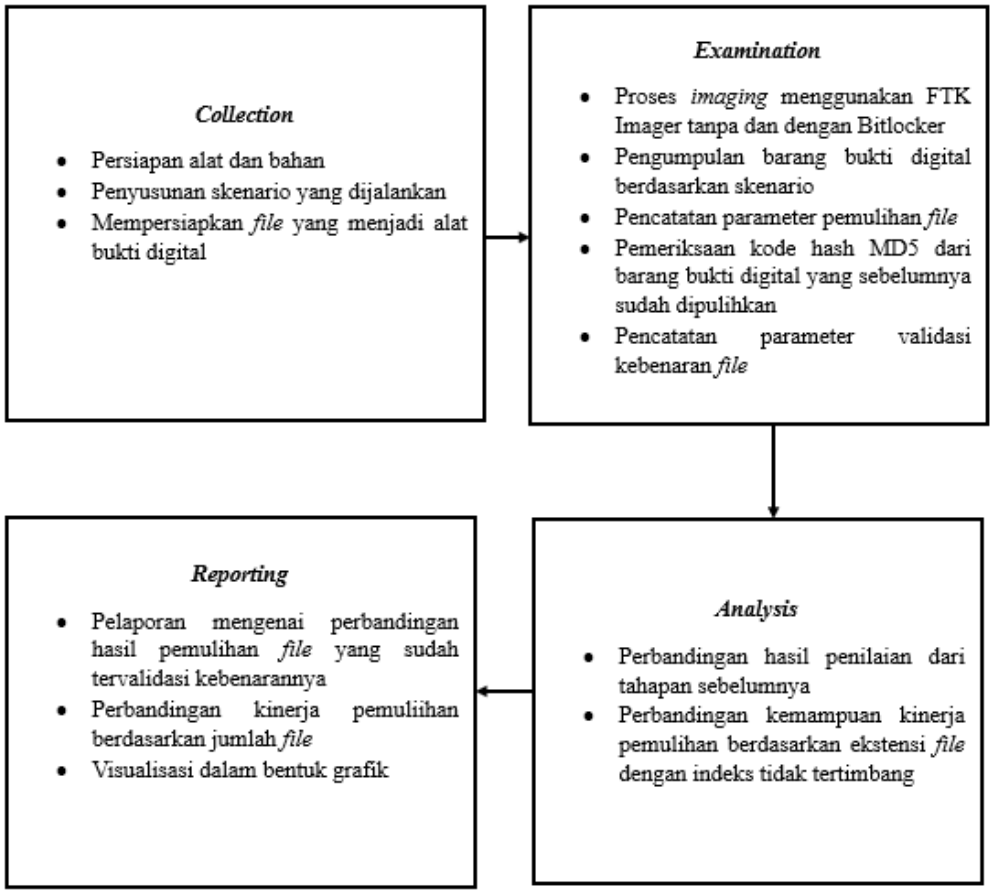
Dengan dilakukan penelitian ini, peneliti dapat memberikan wawasan yang berharga dalam memilih perangkat lunak yang paling sesuai dengan tujuan dan kebutuhan forensik tertentu. Ini akan membantu profesional forensik digital dalam menjalankan tugas mereka dengan lebih efektif dan efisien, serta mendukung integritas dan keamanan data. Selain itu, penelitian ini juga dapat memberikan kontribusi kepada pembaca dalam pengembangan lebih lanjut di bidang digital forensik.

METODE PENELITIAN

Metodologi yang dilakukan pada penelitian ini yaitu National Institute of Standards Technology (NIST) , Tahapan metodologi NIST ini dimulai dari Collection (Pengumpulan data),

Examination (Pengolahan data), Analysis (analisis hasil pemeriksaan), Reporting (Pelaporan).

Berikut ini merupakan rancangan dari penelitian yang akan dilakukan dengan menggunakan metodologi *framework* NIST (*National Institute of Standards Technology*) :



Gambar 3.1 Rancangan Penelitian

Adapun penjelasan mengenai rancangan penelitian yang akan dilakukan adalah sebagai berikut:

1. Collection (Pengumpulan)

Pada tahap ini akan dilakukan proses persiapan sebelum melakukan analisis perbandingan perangkat lunak untuk melakukan *file carving*. Adapun persiapan yang dilakukan yaitu :

a. Persiapan Alat dan Bahan

Diperlukan alat dan bahan sebagai penunjang dalam melakukan proses penelitian ini. Alat dan Bahan yang dibutuhkan berupa perangkat keras dan perangkat lunak seperti pada Tabel 1 berikut.

Tabel 1 Alat dan Bahan

Kategori	Nama	Kegunaan
Perangkat Keras	Laptop Acer Aspire E5-475G Windows 10 Pro	Digunakan untuk media dalam melakukan proses analisis forensik digital sekaligus pembuatan laporan penelitian
	Laptop Asus A455L Linux Ubuntu 22.04.1	Digunakan untuk media dalam melakukan proses analisis forensik digital
	Flash Drive SanDisk 16 GB	Digunakan untuk media penyimpanan *file* berisi barang bukti digital sekaligus menjadi barang bukti elektronik
Perangkat Lunak	FTK Imager	Digunakan untuk membuat *image* atau proses *imaging*
	Autopsy, PhotoRec, Scalpel, Foremost	Digunakan untuk analisis forensik digital dalam melakukan *file carving*
	BitLocker	Digunakan untuk mengenkripsi atau mengunci partisi pada windows dan *flash disk*

b. Persiapan Penyusunan Skenario

Skenario yang disusun pada penelitian ini adalah peneliti akan memasukkan *file* kedalam *flash drive* yang akan dijadikan sebagai kasus penemuan barang bukti elektronik dengan jenis dan ekstensi *file* berebeda yaitu gambar (jpg, png), video (mp4, avi), rekaman audio (mp3, wav), dan dokumen (docx, pdf). Setelah itu peneliti akan menghapus permanen seluruh isi dari *flash disk* yang menjadi temuan barang bukti elektronik, kemudian akan dilakukan analisis forensik digital pada *flash drive* tersebut untuk dilakukan *file carving* atau memulihkan kembali seluruh *file* yang menjadi barang bukti digital nantinya. Evaluasi kinerja perangkat lunak akan dilakukan pembagian skenario berdasarkan kondisi berbeda yaitu menggunakan *file image*

tanpa BitLocker, *file image* dengan BitLocker, dan *flash drive* langsung pada setiap jenis *file* gambar, *file* video, *file* audio, *file* dokumen. Selain itu terdapat pengujian yang akan dilakukan untuk analisis evaluasi kinerja berdasarkan 3 parameter yaitu kecepatan proses pemulihan, jumlah *file* yangberhasil dipulihkan, dan kebenaran *file* yang dipulihkan.

c. Persiapan file yang menjadi alat bukti digital

Pada tahap ini akan dilakukan proses pengumpulan barang bukti digital melalui pendekatan *static forensics* yaitu dengan melakukan proses *imaging* atau membuat salinan berupa *file* image dari *flash drive* yang menjadi barang bukti elektronik menggunakan perangkat lunak FTK Imager, proses *imaging* dilakukan sebanyak dua kali, yang pertama tanpa menggunakan enkripsi BitLocker dan keduamenggunakan enkripsi BitLocker. Selanjutnya dilakukan pengumpulan barang bukti digital berdasarkan 3 skenario yang sudah disusun yaitu *file image* tanpa BitLocker, *file image* dengan BitLocker, dan *flash drive* langsung. Pengumpulan dilakukan dengan teknik *file carving* dengan perangkat lunak Autopsy, PhotoRec, Scalpel, dan Foremost. Dalam melakukan pengumpulan barang bukti digital dilakukan juga pencatatan *file* yang berhasil dipulihkan serta kecepatan proses pemulihan pada setiap perangkat lunak.

2. Examination (Pemeriksaan)

Pada tahap ini akan dilakukan proses pengumpulan dan pemeriksaan barang bukti digital melalui pendekatan static forensics yaitu dengan melakukan proses imaging atau membuat salinan berupa file image dari flash drive yang menjadi barang bukti elektronik menggunakan perangkat lunak FTK Imager, proses imaging dilakukan sebanyak dua kali, yang pertama tanpa menggunakan enkripsi BitLocker dan kedua menggunakan enkripsi BitLocker. Selanjutnya dilakukan pengumpulan barang bukti digital berdasarkan 3 skenario yang sudah disusun yaitu file image tanpa BitLocker, file image dengan BitLocker, dan flash drive langsung. Pengumpulan dilakukan dengan teknik file carving dengan perangkat lunak Autopsy, PhotoRec, Scalpel, dan Foremost. Dalam melakukan pengumpulan barang bukti digital dilakukan juga pencatatan file yang berhasil dipulihkan serta kecepatan proses pemulihan pada setiap perangkat lunak.

Setelah dilakukan proses pemeriksaan dari barang bukti digital yang sebelumnya telah dipulihkan berdasarkan 3 skenario dan 4 perangkat lunak yang digunakan dalam *file carving*. Hasil dari masing-masing proses skenario dan perangkat lunak memiliki nilai unik hash MD5 yang digunakan dalam pengecekanintegritas dari barang bukti digital tersebut. Hash MD5 dari *file* pemulihan akan dibandingkan dengan hash MD5 *file* aslinya dan harus memiliki nilai hash yang sesuai sehingga dapat tervalidasi kebenarannya dan dapat

digunakan pada proses berikutnya dalam menganalisis evaluasi kinerja perangkat lunak forensik digital untuk melakukan *file carving*.

3. Analysis (Analisis)

Pada tahap ini akan 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 yaitu kecepatan proses pemulihan, jumlah *file* yang berhasil dipulihkan, dan kebenaran *file* yang dipulihkan akan dibandingkan pada setiap skenarionya dengan membuat skema pada setiap jenis *file*, sehingga hasil perbandingan akan dianalisis untuk mendapatkan hasil kinerja perangkat lunak pada setiap jenis *file* yang ada di setiap skenario. Selain itu pada tahap analisis dilakukan perbandinganekstensi *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.

4. Reporting (Pelaporan)

Pada tahap ini akan 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 dihitung menggunakan rumus indeks tidak tertimbang untuk mengetahui kinerja terbaik dari perangkat lunak *file carving*, selain itu hasil dari perbandingan juga divisualisasikan dalam bentuk grafik berdasarkan skenario yang ada agar lebih mudah dipahami setiap orang.

HASIL DAN PEMBAHASAN

Tahap ini merupakan bentuk pelaporan mengenai pengetahuan yang didapat dari proses sebelumnya. Perbandingan setiap perangkat lunak untuk melakukan *file carving* meliputi hasil proses disajikan dalam bentuk tabel agar dapat lebih mudah dipahami. Pada Tabel 4.58 berikut adalah rekap dari hasil pemulihan *file* yang diperoleh dan sudah terbukti kebenarannya dari skenario 1.

Tabel 4.2 Pelaporan Skenario 1

Skenario 1				
	Autopsy	PhotoRec	Scalpel	Foremost
Kecepatan Proses	51 menit 38 detik	6 menit 58 detik	16 menit 16 detik	29 menit 41 detik
Gambar	5	5	5	0
Video	10	10	0	0
Audio	10	10	5	0
Dokumen	9	9	1	6
TOTAL FILE	34	34	11	6

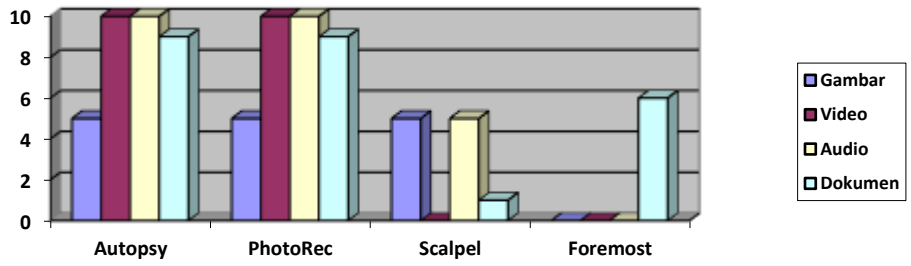
Hasil dari rumus indeks tidak tertimbang dari skenario 1 berdasarkan Tabel 4.58 untuk kinerja perangkat lunak Autopsy adalah 85%, PhotoRec adalah 85%, Scalpel adalah 27,5%, dan Foremost adalah 15%.

$$\text{Hasil Kinerja Autopsy} = \frac{34}{40} \text{x } 100\% = 85\% \quad (4.6)$$

$$\text{Hasil Kinerja PhotoRec} = \frac{34}{40} \text{x } 100\% = 85\% \quad (4.7)$$

$$\text{Hasil Kinerja Scalpel} = \frac{11}{40} \text{x } 100\% = 27{,}5\% \quad (4.8)$$

$$\text{Hasil Kinerja Foremost} = \frac{6}{40} \text{x } 100\% = 15\% \quad (4.9)$$



Gambar 4.2 Grafik Hasil Pemulihan File Skenario 1

Pada skenario 1 perangkat lunak dengan kinerja terbaik adalah PhotoRec karena memiliki kecepatan proses tercepat dan paramteter pemulihan dan persentase kebenaran *file* terbaik, grafik hasil pemulihan *file* dapat dilihat pada Gambar 4.55

Pada Tabel 4.59 adalah rekap dari hasil pemulihan *file* yang diperoleh dan sudah terbukti kebenarannya dari skenario 2.

Tabel 4.3 Pelaporan Skenario 2

Skenario 2				
	Autopsy	PhotoRec	Scalpel	Foremost
Kecepatan Proses	*Error*	10 menit 0 detik	16 menit 29 detik	29 menit 22 detik
Gambar	*null*	4	0	0
Video	*null*	10	0	0
Audio	*null*	8	0	0
Dokumen	*null*	9	1	6
TOTAL FILE	*null*	31	1	6

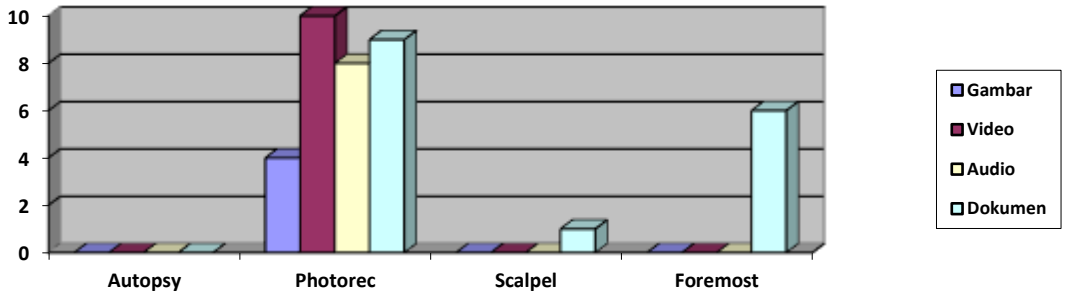
Hasil dari rumus indeks tidak tertimbang dari skenario 2 berdasarkan Tabel 4.59 untuk kinerja perangkat lunak Autopsy adalah tidak ada karena mengalami *error*, PhotoRec adalah 80%, Scalpel adalah 0%, dan Foremost adalah 20%.

$$\text{Hasil Kinerja Autopsy} = \frac{0}{40} \text{x } 100\% = 0\% \quad (4.10)$$

$$\text{Hasil Kinerja PhotoRec} = \frac{31}{40} \text{x } 100\% = 77{,}5\% \quad (4.11)$$

$$\text{Hasil Kinerja Scalpel} = \frac{1}{40} \text{x } 100\% = 2{,}5\% \quad (4.12)$$

$$\text{Hasil Kinerja Foremost} = \frac{6}{40} \text{x } 100\% = 15\% \quad (4.)$$



Gambar 4.3 Grafik Hasil Pemulihan File Skenario 2

Pada skenario 2 perangkat lunak dengan kinerja terbaik adalah PhotoRec karena memiliki kecepatan proses tercepat dan paramteter pemulihan dan persentase kebenaran *file* terbaik. Selain itu pada perangkat lunak Autopsy tidak dapat mengolah *file image* dengan enkripsi BitLocker sehingga proses analisis tidak dapat dilanjutkan, grafik hasil pemulihan *file* dapat dilihat pada Gambar 4.56

Pada Tabel 4.60 adalah rekap dari hasil pemulihan *file* yang diperoleh dan sudah terbukti kebenarannya dari skenario 3.

Tabel 4.4 Pelaporan Skenario 3

Skenario 3				
	Autopsy	PhotoRec	Scalpel	Foremost
Kecepatan Proses	56 menit 44 detik	11 menit 53 detik	34 menit 15 detik	26 menit 16 detik
Gambar	4	4	0	0
Video	10	10	0	0
Audio	8	8	5	0
Dokumen	9	9	1	0
TOTAL FILE	31	31	6	0

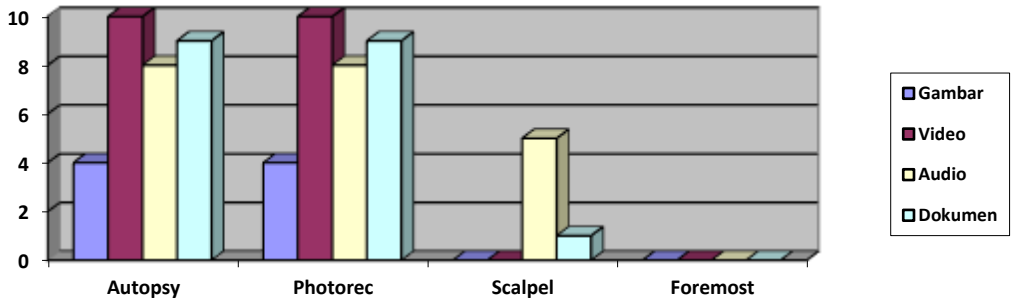
Hasil dari rumus indeks tidak tertimbang dari skenario 3 berdasarkan Tabel 4.60 untuk kinerja perangkat lunak Autopsy adalah 95%, PhotoRec adalah 95%, Scalpel adalah 0%, dan Foremost adalah 35%.

$$\text{Hasil Kinerja Autopsy} = \frac{31}{40} \text{x } 100\% = 77{,}5\% \quad (4.2)$$

$$\text{Hasil Kinerja PhotoRec} = \frac{31}{40} \text{x } 100\% = 77{,}5\% \quad (4.3)$$

$$\text{Hasil Kinerja Scalpel} = \frac{6}{40} \text{x } 100\% = 15\% \quad (4.4)$$

$$\text{Hasil Kinerja Foremost} = \frac{0}{40} \text{x } 100\% = 0\% \quad (4.5)$$



Gambar 4.4 Grafik Hasil Pemulihan File Skenario 3

Pada skenario 3 perangkat lunak dengan kinerja terbaik adalah PhotoRec karena memiliki kecepatan proses tercepat dan paramteter pemulihan dan persentase kebenaran *file* terbaik menyaingi perangkat lunak Autopsy yang memakan waktu cukup lama, grafik hasil pemulihan *file* dapat dilihat pada Gambar 4.57 berikut.

Berdasarkan pemaparan diatas dapat diambil rata-rata secara keseluruhan perentase dari kinerja pemulihan dan kebenaran *file* dari setiap perangkat lunak adalah sebagai berikut.

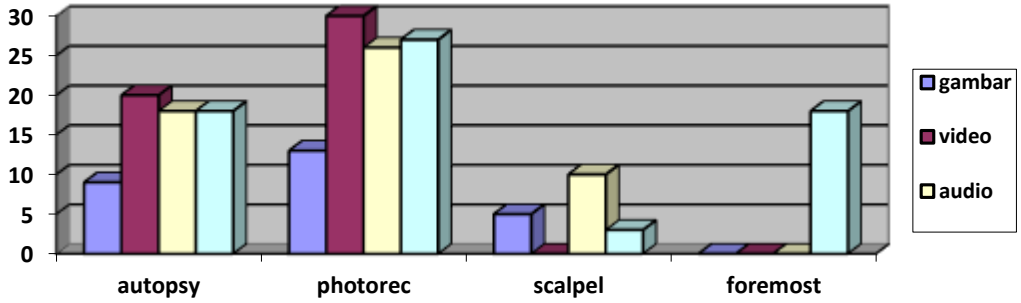
$$\text{Hasil kinerja rata} - \text{rata Autopsy} = \frac{85 + 0 + 77{,}5}{3} \text{ x } 100\% = 54{,}16\%$$

$$\text{Hasil kinerja rata} - \text{rata PhotoRec} = \frac{85 + 77{,}5 + 77{,}5}{3} \text{ x } 100\% = 80\%$$

$$\text{Hasil kinerja rata} - \text{rata Scalpel} = \frac{27{,}5 + 2{,}5 + 15}{3} \text{ x } 100\% \ = \ 15\%$$

$$\text{Hasil kinerja rata} - \text{rata Foremost} = \frac{15 + 15 + 0}{3} \text{ x } 100\% \ = \ 10\%$$

Grafik hasil pemulihan *file* secara keseluruhan dapat dilihat pada Gambar 4.58 berikut ini, menunjukkan PhotoRec memiliki hasil pemulihan dengan validasi kebenaran terbaik.



Gambar 4.5 Grafik Hasil Pemulihan Keseluruhan

Hasil evaluasi terhadap kinerja perangkat lunak forensik digital untuk *file carving* berdasarkan 3 parameter penilaian dan keseluruhan skenario yang dijalankan menghasilkan perangkat lunak terbaik dalam melakukan *file carving* adalah PhotoRec dengan rata-rata kinerja 80%. Selain itu perangkat lunak terbaik kedua adalah Autopsy dengan rata-rata kinerja 54,16%. Selanjutnya perangkat lunak terbaik ketiga adalah Scalpel memiliki rata-rata kinerja 15%. Sedangkan perangkat lunak Foremost mendapat peringkat terakhir yang memiliki nilai rata – rata kerja 10%.

DAFTAR PUSTAKA

Ali, R. R., Mohamad, K. M., Jamel, S., & Khalid, S. K. (2018). A Review of Digital Forensics Methods For JPEG File Carving. *Journal of Theoretical and Applied Information Technology, 96*(17).

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Efendi, T. F., Rahmadi, R., & Prayudi, Y. (2020). Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital. Jurnal Teknologi dan Manajemen Informatika, 6(2), 53-63.

Faiz, M. N., Prabowo, W. A., & Sidiq, M. F. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *Journal of Informatics, Information System, Software Engineering and Applications, 1*(1).

Pratama, A. K., Carudin, C., & Yusup, D. (2021). Analisis Perbandingan Perangkat Lunak Forensik

Digital untuk File. *Jurnal Sistem dan Teknologi Informasi*.

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), 3*(1).

Setiawan, M. N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3). *DATIN LAW JURNAL*, 1-21.

Sila, G. E., & Taufik, C. M. (2023). Literasi Digital Untuk Melindungi Masyarakat Dari Kejahatan Siber. KOMVERSAL, 5(1), 112-123.

Yudhana, A., Riadi, I., & Anshori, I. (2018). IDENTIFICATION OF DIGITAL EVIDENCE FACEBOOK MESSENGER ON MOBILE PHONE WITH NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY (NIST) METHOD. Jurnal Ilmiah Kursor, 9(3).

Yuwono, D. T., & W., Y. (2020). ANALISIS PERBANDINGAN FILECARVING DENGAN METODE NIST. Jurnal J-Sakti, 2(2).