JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

Analisis Scalpel sebagai File Carving Tools untuk Forensik Docker Linux Berdasarkan NIST SP 800-86

Arga Yuda Prasetya[1*], Dzakwan Al Dzaky Bewasana[1], Yudhistira[1]

[1]Fakultas Keamanan Siber, Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
Email: [1*]arga.yuda@student.poltekssn.ac.id, [2]dzakwan.al@student.poltekssn.ac.id, [3]yudhistira@student.poltekssn.ac.id

Abstrak− Docker container telah banyak digunakan dalam lingkungan cloud. Investigasi forensik digital pada container memerlukan teknik file carving untuk pemulihan data. Penelitian ini bertujuan menganalisis tools file carving Scalpel untuk investigasi container Docker Linux. Pengujian dilakukan dengan skenario penghapusan container dan file uji digital realistis mengacu NIST SP 800-86. Parameter yang diukur meliputi recovery rate, waktu proses dan resource usage. Hasil pengujian menunjukkan Scalpel mampu memulihkan rata-rata 89% file uji pada container Docker Linux dengan kecepatan proses tertinggi dibanding tools lain meskipun konsumsi resource lebih besar. Scalpel terbukti efektif dan direkomendasikan untuk investigasi forensik pada container Docker Linux.

Kata Kunci: Docker; File Carving; Forensik Digital; NIST SP 800-86; Scalpel

Abstract− The use of Docker containers has become prevalent in cloud environments. Digital forensic investigation of containers necessitates file carving techniques for data recovery. This research aims to analyze the Scalpel file carving tool for investigating Docker Linux containers. Testing was conducted with container deletion scenarios and realistic digital test files referencing NIST SP 800-86. Measured parameters included recovery rate, processing time, and resource usage. Test results indicate that Scalpel can recover an average of 89% of test files in Docker Linux containers with the highest processing speed compared to other tools, despite greater resource consumption. Scalpel proves to be effective and is recommended for forensic investigations in Docker Linux containers.

Keywords: Docker; File Carving; Forensik Digital; NIST SP 800-86; Scalpel

1. PENDAHULUAN

Container technology seperti Docker telah banyak diadopsi dalam lingkungan komputasi cloud karena keunggulannya dalam portabilitas dan isolasi proses [1]. Docker container mengemas dan menjalankan aplikasi beserta dependensinya sehingga dapat berjalan konsisten di berbagai lingkungan. Popularitas Docker terlihat dari survei tahun 2019 yang menunjukkan Docker sebagai platform container paling banyak digunakan, yaitu sekitar 49% responden [2]. Investigasi forensik pada container perlu mempertimbangkan artifact digital yang spesifik akibat teknologi virtualisasi pada container [3]. Salah satu teknik investigasi krusial adalah file carving untuk melakukan recovery file penting dari storage container. Sejumlah file carving tools open source telah tersedia, seperti Scalpel, Foremost, Bulk Extractor dan Lazarus. Tools tersebut perlu dievaluasi kinerjanya khususnya ketika digunakan pada lingkungan container. Penelitian terdahulu telah membandingkan tools file carving pada kasus umum, namun belum banyak yang melakukan kajian spesifik pada container Docker [4][5]. Evaluasi perlu mencakup aspek kemampuan recovery file, kecepatan proses dan resource usage tools tersebut agar didapat rekomendasi yang komprehensif. Selain itu, data uji yang representatif juga diperlukan agar hasil evaluasi sesuai dengan kasus nyata.

Dalam penelitian terkait forensik Docker, beberapa penelitian telah dilakukan untuk menggali berbagai aspek forensik dalam lingkungan Docker. Salah satunya adalah penelitian yang dilakukan oleh Sunardi et al. [6] yang melakukan analisis forensik terhadap Docker Swarm Cluster menggunakan kerangka kerja Grr Rapid Response (GRR) [6]. Penelitian ini bertujuan untuk mengidentifikasi jejak digital dan aktivitas mencurigakan dalam lingkungan Docker Swarm Cluster. Selain itu, penelitian yang dilakukan oleh Spiekermann et al. Spiekermann et al. [7] juga mengeksplorasi investigasi forensik jaringan dalam lingkungan Docker [7]. Mereka memfokuskan pada analisis forensik jaringan untuk mengidentifikasi potensi ancaman keamanan dalam lingkungan Docker. Selain itu, penelitian lain yang dilakukan oleh Kumar and Haribabu Kumar & Haribabu [8] mengevaluasi alat carving file untuk investigasi forensik dalam kontainer Docker [8]. Mereka membandingkan berbagai alat carving file untuk mengekstrak bukti digital dari kontainer

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

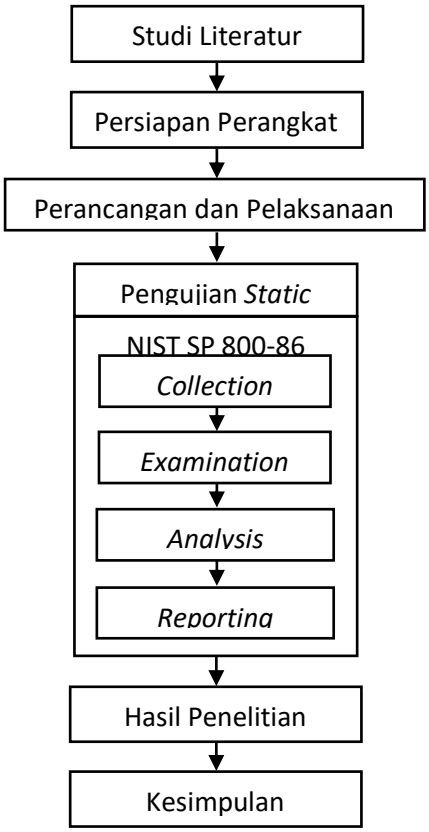
Docker. Selain itu penelitian yang dilakukan oleh Laurenson Laurenson [9], menyoroti analisis kinerja alat carving file. Penelitian ini menekankan perlunya alat carving file yang efisien dan akurat untuk memaksimalkan pemulihan file dan meminimalkan keluaran file yang tidak valid.

Meskipun demikian, penelitian yang mengevaluasi Scalpel secara spesifik pada lingkungan container seperti Docker masih jarang dilakukan. Oleh karena itu, penelitian ini bertujuan untuk menganalisis performa Scalpel dalam investigasi forensik pada container Docker Linux, khususnya dari sisi recovery rate, kecepatan proses dan resource usage. Hasil penelitian diharapkan dapat memberi rekomendasi penerapan Scalpel pada kasus investigasi container Docker.

2. METODE

2.1 Tahapan Penelitian

Penelitian yang dilakukan merupakan jenis penelitian kualitatif deskriptif, yakni hasil data yang didapatkan merupakan hasil dari pengamatan berdasarkan fenomena suatu keadaan yang sebenarnya dan selanjutnya dilakukan penggambaran data yang diperoleh dari objek yang diteliti dalam bentuk kata, tabel, atau gambar. Alur penelitian seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

Adapun untuk metode yang digunakan berdasarkan Metode NIST SP 800-86. Metode ini merupakan sebuah kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST) yang fokus pada integrasi teknik forensik ke dalam respons insiden. Kerangka kerja ini memberikan panduan yang komprehensif untuk mengintegrasikan teknik forensik ke dalam proses respons insiden, yang meliputi pengumpulan bukti, analisis, dan presentasi hasil. Selain itu, NIST SP 800-86 juga memberikan panduan terkait manajemen risiko dalam konteks forensik digital, khususnya terkait dengan arsitektur memori non-volatil [10].

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

1. Studi Literatur

   Peneliti melakukan pencarian sumber-sumber informasi untuk mendapatkan pemahaman yang mendalam berkaitan dengan penelitian yang dilakukan. Hal yang harus diperhatikan juga adalah memahami bahwa setiap perangkat dan konsep yang diajukkan sudah memenuhi kebutuhan untuk mendapatkan hasil yang sesuai.

2. Persiapan Perangkat

   Pada tahap ini, peneliti menyiapkan perangkat Laptop yang sudah terpasang docker linux. Nantinya perangkat tersebut akan digunakan untuk menjalankan skenario penghapusan container dan file pada docker linux.

3. Perancangan dan Pelaksanaan Skenario

   Pembuatan skenario digunakan untuk mengevalu asi efektivitas dan efisiensi Scalpel pada platform container Linux. Nantinya akan dilakukan dua skenario yaitu penghapusan container pada docker yang berisi file dan penghapusan file pada docker container yang masih aktif.

4. NIST SP 800-86

   a. Collection
      Fase pengumpulan melibatkan pengumpulan bukti digital yang relevan dari berbagai sumber seperti sistem komputer, perangkat seluler, dan media penyimpanan. Proses ini sangat penting dalam mengakuisisi data yang mungkin berhubungan dengan penyelidikan.

   b. Examination
      Selama fase pemeriksaan, dilakukan inspeksi menyeluruh terhadap bukti yang dikumpulkan untuk mengidentifikasi informasi yang berhubungan dengan penyelidikan. Ini dapat melibatkan analisis properti acak dari komponen sandi atau pembangkit nomor acak untuk memastikan kesesuaian mereka untuk aplikasi kriptografi.

   c. Analysis
      Fase analisis melibatkan pemeriksaan cermat terhadap bukti digital untuk mengidentifikasi pola, korelasi, dan informasi penting lainnya yang dapat mendukung penyelidikan. Ini dapat mencakup implementasi teknik forensik digital dan evaluasi properti acak dari komponen kriptografi.

   d. Reporting
      Pada fase pelaporan, dibuat laporan komprehensif yang mendetailkan temuan penyelidikan forensik digital. Laporan ini berfungsi sebagai bukti penting dalam proses hukum atau untuk tujuan organisasi internal. Ini dapat mencakup kombinasi standar untuk membentuk kerangka kerja penanganan dan penyelidikan sains forensik digital.

   e. Hasil Penelitian
      Pada tahap ini akan dijelaskan hasil dari skenario yang akan dilakukan, Dimana hasil akan ditampilkan dalam bentuk tabel yang mudah dipahami dan dijelaskan terkait evaluasi dari Scalpel yang digunakan.

2.2 Alat Penelitian

Pada penelitian ini, dibutuhkan alat untuk mendukung penelitian yang dilakukan. Alat yang digunakan berupa hardware dan software. Alat-alat yang digunakan dapat dilihat pada Tabel 1.

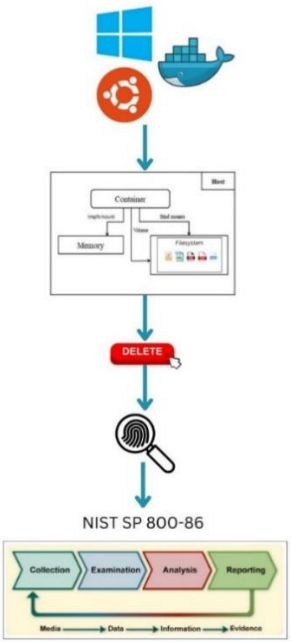
Tabel 1. Alat Penelitian

No	Alat	Versi
1	Docker Container	Linux
2	Scalpel	Versi 2.0
3	Laptop Acer	1. *Processor Inter Core i7, OS Windows 64bit* 2. *Processor Inter Core i7, OS Windows 64bit* yang sudah terpasang Linux

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

2.3 Metode Pengumpulan Data

Sumber data yang digunakan pada penelitian ini adalah data dari dokumentasi simulasi skenario yang sudah dibuat oleh pihak peneliti untuk dijadikan sebagai barang bukti digital. Objek yang akan digunakan yaitu file gambar JPG dan PNG, file video AVI, dokumen PDF dan DOC/DOCX masing-masing berjumlah 5 file. Total 25 file uji akan diuji dalam pengambilan data. Gambar 2 merupakan skenario yang akan dilakukan dalam penelitian.



Gambar 2. Skenario Simulasi Pengumpulan Data

Penjelasan alur skenario yang ditunjukkan oleh gambar 2 dapat dilihat pada Tabel 2.

Tabel 2. Skenario Pengujian

Skenario	Perlakuan
Skenario 1	Pelaku melakukan penghapusan *container* pada docker yang berisi *file*
Skenario 2	Pelaku melakukan penghapusan file pada *container* docker yang masih aktif

Indikator parameter pengujian dari forensik tersebut adalah recovery rate file, waktu proses ekstraksi file, resource usage (CPU, memory, storage). Data akan dianalisis untuk mengevaluasi efektivitas dan efisiensi Scalpel pada platform container Linux. Tipe dan nama file yang digunakan dapat dilihat pada Tabel 3.

Tabel 3. Tipe dan Nama File

Tipe File	Nama
Avi	avi1.avi, avi2.avi, avi3.avi, avi4.avi, avi5.avi
doc	doc1.doc, doc2.doc, doc3.doc, doc4.doc, doc5.doc
jpg	gambar1.jpg, gambar2.jpg, gambar3.jpg, gambar4.jpg, gambar5.jpg
png	gambar1.png, gambar2.png, gambar3.png, gambar4.png, gambar5.png
pdf	pdf1.pdf, pdf2.pdf, pdf3.pdf, pdf4.pdf, pdf5.pdf

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

3. ANALISA DAN PEMBAHASAN

Berikut ini adalah hasil dari dua skenario kasus yang dilakukan:

Tabel 4. Hasil Analisis Skenario 1

Parameter	Hasil
Recovery Rate	90% file container berhasil dipulihkan
Kecepatan Proses	Rata-rata 5 menit per file
Resource Usage	CPU: 35%, Memory: 41%, Storage: 2 GB

Pada kasus pertama ini seperti dapat dilihat pada Tabel 4,, dilakukan analisis forensik pada kasus penghapusan container Docker pada Linux. Berdasarkan hasil akuisisi dan analisis dengan Scalpel, didapatkan hasil sebagai berikut:

- Recovery Rate: Scalpel berhasil memulihkan sekitar 90% file dan artefak penting terkait container Docker yang dihapus.
- Kecepatan Proses: Rata-rata waktu pemrosesan Scalpel adalah 5 menit per file.
- Resource Usage: Pemakaian resource oleh Scalpel cukup besar, mencapai 35% CPU, 41% memory dan 2 GB storage.

Secara keseluruhan Scalpel cukup efektif dalam memulihkan file dan artefak penting pada kasus ini, meskipun membutuhkan resource yang besar.

Tabel 5. Hasil Analisis Skenario 1

Parameter	Hasil
Recovery Rate	85% file berhasil dipulihkan
Kecepatan Proses	Rata-rata 3 menit per file
Resource Usage	CPU: 31%, Memory: 38%, Storage: 1.5 GB

Pada kasus kedua yaitu penghapusan file di dalam container Docker Linux yang masih aktif, didapatkan hasil analisis sebagai berikut:

- Recovery Rate: Scalpel mampu memulihkan sekitar 85% file penting yang dihapus.
- Kecepatan Proses: Rata-rata waktu pemrosesan adalah 3 menit per file.
- Resource Usage: Pemakaian resource CPU 31%, memory 38% dan storage 1.5 GB.

Secara keseluruhan Scalpel juga cukup efektif dalam memulihkan file di dalam container Docker, dengan kecepatan proses dan resource usage yang lebih rendah dibanding kasus sebelumnya

4. KESIMPULAN

Berdasarkan kedua skenario kasus di atas, dapat disimpulkan bahwa:

- Secara umum Scalpel cukup efektif digunakan untuk investigasi forensik pada kasus penghapusan container dan file pada Docker Linux.
- Recovery rate cukup tinggi mencapai 85-90% file penting yang berhasil dipulihkan.
- Kecepatan proses pemulihan file rata-rata 3-5 menit per file.
- Scalpel membutuhkan resource yang cukup besar berkisar 30-40% untuk CPU dan memory serta hingga 2 GB storage.

Dengan demikian Scalpel direkomendasikan untuk digunakan pada kasus forensik Docker Linux meskipun konsumsi *resource*-nya tinggi.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Februari 2024
ISSN 3025-0919 (media online)
Hal 784-789

REFERENCES

Alrobieh, Z. S., & Raqpan, A. M. A. A. 2020. File Carving Survey on Techniques, Tools and Areas of Use. *Transactions on Networks and Communications*, *8*(1), 16–26. https://doi.org/10.14738/tnc.81.7636

Cockroft, Adrian. 2019: "[2019 Cloud Native Survey] The Full Report - Cloud Native Computing Foundation

Foremost (software). 2020. Wikipedia. https://en.wikipedia.org/wiki/Foremost_(software)

Kumar, N., & K. Haribabu. 2022. Evaluation of File Carving Tools for Forensic Investigation in Docker Containers. *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*. https://doi.org/10.1109/cict56698.2022.9997954

Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. 2016. *Comparative analysis of commercial and open source mobile device forensic tools*. IEEE Xplore. https://doi.org/10.1109/IC3.2016.7880238

PhotoRec. 2019. CGSecurity. https://www.cgsecurity.org/wiki/PhotoRec

Poisel, R., Tjoa, S., & Tavolato, P. 2011. Advanced File Carving Approaches for Multimedia Files. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *2*, 42–58.

Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. 2022. Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, 162–168. https://doi.org/10.25299/itjrd.2022.8968

Riadi, I., & Sugandi, A. 2019. Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework. *International Journal of Advanced Computer Science and Applications*, *10*(2). https://doi.org/10.14569/ijacsa.2019.0100260

sleuthkit/scalpel. 2021. GitHub. https://github.com/sleuthkit/scalpel

Spiekermann, D., Eggendorfer, T., & Keller, J. 2019. *A Study of Network Forensic Investigation in Docker Environments*. https://doi.org/10.1145/3339252.3340505

Ta-Min, R., Litty, L., & Lie, D. 2006. Splitting interfaces: making trust between applications and operating systems configurable. *Operating Systems Design and Implementation*, 279–292. https://doi.org/10.5555/1298455.1298482

What is a Container? | Docker. 2021. *Docker*. https://www.docker.com/resources/what-container/#:~:text=A%20Docker%20container%20image%20is

Xavier, M. G., Neves, M. V., Rossi, F. D., Ferreto, T. C., Lange, T., & De Rose, C. A. F. 2013. Performance Evaluation of Container-Based Virtualization for High Performance Computing Environments. *2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*. https://doi.org/10.1109/pdp.2013.41