JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

Implementasi Digital Forensik pada *VMware ESXi Server* Berbasis OS Windows 10 Menggunakan GCFIM

Irman Yunal Wirdani[1], Muhammad Habibi Motaain Nirbaya[1], Saca Ilmare Dinbiru[1*]

[1]Fakultas Keamanan Siber, Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
Email: [1]irman.yunal@student.poltekssn.ac.id, [2]muhammad.habibi@student.poltekssn.ac.id, [3*]saca.ilmare@student.poltekssn.ac.id

Abstrak− Dalam menghadapi perkembangan teknologi informasi, implementasi forensik digital pada lingkungan virtualisasi seperti Server VMware ESXi dan sistem operasi Windows 10 menjadi semakin penting. Virtualisasi server memungkinkan penggunaan bersama perangkat keras oleh sistem operasi yang berbeda, menghasilkan efisiensi sumber daya dan penghematan biaya. Dalam konteks ini, forensik digital pada VMware ESXi Server menjadi krusial untuk menyelidiki bukti digital dalam lingkungan virtual yang semakin bergantung pada infrastruktur TI modern. Penelitian ini memfokuskan forensik digital pada VMware ESXi Server dengan menggunakan Framework Generic Computer Forensic Investigation Model (GCFIM) berbasis OS Windows 10 serta dengan menggunakan tools Sleuth Kit (+Autopsy) dan FTK Imager dalam pelaksanaan forensic digitalnya. Pilihan Windows 10 sebagai dasar implementasi karena sistem operasi tersebut memiliki banyak pengguna. GCFIM memberikan pendekatan terstruktur untuk investigasi forensik digital, meningkatkan koordinasi dan efisiensi analisis bukti digital. Penelitian ini bertujuan untuk mengeksplorasi server VMware ESXi dengan metode GCFIM, terutama dalam konteks Windows 10, dengan harapan memperoleh akuisisi seluruh media virtualisasi penyimpanan. Temuan dari penelitian ini diharapkan dapat memberikan wawasan baru dalam pengembangan metode forensik digital untuk lingkungan virtual yang semakin kompleks.

Kata Kunci: Forensik Digital; GCFIM; VMware ESXI Server; Windows 10

Abstract− In the face of the development of information technology, the implementation of digital forensics on virtualization environments such as VMware ESXi Servers and Windows 10 operating systems is becoming increasingly important. Server virtualization allows the shared use of hardware by different operating systems, resulting in resource efficiency and cost savings. In this context, digital forensics on VMware ESXi Server becomes crucial for investigating digital evidence in virtualized environments that increasingly rely on modern IT infrastructure. This research focuses on digital forensics on VMware ESXi Server by using the Generic Computer Forensic Investigation Model (GCFIM) Framework based on Windows 10 OS and by using Sleuth Kit (+Autopsy) and FTK Imager tools in its digital forensic implementation. The choice of Windows 10 as the basis for implementation is because the operating system has many users. GCFIM provides a structured approach to digital forensic investigations, improving the coordination and efficiency of digital evidence analysis. This research aims to explore VMware ESXi servers with the GCFIM method, especially in the context of Windows 10, in the hope of obtaining acquisition of the entire storage virtualization medium. The findings from this research are expected to provide new insights in the development of digital forensics methods for increasingly complex virtual environments.

Keywords: Digital Forensic; GCFIM Method; VMware ESXI Server; Windows 10

1. PENDAHULUAN

Dalam era teknologi informasi yang terus berkembang, implementasi forensik digital pada lingkungan virtualisasi menjadi semakin krusial, terutama dengan adopsi teknologi seperti Server VMware ESXi dan sistem operasi Windows 10. Virtualisasi server adalah suatu teknik yang memungkinkan sistem operasi yang berbeda untuk menggunakan perangkat keras yang sama dan beroperasi secara bersamaan (Kumar & Charu, 2015). Penggunaan virtualisasi server memungkinkan penghematan sumber daya oleh orgaisasi untuk menekan biaya pembelian server baru dan terkait biaya pemeliharaan server (Ali & Sudyana, 2014). Penerapan forensik digital pada VMware ESXi Server sangat penting karena semakin bergantungnya lingkungan virtual pada infrastruktur TI modern. Kebutuhan analisis forensik pada virtual machine menjadi semakin penting untuk menyelidiki dan menganalisis bukti digital dalam lingkungan tersebut (Adam et al., 2022).

Pemilihan sistem operasi Windows 10 pada penelitian ini sebagai dasar implementasi yang sangatlah penting, karena sistem operasi ini banyak digunakan di lingkungan perusahaan dan memerlukan pertimbangan khusus untuk proses forensik digital (Adams et al., 2013). Penggunaan kerangka GCFIM memberikan pendekatan terstruktur terhadap investigasi forensik digital,

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

memastikan bahwa semua langkah yang diperlukan telah diambil untuk melestarikan, mengumpulkan, memeriksa, dan menganalisis bukti digital dengan cara yang baik secara forensik (Riadi et al., 2023). Kelebihan GCFIM mencakup kemampuannya untuk memfasilitasi identifikasi dan analisis bukti digital secara lebih terkoordinasi, sehingga investigator dapat mengikuti langkah-langkah yang terdefinisi dengan jelas, meningkatkan keakuratan dan efisiensi investigasi.

Pada penelitian (Sudyana, Prayudi, et al., 2019), dilakukan akuisisi dan analisis virtualisasi server menggunakan metode live forensik, dengan hasil akuisisi berhasil membaca seluruh isi partisi file dalam VM Ubuntu dan menemukan kembali enam file yang terhapus. Pada penelitian yang dilakukan Lim dkk (Lim et al., 2012), dilakukan penelitian untuk menyelidiki metode forensik digital untuk mesin virtual VMware Workstation dengan hasil memberikan metode pemulihan yang berharga bagi para penyelidik, memungkinkan mereka menyelidiki mesin virtual yang rusak secara efektif. pada penelitian (Domingues et al., 2022) dilakukan penelitian untuk mengalasisis sistem notifikasi Push Windows (WPN) Windows 10 dan 11 dengan hasil identifikasi artefak forensik yang terkait dengan WPN di Windows 10 dan Windows 11. sedangkan penelitian yang dilakukan oleh sudyana, et al (Sudyana, Putra, et al., 2019), dilakukan investigasi forensik digital terhadap virtualisasi server Proxmox dengan mengakuisisi seluruh media virtualisasi penyimpanan dan melakukan pengecekan terhadap hasil akuisisi tersebut dengan menggunakan metode SNI 27037:2014 dengan hasil yang menunjukkan bahwa teknik akuisisi dengan mengakuisisi seluruh media penyimpanan pada Proxmox tidak dapat digunakan karena struktur file dan folder bukti tidak dapat terbaca dengan sempurna.

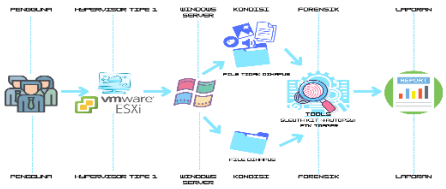
Oleh karena itu, berdasarkan penelitian terkait yang telah dijelaskan pada paragraf sebelumnya, penelitian ini dapat mengisi kesenjangan pengetahuan yang teridentifikasi. Seiring dengan penelitian sebelumnya yang fokus pada akuisisi dan analisis virtualisasi server, serta investigasi forensik digital pada berbagai platform seperti mesin virtual VMware Workstation dan sistem operasi Windows 10 dan 11, penelitian ini memfokuskan perhatian pada forensik digital pada VMware ESXi Server. Dengan menggunakan Framework Generic Computer Forensic Investigation Model (GCFIM) berbasis OS Windows 10. Pada penelitian ini juga akan menggunakan tools berupa Sleuth Kit (+Autopsy) dan FTK Imager karena memungkinkan untuk pemulihan data yang sesuai dengan skenario awal. Tools ini memiliki fungsi untuk akusisi, yang dapat diimplementasikan pada GCFIM pada bagian acquisition & preservation dan analysis yang memiliki kelebihan yaitu meliputi sumber terbuka, antarmuka pengguna grafis yang ramah pengguna, dan modularitas melalui sistem plug-in. Di sisi lain, FTK Imager unggul dengan kecepatan tinggi, dukungan untuk beberapa format file gambar, fitur pencarian yang efisien, serta integrasi yang baik dengan Forensic Toolkit (FTK). Penelitian ini bertujuan memberikan kontribusi signifikan dalam meningkatkan pemahaman forensik digital pada lingkungan server virtual VMware ESXi, dengan tujuan akhir memperoleh akuisisi seluruh media virtualisasi penyimpanan serta dapat memberikan wawasan baru dalam pengembangan metode forensik digital di lingkungan virtual yang kompleks.

2. METODE

Penelitian ini menggunakan pendekatan kualitatif dalam pengumpulan dan pengolahan data yang mana data akan didapatkan dengan cara pengumpulan data dan analisis data yang didapatkan dari keadaan yang sebenarnya. Pendekatan ini juga didukung dengan dilakukannya studi literatur mengenai penelitian yang dilakukan dan percobaan penelitian. Pengkajian hasil dilakukan dengan pendekatan kuantitatif yang mana hasil akan diolah dalam bentuk grafik dan persentase.

Bukti digital yang didapatkan dari hasil forensik pada penelitian ini akan ditampilkan sesuai dengan skenario yang ditunjukan pada Gambar 1.

2.1 Skenario Penelitian



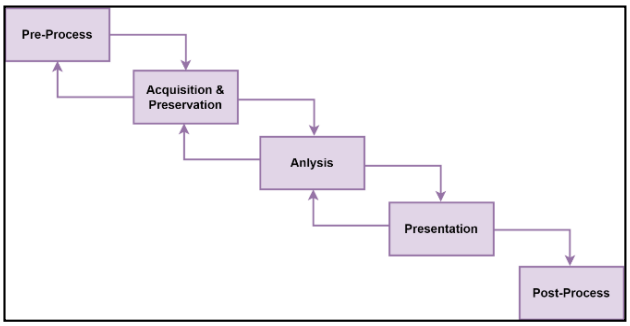
Gambar 1. Skenario Penelitian

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

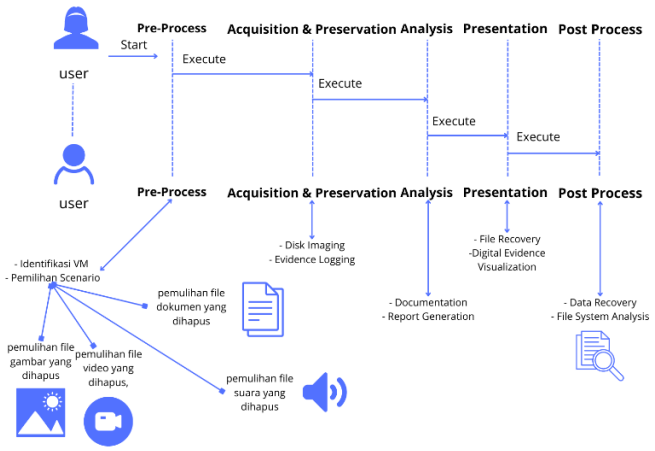
Skenario penelitian ini menggunakan metode GCFIM Framework dalam melakukan proses forensik digital pada virtual machine VMWare ESXi Server yang menunjukan hasil atau bukti digital setelah VM tersebut di forensik. Pada metode GCFIM Framework ini memberikan lima tahapan proses, yang diantaranya *Pre-Process*, *Acquisition & Preservation*, *Analysis*, *Presentation*, and *Post-Process*. Penelitian ini menggunakan *tools* Sleuth Kit (+Autopsy) dan FTK Imager. Pada gambar diatas, digambarkan skenario penelitian yang menjelaskan mengenai skenario penelitian yang diawali dengan penggunaan VMware untuk ESXi Server. Pada ESXi Server tersebut dipasangkan Windows 10 beserta dengan empat jenis *file* yang berbeda. Penelitian ini menggunakan dua skenario yang dibagi berdasarkan objeknya. Skenario I pemulihan *file* saat seluruh jenis *file* tidak dihapus dan skenario II merupakan pemulihan seluruh jenis *file* ketika *file* tersebut dihapus. Kedua scenario tersebut akan diuji dengan metode GCFIM Framework dan didapatkan bukti digitalnya berdasarkan jenis *file* yang berbeda. Pengujian dilakukan dengan melakukan forensik sejumlah 40 *file* berdasarkan pembagian tiap jenis dari video, dokumen, *file* suara, dan gambar masing-masing 10 item.

2.2 Tahapan Penelitian

Penelitian ini dilakukan dengan metode atau kerangka kerja GCFIM. Metode ini menunjukan Langkah-langkah yang sistematis dengan alur bolak-balik yang mana memungkinkan peneliti untuk Kembali ke tahap awal atau tahap sebelumnya jika terdapat perubahan dalam proses investigasi. Berikut tahapan yang digunakan dalam penelitian ini dengan menggunakan GCFIM:



Gambar 2. GCFIM *Method*



Gambar 3. Metode GCFIM serta Penggunaan *Tools*

2.2.1 *Pre-Process*

Dilakukannya kegiatan mempersiapkan kebutuhan investigasi, seperti tools, lingkungan forensik, dan sebagainya.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

2.2.2 *Acquisition & Preservation*

Dilakukannya kegiatan pengumpulan bukti digital atau data yang relevan dan pengamanan lingkungan yang akan di forensik, serta menjaga integritas dari bukti digitalnya.

2.2.3 *Analysis*

Dilakukannya analisis terhadap data yang didapat atau bukti digital yang didapat dengan tujuan untuk mengidentifikasi bukti digital yang didapatkan

2.2.4 *Presentation*

Dilakukan pemaparan hasil analisis kepada pihak yang berwenang dengan bahasa yang mudah dimengerti atas pelaksanaan forensik dengan didukung oleh bukti-bukti yang ada. Dengan adanya tahapan ini maka akan dihasilkan Keputusan yang dapat menjadi pendukung di hukum.

2.2.5 *Post-Process*

Dilakukan pengembalian bukti digital dan bukti fisik jika ada kepada pihak yang berwenang. Selain itu, investigator memastikan Kembali semua tahapan dari forensik digital ini terlaksana semua dan sesuai dengan protokolnya.

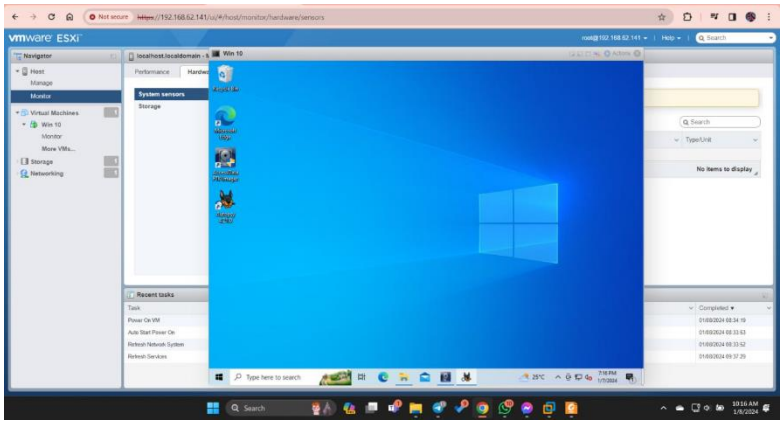
3. ANALISA DAN PEMBAHASAN

3.1 *Pre-Process*

Pada penelitian ini, penulis menggunakan tools berupa Sleuthkit (+Autopsy) dan FTK Imager yang dijalankan pada sistem operasi Windows 10 di dalam Esxi server. Berikut merupakan rincian dari tools dan lingkungan forensik yang digunakan.

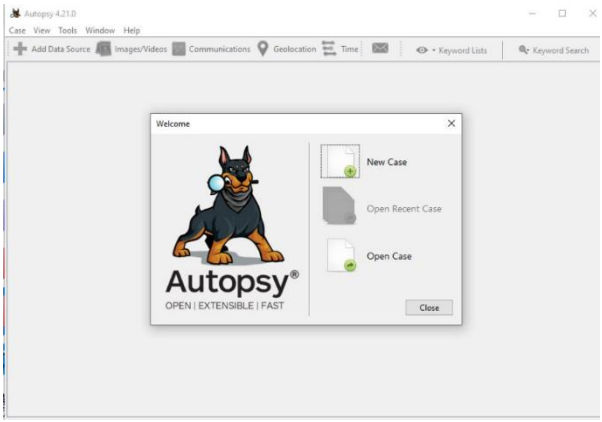
Tabel 3.1 Rincian Lingkungan Forensik

No	Objek dan Perangkat	Keterangan
1	Esxi Server	Versi 7
2	Sistem Operasi	Windows 10
3	FTK Imager	Versi 4.7.12
4	Autopsy	Versi 4.21.0.6
5	Flashdisk Sandisk	16 GB

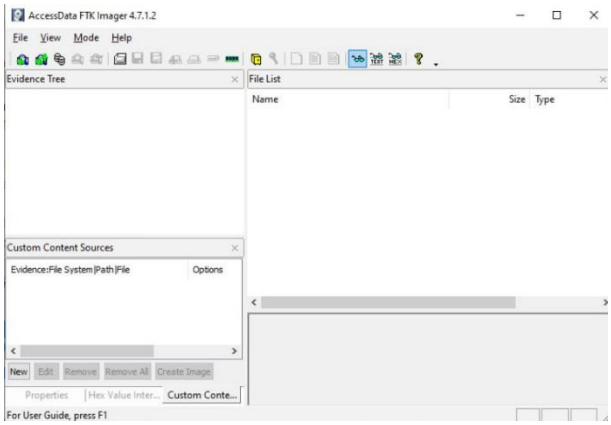


Gambar 4. Tampilan Windows 10

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773



Gambar 5. Tampilan *Autopsy*



Gambar 6. Tampilan FTK Imager

3.2 *Acquisition & Preservation*

Setelah mempersiapkan kebutuhan investigasi, dokumentasi dan pelabelan perangkat dilakukan pada tahap ini. Hasil identifikasi yang dilakukan peneliti ditunjukan pada tabel 3.2 sebagai berikut.

Tabel 2. Identifikasi Bukti Elektronik

Bukti Elektronik	Hasil Identifikasi
	1. Barang bukti dalam keadaan menyala 2. Bukti adalah laptop ASUS ROG STRIX G15 3. *System model:* ROG Strix G513RC_G512RC 4. *System Manufacture:* ASUSTek COMPUTER. INC 5. OS: Windows 11 Home Single Language 64-bit (10.0, Build 22631) 6. *Processor:* AMD Rayzen 7 6800HS with Radeon Graphics 7. S/N: R1NRKD021302049 8. RAM: 16GB 9. ROM: 1TB
	1. Barang bukti adalah Flashdisk Cruzer Blade Sandisk 2. Flashdisk berukuran 16 GB 3. Series: SDCZ50-016G

Selanjutnya tahap akuisisi yang merupakan tahap pengumpulan data pada perangkat dengan skenario yang sebelumnya ditentukan. Pengambilan data menggunakan metode *static forensics* yang

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

dilakukan pengambilan data pada memori internal pada windows 10 dalam Esxi server. Tahap ini dilakukan dengan menggunakan tools FTK Imager. Tahap ini dilakukan sebanyak skenario dengan file tidak dihapus dan file dihapus. Berikut adalah hasil perolehan yang dilakukan pada Tabel 3.

Tabel 3. Hasil Akuisisi Semua Dokumen Dihapus.

Jenis	.001
Ukuran	14664 MB
Nilai Hash	48df887f57787b8beb4209e72a87ed6e (MD5)
Durasi	2 menit 57 detik

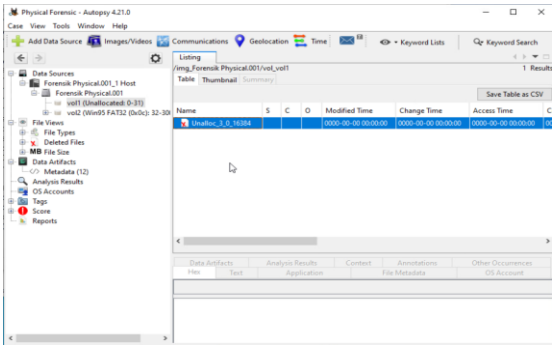
Tabel 2. Hasil Akuisisi Semua Dokumen Tidak Dihapus.

	Jenis	Ukuran	Nilai Hasil
Dokumen Berkas (.pdf, .txt, .xlsx)	.ad1	435 KB	31d1da05d0f07ce9add18f5cb7e67281
Dokumen Gambar (.png)	.ad1	22.7 MB	31d1da05d0f07ce9add18f5cb7e67281
Dokumen Suara (.mp3)	.ad1	1.81 MB	c249cc0d14edd6dfc75e051d161ad881
Dokumen Video (.mp4)	.ad1	21.9 MB	1677fc32abd10c993c2d889aa0117f89

3.3 Analysis

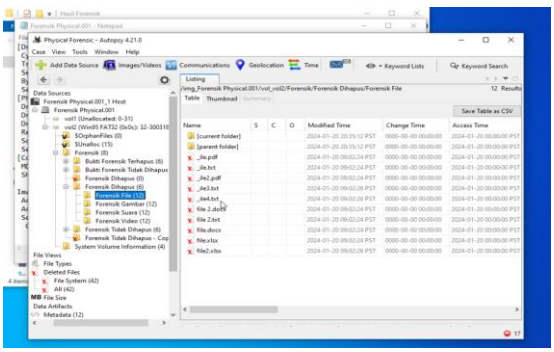
Setelah tahap akuisisi dan preservasi, langkah selanjutnya adalah menganalisis hasil yang di`peroleh. Data hasil skenario akan dikumpulkan untuk dilakukan analisis. Tahap analisis dilakukan untuk menemukan bukti digital dari skenario yang dijalankan menggunakan *tools Autopsy*.

Pada gambar 7. di bawah ini adalah hasil dari proses eksaminasi pada vol1 dan ditemukan hanya satu file.



Gambar 7. Hasil Eksaminasi

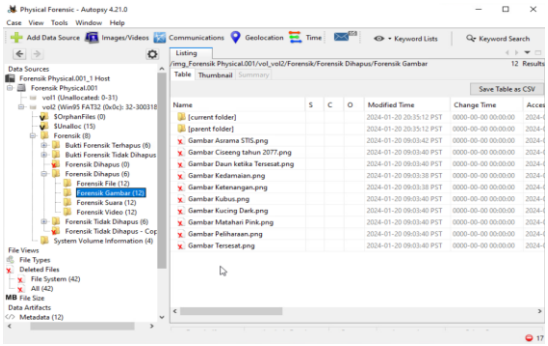
Gambar 8 di bawah adalah hasil dari proses eksaminasi pada vol2 dengan hasil ditemukan 14 dokumen dan 10 file.



Gambar 8. Hasil Akuisisi File Dihapus

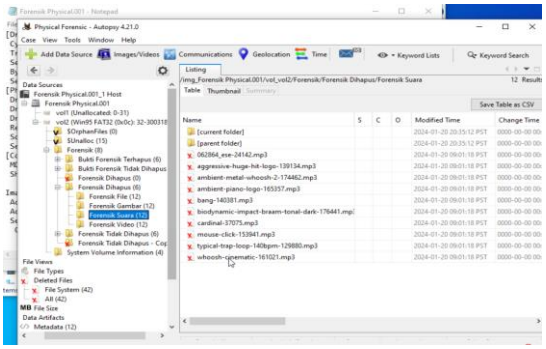
JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

Gambar 9 di bawah adalah hasil dari proses eksaminasi pada vol2 pada dokumen forensik gambar dan ditemukan 10 file.



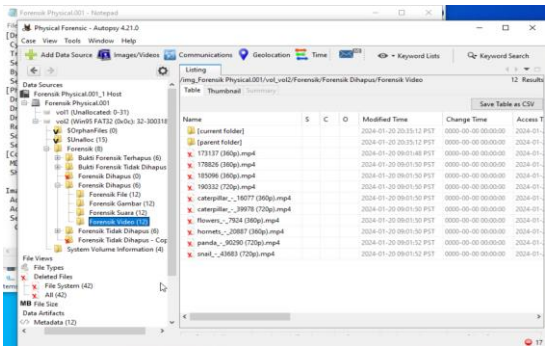
Gambar 9. Hasil Akuisis Gambar Dihapus

Gambar 10. di bawah adalah hasil dari proses eksaminasi pada vol2 pada dokumen forensik suara dan ditemukan 10 file.



Gambar 10. Hasil Akuisisi Suara Dihapus

Gambar 11 di bawah adalah hasil dari proses eksaminasi pada vol2 pada dokumen forensik video dan ditemukan 10 file.



Gambar 11. Hasil Akuisisi Video Dihapus

Tabel 5 menyajikan hasil akuisisi dan pemulihan dari beberapa dokumen dengan ekstensi yang berbeda-beda dengan skenario tidak dihapus objek-objeknya.

Tabel 3. Persentase Keberhasilan Akuisisi dan *Recovery* Pada Dokumen Tidak Dihapus

Objek / Tools	Akuisisi (FTK Imager)	Recovery (FTK Imager)
Dokumen Berkas (.pdf, .txt, .xlsx)	100%	100%
Dokumen Gambar (.png)	100%	100%

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

Dokumen Suara (.mp3)	100%	100%
Dokumen Video (.mp4)	100%	100%

Tabel 6. menyajikan hasil akuisisi dan pemulihan dari beberapa dokumen dengan ekstensi yang berbeda-beda dengan skenario dihapus objek-objeknya. Semua dokumen yang telah dihapus dapat dipulihkan kembali.

Tabel 4. Persentase Keberhasilan Akuisisi dan Recovery Pada Dokumen Dihapus

Objek / Tools	Akuisisi (FTK Imager)	Recovery (Autopsy)
Dokumen Berkas (.pdf, .txt, .xlsx)	100%	100%
Dokumen Gambar (.png)	100%	100%
Dokumen Suara (.mp3)	100%	100%
Dokumen Video (.mp4)	100%	100%

Tabel 7. menyajikan direktori penyimpanan dimana ditemukannya artefak yang telah dihapus pada *tools autopsy*.

Tabel 5. Direktori Penyimpanan Ditemukannya Artefak yang Telah Dihapus

Objek / Path	Direktori Penyimpanan Objek Tidak Dihapus	Direktori Penyimpanan Objek Dihapus
Dokumen Berkas (.pdf, .txt, .xlsx)	C:\Users\Saca Ilmare\Documents\Forensik Tidak Dihapus/Forensik File	/img_Forensik Physical.001/vol_vol2/Forensik/Forensik Dihapus/Forensik File
Dokumen Gambar (.png)	C:\Users\Saca Ilmare\Documents\Forensik Tidak Dihapus/Forensik Gambar	/img_Forensik Physical.001/vol_vol2/Forensik/Forensik Dihapus/Forensik Gambar
Dokumen Suara (.mp3)	C:\Users\Saca Ilmare\Documents\Forensik Tidak Dihapus/Forensik Suara	/img_Forensik Physical.001/vol_vol2/Forensik/ Forensik Dihapus/Forensik Suara
Dokumen Video (.mp4)	C:\Users\Saca Ilmare\Documents\Forensik Tidak Dihapus/Forensik Video	/img_Forensik Physical.001/vol_vol2/Forensik/ Forensik Dihapus/Forensik Video

3.4 *Presentation*

Penyajian dalam kerangka GCFIM (*Global Computer Forensic Investigation Methodology*) menandai langkah akhir dari proses investigasi forensik komputer. Tujuan pada tahap ini adalah untuk memaparkan hasil investigasi kepada pemangku kepentingan, baik dari internal maupun eksternal, dengan cara yang jelas dan komprehensif.

3.5 *Post-Process*

GCFIM (*Global Computer Forensic Investigation Methodology*) adalah suatu metodologi investigasi forensik komputer yang mencakup berbagai tahapan untuk mengumpulkan, menganalisis, dan menyajikan bukti digital. Tahap post-process atau pasca-investigasi pada GCFIM berperan sebagai langkah terakhir untuk menyelesaikan investigasi forensik digital, memastikan bahwa semua tahapan telah dilaksanakan dengan benar sesuai protokol yang telah ditetapkan. *Post-process* pada GCFIM terdiri dari beberapa hal, diantaranya yaitu pengembalian bukti digital dan fisik kepada pemilik bukti, pemeriksaan kembali (*Review*), pembuatan laporan akhir, pemusnahan sumber daya yang telah diforensik pada seseorang yang melakukan forensik, dan memperjelas mengenai evaluasi dan pembelajaran (*Lessons Learned*) karena penelitian ini dapat dijadikan acuan, pembelajaran, atau wawasan untuk penelitian lain terutama forensik.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 765-773

4. KESIMPULAN

Setelah peneliti menganalisis bukti digital melalui berbagai tahap dan skenario percobaan, maka dapat menarik kesimpulan. Dimana hasil dari penelitian digital forensik pada *VMware ESXi server* berbasis OS windows 10 menggunakan *Framework Generic Computer Forensic Investigation Model* (GCFIM) melalui dua skenario yaitu pada skenario pertama file tidak dihapus dan skenario kedua file dihapus, mendapatkan 100% bukti digital dari 10 dokumen file, 10 file gambar, 10 file suara, dan 10 file video. Pada skenario pertama, proses acquisition yang telah dilakukan dan terverifikasi bahwa tidak ada perubahan pada file, dapat disimpulkan bahwa file yang tidak dihapus masih dapat diakses dengan normal. Pada skenario kedua, *flashdisk* diformat menggunakan sistem file NFTS, namun hasil pemulihan tidak optimal. Kemudian, mencoba memformat dengan sistem file FAT32 menghasilkan pemulihan yang maksimal. Hasil pemeriksaan dan analisis menunjukkan bahwa semua jenis file, seperti dokumen, gambar, file suara, dan video yang dihapus, tetap dapat dibuka kembali melalui aplikasi autopsy. Hal ini dikarenakan flashdisk masih menyimpan jejak file yang dihapus di bagian deleted files, mirip dengan fitur recycle bin pada Windows yang memungkinkan pemulihan. Oleh karena itu, meskipun sudah dihapus, file tersebut masih dapat dipulihkan, dan file yang dihapus ditandai dengan tanda silang pada ikonnya.

REFERENCES

Ali, & Sudyana, D. 2014. *Virtualization Technology for Optimizing Server Resource Usage*. https://www.researchgate.net/publication/309920996

Adam, M., Alwi, E. I., & As'ad, I. 2022. *Analisis Forensik Terhadap Serangan Ddos Ping of Death pada Server* (Vol. 5, Issue 1).

Adams, R., Hobbs, V., & Mann, G. 2013. The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2013.1154

Domingues, P., Andrade, L., & Frade, M. 2022. A Digital Forensic View of Windows 10 Notifications. *Forensic Sciences*, *2*(1), 88–106. https://doi.org/10.3390/forensicsci2010007

Kumar, R., & Charu, S. 2015. An Importance of Using Virtualization Technology in Cloud Computing. In *Global Journal of Computers & Technology* (Vol. 1, Issue 2). www.gpcpublishing.com

Lim, S., Yoo, B., Park, J., Byun, K. D., & Lee, S. 2012. A research on the investigation method of digital forensics for a VMware Workstation's virtual machine. *Mathematical and Computer Modelling*, *55*(1–2), 151–160. https://doi.org/10.1016/j.mcm.2011.02.011

Riadi, I., Yudhana, A., & Saputra, R. V. A. 2023. Forensik Video Pada CCTV Menggunakan Framework Generic Computer Forensics Investigation Model (GCFIM). *JURIKOM (Jurnal Riset Komputer)*, *10*(2), 540. https://doi.org/10.30865/jurikom.v10i2.5888

Sudyana, D., Prayudi, Y., Mukhtar, H., & Sugiantoro, B. 2019. *Server Virtualization Acquisition Using Live Forensics Method*.

Sudyana, D., Putra, R. T., & Soni, S. 2019. Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037:2014. *Sinkron*, *3*(2), 67–72. https://doi.org/10.33395/sinkron.v3i2.10029