TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Analisis Forensik Ransomware Pada Sistem Berbasis Linux dengan Pendekatan Perbandingan Disk

Revandho Vianuara Dirgantoro*, Ahmad Luthfi

Fakultas Teknik Infustri, Program Studi Informatika, Universitas Islam Indonesia, Yogyakarta, Indonesia
Email: 1,*21917019@students.uii.ac.id, 2ahmad.luthfi@uii.ac.id
Email Penulis Korespondensi: 21917019@students.uii.ac.id

Abstrak–Penelitian ini bertujuan untuk menganalisis dampak infeksi *ransomware* Monti terhadap sistem operasi Linux melalui pendekatan forensik digital berbasis artefak dan metadata. Pengujian dilakukan dalam lingkungan laboratorium terisolasi menggunakan perangkat keras nyata, dengan metode akuisisi RAM dan *disk imaging* pada dua kondisi sistem: sebelum dan sesudah infeksi. Proses eksekusi *ransomware* dilakukan melalui *binary* monti.elf yang dijalankan dari direktori sementara /tmp, memicu enkripsi terhadap *file* operasional di direktori /Documents. Analisis dilakukan menggunakan tool Sleuthkit, dengan fokus pada struktur *file system*, *inode*, *timestamp*, dan distribusi artefak. Hasil menunjukkan bahwa *ransomware* Monti menggunakan teknik *in-place encryption*, di mana *file* asli disandikan tanpa perubahan *inode*. Artefak *ransomware* yang ditemukan meliputi *file* terenkripsi (.puuuk, .monti), *ransom note* (*readme.txt*), *log* eksekusi (result.txt), dan *binary* eksekusi (monti.elf). Seluruh artefak memiliki *timestamp* identik, mengindikasikan eksekusi otomatis dalam satu sesi. Validasi dilakukan melalui perbandingan sistem bersih dan terinfeksi, serta analisis entropy dan struktur komunikasi TOR dalam *ransom note*. Temuan ini memperkuat bahwa Monti beroperasi sebagai bagian dari ekosistem *Ransomware*-as-a-Service (RaaS), dengan pola infeksi yang efisien dan terstruktur. Penelitian ini memberikan kontribusi penting dalam pemetaan artefak *ransomware* Monti dan pengembangan metodo*log*i investigasi forensik berbasis Linux.

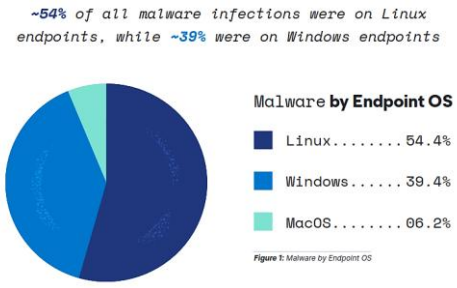
Kata Kunci: *Ransomware* Monti; Forensik Digital; Linux, In-Place Encryption; Sleuthkit, Artefak; TOR; RaaS

Abstract–This study aims to analyze the impact of Monti ransomware infection on Linux operating systems through a digital forensic approach based on artefacts and metadata. The investigation was conducted in an isolated laboratory environment using physical hardware, employing RAM acquisition and disk imaging methods on two system states: before and after infection. The ransomware execution was triggered by the monti.elf binary located in the temporary /tmp direktori, initiating encryption of operational files within the /Documents direktori. The analysis utilized Sleuthkit tools, focusing on file system structures, inode metadata, timestamps, and artefact distribution. Findings indicate that Monti employs an in-place encryption technique, replacing file contents without altering inode or block location. Key artefacts identified include encrypted files (.puuuk, .monti), ransom notes (readme.txt), execution logs (result.txt), and the ransomware binary (monti.elf). All artefacts share identical timestamps, suggesting automated execution within a single session. Validation was performed through comparative analysis of clean and infected systems, entropy measurements, and examination of TOR-based communication structures embedded in the ransom notes. These findings confirm that Monti operates as part of a Ransomware-as-a-Service (RaaS) ecosystem, with a structured and efficient infection pattern. This research contributes to the mapping of Monti ransomware artefacts and the development of forensic investigation methodologies tailored for Linux environments.

Keywords: Monti Ransomware; Digital Forensics; Linux; In-Place Encryption; Sleuthkit; Artefacts; TOR; RaaS

1. PENDAHULUAN

Malware semakin berkembang dan kompleks, dengan kemampuan mengadaptasi perilaku sistem yang ditargetkan sehingga sulit dideteksi. Identifikasi dan kombinasi faktor spesifik dari sistem yang terinfeksi menjadi kunci dalam pendeteksian *malware*. Kolaborasi antara pihak terkait dan peningkatan edukasi keamanan siber diperlukan untuk mengurangi risiko serangan *malware* (Imamverdiyev & Baghirov, 2024; Kumar et al., 2020). Windows adalah target utama serangan *malware*, dan para ahli keamanan siber telah fokus pada *malware* yang berbasis Windows. Namun, popularitas perangkat *Embedded* menyebabkan perubahan dalam jenis *malware* yang muncul. Perangkat *Embedded* telah digunakan dalam industri selama bertahun-tahun, namun kini semakin banyak digunakan dalam kehidupan sehari-hari, terutama karena perkembangan *Internet of Things* (IoT) (Alenezi et al., 2020; Ferdous et al., 2023).



Gambar 1. *Malware by Endpoint OS (Global Threat Report, 2022)*

Serangan *malware* terus menjadi ancaman siber paling distruptif di dalam era digital, menimbulkan kerugian finansial yang massif dan mengganggu operasional vital di berbagai sektor, mulai dari pemerintahan, Kesehatan, hingga infrastruktur kritis. Laporan (IBM Security, 2022) dan (IBM Security, 23 C.E.) industri yang bergerak dalam bidang

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

manufaktur masih menjadi yang tertinggi dalam serangan *malware*, namun *malware* yang digunakan dalam serangan sistem berbasis Linux menggunakan kode lama. Sebesar 54,4% *malware* menargetkan Linux, 34,4% menargetkan windows, dan 6,2% menargetkan MacOS. Tingginya infeksi pada sistem berbasis Linux disebabkan oleh banyak korporasi atau organisasi mengadopsi pendekatan *hybreid-cloud* dan menggunakan sistem Linux sebagai *backend* mereka.

Meskipun sistem operasi Linux secara historis diangga memiliki keamanan yang lebih kuat dibandingkan platform lain, semakin luasnya adopsi pada lingkungan server, *cloud computing*, perangkat *Internet of Things* (IoT), dana *embedded system* menjadikannya target yang menarik bagi pelaku kejahatan siber. Hal ini terbukti banyaknya laporan insiden *ransomware* yang menargetkan server – server berbasis Linux. Serangan *malware* terhadap sistem berbasis Linux terjadi diberbagai belahan dunia (Hristev et al., 2022; Korac et al., 2024). Cina menyebar varian *malware* Linux baru bernama PingPull sebagai bagian dari serangan *cyber espionage*. *Malware* ini sebelumnya dikenal sebagai 'Sword2033'. PingPull adalah RAT (*Remote Access Trojan*) yang menargetkan organisasi pemerintahan dan finansial di Australia, Rusia, Belgia, Malaysia, Vietnam, dan Filipina (Bill, 2023; Global Threat Report, 2022). Transparent Tribe merupakan kelompok peretas dari Pakistan menggunakan tool 2FA agensi pemerintah India untuk menyebarkan *backdoor* Linux baru bernama Poseidon. Kelompok ini dikenal sebagai APT36 dan telah menargetkan organisasi pemerintah India, militer, kontraktor pertahanan, dan entitas pendidikan (Ravie, 2023).

Malware atau Malicious Software adalah perangkat lunak berbahaya yang dirancang untuk mengganggu sistem, mencuri data, atau merusak *file*. Salah satu variannya adalah *ransomware*, yang mengenkripsi data korban untik pemerasan. *Ransomware* diklasifikasikan berdasarkan metode enkripsinya, termasuk *Hybrid Key Crypto-Ransomware* (HCR) yang menggabungkan enkripsi simetris dan asimetris, dan menjadi focus utama dalam analisis artefak pada sistem Linux yang terinfeksi (Davies et al., 2020; Kim et al., 2022; Koutsokostas & Patsakis, 2021; Umar et al., 2021).

Salah satu varian *ransomware* yang menunjukkan peningkatan aktivitas dan patut menjadi perhatian adalah Monti *Ransomware*, yang dikenal sebagai turunan dari keluarga Conti yang tangguh. Monti *Ransomware* telah dilaporan menargetkan berbagai organisasi, emnunjukkan kemampuan enkripsi yang efisien dan taktik penyebaran yang agresif. Salah satunya, terjadi serangan dari sebuah kelompok yang menggunakan Monti *Ransomware* untuk menyerang server sebuah universitas di negeara New Zealand, kelompok tersebut mengklaim bahwa telah mencuri data sebanyak 60 Giga*byte*s dari universitas tersebut(Jonathan, 2023). Serangan terbaru menargetkan sebuah perusahaan yang bergerak dalam bidang telekomunikasi di negara Amerika, kerugian yang disebabkan oleh serangan tersebut masih belum jelas. Namun serangannya dapat berupa enkripsi data, pencurian data, dan pemerasan(*Monti Ransomware Strikes Again: Omni Fiber LLC Falls Victim to Cyberattack - UNDERCODE NEWS*, 2025).

Penyelidikan kejahatan siber seperti serangan *ransomware* membutuhkan analisa *ransomware*. Hal ini membantu penyidik menentukan karakteristik dan identitas *ransomware* yang terlibat dalam tindak kejahatan digital (Joseph & Norman, 2020; Vehabovic et al., 2022). Analisa difokuskan pada *ransomware* pada sistem operasi Linux dengan melakukan pencarian dan analisis berbagai jenis *ransomware* di lingkungan Linux. Proses rekonstruksi dalam digital forensik dimanfaatkan untuk mengungkap apa yang terjadi dalam sistem yang terdampak oleh *ransomware* tersebut (Arfeen et al., 2022; Kara & Aydos, 2022). Penggunaan artifak dan data dalam digital forensik memungkinkan rekonstruksi serangan *ransomware* pada sistem operasi Linux, untuk memahami cara kerja dan dampak *ransomware* pada Linux. . Attribusi adalah proses untuk menentukan tindakan atau tujuan dari kejahatan yang dilakukan oleh individu atau kelompok (Esteves et al., 2023; Karafili et al., 2020).

Para siber kirminal mengembangkan *ransomware* agar tidak dapat atau sulit untuk dianalisa, ini bertujuan untuk mengaburkan jejak digitalnya atau mempertahankan kendali dari sebuah sistemnya. Beberapa Teknik yang digunakan, daintaranya *Code Obfuscation* yang meliputi eknripsi, *flattening control flow*, dan menambahkan *spurious code*. Teknik selanjutnya adalah sandbox evasion, dimana para siber kriminal memasukkan sebuah code untuk melakukan pengecekan atau mendeteksi apakah *malware* dieksekusi dalam sebuah lingkungan tertentu, seperti sandbox atau Virtual Machine (Wong et al., 2024). Dalam menghadapi ancaman ini, kemampuan untuk melakukan analisis forensik digital yang mendalam menjadi krusial. Analisis ini tidak hanya bertujuan untuk mengidentifikasi jejak digital yang ditinggalkan oleh *ransomware*, tetapi juga untuk memahami vektor serangan, metode penyebarannya, teknik penghindaran deteksi, serta dampak yang ditimbulkan. Informasi ini sangat berharga untuk proses investigasi, pemulihan sistem, dan oengembangan strategi pertahanan yang lebih efektif (Nayak et al., 2023; Yadav et al., 2024).

Penelitian (Carrillo-Mondéjar et al., 2020), berfokus pada *malware* yang menyerang perangkat *Internet of Things* (*IoT*), dengan memanfaatkan *machine learning*, peneliti menggunakan metode analisa *static* dan *dynamic* untuk mengusulkan metode baru. Dari penelitian tersebut, karakteristik *malware* dapat diekstraksi dengan menggunakan metode analisa yang diusulkan. Penelitian (De Vicente Mohino et al., 2021), peneliti mengusulkan metode analisa *malware* yang dikhususkan pada sistem Linux. Hasil dari penelitian tersebut, metode yang diusulkan dapt membantu mempertajam hasil dan kesimpulan dari karakteristik *malware*.

Pada penelitian (Li et al., 2024), peneliti meneliti bagaimana teknik untuk menghindari analisa dynamic pada android yang digunakan baik aplikasi maupun *malware* (*malicious software*). Hasil dari penelitiannya menyatakan bahwa terdapat kegagalan terhadap efektifitas dari analisa dynamic untuk melawan teknik penghindarannya. Penelitian (Imamverdiyev & Baghirov, 2024), peneliti meneliti mengenai teknik menghindari atau evasion dan beberapa langkah – langkah praktis untuk menanganinya. Dengan mengurai teknik untuk menghindari analisa dari studi ini dapat memberikan wawasan mengenai teknik penghindaran yang semakin berkembang mengikuti dengan lingkungan tekno*log*i yang ada.

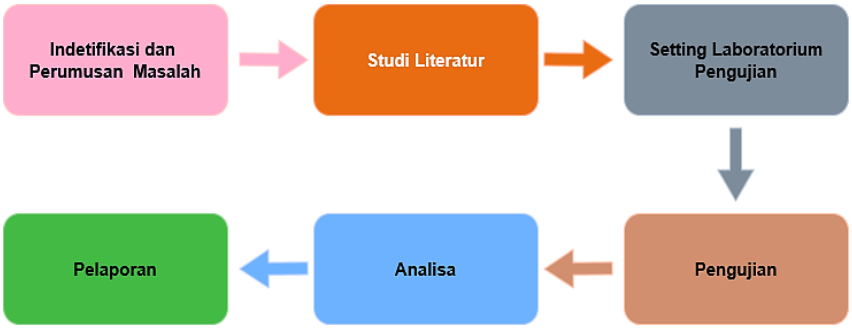
TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Penelitian ini mengusulkan analisis forensic komparatif berbasis artefak digital sebagai metodo*log*i yang tepat unutk mengatasi kesenjangan tersebut. Pendekatan ini akan focus pada identifikasi perubahan sistematis yang ditimbulkan oleh Monti *Ransomware* pada sistem Linux melalui analisis *disk imaging* dan memory dump. Dengan membandingkan artefak yang ditemukan pada sistem yang terinfeksi dengan sistem yang bersih, penelitian ini bertujuan untuk secara komprehensif mendokumentasikan jejak yang digtinggalkan oleh monti *ransomware*, termasuk *file* enkripsi, modifikasi konfigurasi, proses yang aktif, dan jejak dalam memori. Teknik ini dinilai lebih aman dan relevan dalam konteks penyelidiikan digital forensic, karena tidak memerlukan eksekusi langsung *ransomware* pada lingkungan yang terbuka.

Dengan demikian penelitian ini memiliki urgensi yang tinggi untuk mengembangkan pemahaman yang lebih baik tentang bagaimana Monti *Ransomware* beroperasi di ingkungan Linux dan bagaimana artefak digitalnya dapat dianalisis. Hasil penelitian ini diharapkan dapat menjadi panduan teknis bagi para praktisi forensic digital dan professional keamanan siber, serta berkontribusi pada pengembangan metodo*log*i investigasi yang lebih standar dan efektif dalam menghadapi ancaman *ransomware* yang terus berkembang di ekosistem Linux.

2. METODOLOGI PENELITIAN

Berikut Gambar 1 merupakan tahapan dari penelitian.



Gambar 2. Tahapan Penelitian

2.1 Identifikasi dan Perumusan

Tahap awal penelitian yang melibatkan indentifikasi masalah melalui penelusuran berita siber, laporan dari organisasi keamanan siber, serta jurnal ilmiah terbaru yang membahas serangan *malware* pada sistem operasi berbasis Linux. Proses ini dilakukan untuk mengkonfirmasi tren peningkatan serangan *ransomware* terhadap Linux dan mengidentifikasi ancaman spesifik seperti Monti *Ransomware*.

2.2 Studi Literatur

Tahap studi literatur adalah fondasi teoritis dan empiris penelitian. Tahap ini dilakukan secara berkelanjutan, dimulai setelah mengidentifikasi masalah, untuk memperkuat dasar teori, memahami *state of the art* dalam analisis forensik *malware*, serta mengidentifikasi kesenjangan penelitian. Sumber referensi yang digunakan berupa jurnal ilmiah, buku teks, artikel penelitian dari konferensi, laporan Teknik dari organisasi keamanan siber, dan sumber daring yang terpercaya. Fokus utama dalam studi literatur adalah pada konsep *ransomware*, kemanan sistem operasi Linux, teknik analisis *malware*, tantangan forensic digital pada Linux, dan studi – studi yang berkaitan dengan Monti *Ransomware*. Tujuan dari tahap ini adalah untuk merancang eksperimen yang relevan, memilih alat yang tepat, dan Menyusun metode analisis yang komprehensif.

2.3 Setting Laboratorium Pengujian

Pada tahap ini dijalankan proses untuk membangun laboratorium untuk melakukan pengujian terhadap sampel Monti *Ransomware*.

2.3.1 Perangkat Keras (*Hardware*)

Perangkat yang digunakan adalah laptop pribadi sebagai platform untuk melakukan pengujian. Pemilihan laptop didasarkan ketersediaanya dan spesifikasi yang dianggap cukup untuk menjalankan sampel ransomwre dan alat forensic tanpa virtualisasi ekstensif, sehingga mensimulasikan scenario penyerangan pada perangkat endpoint umum. Laptop Lenovo Thinkpad X250 dengan processor Intelcore i5, RAM 8GB, Hard*disk* 256GB, dengan sistem operasi Linux Debian 12 64-bit (dengan konfigurasi default, tanpa tambahan sistem keamanan atau virtual machine yang aktif untuk merepresentasikan *user environment* pada umumnya). Untuk menyimpan *file* akuisisi baik *file imaging disk*, digunakan hard*disk* eksternal sebesar 320GB.

2.3.2 Perangkat Lunak (*Software*)

Beberapa alat atau tool penting yang digunakan untuk mendukung proses akuisisi data dan menganalisa.

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Tabel 1. *Software* yang digunakan untuk penelitian

Jenis Artefak	Alat Akuisisi	Deskripsi Singkat Fungsi	Alat Analisis	Deskripsi Singkat Fungsi
Disk	*dc3dd*	Tool *command*-line untuk membuat Salinan bit by bit dari sebuah media penyimpanan (*disk imaging*), dengan fitur *hash*ing dan write-blocking.	Sleuthkit	Kumpulan tool *command*-line untuk menganalisa *file system* dan *disk* image, memungkinkan *file* recovery, analisis metadata dan identifikasi artefak.

2.3.4 Sample *Ransomware*

Sample Monti *Ransomware* diperoleh dari database *malware* terpercara *Malware*Bazar. Sample ini disimpan dalam format terkompresi yang dilindungi dengan kata sandi untuk mencegah eksekusi secara tidak disengaja. Sebelum dieksekusi, sample diekstrasi pada lingkungan yang terisolasi. Untuk mencegah infeksi meluas, koneksi jaringan pada perangakat pengujian dinonaktifkan sebelum sample dieksekusi. Tindakan ini untuk memastikan bahwa *malware* tidak dapat berkomunikasi dengan server C2 (*Command* and Control) atau menyebar ke perangkat lain dalam jaringan yang sama.

Pemilihan Monti *Ransomware* dalam penelitian ini didasarkan pada beberapa pertimbangan akademis dan praktis. Pertama, Monti adalah salah satu varian *ransomware* yang relative baru namun memiliki kemiripan dengan *ransomware* yang terkenal seperti Conti. Kedua, Monti tidak hanya menargetkan sistem berbasis Windows, tetapi juga sistem Linux. Ini menunjukkan bahwa peningkatan serangan infeksi *malware* pada sistem Linux mengalami peningkatan. Yang ketiga, Monti lebih *accessible* sebagai sampel penelitian dan dapat dieksekusi dalam lingkungan yang terkontrol. Dengan pertimbangan tersebut, Monti *ransomware* dipandang sebagai sampel representatif yang mampu menggambarkan dinamika ancaman *ransomware* pada sistem berbasis Linux sekaliguns memberikan peluang untuk mengidentifikasi artefak digital forensic yang relevan.

2.4 Pengujian

Pada tahap ini dilakukan pengujian atau uji coba menggunakan laboratorium yang dibangun. Dengan mengeksekusi *ransomware* pada perangkat (laptop), agar dapat mengetahui artefak yang ditinggalkan dan juga perilakunya. Setelah melakukan eksekusi maka akan dilakukan proses akuisisi, dimana proses ini untuk mendapatkan *file imaging* sebelum dan setelah *ransomware* menginfeksi.

2.4.1 Akuisisi Sistem Bersih (*Pre-Infection Baseline*)

Sebelum mengeksekusi *ransomware*, dilakukan akuisisi data dari sistem yang belum terinfeksi (clean state) untuk dijadikan sebagai perbandingan.

a. Preservasi Integritas *Disk*
   Untuk memastikan tidak ada modifikasi pada *disk* penyimpanan selama proses akuisisi berlangsung, digunakan mekanisme bernama write-blocking. Dalam implementasinya menggunakan *software* writeblocker yang ada pada Linux, menggunakan *blockdev*. Penggunaan *software write-blocker* blockdev dipilih karena keterbatasan sumber daya, namun disadari adanya resiko interaksi kernel yang lebih tinggi dibandingkan *hardware* weite-blcoker. Untuk menggunakan tool ini, *"blockdev –setro /dev/sdX*", ini akan mencegah *disk* penyimpanan berubah ketika proses akuisisi berlangsung.
b. Akuisisi *Disk*
   Proses akuisisi menggunakan *dc3dd*(atau *dcfldd*), sebuah tool untuk menyalin bit by bit dari seluruh Hard *Disk* (256GB). Perintah yang dimasukkan untuk menggunakan tool ini adalah "*sudo dc3dd if=/dev/sdX of=/path/to/disk_image.dd hash=sha256 log=/path/to/disk_image.log*". Nilai *hash* 256 disimpan dalam bentuk teks dalam sebuah *file* yang digunakan untuk memverifikasi integritas di kemudian hari.

2.4.2 Mengeksekusi *Ransomware*

Setelah mengakuisisi sistem bersih, selanjutnya proses untuk mengeksekusi *ransomware* pada sistem pengujian. Sample Monti *Ransomware* (dengan format ELF) dijalankan secara menual melalui terminal. Sebelum dieksekusi, mengubah izin dari monti *ransomware* dengan menggunakan *command* "*chmod +x monti.elf*", selanjutnya sample akan dijalankan pada direktori /tmp. Dengan menggunakan *command* "*./monti.elf –path <direktori atau file target>*", untuk mengeksekusi *ransomware*.

Sistem dikonfigurasi dengan sedemikian rupa agar mengelabuhi *ransomware* agar dapat mengeksekusi, dengan membuat sebuah folder baru Data Pegawai, Data Keuangan, dan Data Penjualan. Masing – masing folder berisi sebuah *file* sebanyak 3 dokumen dengan ekstensi .xlsx, masing – masing *file* memiliki ukuran sebesar 10KB, isi dari dokumen tersebut mengenai catatan fiktif dari sebuah organisasi didalam folder /Documents. Total data yang dienkripsi mencapai 390KB. Selama proses eksekusi, dampak awal yang ditumbulkan oleh *ransomware* secara langsung diamati, termasuk perubahan pada *file*, munculnya *file* tebuasan, dan proses yang berjalan. *Ransomware* diketahui mengenkripsi direktori yang ditargetkan /Documents, dan menambahkan ekstensi .puuuk pada *file* yang terenkripsi, tida lupa membuat *file Readme.txt* sebagai catatan tebusan.

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

2.4.3 Akuisisi Sistem yang Terinfeksi

Proses akuisisi *disk* diulang menggunakan *dc3dd* untuk membuat *disk* image dari sistem yang terinfeksi. Perintah yang sama seperti pada 3.5.1 digunakan, dengan *output* disimpan ke dalam *file* yang terpisah. Tidak lupa nilai *hash* disimpan kembali dalam bentuk teks.

2.5 Analisa

Tahap analisis dilakukan terhadap data yang telah diakuisisi (*disk* image dan memory dump dari sistem bersih dan terinfeksi). Pendekatan yang digunakan untuk menganalisa adalah pendekatan komparatif untuk mengidentifikasi perubahan yang disebabkan oleh Monti *Ransomware*.

2.5.1 Metode analisis komparatif

a. Perbandingan *Disk* Images
   Analisis menggunakan sleuthkit dan alat pendukungnya (fls, icat, blkstat) serta beberapa tools lainnya untuk membandingakan struktur *file*, *timestamp* (*MAC times*), izin *file*, keberadaan *file* yang terenkripsi (.puuuk), dan *file* tebusan (*Readme.txt*) antara sistem yang bersih dan sistem terinfeksi.
   1. Perbandingan *hash file*
      Menggunakan sha256sum untuk mendeteksi perubahan integritas *file* antara sistem bersih dan sistem yang terinfeksi.
   2. Analisis *filesystem*
      Fls digunakan untuk mengekstrak daftar file dan direktori dari image, *istat* digunakan untuk memerikasa metadata *inode*, termasuk *MAC time* dan izin akses.
   3. Identifikasi *file* terenkripsi dan catatan tebusan
      Pencarian *file* dengan ekstensi .puuuk sebagai indikator enkripsi dan melakukan dan memverifikasi keberadaan *file Readme.txt* sebagai *ransom note.*

2.5.2 Tujuan Analisis

Tujuan utama dari analsis ini adalah untuk mengidentifikasi perilaku Monti *Ransomware* dan artefak forensik yang ditinggalkan pada sistem Linux Debian 12 64 bit, sebagai dasar validasi dan dokumentasi dalam konteks investigasi digital forensik.

2.6 Pelaporan

Pelaporan adalah tahap akhir dari penelitian ini, setelah semua proses dilakukan dengan baik dan selesai. Mendokumentasikan seluruh proses penelitian, hasil dari pengujian dan proses analisa yang menghasilkan sebuah kesimpulan. Hasil laporan dari kesimpulan tersebut dapat digunakan sebegai referensi bagi penelitian selanjutnya dan dapat menjadi rujukan untuk para praktisi dalam menganalisa sebuah *ransomware*.

3. HASIL DAN PEMBAHASAN

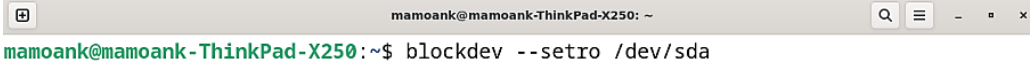
3.1 Setting Laboratorium

Sebelum mengeksekusi *ransomware*, perlu untuk membangun lingkungan laboratorium pengujian yang aman dan terkendali. Laboratorium pengujian tidak akan menggunakan *software* virtual machine, seperti Virtualbox, VMware, Qemu, dan *software* virtual machine lainnya. Namun akan menggunakan *hardware* (laptop) untuk pengujiannya, speseifikasinya sebagai berikut. Lenovo Thinkpad X250 dengan processor Intelcore i5, RAM 8GB, Hard*disk* 256GB, dengan sistem operasi Linux Debian 12 64-bit. Setelah selesai menginstal sistem operasi yang digunakan, perlu untuk membuat sebuah dokumen palsu atau tiruan dengan menggunakan artificial intelegent. Pembuatan dokumen dimaksudkan untuk melihat proses enkripsinya bekerja dan sekaligus menngelabuhi *ransomware* bahwa *hardware* atau laptop sering digunakan oleh suatu pengguna. Selanjutnya dilakukan penginstalan aplikasi atau *software* yang digunakan untuk melakukan akuisi *Disk*, seperti *dc3dd*. Hard*disk* eksternal digunakan untuk menyimpan *file imaging* dan RAM dump dari masing – masing sistem, yang belum terinfeksi dan yang sudah terinfeksi.

3.2 Pengujian

3.2.1 Akuisisi Sistem Bersih

Proses selanjutnya sebelum mengeksekusi *ransomware*, dilakukan proses akuisisi untuk mengambil *file imaging*.

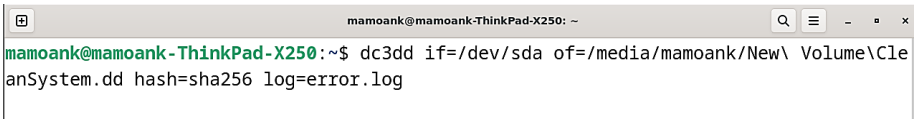


Gambar 3. Linux Writeblocker

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Untuk sistem yang belum terinfeksi sebelum menjalankan proses akusisi *Disk* maka perlu untuk menjalankan *software writeblocker* blockdev untuk menjaga integritas dari data, sehingga data tidak terkontaminasi atau berubah. *Writeblocker* dijalankan dengan perintah "*blockdev –setro /dev/sda*".

Proses selanjutnya mengakuisisi *disk*, untuk sistem yang belum terinfeksi. Tool yang digunakan untuk melakukan akuisisi adalah *dc3dd*, untuk menggunakannya dapat memasukkan *command* "*dc3dd if=/dev/sda of=/media/<user>/<Disk Eksternal>/UbuntuClean.dd log=error.log*".

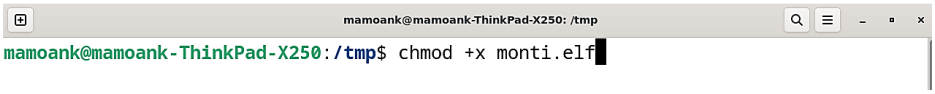


Gambar 4. Akuisisi *Disk* Clean Sistem

Command yang dimasukkan akan melakukan *imaging* dan mengirimkan *file imaging* kedalam *disk* eksternal yang digunakan untuk menyimpan *file* akuisi. Setelah akuisisi *disk* dan RAM selesai, untuk menjaga integritas dari *file* akuisisi perlu untuk menghitung nilai *hash* dari masing – masing *file* akuisisinya.

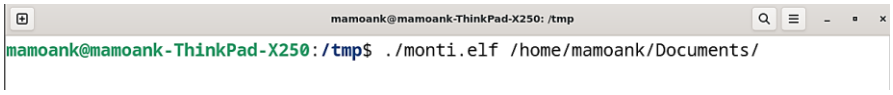
3.2.2 Mengeksekusi *Ransomware*

Setelah selesai dengan konfigurasi laboratorium pengujian dan mengakuisisi *Disk* sistem yang belum terinfeksi, akan dilakukan proses eksekusi atau menjalankan Monti *Ransomware*. Sebelum mengeksekusinya perlu untuk memastikan bahwa *hardware* (laptop) tidak terhubung dengan jaringan internet, karena perlu untuk memastika perangkat – perangkat sekitar aman. Setelah memastikan semua aman, maka Monti *Ransomware* dieksekusi. Untuk menjalankan atau mengeksekusi *ransomware*, perlu mengubah izin eksekusi pada *file ransomware* dengan perintah "*chmod +x Monti Ransomware*".



Gambar 5. Memberikan ijin kepada *file* monti.elf

Setelah memberikan izin untuk dieksekusi, maka *file ransomware* dapat dieksekusi "*./MontiRansomware*". Ketika pertama mengeksekusi *ransomware* terdapat error, karena sample *file* Monti *Ransomware* meminta parameter untuk merujuk pada direktori atau *file* yang akan diinfeksi atau dienkripsi. Dengan menambahkan paramaeter "*./MontiRansomware /home/<user>/Documents*" maka Monti *Ransomware* akan mengeksekusi seluruh *file* yang ada didalam direktori "*/home/<user>/Documents*".



Gambar 6. Mengeksekusi Monti *Ransomware* dengan Parameter

Setelah melakukan pengecekan didalam direktori "/Document", seluruh *file* yang ada didalamnya telah terenkripsi dengan ekstensi "*.puuuk*". Didalamnya terdapat *file* "*Readme.txt*" yang berisi mengenai instruksi untuk melakukan pembayaran tebusan.

3.2.3 Akuisisi Sistem Terinfeksi

Sebelum memulai proses akuisisi pada sistem yang terinfeksi, perlu diperhatikan bahwa langkah – langkah akusisi sebelumnya tidak dapat dilakukan. Karena diperlukan kehati – hatian untuk sistem yang telah terinfeksi, maka ada beberapa langkah yang dijalankan sebelum melakukan akuisisi. Untuk mencegah *ransomware* menyebar kedalam *disk* eksternal yang digunakan, tools writeblocker akan membantu untuk mencegah *ransomware* menginfeksi *disk* eksternal yang menjadi tempat penyimpanan *file* akuisisi. Terdapat 2 jenis *writeblocker* yang dapat digunakan, *software* dan *hardware*. Namun dalam penelitian ini menggunakan *software writeblocker* yang membantu proses akuisisinya.

Command yang dimasukkan "*blockdev –setro /dev/<disk yang ada didalam sistem>*", ini akan membuat *disk* didalam sistem yang akan diakuisisi tidak dapat dimodifikasi dan mencegah *ransomware* untuk menginfeksi *disk* eksternal.

Gambar 7. Linux Writeblocker

Blockdev akan mencegah agar tidak dimodifikasi dan mencegah *ransomware* menginfeksi penyimpanan eksternal. Proses selanjutnya mengakuisisi *disk*, untuk sistem yang terinfeksi. Tools yang digunakan untuk melakukan akuisisi adalah *dc3dd*, untuk menggunakannya dapat memasukkan *command* "*dc3dd if=/dev/sda of=/media/<user>/<Disk Eksternal>/InfectedSystem.dd log=error.log*".

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Gambar 8. Akuisisi *Disk* Sistem Terinfeksi

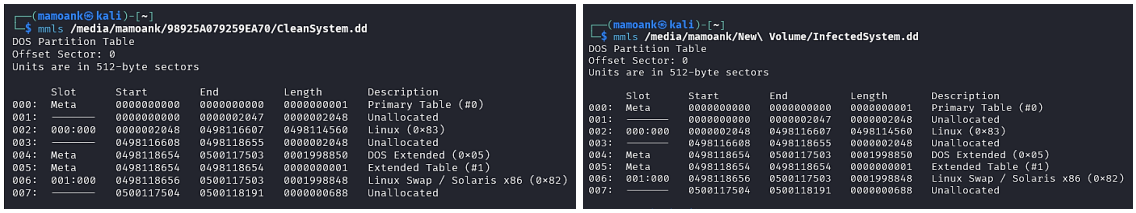
Command yang dimasukkan akan melakukan *imaging* dan mengirimkan *file imaging* kedalam *disk* eksternal yang digunakan untuk menyimpan *file* akuisi. Setelah akuisisi *disk* selesai, untuk menjaga integritas dari *file* akuisisi perlu untuk menghitung nilai *hash* dari masing – masing *file* akuisisinya. Setelah proses mengakuisisi antara sistem yang tidak terinfeksi dan terinfeksi selesai, akan dilanjutkan proses selanjutnya. Yaitu menganalisa *Disk* dengan cara membandingkannya, sehingga akan diketahui perbedaan dari kedua sistem.

3.3 Analisa

Proses analisa perbandingan *disk* adalah proses sistematis yang bertujuan untuk mengidentifikasi perubahan yang terjadi pada struktur dari *file* sistem yang terinfeksi oleh *ransomware*, dengan membandingkan dua kondisi sistem sebelum dan sesudah terinfeksi. Proses perbandingan dilakukan pada dua *disk* image yang diakusisi menggunakan tools *dc3dd* dari sistem yang terinfeksi dan tidak terinfeksi. Tools yang digunakan untuk melakukan analisa *disk* menggunakan *Sleuthkit*, yang memungkinkan untuk menganalisa *file system*, *inode*, *timestamp*, *file* tersembunyi, serta *file* yang telah dihapus atau dimodifikasi.

Proses pertama dalam melakukan analisa *disk imaging* adalah menghitung nilai dari *hash* value *file disk imaging* apakah terdapat perubahan atau tidak. Dalam analisa forensic digital menghitung nilah *hash* bertujuan untuk menjaga inteegritas dari barang bukti yang telah diakuisisi. Untuk menghitung nilai *hash* dari barang butki, digunakan tools dari linux *sha256sum*, *command* yang dimasukkan "*sha256sum <file>*". Dari hasil penghitungan *hash*, *file imaging copy* memiliki nilai *hash* yang sama dengan *file imaging* asli.

Setelah menghitung *hash value* dari masing – masih *file imaging*, dijalankan proses analisa *disk imaging*. Proses pertama adalah memeriksa struktur partisi dari masing – masing sistem, untuk memeriksa skema partisi, menganalisa partisi, dan mencari jika ada kekosongan dalam sistem. Selain itu, dapat membantu mengarahkan proses investigasi lebih lanjut, yang memungkinkan menemukan bukti yang dihapus atau disembunyikan. Tool "*mmls*" digunakan untuk memeriksa table partisinya, contoh penggunaannnya "*mmls <disk imaging>*" yang dapat terlihat pada gambar 9.

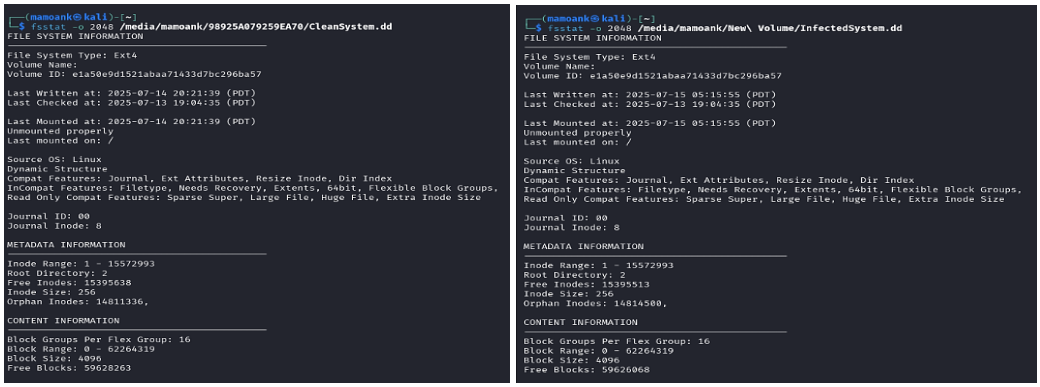


(a) (b)

Gambar 9. *Mmls* Sistem Terinfeksi (a) dan Sistem Bersih (b)

Dari *output* terlihat bahwa kedua sistem memiliki table partisi yang sama, tabel partisi yang digunakan kedua sistem adalah *DOS partition table*, yang dikenal dengan MBR (*Master Boot Record*) partition table. Sebuah tabel partisi yang telah lama digunakan dan masih digunakan dalam berbagai sistem. *Sector* dalam *disk* berukuran 512-*byte*.

Slot 002, memiliki berukuran lebih besar dibandingkan *sector* – *sector* lainnya, *sector* ini berisi partisi sistem operasi utama atau partisi data. Pada *sector* 2048 adalah area dimana Sebagian besar data yang relevan secara forensik ditemukan. Untuk pemeriksaan lebih lanjut, perlu untuk memeriksa *file system* apa yang digunakan pada *sector* 2048. Sehingga untuk memeriksa *file* sistem dapat menggunakan tools "*fsstat*", yang akan menampilkan informasi mengenai *file* sistem. *Command* yang dimasukkan adalah "*fsstat -o <offset sector> <disk imaging>*".

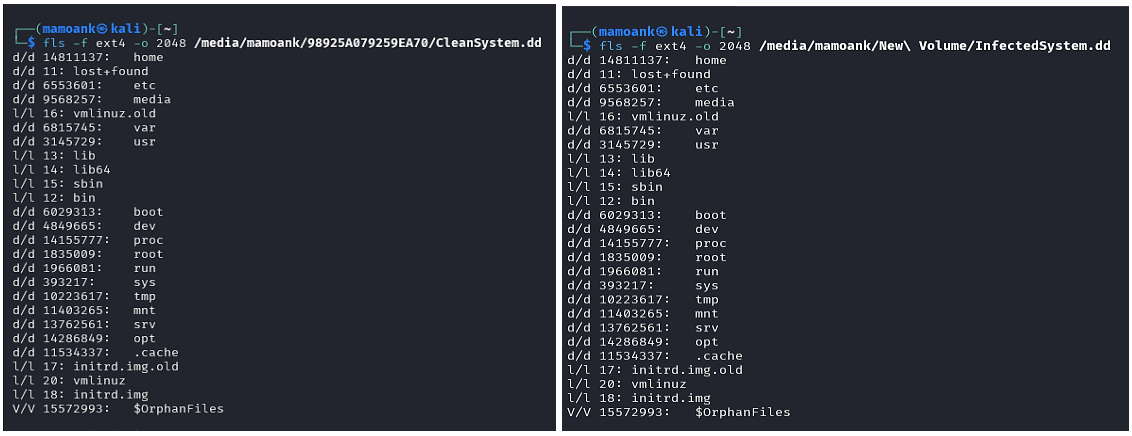


(a) (b)

Gambar 10. *Mmls* Sistem Terinfeksi (a) dan Sistem Bersih (b)

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Dari hasil *output* yang ditampilkan, kedua sistem menggunakan EXT4. Dan terdapat beberapa informasi lainnya mengenai *Volume ID*, *Last Writen*, *Last Checked*, dan informasi lain mengenai *file system* dari kedua sistem. Proses selanjutnya adalah memeriksa *file* yang ada didalam *sector* 2048. Untuk memeriksa *file* yang ada didalamnya baik itu *file* yang terhapus atau disembunyikan, tool "*fls*". Tool ini digunakan untuk melakukan enumerasi direktori dan *file*, termasuk mengidentifikasi *file* yang terhapus maupun yang disembunyikan dari sistem berkas. *Command* yang dimasukkan "*fls -o <offset sector> <file disk imaging>*".

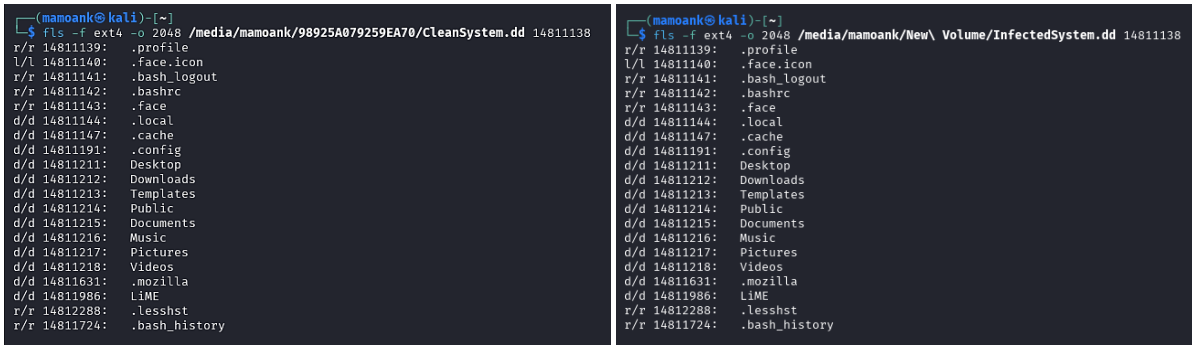


(a) (b)

Gambar 11. *Fls* Sistem Terinfeksi Dan Sistem Bersih

Output dari kedua sistem menunjukkan memiliki kesamaan, partisi dari *sector* 2048 merupakan partisi utama dan menampilkan struktur direktori dari Linux. Dari *output* yang ditampilkan dari tools akan membantu secara langsung mengidentifikasi area yang menjadi kunci untuk investigasi forensik. Pada penelitian ini investigasi akan berfokus pada direktori */Documents* yang berada didalam direktori /*<user>*, untuk melihat perubahan yang terjadi pada sistem.

Proses dilanjutkan dengan menganalisa direktori /*<user>*, tools yang digunakan masih sama *fls*. Namun *command* ditambahkan *inode* dari directori */home* dan dilanjutkan dengan *inode* dari direktori /*<user>*, *command* yang digunakan sebagai berukut "*fls -o <sector> <file imaging> <inode>*". Pada direktori yang dituju berada pada *inode* 14811137 dan masuk kedalam direktori user dengan *inode* 14811138, yang berisi setiap *file* yang akan dianalisa.

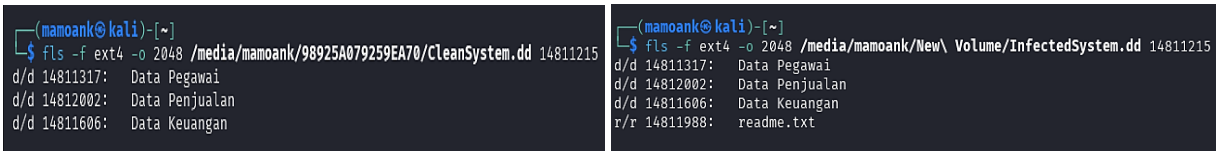


(a) (b)

Gambar 12. *fls* Sistem Terinfeksi (a) dan Sistem Bersih (b)

Dari masing – masing sistem, yang terlihat pada gambar 14 tidak ada perbedaan yang mencolok dari kedua sistem, dan masing – masing dari sistem masih memiliki kesamaan. Untuk proses selanjutnya akan dilakukan pemeriksaan pada direktori */Documents*, karena menjadi sasaran dalam serangan *malware*.

Untuk memeriksa direktori /Documents, penggunaan tool *fls* masih digunakan untuk membantu dalam pemeriksaannya dengan menambahkan *inode* direktori */Documents* miliki. *Output* dari penggunaannya dapat terlihat dalam Gambar 13.



(a) (b)

Gambar 13. *fls* Sistem Terinfeksi (a) dan Sistem Bersih Direktori */Documents* (b)

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Analisa pada direktori */Documents* pada sistem yang tidak terinfeksi tidak mengalami modifikasi. Terdapat subdirektori yang berisi mengenai data operasional, tidak ditemukan *file* terenkirpsi, artefak *ransomware*, mauun *file* yang dihapus. Pada sistem yang terinfeksi terdapat penamahan *file readme.txt* yang tidak ditemukan pada sistem yang tidak terinfeksi. *File* ini berstatus aktif (r/r) dan memiliki *inode* 14811988, yang mengindikasi bahwa *Monti Ransomware* telah menyisipkan artefak *ransom note* didalam direktori yang ditergetkan.

Dengan perbedaan dari masing – masing sistem, terdapat *file readme.txt* yang akan dianalisa lebih lanjut untuk mengekstrak informasi yang ditinggalkan oleh *ransomware*. Untuk memeriksa metadata dari *file readme.txt*, yang dapat digunakan untuk mengungkapkan jejak digital dari *file*. "istat" tool yang digunakan untuk melakukan ekstraksi metadata dari sebuah *file*, untuk penggunaanya istat -f <*file system*> -o <*disk sector*> <*disk imaging*> <*inode file*>.

```
┌──(mamoank㉿kali)-[~]
└─$ istat -f ext4 -o 2048 /media/mamoank/New\ Volume/InfectedSystem.dd 14811988
inode: 14811988
Allocated
Group: 1808
Generation Id: 526656151
uid / gid: 1000 / 1000
mode: rrw-------
Flags: Extents,
size: 1907
num of links: 1

Inode Times:
Accessed:       2025-07-15 06:58:17.007987183 (PDT)
File Modified:  2025-07-15 06:58:17.007987183 (PDT)
Inode Modified: 2025-07-15 06:58:17.007987183 (PDT)
File Created:   2025-07-15 06:58:17.007987183 (PDT)

Direct Blocks:
58711669
```

Gambar 14. istat *readme.txt*

Dari hasil analisa metadata terdapat *file readme.txt* yang dilakukan, menunjukkan bahwa ransom nite dibuat secara eksplisit oleh *ransomware* pada tanggal 2025-07-15 pukul 6:58:17 (PDT). *File* ini memiliki *inode* 14811988, dengan status aktif. *Timestamp* akses, modifikasi, dan pembuatan yang identic mengindikasikana bahwa *file* dibuat dalam satu eksekusi.

Pemeriksaan selanjutnya mengekstrak data yang ada didalam *readme.txt* atau *ransom note* dengan menggunakan"*icat*". Sebuah tools yang digunakan untuk melihat isi dari suatu *file*, *command* yang dimasukkan "*icat -o* <*disk sector*> <*disk imaging*> <*inode file*>".

```
┌──(mamoank㉿kali)-[~]
└─$ icat -f ext4 -o 2048 /media/mamoank/New\ Volume/InfectedSystem.dd 14811988
All of your files are currently encrypted by MONTI strain. If you don't know who we are - just "Google it."

As you already know, all of your data has been encrypted by our software.
It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. Howeve
r,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the
 publication of whole compromised data immediately.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid.onion/chat/c7c5b8b0703950c40e6614bf957f94c1/

Our blog :
(also through TOR)

http://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid.onion

YOU SHOULD BE AWARE!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
Inform your supervisors and stay calm!
```

Gambar 15. *icat readme.txt*

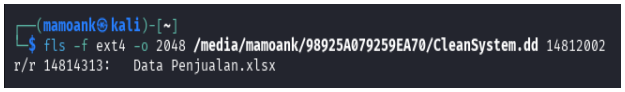
Hasil dari ekstraksi *file readme.txt* melalui icat menunjukkan bahwa *readme.txt* berisi pesan yang sangat terstruktur, berisi mengnai ancaman publikasi data, larangan kontak dengan pihak ketiga, serta instruksi pembayaran melalui jaringan TOR. Pesan untuk membayar tebusan untuk dapat mengakses kembali *file* yang telah terenkripsi merupakan ciri khas dari *ransomware*. Didalam pesan *ransom note* juga terdapat 2 (dua) link untuk melakukan pembayarannya:

1. http://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid.onion/chat/c7c5b8b0703950c40e6614bf957f94c1/
2. http://mb*log*ci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid.onion

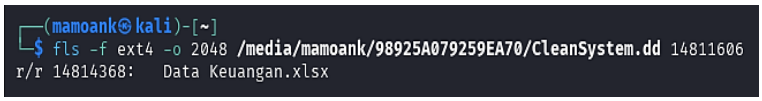
Kedua link hanya dapat diakses menggunakan TOR browser, sehingga diperlukan beberapa pengaturan untuk mengaksesnya. Pemeriksaan dilanjutkan dengan memeriksa subdirektori */Document*s, karena terdapat direktori yang berisi dokumen – dokumen yang dapat dianalisa lebih lanjut. Terdapat 3 folder yang dapat diperiksa, Data Pegawai, Data Penjualan dan Laporan Keuangan.

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

(a)



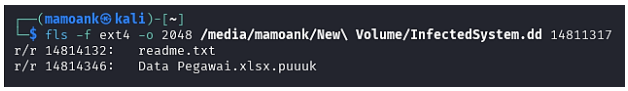
(b)



(c)

Gambar 16. *Subdirektori /Documents* Sistem Tidak Terinfeksi: (a) Data Pegawai, (b) Data Penjualan, dan (c) Data Keuangan

Dari pemeriksaan yang dilakukan, masing – masing subdirektori pada sistem yang tidak terinfeksi berisi satu *file* aktif dengan ekstensi *.xlsx* dengan *inode* masing – masing. Setiap *file* yang ada didalam direktori tidak menunjukkan adanya enkripsi atau modiikasi, dan tidak ditemukan artefak *ransomware* berupa *ransom note* atau *file* yang terenkripsi. Sementara itu pada sistem yang terinfeksi menunjukkan adanya pola infeksi dari masing – masing *file* yang ada didalam direktori.



(a)

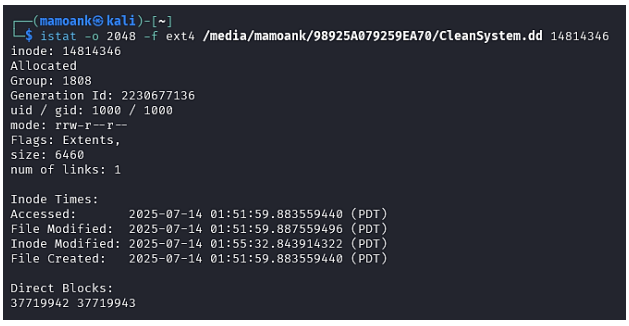
(b)

(c)

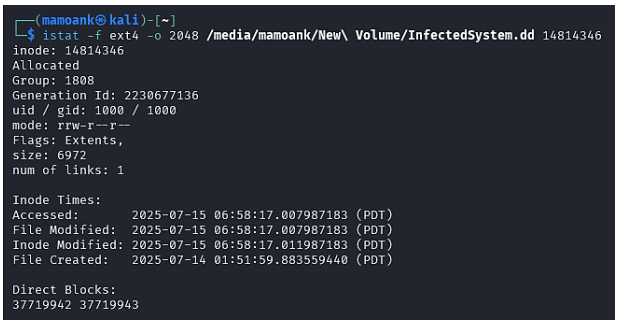
Gambar 17. *Subdirektori /Documents* Sistem Terinfeksi: (a) Data Pegawai, (b) Data Penjualan, dan (c) Data Keuangan

File dengan ekstensi *.xlsx* telah terenkripsi dan ekstensinya telah diganti menjadi *.puuuk*, semetara itu *file readme.txt* muncul pada masing – masing direktori sebagai artefak dari *ransomware*. Ini mengindikasikan bahwa *ransomware* akan menyisipkan *ransom note* pada masing - masing direktori atau *file* yang menjadi targetnya.

Pemeriksaan lebih lanjut dijalankan dengan melihat perubahan yang ada pada metadata salah satu *file* yang ada didalam subdirektori yang terinfeksi. Kita akan mengambil sample dari direktori */Data Pegawai*, dengan menggunakan tool *istat* kita dapat mengekstrak informasi dari *file* tersebut.



(a)



(b)

Gambar 18. *istat file* Data Pegawai: (a) Sistem bersih dan (b) Sistem terinfeksi

File Data Pegawai.xlsx.puuk didalam direktori */Documents/Pegawai* menunjukkan karakteristik *file* yang terenkripsi *ransomware*. *File* ini berstatus aktif, berukuruan 6972 *byte*s. *Timestamp inode* menunjukkan bahwa *file* asli dibuat pada 2025-07-15 pukul 01:51:59, lalu dienkripsi dalam satu eksekusi *ransomware* pada 2025-07-15 pukul 06:58:17. Perubahan metadata terjadi dalam 4 milidetik setelah modifikasi *file*, menunjukkan proses enkripsi otomatis oleh *binary ransomware*. Hasil dari *istat* menunjukkan bahwa, *UID*, *GID*, dan *permision* tidak mengalami perubahan, blok data tetap berada pada lokasi semula, *timestamp* akses dan modifikasi berubah sesuai dengan waktu eksekusi *ransomware*, Temuan ini memperkuat bahwa *ransomware* Monti menggunakan teknik *in-place encryption*, yaitu mengenkripsi isi *file* secara langsung di lokasi aslinya tanpa membuat salinan baru atau memindahkan *inode*. Teknik ini memungkinkan pelaku untuk menghindari deteksi berbasis perubahan struktur *file system* dan mempercepat proses enkripsi secara efisien.

Selanjutnya pemerikasaan akan berada pada direktori */temp*, karena tempat dimana *ransomware* dieksekusi dan berada. Ini dikarenakan ketika dilakukan restart maka *file ransomware* akan menghilang, sehingga ini mejadi langkah

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

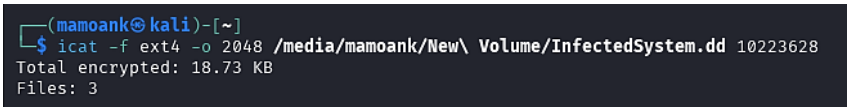
untuk menyembunyikan jejaknya. Dengan menggunakan *fls* dengan *inode* direktori */temp*, "*fls -o <offset> <disk imaging> <inode* direktori */temp>*".

(a) (b)

Gambar 19. *fls* Sistem Terinfeksi (b) dan Sistem Bersih Direktori */tmp* (a)

Pada sistem yang tidak terinfeksi, direktori */tmp* berisi *file* dan folder sementara yang bersifat sistemik. Tidak ditemukan *file* eksekusi *ransomware* atau *file* yang dihapus. Sementara pada sistem yang terifeksi ditemukan artefak eksekusi *ransomware* Monti berupa monti.elf, yang merupakan *binary* Linux ELF yang digunakan utnk menjalankan proses enkripsi secara otomatis. Selain itu ditemukan *file* result.txt yang berisi mengenai *log* atau *output* eksekusi. Artefak yang ditemukan pada sistem yang terinfeksi tidak ditemukan pada sistem yang tidak terinfeksi, sehingga dapat dikategorikan sebagai *Indicator of Compromise* (IoC).

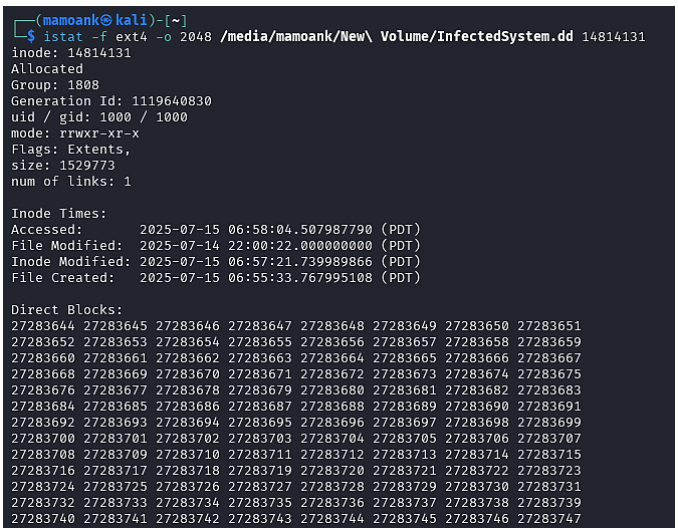
Pemeriksaan akan dilanjutkan pada *file* result.txt, untuk mengkonfirmasi dan memperkuat bahwa *ransomware* Monti tidak hanya menyisipkan *ransom note*, tetapi juga mencatat hasil eksekusi secara local.



Gambar 20. Ekstraksi Data Didalam *file* result.txt

File result.txt berisi ringkasan hasil eksekusi *ransomware* Monti, yaitu jumlah *file* yang terenkripsi dan total ukuran data. *File* ini dibuat secara otomatis oleh *binary* monti.elf dan ini menunjukkan bahwa *ransomware* tidak hanya melakukan enkripsi tetapi juga mnyisipkan *ransom note* tetapi juga mencatat hasil dari *file* yang telah terenkripsi.

Pemeriksaan dilanjutkan untuk memeriksa proses eksekusi dari *ransomware* Monti, monti.elf yang merupakan artefak eksekusi utama dari *ransomware*.



Gambar 21. Ekstraksi Metadata dari monti.elf

Dari hasil pemeriksaan, *file* berstatus aktif dengan ukuran 1,5 MB, dan memiliki *permission* eksekusi yang memungkinkan untuk dijalankan oleh user. Dari *timestamp file* monti.elf menunjukkan bahwa *file* dibuat pada 2025-07-15 pukul 06:55:33, diakses untuk ekseskusi pada pukul 06:58:04, dan memicu proses enkripsi yang menghasilkan artefak .puuuk dan *readme.txt* pada pukul 06:58:17.

Dari Analisa yang dilakukan menggunakan Sleuthkit menunjukkan beberapa perbedaan yang ditemukan beberapa perbedaan diantara sistem yang terinfeksi dan yang tidak terinfeksi.

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Tabel 2. Hasil analisa Perbandingan *Disk* Image

Temuan	Sistem Belum Terinfeksi	Sistem Terinfeksi
/Documents/Data Pegawai.xlsx	Aktif, *inode* 14814346	*File* terenkripsi Data Pegawai.xlsx.puuuk
/Documents/Data Penjualan.xlsx	Aktif, *inode* 14814313	*File* terenkripsi Data Penjualan.xlsx.puuuk
/Documents/Data Keuangan.xlsx	Aktif, *inode* 14814368	*File* terenkripsi Data Keuangan.xlsx.monti
readme.txt (global dan lokal)	Tidak ada	Ada di /Documents dan semua subdirektori
Timestamp artefak .puuuk / .monti	Tidak ada	2025-07-15 06:58:17 PDT
/tmp/monti.elf	Tidak ada	Ada, *inode* 14814131
/tmp/result.txt	Tidak ada	Ada, *inode* 10223628
Timestamp eksekusi monti.elf	Tidak ada	Akses: 2025-07-15 06:58:04 PDT

4. KESIMPULAN

Penelitian ini berhasil mengidentifikasi dan memvalidasi dampak infeksi *ransomware* Monti terhadap sistem Linux melalui pendekatan forensik digital berbasis artefak dan metadata. Proses dilakukan dengan membandingkan dua kondisi sistem sebelum dan sesudah infeksi menggunakan Teknik akuisisi *disk imaging* serta analisis granular terhadap struktru *file system*, *inode* dan *timestamp*. Eksekusi *ransomware* dilakukan melaui *binary* monti.elf yang dijalankan dari direktori sementara */tmp*, dengan *permission* eksekusi aktif dan *timestamp* akses yang konsisten dengan waktu pembuatan artefak. Proses enkripsi berlangsung secara otomatis dan simultan terhadap *file* operasional di dalam ditektori */Documents*, dengan mempertahankan *inode* dan lokasi blok data asli. Sebagai contoh, *file Data Pegawai.xlsx.puuuk* memiliki ukuran 6972 *byte*s dan *inode* tetap (*inode*:14814346), menunjukkan bahwa proses enkripsi dilakukan secara *in-place* tanpa relokasi struktur *file*. *Timestamp inode* menunjukkan bahwa *file* asli dibuat pada 2025-07-15 pukul 01:51:59, kemudian dimodifikasi oeh proses enkripsi *ransomware* pada 2025-07-15 pukul 06:58:17. Perubahan metadata terjadi hanya dalam rentang 4 milidetik setelah modifikasi isi *file*. Hal ini mengindikasikan kecepatan eksekusi yang tinggi dan terotomatisasi. Artefak *ransomware* yang ditemukan meliputi, file terenkripsi dengan ekstensi .puuuk, ransomnote *readme.txt* yang disisipkan di setiap direktori yang menjadi target, file result.txt sebagai *log* internal hasil eksekusi, *binary* eksekusi monti.elf sebagai artefak utama. Selurruh artefak memiliki *timestamp* identik, memperkuat bahwa proses infeksi terjadi dalam satu sesi eksekusi. *File readme.txt* berisi instruksi pembayaran melalui jaringan TOR dan ID korban, memperkuat bahwa Monti beroperasi sebagai bagian dari ekosistem *Ransomware-as-a-Service* (RaaS). Perbandingan sistem bersih dan sistem terinfeksi menunjukkan perbedaan signifikan dalam struktur direktori, keberadaan artefak, dan perubahan metadata. Temuan ini memperkuat validasi bahwa *ransomware* Monti menyasar file secara spesifik, menyisipkan artekan komunikasi, dan mencatat hasil eksekusi secara local. Dengan demikian, seluruh artefak yang ditemukan dapat dikategorikan sebagai indikator kompromi (IoC) yang sah dan relevan untuk proses investigasi, mitigasi, dan dokumentasi insiden. Penelitian ini memberikan kontribusi penting dalam pemetaan pola infeksi *ransomware* Monti, serta memperkuat metodo*log*i investigasi forensik berbasis artefak, *timestamp*, dan struktur *file system*. Saran untuk penelitian selanjutnya Adalah memperluas analisis ke artefak RAM dan proses aktif menggunakan Volatility3, serta menguji barian Monti lainnya untuk memetakan perbedaan Teknik enkripsi dan distribusi artefak. Penelitian lanjutan juga dapat mengeksplorasi integrasi threat intelligence untuk memperkuat deteksi dini dan response insiden berbasis artefak.

REFERENCES

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques: A Review. In *International Journal of Communication Networks and Information Security (IJCNIS* (Vol. 12, Issue 3).

Arfeen, A., Asim Khan, M., Zafar, O., & Ahsan, U. (2022). Process based volatile memory forensics for ransomware detection. *Concurrency and Computation: Practice and Experience*, *34*(4). https://doi.org/10.1002/cpe.6672

Carrillo-Mondéjar, J., Martínez, J. L., & Suarez-Tangil, G. (2020). Characterizing Linux-based Malware: Findings and Recent Trends. *Future Generation Computer Systems*, *110*, 267–281. https://bitbucket.org/Dankitan/

Bill, T. (2023, April 23). *Chinese hackers use new Linux malware variants for espionage*. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-linux-malware-variants-for-espionage/

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation*, *33*, 300979. https://doi.org/10.1016/j.fsidi.2020.300979

De Vicente Mohino, J. J., Higuera, J. B., Higuera, J. R. B., Montalvo, J. A. S., Rubio, M. S., & Herraiz, J. J. M. (2021). MMALE A Methodology for Malware Analysis in Linux Environments. *Computers, Materials and Continua*, *67*(2), 1447–1469. https://doi.org/10.32604/cmc.2021.014596

Esteves, T., Pereira, B., Oliveira, R. P., Marco, J., & Paulo, J. (2023). CRIBA: A Tool for Comprehensive Analysis of Cryptographic Ransomware's I/O Behavior. *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 46–58. https://doi.org/10.1109/SRDS60354.2023.00015


TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 748-760
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8341

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2023). A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms. *IEEE Access*, *11*, 121118–121141. https://doi.org/10.1109/ACCESS.2023.3328351

Global Threat Report. (2022).

Hristev, R., Veselinova, M., & Kolev, K. (2022). Ransomware Target: Linux. Recover Linux Data Arrays after Ransomware Attack. *Technology, Engineering & Mathematics (EPSTEM)*, *19*. www.isres.org

IBM Security. (23 C.E.). *IBM Security X-Force Threat Intelligence Index 2023*.

Imamverdiyev, Y., & Baghirov, E. (2024). Evasion Techniques In Malware Detection: Challenges And Countermeasures. *Problems of Information Technology*, *15*(2), 9–15. https://doi.org/10.25045/jpit.v15.i2.02

Joseph, P., & Norman, J. (2020). Systematic Memory Forensic Analysis of Ransomware using Digital Forensic Tools. *International Journal of Natural Computing Research*, *9*(2), 61–81. https://doi.org/10.4018/ijncr.2020040105

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, *190*. https://doi.org/10.1016/j.eswa.2021.116198

Karafili, E., Wang, L., & Lupu, E. C. (2020). An Argumentation-Based Reasoner to Assist Digital Investigation and Attribution of Cyber-Attacks. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/j.fsidi.2020.300925

Kim, G., Kim, S., Kang, S., & Kim, J. (2022). A method for decrypting data infected with Hive ransomware. *Journal of Information Security and Applications*, *71*, 103387. https://doi.org/10.1016/j.jisa.2022.103387

Korac, S., Maglaras, L., Moradpoor, N., Buchanan, B., & Canberk, B. (2024). *Ransomware: Analysis and Evaluation of Live Forensic Techniques and the Impact on Linux based IoT Systems*. http://arxiv.org/abs/2403.17571

Koutsokostas, V., & Patsakis, C. (2021). *Python and Malware: Developing Stealth and Evasive Malware Without Obfuscation*. http://arxiv.org/abs/2105.00565

Kumar, K. A., Raman, A., Gupta, C., & Pillai, R. R. (2020). The recent trends in malware evolution, detection and analysis for android devices. *Journal of Engineering Science and Technology Review*, *13*(4). https://doi.org/10.25103/jestr.134.25

Li, S., Li, R., Yang, S., & Diao, W. (2024). Android's Cat-And-Mouse Game: Understanding Evasion Techniques against Dynamic Analysis. *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, 192–203. https://doi.org/10.1109/ISSRE62328.2024.00028

Monti Ransomware Strikes Again: Omni Fiber LLC Falls Victim to Cyberattack - UNDERCODE NEWS. (2025, January). https://undercodenews.com/monti-ransomware-strikes-again-omni-fiber-llc-falls-victim-to-cyberattack/

Nayak, S. C., Tiwari, V., & Samanthula, B. K. (2023). Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform. *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023*, 605–611. https://doi.org/10.1109/CCWC57344.2023.10099169

Jonathan, G. (2023, September). *New Zealand university operating despite cyberattack | The Record from Recorded Future News*. https://therecord.media/auckland-university-operating-cyberattack

Ravie, L. (2023, April 19). *Pakistani Hackers Use Linux Malware Poseidon to Target Indian Government Agencies*. https://thehackernews.com/2023/04/pakistani-hackers-use-linux-malware.html

Umar, R., Riadi, I., & Kusuma, R. S. (2021). Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method. *IJID (International Journal on Informatics for Development)*, *10*(1), 53–61. https://doi.org/10.14421/ijid.2021.2423

Vehabovic, A., Ghani, N., Bou-Harb, E., Crichigno, J., & Yayimli, A. (2022). Ransomware Detection and Classification Strategies. *2022 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2022*, 316–324. https://doi.org/10.1109/BlackSeaCom54372.2022.9858296

Wong, M. Y., Landen, M., Li, F., Monrose, F., & Ahamad, M. (2024). *Comparing Malware Evasion Theory with Practice: Results from Interviews with Expert Analysts*. https://www.usenix.org/conference/soups2024/presentation/yong-wong

IBM Security. (2022). *X-Force Threat Intelligence Index 2022 Full Report*.

Yadav, R., Warang, V., & Kaur, J. (2024). Understanding and Mitigating Ransomware Threats: A Comprehensive Analysis at Guru Nanak Institute of Management Studies. In *International Journal of Scientific Research & Engineering Trends*, 10(5).