CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 1, Mei 2025, hlm. 53-62

Penerapan Metode NIST Dalam Analisis Forensik Digital Pasca Serangan Siber (Studi Kasus : Pt.Analis Digital Forensik)

[1]Muhammad Rafi Ilmuna Ihsan,[2]Apriade Voutama

[1,2]Prodi Sistem Informasi,Universitas Singaperbangsa Karawang,Karawang,Indonesia
Email: [1]muhrafiilmuna@gmail.com,[2] apriade.voutama@staff.unsika.ac.id

Abstrak

Serangan siber semakin meningkat dan menargetkan berbagai sektor industri, termasuk PT. Satseet International yang mengalami serangan pada sistem Human Resource Management System (HRMS) dan web server antara 5 - 19 November 2024. Studi kasus ini dilakukan dalam rangka program Magang dan Studi Independen Bersertifikat (MSIB) pada PT.Analis Forensik Digital.Metodologi yang digunakan adalah metode National Institute of Standards and Technology (NIST) guna mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti digital secara sistematis.Hasil analisis menunjukkan bahwa serangan dilakukan oleh kelompok BlackPython Team dengan teknik *Directory Traversal*, *Remote Code Execution* (RCE), dan *Ransomware*. Dampak serangan ini meliputi enkripsi data penting perusahaan, kebocoran data sensitif karyawan, gangguan operasional HRMS, serta potensi kerugian reputasi dan konsekuensi hukum. Melalui metode NIST, investigasi berhasil mengungkap pola serangan, mengidentifikasi titik masuk pelaku, serta memberikan rekomendasi mitigasi keamanan. Beberapa langkah yang disarankan meliputi penerapan firewall yang lebih ketat, pelatihan keamanan bagi karyawan, strategi *backup* dan *recovery* yang kuat, serta penguatan kebijakan keamanan data.Penelitian ini dapat membantu perusahaan dalam meningkatkan keamanannya.

Kata kunci: *Forensik Digital,Serangan Siber,NIST,RCE,Ransomware*

Implementation Of The Nist Method In Digital Forensic Analysis After A Cyber Attack (Case Study: Pt. Analis Digital Forensik)

Abstract

Cyberattacks are increasing and targeting various industrial sectors, including PT. Satseet International, which experienced an attack on its Human Resource Management System (HRMS) and web server between November 5 - 19, 2024.x This case study was conducted as part of the Certified Independent Study and Internship Program (MSIB) at PT. Analis Forensik Digital.The methodology used follows the National Institute of Standards and Technology (NIST) framework to systematically identify, collect, analyze, and report digital evidence. The analysis results indicate that the attack was carried out by the BlackPython Team using Directory Traversal, Remote Code Execution (RCE), and Ransomware techniques.The impact of this attack includes the encryption of critical company data, the leakage of sensitive employee information, disruptions to HRMS operations, and potential reputational damage and legal consequences. Using the NIST method, the investigation successfully uncovered the attack patterns, identified the attacker's entry points, and provided security mitigation recommendations.Some suggested measures include implementing stricter firewall policies, conducting security training for employees, establishing strong backup and recovery strategies, and strengthening data security policies. This research can help PT. Satseet International and other companies enhance their cybersecurity.

***Keywords**: Digital Forensics, Cyberattack, NIST, RCE, Ransomware*

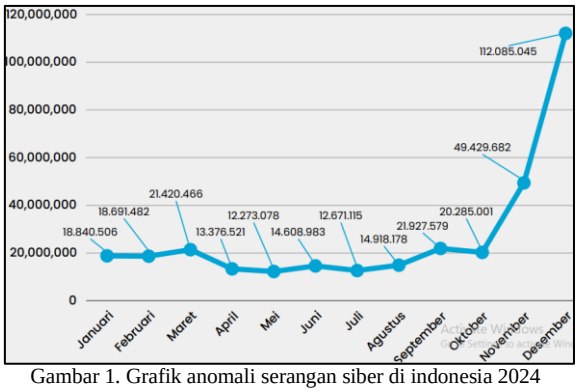
1. PENDAHULUAN

Dalam era digital ini perkembangan teknologi informasi semakin cepat.Hal ini membawa perubahan-perubahan besar disetiap aspek kehidupan manusia, termasuk dalam dunia industri.Kemajuan dibidang komputer,internet hingga kecerdasan buatan telah memungkinkan perusahaan untuk meningkatkan produksi, mempercepat proses bisnis,hingga memberikan pelayanan terbaik untuk pelanggan (Ramadhan, Kudus Zaini, et al., 2022).Transformasi ini menjadikan teknologi sebagai bagian penting dari setiap bisnis dan tak terpisahkan diberbagai sektor, mulai dari manufaktur, keuangan hingga teknologi informasi agar tetap berdaya saing (Ray et al., 2023).

Namun seiring dengan meningkatnya ketergantungan perusahaan terhadap teknologi, serangan terhadap keamanan siber juga meningkat dan berkembang (Riskiyadi, 2020).Serangan siber dapat mengakibatkan kerugian yang signifikan baik

dalam bentuk serangan *malware*,peretasan sistem hingga kebocoran data (Susanto et al., 2023).Dampak serangan ini tidak hanya dapat mengganggu jalannya operasional bisnis ataupun kerugian finansial namun juga dapat menurunkan kepercayaan pelanggan (Novita et al., 2023).

Di Indonesia sendiri sebuah penelitian menunjukkan bahwa serangan siber meningkat setiap tahun, pada tahun 2019-2020 serangan siber meningkat 9,35% sedangkan pada tahun 2020-2021 meningkat sebesar 6,15% (Parulian et al., n.d.).



Gambar 1. Grafik anomali serangan siber di indonesia 2024

Pada Gambar 1 merupakan grafik anomali serangan siber berdasarkan laporan yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN),total trafik anomali serangan siber di indonesia tahun 2024 mencapai 330.527.636 aktivitas mencurigakan. Aktivitas tertinggi terjadi pada bulan Desember dengan 112.085.045.Aktivitas ini berpotensi menyebabkan penurunan performa perangkat jaringan hingga pencurian data sensitif.Dengan tingginya percobaan serangan, sayangnya indonesia masih dalam keadaan yang lemah dalam keamanan siber.

Untuk mengatasi berbagai ancaman tersebut,perusahaan perlu menerapkan keamanan siber yang kuat untuk melindungi sistem mereka.Keamanan siber melindungi berbagai aspek, seperti pengamanan jaringan,proteksi terhadap data maupun menerapkan kebijakan atau standar operasional yang tegas untuk mengurangi risiko serangan (Tri Ginanjar Laksana & Sri Mulyani, 2024).Dan salah satu bagian keamanan siber yang berperan sangat penting adalah kemampuan untuk merespon dan menyelidiki serangan yang telah terjadi untuk mencegah kejadian serupa dimasa mendatang.

Salah satu pendekatan yang digunakan dalam menangani serangan pasca kejadian adalah forensik digital. Forensik digital menjadi aspek krusial dalam dalam mengidentifikasi sumber serangan,eksploitasi yang dilakukan,hingga dampak yang ditimbulkan (Amsori et al., 2024).Forensik digital menerapkan investigasi dan identifikasi dalam menindak kejahatan digital.Sehingga perusahaan memiliki strategi mitigasi dan respon yang efektif untuk menghadapi kejadian tersebut

Makalah ini melakukan investigasi forensik digital pasca serangan siber terhadap web server PT.Satseet International guna memahami bagaimana investigasi forensik digital diterapkan dalam kondisi yang terkontrol untuk mengevaluasi sejauh mana langkah-langkah mitigasi dapat dilakukan guna meningkatkan keamanan sistem perusahaan.

Salah satu metode yang sering digunakan dalam forensik digital adalah metode dari *National Institue of Standard and Technology* (NIST) yaitu NIST 800 SP 86.Metode ini menyediakan pendekatan yang sistematis mencakup 4 Tahapan utama yaitu *Collection* (Pengumpulan), *Examination* (Pengolahan), *Analysis* (Analisis) dan *Reporting* (Laporan).Berbagai penelitian telah membahas efektifitas NIST 800 SP-86 dalam menangani berbagai jenis serangan siber seperti pada sektor keuangan,pemerintahan dan sektor lainnya.

Namun mayoritas penelitian digital forensik berfokus pada objek atau perangkat tertentu.Pendekatan ini seringkali terfragmentasi dan tidak melihat serangan siber dalam skala yang lebih luas,terutama dalam konteks perusahaan secara keseluruhan.Jarang sekali penelitian yang meninjau bagaimana serangan terjadi dari awal hingga akhir dalam sebuah organisasi yang melibatkan banyak aspek seperti bagaimana serangan terjadi, apa dampak yang diberikan, dan bagaimana strategi keamanan dapat dapat ditingkatkan untuk mencegah serangan serupa dimasa depan.

Makalah ini melakukan analisis digital forensik terhadap PT. Satseet International menggunakan metode NIST 800 SP-86 untuk menginvestigasi insiden, mengidentifikasi bukti digital, serta memberikan rekomendasi perbaikan keamanan berdasarkan hasil investigasi. Penelitian ini mengkaji serangan siber multi-vektor yang melibatkan teknik *Directory Traversal*, *Remote Code Execution (RCE)*, dan *Ransomware* secara bersamaan. Berbeda dengan penelitian sebelumnya yang sering fokus pada satu jenis serangan atau analisis parsial, makalah ini memberikan analisis kronologis terperinci dan solusi mitigasi,sehingga memperluas pemahaman tentang modus operandi kelompok peretas dan meningkatkan efektivitas langkah keamanan di lingkungan korporasi.

2. TINJAUAN PUSTAKA

2.1. Keamanan Siber

Keamanan siber adalah kegiatan yang dimaksudkan untuk melindungi perangkat elektronik,jaringan maupun data pribadi dari berbagai ancaman siber seperti pencurian data, peretasan,malware,hingga akses yang tidak sah..S saat ini keamanan siber semakin populer dan dibutuhkan karena meningkatnya penggunaan perangkat komputer dan internet dalam kehidupan sehari hari (Budi et al., 2021).

Dengan meningkatnya kejahatan siber saat ini keamanan siber menjadi tantangan utama dalam

berbagai sektor(Aryapranata et al., 2024). Ancaman seperti *phising*,*ransomeware*, dan serangan DDoS terus berkembang.Oleh karena itu, penerapan keamanan sistem yang kuat menjadi kebutuhan yang tidak dapat ditinggalkan.Selain itu peran teknologi dan sumber daya manusia memainkan peran kunci dalam meningkatkan keamanan siber.

2.2. Serangan Siber

Serangan siber adalah aksi penyerangan melalui jaringan atau sistem telekomunikasi terhadap situs, sistem, atau perangkat komputer lain (Luthfah, 2021).Serangan siber ini terus mengalami perkembangan.Serangan siber bisa menyerang siapapun, dimanapun dan kapanpun.Namun sayangnya masih banyak pelaku bisnis yang kurang paham atau bahkan tidak mengerti betapa pentingnya keamanan siber (Pringsewu & Septasari, 2024).

Serangan siber menjadi ancaman serius karena nilai kerugian yang diberikan dalam skala dunia bisa mencapai pendapatan sebuah negara (Iman et al., 2020).Serangan siber adalah dampak dari ketersediaan berlebih dan kemampuan pengguna komputer ditangan yang tidak bertanggung jawab.

2.3. Forensik Digital

Penanganan kasus kejahatan siber dilakukan dengan kegiatan investigasi yang dikenal sebagai Forensik Digital.Forensik Digital adalah sebuah prosedur atau teknik investigasi kejahatan siber (Rezki Syaputra & Syaifudin, 2020).Forensik Digital juga bisa dikatakan sebagai ilmu untuk memulihkan bukti digital dari suatu perangkat dengan sebuah metode untuk mengumpulkan data atau bukti yang dapat diterina secara hukum dipengadilan sebagai alat pembuktian (Fitriana et al., n.d.).Dalam konteks forensik digital, di indonesia sendiri telah digunakan dalam berbagai kasus seperti kasus korupsi maupun peretasan.

2.4. NIST SP 800-86

NIST adalah sebuah lembaga yanng memberikan panduan teknis maupun konsep terhadap ilmu pengetahuan teutama ilmu terapan.NIST telah memberikan kontribusi penting dalam berbagai bidang seperti forensika digital dan keamanan siber.Walaupun NIST bukan satu-satunya lembaga yang memberikan metode, akan tetapi metode dan panduannya telah digunakan oleh berbagai pihak mulai dari pemerintah, industri hingga para peneliti dan akademisi.NIST juga mengeluarkan salah satu metode standar dalam melakukan analisis terhadap bukti digital yaitu NIST SP 800-86 (Faizal, 2024).

NIST SP 800-86 adalah sebuah metode yang diterbitkan oleh National Institute of Standards and Technology (NIST) yang digunakan sebagai panduan kerja untuk melakukan analisis bukti digital di perangkat komputer.Metode ini dapat digunakan sebagai prosedur dalam analisis digital forensik secara komprehensif dan panduannya masih relevan dalam penanganan bukti digital saat ini.Proses investigasi yang dijelaskan pada NIST mencakup tahap-tahap *Collection* (pengumpulan) ,*Examination* (Pemeriksaan),*Analysis* (Analisis) dan Reporting (Laporan). Keempat tahap ini saling terintegrasi dan ditujukan untuk menjaga integritas bukti serta memastikan hasil investigasi yang valid (Ramadhan, Rachmat Setiawan, et al., 2022).

Metode yang diberikan NIST berasal dari penelitian yang ketat dan riset yang mendalam dan secara sistematis mengidentifikasi baik kelebihan maupun kekurangannya, kemudian di publikasikan melalui literatur ilmiah.Proses penyempurnaan terhadap metode ini dilakukan secara iteratif dan berkelanjutan. Hal ini mencerminkan adanya prinsip ketelitian ilmiah dalam pengembangan metodologinya. Dengan demikian, standar NIST SP 800-86 tidak hanya memiliki validitas tinggi, tetapi juga reliabilitas yang baik karena konsistensi dan kemampuan replikasi prosedurnya dalam berbagai konteks investigasi digital (Faizal & Luthfi, 2024).

Beberapa penelitian membuktikan bahwa NIST 800-86 efektif digunakan untuk menelusuri jejak serangan atau mengumpulkan bukti digital,seperti penelitian yang dilakukan oleh (Prakoso & Khamas Heikmakhtiar, 2024) menggunakan metode NIST 800-86 untuk mendeteksi serangan spoofing ARP dan DNS, membuktikan pentingnya pemantauan jaringan dan analisis forensik yang sistematis dalam mencegah serangan tersebut. (Wijaya Kusuma et al., 2024) juga menerapkan metode NIST SP 800-86 untuk menganalisis data yang dihapus pada media penyimpanan flash disk dengan menggunakan tools forensik seperti *FTK Imager*, *Autopsy*, dan *HashGenerator*, penelitian tersebut berhasil mengungkap metadata file terhapus dan perbedaan perlakuan penghapusan data.

3. METODOLOGI PENELITIAN

Dalam makalah ini menggunakan metode Forensik Digital yang dibuat oleh National Institute of Standard and Technology (NIST) yaitu metode NIST SP 800-86.

Gambar 2. Alur Proses Metode NIST 800-86

Gambar 2 adalah alur proses dari metode NIST SP 800-86.Proses metode ini terdiri dari 4 tahapan yaitu *Collection* (pengumpulan) yang merupakan tahap untuk mengumpulkan data guna mendukung proses penyelidikan mencari barang bukti digital.pada tahap ini data dikumpulkan dengan cara pengambilan bukti digital dari berbagai sumber

seperti perangkat keras,perangkat lunak maupun jaringan.Proses ini dilakukan untuk menjaga integritas bukti agar tetap valid dalam investigasi.

Examination (Pengolahan Data) merupakan tahap pemeriksaan data yang telah dikumpulkan.pemeriksaan dilakukan untuk mengekstrak,menyaring, dan mengorganisir data data mentah yang relevan.Teknik seperti hashing,filtering, dan metadata extraction digunakan untuk memastikan data tidak mengalami perubahan.

Selanjutnya tahap *Analysis* (Analisis), pada tahap ini data yang sudah diperiksa akan dianalisis lebih lanjut untuk mengidentifikasi pola serangan,jejak penyerang hingga dampak yang ditimbulkan.Data tersebut dianalisis secara komprehensif dengan metode yang benar dan sah secara hukum untuk dibuktikan.Hasil analisis ini akan dijadikan dasar dalam penyusunan laporan serta dapat dipertanggung jawabkan secara ilmiah dan hukum.

Terakhir adalah *Reporting* (Laporan) merupakan tahap yang dilakukan setelah barang bukti diperoleh dan dianalisis.Temuan dalam proses analisis akan disusun dalam laporan forensik secara sistematis.Laporan harus disusun mempertimbangkan aspek legalitas sehingga dapat digunakan dalam proses hukum.

3.1. Ringkasan Peristiwa Serangan

Pada ringkasan serangan ini akan menjelaskan peristiwa serangan berdasarkan urutan waktu untuk mempermudah investigasi.

a. 19 November 2024,PT.Satseet International .mengalami serangan siber serius yang menargetkan sistem *Human Resources Management System* (HMRS) mereka.Insiden ini ditandai dengan dienkripsinya data penting perusahaan.
b. 22 November 2024, Kelompok penyerang bernama BlackPython Team meng-klaim pencurian data sensitif karyawan yang dipublikasikan melalui platform telegram.

3.2. Alat penelitian

Pada Tabel 1 merupakan alat yang digunakan dalam investigasi forensik digital ini.

Tabel 1.Alat yang digunakan

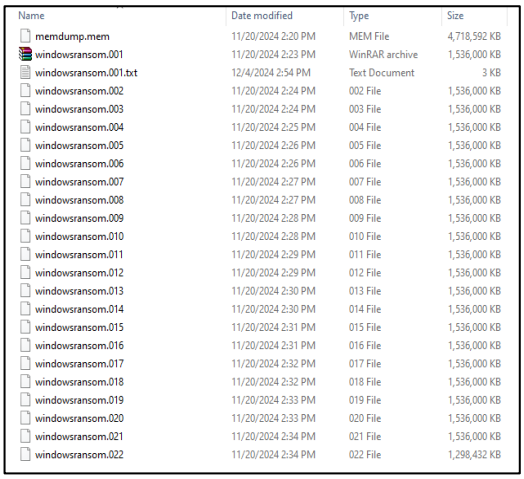
Nama Alat	Versi	Fungsi
Wireshark	4.4.2	Sebagai network protocol analyzer yang digunakan untuk menganalisis lalu lintas jaringan secara real-time
FTK Imager	4.7.1.2	Sebagai alat akuisisi untuk membuat dan menganalisis disk image dari perangkat yang diperiksa
Autopsy	4.21.0	Sebagai alat untuk menganalisis bukti digital dari perangkat penyimpanan
VirusTotal	-	Layanan berbasis cloud yang digunakan untuk menganalisis file atau url terhadap berbagai database antivirus dan mesin deteksi malware

4. HASIL DAN PEMBAHASAN

4.1. Tahap *Collection* (Pengumpulan)

Berdasarkan data akuisisi yang diterima, dilakukan proses pengumpulan bukti digital untuk mendukung investigasi forensik serangan siber terhadap sistem HRMS PT.Satseet International.Data yang telah diterima meliputi:

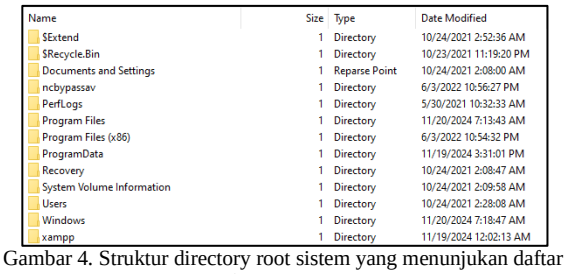
1. File bernama *windowsransom* berupa *disk image* dari folder dan direktori yang terdapat dalam komputer korban
2. Hasil dari proses *live acquisition* ,yang dilakukan pihak perusahaan terhadap sistem dalam keadaan aktif.



Name	Date modified	Type	Size
memdump.mem	11/20/2024 2:20 PM	MEM File	4,718,592 KB
windowsransom.001	11/20/2024 2:23 PM	WinRAR archive	1,536,000 KB
windowsransom.001.txt	12/4/2024 2:54 PM	Text Document	3 KB
windowsransom.002	11/20/2024 2:24 PM	002 File	1,536,000 KB
windowsransom.003	11/20/2024 2:24 PM	003 File	1,536,000 KB
windowsransom.004	11/20/2024 2:25 PM	004 File	1,536,000 KB
windowsransom.005	11/20/2024 2:26 PM	005 File	1,536,000 KB
windowsransom.006	11/20/2024 2:26 PM	006 File	1,536,000 KB
windowsransom.007	11/20/2024 2:27 PM	007 File	1,536,000 KB
windowsransom.008	11/20/2024 2:27 PM	008 File	1,536,000 KB
windowsransom.009	11/20/2024 2:28 PM	009 File	1,536,000 KB
windowsransom.010	11/20/2024 2:28 PM	010 File	1,536,000 KB
windowsransom.011	11/20/2024 2:29 PM	011 File	1,536,000 KB
windowsransom.012	11/20/2024 2:29 PM	012 File	1,536,000 KB
windowsransom.013	11/20/2024 2:30 PM	013 File	1,536,000 KB
windowsransom.014	11/20/2024 2:30 PM	014 File	1,536,000 KB
windowsransom.015	11/20/2024 2:31 PM	015 File	1,536,000 KB
windowsransom.016	11/20/2024 2:31 PM	016 File	1,536,000 KB
windowsransom.017	11/20/2024 2:32 PM	017 File	1,536,000 KB
windowsransom.018	11/20/2024 2:32 PM	018 File	1,536,000 KB
windowsransom.019	11/20/2024 2:33 PM	019 File	1,536,000 KB
windowsransom.020	11/20/2024 2:33 PM	020 File	1,536,000 KB
windowsransom.021	11/20/2024 2:34 PM	021 File	1,536,000 KB
windowsransom.022	11/20/2024 2:34 PM	022 File	1,298,432 KB

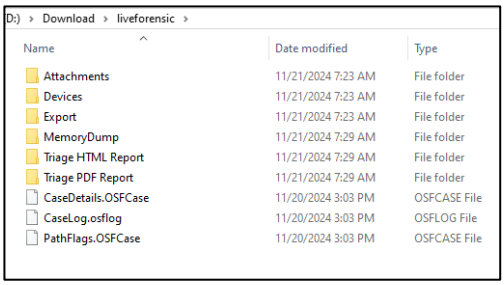
Gambar 3. File yang diterima dari hasil akuisisi

Gambar 3 merupakan file hasil *disk image* folder didalam komputer korban. Setelah menganalisis file *windowsransom* menggunakan software *FTK Imager*, ditemukan beberapa folder dan directory penting yang umum terdapat pada sistem operasi *windows*.Gambar 4 merupakan daftar folder yang terdeteksi pada *FTK Imager*.



Gambar 4. Struktur directory root sistem yang menunjukan daftar folder utama

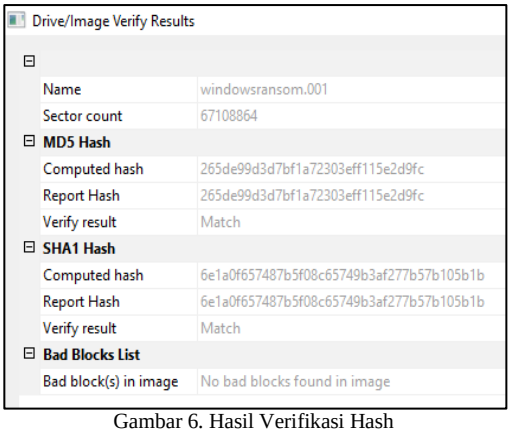
Hasil *liveforensic* juga didapatkan beberapa folder, seperti file memorydump. Log aktif perangkat dan juga berbagai macam informasi sistem yang tertangkap dalam perangkat.Gambar 5 merupakan hasil dari *live acquisition*.



Gambar 5. Hasil live acquisition

4.2. Tahap *Examination* (Pengolahan)

Selanjutnya, data asli hasil akuisisi tetap perlu dilakukan *imaging* ulang untuk memastikan integritas data bukti digital dan mematuhi prinsip-prinsip forensik.Dengan *imaging* ulang,kita dapat memastikan bahwa salinan yang dianalisis merupakan representasi data yang akurat dari data asli.



Gambar 6. Hasil Verifikasi Hash

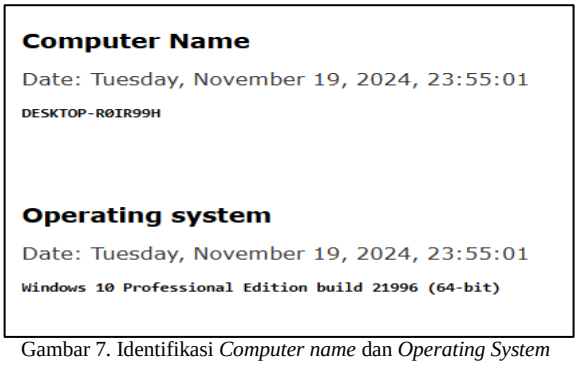
Gambar 6 merupakan hasil verifikasi hash file yang sudah di*imaging* ulang. Data asli dilakukan verifikasi untuk memastikan bahwa image yang dihasilkan identik dengan data yang diambil.terlihat bahwa hasil *verify result* dari MD5 dan SHA1 menunjukkan hasil *match* atau cocok yang menandakan bahwa data tidak berubah.

4.3. Tahap *Analysis* (Analisis)

Setelah dilakukan tahap *examination* atau pengolahan data, selanjutnya adalah tahap analysis untuk melihat secara rinci hasil dari examination guna mendapatkan bukti digital.

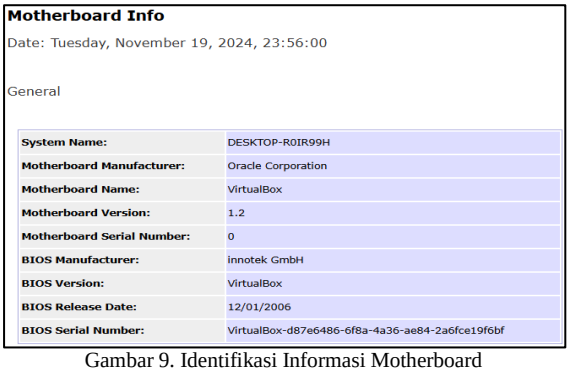
a. Identifikasi Sistem

Berikut adalah hasil identifikasi sistem yang didapatkan dari analisis file *live forensic* yang diterima sebelumnya.Hasil identifikasi menemukan beberapa bukti digital seperti nama komputer,sistem operasi, informasi jaringan dan informasi *motherboard*. Hasil identifikasi dapat dilihat pada Gambar 7,8 dan 9.



Gambar 7. Identifikasi *Computer name* dan *Operating System*

Gambar 8. Identifikasi Informasi Jaringan



Gambar 9. Identifikasi Informasi Motherboard

Dari analisis identifikasi sistem menghasilkan beberapa komponen penting yang akan berguna untuk analisis bukti lebih lanjut.Tabel 2 merupakan bukti penting dari hasil identifikasi sistem yang telah dilakukan.

Tabel 2. Bukti Penting Hasil Identifikasi Sistem

Komponen	Keterangan
OS	Microsoft Windows 11 Pro

Komponen	Keterangan
OS Version	10.0.21966 N/A Build 21996
Hostname	DESKTOP-R0IR99H
Network	Ipv4 192.168.1.28

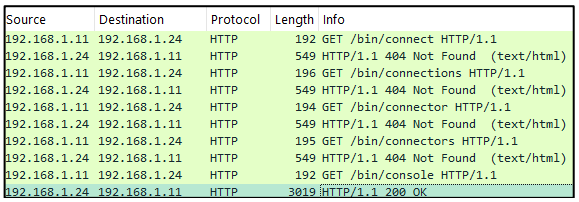
b. Kronologis Kejadian

Setelah melakukan identifikasi sistem, selanjutnya adalah mengumpulkan berbagai bukti untuk mengurutkan kronologis kejadian yang terjadi.Tabel 3 adalah hasil analisis kronologis kejadian menggunakan standar Waktu Indonesia Barat.

Tabel 3. Hasil Kronologis Kejadian

Tanggal	Waktu	User	Keterangan
5/11/2024	19:58 WIB	Pelaku	Melakukan directory traversal
5/11/2024	19:58 WIB	Pelaku	Directory traversal berhasil menemukan file sensitif
6/11/2024	17:54 WIB	Local User 2	Menerima Email dari Maya Putri terkait pertanyaan informasilowongan kerja
19/11/2024	22:18 WIB	Local User 1	Sebuah Email mencurigakan masuk di Akun ”Ahmad Habibie”
20/11/2024	13:23 WIB	Pelaku	User Mencoba Mengakses Web PT satseet
20/11/2024	13:29 WIB	Pelaku	User Login ke Akun Web PT Satseet
20/11/2024	13:29 WIB	Pelaku	User melakukan Inisiasi Koneksi Dengan local user 1
20/11/2024	13:30 WIB	Local User 1	Login ke dalam Email ‘Ahmad Habibi”
20/11/2024	13:31 WIB	Local User 1	Download File Folline zip melalui Email
20/11/2024	13:33 WIB	Local User 1	Mengakses File Dokumen Riwayat Hidup M.P Follina
20/11/2024	13:49 WIB	Local User 1	Akses file update.exe
20/11/2024	13:50 WIB	Local User 1	Akses file ransome.exe
20/11/2024	13:59 WIB	Local User 1	Beberapa file terkunci

Saat menganalisis folder Dalam analisis jaringan menggunakan *wireshark*,Pada tanggal 5 November 2024 ditemukan percobaan serangan *directory traversal* oleh pelaku yang menggunakan IP 192.168.1.11.Pelaku berhasil menemukan sebuah data sensitif. *Directory Traversal* atau *Path Travesal* adalah sebuah serangan keamanan web yang dimana bertujuan untuk mengakses direktori atau file yang berada di luar *Directory Root Web* (Adinda Amelia, 2024).Gambar 10 merupakan bukti percobaan serangan yang dilakukan pelaku, yang didapatkan melalui hasil analisis menggunakan wireshark



Source	Destination	Protocol	Length	Info
192.168.1.11	192.168.1.24	HTTP	192	GET /bin/connect HTTP/1.1
192.168.1.24	192.168.1.11	HTTP	549	HTTP/1.1 404 Not Found (text/html)
192.168.1.11	192.168.1.24	HTTP	196	GET /bin/connections HTTP/1.1
192.168.1.24	192.168.1.11	HTTP	549	HTTP/1.1 404 Not Found (text/html)
192.168.1.11	192.168.1.24	HTTP	194	GET /bin/connector HTTP/1.1
192.168.1.24	192.168.1.11	HTTP	549	HTTP/1.1 404 Not Found (text/html)
192.168.1.11	192.168.1.24	HTTP	195	GET /bin/connectors HTTP/1.1
192.168.1.24	192.168.1.11	HTTP	549	HTTP/1.1 404 Not Found (text/html)
192.168.1.11	192.168.1.24	HTTP	192	GET /bin/console HTTP/1.1
192.168.1.24	192.168.1.11	HTTP	3019	HTTP/1.1 200 OK

Gambar 10. Percobaan serangan directory traversal.

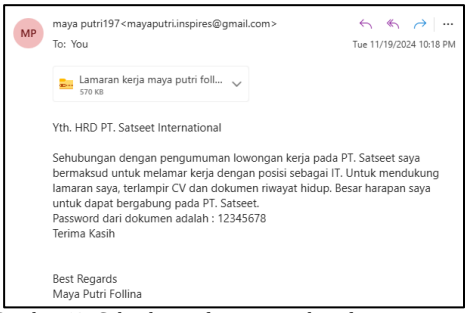
console - Notepad

File Edit Format View Help

```
if (php_sapi_name() !== 'cli') {
    echo 'Unauthorized';
    exit(1);
}

$pathToAutoload = realpath(__DIR__ . '/../src/vendor/autoload.php');

$errorMessage = "
Cannot find composer dependencies.
Run below command and try again;\n
$ cd %s
$ composer install -d src
";

if (!$pathToAutoload) {
    echo sprintf($errorMessage, realpath(__DIR__ . '/../'));
    exit(1);
}

use OrangeHRM\Config\Config;
use OrangeHRM\Core\Command\CacheClearCommand;
use OrangeHRM\Core\Command\GenerateDoctrineProxiesCommand;
use OrangeHRM\Framework\Console\Console;
use OrangeHRM\Framework\Console\ConsoleConfigurationInterface;
use OrangeHRM\Framework\Framework;
use OrangeHRM\Framework\Http\Request;
use OrangeHRM\Framework\PluginConfigurationInterface;
use Symfony\Component\Console\Input\ArgvInput;
use Symfony\Component\Console\Output\ConsoleOutput;
use Symfony\Component\Console\Style\SymfonyStyle;

set_time_limit(0);

require_once $pathToAutoload;
```

Gambar 11. File Sensitif dalam web server

Gambar 11 merupakan file sensitif yang ditemukan oleh pelaku saat melakukan *directory traversal*.Setelah berhasilnya percobaan serangan *directory traversal* pada 6 November 2024,Local user dalam akun email atas nama Ahmad Habibie menerima sebuah email dari Maya Putri terkait pertanyaan informasi lowongan kerja, lalu pada tanggal 20 November 2024 sebuah email mencurigakan oleh pengirim yang sama.Gambar 11 adalah bukti email mencurigakan dari pengirim bernama Maya Putri.



MP

maya putri197<mayaputri.inspires@gmail.com>

To: You

Tue 11/19/2024 10:18 PM

Lamaran kerja maya putri foll...
570 KB

Yth. HRD PT. Satseet International

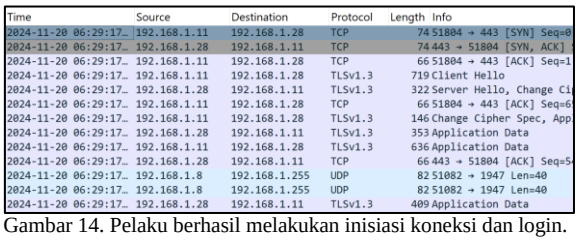
Sehubungan dengan pengumuman lowongan kerja pada PT. Satseet saya bermaksud untuk melamar kerja dengan posisi sebagai IT. Untuk mendukung lamaran saya, terlampir CV dan dokumen riwayat hidup. Besar harapan saya untuk dapat bergabung pada PT. Satseet.
Password dari dokumen adalah : 12345678
Terima Kasih

Best Regards
Maya Putri Follina

Gambar 12. Sebuah email mencurigakan dari maya putri

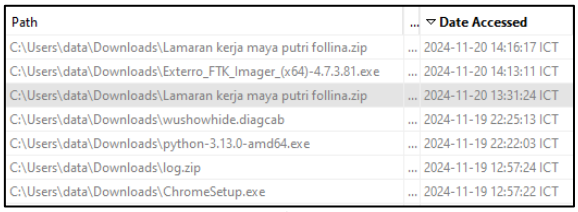
Selanjutnya pada tanggal 20 November 2024 pelaku berhasil login ke akun di HRMS PT Satseet International dan berhasil melakukan inisiasi koneksi pada server perusahaan.Gambar 13 dan 14 merupakan bukti bahwa pelaku telah berhasil melakukan inisiasi koneksi pada dengan server perusahaan.

Gambar 13. Pelaku berhasil melakukan inisiasi koneksi dan login.



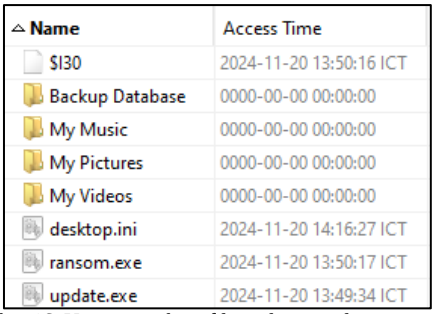
Gambar 14. Pelaku berhasil melakukan inisiasi koneksi dan login.

Selanjutnya pada tanggal 20 November 2024, pukul 13:29 WIB korban melakukan login email dan mengunduh file lamaran kerja dari email atas nama maya putri.Gambar 15 adalah bukti bahwa korban melakukan mengunduh file lamaran kerja dari maya putri

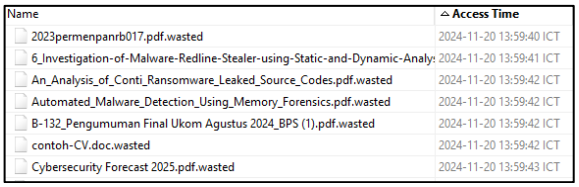


Gambar 15.Korban mengunduh file lamaran kerja dari maya putri

Setelah mengunduh file email, korban mengakses file tersebut yaitu file dokumen riwayat hidup M.P Follina.Setelah itu korban mengakses sebuah file bernama *update.exe* dan tidak lama korban juga mengakses sebuah file yaitu *ransom.exe* yang dimana bertepatan dengan dienkripsinya file file dalam server perusahaan.Bukti akses kedua file tersebut oleh korban ditampilkan pada gambar 16.



Gambar 16. User mengakses file update.exe dan ransom.exe



Gambar 17. Terenkripsinya file file dalam perangkat.

Gambar 17 adalah file file yang terenkripsi oleh sistem tidak lama setelah korban meng-akses file *ransom.exe* dan *update.ex*.Setelah dilakukan proses analisis pada kedua file tersebut terdapat beberapa hasil yaitu, pada file dokumen riwayat hidup follina ditemukan bahwa File ini memiliki eksploitasi yang mengacu pada CVE-2022-30190 (dikenal sebagai *Follina Exploit*), yang merupakan kerentanan di Microsoft Office yang memungkinkan *Remote Code Execution* (RCE).RCE adalah sebuah kerentanan yang memungkinkan penyerang dapat melakukan pengorperasian suatu perintah dari jarak jauh (Anis et al., 2022).Hasil analisis file dokumen M.P follina ditampilkan pada Gambar 18.

Gambar 18. Hasil analisis dokumen M.P Follina menggunakan *VirusTotal*

Selanjutnya adalah, file *update.exe* menunjukkan bahwa file ini termasuk kelompok trojan dan dapat berfungsi sebagai *backdoor* atau alat perusak lainnya. VirusTotal mendeteksi file ini sebagai Trojan dengan berbagai label, seperti

a. Trojan.Win32/Shell.R128S
b. Backdoor.Win/shellcode.apid(dyn)
c. Win.Trojan.CryptZ.Marte.1.Gen

Label diatas mengindikasikan bahwa file ini mungkin digunakan untuk mempertahankan koneksi *Follina exploit.*File ini menyerang atau mengakses sistem dengan cara tidak sah, termasuk kemungkinan untuk mengeksekusi perintah jarak jauh.Hasil analisis file update.exe ditampilkan pada Gambar 19.

Gambar 19. Hasil analisis *update.exe* menggunakan VirusTotal

Lalu File *ransom.exe* atau nama sebelumnya yaitu *main_v2.exe* menunjukkan file tersebut terdeteksi sebagai *malicious* file atau file yang berbahaya..Ini menunjukkan bahwa file tersebut

hampir pasti merupakan ancaman keamanan.Pada VirusTotal mendeteksi file ini sebagai *ransomware* atau *trojan*, VirusTotal mendeteksi file ini sebagai *ransomware* atau *trojan* dengan nama-nama seperti:

a. Ransom:Win32/Filecoder
b. Trojan.Ransom.CFP
c. Python.Filecoder

Ransomware adalah sebuah *malware* yang menggunakan teknik keamanan kriptografi untuk mengunci file dan meminta imbalan atas data yang dikunci(Sainuri Mubarak et al., 2024).Label ini menunjukkan bahwa file tersebut dapat mengenkripsi file korban.Hasil analisis file *ransom.exe* ditampilkan pada Gambar 20.

Gambar 20. Hasil analisis *ransom.exe* menggunakan virus total

4.4. Tahap *Reporting* (Laporan)

Setelah melakukan tahap *analysis* selanjutnya adalah tahapan *reporting* yang merupakan tahap terakhir dari metode NIST. Laporan ini mencakup rangkuman bukti digital, metode analisis yang digunakan, temuan utama, serta rekomendasi untuk mitigasi dan peningkatan keamanan sistem PT. Satseet International.Tabel 4 merupakan laporan singkat hasil dari analisis digital forensik yang telah dilakukan.

Tabel 4. Laporan Singkat Hasil Analisis Dgital forensik

Kategori	Deskripsi
Tanggal Insiden	5 - 19 November 2024
Sistem yang diserang	HRMS dan Server
Jenis Serangan	*Directory Traversal*,*RCE Attack* dan *Ransomware*
Kelompok Pelaku	*BlackPython Team*
Dampak	a. Enkripsi data penting Perusahaan b. Kebocoran data sensitif karyawan c. Gangguan operasional HRMS d. Potensi kerugian reputasi dan konsekuensi Hukum
Rekomendasi	a. Meningkatkan sistem keamanan jaringan b. Melakukan pelatihan keamanan siber kepada karyawan c. Menerapkan strategi Backup dan Recovery yang lebih kuat d. Memperkuat kebijakan kemanan data

5. KESIMPULAN DAN SARAN

Dari proses analisis yang telah dilakukan di dapat kesimpulan pada serangan yang telah terjadi pada PT Satseet International yaitu:

1. Serangan dimulai pada 5 November 2024, ketika pelaku berhasil melakukan directory traversal pada server web perusahaan. Serangan ini memungkinkan akses ke file sensitif di luar direktori *root web*, yang mengindikasikan kelemahan konfigurasi pada sistem *web server*.
2. Pada 6 November 2024, seorang pengguna internal menerima email bertopik rekrutmen dari pengirim bernama Maya Putri. Pesan ini menjadi bagian dari rangkaian *spear-phishing* yang digunakan untuk menjebak korban agar membuka lampiran berbahaya.
3. Puncak serangan terjadi pada 20 November 2024, ketika pelaku berhasil login ke sistem HRMS perusahaan dan memulai koneksi ke server internal. Di waktu yang hampir bersamaan, korban membuka email berisi file *Folline.zip* dan menjalankan dokumen yang mengandung eksploitasi CVE-2022-30190 (*Follina Exploit*) untuk menjalankan perintah jarak jauh. Selanjutnya, korban tanpa sadar mengeksekusi *update.exe* dan *ransom.exe*, yang masing-masing teridentifikasi sebagai *trojan backdoor* dan *ransomware*, hingga akhirnya menyebabkan enkripsi terhadap file-file penting perusahaan.
4. Identitas pelaku berhasil ditelusuri sebagai kelompok bernama *BlackPython Team*, yang diduga memiliki motif keuntungan finansial melalui pemerasan data (ransom) dan eksploitasi sistem.
5. Dampak yang ditimbulkan meliputi enkripsi dan hilangnya akses terhadap data internal perusahaan, kebocoran data sensitif karyawan, gangguan pada operasional sistem HRMS, serta potens kerugian reputasi dan hukum bagi perusahaan.

Penelitian ini memberikan gambaran konkret tentang bagaimana serangan siber seperti *directory traversa*l,*Remote Code Execution* (RCE), dan *ransomware* dapat terjadi secara bertahap dan terorganisir. Temuan ini dapat digunakan oleh tim

keamanan TI untuk menyusun prosedur deteksi dini dan respons insiden yang lebih efektif. Selain itu, hasil analisis terhadap file berbahaya dan jalur penyebarannya dapat menjadi dasar untuk menyusun kebijakan *email filtering*, pelatihan keamanan siber kepada karyawan, serta penguatan sistem *backup* dan *recovery*. Penelitian ini juga menekankan pentingnya memantau aktivitas login dan koneksi dalam sistem sebagai langkah preventif terhadap serangan siber.

Namun, Penelitian ini masih memiliki beberapa keterbatasan seperti pada analisis data log dan bukti digital yang tersedia selama 5-19 November 2024, sehingga kemungkinan ada aktivitas yang tidak terekam. Deteksi serangan bergantung pada alat seperti *Wireshark* dan *VirusTotal* yang memiliki keterbatasan dalam mengenali serangan baru. Identifikasi pelaku masih bersifat indikatif dan memerlukan bukti tambahan. Fokus penelitian hanya pada sistem HRMS dan server PT Satseet International, sehingga hasilnya belum bisa digeneralisasi ke sistem lain.

Adapun saran untuk penelitian selanjutnya, disarankan menggunakan sistem pemantauan keamanan real-time dan metode forensik yang lebih lengkap untuk mendeteksi serangan baru. Cakupan analisis bisa diperluas ke sistem lain agar keamanan lebih menyeluruh. Selain itu, pengembangan teknik untuk memperkuat bukti digital dan identifikasi pelaku akan membantu proses mitigasi dan penegakan hukum.

6. UCAPAN TERIMA KASIH

Dengan penuh rasa hormat dan terima kasih, saya mengucapkan apresiasi yang sebesar-besarnya kepada Bapak Setiya Nurbaya dan Bapak Apriyade Voutama atas bimbingan, arahan, serta ilmu yang telah diberikan selama proses penelitian ini. Dukungan dan masukan yang berharga dari Bapak berperan penting dalam kelancaran serta keberhasilan penelitian ini.

Saya juga ingin menyampaikan terima kasih yang tulus kepada seluruh teman-teman yang telah membantu dalam berbagai aspek penelitian ini, baik dalam pengumpulan data, analisis, maupun dukungan moral yang tiada henti. Tanpa kerja sama dan bantuan dari kalian, penelitian ini tidak akan dapat terselesaikan dengan baik. Semoga segala kebaikan dan ilmu yang telah dibagikan menjadi manfaat bagi kita semua.

DAFTAR PUSTAKA

Adinda Amelia. (2024). *Pengembangan Sistem Visualisasi Log untuk Evaluasi Keamanan Web Server (Studi Kasus Website Prodi Teknik Informatika UIN Syarif Hidayatullah Jakarta)*. https://repository.uinjkt.ac.id/dspace/handle/123456789/80488

Amsori, Fakhri Awaluddin, & Momon Mulyana. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Journal Humaniora: Jurnal Hukum Dan Ilmu Sosial*.

Anis, M., Hilmi, A., Keamanan, P., Upload…, F., & Yunan, R. K. (2022). *Pengujian Keamanan Fitur Upload File Pada Sistem Aplikasi Web*. *7*(1). https://github.com/anghilmi/file_upload_vuln.

Aryapranata, A., Al Rasyid, Y., Agsena, Y. P., & Hermanto, S. (2024). Keamanan Siber dalam Era Digital: Tantangan dan Solusi. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *8*(2), 109–114. https://doi.org/10.55886/infokom.v8i2.932

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Faizal, A. (2024). *Akuisisi Bukti Digital Pada Network Attached Storage (NAS)*. https://dspace.uii.ac.id/handle/123456789/51389

Faizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Fitriana, M., Ar, K., & Marsya, J. M. (n.d.). PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME. In *Jurnal Pendidikan Teknologi Informasi* (Vol. 4, Issue 1).

Iman, N., Susanto, A., & Inggi, R. (2020). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi Dan Komputer*, *9*(3), 186. https://doi.org/10.22441/incomtech.v9i3.7210

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *TerAs Law Review : Jurnal Hukum Humaniter Dan HAM*, *3*(1), 11–22. https://doi.org/10.25105/teras-lrev.v3i1.10742

Novita, A. P., Fatmanegara, F., Runtuwene, J. J., Samuela, J. T., Syahbani, M. F., Studi, P., Informasi, S., & Kunci, K. (2023). CYBER SECURITY THREATS; ANALISIS DAN MITIGASI RESIKO RANSOMWARE DI INDONESIA. *Jurnal Simasi : Jurnal Ilmiah*

Sistem Informasi, *3*(1), 160–169. https://doi.org/10.46306/sm.v3i1

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (n.d.). *Ancaman dan Solusi Serangan Siber di Indonesia*. http://ejournal.upi.edu/index.php/TELNECT/

Prakoso, G., & Khamas Heikmakhtiar, A. (2024). Analisis Keamanan Jaringan: ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology. *Journal on Education*, *06*(02), 12895–12902.

Pringsewu, U. A., & Septasari, D. (2024). *Cyber Security and The Challenge of Society 5.0 Era inIndonesia*.http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Ramadhan, R. A., Kudus Zaini, A., & Mardafora, J. (2022). *Pelatihan Investigasi Digital Forensik*. https://journal.uir.ac.id/index.php/jpmpip/article/view/11003

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

Ray, A., Firdaus, S., & Voutama, A. (2023). *Memanfaatkan Kerentanan Broken Access Control Pada Website Orami Untuk Membatalkan Pesanan Dan Meniru Identitas Pengguna*. https://jurnal.unai.edu/index.php/teika

Rezki Syaputra, & Syaifudin. (2020). Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis. *Jurnal Jaringan Komputer Dan Keamanan*, *01*.

Riskiyadi, M. (2020). *INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME* (Vol. 3, Issue 2).

Sainuri Mubarak, A., Nur Insirat, M., Nurul Lutfiya, M., Negeri, S., Muhammadiyah Makassar, U., & Negeri Makassar, U. (2024). *SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention*. https://doi.org/10.31284/p.snestik.2024.5588

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. *Journal of Business and Entrepreneurship*, *11*(1), 23–33. https://doi.org/10.46273/job&e.v11i1.365

Tri Ginanjar Laksana, & Sri Mulyani. (2024). PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN. *JURNALJUKIM*.

Wijaya Kusuma, A., Alwi, E. I., & Ramdaniah, R. (2024). *Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)* (Vol. 7, Issue 1).