# ANALISIS DIGITAL FORENSIK TERHADAP PT HERBAL PHARMACEUTICAL: STUDI KASUS PT ANALIS FORENSIK DIGITAL

**KERJA PRAKTIK**

**Program Studi**

**S1 Sistem Informasi**

**Oleh:**

**SOPHIE ANASTASYA PUTRI BR**

**21410100012**

**FAKULTAS TEKNOLOGI DAN INFORMATIKA**

**UNIVERSITAS DINAMIKA**

**2024**

# ANALISIS DIGITAL FORENSIK TERHADAP PT HERBAL PHARMACEUTICAL: STUDI KASUS PT ANALIS FORENSIK DIGITAL

Diajukan sebagai salah satu syarat untuk menyelesaikan

Program Sarjana


**Disusun Oleh :**

| | | |
|---|---|---|
| **Nama** | **:** | **Sophie Anastasya Putri BR** |
| **Nim** | **:** | **21410100012** |
| **Program** | **:** | **S1 (Strata Satu)** |
| **Jurusan** | **:** | **Sistem Informasi** |

**FAKULTAS TEKNOLOGI DAN INFORMATIKA**

**UNIVERSITAS DINAMIKA**


**2024**

Selalu ada jalan untuk setiap persoalan

Sophie Anastasya Putri BR

*Laporan Kerja Praktik ini*

*Saya persembahkan kepada*

*Keluarga, Dosen Pembimbing, dan*

*Teman-teman yang saya kasihi*

**LEMBAR PENGESAHAN**

**ANALISIS DIGITAL FORENSIK TERHADAP PT HERBAL PHARMACEUTICAL: STUDI KASUS PT ANALIS FORENSIK DIGITAL**

Laporan kerja praktik oleh

Sophie Anastasya Putri BR

**NIM: 21410100012**

Telah diperiksa, diuji, dan disetujui

Surabaya, 5 Agustus 2024

Disetujui

| Dosen Pembimbing, | Penyelia, |
|---|---|
| Ayuningtyas cn=Ayuningtyas, o=Universitas Dinamika, ou=Sistem Informasi, email=tyas@dinamika.ac.id, c=ID 2024.08.05 22:34:57 +07'00' | analis FORENSIK DIGITAL |
| **Ayuningtyas, S.Kom., M.MT,** | **Setiya Purbaya** |
| NIDN: 0722047801 | |

Mengetahui,
Ketua Program Studi S1 Sistem Informasi

Digitally signed by Julianto
Date: 2024.08.07 17:49:19 +07'00'

**Julianto Lemantara, S.Kom., M.Eng**
NIDN: 0722108601

## PERNYATAAN

## PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa **Universitas Dinamika**, Saya:

| | |
|---|---|
| Nama | : **Sophie Anastasya Putri BR** |
| NIM | : **21410100012** |
| Program Studi | : **S1 Sistem Informasi** |
| Fakultas | : **Fakultas Teknologi dan Informatika** |
| Jenis Karya | : **Laporan Kerja Praktik** |
| Judul Karya | : **ANALISIS DIGITAL FORENSIK TERHADAP PT HERBAL PHARMACEUTICAL: STUDI KASUS PT ANALIS FORENSIK DIGITAL** |

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, Saya menyetujui memberikan kepada **Universitas Dinamika** Hak Bebas Royalti Non-Eksklusif (***Non-Exclusive Royalty Free Right***) atas seluruh isi/sebagian karya ilmiah Saya tersebut diatas untuk disimpan, dialihmediakan, dan dikelola dalam bentuk pangkalan data (***database***) untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama Saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.
2. Karya tersebut diatas adalah hasil karya asli Saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya, atau pendapat orang lain yang ada dalam karya ilmiah ini semata-mata hanya sebagai rujukan yang dicantumkan dalam Daftar Pustaka Saya.
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiasi pada karya ilmiah ini, maka Saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada Saya.

Demikan surat pernyataan ini Saya buat dengan sebenar-benarnya.

Surabaya, 10 Juli 2024


Sophie Anastasya Putri BR
NIM: 21410100012

# ABSTRAK

Penelitian ini bertujuan untuk menganalisis serangan siber yang terjadi pada web server milik PT Herbal Pharmaceutical melalui pendekatan forensik digital. Studi kasus ini dilakukan dalam rangka program Magang dan Studi Independen Bersertifikat (MSIB) di PT Analis Forensik Digital (PT AFD). Metodologi yang digunakan meliputi pengumpulan data, eksaminasi, analisis, dan pelaporan berdasarkan standar NIST. Data yang dianalisis mencakup log server Apache2 yang mencatat aktivitas selama periode serangan dari Februari hingga Mei 2024. Hasil analisis menunjukkan adanya serangan web *defacement, ransomware*, dan akses ilegal yang dilakukan oleh pelaku. Penelitian ini memberikan pemahaman mendalam tentang jenis-jenis serangan yang dapat menargetkan web server, metode yang digunakan oleh penyerang, serta dampak dari serangan tersebut. Selain itu, laporan ini juga menyusun rekomendasi langkah mitigasi dan pencegahan untuk meningkatkan keamanan siber di masa mendatang. Temuan ini dapat membantu PT Herbal Pharmaceutical dalam memperkuat sistem keamanannya dan memberikan kontribusi bagi pengembangan praktik forensik digital di Indonesia.

**Kata Kunci**: *Forensik Digital, MSIB, Serangan Siber, PT Herbal Pharmaceutical, PT Analis Forensik Digital , Web Server*

# KATA PENGANTAR

Puji syukur dengan kehadirat Tuhan Yang Maha Esa yang telah memberikan berkat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan kerja praktik ini dengan judul "ANALISIS FORENSIK DIGITAL TERHADAP PT HERBAL PHARMACEUTICAL: STUDI KASUS MSIB PT ANALIS FORENSIK DIGITAL" ini dengan baik dan lancar. Penyelesaian laporan Kerja Praktik ini sebagai syarat wajib untuk menyelesaikan program sarjana. Tidak terlepas dari bantuan dari pihak yang telah memberikan masukan, nasihat, saran, kritik kepada penulis. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada:

1. Ayah dan Ibu tercinta yang memberikan doa dan dukungan penuh kepada saya
2. Ibu Ayuningtyas, S.Kom., M.MT. selaku Dosen Pembimbing yang sudah memberikan masukan, nasihat, motivasi, dan bimbingan selama proses penyelesaian kerja praktik.
3. Pak Setiya Purbaya selaku mentor Analis Forensik Digital di kelompok penulis yang selalu membimbing penulis secara langsung selama kegiatan Magang dan Studi Independen Bersertifikat berlangsung.
4. Untuk sahabat dan teman – teman perkuliahan di Universitas Dinamika Surabaya yang telah membantu dalam proses penyelesaian kerja praktik.

Penulis menyadari bahwa laporan ini masih jauh dari kata sempurna. Dengan demikian penulis mengharapkan kritik dan saran yang membangun dari pembaca untuk penyempurnaan dalam menyelesaikan laporan. Semoga laporan Kerja Praktik ini dapat bermanfaat untuk penulis sendiri, dan para pembaca.

Surabaya, 18 Juli 2024

Penulis

# DAFTAR ISI

**Halaman**

# DAFTAR GAMBAR

**Halaman**

## DAFTAR LAMPIRAN

**Halaman**

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

PT Herbal Pharmaceutical telah mengalami serangkaian insiden keamanan yang menunjukkan adanya upaya peretasan terhadap aplikasi web yang mereka gunakan. Insiden-insiden ini termasuk penyisipan *file* mencurigakan, perubahan data secara tidak sah, dan manipulasi hak akses pengguna. Dalam hal ini, akan dilakukan identifikasi kejanggalan yang terjadi pada berbagai fitur dan komponen aplikasi web tersebut, serta memberikan analisis terhadap pola serangan yang ditemukan berdasarkan *log* aktivitas web server. Untuk metode yang digunakan dalam proses analisis ini menggunakan metode *National Institute of Standart and Technology* (NIST). Tujuan dari penelitian ini adalah untuk mengetahui apakah benar barang bukti yang disita "*evidence tsk.ova*" merupakan alat yang digunakan untuk melakukan serangan terhadap web server milik PT Herbal Pharmaceutical.

Di era digital saat ini, web server adalah komponen penting yang sangat diandalkan dan saling terhubung. Kejahatan dunia maya meningkat, dan pelaku memanfaatkan pasar gelap untuk mendapatkan data yang bocor dan serangan *ransomware*. Sebaliknya, penyerang dapat dengan mudah mengakses jaringan komputer jarak jauh melalui web server dan aplikasi web. Fakta ini meningkatkan keterlibatan server web dalam forensik digital secara signifikan. (Hilgert, 2023).

Situs web memiliki peran penting untuk memenuhi kebutuhan pengguna. Situs-situs ini dijaga agar tetap aman. Penyerang dapat meretas situs web tanpa sepengetahuan pengembangnya dan mereka dapat bebas melakukan aktivitas

penipuan di situs web. Dalam lingkungan bisnis global, jika sebuah perusahaan tidak memiliki situs web, maka perusahaan tersebut dapat dianggap tidak berpartisipasi aktif dalam perekonomian saat ini.

Perusakan situs web adalah jenis serangan *cyber* yang umum. Dalam *defacement web* penyerang mengubah tampilan visual halaman web. (Verma, 2015). Kondisi ini berdampak pada PT Herbal Pharmaceutical yang memiliki web server tersebut. Sehingga untuk mengatasi masalah ini, diperlukan solusi untuk menyelidiki kasus nyata dan analisis forensik untuk mencegah hal-hal yang tidak diinginkan. Solusi untuk mencegah hal-hal tersebut dengan cara menghapus *file* berbahaya dari server, mengimplementasikan langkah-langkah keamanan yang lebih ketat serta memperbaharui perangkat lunak, meningkatkan konfigurasi keamanan, memantau *log* server secara rutin dan melakukan audit keamanan secara berkala untuk mencegah serangan serupa di masa mendatang. Dalam hasil penelitian ini dilakukan identifikasi kejanggalan yang terjadi pada berbagai fitur dan komponen aplikasi web tersebut, serta memberikan analisis terhadap pola serangan yang ditemukan berdasarkan *log* aktivitas web server.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, berikut rumusan masalah yang dihasilkan adalah bagaimana analisis digital forensik dalam investigasi forensik serangan terhadap perusahaan PT Herbal Pharmaceutical.

## 1.3 Batasan Masalah

Berdasarkan uraian di atas, maka dalam pelaksanaan Kerja Praktik terdapat beberapa batasan masalah, antara lain :

1. Laporan ini hanya akan membahas serangan yang umum terjadi pada *Web Server Apache2*, seperti *Remote Code Execution (RCE).*
2. Analisis forensik terbatas pada pengumpulan dan analisis data *log server Apache2.*
3. Data yang dianalisis terbatas pada *log* yang tersedia selama periode serangan bulan juni sampai mei tanggal 12 Februari 2024 dan berakhir pada tanggal 7 Mei 2024 beserta data yang dikumpulkan selama investigasi.

## 1.4 Tujuan

Berdasarkan uraian dari latar belakang dan rumusan masalah, maka dapat disesuaikan bahwa, tujuan dari kerja praktik ini yaitu mengidentifikasi sumber serangan, menganalisis metode yang digunakan oleh penyerang, menilai dampak serangan terhadap server serta menyusun rekomendasi langkah mitigasi dan pencegahan di masa mendatang.

## 1.5 Manfaat

Adapun manfaat dari pelaksanaan Kerja Praktik ini antaralain sebagai berikut:

1. Laporan ini membantu pemahaman mendalam tentang berbagai jenis serangan yang dapat menargetkan *Web Server Apache2*, serta bagaimana serangan tersebut dilakukan dan apa dampaknya.
2. Memberikan dasar untuk melakukan audit keamanan dan perbaikan sistem yang lebih baik.
3. Menyediakan contoh nyata tentang bagaimana serangan terjadi dan pentingnya penerapan praktik keamanan yang baik.

# BAB II

# GAMBARAN UMUM

## 2.1 Latar Belakang Perusahaan

Perusahaan yang memberikan *project* ini selama program Magang dan Studi Independen Bersertifikat Batch 6 adalah PT Analis Forensik Digital divisi khusus dari RootBrain (IT Security Training & Consulting). PT Analis Forensik Digital adalah perusahaan yang menyediakan Investigasi Forensik Digital, Analisa Forensik Digital, dan Laporan Forensik, serta Saksi Ahli (baik menjadi ahli pada tahap Penyelidikan, Penyidikan, hingga Saksi Ahli di Persidangan) terhadap lembaga hukum seperti Kepolisian, Advokat, Kantor Pengacara, Lembaga Pemerintahan, dan Lokasi PT Analis Forensik Digital adalah di Gedung Global Intermedia Lantai 1, Jl. Taman Siswa No. 125 Yogyakarta, Indonesia. PT Analis Forensik Digital berlokasi di Jl. Taman Siswa No 125 Yogyakarta – Indonesia, Gedung Global Intermedia Lt. 1. Logo dari PT Analis Forensik Digital sendiri dapat dilihat pada Gambar 2.1.



(rootbrain, 2020)

Gambar 2. 1 Logo PT Analis Digital Forensik

## 2.2 Identitas Perusahaan

| | | |
|---|---|---|
| Nama Instansi | : | PT Analis Digital Forensik |
| Alamat | : | Jl. Taman Siswa No 125 Yogyakarta – Indonesia, Gedung Global Intermedia Lt. 1 |
| No. Telepon | : | 08112507224 |
| *Website* | : | https://forensikdigital.com/ |
| Email | : | forensik@rootbrain.com |

## 2.3 Visi dan Misi Perusahaan

Menjadi perusahaan swasta tercanggih dan terlengkap sehingga dapat memberikan pelayanan prima di bidang forensik digital dan keamanan siber *(cybersecurity)*. Kami berkeinginan memiliki cabang di seluruh kota di tanah air untuk mampu melayani setiap orang atau lembaga maupun perusahaan dalam bidang forensik digital dan *cybersecurity*. Ikut membantu *corporate*, lembaga swasta maupun pemerintah dalam bidang penegakan hukum (*law enforcement*) yang saat ini mulai kewalahan dalam menghadapi kasus kasus terkait penanganan barang bukti elektronik maupun kasus insiden *cybersecurity*. (rootbrain, 2020)

## 2.4 Struktur Organisasi

Struktur organisasi dari PT Analis Forensik Digital merupakan founder dan CEO RootBrain.Com adalah bapak Josua M Sinambela, S.T., M.Eng. sebagai (*Principal Consultant, Digital Forensic Expert, Expert Witness)* membantu lembaga Kepolisian, *Advocat*, Lembaga Pemerintahan dalam menangani kasus kasus berkaitan *Cyber* dan *ITE*, sebagai Digital Forensic Analyst dan saksi Ahli diberbagai persidangan, selanjutnya ada bapak Pratomo Djati Nugroho, S.Pi., M.

Kom sebagai (*Digital Forensic Expert*) dan bapak Dedy Haryadi, S. T, M. Kom. sebagai (*Digital Forensic Expert*). Untuk lebih jelasnya, struktur organisasi dapat dilihat pada Gambar 2.2.


Gambar 1. 2 Struktur Organisasi PT Analis Forensik Digital



PT Analis Forensik Digital memiliki susunan struktur bagian Direksi, Tim Ahli dan *Investigator*, bagian *Operational* dalam organisasi. Struktur ini mencakup peran dan tanggung jawab dari berbagai bagian dalam struktur organisasi, memberikan gambaran yang jelas tentang bagaimana setiap bagian berkontribusi terhadap keberhasilan perusahaan. Karakteristik berikut ini penting dalam struktur organisasi PT Analis Forensik Digital :

A. *Chief Executive Officer* (CEO) memiliki tugas dan tanggung jawab sebagai berikut .

1. Bertanggung jawab atas keseluruhan operasional perusahaan.
2. Menentukan visi dan misi perusahaan serta memastikan implementasinya.
3. Membuat keputusan strategis yang mempengaruhi arah perusahaan.

B. Ahli *IT*, memiliki tugas dan tanggung jawab seperti berikut .

1. Bertanggung jawab atas infrastruktur teknologi informasi perusahaan.
2. Mengelola keamanan siber dan memastikan integritas data.
3. Mendukung kebutuhan teknologi dari berbagai departemen.

C. *Investigator* Internal, memiliki tugas dan tanggung jawab seperti berikut.

1. Bertanggung jawab atas infrastruktur teknologi informasi perusahaan.
2. Mengelola keamanan siber dan memastikan integritas data.
3. Mendukung kebutuhan teknologi dari berbagai departemen.

D. *Investigator* Keamanan, memiliki tugas dan tanggung jawab seperti berikut.

1. Menyelidiki insiden keamanan fisik atau digital.
2. Mengidentifikasi pelanggaran dan merumuskan langkah-langkah mitigasi.
3. Bekerja sama dengan pihak berwenang jika diperlukan.

E. *Operational*, memiliki tugas dan tanggung jawab seperti berikut.

1. Menyusun laporan operasional rutin untuk manajemen dan pemangku kepentingan lainnya.
2. Memastikan bahwa semua proses dan kegiatan didokumentasikan dengan baik.
3. Menyusun jadwal pemeliharaan untuk peralatan dan fasilitas untuk mencegah kerusakan dan gangguan operasional.

# BAB III

# LANDASAN TEORI

## 3.1 Kali Linux

*Kali Linux*, distribusi *Linux* berbasis *Debian* yang dikembangkan oleh *Offensive Security*, menawarkan berbagai alat untuk pengujian keamanan jaringan, analisis forensik digital, dan penetrasi sistem. Bagi para profesional keamanan siber, peneliti, dan penggemar keamanan, Kali Linux adalah alat yang sangat penting dan serbaguna. (OffSec, 2024)

## 3.2 Ubuntu

*Ubuntu*, dikembangkan oleh Canonical Ltd., merupakan sistem operasi berbasis Linux yang umum digunakan untuk desktop, server, bahkan perangkat *IoT*. *Ubuntu* adalah salah satu distribusi *Linux* yang paling umum digunakan untuk menjalankan web server dan berlisensi gratis dan *open source*. (Canonical.Ltd, 2024).

## 3.3 Splunk

*Splunk* dibuat untuk memecahkan masalah infrastruktur digital yang rumit pada tahun 2003. Sejak awal, kami—dikenal sebagai "*Splunk*"—telah membantu organisasi mengeksplorasi kedalaman data mereka seperti spelunker di dalam gua. *Cisco* membeli *Splunk* pada tahun 2024 untuk membantu bisnis terus membangun ketahanan di seluruh jejak digital mereka. Saat ini, sejumlah besar perusahaan terbesar dan paling kompleks di dunia bergantung pada *Splunk* untuk memastikan bahwa sistem penting dan vital mereka tetap aman dan andal. (Splunk, 2024)

### 3.4 SSH

*SSH*, juga dikenal sebagai klien *SSH*, adalah program yang memungkinkan Anda masuk dan menjalankan perintah pada mesin jarak jauh. Ini dirancang untuk memungkinkan dua host yang tidak dapat dipercaya berbicara satu sama lain secara aman melalui jaringan yang tidak aman. Saluran aman juga dapat digunakan untuk mengirimkan koneksi *X11*, *port TCP* apa pun, dan *soket* domain *UNIX*. *SSH* dapat menghubungkan dan masuk ke tujuan tertentu dengan alamat IP [user@] nama host atau *URI*, misalnya ssh://[user@]namahost[:port]. Pengguna harus memverifikasi identitasnya ke mesin jarak jauh dengan menggunakan salah satu metode yang tersedia. Sebuah perintah akan dieksekusi pada *host* jarak jauh, bukan pada *shell login*. Baris perintah lengkap mungkin hanya perintah atau mungkin memiliki argumen tambahan. Jika ada, argumen akan ditambahkan ke perintah, dipisahkan dengan spasi, sebelum dikirim ke server untuk dieksekusi. (Ylonen, 2024)

### 3.5 Open SSL

*OpenSSL* adalah perpustakaan perangkat lunak untuk aplikasi yang memungkinkan komunikasi aman melalui jaringan komputer terhadap penyadapan serta memungkinkan pihak di ujung lain untuk diidentifikasi. *OpenSSL* merupakan implementasi *open source* dari protokol *SSL* dan *TLS* yang banyak digunakan oleh server Internet, termasuk sebagian besar situs web *HTTPS*. Pustaka inti, yang ditulis dalam bahasa pemrograman C, menjalankan tugas *kriptografi* dasar dan menyediakan berbagai fitur. *Wrapper* tersedia untuk memungkinkan perpustakaan *OpenSSL* digunakan dalam berbagai bahasa komputer. Sebagian besar sistem operasi *Unix* (seperti *Linux, macOS,* dan *BSD), Microsoft Windows*, dan *OpenVMS* mendukung *OpenSSL*. (OpenSSL Project, 2024)

### 3.6 SCP

*SCP (Secure, Contain, Protect)* adalah sebuah karya fiksi kolaboratif yang berasal dari proyek wiki yang didedikasikan untuk menciptakan dan mencatat *"SCP"* yaitu entitas, lokasi, artefak, dan fenomena yang dianggap aneh, berbahaya, atau supernatural yang beroperasi secara sembunyi-sembunyi dan mendunia. Yayasan ini beroperasi di luar yurisdiksi dan diberi wewenang dan dipercayakan oleh setiap pemerintah nasional untuk membendung objek, entitas, dan fenomena Banyak dari *anomali* ini membahayakan kesehatan fisik dan mental dunia. Semuanya melanggar hukum alam yang diyakini oleh masyarakat global secara implisit. Rumah Tangga memiliki database informasi yang luas tentang anomali yang memerlukan Prosedur Penahanan Khusus, atau "*SCP*". Basis data utama berisi ringkasan *anomali* tersebut dan prosedur darurat untuk memelihara atau membangun kembali penahanan yang aman dalam kasus pelanggaran atau peristiwa lainnya.(Wikidot.com, 2024)

### 3.7 National Institute of Standart and Technology (NIST)

Bagian dari ilmu forensik adalah forensik digital. Ini dianggap sebagai penerapan ilmu pengetahuan untuk identifikasi, pengumpulan, pemeriksaan, dan analisis data, sambil tetap menjaga integritas data yang ketat. Teknik forensik digital dapat digunakan untuk berbagai tujuan, seperti menyelidiki pelanggaran kebijakan dan kejahatan internal, merekonstruksi peristiwa keamanan, memecahkan masalah operasional, dan memulihkan sistem dari kerusakan yang tidak disengaja. Dalam pedoman ini, forensik digital dibahas dari sudut pandang sistem, bukan dari sudut pandang penegakan hukum. Forensik Digital adalah disiplin ilmu yang juga merupakan disiplin seni. Tidak ada metode teknis

*deterministik* yang akan mengarahkan analis langsung ke jawabannya. Untuk mencapai tingkat keterampilan yang mahir, banyak latihan dan pelatihan diperlukan.

*NIST SP 800-86* adalah pedoman untuk memasukkan teknik forensik ke dalam respons insiden proses. Ini terdiri dari empat tahap utama: Pengumpulan Data yang relevan diidentifikasi, diberi label, dicatat, dan dikumpulkan. Pemeriksaan Alat dan teknik forensik digunakan untuk mengidentifikasi dan mengekstraksi informasi yang relevan dari data yang dikumpulkan. Analisis Informasi dianalisis untuk menemukan bukti yang dapat menjelaskan dasar masalah. Pelaporan menguraikan hasil dan membuat saran tambahan. (Salfati, 2022)

# BAB IV

# DESKRIPSI PEKERJAAN

## 4.1 Metodologi Penelitian

Dalam pembuatan laporan ini, metode yang digunakan yaitu metode yang umum digunakan dalam digital forensik pada *scope storage* dengan tahapan, seperti koleksi, eksaminasi, analisis dan pelaporan pada gambar 4.1.


Gambar 4. 1 Alur proses pada metode NIST

Koleksi bertujuan untuk mengumpulkan data digital dengan cara yang melindungi integritas bukti dengan cara identifikasi dan penyelamatan bukti, dokumentasi, pembuatan image forensik dan terakhir *hashing*. Eksaminasi bertujuan mengungkap dan mengisolasi data relevan dari image forensik untuk dianalisis lebih lanjut dengan cara pemulihan data yang dihapus, identifikasi file tersembunyi, eksaminasi sistem file dan analisis artefak sistem. Analisis bertujuan menginterpretasikan data yang dikumpulkan untuk membangun narasi tentang kejadian yang terjadi dengan cara menyusun kronologi aktivitas, menghubungkan korelasi data, menganalisis komunikasi dan identifikasi bukti penting. Pelaporan bertujuan menyusun laporan yang menjelaskan temuan secara jelas dan terstruktur untuk digunakan dalam proses hukum atau investigasi lebih lanjut dengan cara mendokumentasi temuan, membuat laporan tertulis,penyajian bukti dan penyediaan kesaksian ahli. (Riadi, 2020).

Tahapan pertama dimulai dengan melakukan pengumpulan bukti yaitu mengumpulkan dan mengamankan *log server apache2*. Tahap kedua melakukan analisis log untuk mencari pola serangan, sumber *IP*, dan metode yang digunakan. Tahap ketiga yaitu identifikasi kerentanan seperti menentukan jenis kerentanan yang dieksploitasi, tahap keempat menilai dampak serangan terhadap integritas dan ketersediaan sistem dan terakhir tahap kelima menyusun laporan berdasarkan temuan dari analisis *log*.

**4.2 Ringkasan Kronologi**

Di dalam ringkasan kronologi ini akan dijelaskan penyusunan suatu kejadian atau peristiwa berdasarkan urutan waktu atau urutan kejadian yang terjadi.

1. 12-02-2024 pukul 11.15 detik 4 : Pelaku memanfaatkan celah di web server yaitu *broken acces control* menggunakan akun pegawai siobat, pelaku mengubah data hasil evaluasi sebanyak 16 item
2. 12-02-2024 pukul 11.28 detik 18 : Pelaku terindikasi melakukan perubahan data hasil evaluasi dan mengubah *privilege* akun dengan memanfaatkan *broken access control* tersebut untuk mengubah data instrumen pengujian
3. 12-02-2024 pukul 11.39 detik 57 : Pelaku mengubah data instrumen pengujian melalui celah *broken acces control* dengan cara pelaku masuk menggunakan akun pegawai siobat dan pelaku melakukan penghapusan, merubah deskripsi lalu menyisipkan *script*, merubah gambar, menambahkan item yang ada di instrumen pengujian dengan *id 390, 388* dan, 387.
4. 12-02-2024 pukul 16.08 detik 53 - 16.12 detik 20 : Pelaku mengubah deskripsi item dengan *id 387*

5. 7-05-2024 pukul 21.36 detik 39 : Pelaku menambahkan item yang memiliki *id 390* menggunakan akun admin
6. 7-05-2024 pukul 05.00 detik 30 : Pelaku berhasil menyisipkan *ransomware* ke dalam web server

### 4.3 Permintaan Pemeriksaan

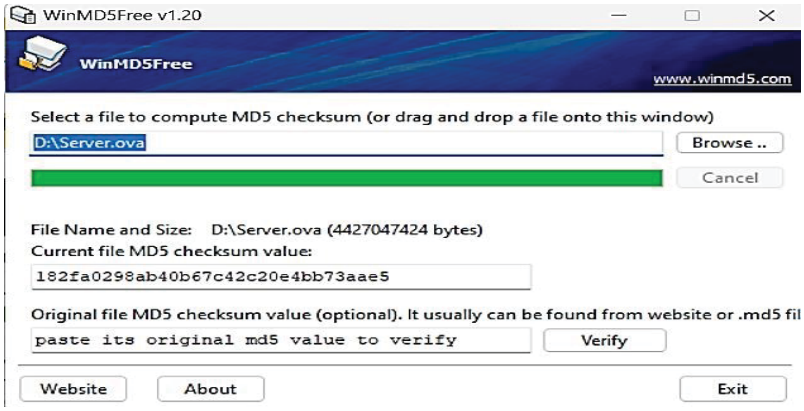
Pada tanggal 16 Mei 2024 , klien dari PT Herbal Pharmaceutical meminta kepada tim forensik 18 untuk melakukan pemeriksaan digital forensik terhadap barang bukti elektronik yang terkait dengan kasus web *defacement, ransomware*, dan *illegal acces* terhadap server milik PT Herbal Pharmaceutical.

### 4.4 Barang Bukti Yang Diperiksa

Barang bukti yang diperiksa adalah benda atau materi yang digunakan dalam penyelidikan ditemukan atau disita, serta langkah-langkah yang diambil untuk memastikan keaslian dan keadaan barang bukti tersebut tidak terganggu atau terubah.

#### 4.4.1 Detail Barang Bukti Elektronik

Server Ova dengan sistem operasi Ubuntu (64 Bit) digunakan untuk mendistribusikan dan mengimpor mesin virtual yang dibuat menggunakan teknologi Open Virtualization Format (OVF) seperti gambar 4.2 dibawah ini.



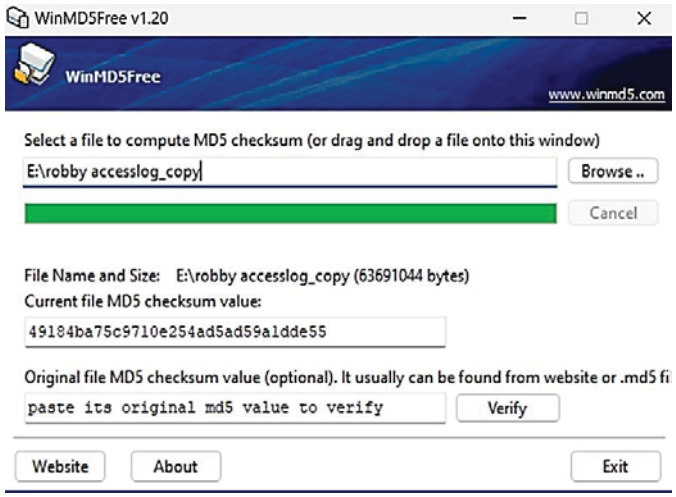

Gambar 2. 2 Server Ova

## A. Log yang dianalisis

Terdapat beberapa log yang harus diperhatikan, diantara adalah sebagai berikut ini:

a) Access.log

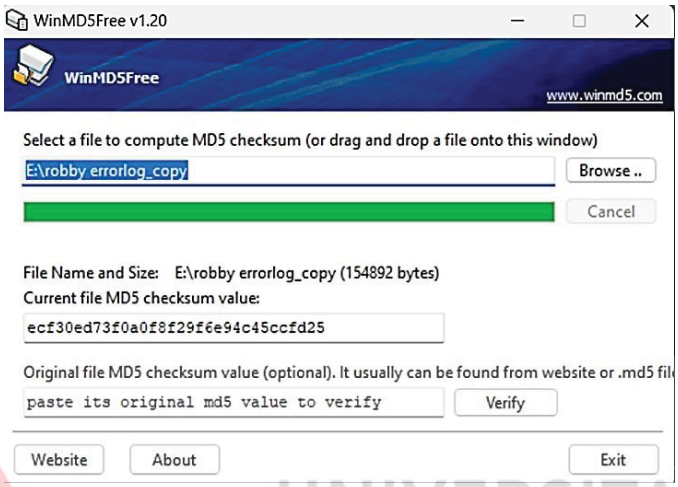
Digunakan untuk melacak aktivitas pengguna dan mengidentifikasi siapa yang telah mengakses sistem, kapan pelaku mengaksesnya, dan tindakan apa yang pelaku lakukan selama akses tersebut hasil dari log yang di analisis seperti gambar 4.3 dibawah ini.




Gambar 4. 3 access.log

b) Error.log

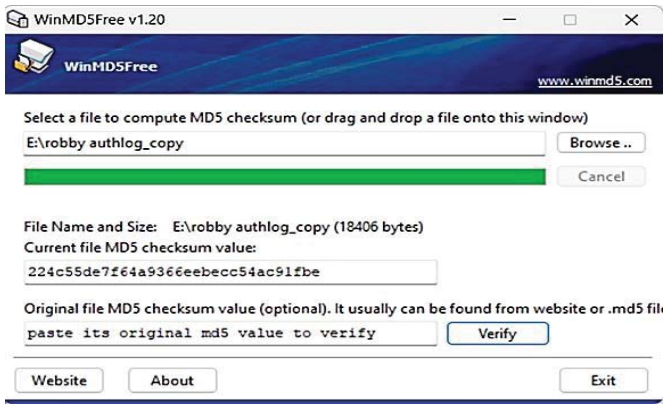
Berisi informasi tentang kesalahan atau masalah yang terjadi pada suatu sistem atau aplikasi. *Log* ini digunakan untuk mendiagnosis dan memperbaiki masalah yang terjadi. Hasil dari log yang di analisis seperti gambar 4.4 dibawah ini.




Gambar 4. 4 error.log

c) Auth.log

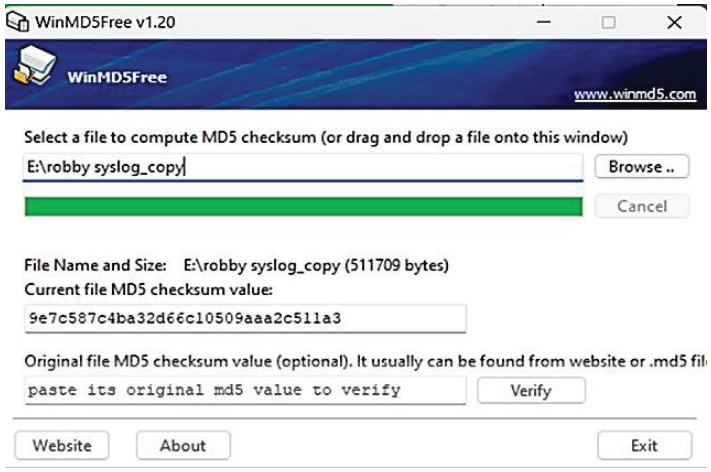
*File log* yang mencatat semua aktivitas autentikasi yang terjadi di sistem komputer atau jaringan. Digunakan untuk memantau keamanan sistem dan mendeteksi aktivitas yang mencurigakan atau upaya akses tidak sah. Hasil dari log yang di analisis seperti gambar 4.5 dibawah ini.




Gambar 4. 5 auth.log

d) Syslog

Digunakan untuk mengumpulkan, memproses, dan mengelola pesan *log* dari berbagai sumber, termasuk aplikasi, sistem operasi, dan perangkat jaringan. Hasil dari log yang di analisis seperti gambar 4.6 dibawah ini.



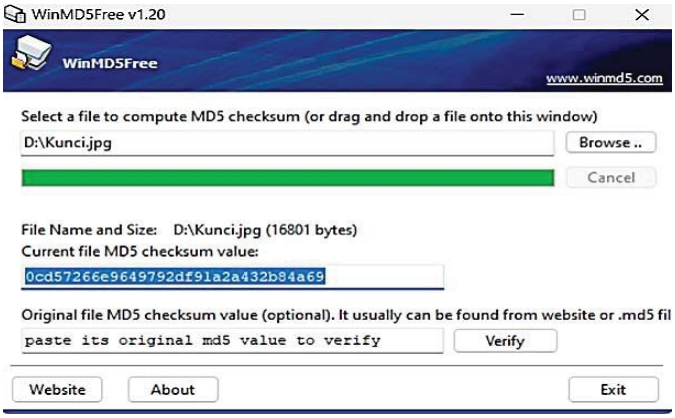

Gambar 4. 6 syslog

**B. Analisis Direktori Web Aplikasi**

Dilakukan analisis pada direktori web aplikasi yang bernama siobat, di mana ditemukan *file-file* yang disisipkan oleh pelaku. Di dalam direktori ini juga terdapat folder yang berisi *file ransomware* seperti berikut:

a. Kunci.jpg

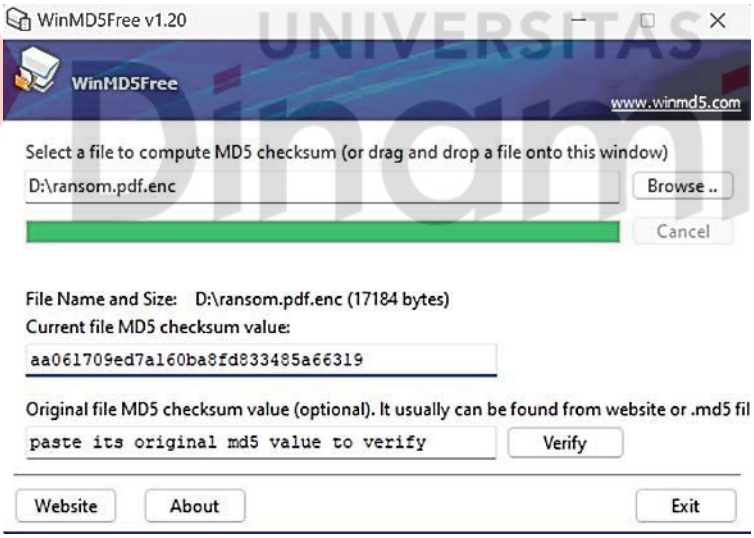
Aplikasi *WinMD5Free* yang digunakan untuk menghitung nilai checksum *MD5* dari sebuah *file kunci.jpg* seperti gambar 4.7 dibawah ini.




Gambar 4. 7 kunci.jpg

b. Ransom.pdf.enc

Aplikasi *WinMD5Free* yang digunakan untuk menghitung nilai checksum *MD5* dari sebuah *file ransom.pdf.enc* seperti gambar 4.8 dibawah ini.




Gambar 4. 8 ransom.pdf.enc

c. Evidience TSK.ova

Barang bukti ini merupakan *device* yang digunakan pelaku untuk melakukan serangan. Analisis dilakukan untuk menggali jejak pelaku dalam

melakukan serangan serta mencocokkan data-data bukti yang ada di dalam *device* pelaku dengan data bukti yang ada pada *server.ova*.

d. Identifikasi Sistem

Hasil Identifikasi Sistem Umum

| | |
|---|---|
| Nama Host | : cyberlabs |
| Virtualisasi | : Oracle VirtualBox |
| Sistem Operasi | : Ubuntu 22.04.4 LTS |
| Kernel | : Linux 5.15.0-105-generic |
| Arsitektur | : x86-64 |
| Vendor Perangkat Keras | : innotek GmbH |
| Model Perangkat Keras | : VirtualBoX |

e. Detail Hasil Identifikasi

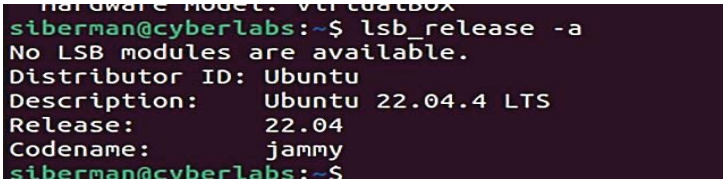
1) Hostname

Digunakan untuk mengakses perangkat melalui jaringan, dan seringkali digunakan dalam konfigurasi jaringan dan komunikasi antar perangkat. Perintah '*hostnamectl'* untuk mengelola dan menampilkan informasi terkait nama host (hostname) seperti gambar 4.9 dibawah ini.


Gambar 4. 9 Hostname

2) Informasi OS

Digunakan untuk memahami lingkungan komputasi Linux yang pelaku gunakan. Perintah "*lsb_release -a"* untuk menampilkan informasi tentang distribusi Linux yang sedang berjalan seperti gambar 4.10 dibawah ini.




Gambar 4. 10 Informasi OS

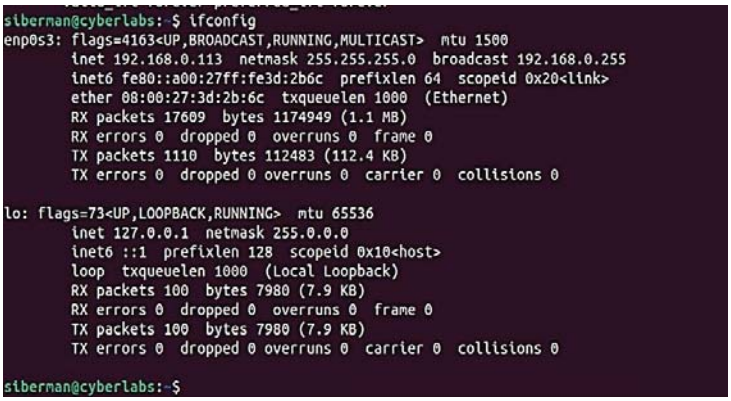
3) Alamat IP

Digunakan untuk mengidentifikasi dan lokasi perangkat di jaringan. Perintah "*ip addr"* untuk menampilkan, mengatur, dan memanipulasi alamat IP dan properti jaringan lainnya pada sistem. Seperti gambar 4.11 dibawah ini.


Gambar 4. 11 Alamat IP

4) Konfigurasi Jaringan

Digunakan untuk mengatur dan mengelola koneksi antar perangkat dalam suatu jaringan komputer. Perintah *"ifconfig"* untuk mengonfigurasi, mengontrol, dan memeriksa antarmuka jaringan. Seperti gambar 4.12 dibawah ini.




Gambar 4. 12 Konfigurasi Jaringan

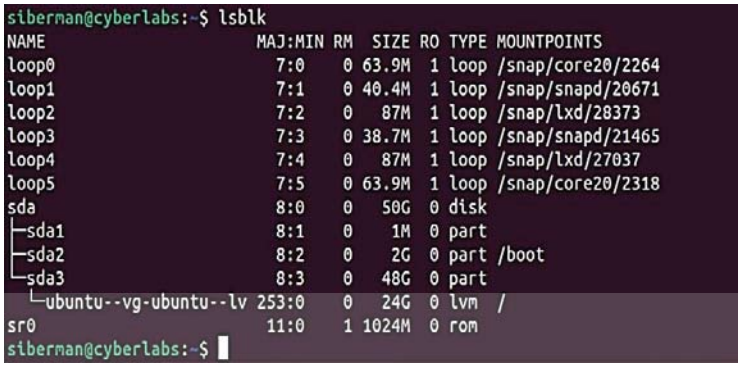
5) CPU

Digunakan untuk mengeksekusi instruksi-instruksi program komputer dan melakukan pemrosesan data. Perintah *"lscpu"* untuk menampilkan informasi tentang arsitektur CPU dan unit pemrosesan pusat (CPU) di sistem pengguna. Seperti gambar 4.13 dibawah ini.


Gambar 4. 13 CPU

6) Storage

Digunakan untuk menyimpan, mengakses, dan memanfaatkan informasi secara efisien. Perintah *"lsblk"* untuk menampilkan informasi tentang semua perangkat *blok (block devices)* yang tersedia di sistem, seperti USB drive. Seperti gambar 4.14 dibawah ini.




Gambar 4. 14 Storage

7) Memori yang tersedia

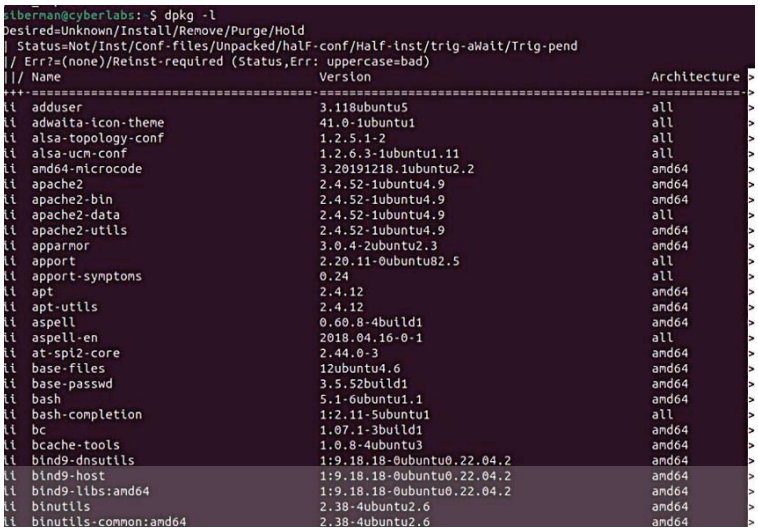
Digunakan untuk menyimpan dan mengakses informasi. Perintah "*free -h*" untuk menampilkan informasi tentang penggunaan memori di sistem. Seperti gambar 4.15 dibawah ini.


Gambar 4. 15 Memori yang tersedia

8) Paket yang terinstal

Kumpulan file yang berisi program atau perangkat lunak yang digunakan untuk menginstal atau menghapus perangkat lunak tersebut. Perintah "*dpkg -l*" untuk menampilkan daftar semua paket yang diinstal di sistem, selain itu bisa

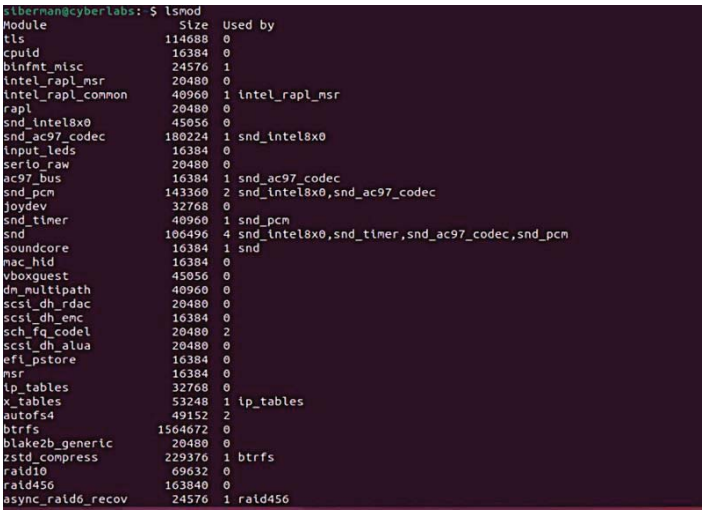
menjadi alat yang sangat berguna seperti manajemen paket, memberikan pandangan tentang paket yang terpasang, versinya, dan statusnya. Seperti gambar 4.16 dibawah ini.




Gambar 4. 16 Paket yang terinstal

9) Modul kernel yang dimuat

Digunakan untuk menambahkan *driver* perangkat keras baru, yang memungkinkan *kernel* untuk berinteraksi dengan perangkat keras yang tidak didukung secara langsung oleh *kernel* utama. Perintah "*lsmod*" untuk menampilkan daftar modul *kernel* yang saat ini dimuat di sistem. Seperti gambar 4.17 dibawah ini.



```
stberman@cyberlabs: $ lsmod
Module                  Size  Used by
tls                   114688  0
cpuid                  16384  0
binfmt_misc            24576  1
intel_rapl_msr         20480  0
intel_rapl_common      40960  1 intel_rapl_msr
rapl                   20480  0
snd_intel8x0           45056  0
snd_ac97_codec        180224  1 snd_intel8x0
input_leds             16384  0
serio_raw              20480  0
ac97_bus               16384  1 snd_ac97_codec
snd_pcm               143360  2 snd_intel8x0,snd_ac97_codec
joydev                 32768  0
snd_timer              40960  1 snd_pcm
snd                   106496  4 snd_intel8x0,snd_timer,snd_ac97_codec,snd_pcm
soundcore              16384  1 snd
mac_hid                16384  0
vboxguest              45056  0
dm_multipath           40960  0
scsi_dh_rdac           20480  0
scsi_dh_emc            16384  0
sch_fq_codel           20480  2
scsi_dh_alua           20480  0
efi_pstore             16384  0
msr                    16384  0
ip_tables              32768  0
x_tables               53248  1 ip_tables
autofs4                49152  2
btrfs                1564672  0
blake2b_generic        20480  0
zstd_compress         229376  1 btrfs
raid10                 69632  0
raid456               163840  0
async_raid6_recov      24576  1 raid456
```

Gambar 4. 17 Modul kernel

### 4.4.2 Perolehan Barang Bukti

Barang bukti elektronik diperoleh dari klien kami PT Herbal Pharmaceutical pada tanggal 16 Mei 2024. Barang bukti diterima dalam keadaan utuh berbentuk *file ova.*

## 4.5 Peralatan dan Software yang digunakan

Peralatan dan software yang digunakan dalam pemeriksaan digital forensik ini adalah:

1. Ubuntu
2. Kali Linux
3. Splunk
4. SSH
5. Open SSL
6. SCP

### 4.6 Proses Akuisisi

Proses akuisisi dilakukan dengan menggunakan *SSH* di *kali Linux* untuk menghubungkan *device* penulis ke server lalu penulis mengambil *log* yang diperlukan seperti *Acces log, Error log, Syslog, Auth.log, Kunci.jpg, ransom.pdf.enc*. Hasil akuisisi disimpan dalam *flashdisk* dan dalam *device* penulis.

### 4.7 Proses Analisis Hasil Ekstraksi

Proses analisis hasil ekstraksi dilakukan dengan menggunakan *Splunk*. Hasil analisis didokumentasikan dalam *JPG* dengan *Screenshot device* penulis dan sebagian ada yang menjadi *file* dengan format *txt* seperti *file log*.

### 4.8 Proses Analisis

Proses analisis untuk memahami, mengevaluasi, dan menarik kesimpulan dari data atau informasi tertentu serta menentukan tujuan analisis dan memahami pertanyaan atau masalah yang ingin dipecahkan.

#### 4.8.1 Pengambilan log di dalam server

Penggunaan *tool* SSH dan SCP untuk pengambilan *log* yang dibutuhkan seperti *Acces log, Error log, Syslog*, dan *Auth log* untuk dianalisa *log* serangan nya.

#### 4.8.2 Analisa web server yang diserang

Analisis dengan memperhatikan setiap bagian dari web server dan ditemukan banyak kejanggalan seperti terdapat *file-file* aneh yang diduga disisipkan menggunakan *tool* anti forensik oleh pelaku untuk melakukan *backdoor shell* di dalam web server milik PT Herbal Pharmaceutical, *privilege* dari kelas akun yang

telah diubah tanpa sepengetahuan admin, dan perubahan item di beberapa menu dalam web server tersebut.

### 4.8.3 Analisa log server

Analisis *log* server yang telah diakuisisi dari server seperti *access log, error log, syslog*, dan *auth log* menggunakan Splunk dan ditemukan banyak *log* mencurigakan seperti pengunggahan *file superstar reverse.php, june.php, cobalagi.php, reverse.php*, dan lain-lain ke dalam web server. Kemudian, pelaku juga melakukan perubahan item di beberapa menu seperti menu Hasil Evaluasi Obat, Instrumen Pengujian, dan *Privilege Configuration*. Semua *log* yang berhubungan dengan serangan ke web server telah dicocokan dengan menu user *log acces* yang ada di web server dan menghasilkan hasil yang valid.

### 4.8.4 Analisa direktori server

Analisis isi dari direktori didapati folder bernama siobat, folder atau direktori tersebut telah disisipi beberapa *file* oleh pelaku sesuai dengan *log* yang ada di *file acces.log* dan *user log acces* di web server seperti *hacked1.jpg, hacked.jpg, kunci.jpg*, dan *file-file* yang berhasil disisipkan ke web server pun ada di dalam direktori siobat. Beberapa *file* dapat dibuka namun ada satu *file* yang kemungkinan terenkripsi dan perlu dianalisis lanjut yaitu *file kunci.jpg* dan *ransom.pdf.enc*

### 4.8.5 Analisa ova device pelaku

Pelaku menggunakan *device* dengan sistem operasi *Debian*. Pada direktori dan tampilan desktop *device* tersebut terdapat *file-file backdoor shell* yang telah berhasil disisipkan ke dalam web server korban. Pengecekan juga dilakukan pada

bagian riwayat peramban pelaku yang menggunakan peramban berjenis *Mozilla Firefox* sesuai dengan yang tertera di *acces log* dan pelaku melakukan *remoting* dari jarak jauh menggunakan peramban tersebut dengan *tool* bernama *b374k*. Kemudian, pelaku juga didapati melakukan pencarian tentang bagaimana cara penginstalan *b374k* dan cara menggunakan nya. *b374k* merupakan *tool* untuk melakukan *remoting* jarak jauh atau melakukan web administrasi tanpa menggunakan cpanel, koneksi SSH, dan lain-lain sehingga pelaku tidak dapat dideteksi dengan mudah.

### 4.8.6 Pembukaan file enkripsi

Analisis *file kunci.jpg* memerlukan teknik anti forensik yaitu penggantian *header* yang bermaksud mengganti format *file* .jpg menjadi .pdf dan setelah penggantian *header* dilakukan isi dari *kunci.jpg* pun dapat terlihat yaitu sebuah kata sandi *AES* dan untuk *mendecrypt file* ransom.pdf.enc digunakan *tool* OpenSSL bawaan Kali Linux, lalu menginputkan perintah dengan memasukan *password* yang didapatkan dari *kunci.jpg* yaitu "kuncirensomwaresimetris". Output hasil deskripsinya berupa *file* ransom.pdf yang akhirnya bisa kami akses berisi kalimat "Selamat anda telah berhasil *men-decrypt file* yang terenkripsi".

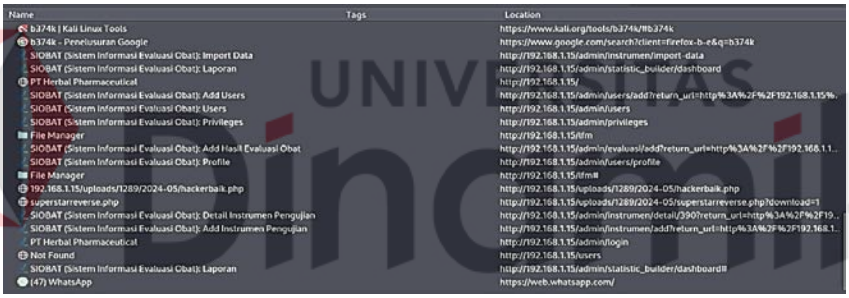
## 4.9 Ringkasan pemeriksaan

Pemeriksaan digital forensik menemukan bukti-bukti yang menguatkan dugaan pencurian data perusahaan. Bukti-bukti tersebut antara lain:

1. Pada gambar 4.18 dibawah ini merupakan *file-file* mencurigakan yang telah berhasil disisipkan.

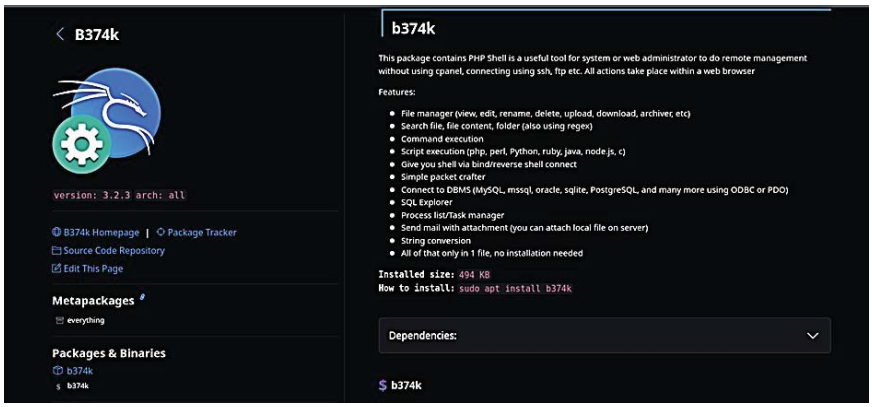

Gambar 4. 18 File Mencurigakan

2. Pada gambar 4.19 dibawah ini merupakan *log* aktivitas yang menunjukan bahwa Nanda Magistra Zulfa telah mengakses *web server* melalui platform *browser Mozilla Firefox* dengan *device Kali Linux.*




Gambar 4. 19 Log Browser Pelaku

3. Pada gambar 4.20 dibawah ini merupakan *software* yang digunakan oleh Nanda Magistra Zulfa adalah *b374k* yang berfungsi untuk melakukan *backdoor shell* tanpa *cpanel*, koneksi *ssh*, dan lain-lain.




Gambar 4. 20 Alat b374k

## 4.10 Temuan

Setelah investigasi selesai dilakukan, berikut ini adalah temuan yang didapatkan:

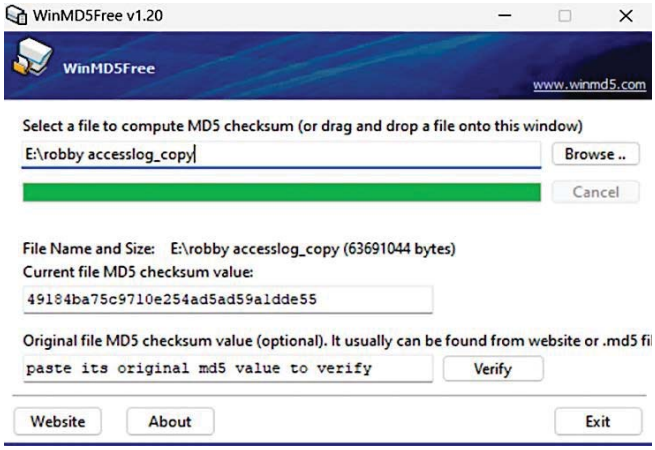
1. Nanda Magistra Zulfa telah menyisipkan *file-file* berbahaya pada *web server* PT Herbal Pharmaceutical secara tidak sah.
2. Nanda Magistra Zulfa telah menggunakan *tool* kali linux dengan nama **b374k** untuk melakukan *remoting* jarak jauh web server milik PT Herbal Pharmaceutical.
3. *File-file* berbahaya yang disisipkan ke dalam *web server* terletak dalam direktori siobat dalam server PT Herbal Pharmaceutical.

## 4.11 Hasil Temuan

Berikut ini adalah *Hashing file* yang telah diakuisisi:

1. Access log

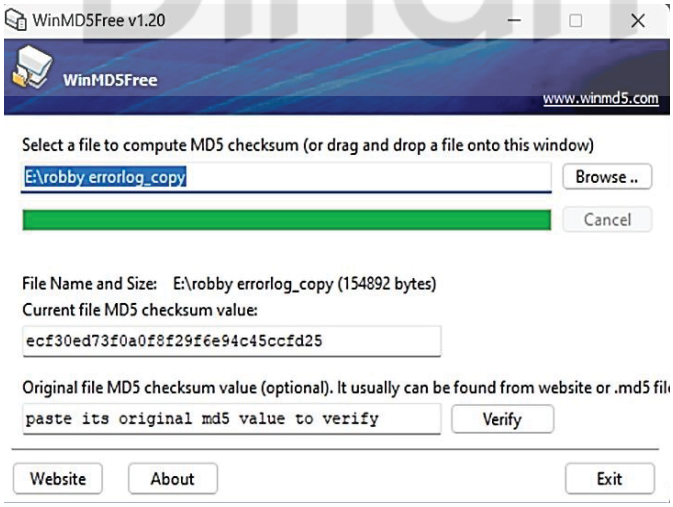
   *Hash* dari *file Access.log* yang telah diakuisisi, bahwa file tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi dan untuk memastikan bahwa bukti digital tidak diubah atau dimanipulasi selama proses investigasi seperti gambar 4.21 dibawah ini.




Gambar 4. 21 hash access.log

2. Error log

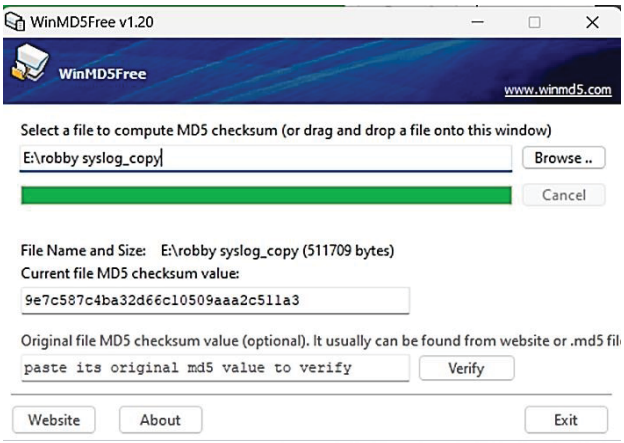
*Hash* dari *file Error.log* yang telah diakuisisi, bahwa *file* tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi serta *file* yang didapatkan adalah *file* yang benar dan tidak dimodifikasi oleh pihak yang tidak berwenang seperti gambar 4.22 dibawah ini.




Gambar 4. 22 hash error.log

3. Syslog

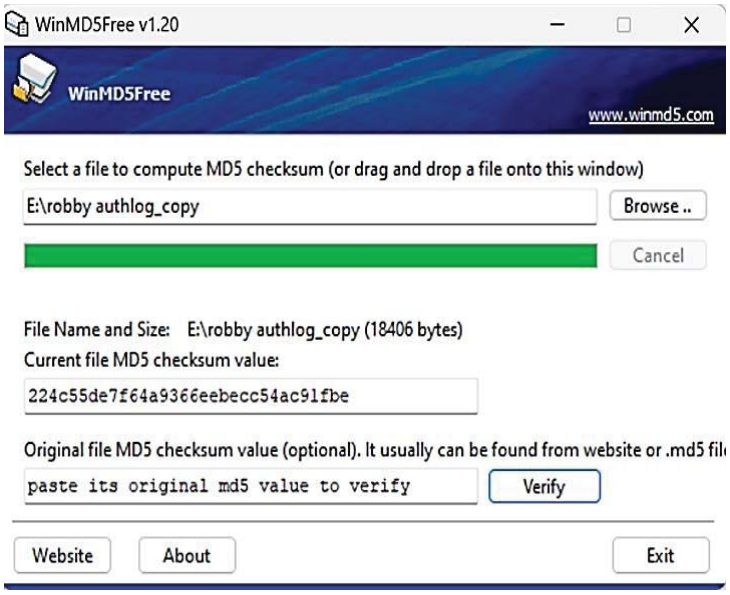
*Hash* dari *file Syslog* yang telah diakuisisi, bahwa *file* tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi serta *file* yang didapatkan adalah *file* yang benar dan tidak dimodifikasi oleh pihak yang tidak berwenang seperti gambar 4.23 dibawah ini.




Gambar 4. 23 hash syslog

4. Auth log

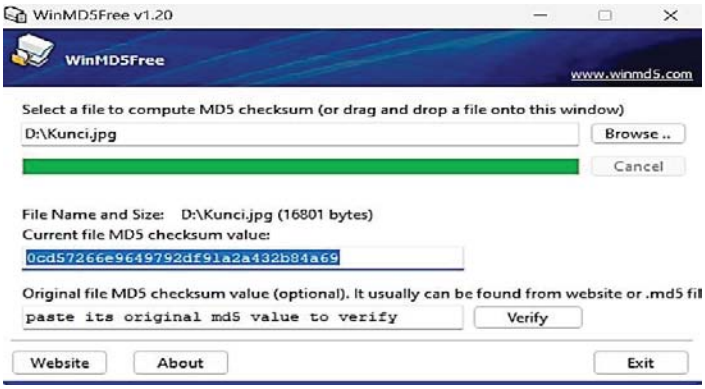
*Hash* dari *file Auth.log* yang telah diakuisisi, bahwa *file* tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi serta *file* yang didapatkan adalah *file* yang masih utuh dan tidak berubah seperti gambar 4.24 dibawah ini.




Gambar 4. 24 hash auth.log

5. File Kunci.jpg

*Hash* dari *file Kunci.jpg* yang telah diakuisisi, bahwa file tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi dan untuk memastikan bahwa bukti digital tidak diubah atau dimanipulasi selama proses investigasi, seperti gambar 4.25 dibawah ini.




Gambar 4. 25 File kunci.jpg

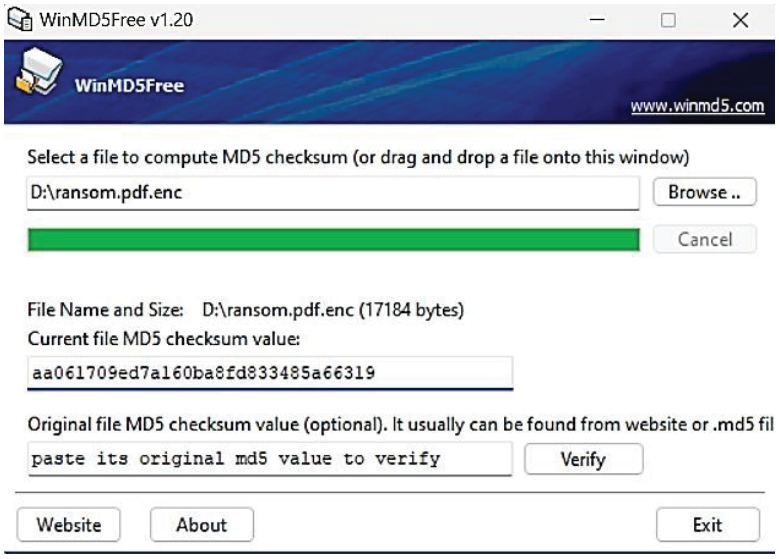
Pada gambar 4.26 didapatkan dari hasil *hash file kunci.jpg* yang telah diamankan oleh tim forensik karna file tersebut dipastikan tidak mengalami

perubahan atau kerusakan selama proses akuisisi dan untuk memastikan bahwa bukti digital tidak diubah atau dimanipulasi selama proses investigasi.


Gambar 4. 26 kunci.pdf

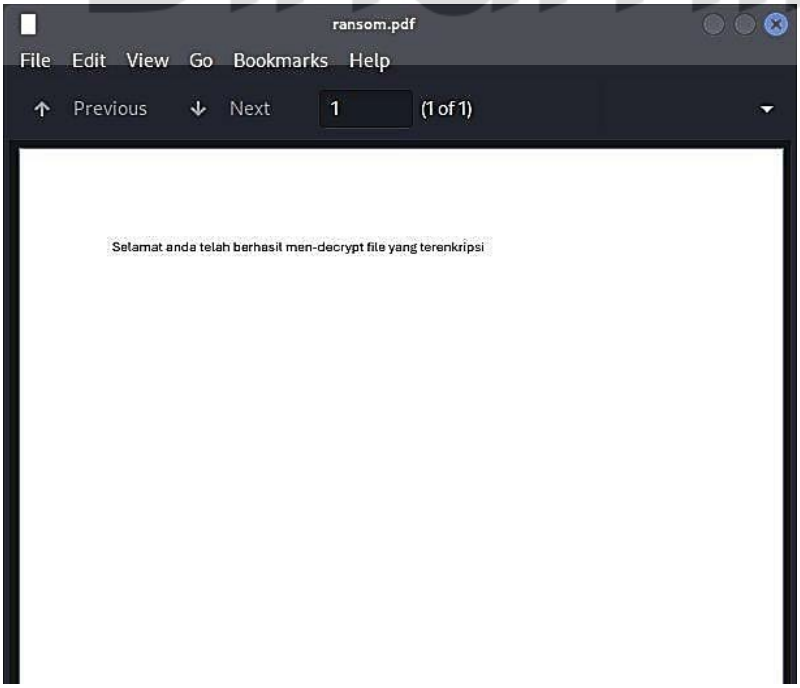
6. File ransom.pdf.enc

   *Hash* dari *file ransom.pdf.enc* yang telah diakuisisi, bahwa *file* tersebut tidak mengalami perubahan atau kerusakan selama proses akuisisi serta *file* yang didapatkan adalah *file* yang benar dan tidak dimodifikasi oleh pihak yang tidak berwenang, seperti gambar 4.27 dibawah ini.




Gambar 4. 27 hash ransom.pdf.enc

Pada gambar 4.28 didapatkan dari hasil *hash file ransom.pdf* yang telah diamankan oleh tim forensik karna file tersebut dipastikan tidak mengalami perubahan atau kerusakan selama proses akuisisi dan untuk memastikan bahwa bukti digital tidak diubah atau dimanipulasi selama proses investigasi.




Gambar 4. 28 ransom.pdf

Kronologi:

Pada bulan februari korban mendapati perubahan data pada 16 data hasil evaluasi obat, yang awalnya hasil evaluasi obat berstatus aman diubah menjadi dilarang. Selain itu, terdapat *file* aneh yang ter-upload pada laman *web*. Pelaku mendapatkan akun untuk dapat masuk ke dalam *web server* dengan banyak kemungkinan seperti *phising* dan lain-lain sehingga perlu analisis lebih lanjut untuk mengetahui nya.

Pelaku memanfaatkan celah di *web server* yaitu *broken access control* pada tanggal 12 februari 2024 pukul 11.15 detik 4 menggunakan akun pegawai.siobat. pelaku mengubah data hasil evaluasi sebanyak 16 item. Bukti log pengubahan yang ada di *access log* pada gambar 4.29 dibawah ini :


Gambar 4. 29 access log 1

Penjelasan dari log :

a. Kegiatan Berulang

Permintaan *POST* ke *endpoint /admin/evaluasi/edit-save/1* terjadi tiga kali dalam waktu yang sangat berdekatan (hanya dalam rentang beberapa menit). Ini menunjukkan bahwa ada tindakan berulang yang dilakukan pada halaman edit evaluasi.

b. Tujuan Permintaan

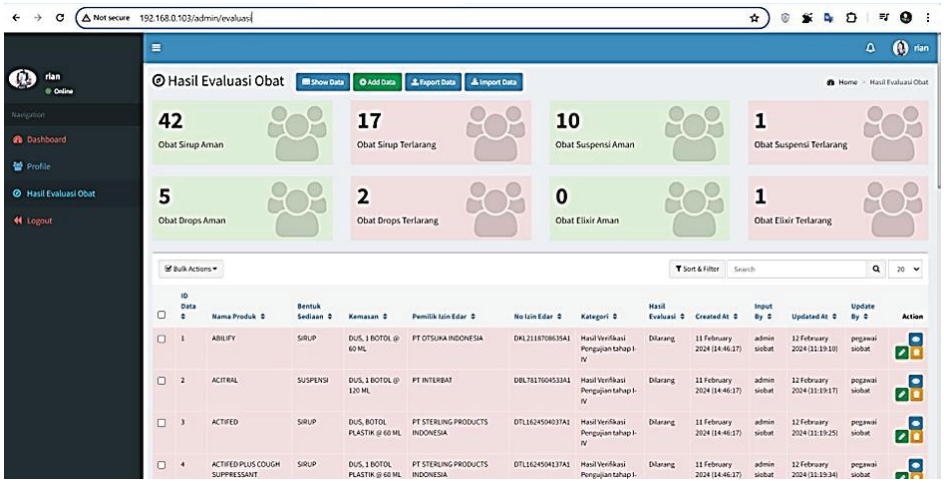
*Endpoint /admin/evaluasi/edit-save/1* kemungkinan besar digunakan untuk menyimpan perubahan yang dilakukan pada entri evaluasi. Karena ini adalah permintaan *POST*, pengguna mengirimkan data untuk disimpan di *server*.

c. Kode Status 302

Setiap permintaan menerima kode status *302*, yang berarti bahwa setelah permintaan *POST* berhasil diterima oleh server, pengguna dialihkan ke halaman lain. Ini bisa menjadi halaman konfirmasi atau halaman lain yang menunjukkan hasil dari penyimpanan data.

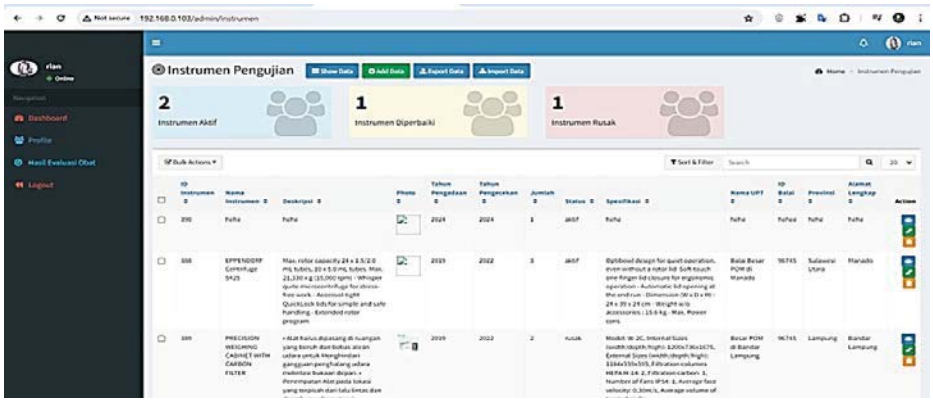
d. Referrer dan User-Agent

Semua permintaan memiliki *referrer* yang sama, menunjukkan bahwa semua tindakan berasal dari halaman *http:///192.168.43.191 /admin/evaluasi/edit/1*. *User-Agent* menunjukkan bahwa permintaan ini dilakukan dari *browser Firefox* versi *115.0* di sistem *operasi Linux x86_64*. Dengan catatan semua *log* dilakukan oleh pelaku yang sama dengan *IP 192.168.43.109* dan semua *log* yang mengindikasikan perubahan data hasil evaluasi memiliki ciri-ciri yang sama, perubahan data hasil evaluasi data berakhir pada pukul 11.28 detik 18. Dilanjutkan dengan pelaku mengubah data instrumen pengujian melalui celah *broken acces control* dengan cara pelaku masuk menggunakan akun pegawai siobat pada pukul 11.39 detik 57 Seperti gambar 4.30 dibawah ini.



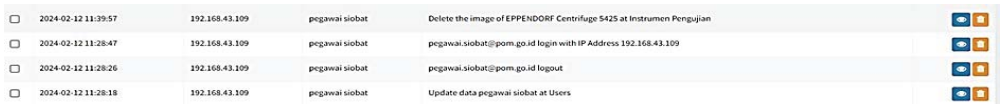

Gambar 4. 30 akun pegawai siobat

Terlihat bahwa akun pegawai hanya bisa mengakses menu hasil evaluasi dan tidak dapat mengakses menu instrument pengujian karena tidak tersedia. Pelaku mengubah url *http://192.168.0.103/admin/evaluasi* menjadi *http://192.168.0.103/admin/instrumen* dan terlihat bahwa pelaku dapat memasuki menu instrument pengujian menggunakan akun dengan *privilege* pegawai melalui celah *broken access control* seperti gambar 4.31 dibawah ini.




Gambar 4. 31 data instrumen pengujian

Lalu pada pukul 11.28 detik 18 pelaku mengubah *privilege* akun dengan memanfaatkan *broken access control* tersebut untuk mengubah data instrumen pengujian seperti gambar 4.32 dibawah ini.



| | | | | |
|---|---|---|---|---|
| 2024-02-12 11:39:57 | 192.168.43.109 | pegawai siobat | Delete the image of EPPENDORF Centrifuge 5425 at Instrumen Pengujian | |
| 2024-02-12 11:28:47 | 192.168.43.109 | pegawai siobat | pegawai.siobat@pom.go.id login with IP Address 192.168.43.109 | |
| 2024-02-12 11:28:26 | 192.168.43.109 | pegawai siobat | pegawai.siobat@pom.go.id logout | |
| 2024-02-12 11:28:18 | 192.168.43.109 | pegawai siobat | Update data pegawai siobat at Users | |

Gambar 4. 32 history perubahan data

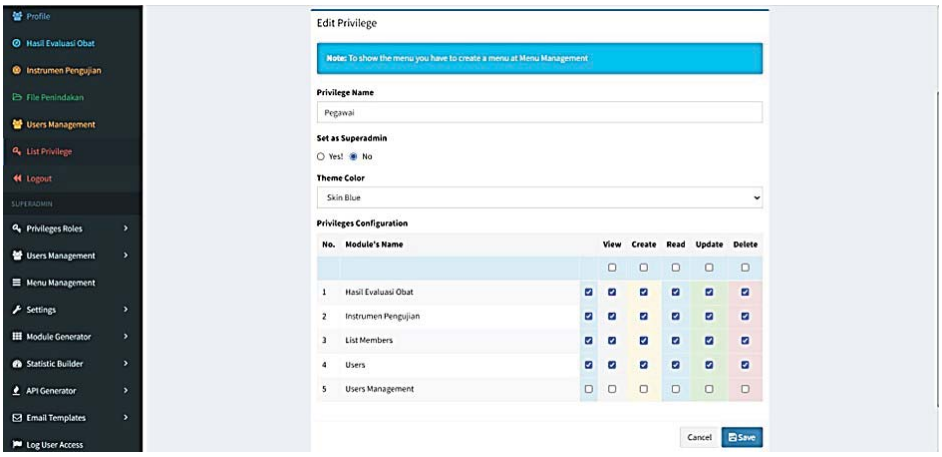
2/12/24 11:28:18.000 AM
192.168.43.109 - - [12/Feb/2024:04:28:18 +0000] "GET /admin/users?q=pegawai.siobat HTTP/1.1" 200 10168 "http://192.168.43.191/admin/users/edit/1291?return_url=http%3A%2F%2F192.168.43.191%2Fadmin%2Fusers%3Fq%3Dpegawai.siobat&parent_id=&parent_field=" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
host = DESKTOP-PS3P1BB | source = robby accesslog_copy | sourcetype = accesslog punya robby

2/12/24 11:28:00.000 AM
192.168.43.109 - - [12/Feb/2024:04:28:00 +0000] "GET /admin/users/edit/1291?return_url=http%3A%2F%2F192.168.43.191%2Fadmin%2Fusers%3Fq%3Dpegawai.siobat&parent_id=&parent_field= HTTP/1.1" 200 5896 "http://192.168.43.191/admin/users?q=pegawai.siobat" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
host = DESKTOP-PS3P1BB | source = robby accesslog_copy | sourcetype = accesslog punya robby

Gambar 4. 33 accesslog pegawai.siobat

Penjelasan log:

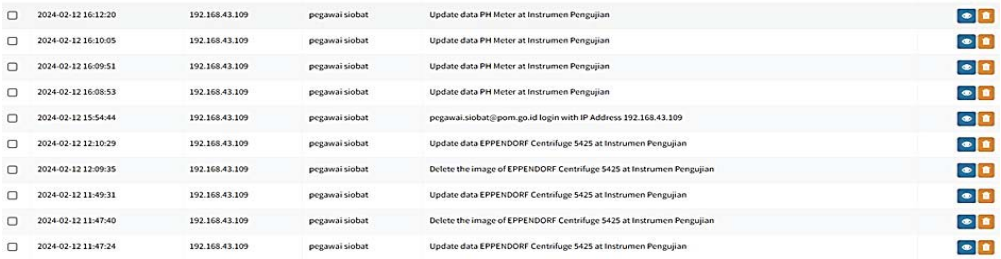
Pada gambar 4.33 merupakan aktivitas yang menunjukkan bahwa pengguna dari alamat *IP 192.168.43.109* sedang mencari pengguna dengan kata kunci pegawai.siobat di sistem admin dan kemudian mengedit informasi dari pengguna yang ditemukan dengan *ID 1291*. Kedua permintaan berhasil diproses oleh server dan mengembalikan halaman yang sesuai. Aktivitas ini merupakan bagian dari tugas administrasi dan pelaku berhasil mengubah *data user*. *Broken Access Control* adalah salah satu kerentanan keamanan yang sering ditemukan dalam aplikasi *web*, di mana aplikasi tidak dengan benar mengatur dan menegakkan hak akses pengguna. Kerentanan ini memungkinkan pengguna untuk mengakses data atau fungsi yang seharusnya tidak mereka miliki. Dikarenakan kerentanan ini pelaku dapat memanfaatkan celah yang sangat fatal untuk sebuah *web server* dalam pengelolaan akun.



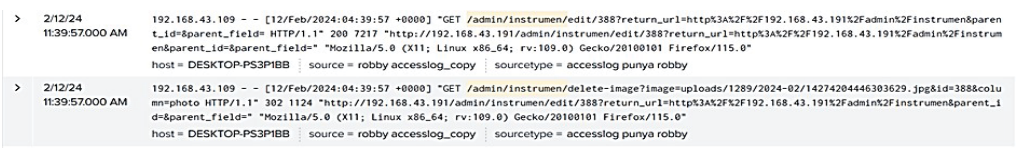

Gambar 4. 34 edit privilege

Pada gambar 4.34 salah satu contoh sebuah *broken access control* yang memanfaatkan perubahan hak *privilege configuration* yang dapat diubah tanpa harus mengubah *privilege* dari akun tersebut.

Pada gambar 4.35 terlihat pukul 11.39 detik 57 , pelaku melakukan penghapusan, merubah deskripsi lalu menyisipkan *script*, merubah gambar, menambahkan item yang ada di instrumen pengujian dengan *id 390, 388 dan, 387.*




Gambar 4. 35 history perubahan instrumen pengujian




Gambar 4. 36 accesslog penghapusan gambar

Penjelasan log:

Pada gambar 4.36 adanya permintaan tersebut yang memiliki pola yang sama, yaitu mengirimkan permintaan *POST* ke *endpoint /admin/instrumen/edit-save/388* dengan status *kode 302 (Found). Referer* dari setiap permintaan adalah *http://192.168.43.191 /admin/instrumen/edit/388?return_url=http%3A%2F%2F192.168.43.191%2Fadmin%2Finstrumen&parent_id=&parent_field=*. Pengguna menggunakan peramban *Firefox versi 115.0* di platform *Linux x86_64* untuk melakukan permintaan ini. Dengan pola yang serupa dan frekuensi yang berdekatan, ini menunjukkan bahwa pengguna sedang melakukan beberapa upaya penyimpanan perubahan pada instrumen dengan *Id 388*. Setelah berhasil menghapus gambar, pelaku menyisipkan file yang berfungsi untuk *backdoor shell system web server* dengan *file* bernama *b374k.php* . Pada pukul 16.08 detik 53 , pelaku mengubah deskripsi item dengan *id 387* sampai pukul 16.12 detik 20.


Gambar 4. 37 accesslog perubahan admin instrumen

Penjelasan log:

Pada gambar 4.38 merupakan aktivitas yang menunjukkan bahwa pengguna dari alamat *IP 192.168.43.109* sedang mengakses dan mengedit data instrumen di halaman admin. Pertama, pengguna membuka halaman instrumen *(GET /admin/instrumen)*, kemudian menyimpan perubahan yang dilakukan pada instrumen dengan *Id 387 (POST /admin/instrumen/edit-save/387).* Permintaan *GET*

berhasil menampilkan halaman instrumen, sementara permintaan *POST* berhasil menyimpan perubahan dan mengarahkan pengguna ke halaman lain. Pada tanggal 7 Mei 2024, pelaku menambahkan item yang memiliki *id 390* menggunakan akun admin pada pukul 21.36 detik 39.


Gambar 4. 38 item baru di admin instrument

Penjelasan log:

Pada gambar 4.38 merupakan aktivitas yang menunjukkan bahwa pengguna dari alamat *IP 192.168.1.16* sedang berinteraksi dengan halaman admin untuk instrumen. Pertama, pengguna menambahkan data instrumen baru *(POST /admin/instrumen/add-save)*, kemudian membuka halaman instrumen *(GET /admin/instrumen)*, dan akhirnya mengakses halaman edit untuk instrumen dengan *Id 390 (GET /admin/instrumen/edit/390)*. Semua permintaan berhasil diproses oleh server. Setelah berhasil menambahkan item, pelaku juga berhasil menyisipkan *file* bernama *June.php* dan berfungsi sama dengan file *b374k.php* yaitu sebagai *backdoor shell system* untuk peremotan jarak jauh.

Dan pada tanggal 12 Februari sampai 7 Mei 2024 pelaku menyisipkan ransom file kedalam direktori server seperti gambar 4.39 dibawah ini.


Gambar 4. 39 file ransom

Bukti dari device pelaku *Evidence TSK* yang telah dikumpulkan bahwa semua informasi dan bukti yang relevan dikumpulkan secara sistematis serta dapat dipertanggungjawabkan yaitu :

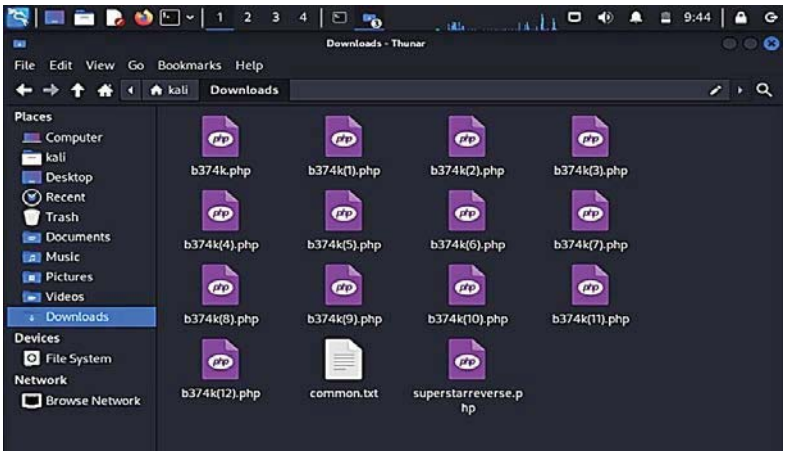
a. File disisipkan

Pada gambar 4.40 dibawah ini ditemukan *file* yang berhasil disisipkan pelaku ke dalam *web server* seperti *superstarreverse, June*, dan lain-lain.


Gambar 4. 40 Bukti file yang disisipkan

b. File b374k

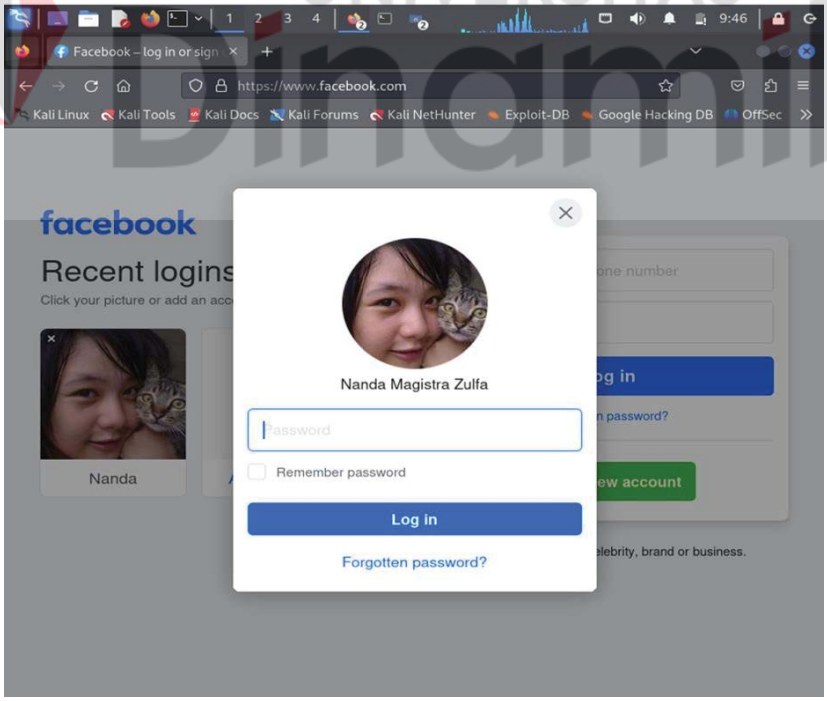
Pada gambar 4.41 dibawah ini ditemukan juga *file backdoor shell b374k* di dalam folder download pelaku.




Gambar 4. 41 file b347k di folder download

c. Akun facebook pelaku

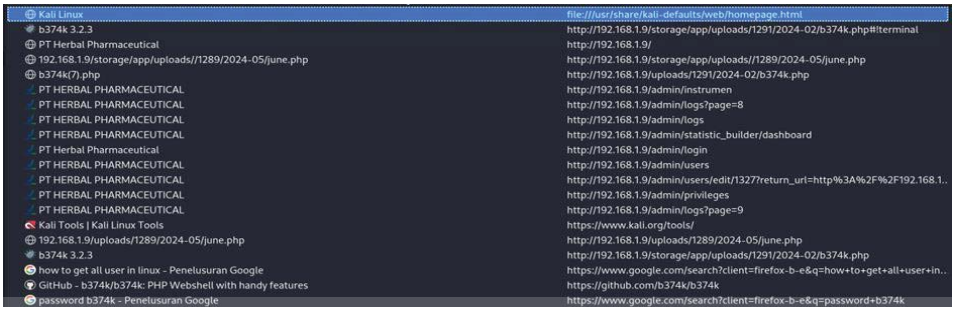
Pada gambar 4.42 dibawah ini merupakan akun dari pelaku terdeteksi sebagai akun facebook dengan nama Nanda Magistra Zulfa.




Gambar 4. 42 Akun facebook pelaku

d. History web pelaku

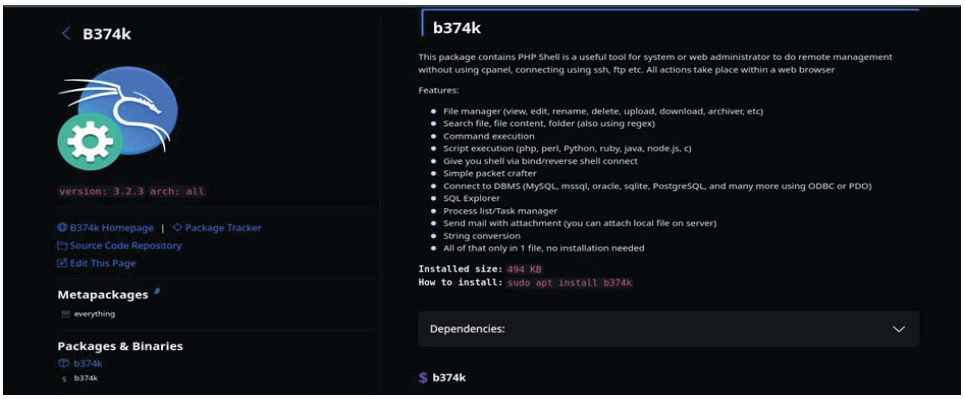
Pada gambar 4.43 dibawah ini terlihat bahwa histori *firefox* milik pelaku menunjukan bahwa pelaku melakukan *remoting* web server melalui platform *browser* tersebut dan melakukan penyisipan data berbahaya dengan *browser mozilla firefox*.




Gambar 4. 43 history web pelaku

e. Alat b347k

Pada gambar 4.44 dibawah ini diketahui bahwa *b374k* adalah alat untuk *remoting* jarak jauh *system* atau *web* administrasi tanpa menggunakan *cpanel*, koneksi dengan *ssh*, dan lain-lain. *File-file* mencurigakan yang ada di server dan device pelaku.

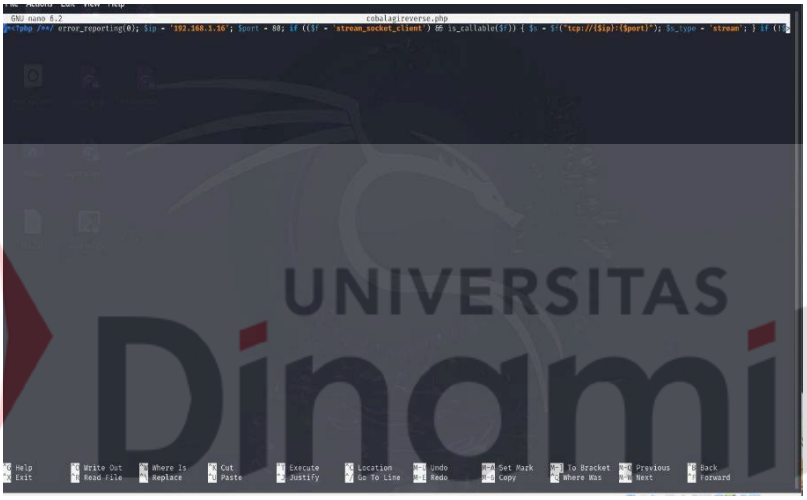



Gambar 4. 44 alat b347k

Perbandingan bukti yang telah didapatkan tim forensik antara server milik tim forensik dengan *device* milik pelaku seperti :

a. cobalagireverse.php

Pada gambar 4.45 dibawah ini merupakan server hasil analisis forensik digital dari tim yang sudah dilakukan pengambilan data dari *device* pelaku. *File cobalagireverse.php* merupakan *file PHP* yang dirancang untuk membalik atau memanipulasi string dengan menggunakan fungsi *PHP* .



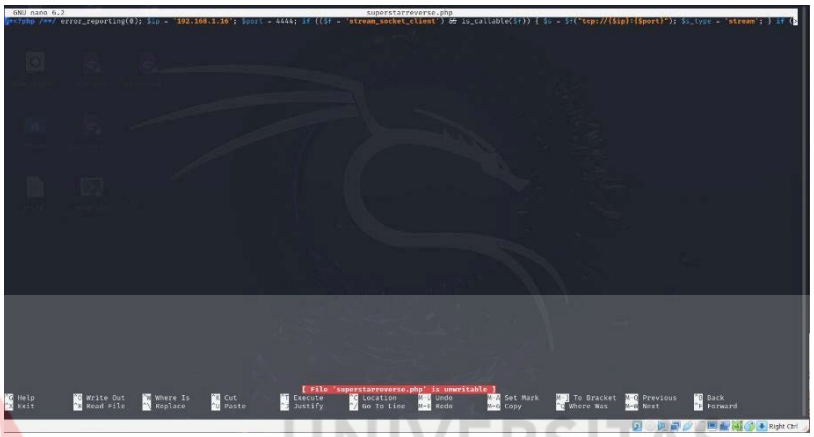
Gambar 4. 45 milik server

Gambar 4.46 dibawah ini merupakan tampilan dari *device* pelaku yang sudah tim forensik temukan dari *remoting* jarak jauh dan menghasilkan hasil yang sama dari server yang sebelumnya didapatkan.

Gambar 4. 46 milik pelaku

b. Superstarreverse.php

Pada gambar 4.47 merupakan milik server. *Superstarreverse.php* sebuah *file* atau skrip yang dirancang untuk melakukan operasi pembalikan *string* atau manipulasi data lain bahwa *file* tersebut melakukan fungsi *reverse* atau pembalikan yang sudah didapatkan dari server tim.



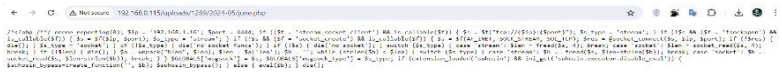
Gambar 4. 47 milik server 2

Gambar 4.48 dibawah ini merupakan tampilan dari *device* pelaku yang sudah tim forensik temukan dari *remoting* jarak jauh dan menghasilkan hasil yang sama dari server yang sebelumnya didapatkan.

Gambar 4. 48 milik pelaku 2

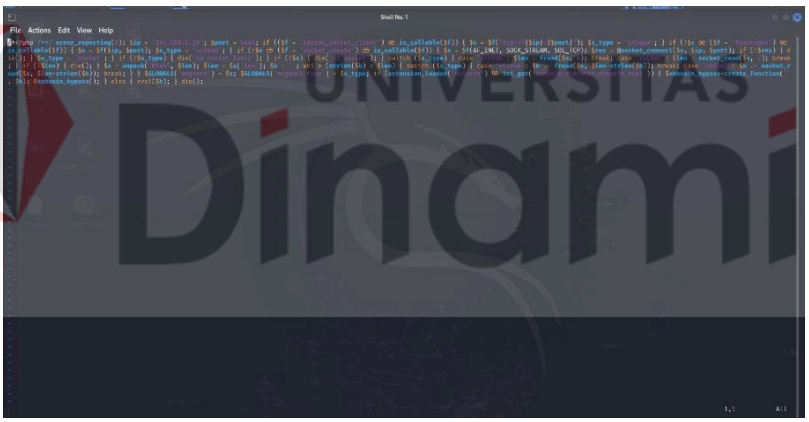
c. June.php

Pada gambar 4.49 merupakan milik server yang telah tim forensik temukan. *June.php* adalah skrip *PHP* yang dibuat untuk tujuan tertentu, seperti manipulasi data, menampilkan konten dinamis, atau memproses input pengguna.



Gambar 4. 49 milik server 3

Gambar 4.50 dibawah ini merupakan tampilan dari *device* pelaku yang sudah tim forensik temukan dari *remoting* jarak jauh dan menghasilkan hasil yang sama dari server yang sebelumnya didapatkan.



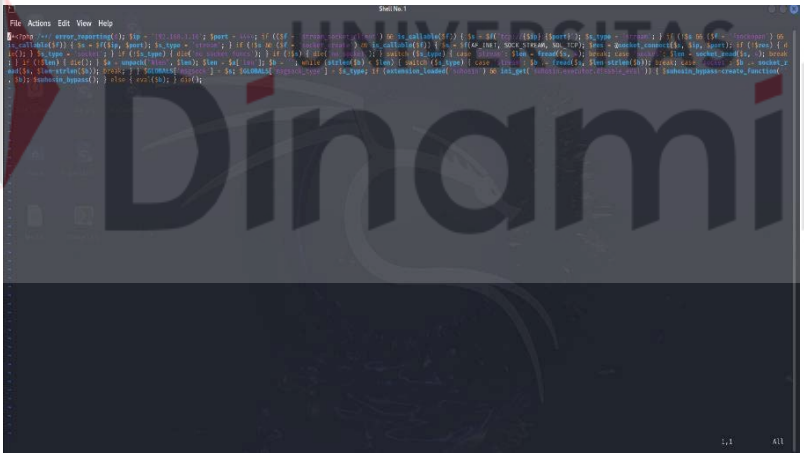
Gambar 4. 50 milik pelaku 3

d. hackerbaik.php

Pada gambar 4.51 merupakan milik server yang telah tim forensik dapatkan. *file hackerbaik.php* berisi kode atau skrip yang digunakan oleh pelaku untuk menguji keamanan sistem, mengidentifikasi kerentanan, atau menunjukkan praktik terbaik dalam pengkodean aman.

Gambar 4. 51 milik server 4

Gambar 4.52 dibawah ini merupakan tampilan dari *device* pelaku yang sudah tim forensik dapatkan dari *remoting* jarak jauh dan menghasilkan hasil yang sama dari server yang sebelumnya didapatkan.



Gambar 4. 52 milik pelaku 4

Semua isi *file* yang ada di *web server* dan *device* pelaku memiliki isi yang sama dan itu membuktikan bahwa penyisipan *file* berbahaya berhasil dilakukan oleh pelaku.

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Berikut adalah laporan dari hasil analisis digital forensik terhadap PT Herbal Pharmaceutical:

1. Pemeriksaan digital forensik menemukan bukti-bukti yang kuat *log* server yang membuktikan bahwa awal serangan terjadi pada tanggal 12 Februari 2024 dan berakhir pada tanggal 7 Mei 2024.
2. Barang bukti yang disita "evidence tsk.ova" terbukti sebagai alat yang digunakan oleh pelaku untuk melakukan serangan dengan jenis *backdoor shell* dan *broken access control* dengan bukti *tool b374k* yang terinstal di dalam *device* pelaku dan *history* dari browser mozilla firefox yang menunjukan bahwa ada nya kegiatan penyerangan sesuai dengan *log* server yang telah di analisa.
3. Ditemukan pelaku dari akun facebook yang tercantum pada browser device yaitu Nanda Magistra Zulfa.
4. Metode yang digunakan pelaku adalah pemanfaatan *broken access control* yang ada di web server dan penggunaan *tool b374k* yang telah di analisa, merupakan sebuah *tool* untuk *remoting* jarak jauh system atau web administrasi tanpa menggunakan *cpanel*, koneksi dengan ssh, dan lain-lain.

## 5.2 Saran

Untuk mengatasi serangan ini agar tidak terjadi serangan yang sama di kemudian hari disarankan untuk mengimplementasikan langkah-langkah keamanan yang lebih ketat, seperti memperbarui perangkat lunak, meningkatkan konfigurasi

keamanan, dan memantau log server secara rutin serta melakukan audit keamanan secara berkala untuk mencegah serangan serupa di masa mendatang.

# DAFTAR PUSTAKA


Tatu Ylonen, Aaron Campbell, Bob Beck, Markus Friedl, Niels Provos, Theo de Raadt, & Dug Song. (2024). *Open BSD manual page server. General Commands Manual. DESCRIPTION*. OpenBSD Manual Page Server. Retrieved from open bsd : https://man.openbsd.org/ssh.1

OpenSSL Project. (2024). *OpenSSL Cryptography and SSL/TLS Toolkit Overview*. Retrieved from: https://wiki.openssl.org/index.php/OpenSSL_Overview

Wikidot.com. (2024, June 17). *About The SCP Foundation Secure, Contain, Protect*. Retrieved from wikidot.com: https://scp-wiki.wikidot.com/

Offsec. (2024). *What is Kali Linux, and what is a Penetration Testing Distribution?* Retrieved from kali: https://www.kali.org/

Canonical.Ltd. (2024). *Ubuntu community. What is Ubuntu Advantage?* Retrieved from ubuntu: https://ubuntu.com/

Splunk. (2024). *About Splunk. The power of data. The potential for progress.* Retrieved from splunk: https://www.splunk.com/

rootbrain. (2021). *About Us dan Visi Misi PT Analis Forensik Digital*. Retrieved from analis: https://analis.id/

Hilgert, J. N., Schell, R., Jakobs, C., & Lambertz, M. (2023). About the applicability of Apache2 web server memory forensics. *Forensic Science International: Digital Investigation*, *46*. https://doi.org/10.1016/j.fsidi.2023.301610

Salfati, E., & Pease, M. (2022). *Digital Forensics and Incident Response (DFIR) framework for Operational Technology (OT)*. https://doi.org/10.6028/NIST.IR.8428

Verma, R. K., Student, M. E., & Sayyad, S. (n.d.). *Implementation of Web Defacement Detection Technique*.

Imam Riadi, Abdul Fadlil, & Muhammad Immawan Aulia. (2020). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(5), 820–828. https://doi.org/10.29207/resti.v4i5.2224