# Laporan Investigasi Forensik Digital

| **Informasi Kasus** | |
|---|---|
| **ID Kasus** | CASE-2025-001 |
| **Subjek** | Analisis Artefak Steganografi (OpenStego) |
| **Framework** | Integrated Digital Forensics Investigation Framework (IDFIF v2) |
| **Tanggal** | 18 Desember 2025 |
| **Investigator** | $$Nama Anda/Organisasi$$ |
| **Status** | Ditutup / Selesai |

## 1. Fase I: Pra-Proses (Pre-Process)

**Definisi:** Fase ini melibatkan persiapan administratif dan teknis yang diperlukan sebelum investigasi sebenarnya dimulai.

### 1.1. Otorisasi & Pemberitahuan

- **Otorisasi:** Investigasi disahkan di bawah direktif untuk menganalisis kebocoran komunikasi internal.
- **Lingkup:** Analisis file gambar yang dicurigai mengandung data tersembunyi (Steganografi).

### 1.2. Persiapan (Lingkungan Forensik)

Workstation disterilkan untuk memastikan tidak ada kontaminasi silang. Alat-alat berikut divalidasi dan disiapkan:

**Tabel 1: Inventaris Perangkat Forensik**

| **Nama Alat** | **Versi** | **Sumber** | **Fungsi** |
|---|---|---|---|
| **OpenStego** | v0.7.x | GitHub Resmi | Penyisipan/Ekstraksi Steganografi |
| **Java JDK** | JDK 21 | Oracle | Dependensi |

| | | | |
|---|---|---|---|
| | | | Runtime |
| **CertUtil** | Built-in | Windows OS | Hashing Integritas (SHA-256) |
| **Notepad++** | v8.x | Situs Resmi | Analisis Teks/Hex |

# 2. Fase II: Proses Reaktif (Reactive Process)

**Definisi:** Fase operasional di mana barang bukti diidentifikasi, dikumpulkan, dijaga integritasnya, dan dianalisis.

## 2.1. Identifikasi & Pengumpulan

Dua artefak utama diidentifikasi dan diakuisisi untuk dianalisis.

**Tabel 2: Inventaris Barang Bukti**

| ID Barang Bukti | Deskripsi | Sumber | Status |
|---|---|---|---|
| **EVID-001** | Gambar Cover Asli | Repositori GitHub | **Bersih** / Baseline |
| **EVID-002** | Gambar Stego Suspek | File yang Dicegat | **Dimodifikasi** / Suspek |
| **EVID-003** | Catatan Fisik | Tas Suspek | Bukti Fisik |

**Visual Barang Bukti:**

*Gambar 1: Representasi visual dari gambar cover asli (EVID-001).*

*Gambar 2: Representasi visual dari gambar stego suspek (EVID-002).*

## 2.2. Preservasi (Verifikasi Integritas)

Untuk menetapkan rantai kepemilikan bukti (*chain of custody*) dan membuktikan adanya perubahan, hash kriptografi dihasilkan segera setelah akuisisi.

**Tabel 3: Analisis Perbandingan Hash**

| Artefak | Algoritma | Nilai Hash | Status |
|---|---|---|---|
| **EVID-001** | SHA-256 | f81a3b9e97855770 | Baseline |

| | | | |
|---|---|---|---|
| | | 5ed2e205e0ce21be40acb50a2db1ead9dde3cb7c78b69e0e | |
| **EVID-002** | SHA-256 | b1ff74866a289341a695552be19e2e544a933cb6fc660b1bf930a8df2c0da1f7 | **Dimodifikasi** |

- **Observasi:** Ketidakcocokan hash yang jelas mengonfirmasi bahwa **EVID-002** telah diubah pada tingkat bit dibandingkan dengan **EVID-001**, yang mengindikasikan kemungkinan adanya data yang disisipkan.

## 2.3. Pemeriksaan (Steganalysis)

Tahap ini berfokus pada pemulihan muatan tersembunyi (*payload*) dari **EVID-002**.

### A. Penemuan Kredensial (Kriptanalisis)

Sebuah catatan fisik (**EVID-003**) yang ditemukan dari suspek berisi string kpvgtp4247. String ini dianalisis sebagai Caesar Cipher.

**Bukti Fisik:**

*Gambar 3: Pindaian catatan yang ditemukan di tas suspek berisi ciphertext.*

**Tabel 4: Rincian Kriptanalisis (Caesar Cipher)**

| **Ciphertext** | **k** | **p** | **v** | **g** | **t** | **p** | **4** | **2** | **4** | **7** |
|---|---|---|---|---|---|---|---|---|---|---|
| **Geseran (Shift)** | -2 | -2 | -2 | -2 | -2 | -2 | -2 | -2 | -2 | -2 |
| **Plaintext** | **i** | **n** | **t** | **e** | **r** | **n** | **2** | **0** | **2** | **5** |

- **Passphrase Dipulihkan:** intern2025

### B. Eksekusi Ekstraksi

1. **Alat:** OpenStego (Mode Ekstrak).
2. **Input:** EVID-002.
3. **Password:** intern2025 (Diperoleh dari EVID-003).
4. **Hasil:** Ekstraksi file teks tersembunyi berhasil.

**Proses Forensik:**

*Gambar 4: Tangkapan layar OpenStego berhasil mengekstrak data menggunakan password yang dipulihkan.*

### 2.4. Analisis (Tinjauan Konten)

Artefak yang diekstrak dianalisis relevansinya terhadap investigasi.

- **File Diekstrak:** aboutintern.txt
- **Tipe File:** Teks Biasa (.txt)
- **Transkrip Konten:**"Today Internship Report is The first day, you need to prepare some x to got y, i'll give you the detail, meet me at koperasi"

**Konten Diekstrak:**

*Gambar 5: Tangkapan layar file teks yang diekstrak dibuka di editor teks.*

- **Interpretasi:** Pesan tersebut mengindikasikan permintaan pertemuan rahasia di "koperasi" (kantin). Teks tersebut menyiratkan pertukaran detail ("siapkan x untuk mendapatkan y") mengenai laporan magang.

## 3. Fase III: Pasca-Proses (Post-Process)

**Definisi:** Fase terakhir yang melibatkan rekonstruksi kejadian dan penyebaran laporan akhir.

### 3.1. Rekonstruksi

Berdasarkan analisis semua artefak, linimasa kejadian berikut telah direkonstruksi.

**Tabel 5: Rekonstruksi Kejadian**

| Urutan | Kejadian | Deskripsi | Artefak Terkait |
|---|---|---|---|
| **1** | Pembuatan | Aktor memilih gambar cover standar. | EVID-001 |
| **2** | Enkripsi | Aktor mengenkripsi password intern2025 menjadi | EVID-003 |

| | | | |
|---|---|---|---|
| | | kpvgtp4247 pada catatan fisik. | |
| **3** | Penyisipan | Aktor menggunakan OpenStego untuk menyembunyikan aboutintern.txt di dalam gambar cover. | EVID-002 |
| **4** | Transmisi | Gambar yang dimodifikasi dikirim/disimpan, menunggu penerima. | EVID-002 |
| **5** | Pemulihan | Investigator mencegat gambar dan mendekripsi catatan untuk memulihkan muatan data. | Semua Artefak |

## 3.2. Kesimpulan

Analisis forensik secara meyakinkan membuktikan penggunaan steganografi.

1. **Steganografi Dikonfirmasi:** Ketidakcocokan hash antara EVID-001 dan EVID-002.
2. **Kredensial Dipulihkan:** EVID-003 (Ciphertext) berhasil didekripsi menjadi intern2025.
3. **Muatan Diekstrak:** aboutintern.txt dipulihkan berisi intelijen yang dapat ditindaklanjuti mengenai pertemuan fisik.

## 3.3. Diseminasi (Rekomendasi)

- **Tindakan Segera:** Amankan lokasi "koperasi" yang disebutkan dalam muatan data.
- **Tinjauan Kebijakan:** Tinjau pembatasan organisasi terhadap instalasi Java dan alat steganografi (OpenStego) pada perangkat endpoint.

**Akhir Laporan**