LAPORAN DETAIL LANGKAH INVESTIGASI: SIMULASI STEGANOGRAFI

Ujian Akhir Semester Mata Kuliah Digital Forensik

Dosen Pengampu : Deni Suprihadi, S.T, M.Kom., MCE.

Disusun Oleh

Adrian Muhamad Ghofur

20221310101

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER DAN SISTEM INFORMASI

UNIVERSITAS KEBANGSAAN REPUBLIK INDONESIA

TAHUN 2025

ID Kasus: SIM-STEGANO-ADRIAN-001

Tanggal Investigasi: 15 Januari 2026

Investigator: Adrian Muhamad Ghofur

Alat Utama: Steghide v0.5.1, PowerShell (Get-FileHash)

1. TUJUAN INVESTIGASI

Tujuan dari prosedur ini adalah untuk mensimulasikan siklus hidup steganografi digital, mulai dari persiapan media, penyisipan pesan rahasia, hingga ekstraksi kembali data tersebut. Prosedur ini berfungsi sebagai kontrol kualitas untuk memahami bagaimana jejak digital terbentuk selama proses steganografi berlangsung.

2. TAHAP 1: VERIFIKASI INTEGRITAS AWAL (PRESERVASI)

Sebelum melakukan modifikasi apa pun, investigator harus mencatat identitas digital dari file media (cover file). Hal ini dilakukan untuk memastikan bahwa kita memiliki titik referensi yang pasti (Baseline).

2.1 Identifikasi File Sumber

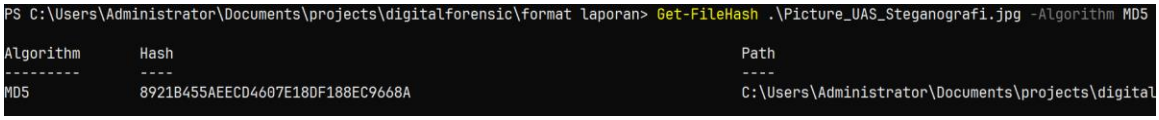
Gambar 1 Picture UAS Steganografi

1. **Nama File:** Picture_UAS_Steganografi.jpg
2. **Tipe File:** JPEG Image
3. **Ukuran:** 90,417 Bytes

2.2 Perhitungan Nilai Hash (MD5)

Nilai hash MD5 digunakan sebagai "sidik jari digital". Jika satu bit saja berubah dalam file ini, nilai hash akan berubah total.

Perintah PowerShell:



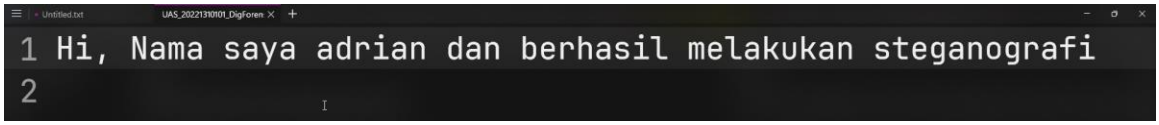
Output Verifikasi:

Algorithm	**Hash**
MD5	8921B455AEECD4607E18DF188EC9668A

3. TAHAP 2: PROSES PENYISIPAN DATA (HIDE DATA)

Pada tahap ini, investigator menyisipkan pesan tekstual ke dalam media gambar menggunakan algoritma penyisipan LSB (Least Significant Bit) yang disediakan oleh alat steghide.

3.1 Persiapan Pesan Rahasia

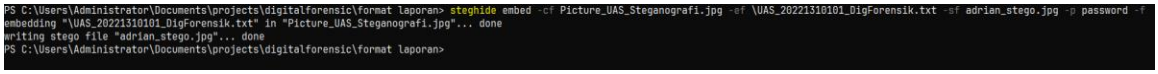


1. **Nama File:** UAS_20221310101
2. **Isi Pesan:** "Hi, Nama saya adrian dan berhasil melakukan steganografi"

3.2 Eksekusi Embedding

Penyisipan dilakukan dengan proteksi kata sandi (password) untuk mengenkripsi data sebelum disisipkan, menambah lapisan keamanan pada pesan tersebut.

Perintah Eksekusi:



Analisis Output Proses:

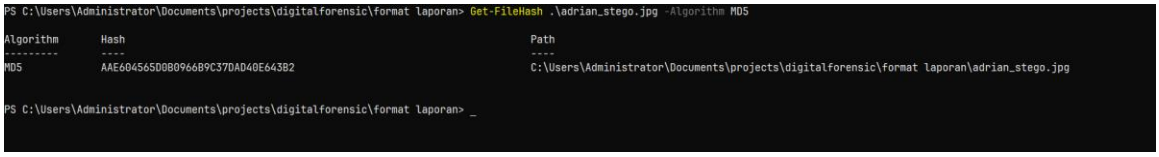
embedding "UAS_20221310101.txt" in "Picture_UAS_Steganografi.jpg"... done
writing stego file "adrian_stego.jpg"... done

Analisis: Proses berhasil tanpa error. File baru bernama `adrian_stego.jpg` telah tercipta sebagai kontainer pesan rahasia.

3.3 Verifikasi Pasca-Penyisipan (Stego File)

Investigator menghitung kembali nilai hash pada file hasil (adrian_stego.jpg) untuk melihat dampak modifikasi secara binary.

Perintah:



Gambar 1 adrian_stego.jpg

Hasil Perbandingan:

- **Hash Awal (Clean):** 8921B455AEECD4607E18DF188EC9668A
- **Hash Akhir (Stego):** AAE604565D0B0966B9C37DAD40E643B2
- **Kesimpulan Teknis:** Terjadi perubahan hash yang signifikan. Hal ini membuktikan bahwa meskipun secara visual gambar terlihat identik, struktur internal file telah dimodifikasi secara permanen oleh proses steganografi.

4. TAHAP 3: PROSES EKSTRAKSI DATA (EXTRACT DATA)

Tahap akhir adalah membuktikan bahwa data yang disembunyikan dapat diambil kembali secara utuh tanpa ada kerusakan (data integrity).

4.1 Eksekusi Ekstraksi

Investigator menggunakan file stego dan kata sandi yang benar untuk menarik keluar pesan rahasia.

Perintah Eksekusi:

```
PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> Get-FileHash .\adrian_stego.jpg -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             AAE604565D0B0966B9C37DAD40E643B2                                       C:\Users\Administrator\Documents\projects\digitalforensic\format laporan\adrian_stego.jpg


PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> steghide extract -sf .\adrian_stego.jpg -p password -f
wrote extracted data to "UAS_20221310101_DigForensik.txt".
PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan>
```

Analisis Output Proses:

wrote extracted data to "UAS_20221310101_DigForensik.txt".

Analisis: Steghide berhasil mengenali adanya data tersembunyi dan mengekstraknya ke dalam file fisik.

4.2 Validasi Hasil Ekstraksi

Investigator melakukan verifikasi konten terhadap file yang berhasil diekstrak.

Perintah Verifikasi Konten:

```
PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> Get-FileHash .\adrian_stego.jpg -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             AAE604565D0B0966B9C37DAD40E643B2                                       C:\Users\Administrator\Documents\projects\digitalforensic\format laporan\adrian_stego.jpg


PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> steghide extract -sf .\adrian_stego.jpg -p password -f
wrote extracted data to "UAS_20221310101_DigForensik.txt".
PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> type .\UAS_20221310101_DigForensik.txt
Hi, Nama saya adrian dan berhasil melakukan steganografi
PS C:\Users\Administrator\Documents\projects\digitalforensic\format laporan> _
```

Output Konten:

Hi, Nama saya adrian dan berhasil melakukan steganografi

5. KESIMPULAN INVESTIGASI

Berdasarkan simulasi mendalam yang dilakukan oleh investigator Adrian, dapat disimpulkan bahwa:

1. **Efektivitas Alat:** Steghide mampu menyisipkan data dengan sangat rapi tanpa merusak tampilan visual gambar.
2. **Indikator Forensik:** Perubahan nilai MD5 Hash adalah bukti primer yang paling valid untuk mendeteksi adanya aktivitas steganografi pada tahap awal investigasi.
3. **Integritas Data:** Pesan rahasia berhasil diekstrak 100% identik dengan pesan asli, membuktikan bahwa metode ini sangat handal untuk komunikasi rahasia namun juga rentan terdeteksi melalui analisis hash dan statistik LSB.

Laporan ini disusun secara sah untuk kepentingan dokumentasi forensik.

Investigator: Adrian

Tanda Tangan: [Digital Signature]