

# LAPORAN ANALISIS FORENSIK DIGITAL

## Kasus: Analisis File Tersembunyi

Tanggal: [19 06 2025]

---

### NO.1

#### Studi Kasus

Investigasi dilakukan terhadap dugaan pencurian data rahasia perusahaan. Dalam proses analisis, ditemukan file yang dicurigai disembunyikan dengan mengubah ekstensi dan mengompresinya berlapis-lapis.

---

#### Langkah-langkah Analisis

##### 1. Menambahkan Data Sumber:

- File image .E01 ditambahkan ke Autopsy menggunakan fitur "Add Data Source".
- Opsi host: *Generate new host name based on data source name.*

##### 2. Menelusuri File Tersembunyi:

- Di bagian File Views > File Types > Archives ditemukan file:
  - myfilegzip.txt.gz
  - myfilegzip2.txt.gz.0.gz (mencurigakan)
  - myfile.zip, myfile22.zip, dll.

##### 3. Metadata File:

- Created Time: 2011-02-02 15:09:51 WIB
- Modified Time: 2011-02-02 15:09:50 WIB
- Access Time: 2011-02-02 00:00:00 WIB

##### 4. Isi File:

- Dari tab Hex Viewer terlihat isi awal file mengandung nama "myfilegzip2.txt" yang menunjukkan file ini adalah file teks.

##### 5. Ekstraksi File:

- Percobaan ekstraksi gagal dengan pesan:  
*Error 0x8096002A: No error description available*

## Kesimpulan

File myfilegzip2.txt.gz.0.gz terindikasi merupakan file teks yang telah dikompresi dua kali untuk menyembunyikan isinya. File tidak dapat dibuka langsung di Autopsy dan perlu diekstrak menggunakan tools eksternal seperti 7-Zip atau perintah gunzip di Linux.

## Screenshot yang Disarankan untuk Dilampirkan

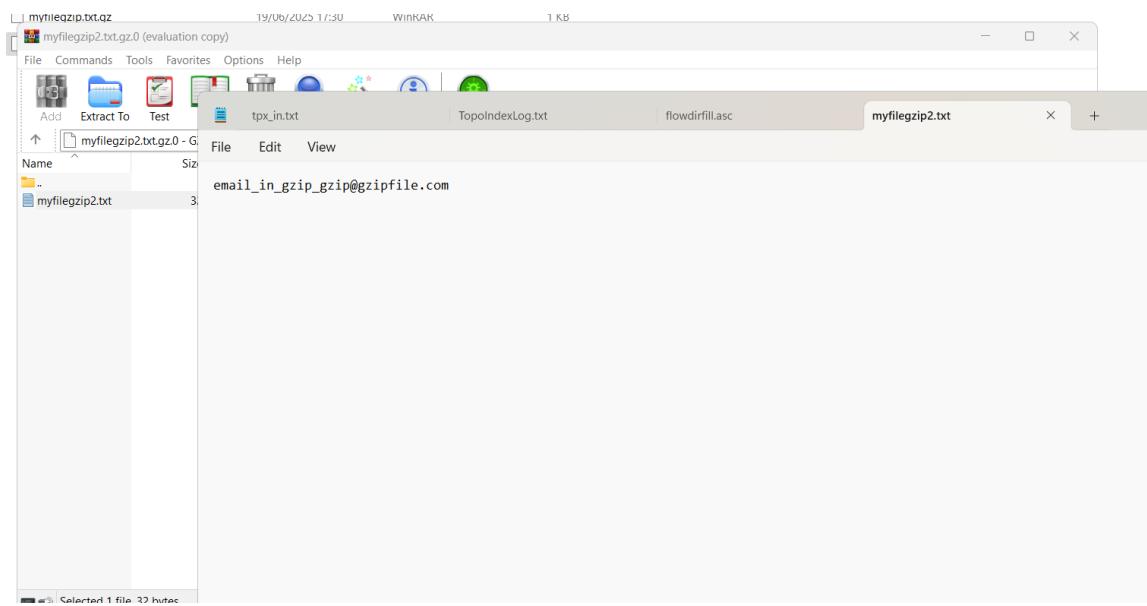
### No Screenshot

The screenshot shows the Autopsy 4.22.1 interface with the following details:

- Case View:** Analysis\_File\_Tersembunyi - Autopsy 4.22.1
- File Sources:** Data Sources, File Views, File Types (Images (3), Videos (0), Audio (0), Archives (5), Databases (0), Documents, Executable), By Extension, By MIME Type (application, image, multipart, text), Deleted Files, File Size, Data Artifacts (Metadata (19)), Analysis Results (Keyword Hits (32), OS Accounts), Tags, Score, Reports.
- Table View:** Shows a list of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, and Size. The highlighted row is 'myfilegzip2.txt.gz.0.gz' with a size of 104 bytes.
- Hex Editor View:** Shows the raw hex dump of the file, starting with 0x00000000: 1F 8B 08 08 05 5B DB 4C 02 03 6D 79 66 69 6C 65 followed by several lines of binary data.

## N o Screenshot

2



---

### Soal 2: Investigasi Aktivitas Internet

#### Deskripsi Kasus:

Dilakukan analisis forensik terhadap sebuah image disk tersangka kasus cyberbullying.

Tujuannya untuk mengidentifikasi aktivitas internet berupa situs web yang dikunjungi, pesan email atau chat, serta membuat timeline aktivitas digital tersangka.

#### Tujuan Investigasi:

- Mengekstrak riwayat browsing dari web browser
  - Mencari dan menganalisis data komunikasi (email, pesan sosial media)
  - Membuat timeline aktivitas internet untuk periode waktu tertentu
- 

### ⌚ Tahapan Investigasi & Temuan

#### 1. Membuka Autopsy dan Memuat Bukti

Langkah:

- Buka Autopsy
- Pilih Open Recent Case atau buat kasus baru (misalnya: cyberbullying\_case)
- Tambahkan Data Source (image file, contoh: nps-2010-emails.E01)

Screenshot yang perlu disertakan:

- Proses Add Data Source dan nama file yang dimuat
- 2. Mengekstrak Data Komunikasi – Email  
Langkah:
  - Buka Analysis Results → Keyword Hits → Email Addresses
  - Ditemukan 32 alamat email
  - Periksa isi email jika tersedia

Screenshot yang perlu disertakan:

- Tampilan daftar Email Addresses
- Isi email atau metadata email (jika ada)

Analisis:

Jumlah alamat email yang ditemukan menunjukkan aktivitas komunikasi tersangka. Jika isi email terkait dengan ancaman, hinaan, atau aktivitas bullying, maka itu dapat dijadikan bukti kuat.

### 3. Pencarian Kata Kunci – Keyword Search

Langkah:

- Di Analysis Results → Keyword Hits
- Cari kata: facebook, message, bully, gmail, chat
- Periksa file yang mengandung kata kunci tersebut

Screenshot yang perlu disertakan:

- Tampilan hasil pencarian Keyword Hits yang relevan

Analisis:

Keyword seperti “bully” atau “message” menunjukkan konteks komunikasi yang perlu diperiksa lebih lanjut.

### 4. Timeline Aktivitas Digital

Langkah:

- Klik tab Timeline di bagian atas
- Pilih rentang waktu (misalnya 1 Januari – 31 Januari 2011)
- Lihat aktivitas file, sistem, email, atau web

Screenshot yang perlu disertakan:

- Tampilan timeline aktivitas tersangka

#### Analisis:

Timeline memperlihatkan kapan file dibuka, email dikirim, atau situs dikunjungi. Ini membantu menentukan kapan cyberbullying terjadi.

#### 5. (Opsiional) Web History & Downloads

Langkah:

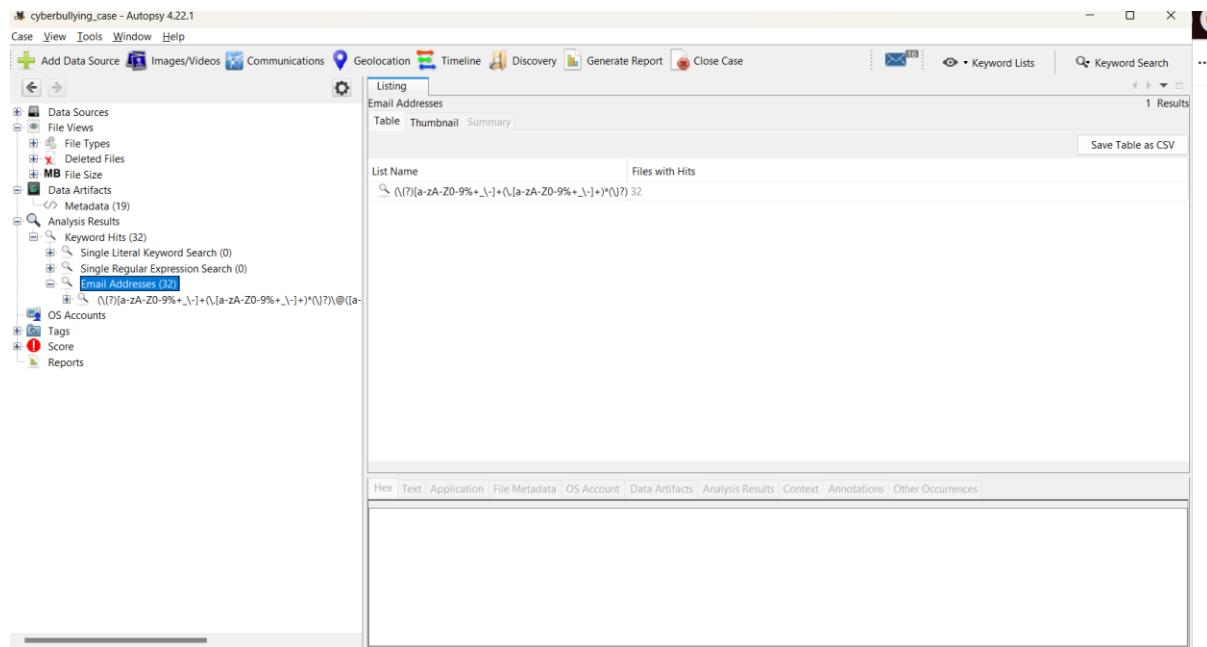
- Cek Analysis Results → Web History
  - Jika kosong, cek Extracted Content → Web Downloads
  - Periksa file yang diunduh atau artefak yang tersimpan
- 



#### Kesimpulan Sementara:

- Autopsy berhasil mengidentifikasi 32 alamat email.
- Hasil pencarian kata kunci menunjukkan potensi aktivitas cyberbullying.
- Timeline menunjukkan kapan aktivitas penting terjadi.
- Jika tidak ditemukan riwayat browsing atau isi pesan, maka kemungkinan tersangka menghapus artefak atau menggunakan metode komunikasi lain.

#### Screenshot



Screenshot of the Autopsy 4.22.1 interface showing the 'Listing' tab of the 'Analysis Results' section. The search query is `(\?)([a-zA-Z0-9%+\.\-]+)([a-zA-Z0-9%+\.\-]+)*(\?)(@[a-zA-Z0-9](\[-A-Z0-9\]*[a-zA-Z0-9])?)`. The results table shows 25 hits across various file types and names.

List Name	Files with Hits
ages_comment@iwork09.com (1)	1
doc_within_doc@document.com (2)	2
docx_within_docx@document.com (3)	3
email_in_gzip@gzipfile.com (1)	1
email_in_gzip_gzip@gzipfile.com (1)	1
email_in_zip@zipfile1.com (1)	1
email_in_zip@zipfile2.com (1)	1
keynote@iwork09.com (1)	1
keynote_comment@iwork09.com (1)	1
numbers@iwork09.com (1)	1
numbers_comment@iwork09.com (1)	1
plain_text@TextEdit.com (1)	1
plain_text_pdf@TextEdit.com (1)	1
plain_utf16@TextEdit.com (1)	1
plain_utf16_pdf@TextEdit.com (1)	1
ppt_within_doc@document.com (1)	1
ppx_within_docx@document.com (2)	2
rtf_text@TextEdit.com (1)	1
rtf_text_pdf@TextEdit.com (1)	1
user_doc@microsoftword.com (1)	1
user_doc_pdf@microsoftword.com (1)	1
user_docx@microsoftword.com (1)	1
user_docx_pdf@microsoftword.com (1)	1
xls_within_doc@document.com (2)	2
xlsx_within_docx@document.com (3)	3

Screenshot of the 'Add Data Source' wizard. Step 5: Add Data Source. The message indicates the data source has been added and files are being analyzed.

Steps:

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Ingest
- Add Data Source

Add Data Source

Data source has been added to the local database. Files are being analyzed.

< Back      Next >      Finish      Cancel      Help

Ub/19/25 17:52:04 WIB No known file search will not be e