

# Forensia - autopsy

Alumno: Anibal Giordani

## Ejercicio Guiado: Análisis Forense con Autopsy

En este ejercicio, los alumnos aprenderán a utilizar **Autopsy**, una herramienta de análisis forense digital. El objetivo es analizar una imagen de disco en busca de **archivos eliminados, metadatos y posibles evidencias ocultas**.

---

### Requisitos Previos

- ✓ Descargar e instalar **Autopsy** en el PC. Puedes obtenerlo desde <https://www.autopsy.com/download/>
  - ✓ Descargar una imagen de disco forense de prueba. Puedes usar imágenes públicas como las de **Digital Corpora** (<https://digitalcorpora.org>).
  - ✓ Conocimientos básicos de sistemas de archivos y recuperación de datos.
- 

### Pasos del Ejercicio

#### 1 Crear un Nuevo Caso

1. Abre **Autopsy** y selecciona "Create New Case".
  2. Introduce un **nombre para el caso** y elige una carpeta donde se almacenará la información.
  3. Haz clic en **"Next"** y selecciona **"Add Data Source"**.
- 

#### 2 Cargar una Imagen de Disco

1. Selecciona **"Disk Image or VM File"** y carga la imagen descargada previamente.
2. Elige los tipos de análisis que quieres realizar (archivos eliminados, historial del navegador, metadatos, etc.).
3. Inicia el análisis y espera a que finalice el proceso.

## 2009 M57-Jean

The M57-Jean scenario is a single disk image scenario involving the exfiltration of corporate documents from the laptop of a senior executive. The scenario involves a small start-up company, M57.Biz. A few weeks into inception a confidential spreadsheet that contains the names and salaries of the company's key employees was found posted to the "comments" section of one of the firm's competitors. The spreadsheet only existed on one of M57's officers, Jean.

Jean says that she has no idea how the data left her laptop and that she must have been hacked.

You have been given a disk image of Jean's laptop. Your job is to figure out how the data was stolen, or if Jean isn't as innocent as she claims.

**Note: Solutions to this problem have been widely distributed on the Internet, so this assignment should only be used for self-study, and not for academic credit.**

Materials:

- Jean's disk in EnCase E01 format:
  - [nps-2008-jean.E01](#)
  - [nps-2008-jean.E02](#)

(Note: nps-2008-jean is a multi-volume Expert Witness file. You need to download both of the files and put them in the same directory, or else you will not be able to process the disk image.)

- Exercise Slides:
  - [M57-Jean.ppt](#) (Microsoft PowerPoint format)
  - [M57-Jean.key](#) (Apple keynote format)
  - [M57-Jean.pdf](#) (Adobe Acrobat format)

Many students have had problems accessing these files with Autopsy. There is nothing wrong with these files or with Autopsy. Students: If you are having problems, you need to speak with your professor.

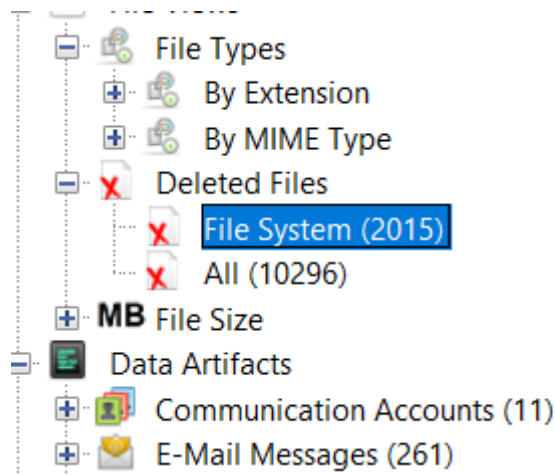
Solutions:

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays a tree view of data sources, including 'Data Sources', 'File Views', 'Data Artifacts', 'Analysis Results', and 'OS Accounts'. The main window is titled 'Run Programs' and shows a table with columns: Source Name, S, C, O, Program Name, Path, Date/Time, Count, and Comments. The table lists various programs and their execution details. The status bar at the bottom indicates 'Analyzing files from nps-2008-jean.E01' with a progress bar at 100%.


Source Name	S	C	O	Program Name	Path	Date/Time	Count	Comments
AGENTSVC.EXE-002E45AB.pf				AGENTSVC.EXE	/WINDOWS/MSAGENT	2008-07-20 02:00:04 CEST	2	Prefetch I
AIM6.EXE-34DC5725.pf				AIM6.EXE	/PROGRAM FILES/AIM6	2008-07-21 03:30:35 CEST	7	Prefetch I
AIMINST.EXE-3391E991.pf				AIMINST.EXE	/DOCUME~1/JEAN/LOCALS~1/TEMP/AIM_68~1.1	2008-07-18 06:29:09 CEST	2	Prefetch I
AIMLANG.EXE-076D401C.pf				AIMLANG.EXE	/DOCUME~1/JEAN/LOCALS~1/TEMP/AIM_68~1.1	2008-07-18 06:29:14 CEST	2	Prefetch I
AIMTUNES.EXE-07EAB0C7.pf				AIMTUNES.EXE	/DOCUMENTS AND SETTINGS/ALL USERS/APPLICATIO...	2008-07-18 06:30:43 CEST	1	Prefetch I
ALSETUP.EXE-38283348.pf				ALSETUP.EXE	/DOCUME~1/JEAN/LOCALS~1/TEMP/AIM_68~1.1	2008-07-18 06:28:48 CEST	1	Prefetch I
AMOS.EXE-219E8DD6.pf				AMOS.EXE	/DOCUME~1/JEAN/LOCALS~1/TEMP/AIM_68~1.1	2008-07-18 06:29:17 CEST	2	Prefetch I
AOLDLMGR.EXE-2D3BD87E.pf				AOLDLMGR.EXE	/DOCUME~1/JEAN/LOCALS~1/TEMP/AIM_68.10.1	2008-07-18 06:30:52 CEST	2	Prefetch I
AOLSOFTWARE.EXE-11870E32.pf				AOLSOFTWARE.EXE	/PROGRAM FILES/AIM6	2008-07-21 03:30:37 CEST	10	Prefetch I
AOLTSERVER.EXE-1584CCF8.pf				AOLTSERVER.EXE	/PROGRAM FILES/AOL/AIM TOOLBAR 5.0	2008-07-20 01:59:25 CEST	3	Prefetch I
CMD.EXE-087B4001.pf				CMD.EXE	/WINDOWS/SYSTEM32	2008-07-19 05:13:13 CEST	11	Prefetch I
CONTROL.EXE-1C26180C.pf				CONTROL.EXE	/WINDOWS/SYSTEM32	2008-07-12 23:16:08 CEST	8	Prefetch I
CSCRIPT.EXE-1C26180C.pf				CSCRIPT.EXE	/WINDOWS/SYSTEM32	2008-06-07 07:06:48 CEST	1	Prefetch I
CSRSS.EXE-12863473.pf				CSRSS.EXE	/WINDOWS/SYSTEM32	2008-07-12 23:15:50 CEST	5	Prefetch I
DEFRAG.EXE-273F131E.pf				DEFRAG.EXE	/WINDOWS/SYSTEM32	2008-07-20 21:43:27 CEST	5	Prefetch I
DFRGNTFS.EXE-269967DF.pf				DFRGNTFS.EXE	/WINDOWS/SYSTEM32	2008-07-20 21:43:28 CEST	5	Prefetch I
EQQTTRANS.EXE-169A1388.pf				EQQTTRANS.EXE	/PROGRAM FILES/TENCENT/QQ GAMES/QQ BUBBLE A...	2008-07-18 06:57:55 CEST	1	Prefetch I

### 3 Buscar Archivos Eliminados

- En la pestaña "File Analysis", navega por las carpetas y busca archivos eliminados.



2. Filtra por **archivos recuperables** y revisa si hay información relevante.


 **Pregunta:** ¿Cuántos archivos eliminados ha recuperado Autopsy? ¿Puedes identificar algún archivo sospechoso?

Se encontraron 2015 archivos eliminados. Hasta el momento, no se identificaron archivos con nombres, extensiones o contenidos claramente sospechosos.

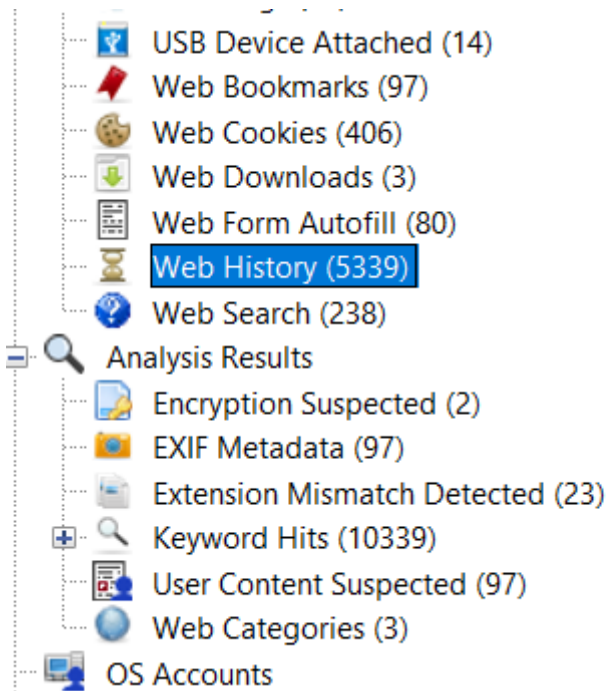
---

#### **4 Analizar el Historial del Navegador**

1. Ve a la pestaña "**Web Artifacts**".
2. Revisa el historial de navegación, cookies y descargas.

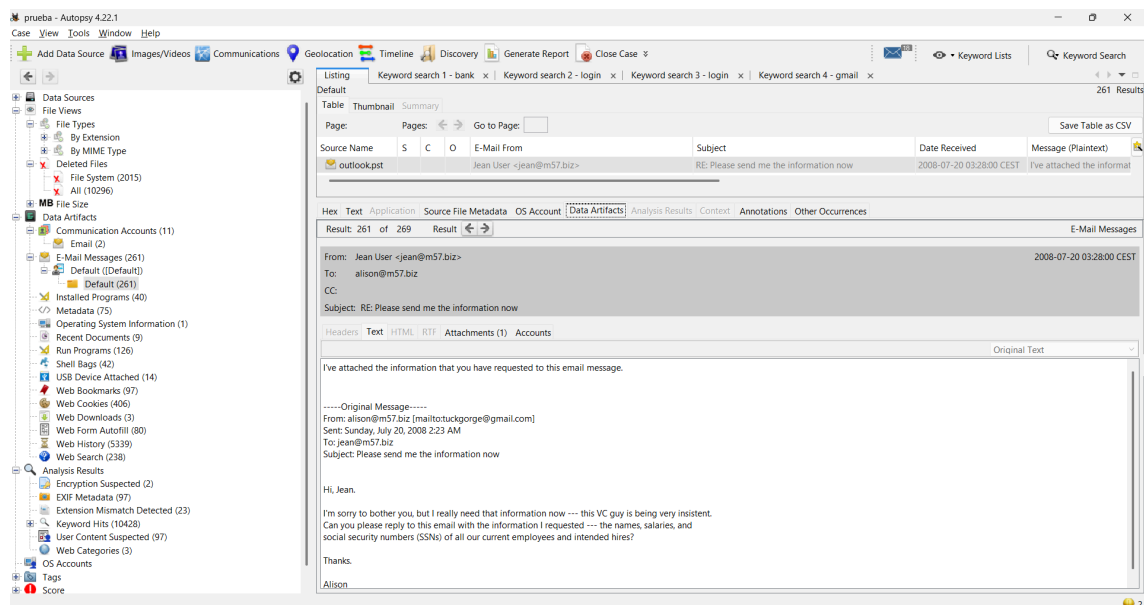
 **Pregunta:** ¿Puedes identificar alguna página web sospechosa visitada desde el dispositivo?

Se accedió a la sección "**Web Artifacts > Web History**" dentro de Autopsy, donde se identificaron un total de **5.339 entradas de historial web**.



Se analizaron 261 correos electrónicos detectados. Se identificaron varios mensajes con archivos adjuntos. Se aplicaron filtros para detectar posibles archivos adjuntos

Se identificaron múltiples correos electrónicos con contenido sensible. En particular, uno enviado por *Jean User* contenía un archivo adjunto y hacía referencia explícita a información confidencial de empleados, como nombres, salarios y SSNs. Esto podría ser evidencia directa de exfiltración de datos corporativos.



## Detalles del correo encontrado

- Remitente: Jean User <jean@m57.biz>

- **Destinatario:** alison@m57.biz
- **Asunto:** "RE: Please send me the information now"
- **Fecha:** 20 de julio de 2008, 03:28
- **Contenido:**

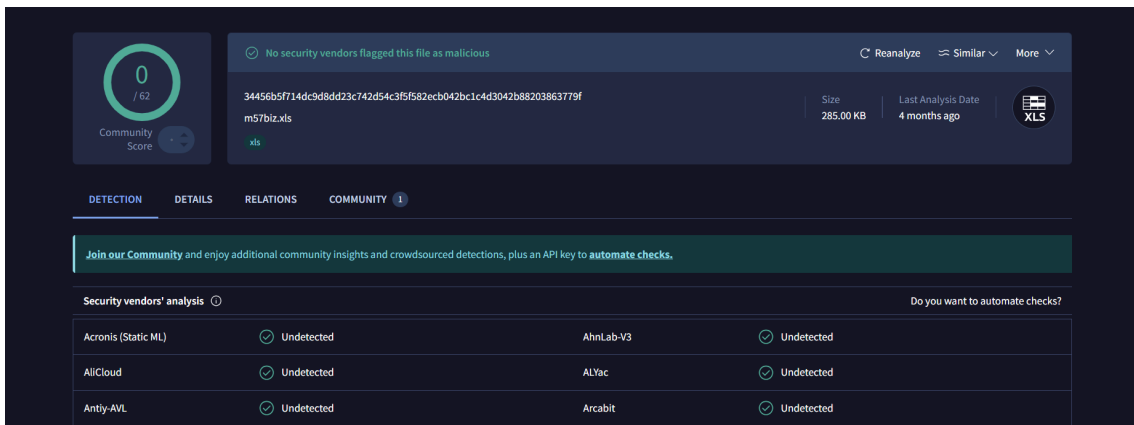
*"I've attached the information that you have requested to this email message."*

El mensaje original incluía una solicitud explícita de:

- Nombres, salarios y números de seguridad social (SSN) de todos los empleados actuales y futuros.

- **Pestaña “Attachments”:** figura un adjunto,

Se extrajo el archivo adjunto, se analizó con virus total, y se abrió con m365.cloud.microsoft/



The screenshot shows the VirusTotal analysis interface for a file named 'm57biz.xls'. The file's SHA-256 hash is 34456b5f714dc9d8d23c742d54c3f5f582ecb042bc1c4d3042b88203863779f. The file size is 285.00 KB and it was last analyzed 4 months ago. The community score is 0/62. A message states: 'No security vendors flagged this file as malicious'. Below this, there is a table showing the results of security vendors' analysis, all of which are 'Undetected'.

Security vendors' analysis			
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected

	A	B	C	D	E	F	G	H
1	M57.biz company							
2								
3								
4								
5								
6					SSN (for background check)			
	Name		Position	Salary				
7	Alison	Smith	President	\$140,000	103-44-3134			
8	Jean	Jones	CFO	\$120,000	432-34-6432			
9								
10	Programmers:							
11	Bob	Blackman	Apps 1	90,000	493-46-3329			
12	Carol	Canfred	Apps 2	110,000	894-33-4560			
13	Dave	Daubert	Q&A	67,000	331-95-1020			
14	Emmy	Arlington	Entry Level	57,000	404-98-4079			
15								
16	Marketing							
17	Gina	Tangers	Creative 1	80,000	980-97-3311			
18	Harris	Jenkins	G & C	105,000	887-33-5532			
19								
20	BizDev							
21	Indy	Counterchng	Outreach	240,000	123-45-6789			
22								
23								
24								
25	Annual Salaries			\$1,009,000				
26	Benefits			30% \$302,700				
27								
28	Total Salaries + Benefits			\$1,311,700				
29	Monthly burn			*****				
30								
31								
32								
33								
34								
35								
36								
37								
38								
39								
40								
41								
42								



## Contenido encontrado en el archivo Excel:

Campo	Detalles
Empresa	M57.biz
Datos personales	Nombres y Apellidos de empleados
Información laboral	Puestos, áreas, y salarios anuales

Datos sensibles	Números de Seguro Social (SSN) — información crítica
Análisis económico	Beneficios del 30% y costos totales de RRHH
Elemento extraño	Imagen de soldados con bandera de EE.UU.


### Hallazgos relevantes:

- El archivo contiene **información confidencial** de empleados clave, que **no debería estar en un documento sin protección**.
- El campo SSN puede usarse para **suplantación de identidad**.
- El mensaje en el email de Alison sugería que Jean compartió el archivo.

---

#### 5 Examinar las Cadenas de Texto (Strings)

1. Abre la pestaña **"Extracted Content"** y busca **cadenas de texto** dentro de los archivos.
2. Utiliza la barra de búsqueda para encontrar palabras clave como "password", "confidential" o "bank".

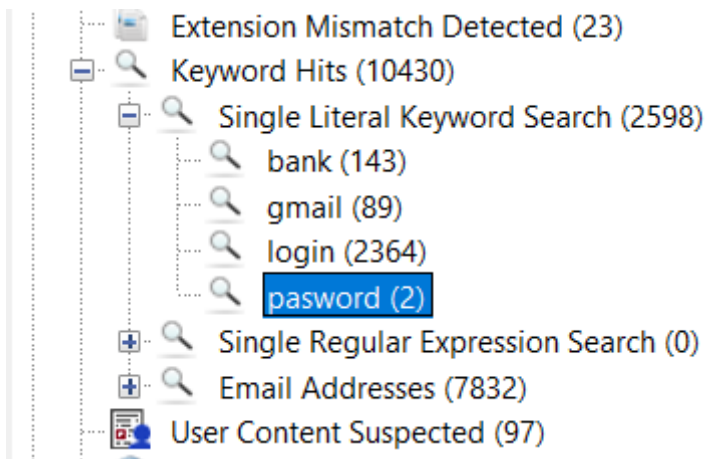
 **Pregunta:** ¿Se encontraron palabras clave sensibles? ¿Cómo podrían ser utilizadas en una investigación?

Palabras clave encontradas:

- "password": 2 coincidencias
- "login": 2364 coincidencias
- "gmail": 89 coincidencias
- "bank": 143 coincidencias

Estas cadenas se hallaron en archivos indexados y registros de formularios web.

Estas palabras podrían indicar actividad relacionada con accesos a cuentas, correos electrónicos o incluso intentos de login en servicios bancarios o plataformas sensibles.



## 6 Generar un Informe

1. Ve a **"Generate Report"** y selecciona **HTML o PDF**.
2. Guarda el informe y revisa los hallazgos principales.

Report Navigation

- Case Summary
- Accounts: Email (11)
- Data Source Usage (1)
- E-Mail Messages (261)
- EXIF Metadata (97)
- Encryption Suspected (2)
- Extension Mismatch Detected (23)
- Installed Programs (40)
- Keyword Hits (10430)
- Metadata (75)
- Operating System Information (1)
- Recent Documents (9)
- Run Programs (126)
- Shell Bags (42)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

### Autopsy Forensic Report

HTML Report Generated on 2025/02/21 12:33:20

Case: prueba  
Number of data sources in case: 1

**Image Information:**

nps-2008-jean.E01

Timezone: Europe/Madrid  
Path: C:\Users\aniba\Desktop\ciber\autopsy\imagen\nps-2008-jean.E01  
Path: C:\Users\aniba\Desktop\ciber\autopsy\imagen\nps-2008-jean.E02

**Software Information:**

Autopsy Version: 4.22.1  
Android Analyzer Module: 4.22.1  
Android Analyzer (aLEAPP) Module: 4.22.1

**Pregunta Final:** Basado en el análisis, ¿qué conclusiones puedes sacar sobre la imagen de disco examinada?

## Conclusiones del Análisis Forense

La imagen de disco examinada (caso *M57-Jean*) contiene múltiples indicios de una posible filtración de datos sensibles desde el equipo de la ejecutiva Jean. Los hallazgos más relevantes incluyen:

**Archivos eliminados:** Se recuperaron **2015 archivos eliminados**, lo cual puede indicar intentos de ocultamiento de evidencia.



**Correos electrónicos:** Se identificó un correo electrónico con un archivo adjunto que contiene nombres, salarios y números de seguridad social de empleados. Este correo fue enviado desde la cuenta de Jean a un tercero, lo que contradice su declaración de desconocimiento.

**Historial web:** El equipo accedió a numerosos servicios web, incluidos sitios de correo electrónico como Gmail, lo cual podría estar relacionado con la exfiltración de datos.

**Cadenas sensibles:** Se encontraron palabras clave como password, login y bank, lo que podría evidenciar el almacenamiento o uso de credenciales y servicios financieros desde el equipo.

**Metadatos y programas instalados:** No se detectaron herramientas de eliminación segura, pero sí uso frecuente de aplicaciones de ofimática y navegación.

## Conclusión General:

Toda la evidencia apunta a que el archivo confidencial fue accedido y enviado desde el equipo de Jean. Si bien no se hallaron indicios de malware, el comportamiento registrado en el sistema sugiere una **filtración de datos intencional o con negligencia grave** desde su estación de trabajo.

---

## Objetivo del Ejercicio

- 🔍 Aprender a manejar **Autopsy** para recuperar archivos, analizar historial de navegación y extraer metadatos.
- 🔍 Comprender cómo se realiza un **análisis forense digital** en dispositivos de almacenamiento.