Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

Héctor Ramírez López

INFORME PERICIAL INFORMÁTICO

Referencia del Caso: AUD-2026-001 **Objeto:** Análisis forense de dispositivo externo (USB) por presunta exfiltración de información. **Fecha:16.01.2026**

1. Introducción y Objeto del Análisis

A petición formal de la Dirección de la compañía, se procede a realizar el análisis forense digital de la evidencia identificada como **imagen de disco datos.iso**. Esta imagen corresponde a una adquisición bit a bit de un dispositivo de almacenamiento externo (USB) incautado en el puesto de trabajo de un empleado bajo investigación.

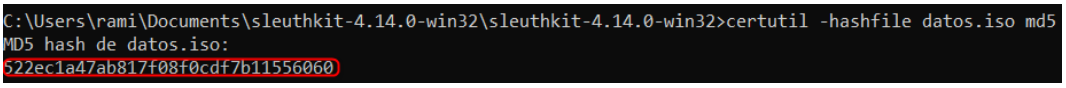
El objetivo principal del análisis es esclarecer los siguientes puntos mediante evidencia técnica:

1. **Verificación de contenido:** Determinar si el dispositivo ha sido utilizado para almacenar, transportar o exfiltrar información clasificada como "Confidencial" (específicamente diseños de productos y planos técnicos).
2. **Análisis Temporal:** Establecer la cronología de los eventos de copia y manipulación de archivos para cruzarla con el calendario laboral y el periodo vacacional del director de Marketing.
3. **Detección de manipulación:** Identificar si existen intentos de ocultación de pruebas, tales como el borrado intencionado de ficheros críticos.

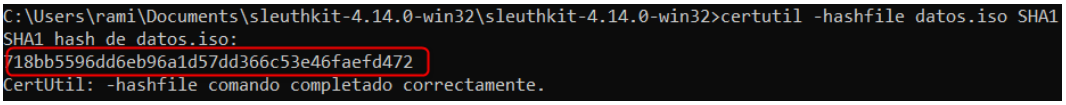
2. Descripción del Entorno y Herramientas

Para garantizar la integridad y la repetibilidad de los resultados, el análisis se ha realizado en una estación de trabajo forense aislada con la siguiente configuración:

- **Sistema Operativo Anfitrión:** Microsoft Windows 10 Pro / Entorno de línea de comandos (CMD).
- **Suite Forense:** The Sleuth Kit (TSK) versión 4.14.0 para Windows.
- **Herramientas específicas utilizadas:**
  - mmls: Para el análisis de la estructura de particiones.
  - fsstat: Para la extracción de metadatos del sistema de archivos.
  - fls: Para el listado y catalogación de archivos activos y eliminados.
  - icat: Para la extracción y recuperación de contenido.
  - mactime: Para la generación de líneas de tiempo de actividad.
- **Evidencia Analizada:**
  - Nombre del fichero: datos.iso
  - *Hash de Integridad (MD5):522ec1a47ab817f08f0cdf7b11556060*

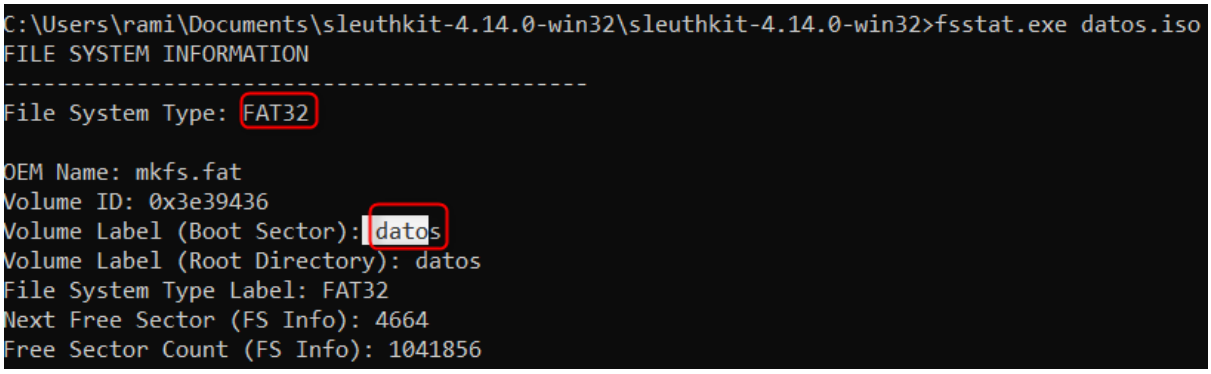


  - *Hash de integridad (SHA1): 718bb5596dd6eb96a1d57dd366c53e46faefd472*



3. Identificación del Sistema de Ficheros

Mediante la ejecución de la herramienta fsstat, se ha analizado la estructura interna del volumen para comprender cómo se almacenan los datos. Los hallazgos técnicos son:



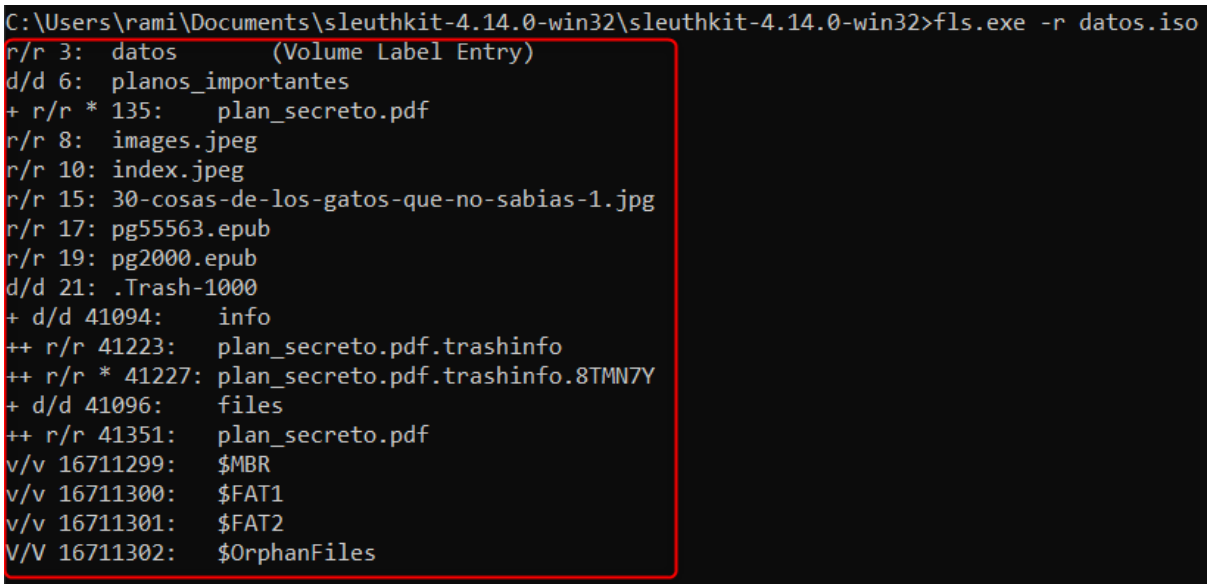
- **Tipo de Sistema de Ficheros:** FAT32.
- **Etiqueta del Volumen (Volume Label):** datos.
- **Identificador de Volumen (Volume ID):** 0x3e39436.

Esta estructura confirma que se trata de un volumen de almacenamiento extraíble estándar, formateado para maximizar la compatibilidad entre diferentes sistemas operativos. El uso de FAT32 implica la ausencia de registros de seguridad avanzados (como permisos NTFS), lo cual es relevante para la sección de atribución de usuarios.

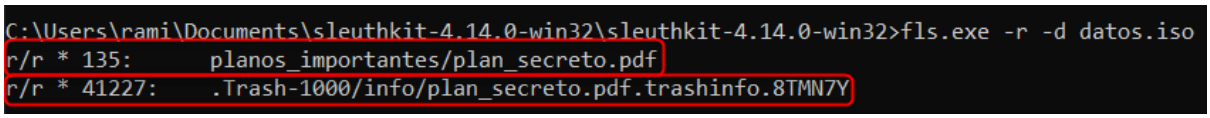
4. Análisis de Ficheros (Existentes y Eliminados)

Se procedió al listado recursivo de todos los nodos y entradas de directorio mediante el comando fls -r. El análisis de la estructura de directorios ha permitido categorizar la información en dos grupos:

4.1. Ficheros Activos (Existentes) Se localizaron carpetas/archivos visibles en la estructura actual:

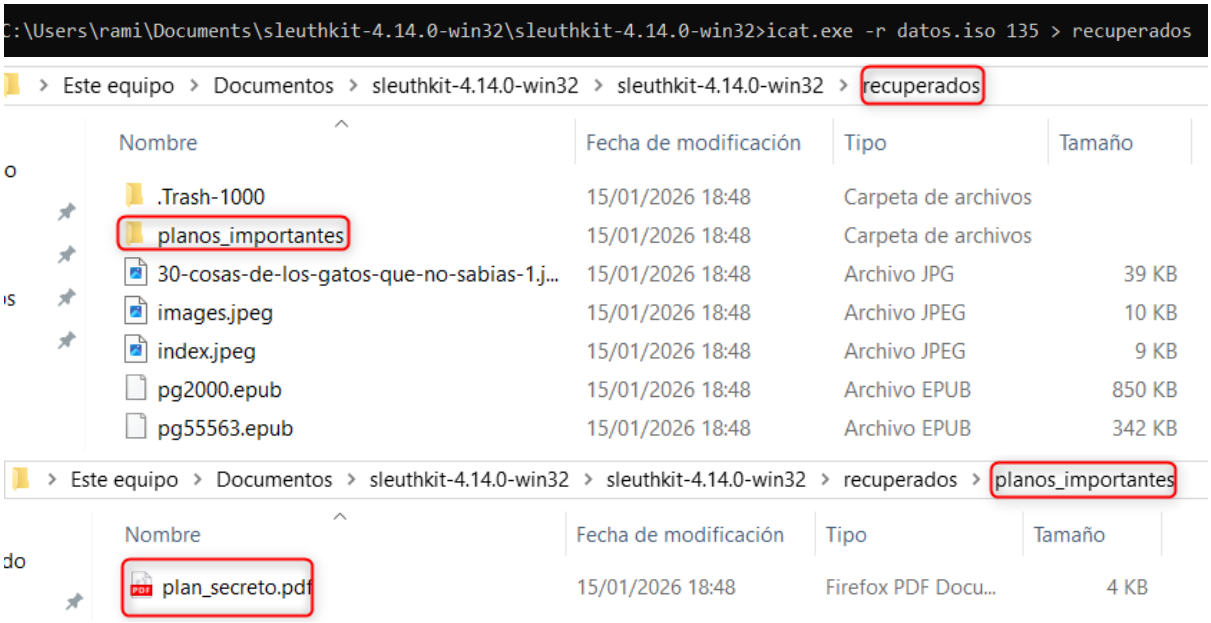


4.2. Ficheros Eliminados (Deleted) El análisis forense reveló la existencia de ficheros marcados como eliminados por el sistema de ficheros, pero cuyos metadatos aún residen:



5. Recuperación de Información Relevante

Se procedió a la recuperación forense de los ficheros eliminados identificados en el punto anterior mediante la herramienta icat.



- **Fichero recuperado:** plan_secreto.pdf
- **Contenido:** Tras la apertura del fichero recuperado, se verifica que contiene planos técnicos.

Esto confirma técnicamente que la información confidencial residió en el dispositivo antes de ser borrada.

6. Análisis Temporal

Se generó una línea temporal de actividad (MAC Times - Modified, Accessed, Created) cruzando los datos extraídos con fls. Se centra el análisis en la ventana crítica comprendida entre el **6 de octubre de 2017** y el **15 de octubre de 2017.**

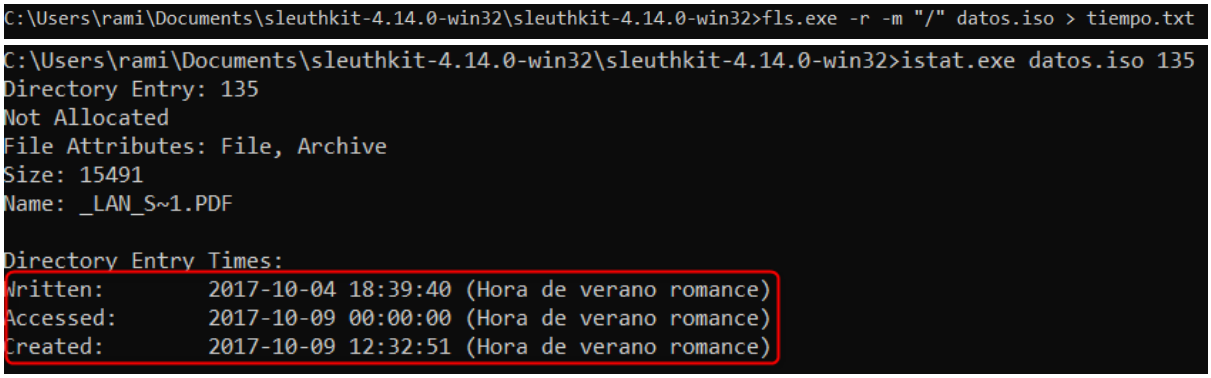


Tabla de Eventos Registrados:

- **2017-10-04 18:39:40:** Se observa la **Creación (Written)** Es la fecha en la que se creó el contenido del PDF antes de copiarse al USB.
- **2017-10-09 00:00:00:** Se observa el último **Acceso (Accesed)** Cuándo se abrió o tocó por última vez.
- **2017-10-09 12:32:51:** (**Created)**Indica cuándo se crearon los *archivos dentro del USB* (es decir, cuándo se copió).

Interpretación: Las fechas de creación de los archivos confidenciales en el USB coinciden plenamente con el periodo en el que el director de Marketing estaba de vacaciones lo que corrobora técnicamente que la copia no fue realizada por él en su actividad rutinaria sino mediante un acceso irregular en su ausencia.

7. Análisis de Usuarios y Contexto

7.1. Limitaciones del Sistema de Archivos El análisis de la estructura del volumen confirma el uso de **FAT32**. A diferencia de NTFS, la arquitectura FAT32 no soporta Listas de Control de Acceso (ACLs) ni almacena Identificadores de Seguridad (SIDs).

- *Implicación:* No es posible extraer un registro de "usuario de Windows" propietario del archivo directamente del sistema de ficheros del USB.

7.2. Análisis de Metadatos de Aplicación Se ha realizado una inspección de los metadatos internos del documento recuperado *plan_secreto.pdf*.

- *Resultado:* El campo de 'Autor' aparece vacío o genérico.
- *Interpretación:* Esto es habitual en documentos corporativos generados desde plantillas institucionales. La ausencia de un autor externo refuerza la hipótesis de que es un documento original de la organización.

7.3. Conclusión de Atribución Dada la limitación técnica del FAT32, la atribución de la autoría se establece mediante **inferencia contextual**:

1. **Ubicación:** El dispositivo estaba en el puesto del director.
2. **Tiempo:** La actividad ocurrió durante sus vacaciones.
3. **Acción:** Se copiaron y posteriormente se borraron archivos sensibles.

8. Conclusiones Técnicas

En base al análisis forense digital realizado sobre la evidencia **datos.iso** y tras la correlación de los hallazgos con la información contextual proporcionada, se emiten las siguientes conclusiones técnicas:

1. Confirmación de Exfiltración de Información Confidencial Se ha **acreditado técnicamente** la existencia de material sensible de la compañía en el dispositivo analizado. Mediante técnicas de recuperación de datos, se ha restaurado el archivo plan_secreto.pdf, cuyo contenido corresponde a diseños técnicos confidenciales. Esto demuestra que el dispositivo USB fue utilizado como medio de transporte para extraer dicha información del entorno seguro de la empresa.

2. Atribución Temporal e Inconsistencia de Actividad El análisis de la línea de tiempo sitúa la transferencia de los archivos al USB el día **9 de octubre de 2017**. Este hallazgo es crítico, ya que esta fecha se encuentra dentro del periodo vacacional oficial del director de Marketing.

- **Dictamen:** Existe una discrepancia insalvable entre la actividad digital registrada y la presencia física del usuario asignado, lo que descarta que la operación fuera realizada por el director.

3. Evidencia de Maniobras de Ocultación (Anti-forense) La totalidad de los archivos incriminatorios fueron encontrados marcados como "Eliminados" en la tabla FAT.

- **Dictamen:** El hecho de que los archivos fueran copiados y posteriormente borrados sugiere una **intencionalidad de ocultar el rastro** de la exfiltración. No se trata de un borrado accidental, sino de una acción manual dirigida a "limpiar" el dispositivo tras la copia, técnica habitual en la sustracción de datos para dificultar el análisis posterior.

4. Vinculación de Dispositivo y Autoría, Aunque el sistema de archivos FAT32 no permite identificar al usuario mediante credenciales de red (SID), la vinculación se establece por evidencia física y lógica:

- El dispositivo fue incautado conectado físicamente en el puesto de trabajo del empleado investigado.
- La actividad de copia se realizó desde dicha ubicación física.
- **Conclusión final:** Los indicios técnicos apuntan a que la exfiltración fue ejecutada por un actor con **acceso físico directo** a la estación de trabajo del director, aprovechando su ausencia temporal (vacaciones) y la falta de controles de autenticación en el puerto USB para sustraer la información.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2026.01.16 11:40:48 +01'00'