

Informe Pericial

Código: A2.4

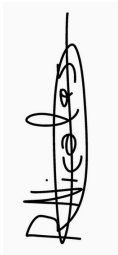
Nombre: Intento de asesinato

Equipo pericial: Grupo 3

Fecha: 16/01/2025

Índice

1. Resumen ejecutivo	2
2. Glosario de términos	2
3. Introducción	2
3.1. Datos del equipo	2
3.2. Antecedentes	3
3.3. Objetivo	3
3.4. Verificación	3
4. Fuente de información	3
4.1. Cadena de custodia	4
5. Análisis	5
5.1. Metodología	5
6. Procesos	5
6.1. Archivos eliminados	5
6.2. Sistema de ficheros	5
6.3. Navegación a través de internet	5
6.4. Línea de tiempo	6
7. Limitaciones	7
8. Conclusión	7
9. Anexo	7



1. Resumen ejecutivo

El análisis forense del disco duro intervenido ha revelado evidencias que podrían vincular al sospechoso con la presunta planificación de un atentado contra figuras políticas en España. Se han identificado documentos y búsquedas relacionadas con La Moncloa, el político Alberto Núñez Feijóo y la presunta fabricación de explosivos.

Entre los hallazgos destacan documentos con información sobre ubicaciones estratégicas, búsquedas sobre armas en armerías de Galicia, así como la visualización del programa de YouTube Los minutos del odio y la descarga del Manual de cocina del anarquista William Powell.

La reconstrucción de la línea temporal sugiere una posible planificación progresiva del atentado, desde la recopilación de información hasta la búsqueda de alojamientos en Madrid.

En conclusión, el informe pericial ha identificado indicios que podrían sugerir una intención del sospechoso de llevar a cabo un ataque. Todas las evidencias han sido analizadas respetando la cadena de custodia y garantizando su integridad para su uso en la investigación.

2. Glosario de términos

- Hash: Función criptográfica que convierte datos en una cadena única de caracteres. Se usa para verificar la integridad de archivos y detectar manipulaciones.
- Imagen forense: Copia exacta de un dispositivo de almacenamiento, creada para análisis sin alterar el original.
- Metadatos: Información técnica asociada a un archivo, como fecha de creación, modificación, acceso, tamaño y ruta de almacenamiento.
- Logon/Shutdown: Momentos registrados por el sistema que indican cuándo un usuario inicia o cierra sesión en un dispositivo.
- Ficheros encriptados: Archivos protegidos mediante contraseñas u otras formas de cifrado para impedir el acceso no autorizado.

3. Introducción

3.1. Datos del equipo

El equipo pericial responsable de la redacción de este informe es el Grupo 3. Los peritos especializados en ciberseguridad en entornos de las tecnologías de la información que conforman dicho equipo son los siguientes:

- Víctor Jiménez Corada, vjimcor955@g.educaand.es
- Nicolás Ruiz Ruiz, nruirui@g.educaand.es
- Israel Valderrama García, ivalgar260@g.educaand.es
- Alejandro Seoane Martínez, aseomar110@g.educaand.es
- Alejandro Díaz Barea, adiabar0510@g.educaand.es

3.2. Antecedentes

Las fuerzas de seguridad del estado han requerido nuestros servicios para llevar a cabo un minucioso análisis forense de un disco duro requisado a un posible criminal. Según la información proporcionada, existen sospechas de que el acusado ha intentado atentar contra un político español. Sin embargo, hasta el momento, no cuentan con las pruebas suficientes para proceder con su detención y enjuiciamiento.

3.3. Objetivo

El objetivo de este análisis es identificar cualquier tipo de información relevante que pueda corroborar o desmentir dichas sospechas. Además, se nos ha proporcionado una serie de preguntas específicas que debemos abordar en el informe pericial, las cuales guiarán nuestra investigación y análisis detallado del contenido del disco duro.

- ¿Cuál es el nombre de usuario del equipo?
- ¿Qué personaje público es el posible objeto del atentado?
- ¿En qué lugar estaba el sospechoso planeando llevar a cabo el atentado?
- ¿Cuáles serían los posibles alojamientos del sospechoso?
- El sospechoso estuvo viendo un programa en YouTube que le ha motivado para llevar a cabo el atentado. ¿Cuál es ese programa?
- Además, el sospechoso ha estado leyendo un libro que le puede ayudar en el atentado. ¿Cuál es ese libro?
- El sospechoso ha estado buscando armas en varias páginas de armerías de Galicia. Sin embargo, sólo ha anotado los precios del material de dos de las armerías que ha visitado. ¿Cuáles son dichas armerías?
- ¿Existe alguna imagen cuyos metadatos EXIF nos puedan ayudar en el caso?

3.4. Verificación

El primer paso realizado a la hora de la obtención de la imagen del disco duro ha sido verificar la integridad de los datos del mismo, haciendo un cálculo del hash tanto MD5, SHA1 y SHA256 como puede verse en la *Figura 1* del anexo adjunto a este documento.

4. Fuente de información

Se nos proporciona el disco duro de la máquina implicada en el caso. Se procede entonces a la comprobación de los hashes, manteniendo así la cadena de custodia que se refleja a continuación:

4.1. Cadena de custodia

Cadena de custodia	
Sección	Campo
1. INFORMACIÓN DEL CASO	
Número de Caso	A2.4
Tipo de Investigación	Análisis Forense
Fecha de Adquisición	10 de enero de 2025 a las 10:05
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
2. DESCRIPCIÓN EVIDENCIA EN ORIGINAL	
Tipo de Dispositivo	Disco Duro (32212254720 bytes = 32,21 GB)
Hash de la Evidencia Original	MD5: 737def84cf9a77415a613a8a162ce8ae SHA1: cd5aad4ff572fe99de0fda1900b6dca6fc430eb8
3. PRESERVACIÓN DE LA EVIDENCIA ORIGINAL	
Fecha de Entrega	9 de enero de 2025
Hora de Entrega	09:00
Recibido por	Manuel Jesús Rivas Sánchez
Ubicación en el Juzgado	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
4. CREACIÓN Y VERIFICACIÓN DE COPIAS	
Fecha y Hora de Creación	9 de enero de 2025 a las 09:00 A.M
Técnico Responsable	Grupo3
Hash de la Copia	MD5: 737def84cf9a77415a613a8a162ce8ae SHA1: cd5aad4ff572fe99de0fda1900b6dca6fc430eb8
Verificación de Integridad	Si
Entregado a	Manuel Jesús Rivas Sánchez
Fecha y Hora de Entrega	17 de enero de 2025 a las 23:59
5. REGISTRO DE ACCESOS Y VERIFICACIONES	

Fecha y Hora	15 de enero de 2025 a las 13:58
Propósito	Análisis de evidencias
Hash Verificado	MD5: 737def84cf9a77415a613a8a162ce8ae SHA1: cd5aad4ff572fe99de0fda1900b6dca6fc430eb8
Coincide con Original (Acceso)	Si

5. Análisis

5.1. Metodología

Primero se le ha calculado el hash del disco duro que se nos ha entregado, para mantener la integridad de los datos que contiene. Se ha hecho uso de la herramienta Autopsy en su versión 4.21.0 para obtener la información referente al caso y calcular los hashes de las evidencias presentadas.

6. Procesos

6.1. Archivos eliminados

En el análisis del disco duro se ha encontrado 16564 archivos eliminados y de esos archivos hay 5008 que se repiten entonces tenemos 11556 archivos eliminados únicos donde hay un archivo único relevante:

- \$RWUQ3ZD.pdf (hallazgo 6)

6.2. Sistema de ficheros

Hemos realizado un análisis a los ficheros del disco duro con el software Autopsy y en los apartados de Images y Documents hemos encontrado varias imágenes que pueden estar relacionadas con el supuesto atentado.

- Una imagen de lo que parece ser google maps en una zona allegada al Palacio de la Moncloa(imagen dentro del hallazgo 4)
- Una imagen de la entrada al Palacio de la Moncloa(hallazgo 7).
- Varias imágenes explicando la elaboración de artefactos explosivos(hallazgos del 8 al 33).

6.3. Navegacion a traves de internet

Como se puede ver del *Hallazgo 1-2* se identificaron búsquedas relevantes organizadas cronológicamente. Entre los hallazgos más destacados:

- Figuras políticas: Consultas sobre Feijóo y Alfonso Rueda, posibles objetivos del atentado.
- Ubicaciones sensibles: Búsquedas sobre el Palacio de La Moncloa.
- Armerías y armamento: Consultas relacionadas con precios de armas en armerías de Galicia, específicamente Santos Cao y Jardín.
- Alojamientos: Búsquedas de hoteles en Madrid, destacando el Hotel Condestable.
- Motivación: Visualización del programa de youtube "Los minutos del odio", del canal Fabián C. Barrio.
- Material de apoyo: Descarga del Manual de cocina del anarquista William Powell, conocido por su contenido relacionado con explosivos.

6.4. Línea de tiempo

En este apartado se ha creado una línea de tiempo de los pasos más importantes que se han identificado que realizó el usuario del ordenador.

Línea cronológica del caso



7. Limitaciones

Como se observa en el Hallazgo 5, se encontró un documento PDF encriptado. Se intentó acceder a su contenido utilizando la herramienta John the Ripper, pero no fue posible obtener la información.

8. Conclusión


El análisis forense del disco duro del investigado, Pacopepe, revela un plan para un atentado contra figuras políticas, con búsquedas específicas sobre Feijóo, Alfonso Rueda, el Palacio de La Moncloa, y alojamientos en el Hostal Condestable y el Hostal Alaska. También se detectó que visitó en el programa de youtube “Los minutos del odio” y el Manual de cocina del anarquista donde se basa para hacer el ataque

El sospechoso realizó consultas y anotaciones sobre precios de armas en Santos Cao y Jardín. Todo el análisis se llevó a cabo respetando la cadena de custodia y manteniendo la integridad de las pruebas mediante una imagen forense. Como limitación nos hemos encontrado un pdf encriptado que resulta imposible acceder (Documento anexos - hallazgo 6)

Las evidencias nos dicen que el sospechoso pretendía hacer un ataque planificado hacia la política, y este informe proporciona información clave para las autoridades en la investigación y prevención de este tipo de actos

9. Anexo

La Declaración de abstención y tacha, el Juramento de promesa, así como las figuras y hallazgos relacionados con el caso, se encuentran recogidos en el siguiente documento:

 Informe Pericial - Anexos

