

Informe de análisis forense

Código: P04

Nombre: Bomb Threat

Equipo pericial: Grupo 3

Fecha: 04/03/2025

Índice

1. Resumen ejecutivo	2
2. Glosario de términos	2
3. Introducción	2
3.1. Datos del equipo	2
3.2. Antecedentes	2
3.3. Objetivo	3
3.4. Verificación	3
4. Fuente de información	3
4.1. Cadena de custodia	3
5. Análisis	4
5.1. Confirmación del nombre del ordenador	4
5.2. Identificación del proceso de visualización de PDFs	4
5.3. Documentos editados durante la intervención	4
5.4. Evidencia de la amenaza de bomba	4
6. Línea de tiempo	5
7. Limitaciones	5
8. Conclusión	5
9. Anexo	5



1. Resumen ejecutivo

El presente informe forense detalla el análisis realizado a una imagen de memoria RAM extraída de un alumno que supuestamente dio una falsa amenaza de bomba. Se identificó una evidencia digital que vincula al usuario **pakopepe88** a través de una conversación en Discord. Se utilizaron herramientas forenses para verificar la integridad de los datos y reconstruir la línea de tiempo de los eventos.

2. Glosario de términos

- **Hash** (SHA-256): Algoritmo criptográfico utilizado para verificar la integridad de archivos, asegurando que no han sido modificados.
- **Volatility**: Herramienta de código abierto para el análisis forense de memoria RAM, que permite la extracción de información como procesos activos, archivos abiertos y conexiones de red.
- **Imagen de memoria RAM**: Captura del contenido de la memoria volátil de un sistema en un momento específico.
- **Dumplt**: Herramienta utilizada para volcar la memoria RAM de un sistema a un archivo para su posterior análisis.
- **Discord**: Plataforma de mensajería y comunicación utilizada para el intercambio de mensajes de texto, voz y archivos.
- **PID** (Process ID): Identificador único asignado a un proceso en ejecución dentro del sistema operativo.
- **PPID** (Parent Process ID): Identificador del proceso padre de otro proceso, utilizado para rastrear la relación entre procesos en ejecución.

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 Díaz Barea, adiabar0510@g.educaand.es
- Alejandro Seoane Martínez, aseomar110@g.educaand.es

3.2. Antecedentes

En una mañana de primavera, el centro escolar fue evacuado tras una llamada anónima que alertaba sobre una bomba. Posteriormente, se identificó a Francisco José Jiménez, un estudiante de bachillerato, como el posible responsable de la llamada.

3.3. Objetivo

El objetivo del análisis forense es determinar la implicación del alumno en la amenaza de bomba reportada, así como identificar cualquier otra actividad relevante que pueda contribuir a la investigación, analizando la imagen de memoria RAM haciendo uso de la herramienta de análisis volatility.

3.4. Verificación

Como se puede ver en la *Figura 1* del anexo adjunto, se ha procedido al cálculo de los hashes de la imagen tanto comprimida como extraída además del archivo de logs proporcionado, coincidiendo estos con los de los archivos originales.

4. Fuente de información

Se nos ha proporcionado una imagen de memoria del ordenador personal de Pacopepe, así como un archivo de log de DumpIt y un archivo de hashes para verificar la integridad de la imagen del disco.

4.1. Cadena de custodia

Cadena de custodia	
Sección	Campo
1. INFORMACIÓN DEL CASO	
Número de Caso	P04
Tipo de Investigación	Análisis forense
Fecha de Adquisición	27 de febrero de 2025 a las 08:00
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
2. DESCRIPCIÓN DE EVIDENCIAS	
Tipo de Dispositivo	Imagen de disco (4294504448 bytes = 3,99 GB)
Nombre del archivo	DESKTOP-01S7HH9-20220408-171552.dmp
Hash de la Evidencia Original (SHA-256)	edcdbcac27263a45d6dfe27f6c8baff55952b2357a70031de20de057730cd359
Tipo de Dispositivo	Imagen disco comprimida (1200000000 bytes = 1,2GB)
Nombre del archivo	DESKTOP-01S7HH9-20220408-171552.dmp.zip
Hash de la Evidencia Original (SHA-256)	2246b2abb178b3a508b5c8207d50e7e6f86d5c1f09487b50d aaa6387bef639f0
Tipo de Dispositivo	Archivo de logs

Nombre del archivo	DESKTOP-01S7HH9-20220408-171552.json
Hash de la Evidencia Original (SHA-256)	cbcd0ac591b4fc425550eb1292ad8f1dddc4b0146a6d0df7b23f6d13fa84b049

5. Análisis

Para el análisis se empleó la herramienta **Volatility 2**, junto con comandos de terminal para examinar la memoria RAM del equipo. Tras la verificación de la integridad de la imagen mediante y seleccionar el perfil, se ha conseguido identificar procesos activos, archivos editados y registros de actividad en plataformas de mensajería.

5.1. Confirmación del nombre del ordenador

El nombre del ordenador fue confirmado como DESKTOP-01S7HH9 mediante la consulta de registros de Windows y las variables de entorno del sistema. Esto lo podemos encontrar en la Figura 2.

5.2. Identificación del proceso de visualización de PDFs


El proceso de la aplicación utilizada para visualizar documentos PDF fue identificado con el PID 7376 y el proceso padre con el PPID 8664. El proceso padre no mostraba procesos adicionales. Véase la Figura 3.

5.3. Documentos editados durante la intervención

Como se puede ver en la Figura 4, se identificaron varios documentos editados durante la intervención policial. Se descartaron los archivos asociados a *Steam* para centrarse en los relevantes al caso. En la *Figura 5*, comprobamos que el proceso padre concuerda con el programa de edición de texto Office.

5.4. Evidencia de la amenaza de bomba


Durante el análisis, se encontró una conversación de Discord en la que el usuario pakopepe88 admite haber realizado la falsa amenaza de bomba para evitar un examen de lengua. En la *Figura 6* puede verse el archivo bruto que contiene la conversación, tras transcribir el archivo a formato legible se puede leer lo siguiente:



```
marcosheredia666:
2022-04-08T16:17:04.625000+00:00: "bah tampoco yo"

pakopepe88:
2022-04-08T16:17:18.582000+00:00: "es ke ni copiar de la wikipedia, te
lo juro."

marcosheredia666:
2022-04-08T16:17:30.368000+00:00: "bueno, yo eso si"
2022-04-08T16:24:56.786000+00:00: "Fuiste tu el que llamó al insti con
la amenaza de bomba, so colgao?"
```



pakopepe88:

2022-04-08T16:25:07.074000+00:00: "si buajajaja"

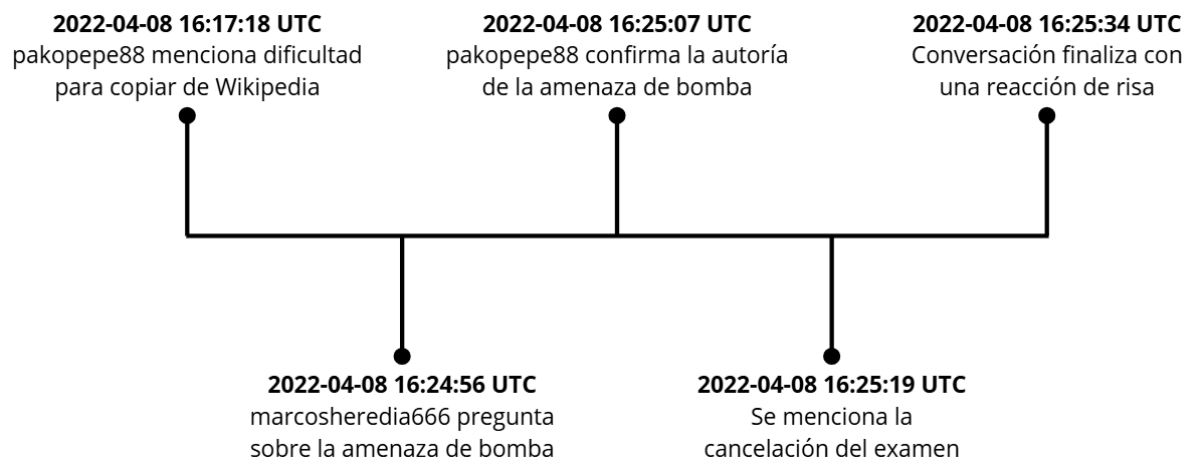
2022-04-08T16:25:19.620000+00:00: "hala, ya no hai examen de lengua"

2022-04-08T16:25:22.568000+00:00: "ke le den por kulo"

marcosheredia666:

2022-04-08T16:25:34.832000+00:00: "🤔"

6. Línea de tiempo



7. Limitaciones


Una de las principales limitaciones en este análisis ha sido la dificultad de encontrar el perfil correcto para interpretar los datos. Dado que Volatility requiere especificar un perfil de sistema operativo que coincida con la memoria volcada, cualquier error en esto afecta en la precisión de los resultados. La falta de un perfil exacto ha complicado el proceso, retrasando la obtención de información.

8. Conclusión

El análisis forense permitió identificar una conversación que tuvo el usuario de discord pakopepe88, el presunto autor de los hechos ocurridos en la institución, en la que confesaba haber realizado la llamada telefónica amenazando al instituto.

9. Anexo

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

 P04-Anexos_Bomb_Threat-G3