Informe de Análisis Forense

Resumen Ejecutivo:

Se llevó a cabo un análisis forense en una partición de 1GB en un sistema operativo Windows. Se agregó y eliminó una fotografía, se añadieron múltiples archivos y carpetas, se creó un archivo Excel confidencial que luego se renombró a prueba1bastionado.pdf. Posteriormente, se realizó una imagen forense de la partición utilizando FTK Imager 4.7.1.2 y se llevó a cabo un análisis adicional utilizando Autopsy 4.21.0. Se identificaron discrepancias de extensión en un archivo que fue renombrado y se recuperó una imagen previamente borrada.

Descripción detallada del proceso:

1. **Creación y manipulación de la partición:**
   - Se creó una partición de 1GB en el sistema operativo Windows.
2. **Manipulación de archivos y carpetas:**
   - Se agregó una fotografía al disco duro y posteriormente se eliminó.
   - Se añadieron 23 archivos y 11 carpetas, incluyendo archivos .txt con correos y URLs, así como un archivo Excel llamado "confidencial".
3. **Modificación de archivo Excel a PDF:**
   - Se utilizó el comando CMD para cambiar la extensión del archivo Excel llamado "confidencial" a prueba1bastionado.pdf.
4. **Creación de imagen forense:**
   - Se realizó una imagen forense de la partición de 1GB utilizando FTK Imager 4.7.1.2.
5. **Análisis forense con Autopsy:**
   - Se utilizó Autopsy 4.21.0 para analizar la imagen forense.
   - Se emplearon los módulos Extension Missmatch Detector, Picture Analyzer y PhotoRec Carver.

6. **Hallazgos durante el análisis con Autopsy:**
    - Se identificó un archivo llamado "prueba1bastionado.pdf" que, al examinar sus metadatos, se descubrió que era un archivo de Microsoft Excel a pesar de tener la extensión PDF.
    - Se encontró una imagen en la sección de archivos borrados, la cual proporcionaba datos de localización y detalles del dispositivo móvil utilizado para tomar la fotografía original.
    - Se recuperó la imagen previamente borrada utilizando la función correspondiente de Autopsy.
7. **Recuperación de la partición original:**
    - Se restauró el tamaño de la partición a su estado original, recuperando el GB eliminado.

Conclusiones:

El análisis forense reveló manipulaciones significativas de archivos y metadatos en la partición de 1GB, incluyendo la modificación de extensiones y la ocultación de datos confidenciales. Además, se pudo recuperar con éxito una imagen previamente eliminada, demostrando la importancia de técnicas forenses para la recuperación de datos.