

Tarea 1: Formatos Imagen Forense

Abisinia Fernández

September 2020

1 Introduction

La creación de imágenes forenses de medios de almacenamiento digital es una tarea cotidiana, ya sea en el ámbito privado como en laboratorios periciales.

Con el objetivo de asegurar que el contenido de un medio que se someterá a algún tipo de análisis forense no sea modificado, se requiere efectuar una copia forense para el resguardo de la evidencia digital, siguiendo las mejores prácticas y normas al respecto.

Entre los requisitos para una copia forense, además de ejecutar la lectura bit a bit en el medio original y su escritura en el medio destino, se debe utilizar al menos un método de verificación probado mediante un algoritmo, el cual se usa únicamente con fines de verificación.

2 Información

2.1 Investigación

- EWF (Expert Witness Compression Format): Este formato cuenta con varias versiones, donde E01 ha sido depreciada. La versión Ex01 mantiene muchos de los principios de diseño centrales de E01. Guarda datos en bloques que son verificados con un código de detección de errores de 32-bits además a todos los datos almacenados en el archivo se le aplica un hash, ya sea md5 o sha1 si es requerido por el usuario. Las mejoras de Ex01 no afectan características del archivo pues varios tribunales toman estos archivos como evidencia aceptada.
- RAW (DD, IMG, RAW): Este formato representa secuencias de bytes capturadas no estructuradas desde un volumen físico o lógico. Este representa cualquier imagen que es únicamente una copia de sector por sector sin comprimir los bits almacenados.
- AFF (Advanced Forensic Format): Al igual que EWF, este cuenta con varias versiones, donde AFFv1-3 ha sido depreciada. Este formato fue

diseñado como una alternativa a los formatos de imagen de disco patentados. AFF ofrece dos beneficios relevantes, permite almacenar metadatos extensos con imágenes y consume menos espacio en disco que las imágenes en otros formatos. En la versión AFF4 las partes sob almacenadas como objetos y URN asignadas que pueden ser utilizado para afirmar hechos sobre los objetos.

2.2 Tabla comparativa

Raw	EWf	AFF
No compresión	Compresión	Puede almacenar imágenes con o sin compresión
No incluye una cabecera para los metadatos.	Contiene tant una cabecera como un final que contienen metadatos sobre la imagen.	Almacena metadatos en la imagen o por separado.
	código de detección de errores.	Provee autenticidad de evidencia con funciones hash tradicionales, como lo son md5 y sha1. Además de firmas digitales avanzadas basadas en certificados x.509.

2.3 Pcap

- Pcap: Este formato se usa ampliamente para la captura de paquetes en la industria de la seguridad en una red. Estos archivos pueden ser aprovechados para identificar archivos eliminados o temporales que pueden haber sido transferidos durante un evento mediante un protocolo de transferencia aun cuando la existencia del archivo no reside en el sistema de archivos a analizar.
- Pcapng: Este formato es una mejora que agrega extensibilidad, portabilidad y la capacidad de combinar y agregar datos a un rastreo de cables.

References

- [1] HARVARD LIBRARY, Revisado el 22 de septiembre del 2020. https://dash.harvard.edu/bitstream/handle/1/2829932/Malan_Advanced-Forensic.pdf?sequence=4
- [2] WE LIVE SECURITY, Revisado el 22 de septiembre del 2020. <https://www.welivesecurity.com/las-es/2020/02/28/benchmarkherramientas-realizar-imagenes-forenses/>

- [3] HARVARD LIBRARY Revisado el 22 de septiembre del 2020. HTC DreamGIAC Global Information Assurance Cetification Paper. <https://www.giac.org/paper/gcfa/10182/forensic-images-viewing-pleasure/126976>
- [4] HARVARD LIBRARY <https://www.google.com/url?sa=trct=jq=esrc=s&source=webcd=cad=rjauact=8ved=2ahUKEwir.6vD1PvrAhVFd6wKHdsvAD0QFjADegQIARABurl=httpsapihttps://www.sans.org/blog/digital-forensic-sifting-mounting-evidence-image-files/>
- [5] ReviverSoft Revisado el 22 de septiembre del 2020. <https://www.reviversoft.com/es/file-extensions/pcap> HTC Dream Keirstenbrager Revisado el 22 Septiembre del 2020. <https://www.keirstenbrager.tech/pcap1/>