Recuperação de Logs no Sistema de Arquivos DHFS4.1

Davi Azevedo de Queiroz Santos[1*]
[1] Polícia Científica do Paraná, Curitiba, Paraná
**Autor; e-mail: davi.santos@policiacientifica.pr.gov.br*

RESUMO
Este trabalho apresenta uma técnica de recuperação de logs armazenados no sistema de arquivo DHFS4.1 e é baseada na assinatura JSON dos campos do banco de dados SQLite. Os resultados mostram que, embora haja dados apenas na memória interna, a maioria dos logs é armazenada somente no disco rígido. Portanto, essa abordagem traz novos elementos para análise pericial de aparelhos DVR em diversos casos.
Palavras-chave: extração de dados, engenharia reversa, DVR.

Introdução
Os aparelhos DVR da marca Intelbras são os mais usados no mercado brasileiro. Portanto, a extração da maior quantidade possível de dados, além de vídeos, é de suma importância para a perícia. Atualmente, não há ferramentas que recuperem corretamente os logs presentes no disco.

Objetivos
Extrair *logs* do sistema de arquivo DHFS4.1[1], que estão presentes nos discos rígidos de DVRs da marca Intelbras a partir da versão 4.0 do *firmware* e de outros fabricantes que o utilizam.

Métodos
Na posição 0x114 do cabeçalho da primeira partição do sistema de arquivos DHFS4.1, em mais de trinta discos rígidos analisados, foi identificado o setor inicial do disco que contém um banco de dados que armazena *logs* no formato SQLite, que possui estrutura conforme [2]. Os dados de *log* de cada registro possuem o formato JSON. Há também outros arquivos presentes como arquivos temporários de diário de reversão do SQLite. Para recuperar todos os registros (*logs*) possíveis, foi realizado o procedimento de *carving* a partir da assinatura JSON desses registros. Em seguida os dados recuperados foram comparados com os registros de eventos extraídos pela interface do aparelho tanto com o disco rígido conectado quanto desconectado.

Resultados e Discussão
Observou-se que há eventos que são gravados exclusivamente na memória interna do aparelho, como datas e horários em que o aparelho foi ligado/desligado e informações do disco rígido e da rede. Contudo, do disco rígido foram recuperadas diversas informações como: acessos, alterações de configurações, vídeos visualizados, perda de sinal de câmeras, detecções de movimento. Estes logs só estavam presentes na interface do aparelho quando o disco rígido estava conectado. Também foram recuperados registros corrompidos, logo é necessária uma análise pelo perito para interpretar corretamente os resultados.

Conclusão
Os dados recuperados são relevantes e úteis em diversos contextos periciais, como por exemplo: quando apenas foi encaminhado o disco rígido, analisar o comportamento do equipamento, identificar possíveis alterações nas configurações do equipamento.

Referências bibliográficas
[1] SANTOS, D. A. Q. Extração de dados do sistema de arquivos DHFS4.1. In: Conferência Internacional de Ciências Forenses, 5., 2021, Foz do Iguaçu. Anais eletrônicos. Interforensics, 2021. p. 54-54.
[2] HOOGENDOORN, I.; BREUK, R. The forensic reliability of recorded video images on digital video recorders by Dahua Technology. 2012. Disponível em: https://bit.ly/3Llpfti. Acesso em: 30 abr. 2023.