The Forensic Potential of MacOS Spotlight PSID.DB: Tracking Illicit Storage Drive Activity Through Artifact Reverse Engineering, Scripting and Analysis

Hale, Ethan (School: South Eugene High School)

Computers are everywhere today, and digital traces often remain that can help reconstruct past events. When available, computer forensic artifacts can be crucial in establishing guilt or innocence in legal proceedings. However, known artifacts often fail to capture information about all files that previously existed on a drive. This study aimed to identify, analyze, and extract more comprehensive historical file information from Apple Spotlight forensic artifacts through research, analysis, and script development. Previous Spotlight research and tools have identified and mapped the Store.db artifact (Atwal et al., 2019). In this study, a new artifact, PSID.DB, was discovered, which may contain information about previously existing files and folders. The PSID proprietary structure was interpreted by examining prior research, hexadecimal patterns, compression, encoding, encryption and common artifact timestamp formats. With this map, I developed a Python script to parse PSID. To assess PSID's value and factors affecting recovery, I conducted tests simulating typical user storage drive activities then compared PSID recovery against (a) known file records and (b) Store.db recovery. Results showed PSID recovery matched or exceeded Store.db whenever PSID was present. In some tests, PSID recovered all previous file records, while in others, it recovered five times as many records as Store.db. The storage drive file system was found to be a key factor affecting PSID recovery. This study mapped the PSID artifact, demonstrated that it can, in some cases, provide a more complete list of historic files than previously researched Spotlight artifacts, and developed a script for forensic examiners to parse PSID.

Awards Won: