Jordan University of Science and Technology

Carving and Clustering Files in RAM for Memory Forensics

Authors: Ziad A. Al-Sharif, Attaa Y. Al-Khalee, Mohammed I. Al-Saleh, and Mahmoud Al-Ayyoub

Abstract: Memory contains vital information about the current state of a system such as processes, network connections and opened files. The contents of a file can be reconstructed from memory either by following the Operating System?s data structures (which might not be always available) or by carving data based on the file?s internal structure. Unfortunately, the problem gets more complicated when carving several files with the same internal structure that happen to coexist in memory. This paper carves chunks of a certain file type from memory and employs clustering techniques to distribute these chunks into their corresponding files. As a running example, we carve and cluster different PDF files. The paper employs the wording similarities among related portions and shows that the Hierarchical clustering algorithm facilitates grouping of the recovered text pieces within an adequate accuracy.