C17 Digital Stratigraphy: Analyzing File Allocation Methods to Uncover Concealment Behavior

Eoghan Casey, PhD, University of Lausanne, Batochime, CH-1015 Lausanne-Dorigny, Lausanne, Vaud, SWITZERLAND*

The goals of this presentation are to: (1) increase knowledge of file allocation methods and traces; (2) review contextual analysis of file allocation traces (digital stratigraphy); and, (3) raise awareness of potential limitations of digital stratigraphy.

This presentation will impact the forensic science community by illustrating how advances in the practice of file system analysis will enable forensic examiners to perform contextual analysis of file allocation traces in order to differentiate between concealment behavior and normal system activity.

When computing devices are used to conceal digital evidence by deleting, reformatting, wiping, or backdating files, it can be challenging to prove concealment behavior versus normal system activity.

There is a common misconception that new files are saved onto storage media in a predictable fashion. Certainly, in the simplest scenarios, such as on a memory card in a digital camera when files are saved in quick succession, there can be a predictable next-available allocation; however, there are situations that will cause file allocation to deviate from predictable or deterministic allocation strategies. In one case, a forensic examiner misinterpreted gaps between allocated files as indications of file wiping.

Furthermore, file initialization can exhibit itself in various ways when different applications, operating systems, and file systems are involved. In one case, a new file system entry was initialized but nothing was saved to disk, leaving untouched data from a prior deleted document in the space allocated to the new file system entry, making it seem like backdating (i.e., a file system entry created in 2015 seemingly containing information dated 2014). To avoid confusion, great care must be taken when interpreting the provenance of deleted data that is recovered from a partially initialized file.

Understanding file allocation methods can provide insight into such concealment behavior, but real world computer use introduces complexity that complicates forensic analysis. Each file system tells a story about the use of that storage media, and analyzing the allocation of files over time can sometimes provide insight into deletion or other concealment activities. As a result, general understanding of file allocation methods can only be used as a starting point, and it is necessary to take the overall context into account when analyzing traces of such concealment behavior. Contextual analysis of file allocation traces is called digital stratigraphy because it has similarities to the concept of stratigraphy in archaeology.

Using examples of forensic analysis from past cases, this presentation demonstrates how digital stratigraphy has been used to address questions of concealment behavior. The challenges, successes, and limitations of this form of forensic analysis are discussed.

File System Forensics, Digital Concealment Behavior, Digital Stratigraphy