Abstract

This paper explores the statistical properties of microfragment recovery techniques used on NTFS filesystems in the use of digital forensics. A microfragment is the remnant file-data existing in the cluster slack after this file has been overwritten. The total amount of cluster slack is related to the size distribution of the overwriting files as well as to the size of cluster. Experiments have been performed by varying the size distributions of the overwriting files as well as the cluster sizes of the partition. These results are then compared with existing analytical models.