

Recovering deleted files (3 of 3)

Description

To recover deleted files, user activity logs, Internet history, and other potentially relevant custodian information, a “physical” copy or forensic image of the hard drive or other media is required. Creating a physical copy or forensic image preserves the entire contents of the media, and makes it possible to recover deleted files, user activity and other potentially relevant artifacts. Several hardware and software products specifically designed to capture a physical copy or forensic image are available.

A computer forensic examiner needs access to the “space” between the visible files that contains deleted information. This space is referred to as unallocated (slack, free, swap) space and requires a physical copy or forensic image.

Copying files from Windows Explorer skips over the unallocated areas mentioned above. Make sure you request a clone or forensic image of any media where you believe deleted activity and file content might reside. Depending on what remains, your computer forensics examiner will be able to recover the deleted activity.

Date

11/27/2025

Date Created

08/05/2008