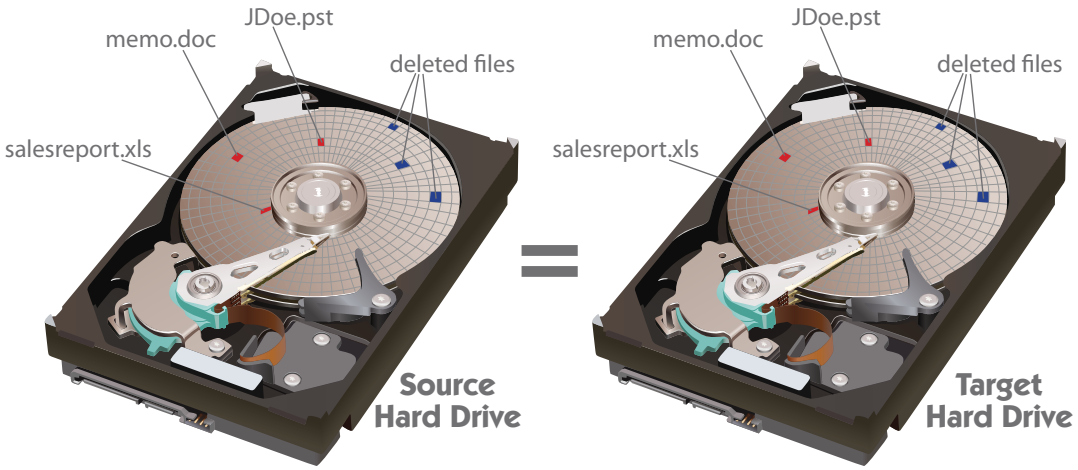
Forensic Image (Clone) vs Active File (Logical) Collections

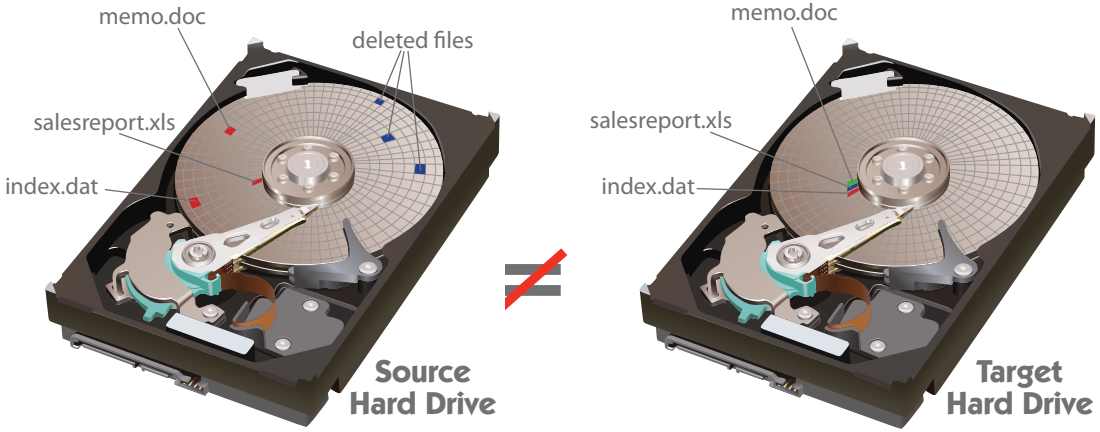


Forensic Image (Clone)

- Allows deleted information (files, email, user logs) to be recovered from source media.
- A forensic image or clone copies the entire contents of the source media including unallocated space.
- A large quantity of data can usually be viewed and recovered from the source media even when it isn't visible in the host computers operating system (i.e. Microsoft Windows).

Active File (Logical) Collections

- If a forensic investigation isn't required an active file collection can reduce costs and the size of the overall file collection.
- Active file collections includes copying files that are currently accessible from the host operating system (i.e. Microsoft Windows).
- Files collected from corporate servers (file shares) commonly use active file collection because it can be cost prohibitive to image servers, the amount of irrelevant data and the inconvenience of shutting down servers or the time required for a live acquisition.



PINPOINT LABORATORIES

www.pinpointlabs.com