# SUMMER 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics, and cybersecurity needs. For this E-Newsletter, we focus on the topic of cloud storage technologies and the impact on legal, compliance, and investigations.

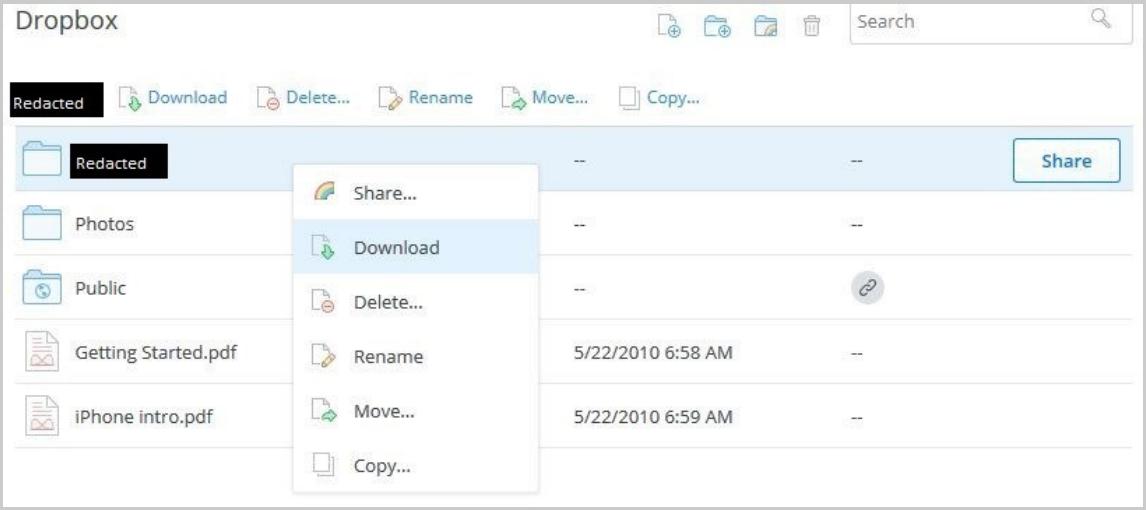
## THE INTRICACIES OF PROPER DATA PRESERVATION OF CLOUD-BASED FILE STORAGE


When storage administrators had local file servers, metadata could easily be preserved through targeted forensic imaging. Now that cloud storage is ubiquitous, and the location of servers is often unclear, data preservation presents different challenges. In fact, when servers are shared by many organizations, as is often the case with cloud storage, targeted forensic imaging is not a viable option in the vast majority of instances. From a data preservation standpoint, there are key issues regarding metadata that must be addressed when dealing with collecting data from a cloud storage site. Two of these issues, the method of file access (e.g. synced to a computer versus downloading from a link), and, the method of controlling access to data from different sources (e.g. shared links, third party applications, etc.) can influence metadata preservation. Since preserving metadata is vital, the two points above will be discussed in detail for Dropbox, Box, and Google Drive.

**Dropbox**

For Dropbox, how a user accesses data can affect the metadata. For instance, if a user has a direct link to a file on Dropbox, once a user downloads the file, the modification date, creation date, and last access date at a system-level are all changed to the date the file was downloaded onto the local machine. Alternatively, if the user syncs to the local machine, then the modification date stays as the original date on which the file was uploaded onto Dropbox. The creation date and last access date will change.

Another interesting note is that a method exists whereby downloading a folder and its contents into a ZIP file will not change the modification date of the files within the downloaded folder. To do this, the user just has to right-click into the empty space next to the name of the folder and click download. In the illustration below, the user selected the “Redacted” folder and right-clicked on the empty space (light blue), the resulting menu includes the “Download” option.




As for controlling access to data, a Dropbox user can share a link to a particular folder within their Dropbox and set the permissions to allow either editing the folder (e.g. edit, delete, and add files to the folder) or view the folder (e.g. view and download the files, but not edit). This can be quite dangerous, since once the link is sent from the basic Dropbox user's account, there is neither control over the recipient forwarding the link, nor is there password protection for the contents. Users must upgrade to Dropbox Business or Pro editions to achieve those protections. However, third-party applications can be controlled by the user by accessing the Security tab in Settings and revoking access to applications that are connected to the Dropbox.

**Box and Google Drive**

Box and Google Drive are very similar to Dropbox in terms of functionality. For both services, if users download data directly onto a local machine, the modification date, creation date, and last access date changes to the download date. In Box, if the native application is used to sync data onto the local machine, the modification date and creation date do not change, but the last access date changes to reflect the last sync onto the local machine. In Google Drive, if the native application is used to sync data onto the local machine, the modification date and last access date do not change, but the creation date changes to reflect the last sync onto the local machine.

Box and Google Drive users have the ability to share links to particular folders and files, and, to set the permissions for editing or viewing only. For Box, there is a business class upgrade for password protecting files and folders, as well as restricting access by date. Google Drive does not have an option to enable password protection for files and folders. However, Google Drive does provide users the option to prevent editors from changing access and adding new users to shared files, as well as preventing commenters and file viewers from downloading, printing, and copying files. In order to access Google Drive, every user needs to have a Google account. As for third party applications, Box enables these applications to access user data through the Box App Marketplace, while data in Google Drive maybe accessed by third party applications or by native Google Apps such as Docs, Slides, and Sheets. Both Box and Google Drive can revoke third-party application access.

**Retrieving Preserved Metadata**

Among Dropbox, Box, and Google Drive, many functional similarities enable user preservation of existing metadata. However, retrieving entire metadata file listings presents another challenge. For example, in Dropbox, a user would have to create a developer web application that calls the metadata portions of the Dropbox API into automated server requests called "Webhooks."

Webhooks serve as a way to notify users, in real-time, when a file changes. The reports sent out go to another server that can receive the reports, and from there, a user or data collection expert can retrieve records of what files changed. Google Drive and Box operate in a similar manner. For Box, metadata fields are also customizable for file classification.

Thankfully, for attorneys, e-discovery professionals, and investigators who rely on proper evidence preservation, forensic data collection from a local computer via the sync folder of each cloud storage application (e.g. Box Sync) is a potential solution. With these advanced technical tools, coupling preservation with syncing data to a local machine from the cloud, digital evidence can be properly preserved. On the local computer, there are also typically log files tracking files that have been synced. These logs are accessible by specialized forensics utilities. With data preservation being one of the most critical steps in discovery, yet typically the lowest cost part of the process, it's important to augment your case team with companies possessing cloud expertise, such as Digital Mountain.

## UPCOMING INDUSTRY EVENTS

**July 2016**
The Masters Conference, Managing the E-Discovery and Social Media Minefield,
New York: July 19

**August 2016**
HTCIA 2016 International Conference & Training Expo,
Las Vegas: August 28-31

ILTACON 2016,
National Harbor: August 28-Sept. 1

**September 2016**
CSA Congress and IAPP Privacy Academy 2016,
San Jose: September 15-16

***Click here to see more upcoming events and links***

*Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.*

**DIGITAL MOUNTAIN, INC.**
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

**www.digitalmountain.com**

***Contact us today!***

***FOLLOW US AT:***