C31 Challenges in Determining End-User Actions Based on Cloud Repository Metadata

Darcie Lynn Winkler, MSFS, Stroz Friedberg, 1150 Connecticut Avenue, NW, Washington, DC 20036*

After attending this presentation, attendees will better understand the challenges involved in drawing conclusions based on metadata from cloud repositories, such as Google® Drive™ and Dropbox™ Paper, in addition to how end-user actions affect the available metadata.

This presentation will impact the forensic science community by providing a clear and concise summary of how end-user actions impact the metadata maintained in cloud-based environments and how this information can be used to make reliable conclusions in digital forensic investigations.

Metadata, or "data about data," is a critical artifact relied upon in many digital forensic investigations and extensive research has been conducted by the digital forensic community to better comprehend how dates of files relate to actions taken by the user; however, cloud metadata is stored and updated differently than metadata on a physical file system, and, thus, the need to understand this tracking system is of the utmost importance. Therefore, this presentation will describe recent research and analysis performed on data stored in Google® Drive™ and Dropbox™ Paper repositories, with a specific emphasis on the analysis of metadata to determine user activity.

The use of various cloud repositories to create, edit, and store documents is becoming more and more commonplace, and the data in these repositories has become increasingly relevant in both civil and criminal digital forensic investigations. Google® Drive™ and Dropbox™ Paper were researched in order to determine what types of metadata are stored and how they relate to common user actions. To replicate as many user scenarios as possible, the web-based interface was used in conjunction with the downloaded applications on a Windows® desktop computer and an Apple® mobile device. Several typical user actions were completed, such as creating, editing, downloading, and uploading documents, while changes made to the metadata were documented.

This presentation will describe how various actions performed by the user can change the metadata between different platforms: the web-based interface, the application on a Windows® machine, and the application on an Apple® iPhone®. For example, while Google® Drive™ maintains date metadata to an extent within the web interface, the created time of the file is overwritten by the time of download, regardless of how it is downloaded; however, the modified date remains unchanged except for the fact that it is represented in Pacific Standard Time despite Google® Drive™ settings being set to Eastern Standard Time. Unlike the original Dropbox™, Dropbox™ Paper allows for the creation and editing of documents and only shows the dates of recent edits within the web-based interface. Once the file created within Dropbox™ Paper is downloaded, the modification date is overwritten with the time of download. Many other situations will be discussed to enhance analyst comprehension of how metadata is affected by common end-user actions.

Forensic analysis of cloud metadata is especially challenging, as new features and versions are constantly being introduced by cloud providers. To overcome the challenges of ever-changing metadata tracking systems, digital forensic analysts need to be aware of the versions and features relevant to their case and, if necessary, verify their understanding of the relationship between user actions and the changes in the metadata in the same environment. Without this comprehension, analysts may be unable to make knowledgeable and accurate conclusions when translating the metadata of a cloud repository file into user-attributable actions.

Cloud Forensics, Google® Drive™ Metadata, Dropbox™ Paper Metadata