The Evolving eDiscovery Landscape: Tackling Cloud Storage's Hashing Puzzle

Description

This is the 3rd article in our cloud collection defensibility series, delving deeper into the intricacies of maintaining data integrity during digital evidence collection from various cloud sources and targets. In this piece, we build on the discussions from our previous articles—exploring ETag verification in Google Docs and unraveling the QuickXOR mystery in Microsoft 365—to address a common yet complex issue in eDiscovery: hash-verifying files across different cloud environments.

The Hashing Challenge in Cloud-Based eDiscovery

The advent of cloud computing has revolutionized how we store and access data. Cloud platforms like Google Drive, OneDrive, AWS, box, and Dropbox have enabled access to files anywhere worldwide, providing convenience and flexibility for users and organizations alike. However, this cloud-based utopia presents unique challenges for legal professionals in eDiscovery and digital forensic collections.

When collecting data for legal purposes, it's not enough to just copy files from one place to another. The integrity of each file must be maintained, proving that it is an exact replica of the original. This is where hashing comes into play. Hash values act as digital fingerprints for files, and unique codes are generated based on the file's content. Ideally, a file's hash value should remain consistent from its original location (the source) to wherever it is stored for review (the target location). Achieving this consistent hash value is the cornerstone of data integrity in eDiscovery and digital forensics.

However, the cloud complicates this process. Different cloud services use various hash types to create hash values, and when copied to other cloud targets, those hash types vary as well. Because of this, it makes it impossible to rely on just the default hash types for comparison. An additional verification process must be added to the workflow to verify files using the stored value for the hash source from the

cloud service provider.

To navigate this challenge, eDiscovery and digital forensics professionals need specialized tools to handle cloud-based collections. These tools can identify the hash type used by the cloud source, accurately access and store the hash value, and ensure that the copying process maintains the integrity of the hash type from the source to the target. Several tools from Pinpoint Labs consider the complexities of whether files are being collected locally or cloud to cloud.

One key feature of these specialized tools is their ability to provide corresponding hash types and values for the copied files. This creates a defensible chain of custody for the digital evidence, ensuring the files are genuine and unaltered.

Furthermore, these tools streamline the collection process, automating the identification and verification of hash values. This saves time and reduces the risk of human error that can come with manual verification. By using such advanced tools, legal professionals can confidently navigate the complexities of cloud data collection and uphold the standards of evidence required in legal proceedings.

As the legal industry continues to contend with the ever-expanding digital landscape, robust and reliable collection tools are becoming increasingly critical. Collecting and verifying digital evidence from cloud sources is paramount to the integrity of the legal process. By understanding and utilizing specialized tools for cloud data collection, legal professionals ensure they can deliver accurate and defensible evidence, no matter where it resides.

The journey of data from cloud to cloud, cloud to local, or network drives is fraught with challenges. Still, with the right tools and understanding, it’s possible to maintain the consistency and integrity of hash values, ensuring the admissibility of digital evidence. As cloud computing continues to grow, so does the importance of mastering these tools and techniques to navigate the cloud confidently and competently.

Date
11/23/2024
Date Created
01/03/2024