Introduction

Creating secure and reliable backups of media is critical to ensure that no data is lost during production and post. Verifying the integrity of files between various companies and or departments however, is a process that has many variables that can lead to confusion and or unnecessary time spent troubleshooting damaged files. Though most agree that this process is vital, different verification methods are utilized, depending on the tools as well as procedures, specified by a given company or individual. The American Society Of Cinematographers (ASC) has developed the ASC Media Hash List (ASC MHL) specification, to standardize the media transfer process with the goal of injecting consistency and efficiency in media workflows.
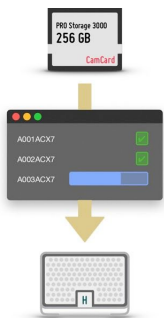
After media is recorded in camera, it needs to be copied to other storage locations, and the camera cards can then be cleared and re-used.

It is common that several companies, or individuals will need to share copies of this media for various work. Some of these people receiving media will create checksums, some will not. The type of checksum created, the formatting and where the verification confirmation is stored, will often vary depending on who is managing the media.

Editorial   **VFX Company**   **Dailies Lab**   **Finishing Company**
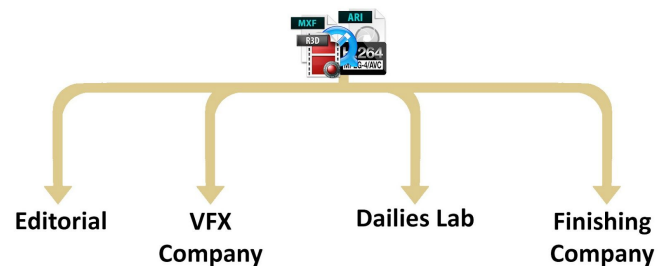
With so many variables at hand and no real standards in practice, ensuring safe handling of production's negative is not a guarantee. If files are found to be damaged, it's very difficult to track down where this occurred within the production's lifespan.

Solution

Productions will continue to use different hash types for their backups and the ASC MHL is not attempting to create yet another to add to the list. Instead, the ASH MHL is a common wrapper that can contain varying hash types, addressing the issues detailed above by standardizing what information is gathered, how it is formatted, where the checksum is placed, and documenting these hashes together with essential file metadata in a human-readable XML format.

A new ASC MHL created for every copy in production or post, when linked together, can provide a chain of custody. This will reveal the number of times files have been copied since acquisition and, if damage has occurred, where and when. Even if one hash type has been used (for example, xxHash) on set, but a different hash type (for example, MD5) used in post, this chain of custody will track the change throughout the file's lifespan. Directory hashes are also provided to reveal if files have been removed, or added to any folder structure previously verified.

The ASC's Advanced Data Management Sub-Committee, with members from studios, software companies, DITs, and post facilities, have collaborated on this effort, to address this problem.

More details will be released soon as to the status on our specification and white paper.