Data Migration

"If it were simple, everyone would be doing it."

The simple definition of data migration is the process of selecting, preparing, extracting, and transforming data, then transferring it from one software solution or storage system to another. If only it were as easy as it sounds. In the context of Law Enforcement, Prosecutors, and Courts, these data migrations usually refer to digital evidence files and records. What many people do not think of, or include in the "simple" migration process, are all of the hash validations, metadata, playback/supporting folders, and audit trails that need to be transferred with the digital evidence files.

There are several reasons to migrate or to perform this "simple function." The need to migrate from an old, outdated software/hardware solution to a new one; the current manufacturer has been sold or is no longer supporting the old version; the secondary devices (i.e., DVDs, CDs, thumb drives, LTO) or storage are failing, or the hardware is becoming obsolete and is almost impossible to find in order to support playback. These are all valid and important reasons to migrate. The big questions become: Can the infrastructure be properly figured out? Can the hardware to playback the files to migrate onto the new platform?

5 Layers of Complication

Complication Layer 1:

There are several types of metadata that needs to be accounted for:

- **Descriptive metadata -** Descriptive metadata is essential for discovering and identifying assets. It is information that describes the asset, such as the asset's title and relevant keywords. Descriptive metadata is how a user locates a file in a particular case or event.

    - For example, Classifications, Suspect Name, Location/Address, Case ID

- **Administrative metadata –** Administrative metadata relates to the technical source of a digital asset. It includes data such as the file type, as well as when and how the asset was created. This is also the type of metadata that relates to usage rights and intellectual property, providing information such as the owner of an asset, where and how it can be used, and the duration a digital asset can be used for the various purposes under the current license.

    - User owner/creator, retention policy, photo vs. video vs. audio file

- **Structural metadata** - Structural metadata is data that indicates how a digital asset is organized, such as how pages in a book are organized to form chapters, or the notes that make up a notebook in Evernote or OneNote. Structural metadata also indicates whether a particular asset is part of a single collection or multiple collections and facilitates the navigation and presentation of information in an electronic resource.

    - Bookmarks/Markers, Chapters (if the video is segmented/chunked into smaller sizes), Exif

Complication Layer 2:

The video files may be proprietary and need to have a specific player or set of files in order to view them. The questions become: Is there a way to convert them? Should the old player be brought into the new solution? Will the new solution even support these options? In any scenario, the file/s will need to be validated that they have not been altered during the conversion or migration. If conversion is an option, then the consideration of maintaining the original and providing a link between the parent (the original) and the child (working product) needs to be captured in the database.

Complication Layer 3:

The timing of the migration from an old system to a new system is complicated. If the old system is still currently in production and being used every day for review and sharing with the other stakeholders, then the audits and metadata are still being added to the files every day. Down time needs to be accounted for, and the timing of the transition must be mapped out in a clear Statement of Work. Without a well-planned procedure, you may inadvertently miss/drop information. Agencies cannot just stop reviewing and sharing evidence essential to day-to-day operations while migrations are completed. Migrating from on-premises to cloud introduces even more timing issues. This is of course assuming the migration is from a current production environment and not an archive type environment.

If migrating from an archive type situation, (the case has been adjudicated and closed, and the files are stored on secondary physical devices or on a NAS/SAN), then there are other concerns. Questions that need to be answered are: Can the secondary devices (i.e., DVDs, CDs, thumb drives, LTO) playback on hardware that is becoming obsolete? Is the manufacturer even still in business? Do the files names contain metadata and/or the folder names where the files reside? If the files are on a NAS/SAN, are they in a structured or unstructured environment, and were they kept in a folder with a naming convention also containing metadata? This is all

metadata that can be parsed as part of the migration process to capture the maximum amount of historical data on the evidence for search and retrieval.

Complication Layer 4:

Metadata mapping from the old system to the new system is another area that is often overlooked in the planning process. Once the old system's metadata fields (descriptive, administrative, structural) have been identified, the fields will need to be massaged to meet the new system's format. Some important considerations are things like the new system's metadata structure does not handle specific types of metadata (i.e., GPS, triggers), or it may have different field names and they need to be mapped from the old name. What do you do with the metadata that is not supported by the new destination systems?

Complication Layer 5:

Hashing the evidence files before doing anything with them and rehashing the files every step of the way is a complication many applications and Windows based processes do not handle correctly, leaving the agency exposed to future authentication challenges. The first thing that must be done prior to moving/replicating a file, is getting each file hashed and then verified against the old systems' hash. This ensures that the files are both authentic and original. If this step is missed, the file will not be deemed authentic once in the new system, which then introduces the risk of the digital evidence being challenged in court.

More layers of concern:

- Many file types are proprietary or have a proprietary container housing standard media and can only be viewed using the old software platform that you are attempting to migrate from.
- The files are stored in a specific folder structure containing several subfolders along with needed supporting files.
- Zipped up files complicate migration (Zipping Evidence Files: The Good, the Bad and the Ugly)
- The old software's APIs might only support placing the audit trails in a PDF, not into a structure that can be parsed.
- The new software platform does not support prepending the audit trails.
- The new software platform does not support the old metadata structure.
    - For example, GPS information, trigger events such as a light bar or a weapon being drawn
- The new software platform does not support folder structures for complex evidence.
    - For example, 3D crime scene recreation, or Cell Phone or Computer HDD dumps

If anything described above is missed, dropped, can't be verified, or played back, then the risk of the evidence files being challenged in court is inevitable, causing a potential chain reaction for appeals.

There are many reasons why migrations occur. The industry has lacked a simple method for migrations to be successfully achieved that **DWS's Data-Central** addresses properly and affordably. **DWS's Data-Central** is middle-ware specifically written with data migration complications in mind. The **DWS** team not only has the software, but the experience to properly and efficiently deal with these issues. If you are migrating soon and would like a demo or more information on **DWS's Data-Central** product, please **CLICK HERE**.

Dynamicworkflowsolutions.com