
M Caruso
D Krewer
J Mullins
Liz Woolcott

Utah State University

Follow this and additional works at: https://digitalcommons.usu.edu/lib_present

Part of the Library and Information Science Commons

Recommended Citation
Recommending community best practices for metadata in the Digital Preservation Network

A progress report by the DPN Preservation Metadata Standards Working Group: Moriah Caruso, Liz Woolcott, Drew Krewer, Jennifer Mullins
Overview

1. About DPN
3. Current and Future Directions
4. Work Accomplished So Far
5. Challenges Encountered
6. Invitation for Feedback
About DPN
About DPN

- “Dark archive”
- “Redundant and varied technical and legal infrastructure to assure the survival, ownership and management of preserved digital content”
- 50+ charter members, including public and private universities and colleges, consortiums, and digital curation service providers
- Collaborative community
- Members are just starting to deposit content
Preservation Metadata Standards Working Group

- Was created to outline the metadata standards that DPN will follow for preservation.
  - Deliverable 1: Define a set of fields that will remain constant and available with all deposits made into DPN.
  - Deliverable 2: Publish a paper documenting process and relevant work done at other institutions leading to the selection of these standards.
- Started its work in January 2016.
Preservation Metadata Working Group

- Members:
  - Moriah Caruso - University of Washington
  - Drew Krewer - University of Houston
  - Jenny Mullins - Dartmouth College
  - Simon O’Riordan - Emory University
  - Liz Woolcott - Utah State University
  - Dave Pcolar - DPN Staff Liaison
Work Accomplished So Far
Use Case Development

To fulfill the goal of having geographically distributed copies of preservation master files, the Library decides to deposit copies of materials in an off-site dark storage environment, such as the Digital Preservation Network. Once deposited, materials cannot be changed or removed. Files need to be packaged so that, when retrieved—whether in one, twenty or fifty years time—they can be understood, verified and used.

Upon retrieval:

● The content and context of files must be discernable.

● There must be proof that the files are identical to the ones initially deposited.

● It must be possible to render the file's content (through current software or emulation), or relate the file to a migrated version along with documentation of the migration event.
<table>
<thead>
<tr>
<th>Description</th>
<th>UH</th>
<th>Penn State</th>
<th>Emory</th>
<th>USU</th>
<th>UW</th>
<th>Dartmouth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptive</td>
<td>Title</td>
<td>dc:title</td>
<td>Title</td>
<td>Title</td>
<td>Title</td>
<td>dc:title</td>
</tr>
<tr>
<td>Descriptive</td>
<td>Creator</td>
<td>dc:creator</td>
<td>Creator</td>
<td></td>
<td></td>
<td>dc:creator</td>
</tr>
<tr>
<td>Descriptive</td>
<td>Date</td>
<td>dc:date</td>
<td>Date-Source</td>
<td>Date-Source</td>
<td>Date-Digitized; Date-Ba</td>
<td>dc:date; dc:date.accessioned</td>
</tr>
<tr>
<td>Descriptive</td>
<td>Description</td>
<td>dc:description</td>
<td>Description</td>
<td></td>
<td></td>
<td>dc:description</td>
</tr>
<tr>
<td>Descriptive</td>
<td>Subject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dc:subject</td>
</tr>
<tr>
<td>Administrative</td>
<td>Rights</td>
<td>Rights</td>
<td>Rights/Access statement</td>
<td>Rights</td>
<td>Rights</td>
<td>dc:_rights</td>
</tr>
<tr>
<td>Administrative</td>
<td>Access Rights</td>
<td>dc:accessRights</td>
<td>Access Rights</td>
<td>Rights/Access statement</td>
<td>Access Rights</td>
<td>dc:accessRights</td>
</tr>
<tr>
<td>Administrative</td>
<td>Identifier</td>
<td>Identifier</td>
<td>Identifier</td>
<td>Identifier-bagLevel</td>
<td>dc:identifier.uri</td>
<td>External-Identifier</td>
</tr>
<tr>
<td>Administrative</td>
<td>Institutional Identifier</td>
<td>Institutional Identifier</td>
<td>Institutional Identifier</td>
<td>Institutional Identifier</td>
<td></td>
<td>Source-Organization</td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Institution</td>
<td>Institution</td>
<td>Institution</td>
<td>Institution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Content Type</td>
<td>Content Type</td>
<td>Type</td>
<td></td>
<td></td>
<td>mimetype/format</td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Formats</td>
<td>Format</td>
<td></td>
<td></td>
<td></td>
<td>mimetype/format</td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Format-Extent</td>
<td>Format-Extent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Associated Items</td>
<td>Identifier-associatedIdentifiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical</td>
<td>Filenames</td>
<td>Filenames</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical</td>
<td>Checksum</td>
<td>Checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descriptive/Administrative</td>
<td>Relation-IsPartOf</td>
<td>Relation-IsPartOf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative</td>
<td>Bagged by</td>
<td>Bagged by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative</td>
<td>Uploaded by</td>
<td>Uploaded by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bag-info.txt</td>
<td>Size</td>
<td>Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bae-info.txt</td>
<td>Organization Address</td>
<td>Organization Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DPN Bag-It Specification Amendment

- Member institution was creating metadata being stored as tag files.
- BagIt File Packaging Format Spec (V0.97) allows for “other tag files”:
  - 2.2.4. Other Tag Files: A bag MAY contain other tag files that are not defined by this specification. **Implementations SHOULD ignore the content of any unexpected tag files, except when they are listed in a tag manifest.** When unexpected tag files are listed in a tag manifest, implementations MUST only treat the content of those tag files as octet streams for the purpose of checksum verification.
- Decision that optional, member-created tag files must be listed in the tag manifest to ensure checksum is recorded.
Current & Future Directions
Current Directions

University of Washington:

A tale of “lost files and mixed blessings”
Metadata:

Preservation gathers:
- Collection-level marc record
- EAD finding aid
- Item level metadata from access systems
- Rights data, donor agreements, supplementary info

Preservation creates: Archivematica-produced METS file with technical metadata
Current Directions

Dartmouth College

Working with what we’ve got
Future Directions

- **Case Study**
  - Finalize core record
  - Evaluate if there are additional ways we can help the membership
Future Directions

- **Focus group**
  - Representative sample of institutions
  - Analyze metadata needs, uses, and workflows
  - Gather feedback
Future Directions

- **Final Deliverables**:
  - Recommendations/best practices for DPN metadata record
  - Toolkit for partners to use
  - Paper outlining the outcomes of the project
Feedback?

- jennifer.l.mullins@dartmouth.edu
- dave@dpn.org
- neilsm@uw.edu
- ajkrewer@uh.edu
- liz.woolcott@usu.edu