VINTAGE FORENSICS

WRANGLING HFS METADATA INTO DFXML

DIANNE DIETRICH • CORNELL UNIVERSITY LIBRARY
@SMALLANDMATH • DD388@CORNELL.EDU
CURATE GEAR 2016 • JANUARY 14, 2016

HOW THIS BEGAN

2013—2015 NEH funded grant to preserve New Media Art

- Translation: CD-ROMs from 1990s—early 2000s
- Also: Artists really like Apple computers

February 2013, first Advisory Board meeting:

“The Sleuth Kit doesn’t support HFS.”

METADATA STRATEGY

1. Determine requirements

2. Look for tools

MORE METADATA STRATEGY

- **For every file system present on an individual disk image**
  - Include file name and basic metadata (i.e., size, creation date, basic identification, etc.)

This sounds a lot like DFXML

EVEN MORE METADATA STRATEGY

Additional namespace and elements

- `hfstype_creator`
- `hfsrsrcsize`
- `hfslocked`
- `hfsflags`

THE CHALLENGE

“The Sleuth Kit doesn’t support HFS.”

- **So one tool can’t do everything**
- **But we have some pieces**
  - disktype to identify file systems
  - TSK for ISO9660
  - hfsutils for HFS

THE CODE

Python wrapper around hfsutils

- **https://github.com/cul-it/hfs2dfxml**

Want to help?

- **Set** `DEBUG = True` **and let's make it happen**