Toward a Digital Acquisition Learning Laboratory

Cal Lee

School of Information and Library Science

University of North Carolina, Chapel Hill

Computer Forensics and Cultural Heritage Meeting

May 14-15, 2010

College Park, MD

UNC
SCHOOL OF INFORMATION
AND LIBRARY SCIENCE

Human activities leave traces

Doors left open

Footprints in the sand

Receipts

Browser cache contents

Temp files

Headers of IP packets

Pixels on the screen of a GPS device

Voice mail messages

Flight prices on an airline web site

All of the traces can convey information

The vast majority of traces only play a role in their immediate context & then disappear

But sometimes we want the traces
to stick around for a while.

Collecting institutions have been in the business of caring for traces for a very long time.

The traces within their care come in clusters:

All the "data elements" of a print document stick together.

The front matter of a book is kept with the book's main payload.

Professionals focus heavily on the integrity of aggregates: collections, fonds, series, files, items, archival information collections, archival information packages.

With digital traces, all of the above considerations apply, but…

There are a lot more digital traces.

They're often highly distributed:

Across networks

Across systems

Across various data stores on a given computer

Users of computer systems encounter the traces in the form of files and documents.

They don't attend directly to the various bits and pieces.

Most cultural heritage professionals are also used to dealing with the file and document level in their everyday lives.

So how do you acquire "personal papers" from a floppy disk?

That's easy…

Right-click

Copy

Paste

This approach risks violating the integrity of materials and losing valuable metadata.

Digital forensics has established principles, technologies and methods for extracting data and associated metadata.

Two streams of activity show great promise for informing the practices of collecting institutions.

(1) a handful of innovative projects of collecting institutions exploring the application of digital forensics to acquisition

(2) vendors and academic programs providing digital forensics training, primarily focused on the preparation of law enforcement officers and criminal investigators

There's currently no mechanism for connecting these two streams of activity.

The Digital Acquisition Learning Laboratory (DALL) project at UNC SILS – funded by the Mellon Foundation - is designed to make these connections.

We'll create, administer and implement a learning laboratory for the application of digital forensics to the acquisition of digital materials.

This includes training, hardware and software for running practical exercises within courses.

Big Goals:

- Translation – established industry models, methods, techniques and resources into forms that are appropriate to information professionals

- Capacity building – training of the trainers, sustainable computer lab arrangements, incorporation into ongoing curriculum, collaboration with collecting-institution partners

Big Questions:

- Which features of the software (using EnCase and FTK in this phase) will be most useful for digital acquisition training?

- What do they need to know to make the right decisions about applying the tools appropriately in collecting contexts?

- How much and what types of adaptation are require in making the translation from the industry's target audience to the cultural heritage audience?

Thank you!