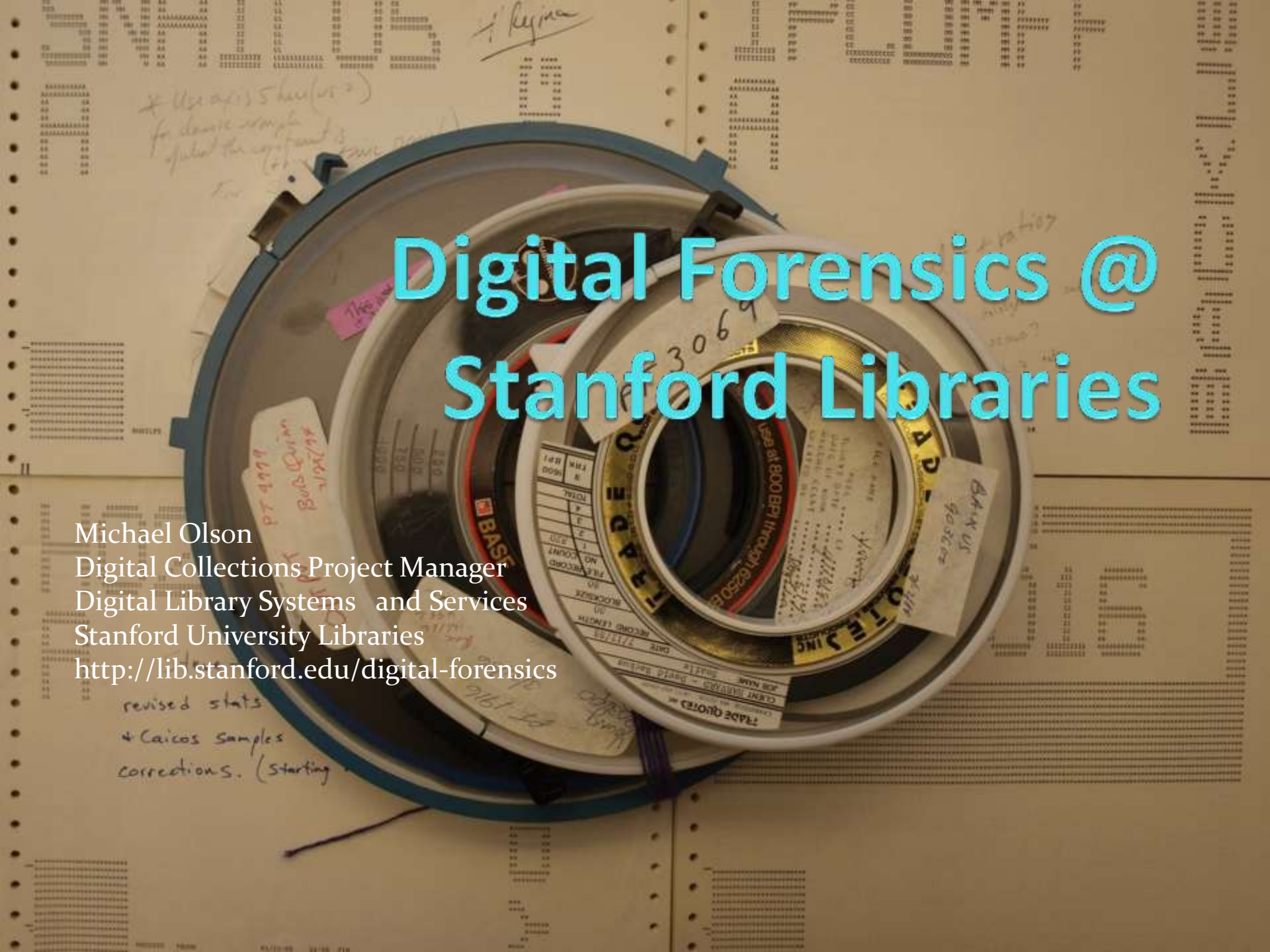


# Digital Forensics @ Stanford Libraries

Michael Olson
Digital Collections Project Manager
Digital Library Systems and Services
Stanford University Libraries
http://lib.stanford.edu/digital-forensics

# Digital Forensics @ Stanford Libraries

- Born Digital Collections
- Digital Forensics Lab
- Evaluation of Forensic Software
- Challenges

# Digital Forensics @ Stanford Libraries

- ~ 18,000 pieces of digital media
- at risk of permanent loss

| | |
|---|---|
| Stephen Cabrinety | Software |
| Robert Creeley Papers | Documents |
| Stephen Jay Gould Papers | Documents |
| Peter Koch – Fine Art Press | Graphics |
| Xanadu Project Collection – | Hypertext |

# Digital Forensics @ Stanford Libraries

Digital Forensics Lab

- 2 Forensic Recovery of Evidence Devices (workstation and laptop)
- 2 Catweasels (floppy disk controller cards)
- Multiple 3 ½”, 5 ¼”, tape, Zip drives
- Copy stand, SLR digital camera
- Assorted write blockers


FRED
Digital Intelligence
Digital Intelligence
Digital Intelligence
DELL

# Digital Forensics @ Stanford Libraries

Forensic Imaging Statistics

- 139 forensically imaged (media creation dates 1990-1995)
- 5 ¼" and 3 ½" diskettes
- 3.7% failure rate (bad sectors)
- 2.3% unable to image – hardware incompatibility

# Digital Forensics @ Stanford Libraries

Software in the Lab

- FTK imager
- Forensic toolkit (FTK) version 3.1.1
- EnCase Forensic version 6.14
- DROID (Digital Record Object Identification)
- Sleuth Kit
- many others.....

# Digital Forensics @ Stanford Libraries

Software Evaluation Criteria

- Skills / training is required
- Cost
- Open Source / Commercial
- Feature set
- Supported file formats and metadata outputs
- Suitability for lab tasks (forensic imaging or analysis)

# Tool Matrix

Edit Add Tools

1 Added by Michael Olson, last edited by Peter Chan on Mar 29, 2010 (view change)

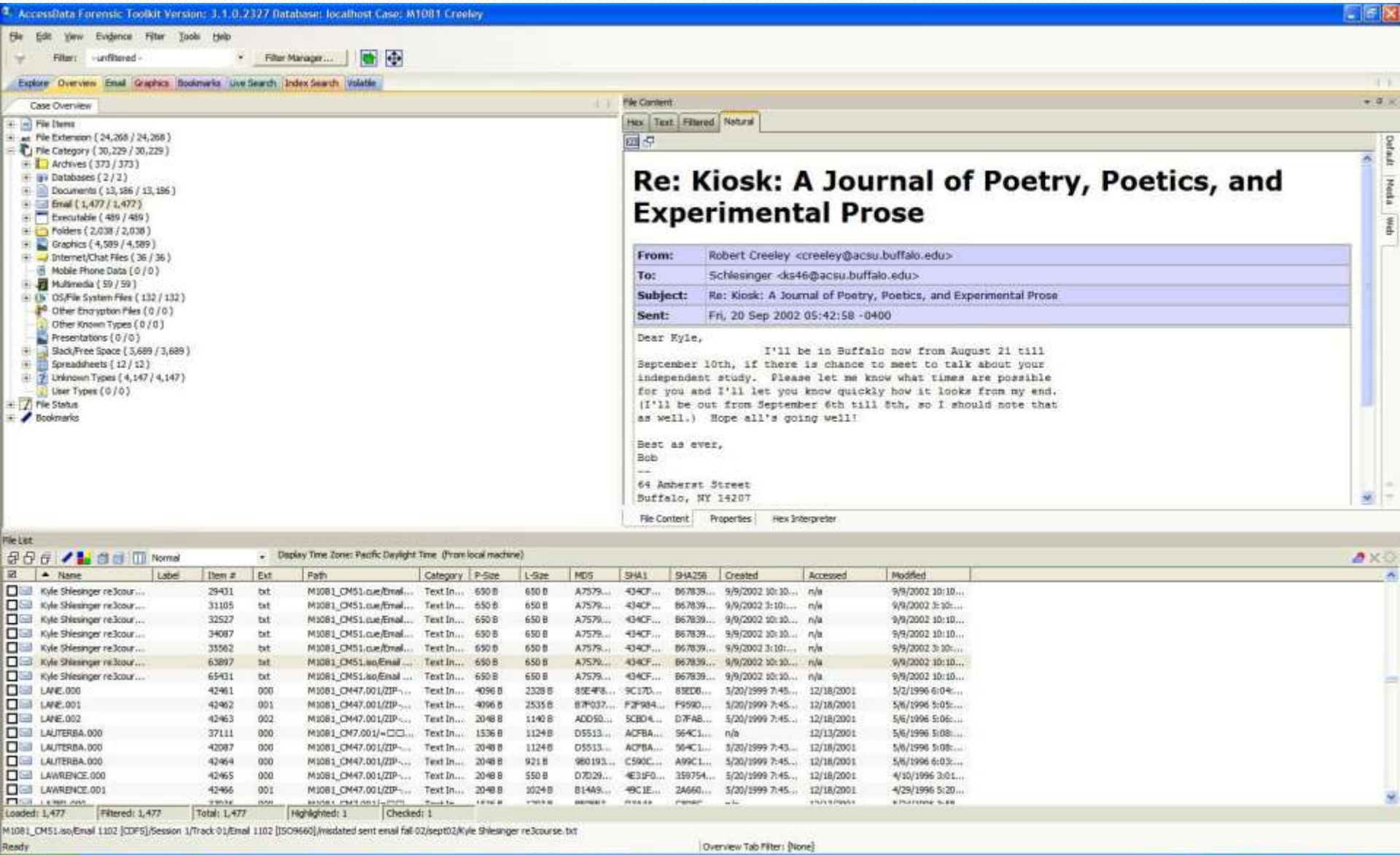
## Digital Archiving Software Tool Matrix

| Tools Name | Description | Pros | Cons | URL | Additional Information |
|---|---|---|---|---|---|
| Hydra (Fedora) | Access repository (Delivery, discovery and participatory system) / Controlled patrons participation | • In-house | | | Access |
| BlueHarvest | Removes DS_Store files, ._ AppleDouble files and hidden folders such as .Trashes from file servers, etc created by Mac | • easy to use | • cost | • URL | Access |
| Many Eyes | Visualization of dataset | • another way to analysis text | | • URL | Access |
| SIMILE - Timeline | Timeline generator | | | | |
| Windows Search 4.0 | Create a full text search envir for MS Office, PDF, Plain text | | | | |
| Camera Control Pro 2 | Enables remote control of ma digital SLR functions from a p computer | | | | |

Gmail - Inbox (13) - glynnedw@gm... | Zimbra: Inbox (38) | Tool Matrix - AIMS - Consul (confl...

| | | | | | |
|---|---|---|---|---|---|
| | | • disk format<br>• designed to work with Catweasel allowing one to image older floppy media | | | |
| The Collaborative Electronic Records Project | Email attachment format analyzer | • free | | • URL | Accession |
| FTK Imager 2.6.1 | Windows based forensic imager that is easy to use | • creates csv file listing that is useful for analysis by digital archivist<br>• creates .txt metadata file including checksums of imaging process | • windows GUI is easy to use<br>• proprietary (not sharable code)<br>• Windows only | • URL<br>• Manual | Accession / Curation |
| FTK Imager Lite version 2.6.1 | Stripped down Windows based forensic imager designed to work off a memory stick | • useful for forensic imaging on machines that are already on | • windows GUI is easy to use<br>• proprietary (not sharable code)<br>• Windows only | • URL | Accession / Curation |
| EnCase Forensic 6.0 | Comprehensive set of forensic utilities | • GUI | • cost | • URL | Accession / Curation |
| FTK 2.0 | Comprehensive set of forensic utilities | • GUI | • cost | • URL | Accession / Curation |
| Sleuth Kit | Forensic analysis tools | • open source | • linux only | • URL | Accession / |

# FTK: Forensic Toolkit
# Creeley email diskette



# Digital Forensics @ Stanford Libraries

Preliminary Findings

- Software requires specialized training
- Tool selection depends upon collection

# Digital Forensics @ Stanford Libraries

Challenges

- Hardware obsolescence (finding the right drive)
- Validation of forensic images?
- Prioritizing and increasing lab throughput
- Methods for describing born digital collections
- Preservation

# Virtual Machine for Gould Word Perfect document