# Digital Forensics @ Stanford Libraries: Why we have FRED and why you don't need one?

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 at Stanford
- Preservation – retaining provenance
- Meet FRED – Forensic Recover of Evidence Device
- Disk Imaging
- Demonstration of Disk Imaging
- Next Steps – a challenge!

# 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

- Born Digital Collections at risk from:

- Media Obsolescence
- Bit Rot
- Software Obsolescence

# Digital Forensics @ Stanford Libraries

- Preservation Strategy

- Move the bits off at risk media
- Back up data

# Digital Forensics @ Stanford Libraries

- Methods for Migrating Data off Digital Media

1. Copy data using your OS
2. Disk Image – bit copy

# Digital Forensics @ Stanford Libraries

What happens to provenance if you do Option 1?

- creation dates change
- context of moved data changes – relationships between files
- file metadata / permissions for data can change

# Digital Forensics @ Stanford Libraries

Option 2, Disk Imaging – what is it?

- bit perfect copy of source data – exact copy
- provenance of data does not change – creation dates, permissions, relationships between files & original OS
- technique used by law enforcement for investigations

# Digital Forensics @ Stanford Libraries

Stanford's Solution – The Digital Forensics Lab

- 2 FREDS - Forensic Recovery of Evidence Devices (workstation and laptop)
- 2 Catweasels (floppy disk controller cards)
- Multiple 3 ½", 5 ¼", tape, Zip drives
- Copy stand, digital camera photograph media
- Assorted write blockers
- Forensic software for disk image capture/analysis


FRED
Digital Intelligence
Digital Intelligence
Digital Intelligence
DELL

# Digital Forensics @ Stanford Libraries

Not all archives need a FRED to do this!

- computer to read the media / run software
- software is freely available to create disk images
- write blockers are inexpensive

# Digital Forensics @ Stanford Libraries

Computers

- still many windows machines available that can run a less modern OS (win xp)
- get a machine that has floppy disk controller chip (<2005)
- collect or retain old drives (5 ¼", zip)

# Digital Forensics @ Stanford Libraries

Forensic Imaging Software

- many commercial and open source solutions available for free:
  - Sluethkit
  - FTK imager ™
  - many others….
  -

# Digital Forensics @ Stanford Libraries

Write Blockers

- hardware to prevent computer from writing to the media
- many types of write blockers
- built into 3 1/2” and 5 1/4” diskettes
- cheap – typically $100-300

# Digital Forensics @ Stanford Libraries

What Does this all mean?

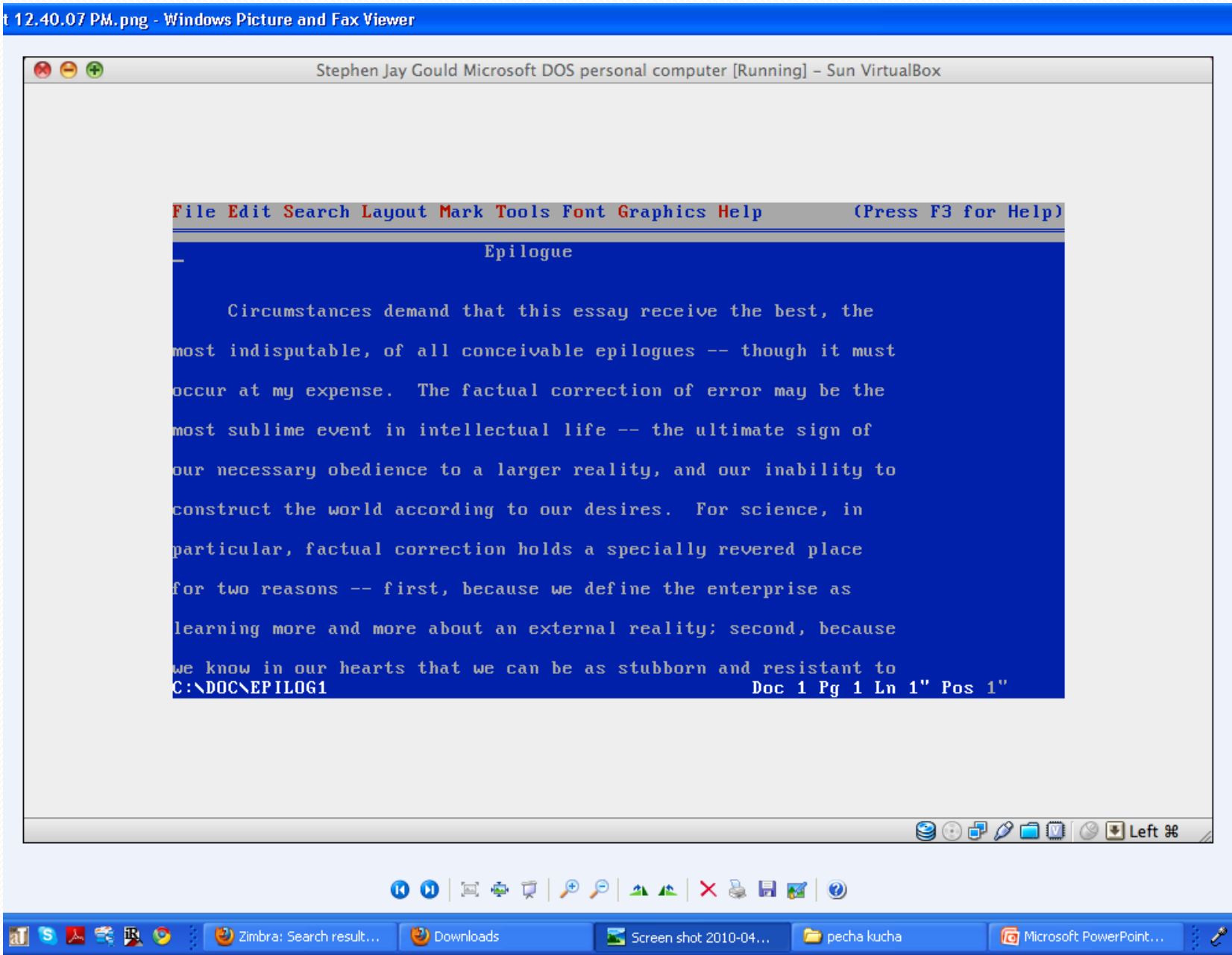
- any archive can get started – at a minimum get the data off old media
- inexpensive
- technically feasible in small archive

# Digital Forensics @ Stanford Libraries

Challenge

- don't wait, get started now!
- stop just boxing and forgetting media
- set up regional centers of expertise focusing on:
  - Media types
  - Technical specialties such as analysis
-

# Virtual Machine for Gould Word Perfect document



# Digital Forensics @ Stanford Libraries

Contact:

Michael Olson, Digital Collections Project Manager
mgolson@stanford.edu
Blog: http://lib.stanford.edu/digital-forensics