

Digital Forensics @ Stanford Libraries

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

revised stats
+ Caicos samples
corrections. (starting



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
- Robert Creeley Papers
- Stephen Jay Gould Papers
- Peter Koch – Fine Art Press
- Xanadu Project Collection –

Software
Documents
Documents
Graphics
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 1/2", 5 1/4", tape, Zip drives
- Copy stand, SLR digital camera
- Assorted write blockers



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)



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	<ul style="list-style-type: none"> In-house 			Access
BlueHarvest	Removes DS_Store files, ._ AppleDouble files and hidden folders such as .Trashes from file servers, etc created by Mac	<ul style="list-style-type: none"> easy to use 	<ul style="list-style-type: none"> cost 	<ul style="list-style-type: none"> URL 	Access
Many Eyes	Visualization of dataset	<ul style="list-style-type: none"> another way to analysis text 		<ul style="list-style-type: none"> URL 	Access

SIMILE - Timeline	Timeline generator
Windows Search 4.0	Create a full text search envin for MS Office, PDF, Plain text
Camera Control Pro 2	Enables remote control of ma digital SLR functions from a p computer

Tools Name	Description	Pros	Cons	URL	Additional Information
			<ul style="list-style-type: none"> disk format designed to work with Catweasel allowing one to image older floppy media 		
The Collaborative Electronic Records Project	Email attachment format analyzer	<ul style="list-style-type: none"> free 		<ul style="list-style-type: none"> URL 	Accession
FTK Imager 2.6.1	Windows based forensic imager that is easy to use	<ul style="list-style-type: none"> creates csv file listing that is useful for analysis by digital archivist creates .txt metadata file including checksums of imaging process 	<ul style="list-style-type: none"> windows GUI is easy to use proprietary (not sharable code) Windows only 	<ul style="list-style-type: none"> URL Manual 	Accession / Curation
FTK Imager Lite version 2.6.1	Stripped down Windows based forensic imager designed to work off a memory stick	<ul style="list-style-type: none"> useful for forensic imaging on machines that are already on 	<ul style="list-style-type: none"> windows GUI is easy to use proprietary (not sharable code) Windows only 	<ul style="list-style-type: none"> URL 	Accession / Curation
EnCase Forensic 6.0	Comprehensive set of forensic utilities	<ul style="list-style-type: none"> GUI 	<ul style="list-style-type: none"> cost 	<ul style="list-style-type: none"> URL 	Accession / Curation
FTK 2.0	Comprehensive set of forensic utilities	<ul style="list-style-type: none"> GUI 	<ul style="list-style-type: none"> cost 	<ul style="list-style-type: none"> URL 	Accession / Curation
Sleuth Kit	Forensic analysis tools				Accession /

FTK: Forensic Toolkit

Creeley email diskette

AccessData Forensic Toolkit Version: 3.1.0.2327 Database: localhost Case: M1081 Creeley

File Edit View Evidence Filter Tools Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview

- File Items
- File Extension (24,268 / 24,268)
- File Category (30,229 / 30,229)
- Archives (373 / 373)
- Databases (2 / 2)
- Documents (13,186 / 13,186)
- Email (1,477 / 1,477)
- Executable (489 / 489)
- Folders (2,038 / 2,038)
- Graphics (4,589 / 4,589)
- Internet/Chat Files (36 / 36)
- Mobile Phone Data (0 / 0)
- Multimedia (59 / 59)
- OS/File System Files (132 / 132)
- Other Encryption Files (0 / 0)
- Other Known Types (0 / 0)
- Presentations (0 / 0)
- Stack/Free Space (3,689 / 3,689)
- Spreadsheets (12 / 12)
- Unknown Types (4,147 / 4,147)
- User Types (0 / 0)

File Content

Hex Text Filtered Natural

Re: Kiosk: A Journal of Poetry, Poetics, and Experimental Prose

From: Robert Creeley <creeley@acsu.buffalo.edu>
To: Schlesinger <ks46@acsu.buffalo.edu>
Subject: Re: Kiosk: A Journal of Poetry, Poetics, and Experimental Prose
Sent: Fri, 20 Sep 2002 05:42:58 -0400

Dear Kyle,

I'll be in Buffalo now from August 21 till September 10th, if there is chance to meet to talk about your independent study. Please let me know what times are possible for you and I'll let you know quickly how it looks from my end. (I'll be out from September 6th till 8th, so I should note that as well.) Hope all's going well!

Best as ever,
Bob

64 Amherst Street
Buffalo, NY 14207

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: Pacific Daylight Time (from local machine)

Item #	Name	Label	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
29431	Kyle Schlesinger re3cour...		txt	M1081_CM51.cue/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 10:10...	n/a	9/9/2002 10:10...
31105	Kyle Schlesinger re3cour...		txt	M1081_CM51.cue/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 1:10...	n/a	9/9/2002 1:10...
32527	Kyle Schlesinger re3cour...		txt	M1081_CM51.cue/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 10:10...	n/a	9/9/2002 10:10...
34087	Kyle Schlesinger re3cour...		txt	M1081_CM51.cue/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 10:10...	n/a	9/9/2002 10:10...
35562	Kyle Schlesinger re3cour...		txt	M1081_CM51.cue/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 3:10...	n/a	9/9/2002 3:10...
63897	Kyle Schlesinger re3cour...		txt	M1081_CM51.iso/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 10:10...	n/a	9/9/2002 10:10...
65431	Kyle Schlesinger re3cour...		txt	M1081_CM51.iso/Email...	Text In...	650 B	650 B	A7579...	434CF...	867839...	9/9/2002 10:10...	n/a	9/9/2002 10:10...
42461	LANE.000		000	M1081_CM47.001/ZIP...	Text In...	4096 B	2328 B	85E4F8...	3C17D...	83ED8...	5/20/1999 7:45...	12/18/2001	5/2/1996 6:04...
42462	LANE.001		001	M1081_CM47.001/ZIP...	Text In...	4096 B	2535 B	87F037...	F2F984...	F9990...	5/20/1999 7:45...	12/18/2001	5/6/1996 5:05...
42463	LANE.002		002	M1081_CM47.001/ZIP...	Text In...	2048 B	1140 B	A0D50...	5CB04...	D7FAB...	5/20/1999 7:45...	12/18/2001	5/6/1996 5:06...
37111	LAUTERBA.000		000	M1081_CM7.001/...	Text In...	1536 B	1124 B	D5513...	ACFBA...	964C...	n/a	12/13/2001	5/6/1996 5:08...
42087	LAUTERBA.000		000	M1081_CM47.001/ZIP...	Text In...	2048 B	1124 B	D5513...	ACFBA...	964C...	5/20/1999 7:45...	12/18/2001	5/6/1996 5:08...
42464	LAUTERBA.000		000	M1081_CM47.001/ZIP...	Text In...	2048 B	921 B	980193...	C590C...	A99C1...	5/20/1999 7:45...	12/18/2001	5/6/1996 6:03...
42465	LAWRENCE.000		000	M1081_CM47.001/ZIP...	Text In...	2048 B	550 B	D7029...	4E31F0...	359754...	5/20/1999 7:45...	12/18/2001	4/30/1996 3:01...
42466	LAWRENCE.001		001	M1081_CM47.001/ZIP...	Text In...	2048 B	3024 B	B14A8...	49C1E...	24660...	5/20/1999 7:45...	12/18/2001	4/29/1996 5:20...

Loaded: 1,477 Filtered: 1,477 Total: 1,477 Highlighted: 1 Checked: 1

M1081_CM51.iso/Email [102] [CDF5] [Session 1/Track 9]/Email [102] [ISO9660]/mediated sent email fail 02/sep02/Kyle Schlesinger re3course.txt

Ready Overview Tab Filter: [None]

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

t 12.40.07 PM.png - Windows Picture and Fax Viewer

