From 0 to 1: On becoming a digital forensics 1100 practitioner 0001100010111000 0001100000001110

> Christie Peterson Records Management & Digital Archivist The Johns Hopkins University Society of American Archivists 15 August 2014

"<u>Happy Binary Day</u>" by <u>EJP Photo</u>, used under <u>CC BY-NC-SA 2.0</u>



# Introduction



"<u>Happy Binary Day</u>" by <u>EJP Photo</u>, used under <u>CC BY-NC-SA 2.0</u>



"<u>All these choices...</u>" by <u>Örjan Mattsson</u>, used under <u>CC BY-NC-SA</u>



# Formal Education



# Digital Archives Specialist

Society of American Archivists CERTIFICATE OF CONTINUING EDUCATION

#### Christie S. Peterson

has been awarded 0.75 continuing education units and 5 section: B.3.c archival recertification credits upon successful completion of

DIGITAL FORENSICS FOR ARCHIVISTS

New York, New York

Nancy P. Draumour

Nancy Perkin Beaumont, Executive Director



June 29, 2012

Date



# A Reading Assignment

	Search Site	Submit ->		Connect login 🗲
Council on			Username (email)	Forgot password?
Library and	Password			
Resources Home Abou	Initiatives & Partners	hips Publicat	ions DLF Awards & Fello	wships Connect

#### Publications

Reports

Ruminations

CLIR Issues

Annual Report

Archives

Other Resources

Ordering Report Prints

Home / Publications / Reports / pub149

#### Abstract

#### Digital Forensics and Born-Digital Content in Cultural Heritage Collections

by Matthew G. Kirschenbaum, Richard Ovenden, Gabriela Redwine with research assistance from Rachel Donahue

December 2010. 93 pp. \$25 ISBN 978-1-932326-37-6 CLIR pub149

#### PDF Download of Complete Report (1 MB file) >>

While the purview of digital forensics was once specialized to fields of law enforcement, computer security, and national defense, the increasing ubiquity of computers and electronic devices means that digital forensics is now used in a wide variety of cases and circumstances. Most records today are born digital, and libraries and other collecting institutions increasingly receive computer storage media as part of their acquisition of "papers" from writers, scholars, scientists, musicians, and public figures. This poses new challenges to librarians, archivists, and curators—challenges related to accessing and

preserving legacy formats, recovering data, ensuring authenticity, and maintaining trust. The methods and tools developed by forensics experts represent a novel approach to these demands. For example, the same forensics software that indexes a criminal suspect's hard drive allows the archivist to prepare a comprehensive manifest of the electronic files a donor has turned over for accession.

This report introduces the field of digital forensics in the cultural heritage sector and explores some points of convergence between the interests of those charged with collecting and maintaining born-digital cultural heritage materials and those charged with collecting and maintaining legal evidence.



**Digital Forensics and** 



# Getting Your Hands Dirty



# BitCurator











# Digging Deeper



# A Necessary First Step

#### Command line makes me feel cool — bash — 80×24

SonyML/bin-debug/assets/icons/icon-medialife-24.png SonyML/bin-debug/assets/icons/icon-medialife-16.png SonyML/bin-debug/assets/player shell new old.png SonyML/bin-debug/main.css SonyML/bin-debug/SonyML-app.xml SonyML/bin-debug/com SonyML/bin-debug/com/adobe SonyML/bin-debug/com/adobe/xml SonyML/bin-debug/com/adobe/xml/syndication SonyML/.actionScriptProperties SonyML/.settings SonyML/.settings/org.eclipse.core.resources.prefs gohub/settings/config.php.sample gohub/includes/includes.php gohub/api/viddler gohub/api/viddler/xmlparser.php gohub/api/viddler/phpviddler.php gohub/api/viddler/php5viddler.php gohub/new albums.php sony/setup.php sony/index.php sony/setup/import.php Updated to revision 6907. Travzi-17:client travis\$ mate

Å.

Å

Å,

Å

А

Å,

А,

A

Å,

A

Å.

Å

U

Ш

Å,

Å

A

Å,

Å,

U U

### http://cli.learncodethehardway.org/book/

# The Command Line Crash Course

This book is a quick super fast course in using the command line. It is intended to be done rapidly in about a day or two, and not meant to teach you advanced shell usage.

# **Table Of Contents**

- Preface
- · Introduction: Shut Up And Shell
- The Setup
- · Paths, Folders, Directories (pwd)
- · What's Your Computer's Name? (hostname)
- Make A Directory (mkdir)
- Change Directory (cd)
- List Directory (Is)
- · Remove Directory (rmdir)
- Moving Around (pushd, popd)



# ubuntu





# DIGITAL FORENSICS WITH OPEN SOURCE TOOLS

Cory Altheide Harlan Carvey



"This is the foundation book for file system analysis. Brian Carrier has done what needed to be done for this field."

—From the Foreword by **Mark M. Pollitt**, President, Digital Evidence Professional Services, Inc., and Retired Director of the FBI's Regional Computer Forensic Laboratory Program

## FILE SYSTEM FORENSIC ANALYSIS



BRIAN CARRIER



# Expanding Your Skills







#### GitHub

📋 anarchivist / fiwalk-dgi

#### Plugins for fiwalk to run processes against files contained within disk images

🕝 32 commits	₽ 3 branches	⊗ 0 releases	P contributors
ប្រា 🕼 branch: master 🗸	fiwalk-dgi / +		E
chmod +x			
anarchivist authored on No	v 27, 2013		latest commit 9b7fa1dd99 🕏
python	chmod executable scripts +x		10 months ago
Tuby	chmod executable scripts +x		10 months ago
	Add license		11 months ago
README.md	Merge branch 'upgrade-and-refactor'		11 months ago
ficonfig.txt	ficonfig.txt: add to git		2 years ago
walkify	chmod +x		9 months ago
walkify.parallel	chmod +x		9 months ago

(2)



"<u>All these choices...</u>" by <u>Örjan Mattsson</u>, used under <u>CC BY-NC-SA</u>