Revisiting Digital Forensics Workflows in Collecting Institutions

Martin Gengenbach

Digital Preservation 2014

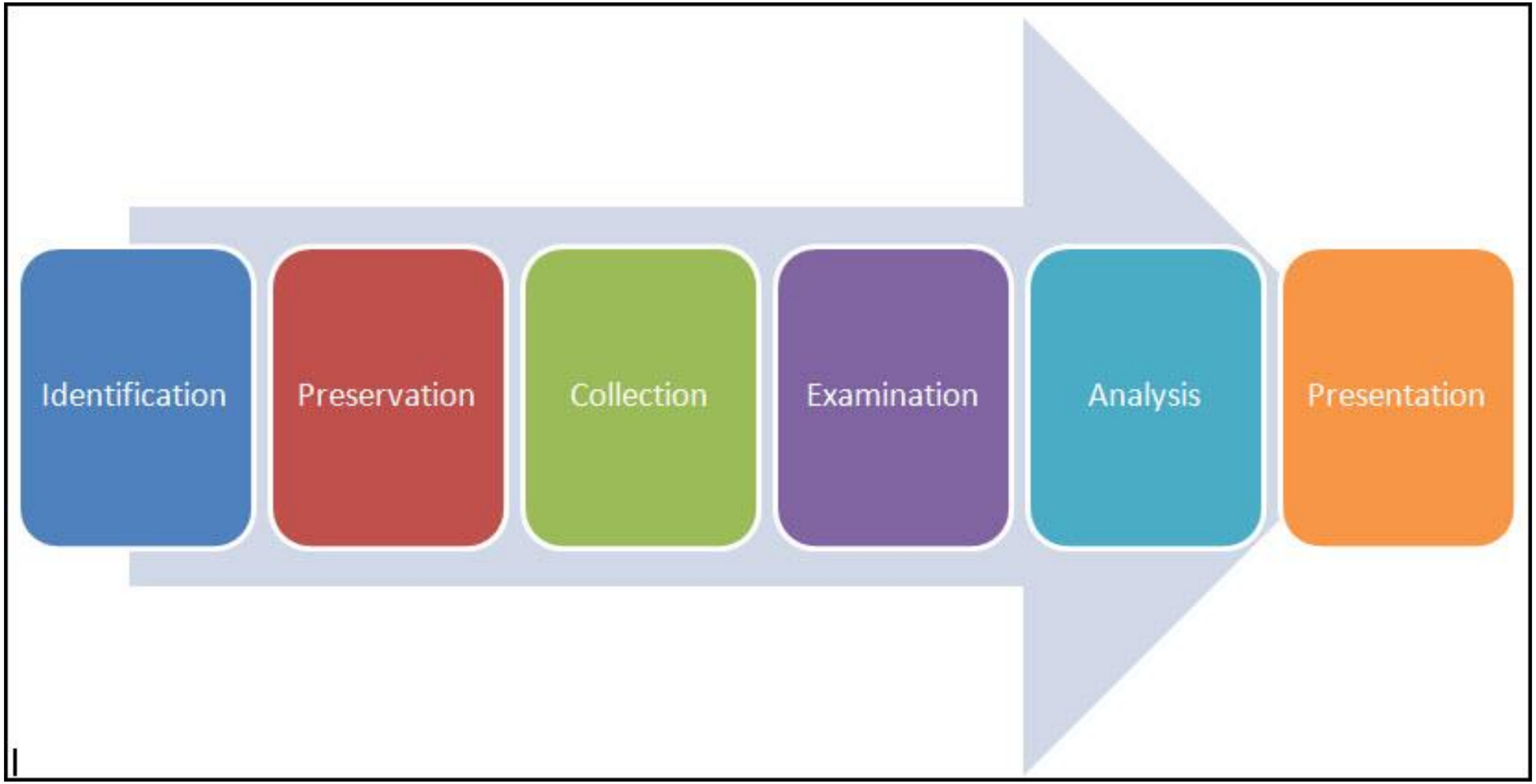
July 22, 2014

Washington Marriot Georgetown, Washington DC

Background

"Floppy disk 2009 G1" by George Chernilevsky https://commons.wikimedia.org/wiki/File:Floppy_disk_2009_G1.jpg#mediaviewer/File:Floppy_disk_2009_G1.jpg

Digital forensics refresher



http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html

Agenda

- "The Way We Do It Here": Mapping Digital Forensics Workflows in Collecting Institutions (2012)
- Revisiting Digital Forensics Workflows in Collecting Institutions:
  the 2014 update
- Conclusions
- Recommendations

“The Way We Do It Here”: Mapping Digital Forensics Workflows in Collecting Institutions

LIBRARY OF CONGRESS

Yale UNIVERSITY

NATIONAL LIBRARY OF AUSTRALIA

Duke UNIVERSITY

MITH MARYLAND INSTITUTE FOR TECHNOLOGY IN THE HUMANITIES

CITY OF VANCOUVER

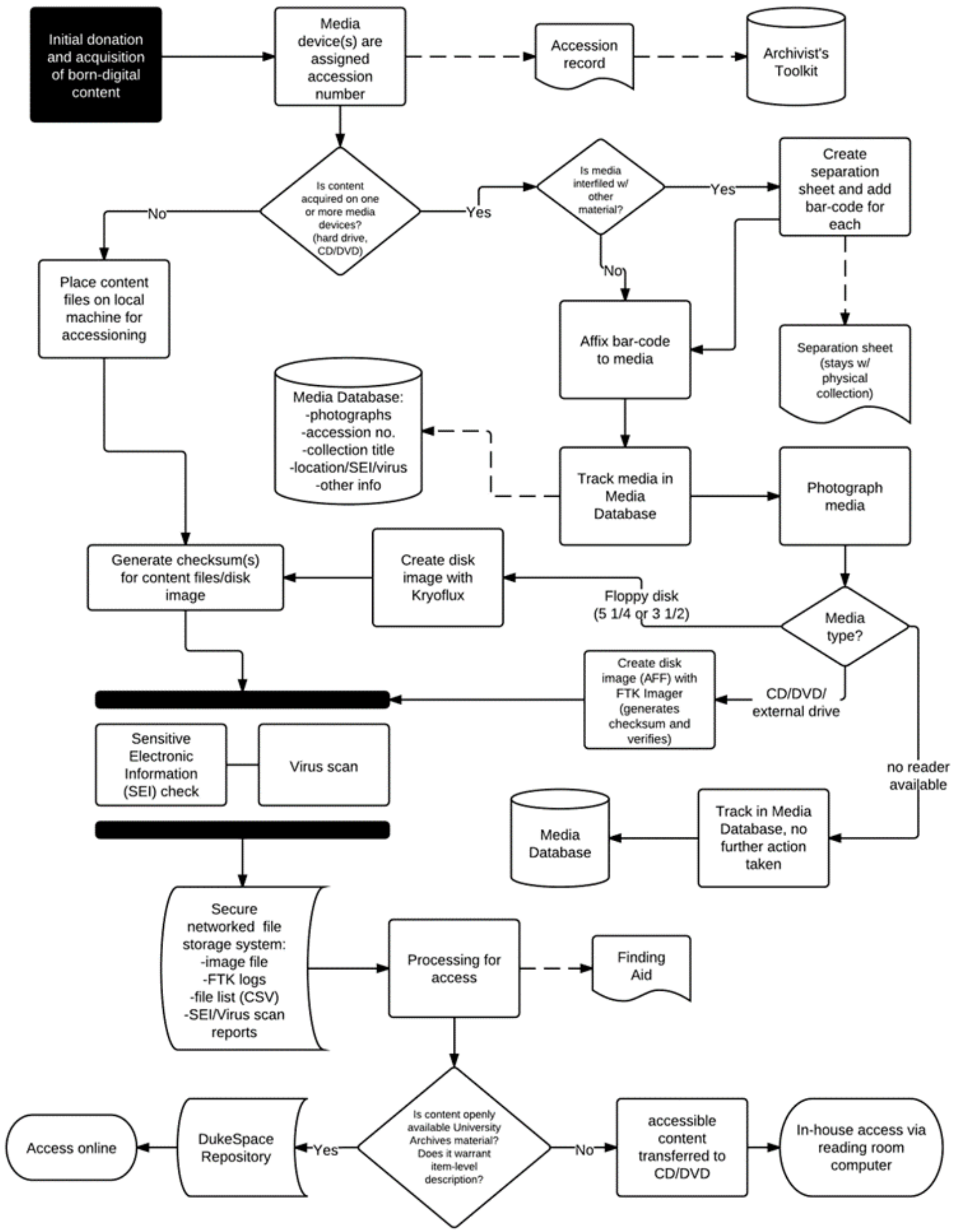
UNIVERSITY of VIRGINIA

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

“The Way We Do It Here”: Analysis

Gengenbach, Martin J. “‘The Way We Do it Here:’ Mapping Digital Forensics Workflows in Collecting Institutions.” A Master’s Paper for the M.S. in L.S degree. August, 2012.

Duke University Archives, born-digital content workflow, June 2012

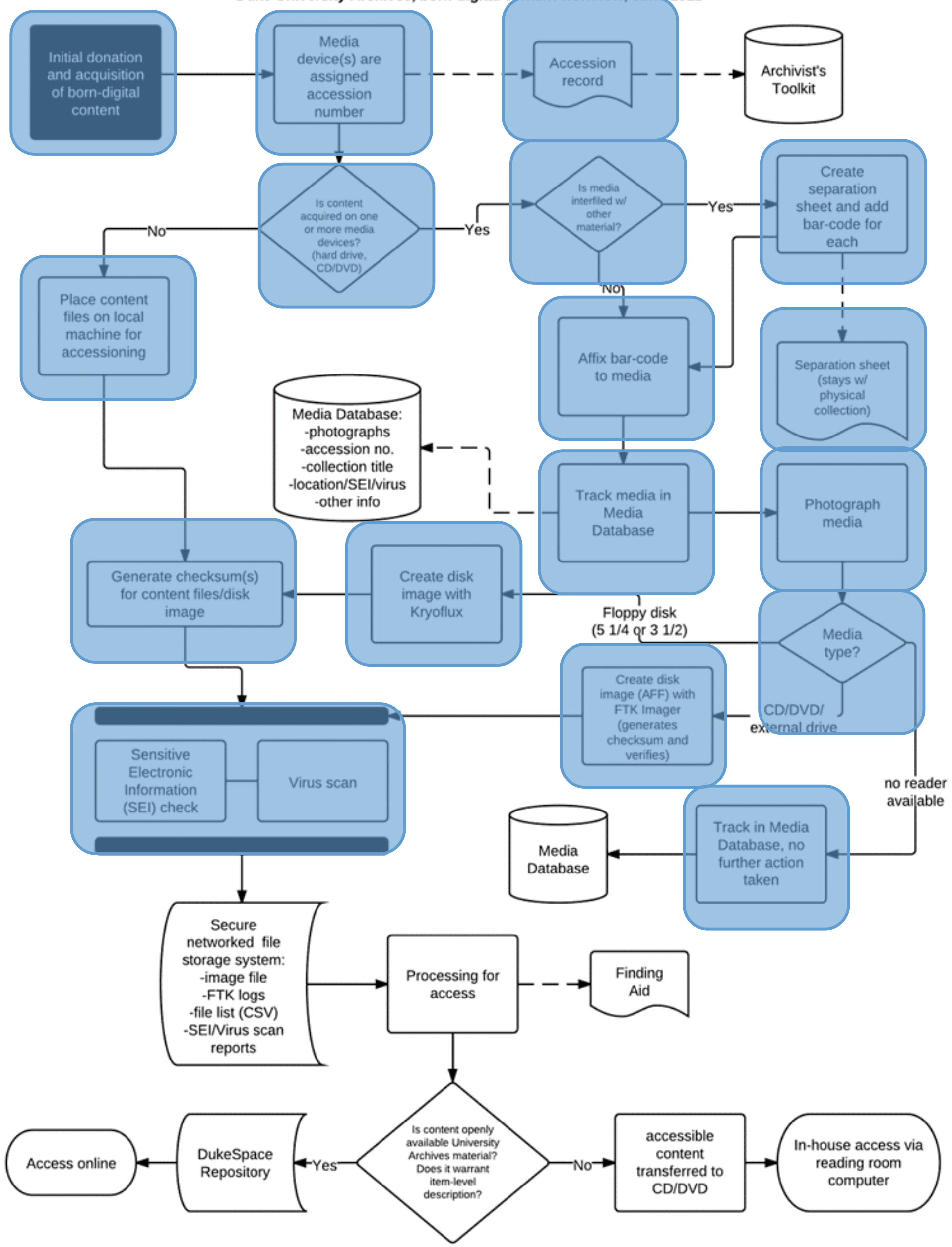


Initial donation and acquisition of born-digital content
Media device(s) are assigned accession number
Accession record
Archivist's Toolkit
Is content acquired on one or more media devices? (hard drive, CD/DVD)
No
Yes
Is media interfiled w/ other material?
Yes
No
Create separation sheet and add bar-code for each
Separation sheet (stays w/ physical collection)
Place content files on local machine for accessioning
Affix bar-code to media
Media Database: -photographs -accession no. -collection title -location/SEI/virus -other info
Track media in Media Database
Photograph media
Generate checksum(s) for content files/disk image
Create disk image with Kryoflux
Floppy disk (5 1/4 or 3 1/2)
Media type?
Create disk image (AFF) with FTK Imager (generates checksum and verifies)
CD/DVD/ external drive
no reader available
Sensitive Electronic Information (SEI) check
Virus scan
Media Database
Track in Media Database, no further action taken
Secure networked file storage system: -image file -FTK logs -file list (CSV) -SEI/Virus scan reports
Processing for access
Finding Aid
Is content openly available University Archives material? Does it warrant item-level description?
Yes
No
DukeSpace Repository
Access online
accessible content transferred to CD/DVD
In-house access via reading room computer

Appraisal and accession

Gengenbach, Martin J. "'The Way We Do it Here:' Mapping Digital Forensics Workflows in Collecting Institutions." A Master's Paper for the M.S. in L.S degree. August, 2012.

Duke University Archives, born-digital content workflow, June 2012



Initial donation and acquisition of born-digital content

Media device(s) are assigned accession number

Accession record

Archivist's Toolkit

Is content acquired on one or more media devices? (hard drive, CD/DVD)

No

Yes

Is media interfiled w/ other material?

Yes

No

Create separation sheet and add bar-code for each

Place content files on local machine for accessioning

Affix bar-code to media

Separation sheet (stays w/ physical collection)

Media Database:
-photographs
-accession no.
-collection title
-location/SEI/virus
-other info

Track media in Media Database

Photograph media

Generate checksum(s) for content files/disk image

Create disk image with Kryoflux

Floppy disk (5 1/4 or 3 1/2)

Media type?

Create disk image (AFF) with FTK Imager (generates checksum and verifies)

CD/DVD/ external drive

Sensitive Electronic Information (SEI) check

Virus scan

no reader available

Media Database

Track in Media Database, no further action taken

Secure networked file storage system:
-image file
-FTK logs
-file list (CSV)
-SEI/Virus scan reports

Processing for access

Finding Aid

Is content openly available University Archives material? Does it warrant item-level description?

Yes

No

Access online

DukeSpace Repository

accessible content transferred to CD/DVD

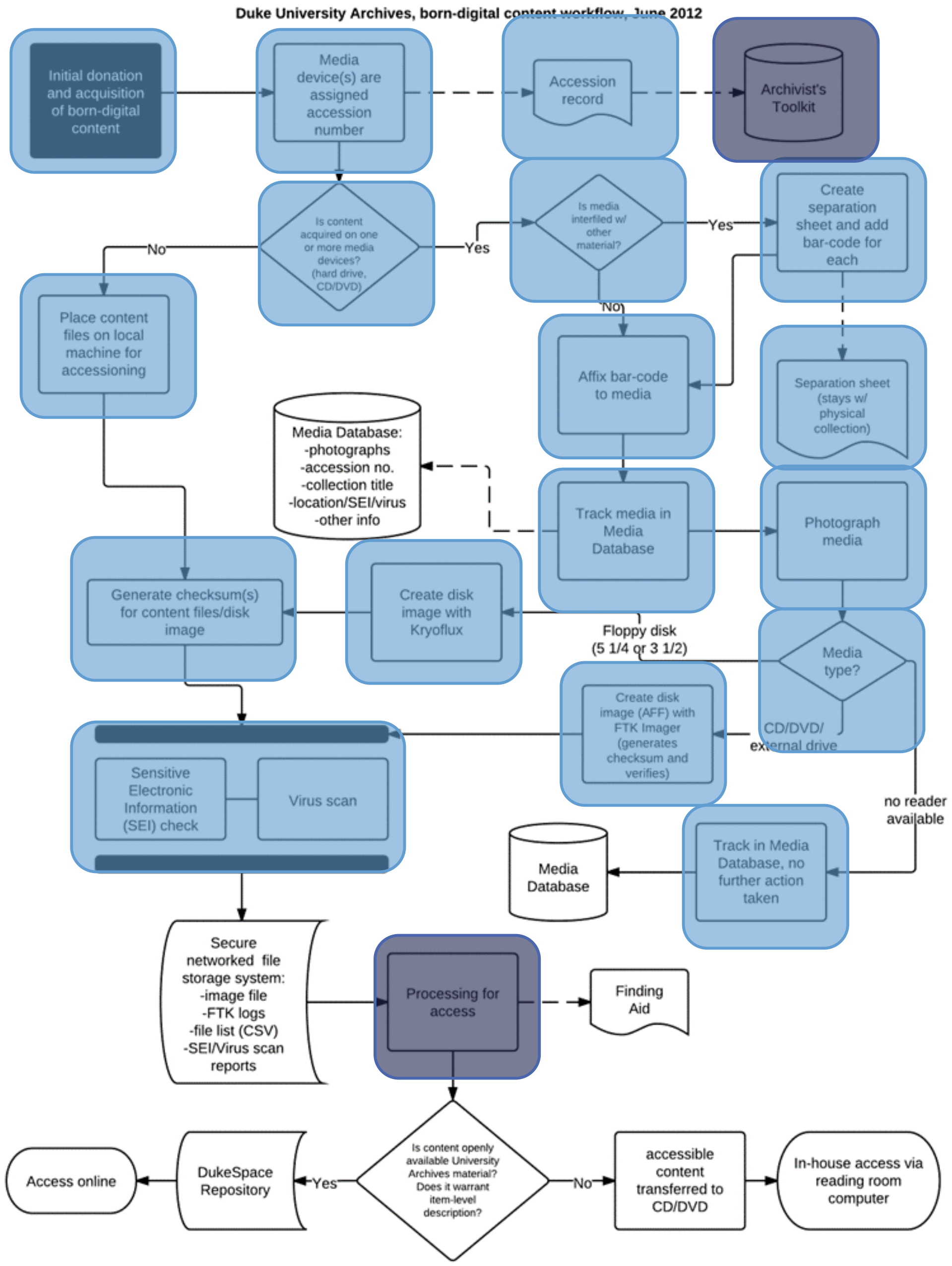
In-house access via reading room computer

22 July 2014

Digital Preservation 2014 - #digpres14

Arrangement and description

Gengenbach, Martin J. "'The Way We Do it Here:' Mapping Digital Forensics Workflows in Collecting Institutions." A Master's Paper for the M.S. in L.S degree. August, 2012.



Duke University Archives, born-digital content workflow, June 2012

Initial donation and acquisition of born-digital content

Media device(s) are assigned accession number

Accession record

Archivist's Toolkit

Is content acquired on one or more media devices? (hard drive, CD/DVD)

No

Yes

Is media interfiled w/ other material?

Yes

No

Create separation sheet and add bar-code for each

Place content files on local machine for accessioning

Affix bar-code to media

Separation sheet (stays w/ physical collection)

Media Database:
-photographs
-accession no.
-collection title
-location/SEI/virus
-other info

Track media in Media Database

Photograph media

Generate checksum(s) for content files/disk image

Create disk image with Kryoflux

Floppy disk (5 1/4 or 3 1/2)

Media type?

Create disk image (AFF) with FTK Imager (generates checksum and verifies)

CD/DVD/ external drive

no reader available

Sensitive Electronic Information (SEI) check

Virus scan

Media Database

Track in Media Database, no further action taken

Secure networked file storage system:
-image file
-FTK logs
-file list (CSV)
-SEI/Virus scan reports

Processing for access

Finding Aid

Is content openly available University Archives material? Does it warrant item-level description?

Yes

No

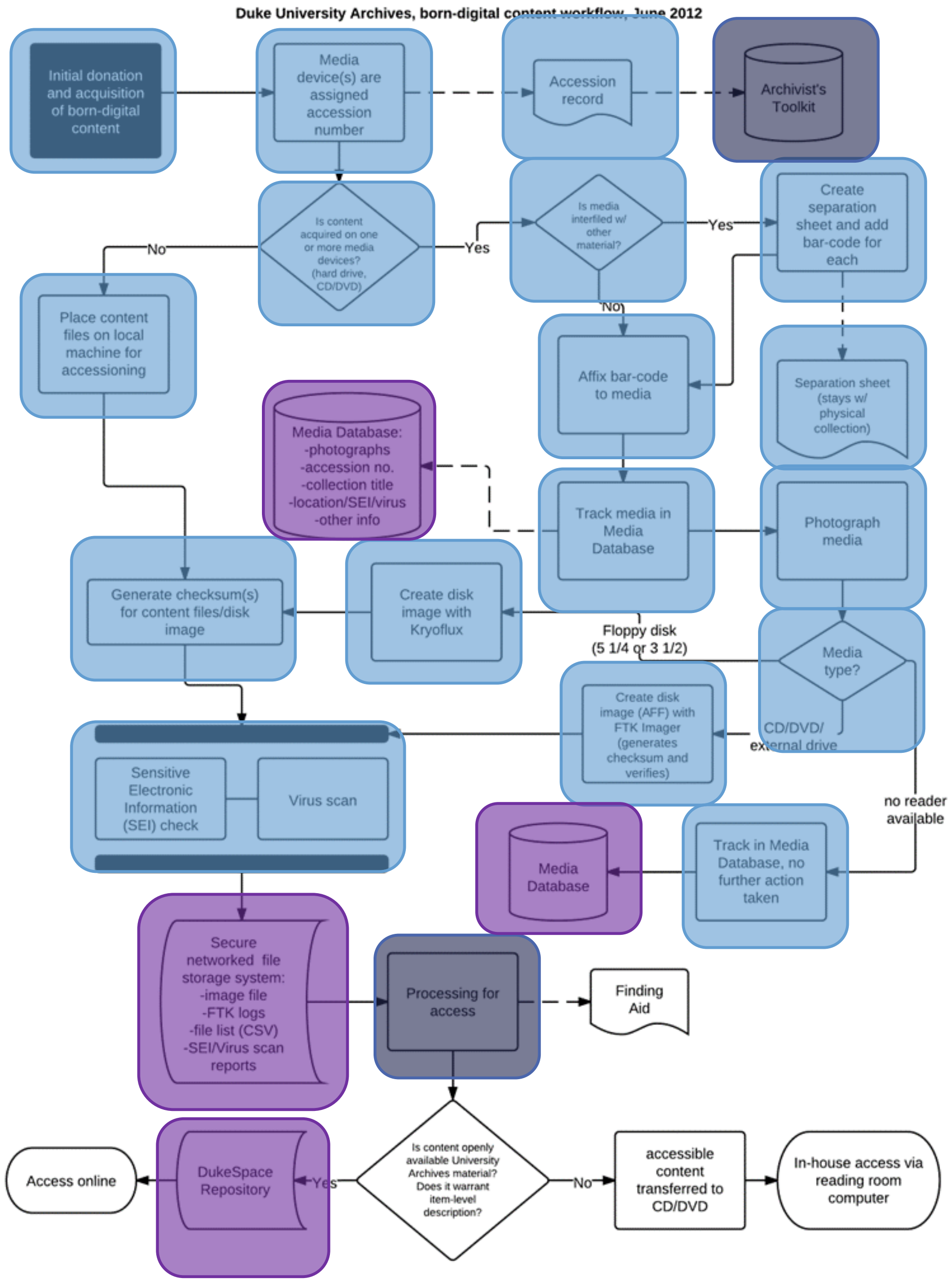
Access online

DukeSpace Repository

accessible content transferred to CD/DVD

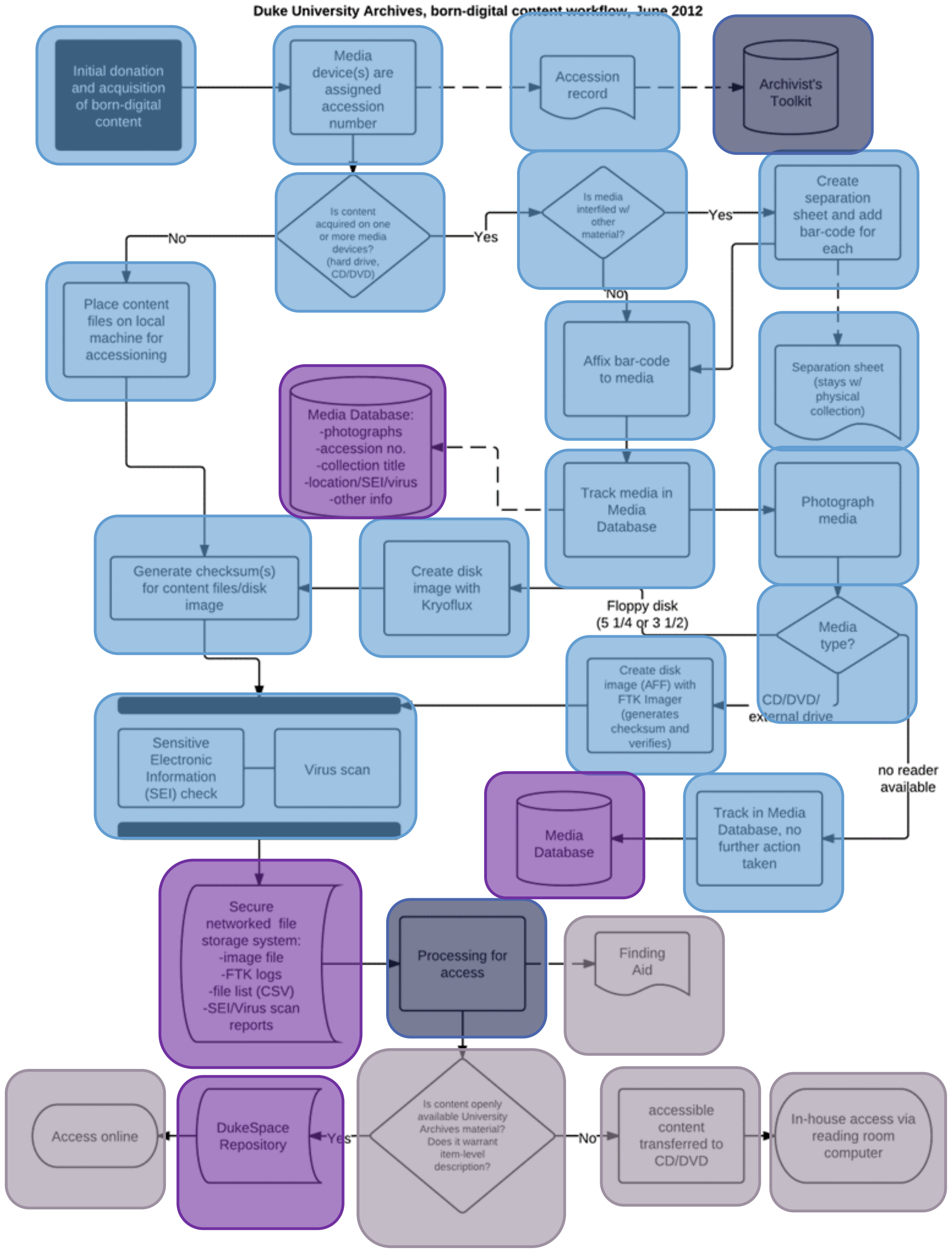
In-house access via reading room computer

Preservation


Duke University Archives, born-digital content workflow, June 2012
Initial donation and acquisition of born-digital content
Media device(s) are assigned accession number
Accession record
Archivist's Toolkit
Is content acquired on one or more media devices? (hard drive, CD/DVD)
No
Yes
Is media interfiled w/ other material?
Yes
No
Create separation sheet and add bar-code for each
Place content files on local machine for accessioning
Affix bar-code to media
Separation sheet (stays w/ physical collection)
Media Database: -photographs -accession no. -collection title -location/SEI/virus -other info
Track media in Media Database
Photograph media
Generate checksum(s) for content files/disk image
Create disk image with Kryoflux
Floppy disk (5 1/4 or 3 1/2)
Media type?
Create disk image (AFF) with FTK Imager (generates checksum and verifies)
CD/DVD/ external drive
no reader available
Sensitive Electronic Information (SEI) check
Virus scan
Media Database
Track in Media Database, no further action taken
Secure networked file storage system: -image file -FTK logs -file list (CSV) -SEI/Virus scan reports
Processing for access
Finding Aid
Is content openly available University Archives material? Does it warrant item-level description?
Yes
No
Access online
DukeSpace Repository
accessible content transferred to CD/DVD
In-house access via reading room computer

Gengenbach, Martin J. "'The Way We Do it Here:' Mapping Digital Forensics Workflows in Collecting Institutions." A Master's Paper for the M.S. in L.S degree. August, 2012.

Access



Duke University Archives, born-digital content workflow, June 2012

Initial donation and acquisition of born-digital content

Media device(s) are assigned accession number

Accession record

Archivist's Toolkit

Is content acquired on one or more media devices? (hard drive, CD/DVD)

No

Yes

Is media interfiled w/ other material?

Yes

No

Create separation sheet and add bar-code for each

Separation sheet (stays w/ physical collection)

Place content files on local machine for accessioning

Affix bar-code to media

Media Database: -photographs -accession no. -collection title -location/SEI/virus -other info

Track media in Media Database

Photograph media

Generate checksum(s) for content files/disk image

Create disk image with Kryoflux

Floppy disk (5 1/4 or 3 1/2)

Media type?

Create disk image (AFF) with FTK Imager (generates checksum and verifies)

CD/DVD/ external drive

no reader available

Sensitive Electronic Information (SEI) check

Virus scan

Media Database

Track in Media Database, no further action taken

Secure networked file storage system: -image file -FTK logs -file list (CSV) -SEI/Virus scan reports

Processing for access

Finding Aid

Is content openly available University Archives material? Does it warrant item-level description?

Yes

No

DukeSpace Repository

Access online

accessible content transferred to CD/DVD

In-house access via reading room computer

Gengenbach, Martin J. "'The Way We Do it Here:' Mapping Digital Forensics Workflows in Collecting Institutions." A Master's Paper for the M.S. in L.S degree. August, 2012.

“The Way We Do It Here”: Findings

- Technical challenges – tools and hardware

“The Way We Do It Here”: Findings

- Technical challenges – tools and hardware
- Challenges to digital forensics workflow output
  - Arrangement and description
  - Access

“The Way We Do It Here”: Findings

- Technical challenges – tools and hardware
- Challenges to digital forensics workflow output
  - Arrangement and description
  - Access
- Collaboration within and between institutions

Time passes…

Postcard, Oppland, Vang, ca 1970. National Library of Norway. Image number blds_05931.

Revisiting Digital Forensics Workflows in Collecting Institutions (2014)

MITH
MARYLAND INSTITUTE FOR TECHNOLOGY IN THE HUMANITIES

Duke
UNIVERSITY

NATIONAL LIBRARY OF AUSTRALIA

UNIVERSITY of VIRGINIA

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

CITY OF VANCOUVER

UNIVERSITY OF MARYLAND

Revisiting Digital Forensics Workflows: Analysis and Findings

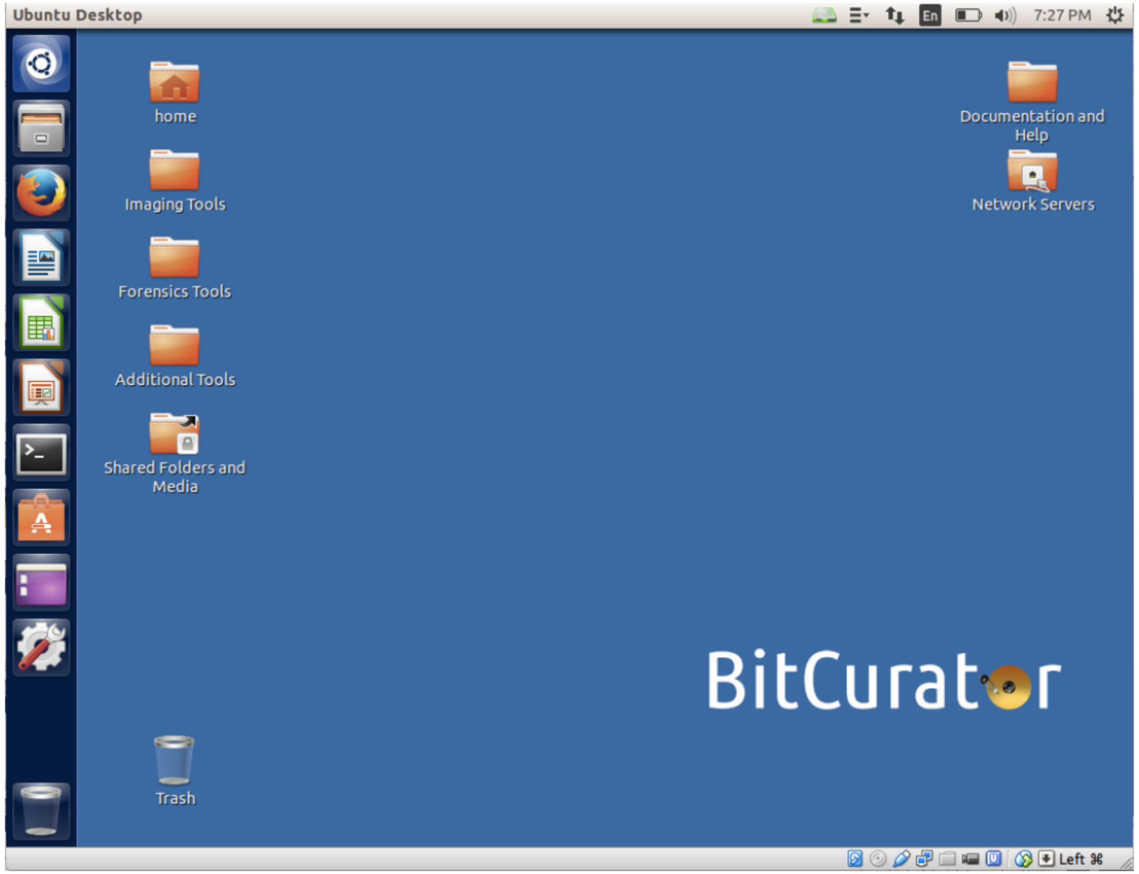
- Core digital forensics acquisition workflows have remained relatively stable…

Revisiting Digital Forensics Workflows: Analysis and Findings

- Core digital forensics acquisition workflows have remained relatively stable…
- Except for:
  - Actors executing the work
  - Systems where content and metadata are stored
  - Tools and formats for disk image creation and analysis

BitCurator

Tools for Digital Forensics Methods and Workflows
in Real-World Collecting Institutions

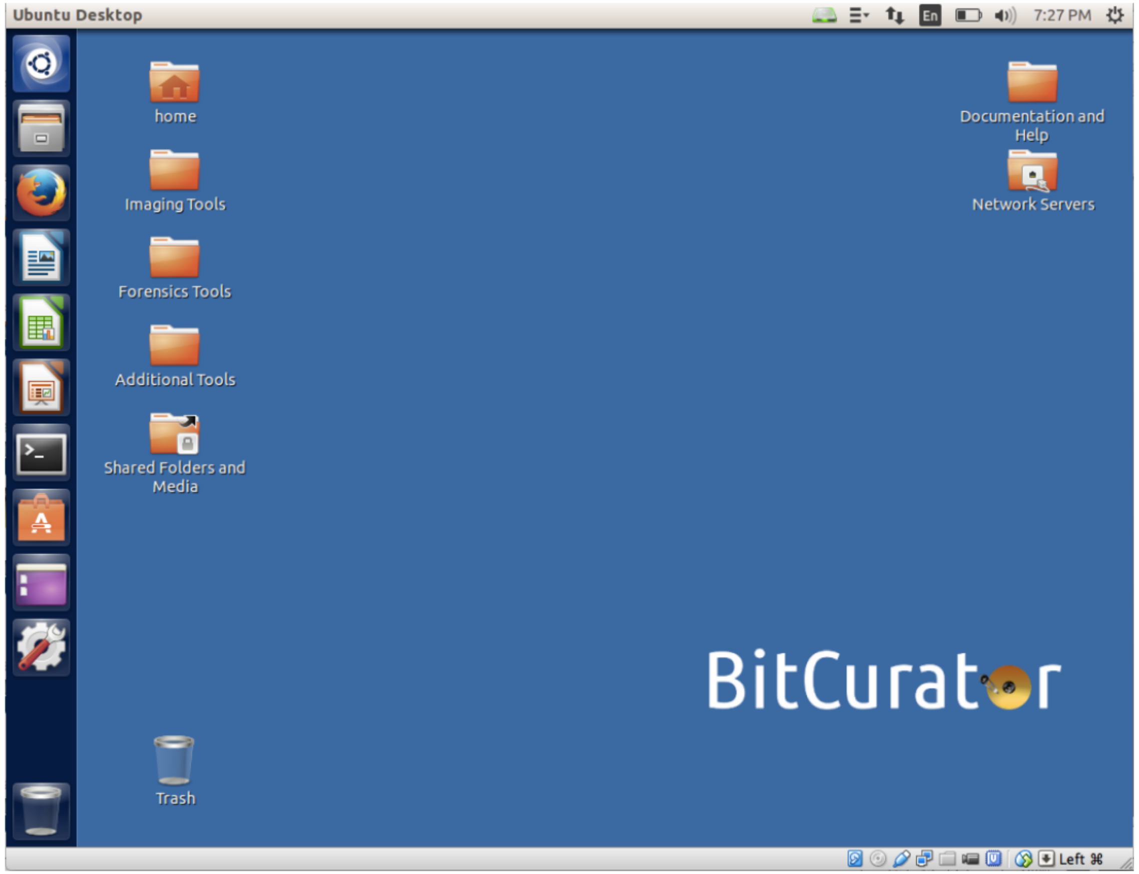


- Forensic disk imaging
- File system analysis
- Identification of PII
- File and metadata export
- Reporting

http://www.bitcurator.net/aboutbc/#project
http://wiki.bitcurator.net/downloads/BitCurator-Quickstart-v0.9.13.pdf

BitCurator

Tools for Digital Forensics Methods and Workflows in Real-World Collecting Institutions



http://www.bitcurator.net/aboutbc/#project
http://wiki.bitcurator.net/downloads/BitCurator-Quickstart-v0.9.13.pdf

BitCurator Project
Porter Olsen
Session 8: West End Ballroom Salon E
9:00-10:15 AM
Wednesday, July 23, 2014

BitCurator

Tools for Digital Forensics Methods and Workflows
in Real-World Collecting Institutions

- Use is high among interview participants
- Supplementing, not replacing, existing tools in participant workflows

http://www.bitcurator.net/aboutbc/#project
http://wiki.bitcurator.net/downloads/BitCurator-Quickstart-v0.9.13.pdf

Revisiting Digital Forensics Workflows: Analysis and Findings

- Disk image format and retention varies
- Ongoing challenges in arrangement and description, access
- Network file transfer and A/V content acquisitions

Conclusions and Recommendations

Sausage Room at Denny's Factory, Waterford, 24 September 1937. Photographed by Poole Photographic Studios. National Library of Ireland. NLI Ref.: P_WP_4245

Conclusions

- Archivist turnover impacts the success of digital forensics workflows

Conclusions

- Archivist turnover impacts the continuing success of digital forensics workflows
- Integrating digital forensics output with existing archival collection management systems is a complex and multifaceted challenge

Conclusions

- Archivist turnover impacts the continuing success of digital forensics workflows
- Integrating digital forensics output with existing archival collection management systems is a complex and multifaceted challenge
- Removable media makes up a small portion of incoming born-digital content
  (but lots of backlog)

Recommendations

- Mitigate risks of turnover
  - Education for existing staff
  - Opportunities for collaboration
  - Delegation/distribution of digital forensics workflow activities

Recommendations

- Mitigate risks of turnover
- Gather metrics for digital forensics capture
  - Necessary for resource allocation
  - Failure rates documented to assess risk of loss

Recommendations

- Mitigate risks of turnover
- Gather metrics for digital forensics capture
- Explore alternative use cases and content streams

Recommendations

- Mitigate risks of turnover
- Gather metrics for digital forensics capture
- Explore alternative use cases and content streams
- More case studies, please!

Thank you to the participants!

2012

- Bradley Daigle
- Michael Forstrom
- Matthew Kirschenbaum
- Leslie Johnston
- Mark Matienzo
- Courtney Mumma
- Erin O’Meara
- David Pearson
- Seth Shaw

2014

- Joanne Archer
- Sue Bigelow
- Ann Cooper
- Matthew Farrell
- Heather Gordon
- Carmel McInerny
- Porter Olsen
- David Pearson
- Gabriela Redwine
- Meg Tuomala

Questions?

Thank you!

Martin.Gengenbach@gmail.com

martinge@gatesarchive.com

@mjgengenbach (but I’m not much of a tweeter)

Resources

AIMS Work Group. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship. 2012.

BitCurator Project website: http://www.bitcurator.net/.

Duryee, Alex. "An Introduction to Optical Media Preservation." *AVPreserve* White Paper. Originally published in *Code4Lib Journal* Issue 24. April 16, 2014.

Digital Forensics Research Working Group. "A Road Map for Digital Forensic Research." Utica, NY. August 7-8, 2001.

Erway, Ricky. "You've Got to Walk Before You Can Run: First Steps for Managing Born-Digital Content Received on Physical Media." OCLC Research Report. June 2012.

Gengenbach, Martin J. "'The Way We Do it Here:' Mapping Digital Forensics Workflows in Collecting Institutions." A Master's Paper for the M.S. in L.S degree. August, 2012.

Kirschenbaum, Matthew G., Richard Ovenden, and Gabriela Redwine. "Digital Forensics and Born-Digital Content in Cultural Heritage Collections." Washington, DC: Council on Library and Information Resources, 2010.

Lee, Christopher A., Kam Woods, Matthew Kirschenbaum, and Alexandra Chassanoff. "From Bitstreams to Heritage: Putting Digital Forensics into Practice in Collecting Institutions." September 30, 2013.

O'Meara, Erin. "No One Cooks the Bacon Alone: Models for Success in Building out a Digitally-Integrated Special Collections Program." Presented at Past Forward!: Meeting Stakeholder Needs in 21st Century Special Collections. New Haven, CT, 4-5 June 2013.

Rice, David, and Chris Lacinak. "Digital Tape Preservation Strategy: Preserving Data or Video?" *AVPreserve* White Paper. December 2, 2009.

Rogers, Corinne, and Jeremy Leighton John. "Shared Perspectives, Common Challenges: A History of Digital Forensics & Ancestral Computing for Digital Heritage," in *The Memory of the World in the Digital Age: Digitization and Preservation*. Vancouver, British Columbia, Canada. 26-28 September, 2012.

Wiley, Laura, Rebecca Skirvin, Peter Chan, and Glynn Edwards. "Capturing and Processing Born-Digital Files in the STOP AIDS Project Records: A Case Study." April 26, 2013.