Accessing the inaccessible: digital forensics at the Dalhousie University Archives

Creighton Barrett
Dalhousie University Archives

Council of Nova Scotia Archives Conference
May 11, 2017

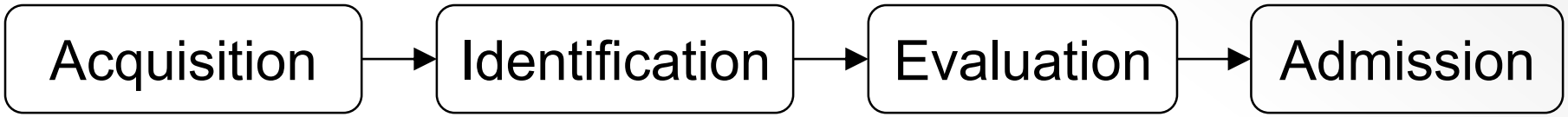
DALHOUSIE UNIVERSITY 1818 2018

Overview

- Introduction to digital forensics in archival repositories
- Development of Dalhousie's digital forensics lab
- Forensic images
- Digital forensics tools and workflows
- Free digital forensics tools
- Ask questions any time!

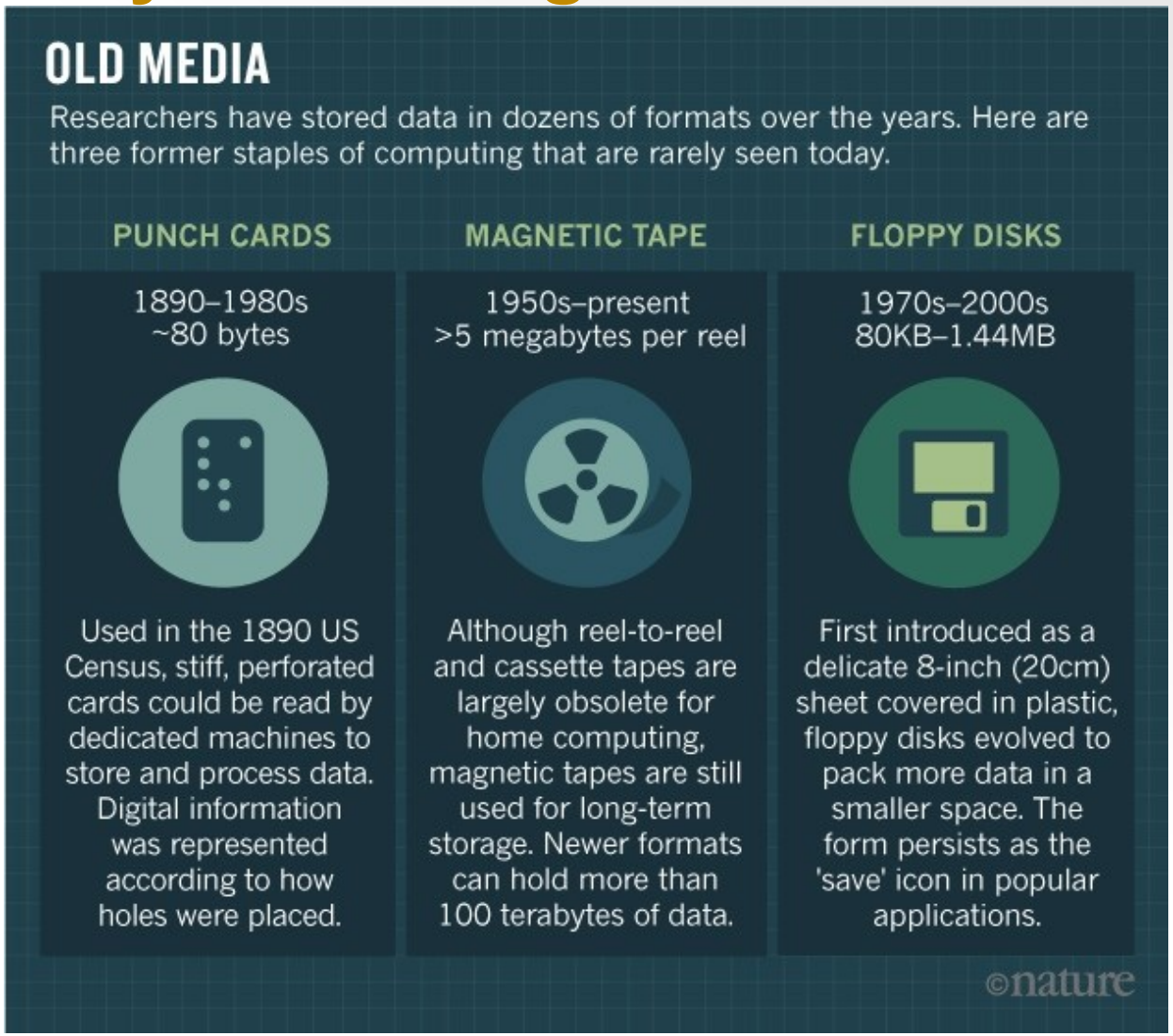
What is digital forensics?

- Forensic science – recovery and investigation of data found in digital storage devices
- Primarily used in criminal investigations, corporate investigations
- Archives are adopting digital forensics techniques to support acquisition, accessioning, preservation, and access



Source: Infosec Institute, Digital Forensic Models (January 25, 2016): http://resources.infosecinstitute.com/digital-forensics-models/

Why have a digital forensics lab?



Source: Baker, M. (2017, May 2). Disks back from the dead. *Nature, 545* (7652), 117–118. https://doi.org/10.1038/545117a

Why have a digital forensics lab?

- Archivists are now working with a wide variety of:
  - Digital storage devices
  - Computer file systems, operating systems, and software
  - File formats
- Digital storage devices are unstable and data is at risk
- Supports archival mission to preserve authenticity and integrity of records

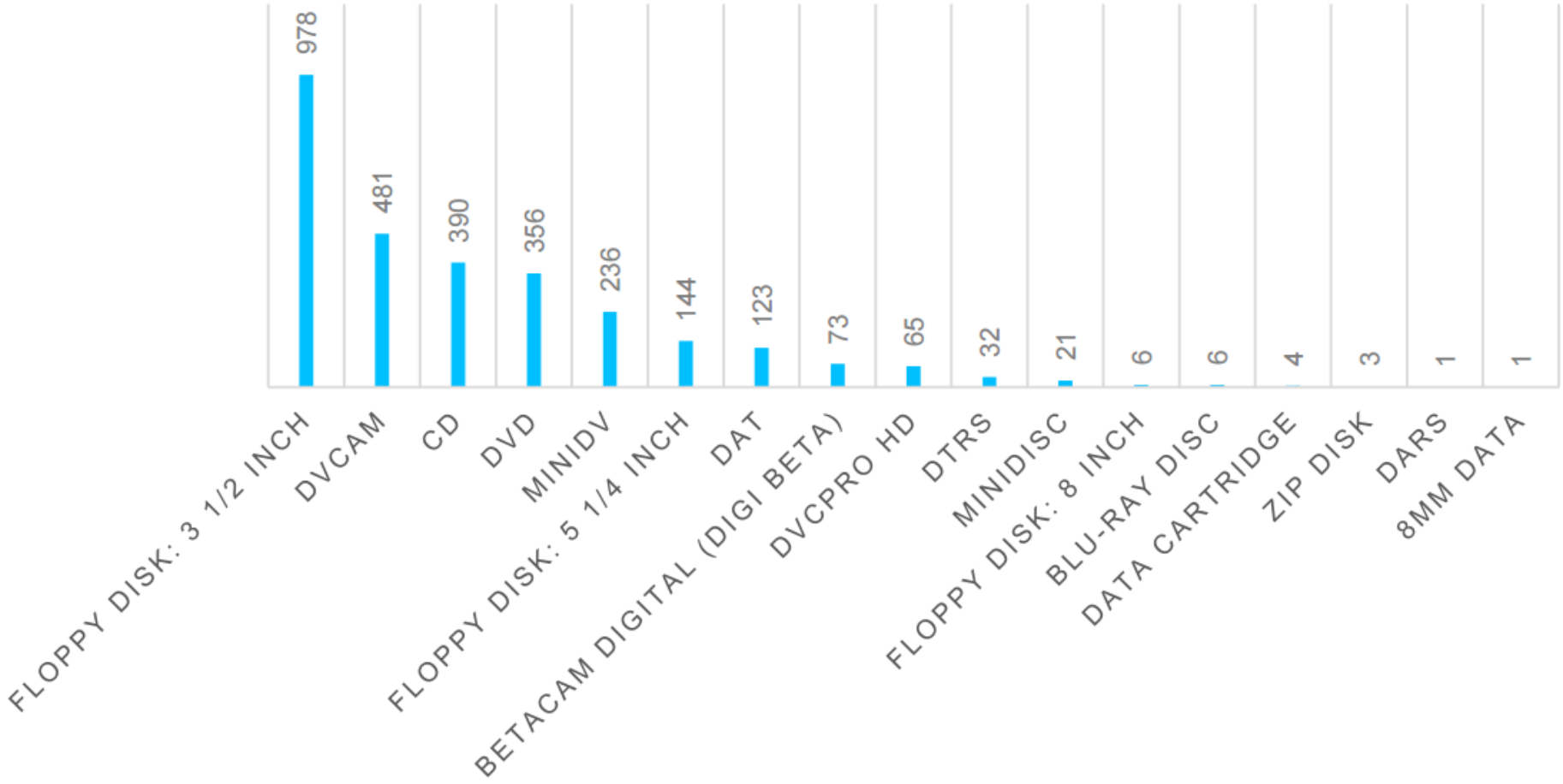
How are archives doing digital forensics work?

- Use write-blockers to create forensic images
- Adopt forensic software (BitCurator or FTK or EnCase)
- Incorporate digital forensics tools and techniques into core archival functions
- New policy decisions (e.g., preserve forensic image or extract files?)
- Archival functions become blurred (e.g., files can be arranged before they are accessioned)

Timeline at Dalhousie

- February 2016 – Acquire forensic workstation
- May – November 2016 – Digital archives collection assessment project: http://hdl.handle.net/10222/72663
- January 2017 – Install BitCurator and Forensic Toolkit (FTK) software
- February 2017 – Advanced computer forensics training
- May 2017 – Launch digital forensics lab
- April 2017 – Dal's first time at BitCurator Users Forum

DIGITAL MEDIA CARRIER FORMATS



Components of Digital Forensics Lab

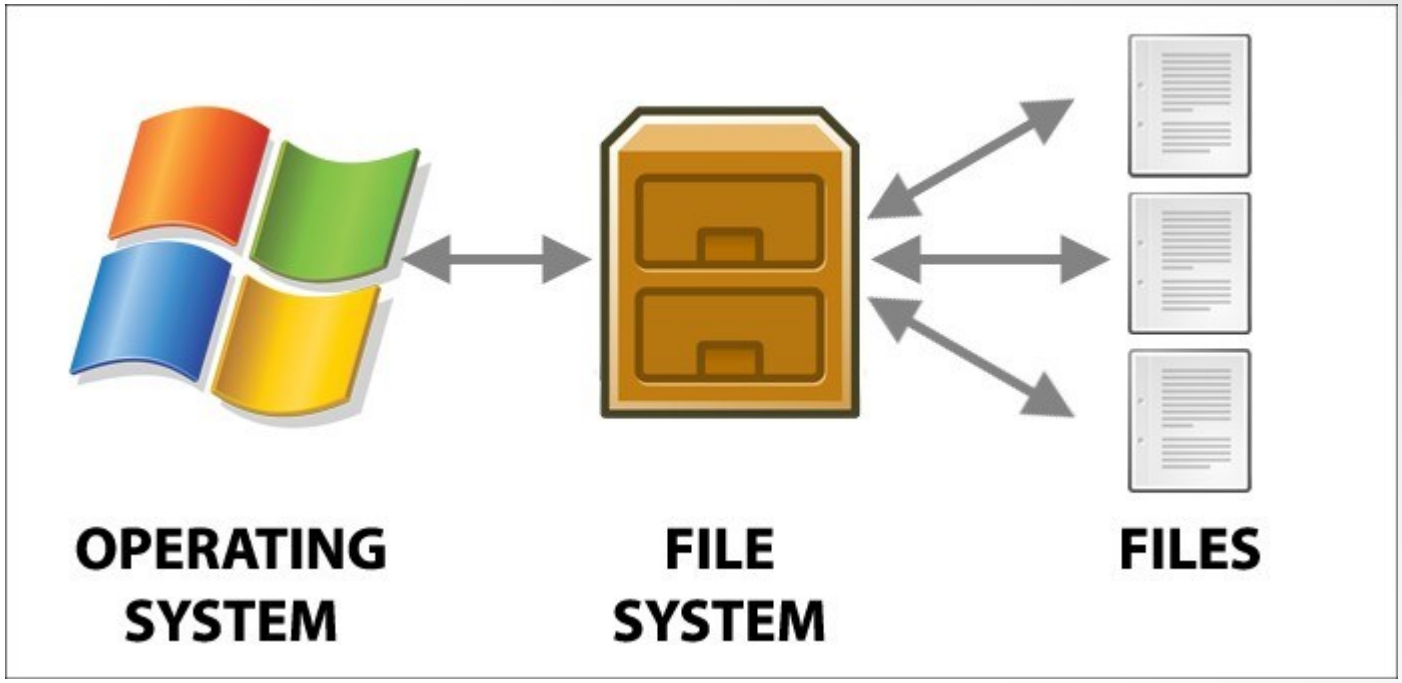
- Forensic tower
  - Dual Intel Xeon processors
  - 64 GB RAM
  - Tableau T35689iu write-blocker
  - AFT EX-S3 forensic card reader
- FTK software
- BitCurator software

Forensic images

What is a forensic image?

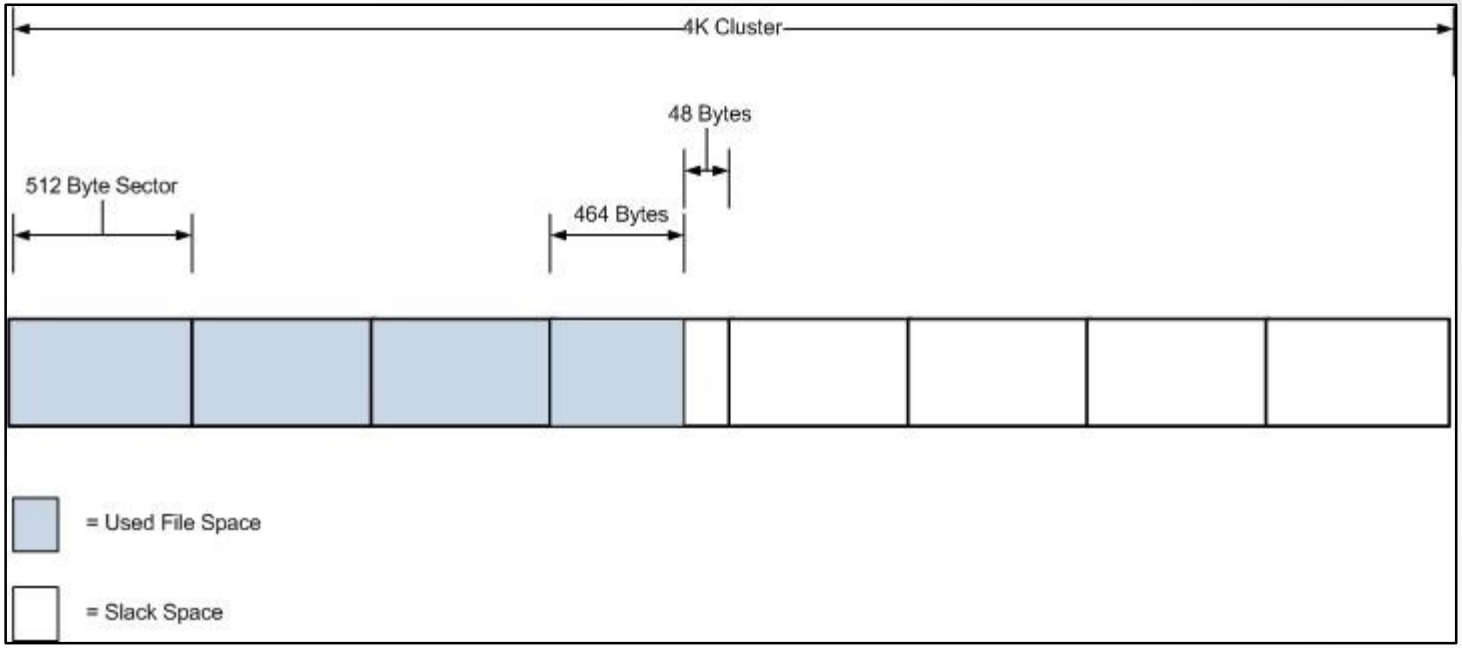
- Complete (i.e., bit-level) copy of a hard drive or other digital storage media
- Includes unallocated space and slack space
- Includes operating system and file system
- Includes computer registry files, browser history, and other contextual information about how the computer was used
- Includes all files on the hard drive

Preserve information about the operating system and file system



Source: Power Data Recovery: The Volume does not contain a recognized file system – how to fix : https://www.powerdatarecovery.com/hard-drive-recovery/volume-not-contain-recognized-file-system.html

Preserve data in slack space / unallocated space



Some differences between forensic and logical images

Forensic image	Logical image
Recovers operating system and file system	Does not recover operating system and file system
Potential for password recovery, decryption, etc.	Almost no potential for password recovery, decryption, etc.
Recover Internet search queries and form data	Cannot recover Internet search queries and form data
Size of entire hard drive, regardless of how many files are stored	Size of files on hard drive

11S45J9439ZVJ4YV036DCR REV:0B
lenovo
intel
CHINA
30V Serial ATA
ASAP

Digital forensics tools


FORENSIC COMPUTERS, INC.
Tableau Forensic Bridge
FORENSIC COMPUTERS
READ ONLY
M-DISC
LG
LIAN LI


Tableau Forensic Bridge
T356789iu
GUIDANCE SOFTWARE
Write Block
Read/Write
Power
Host
Device
Activity
IDE
SATA/SAS
SATA Gen3
Drive Power
PCIe
FireWire
USB 3.0


TABLEAU
2.5" IDE Hard Drive Adapter
Model TDA5-25
Pin 1


Forensic Computers
forensic-computers.com
Forensic Computers
T35689iu Forensic Bridge
Powered by TABLEAU
Pwr
Dev
Host
WrtBlk
Act
SAS
FireWire
USB 3.0
IDE
Insert SUBJECT Drive With Pins Outward
Connect Appropriate Cabling To T35689iu
HC/SDXC
MS/DUO
Forensic Series
EX-53
READ WRITE
M-DISC
LG

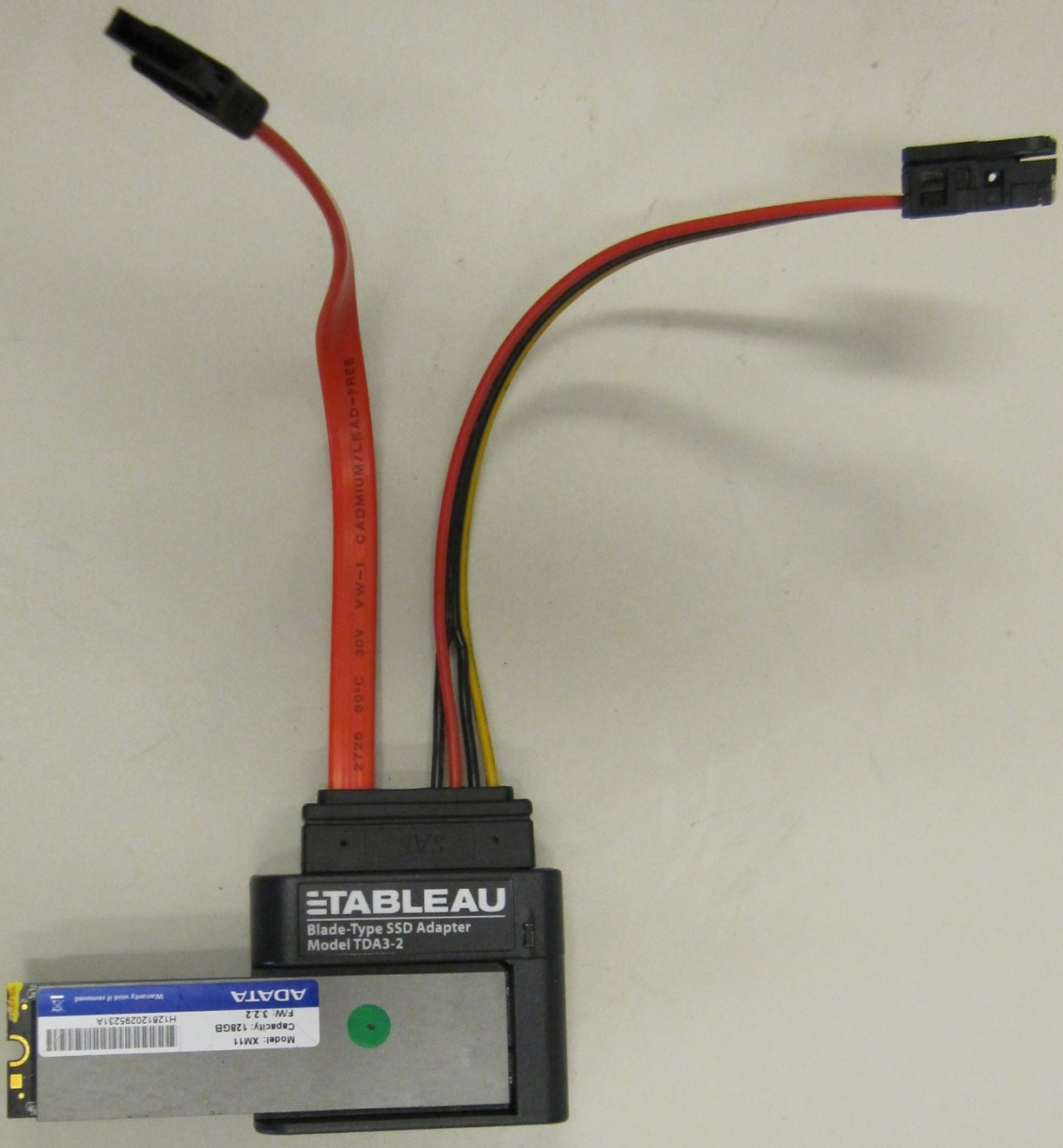
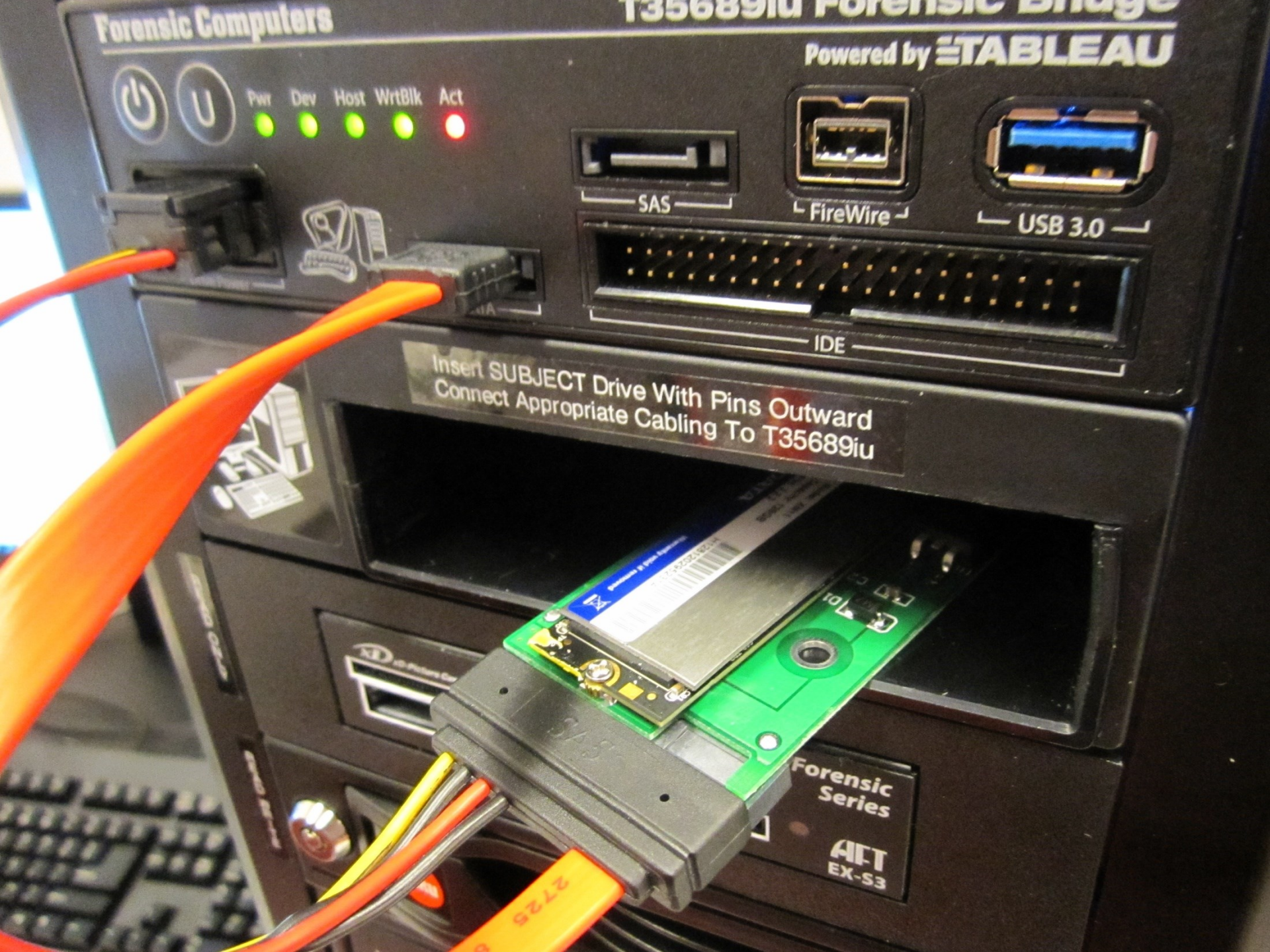


TABLEAU
Blade-Type SSD Adapter
Model TDA3-2
ADATA
Model: XM11
Capacity: 128GB
FW: 3.2.2
H12612029523 1A
Warranty void if removed
2725 80°C 30V VW-1 CADMIUM/LEAD-FREE

ADATA
Warranty void if removed
Model: XM11
Capacity: 128GB
FW: 3.2.2
H1281202952314
2725 80°C 30V VW-1 CADMIUM/LEAD-FREE

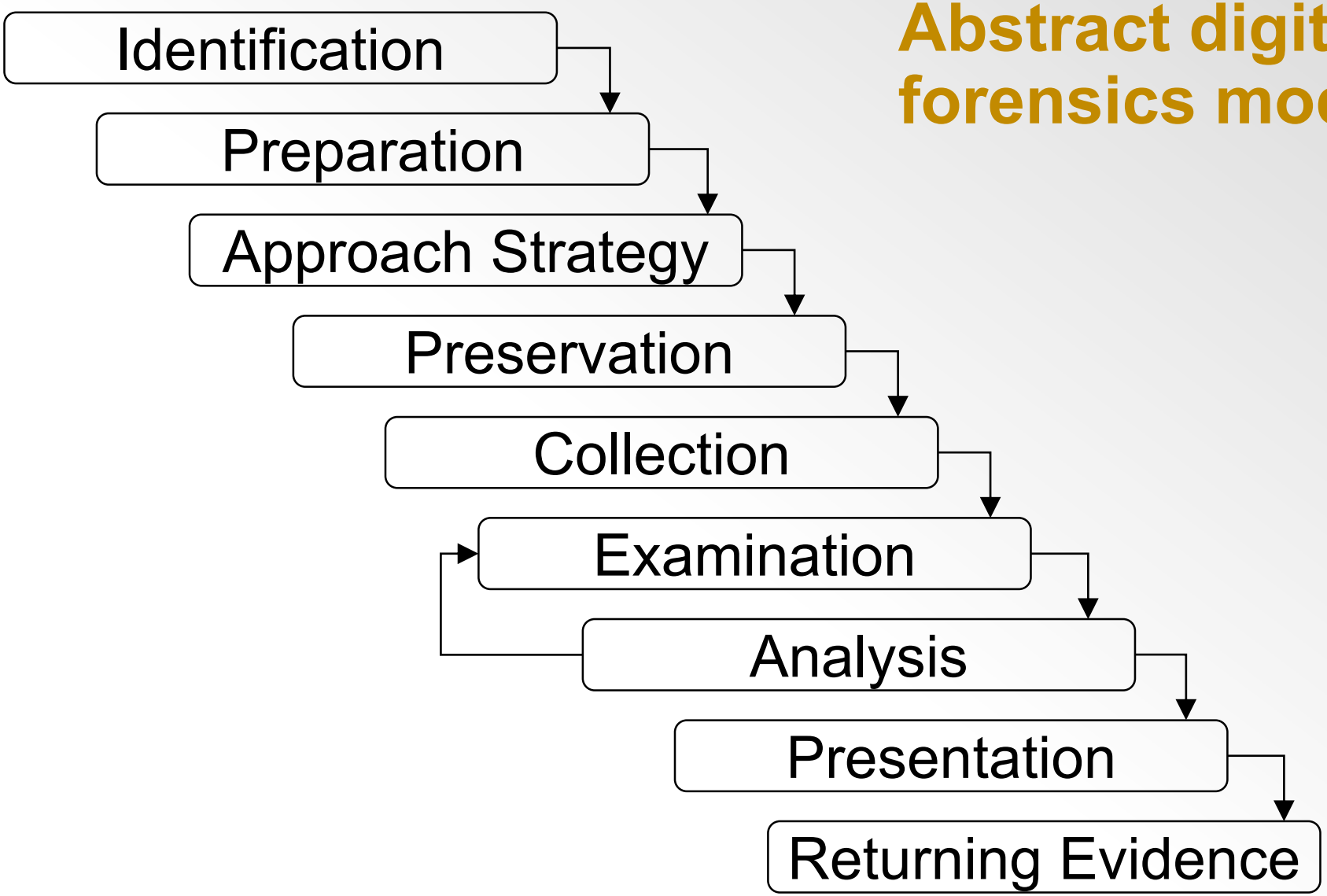

Forensic Computers
T35689iu Forensic Bridge
Powered by TABLEAU
Pwr
Dev
Host
WrtBlk
Act
SAS
FireWire
USB 3.0
IDE
Insert SUBJECT Drive With Pins Outward
Connect Appropriate Cabling To T35689iu
Forensic Series
AFT EX-S3

BitCurator

EnCase®

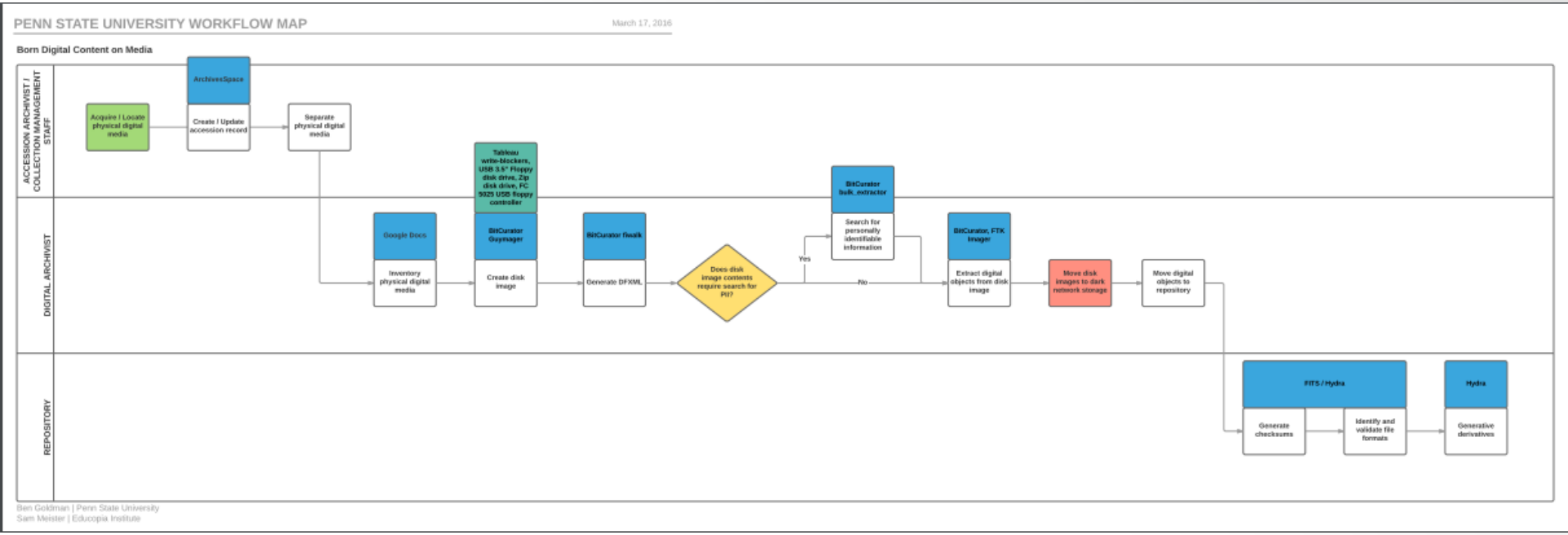
Digital forensics workflows

Abstract digital forensics model

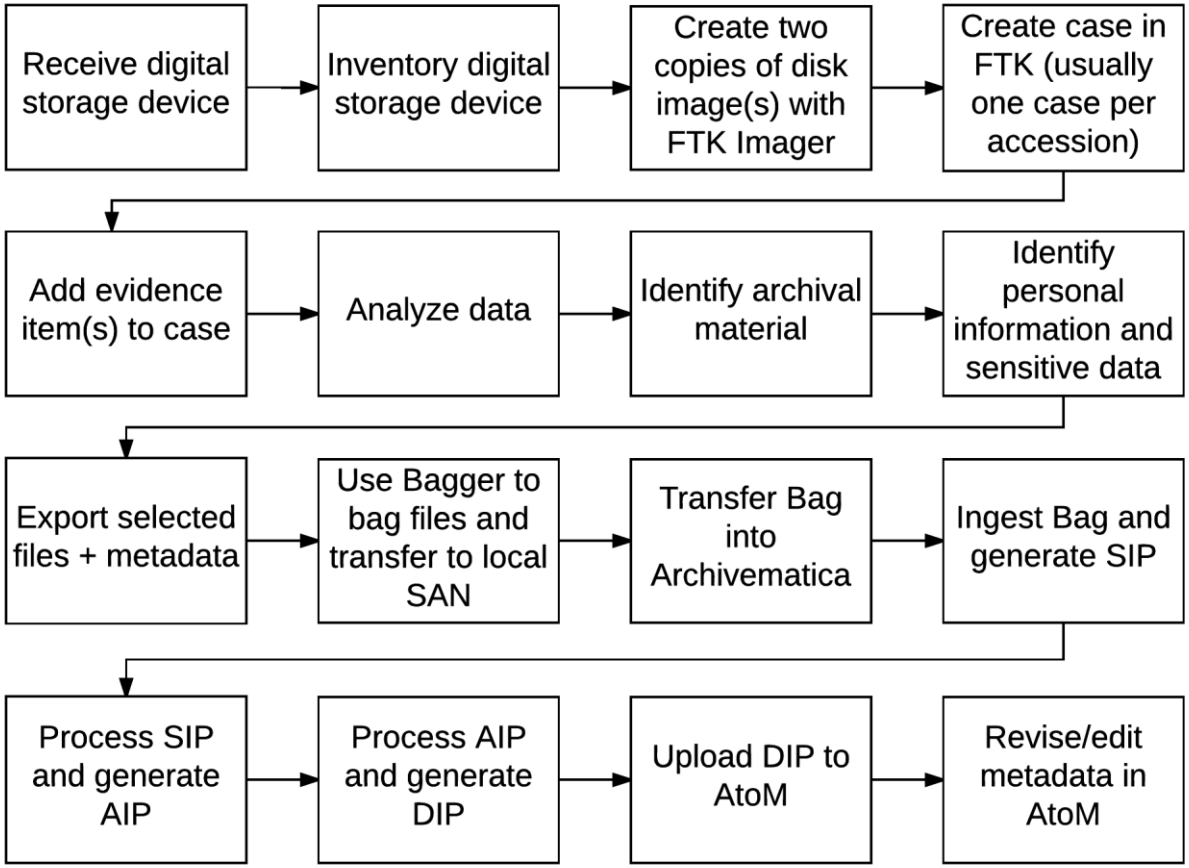


Source: Infosec Institute, Digital Forensic Models (January 25, 2016): http://resources.infosecinstitute.com/digital-forensics-models/

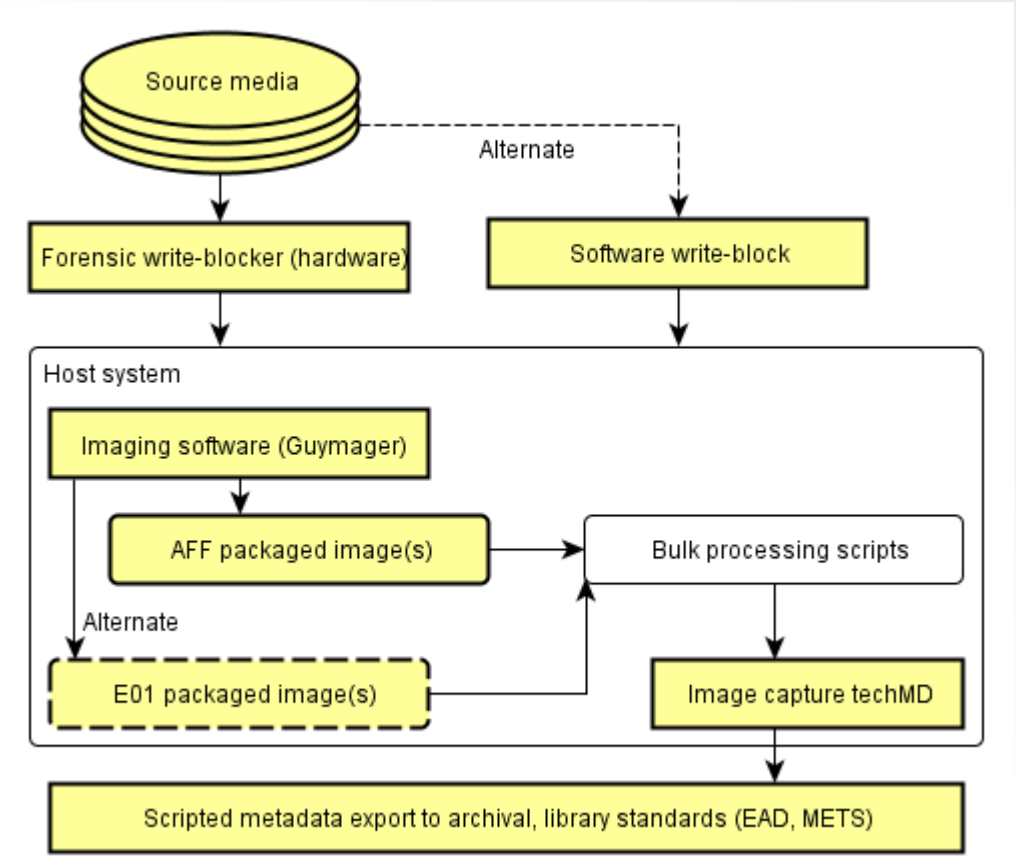
Penn State University workflow



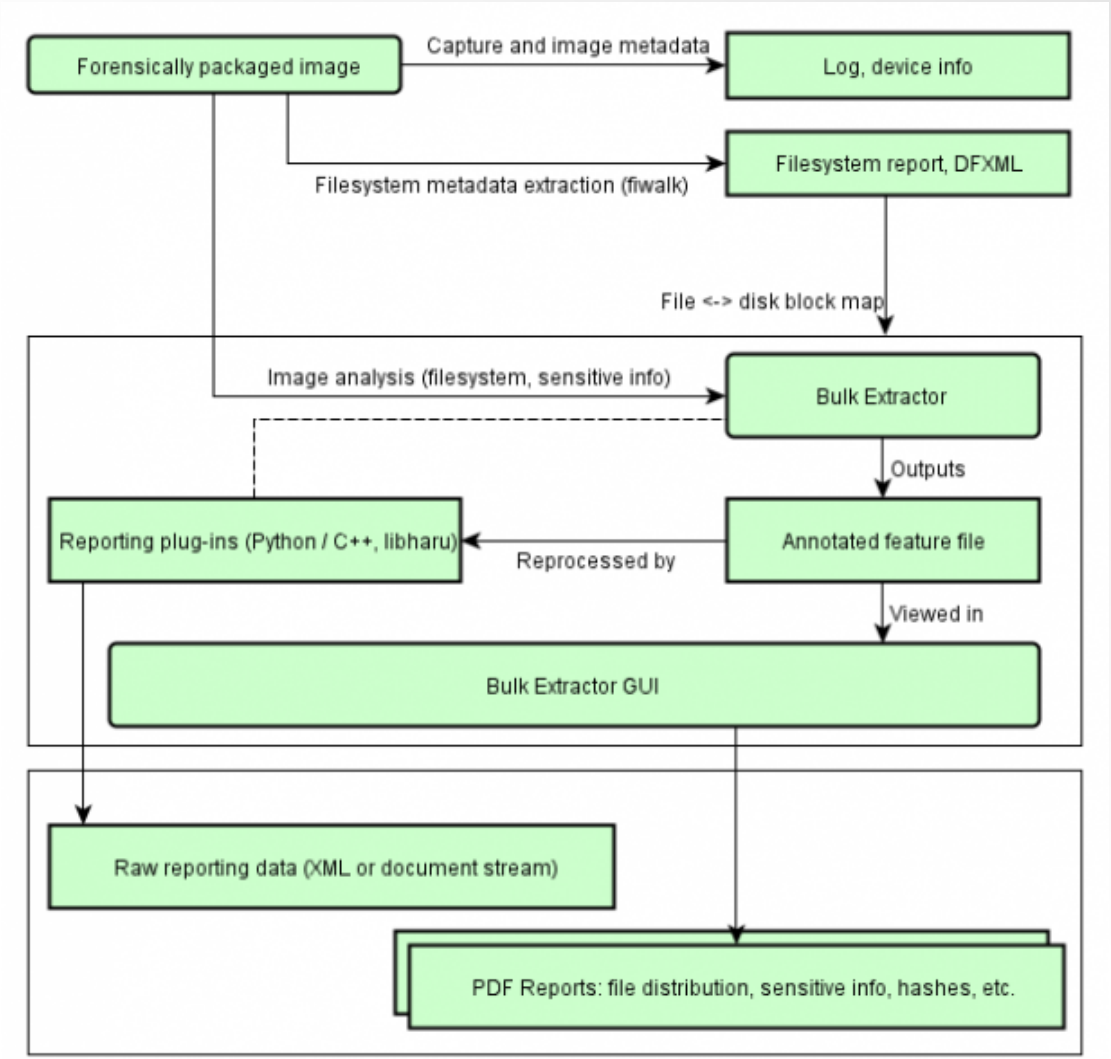
Dalhousie University workflow (draft)



Forensic imaging workflow (BitCurator)



Identify privacy concerns



Bill Freedman fonds filtered in FTK

Filter	Description	# of files	Size
Unfiltered	All files in case	26,651,084	3,568 GB
Primary status	Duplicate File indicator IS “Primary”	731,417	83.48 GB
Secondary status	Duplicate File indicator IS “Secondary”	16,569,218	271.5 GB
KFF Ignore	Match all files where KFF status IS “Ignore”	2,548,119	44.29 GB
No KFF Ignore	Match all files where KFF status IS NOT “Ignore” + KFF status IS “Not checked”	24,102,965	3524 GB
Primary status + No KFF Ignore	Match all files where duplicate file indicator IS “Primary” + KFF status IS NOT “Ignore”	626,351	71.95 GB
Actual files + Primary status + No KFF Ignore	Match all disk-bound files where duplicate file indicator IS “Primary” + KFF status IS NOT “Ignore”	103,412	61.81 GB

Free digital forensics tools and resources – FTK Imager, BitCurator, and SleuthKit

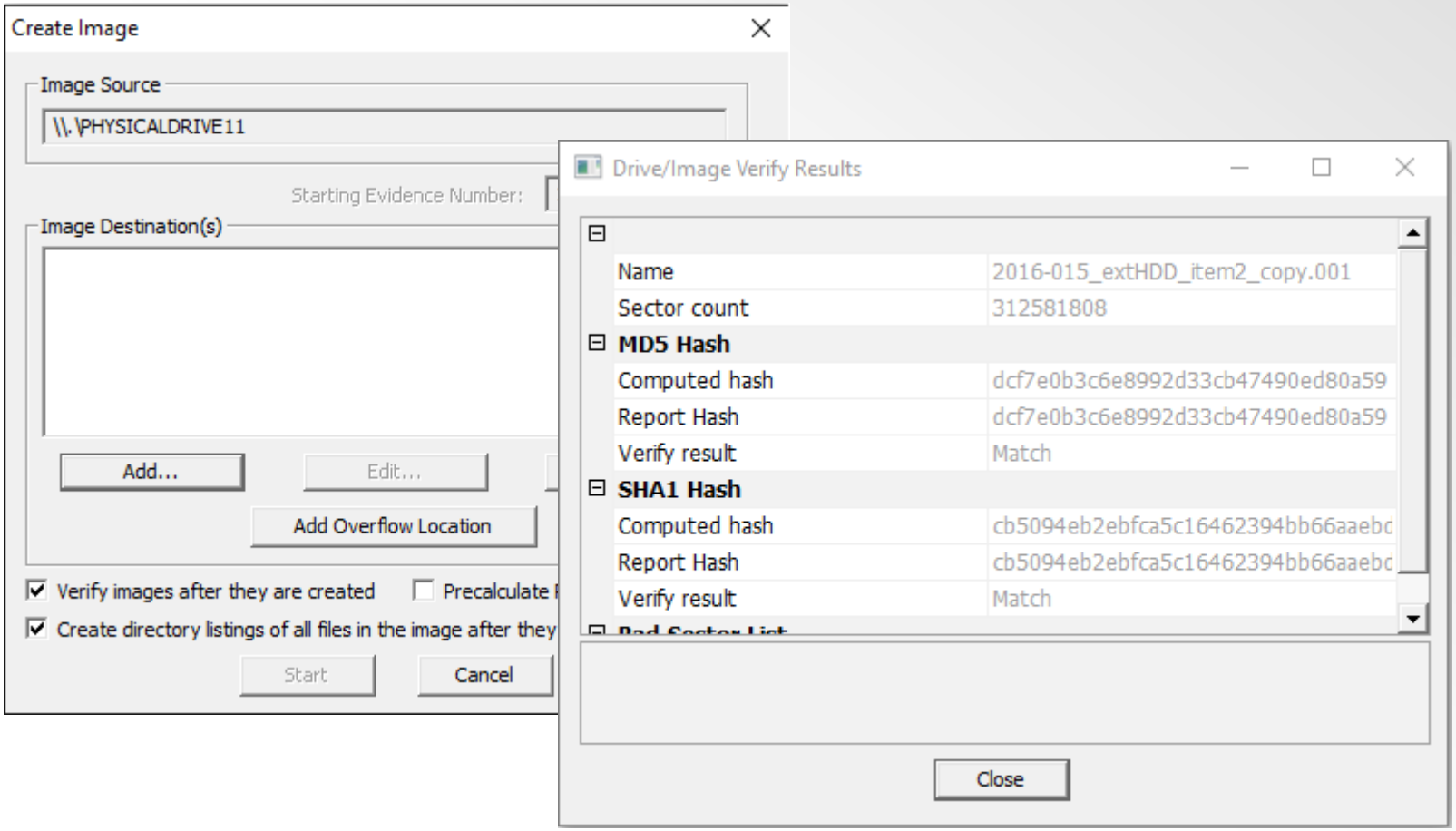
FTK Imager (free download)

- Create forensic images of source media
- Intended for use with hardware write blocker
- Preview, triage, and image
- Export, hash, convert

FTK Imager (free download)

- *Imaging tool* – create forensic images of mounted
- *Preview tool* – preview evidence to determine if further analysis is needed
- *Export tool* – quickly select and export files prior to performing full analysis of the disk image
- FTK Imager can open mounted drive, contents of a folder, or a forensic image
- FTK Imager cannot create image of a networked drive

FTK Imager – Create Image



SleuthKit + Autopsy

Images source: https://www.sleuthkit.org/

SleuthKit + Autopsy

- SleuthKit is a collection of command line tools to investigate disk images
- Tools support the analysis of volume and file system data
- Autopsy is graphical user interface to SleuthKit and other digital forensics tools

Free resources

- Forensics wiki: http://forensicswiki.org/wiki/Main_Page
- List of digital forensics tools: https://en.wikipedia.org/wiki/List_of_digital_forensics_tools
- BitCurator wiki: https://wiki.bitcurator.net/index.php?title=Main_Page