Digital Forensics with BitCurator

Based on the July 29, 2014
BitCurator workshop
at METRO

***

Kevin Schlottmann
August 26, 2014

What is digital forensics?

"Process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable."

http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf

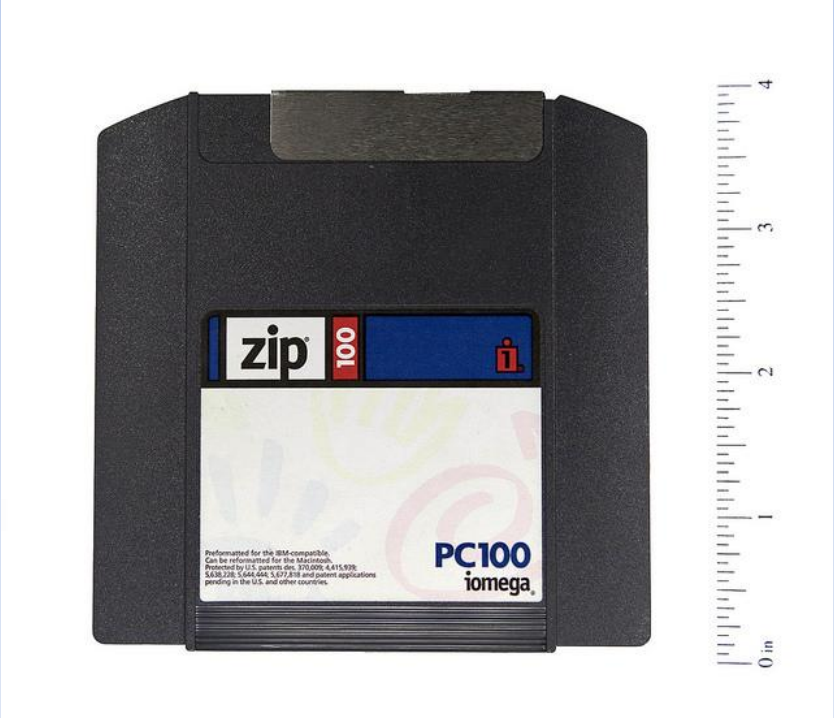
Why apply digital forensics?

*Ensure data integrity

*Ease of automation and processing

Why apply digital forensics?

*In other words: to ensure provenance, original order, chain of custody of digital objects

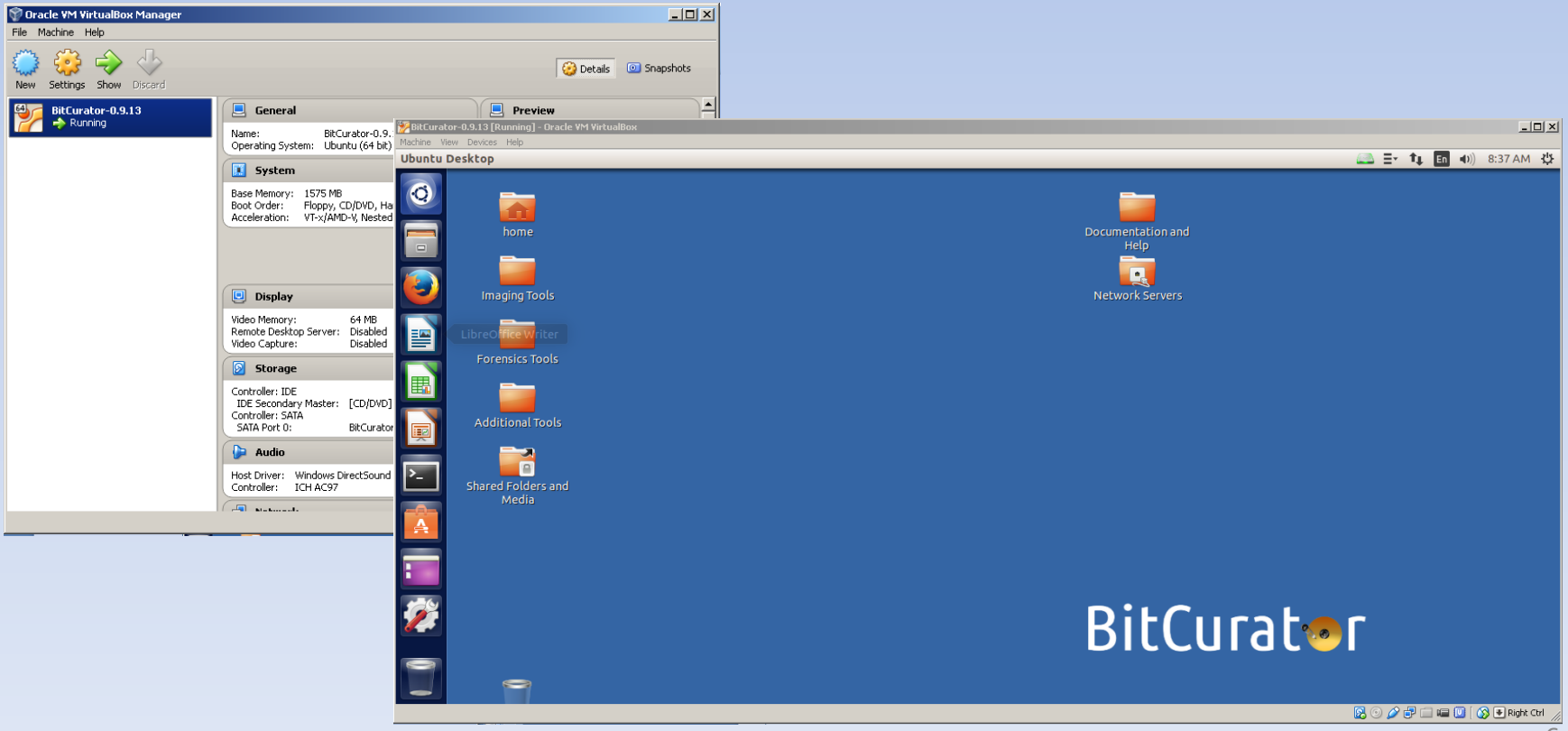


What is BitCurator?

*Customized Linux OS running in virtual machine with a tightly integrated, well-documented suite of open-source digital forensics tools

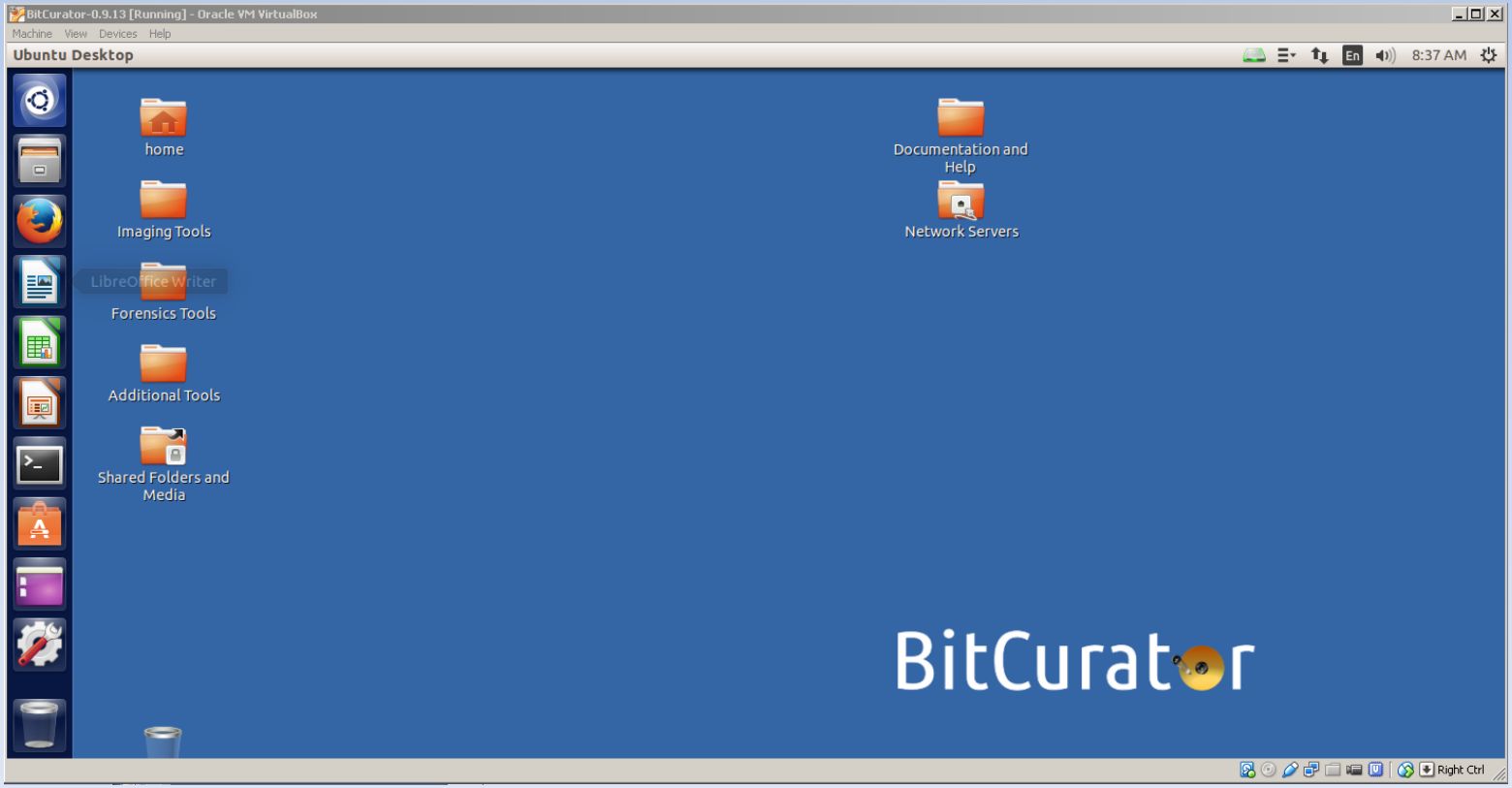
What is BitCurator?

***Customized Linux OS running in virtual machine…**



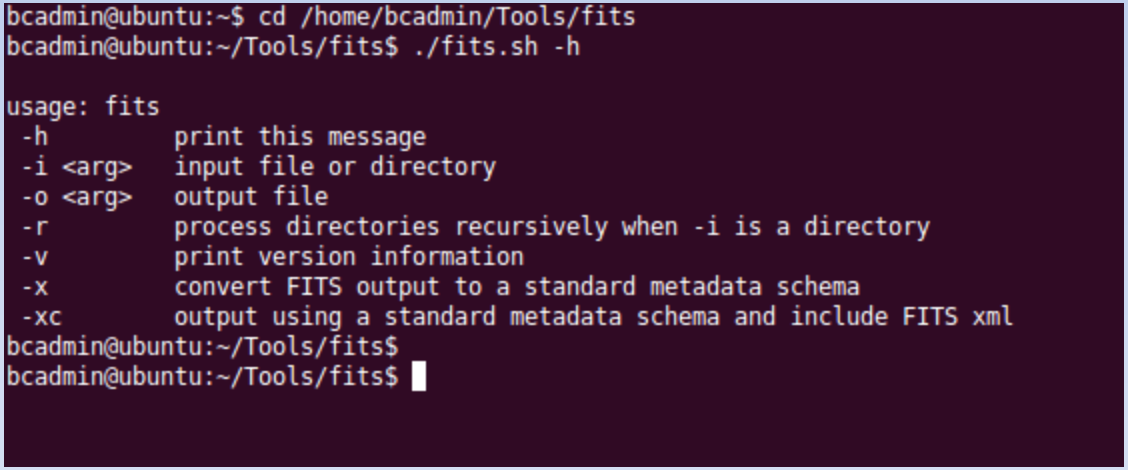
What is BitCurator?

***Customized Linux OS running in virtual machine…**



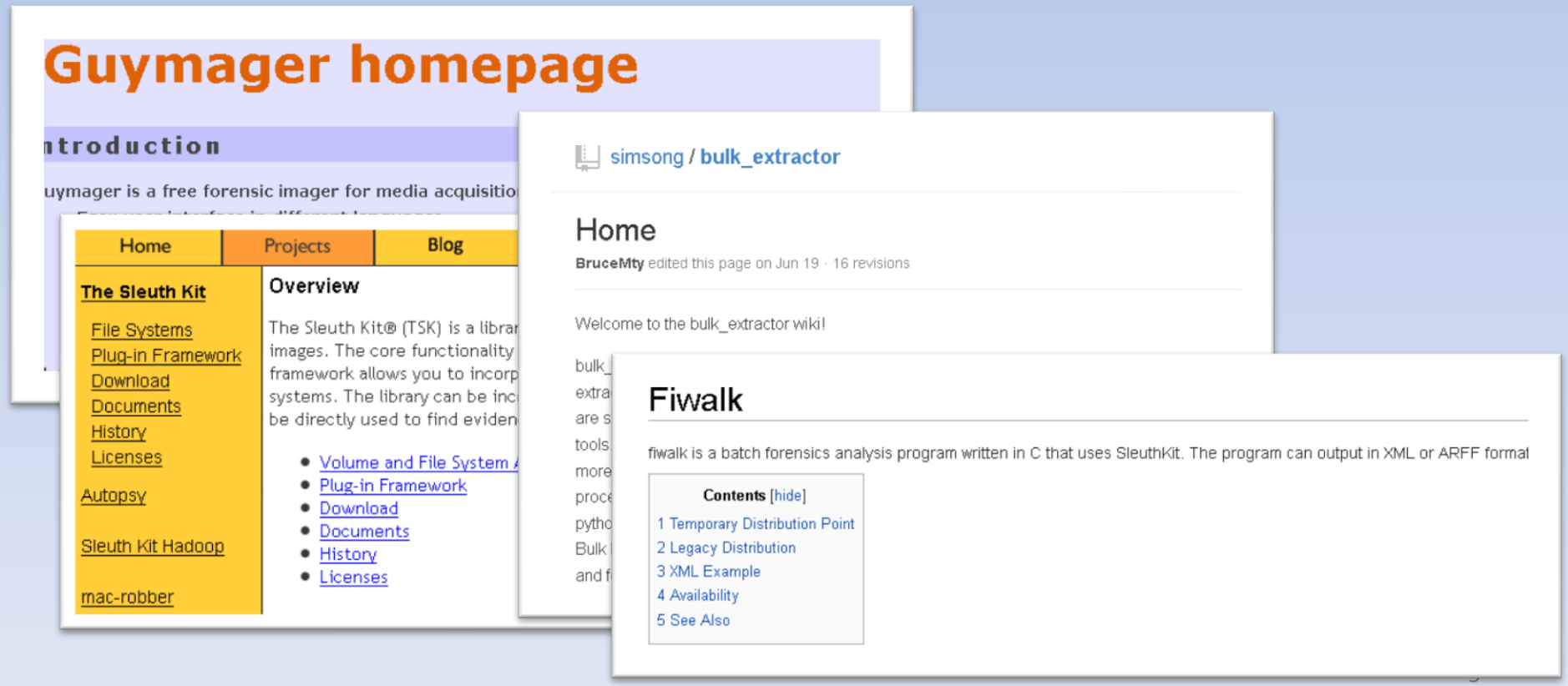
What is BitCurator?

***Customized Linux OS running in virtual machine…**

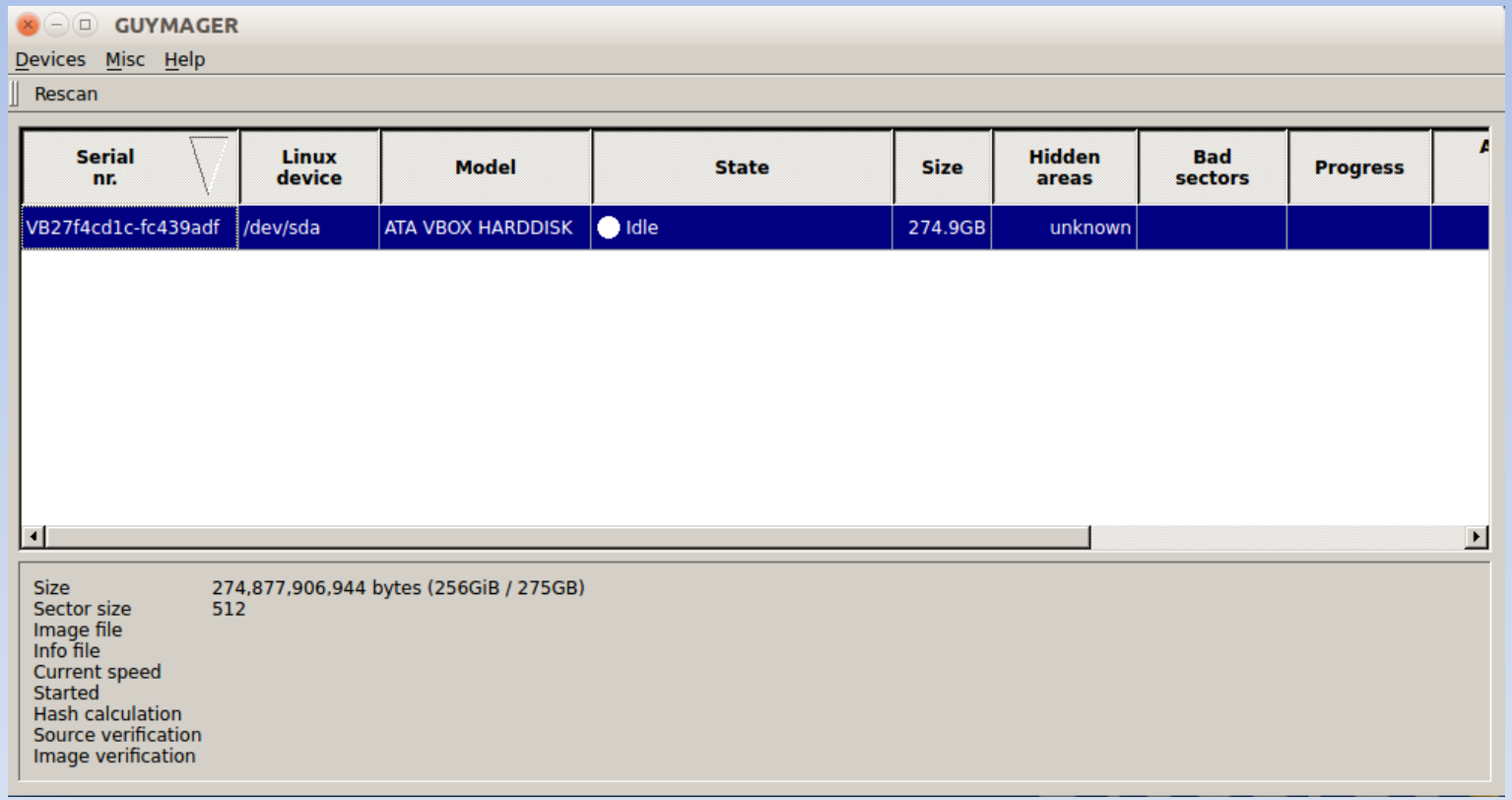


What is BitCurator?

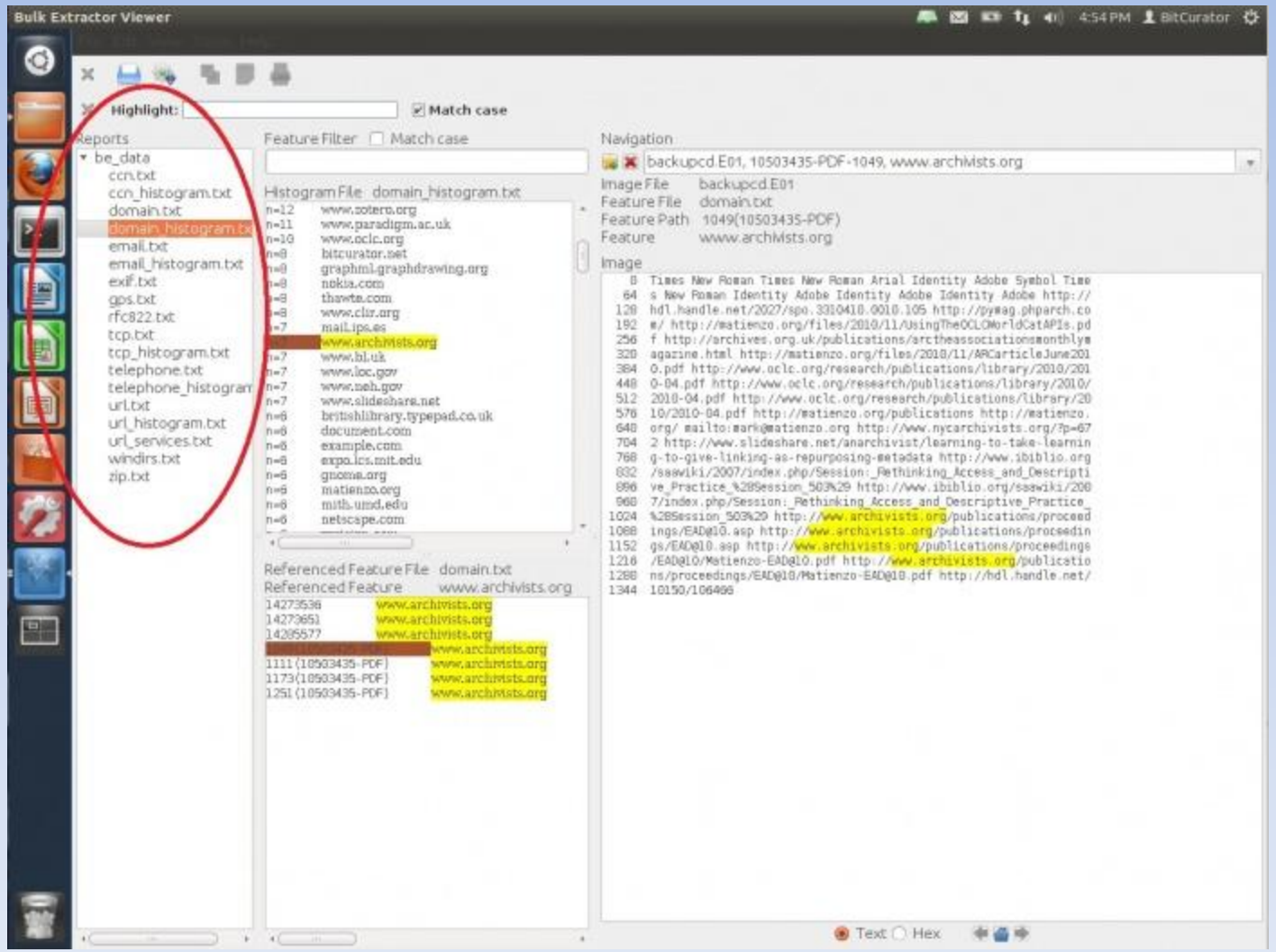
***…a tightly integrated, well-documented suite of open-source digital forensics tools**



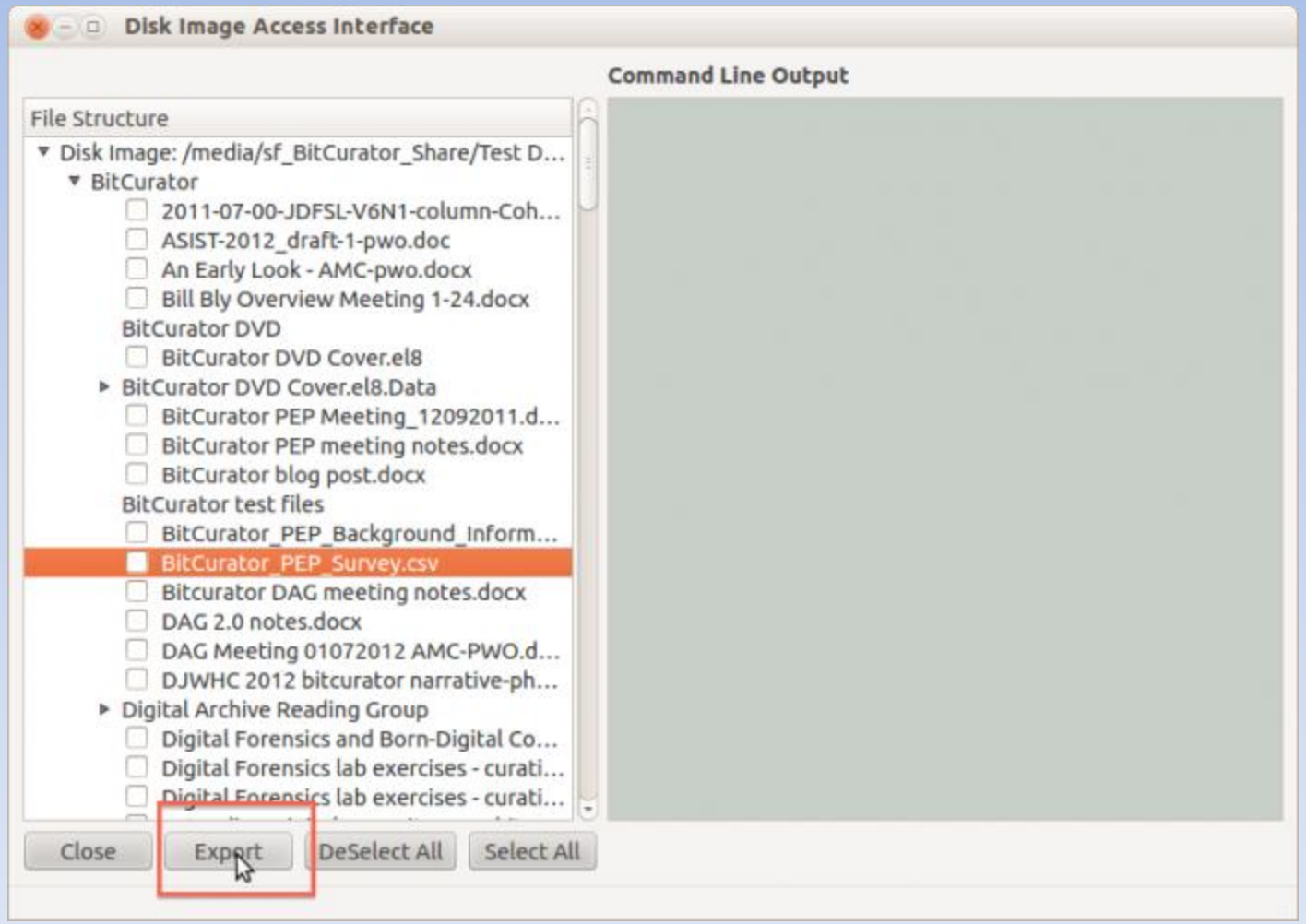
1. Creating a disk image



2. Analyzing the disk image



3. Create access copy



Potential workflows

CJH, METRO, vendor, Partner creates disk image and content reports

CJH or Partner uses BitCurator to analyze data and prepare access copies

CJH, vendor, Partner stores disk image as digital preservation, makes access copies accessible in reading room or remotely

Additional Reading

*BitCurator wiki
[http://wiki.bitcurator.net/index.php?title=Main_Page]

*From Bitstreams to Heritage report
[http://www.bitcurator.net/docs/bitstreams-to-heritage.pdf]

*You've Got to Walk Before You Can Run:First Steps for Managing Born-Digital Content Received on Physical Media
[http://www.oclc.org/content/dam/research/publications/library/2012/2012-06.pdf?urlm=168601]

Thank you!