

BCA-Webtools: Accessing and Visualizing Disk Images in a Web Browser

Kam Woods

UNC School of Information
and Library Science

CurateGear
January 14, 2016
Chapel Hill, NC



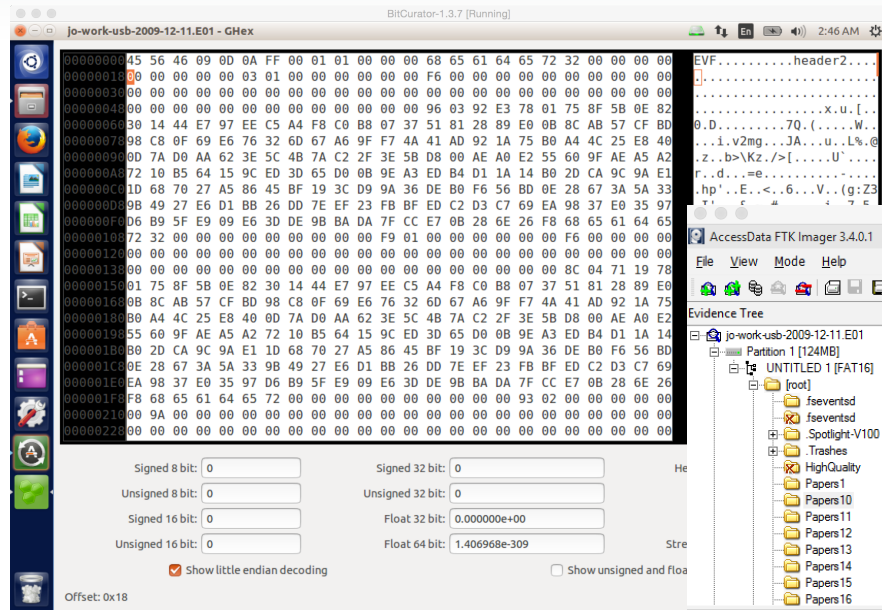
UNC
SCHOOL OF INFORMATION
AND LIBRARY SCIENCE

BitCurator Access **BitCurator**
CONSORTIUM

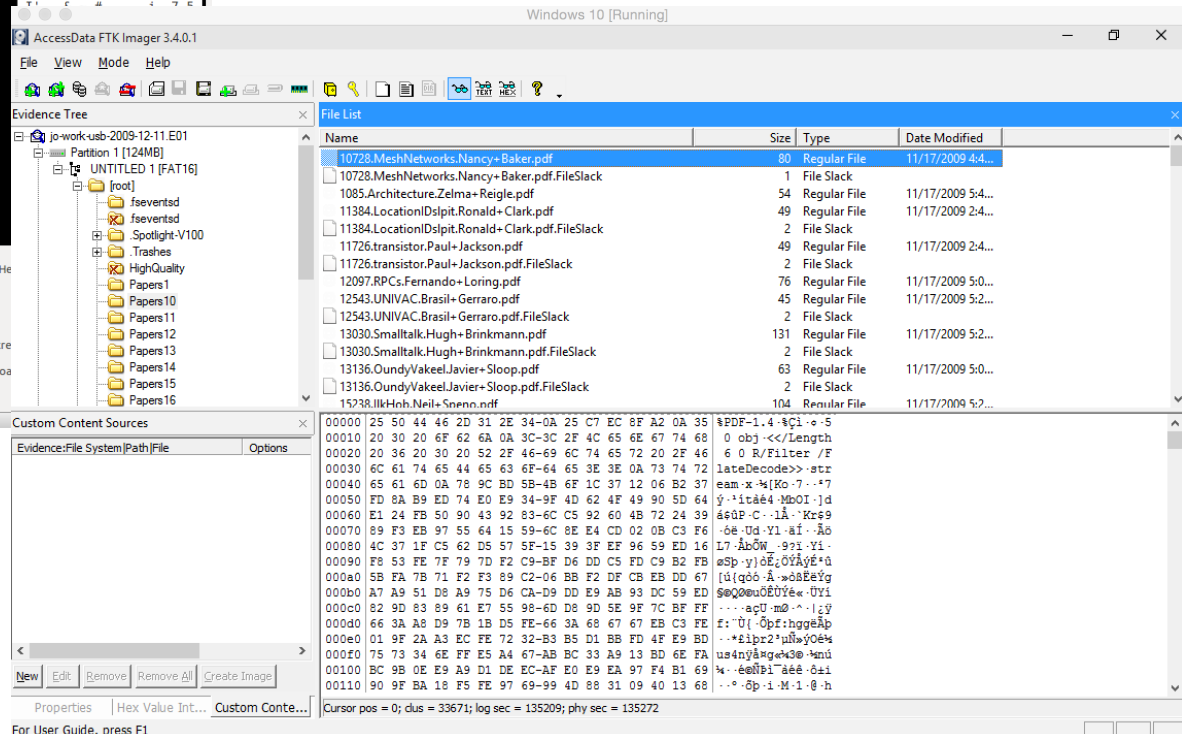
The Andrew W. Mellon Foundation



Lot of ways to look at this data once it has been captured, but many of these tools require significant expertise



Hex view of the disk image



Most forensics tools provide basic viewing capabilities (hex and native). Sophisticated analytics are generally limited to commercial tools.

...can we do better?

The BitCurator Access Project

BitCurator Access is a two-year Andrew W. Mellon Foundation funded project (October 1, 2014 – September 30, 2016) housed in the School of Information and Library Science at the University of North Carolina at Chapel Hill.

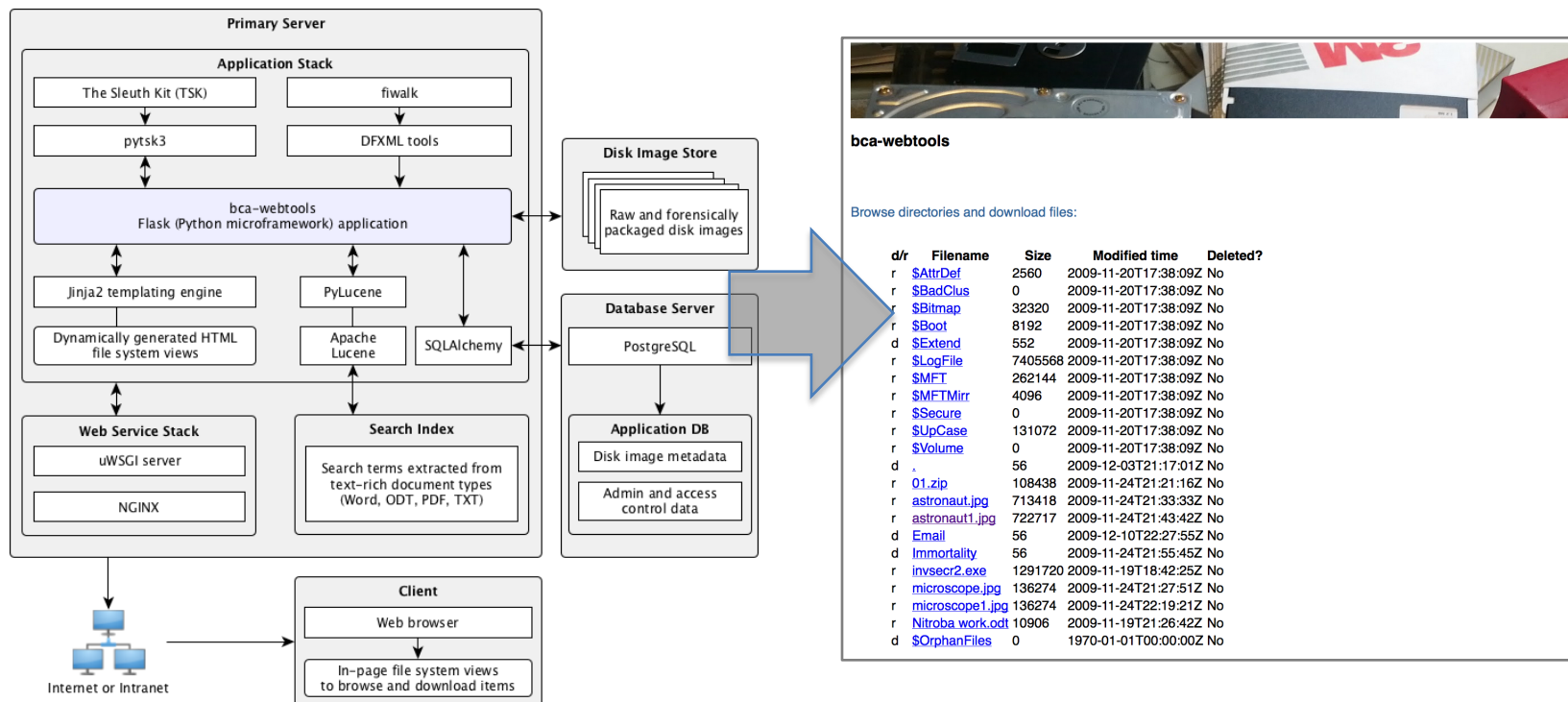
We're developing open source software to support access to disk images. Three core approaches:

- (1) **Tools and reusable libraries to support web access services for disk images**
- (2) Analyzing contents of file systems and associated metadata
- (3) Redacting complex born-digital objects (disk images) and emulated access to redacted images

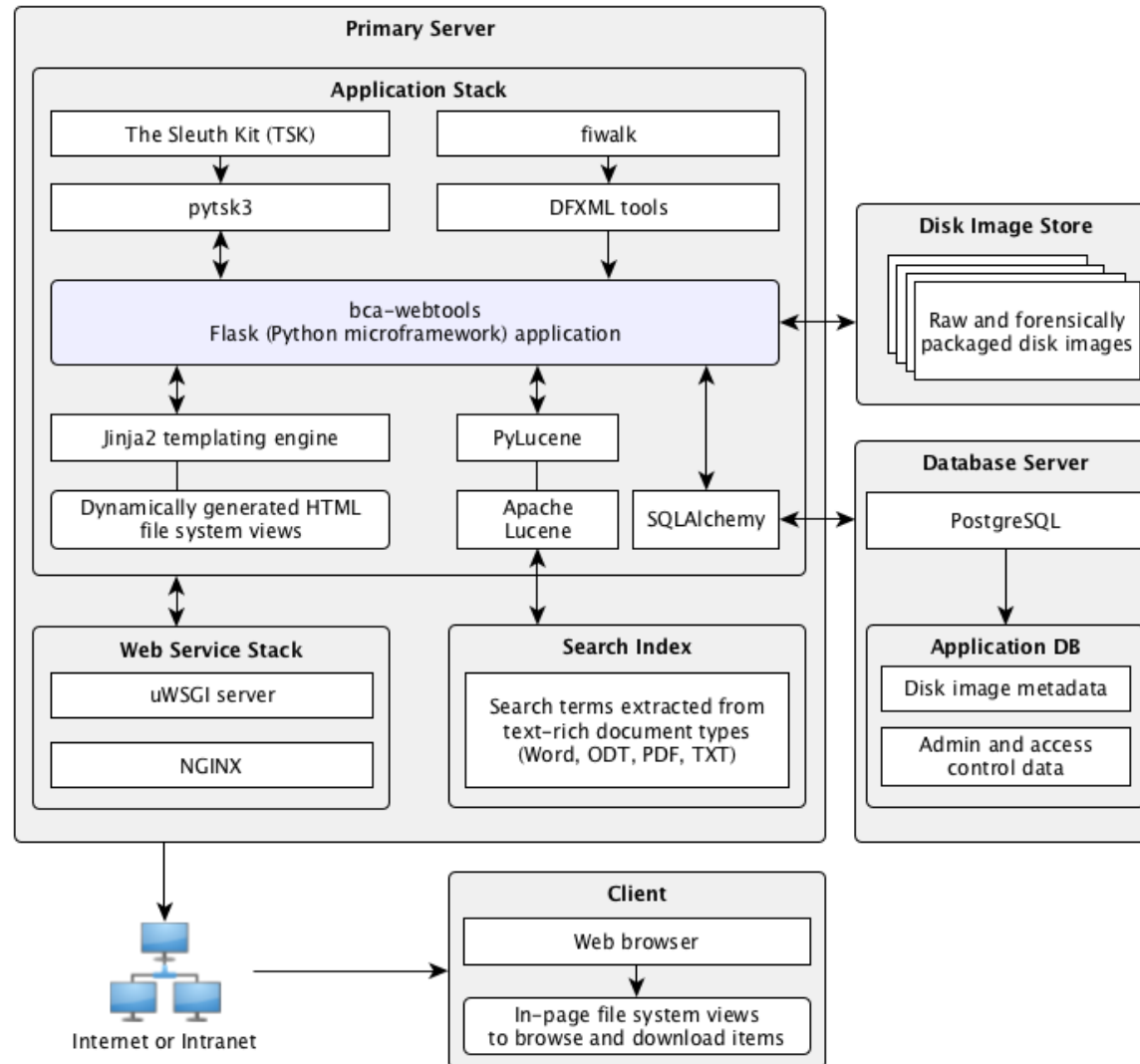
Web access to disk images: (bca-webtools)

Using lightweight web service tools along with digital forensics libraries to produce sophisticated navigation and management interfaces for disk images via a web browser.

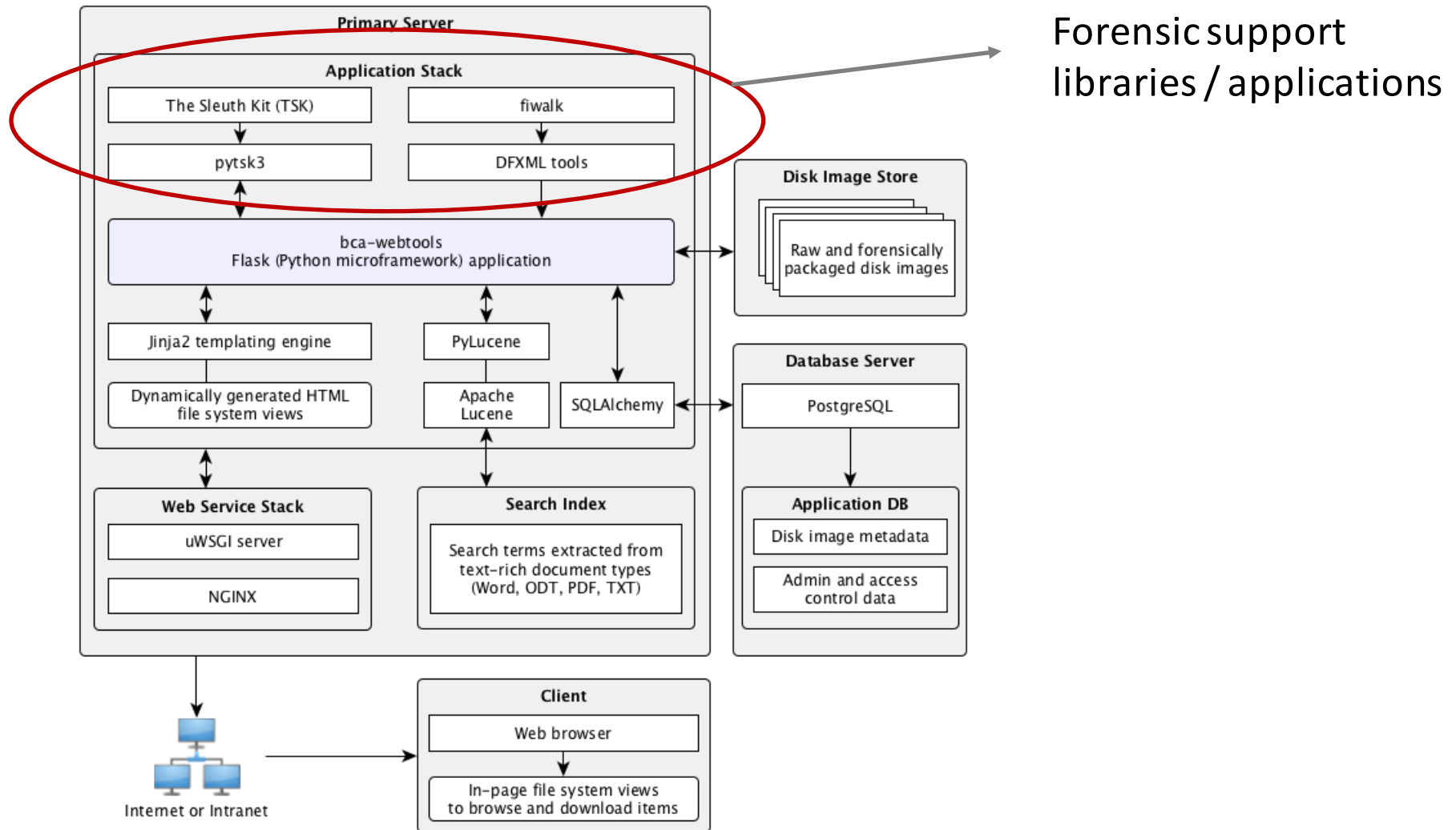
Drop your disk images into a network accessible location, start the service, and begin browsing.



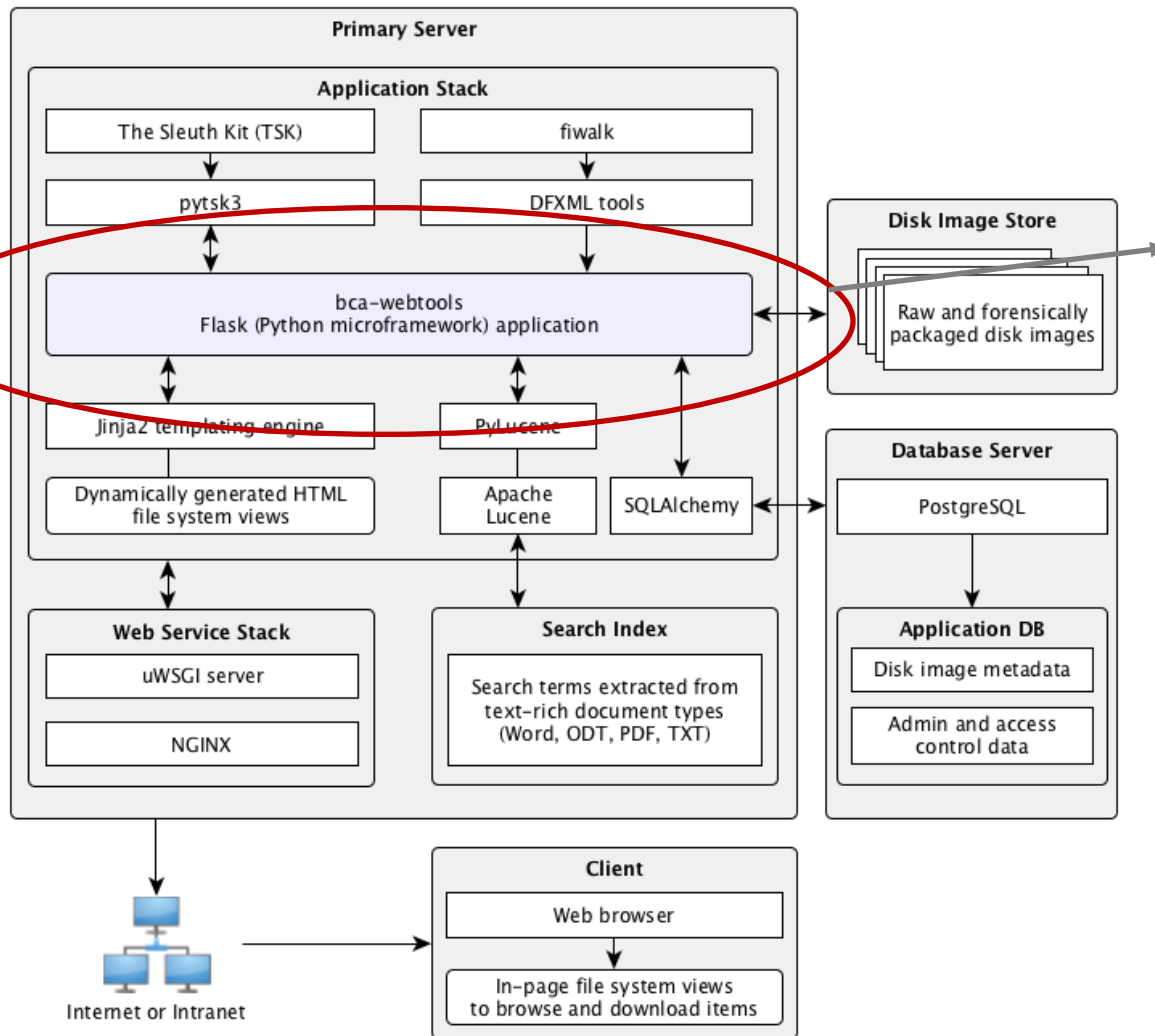
Web access to disk images: (bca-webtools)



Web access to disk images: (bca-webtools)

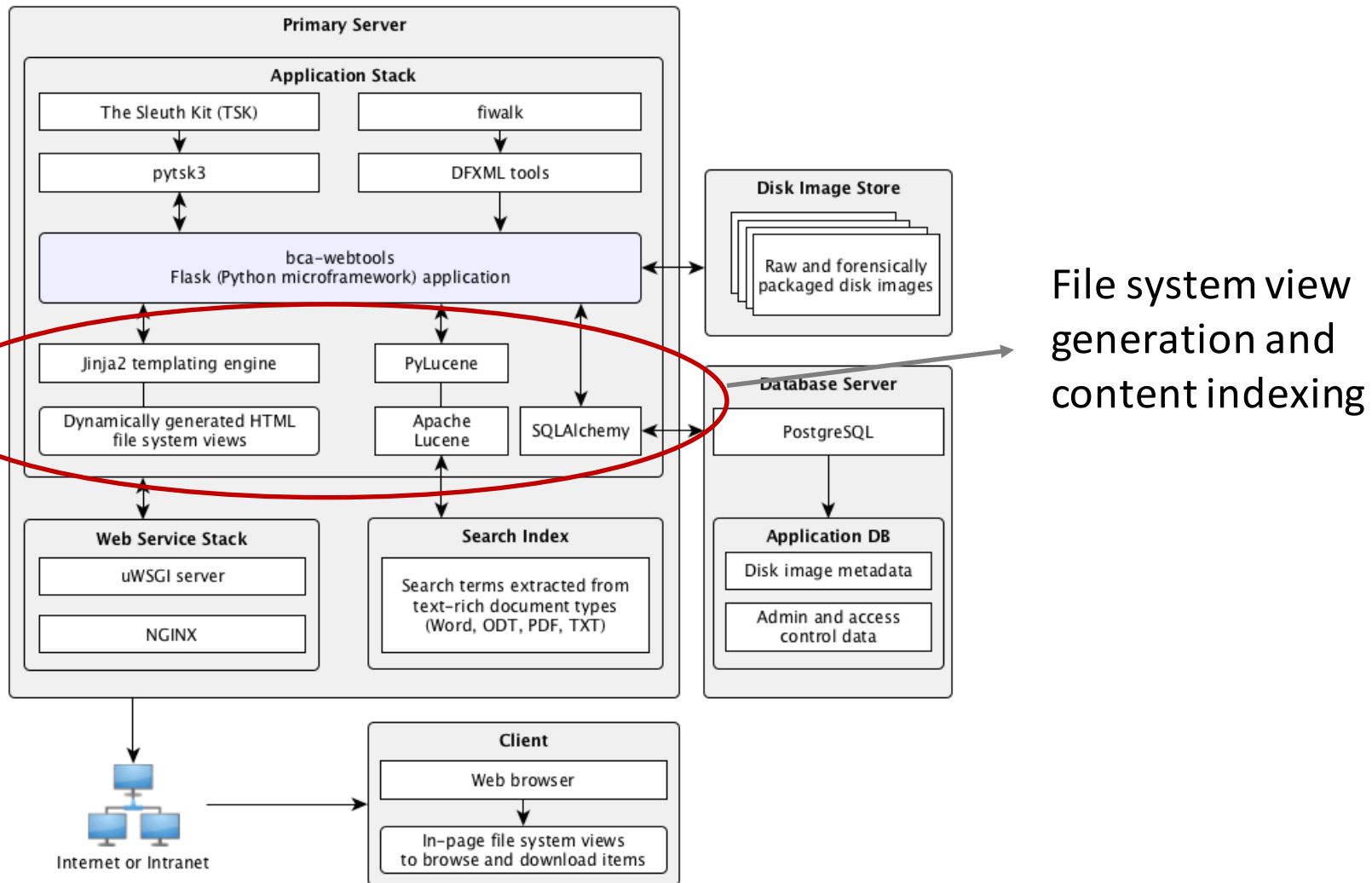


Web access to disk images: (bca-webtools)



Web microservices framework

Web access to disk images: (bca-webtools)



Web access to disk images: (bca-webtools)

The screenshot shows a web browser window with the address bar displaying "127.0.0.1:8080". The page title is "Disk Image Access for the \ x". The BCA Webtools logo is prominently displayed at the top left. Below the logo, a "Home" link is visible. The main content area contains a descriptive paragraph about the application's capabilities and a table of available disk images. To the right, there are search options and a note about the software's beta status.

BCA Webtools

[Home](#)

The bca-webtools application provides access to forensically-packaged (.E01 and .AFF) disk images. Supported file systems include FAT16, FAT32, NTFS, HFS+, and EXT2/3/4. Click on 'Browse' to navigate through the file system(s) within the disk image, or 'Download' to download the complete disk image.

Image Name	Info	Browse	Download
charlie-work-usb-2009-12-11.E01			
nps-2010-emails.E01			
nps-2013-canon1.E01			
terry-work-usb-2009-12-11.E01			

Select an option below to search available disk images by filename or file contents. (Currently indexing all filenames, contents of .doc, .odt, .pdf, and .txt)

☐ Search by filename

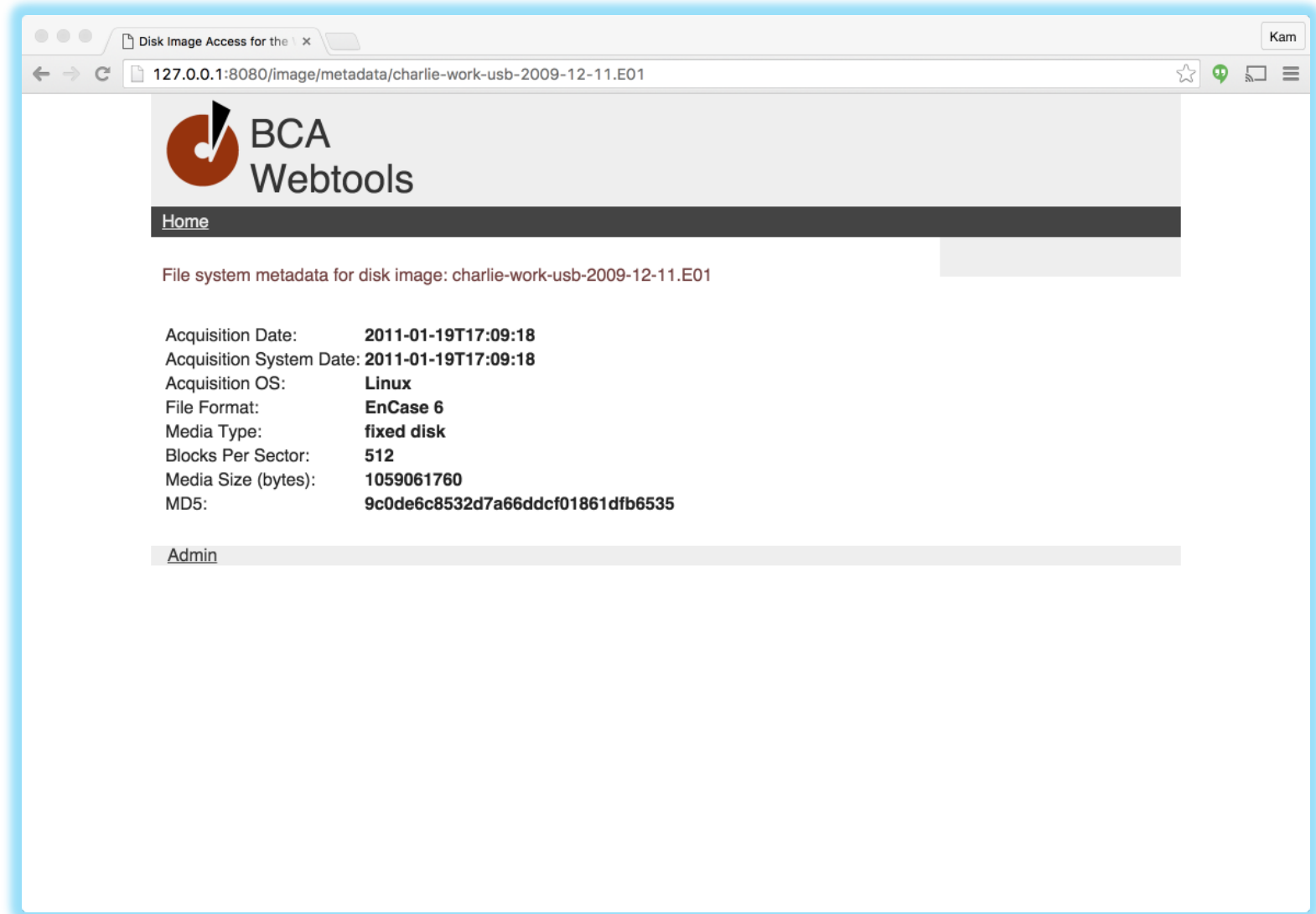
☒ Search by content

Note: This software is in beta. You must populate the DFXML database and generate a search index prior to searching.

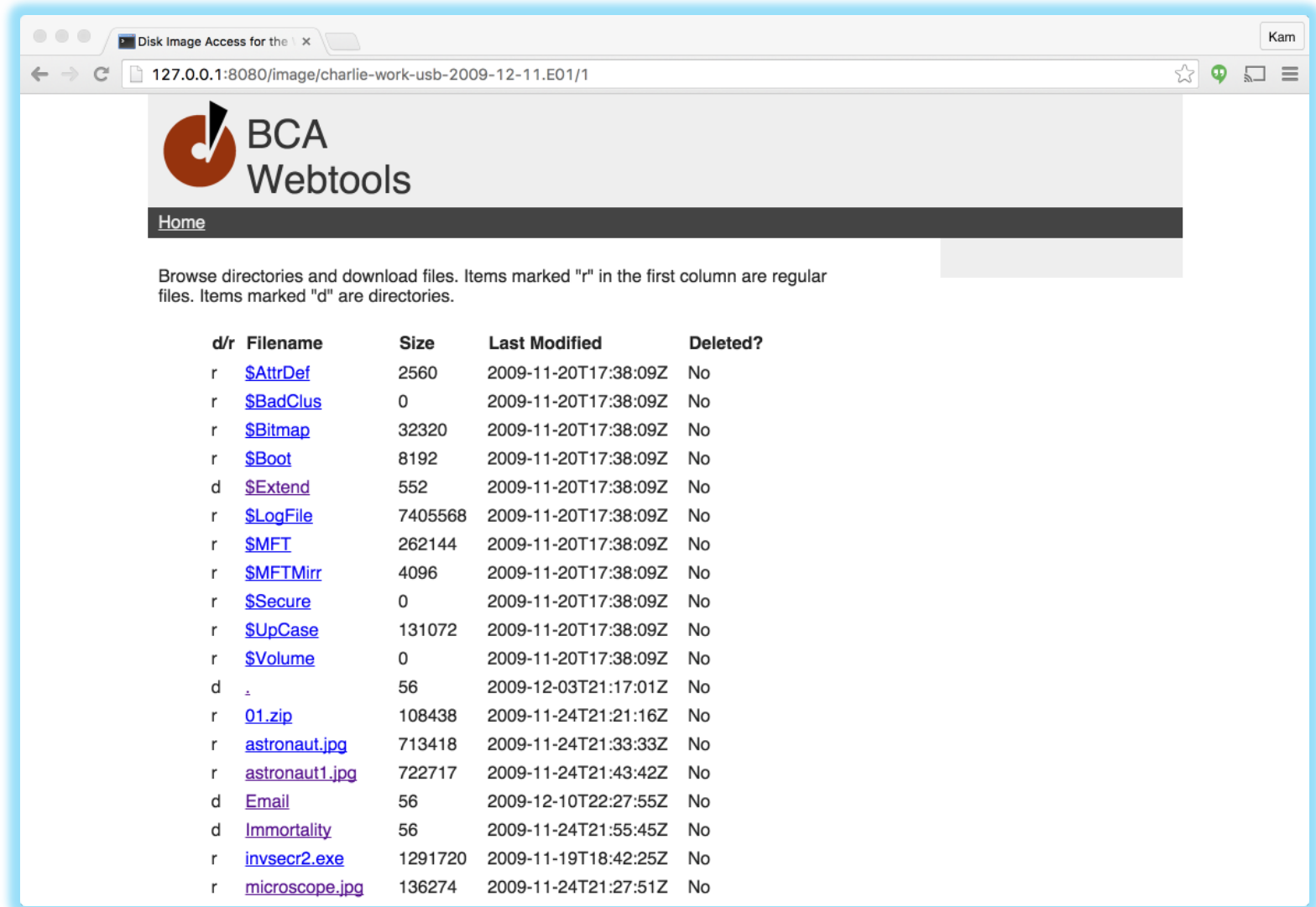
Visit the "Admin" link and select "Build DFXML Table" to enable search by filename. Select "Generate Index" to build the primary content search index.

[Admin](#)

Web access to disk images: (bca-webtools)



Web access to disk images: (bca-webtools)



127.0.0.1:8080/image/charlie-work-usb-2009-12-11.E01/1

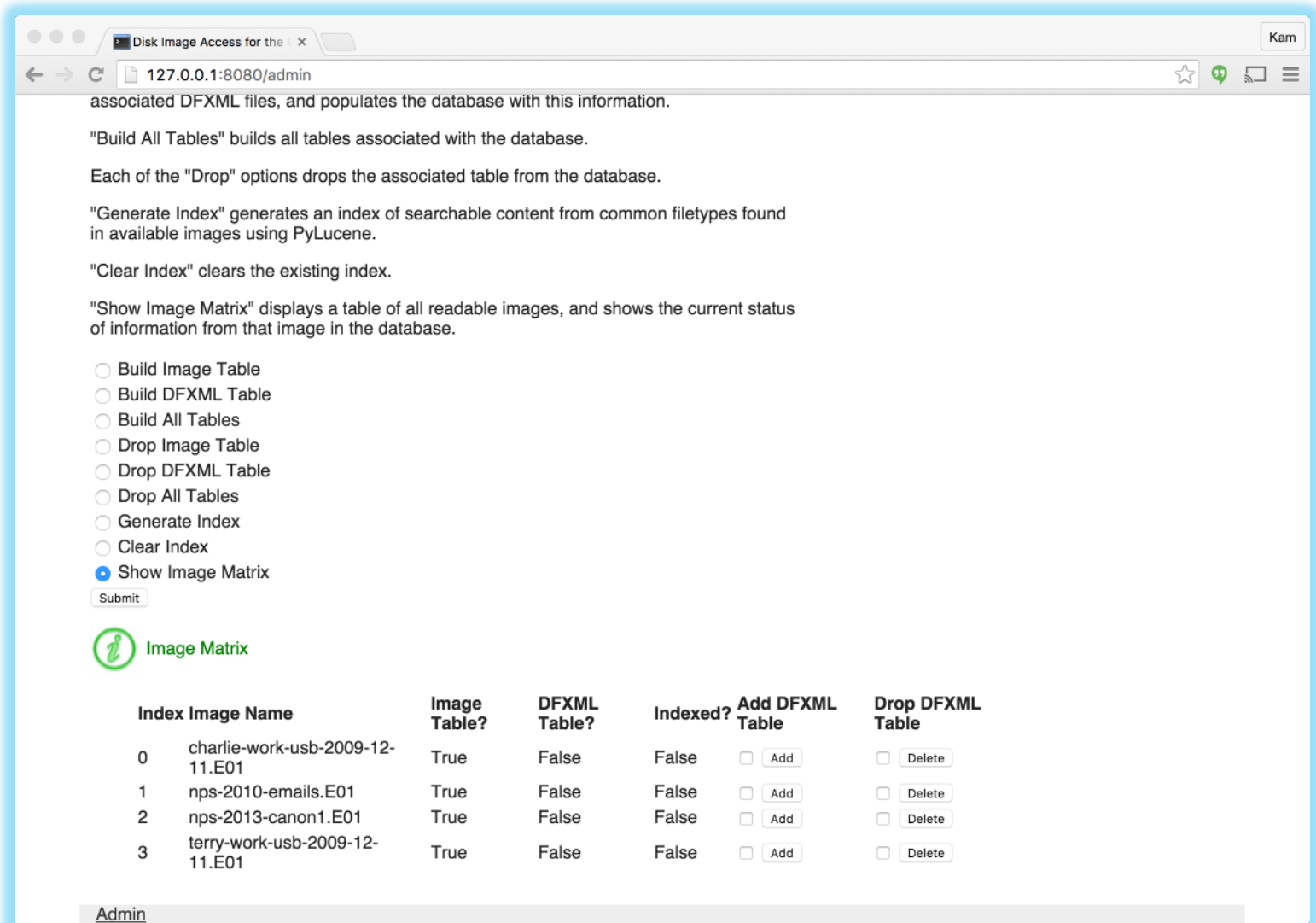
BCA Webtools

[Home](#)

Browse directories and download files. Items marked "r" in the first column are regular files. Items marked "d" are directories.

d/r	Filename	Size	Last Modified	Deleted?
r	\$AttrDef	2560	2009-11-20T17:38:09Z	No
r	\$BadClus	0	2009-11-20T17:38:09Z	No
r	\$Bitmap	32320	2009-11-20T17:38:09Z	No
r	\$Boot	8192	2009-11-20T17:38:09Z	No
d	\$Extend	552	2009-11-20T17:38:09Z	No
r	\$LogFile	7405568	2009-11-20T17:38:09Z	No
r	\$MFT	262144	2009-11-20T17:38:09Z	No
r	\$MFTMirr	4096	2009-11-20T17:38:09Z	No
r	\$Secure	0	2009-11-20T17:38:09Z	No
r	\$UpCase	131072	2009-11-20T17:38:09Z	No
r	\$Volume	0	2009-11-20T17:38:09Z	No
d	.	56	2009-12-03T21:17:01Z	No
r	01.zip	108438	2009-11-24T21:21:16Z	No
r	astronaut.jpg	713418	2009-11-24T21:33:33Z	No
r	astronaut1.jpg	722717	2009-11-24T21:43:42Z	No
d	Email	56	2009-12-10T22:27:55Z	No
d	Immortality	56	2009-11-24T21:55:45Z	No
r	invsecr2.exe	1291720	2009-11-19T18:42:25Z	No
r	microscope.jpg	136274	2009-11-24T21:27:51Z	No

Web access to disk images: (bca-webtools)



associated DFXML files, and populates the database with this information.

"Build All Tables" builds all tables associated with the database.


Each of the "Drop" options drops the associated table from the database.

"Generate Index" generates an index of searchable content from common filetypes found in available images using PyLucene.

"Clear Index" clears the existing index.

"Show Image Matrix" displays a table of all readable images, and shows the current status of information from that image in the database.

- ☐ Build Image Table
- ☐ Build DFXML Table
- ☐ Build All Tables
- ☐ Drop Image Table
- ☐ Drop DFXML Table
- ☐ Drop All Tables
- ☐ Generate Index
- ☐ Clear Index
- ☒ Show Image Matrix

 **Image Matrix**

	Index Image Name	Image Table?	DFXML Table?	Indexed?	Add DFXML Table	Drop DFXML Table
0	charlie-work-usb-2009-12-11.E01	True	False	False	<input type="checkbox"/> Add	<input type="checkbox"/> Delete
1	nps-2010-emails.E01	True	False	False	<input type="checkbox"/> Add	<input type="checkbox"/> Delete
2	nps-2013-canon1.E01	True	False	False	<input type="checkbox"/> Add	<input type="checkbox"/> Delete
3	terry-work-usb-2009-12-11.E01	True	False	False	<input type="checkbox"/> Add	<input type="checkbox"/> Delete

Admin

My Research

A few of the BitCurator team's friends (partners, advisors, or funders):



...and many others contributing in the Google Group:

<https://groups.google.com/forum/#!forum/bitcurator-users>

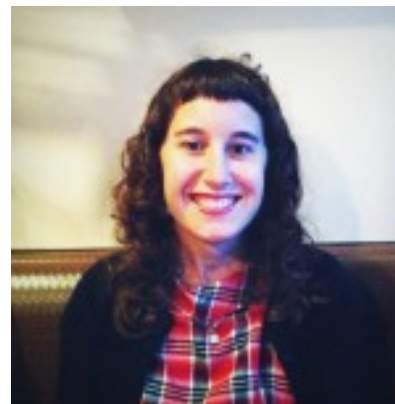
The BitCurator Access Team



Cal Lee
PI



Kam Woods -
Technical Lead
and Co-PI



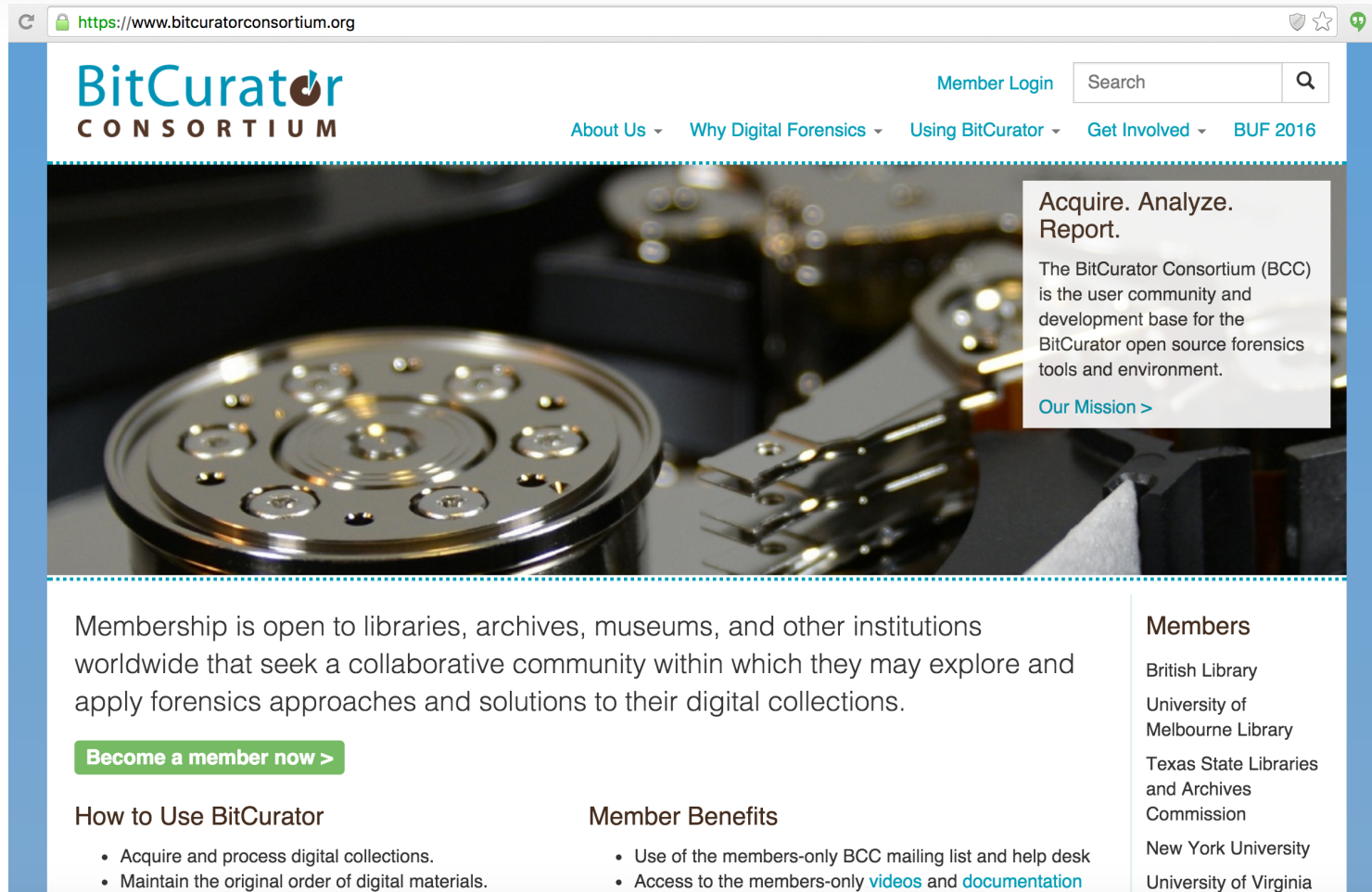
Alex Chassanoff
Project Manager



Sunitha Misra
Software
Developer

...and our advisory board: <http://www.bitcurator.net/bitcurator-access-people/>

Ongoing support for the BitCurator environment is being managed by the BitCurator Consortium



The screenshot shows the BitCurator Consortium website. The header includes the logo, a search bar, and navigation links. The main content area features a large image of a hard drive platter and a text box describing the consortium's mission. Below this, there are sections for membership, benefits, and a list of member institutions.

<https://www.bitcuratorconsortium.org>

BitCurator
CONSORTIUM

Member Login Search

[About Us](#) [Why Digital Forensics](#) [Using BitCurator](#) [Get Involved](#) [BUF 2016](#)

Acquire. Analyze. Report.

The BitCurator Consortium (BCC) is the user community and development base for the BitCurator open source forensics tools and environment.

[Our Mission >](#)

Membership is open to libraries, archives, museums, and other institutions worldwide that seek a collaborative community within which they may explore and apply forensics approaches and solutions to their digital collections.

[Become a member now >](#)

How to Use BitCurator

- Acquire and process digital collections.
- Maintain the original order of digital materials.

Member Benefits

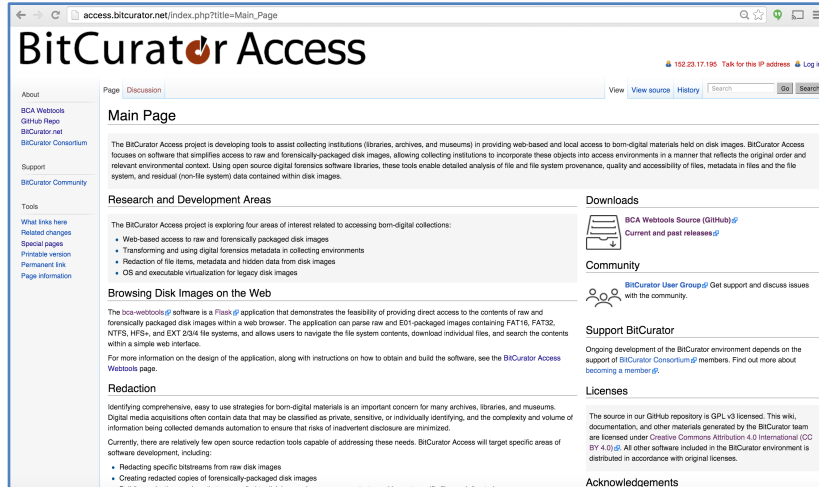
- Use of the members-only BCC mailing list and help desk
- Access to the members-only [videos](#) and [documentation](#)

Members

- British Library
- University of Melbourne Library
- Texas State Libraries and Archives Commission
- New York University
- University of Virginia

<https://www.bitcuratorconsortium.org/>

BitCurator Access and BitCurator Environment Resources



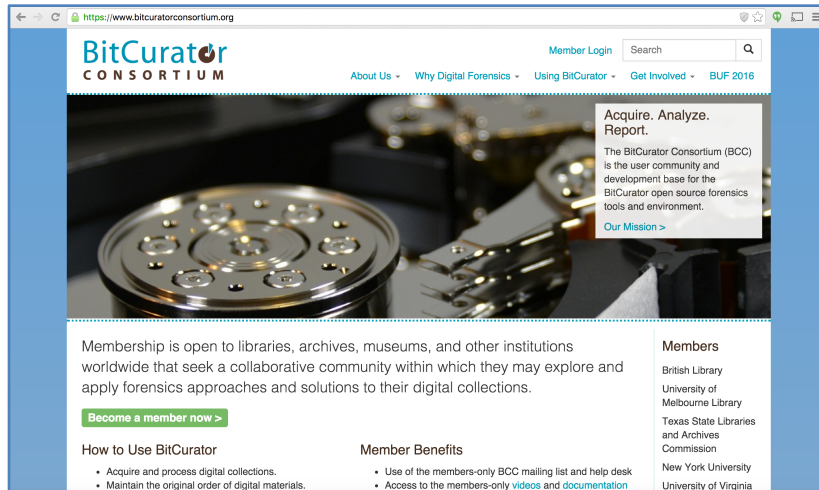
Software

Documentation

Google Group

<http://wiki.bitcurator.net/>

<http://access.bitcurator.net/>



Project overview

Publications

News

Consortium and Membership

<http://www.bitcurator.net/>

<https://www.bitcuratorconsortium.org/>

Or find the research group on Twitter: @bitcurator