State Electronic Records Initiative, Introductory Electronic Records Institute
July 8-12, 2013, Indianapolis, Indiana
Acquisition Lab Exercise Instructions
Instructor: Cal Lee

You work at the Archives of State X. In response to deep budget cuts, the executive branch has recently undergone a major reorganization and reduction of personnel. This has included the elimination of the Department of Configuration Management (DCM) from within the state's Office of Information Technology. On her last day of her employment, the assistant to the Director of DCM (who also served as the records officer) has sent you several boxes full of records from the now-defunct unit. She tells you that all of the boxes contain at least some records that have been scheduled for permanent retention by the state archives.

One of the boxes is full of physical media (CDs, floppies, and an external hard drive). In some cases, she could tell you specifically what was on them and why it was important to retain the records. In other cases, she could only recall that the contents of the media were part of the DCM's efforts to compare configuration management efforts across different states in the U.S.

You examined one of the CDs. There are no labels on the CD itself, but the case containing it has a sticker that reads "Files." You loaded the CD into a drive and used FTK Imager to create a disk image of the CD. You then used FTK Imager to export the files, which you can now find in files.zip. For purposes of tasks 1-4, you should work from files.zip.

Summary of Tools Used in this Exercise

The following tools will be used to illustrate fundamental tasks and concepts. This is not a recommendation or endorsement of any specific applications. These are all applications that run in Windows. There are similar tools that run in Macintosh and Linux/Unix environments. For a suite of free, open-source tools that can perform a variety of forensics tasks, see: http://wiki.bitcurator.net.

- Tool to generate file hashes: md5summer [http://download.cnet.com/MD5summer/3000-2248_4-10050856.html]
- Hex viewer and editor: Cygnus Hex Editor [http://download.cnet.com/Cygnus-Hex-Editor-Free-Edition/3000-2352_4-10448945.html]
- Tool for mounting an ISO file so that Windows treats it like just another drive on your computer: MagicDisc [http://www.magiciso.com/tutorials/miso-magicdisc-history.htm]
- FTK Imager [http://accessdata.com/support/adownloads#FTKImager]

Task 0 – Preparation

- Copy the following:
    - files.zip [http://www.ils.unc.edu/callee/files.zip - save to your desktop]
    - files.iso [http://www.ils.unc.edu/callee/files.iso - save to your desktop]
- Create a folder on your desktop called dcm-files, then extract the contents of files.zip to that folder

Task Set 1 – Seeing what you have – looking in dcm-files

Inspection at the file level

- Based simply on the properties and names of the files and directories (don't open any files yet), try to make some inferences about what these files are and how they might be related.

Looking at names of specific files

- Find a file called Circular.596

- Do you see any other files that have similar names? If so, make note of which ones they are.

Inspection at the bitstream level

- Generate a hex view of the file called Circular.596 – using Cygnus Hex Editor
- What can you infer about this file from looking at the hex representation?
- If you identified other files in task 2, also view those in hex view. Do you notice anything similar?

Investigating the .ISO (disk image) file

- Open FTK Imager
- Go to File | Add Evidence Item…
- Select "Image File"
- Browse to files.iso and then select "Finish"
- Navigate the file tree and discuss what you observe

Task Set 2 – Investigation based on hash values

NOTE: These tasks are based on using md5summer in Windows. You can also generate individual file hashes from the command line in Mac/Unix with the md5 command or use the online utility: at http://www.webutils.pl/MD5_Calculator.

Generate hashes

- Open md5summer
- Select bigschat-files as the root folder
- Select "Create Sums"
- In the "Create list of files to sum" dialog, navigate to the dcm-files folder on your desktop, then select all of the contents of that folder and select "Add"
- Click "Ok"
- Confirm that the md5 hashes are generated
- "Save as" to your desktop as bigshat-files.md5
- Leave the md5summer application running

Finding duplicate files

- Look at the MD5 value of Circular.596
- If you identified other files in task 2, are the values the same or different?
- If you notice something interesting about the MD5 values, what can you infer about what happened to the files?

Verify hash values

- Go back to md5summer (launch it again if you closed the application)
- Select "Verify sums"
- Select the "dcm-files" directory as your root folder
- At the "Open md5sum file" dialog, select bigschat-files.md5 from your desktop and select "Open"
- Note whether there are green dots (verified) by the files or red dots (errors)

Opening files with hex editor

- Pick one or more items from the "files" folder and open them in Cygnus Hex Editor (you can drag the file onto the Cygnus icon on your desktop)
- Look at the hex view of each file and see what it reveals about the bitstream content of the file

Changing content with hex editor

- For one or more of the files, change a bit within the file in Cygnus Hex Editor and then save the changed file
- Note which files you've changed and the SPECIFIC PLACE in the files where you changed bits

Re-Verify hash values

- Be sure to exit out of Cygnus Hex Editor (if files are open in it, the hash calculation might not work correctly)
- Go back to md5summer (launch it again if you closed the application)
- Select "Verify sums"
- Select the "dcm-files" directory as your root folder
- At the "Open md5sum file" dialog, select dcm-files.md5 from your desktop and select "Open"
- Note whether there are green dots (verified) by the files or red dots (errors)

Change content back to earlier state in hex editor

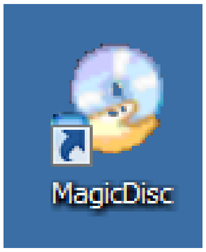
- Open one or more of the files that you changed earlier, and change the bits back to their previous state, and then save the changed file(s)

Re-Verify hash values

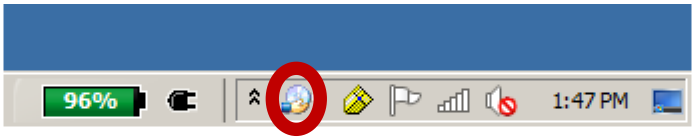
- Go back to md5summer (launch it again if you closed the application)
- Select "Verify sums"
- Select the "dcm-files" directory as your root folder
- At the "Open md5sum file" dialog, select bigschat-files.md5 from your desktop and select "Open"
- Note whether there are green dots (verified) by the files or red dots (errors)

Task Set 3 – Mounting a Disk Image

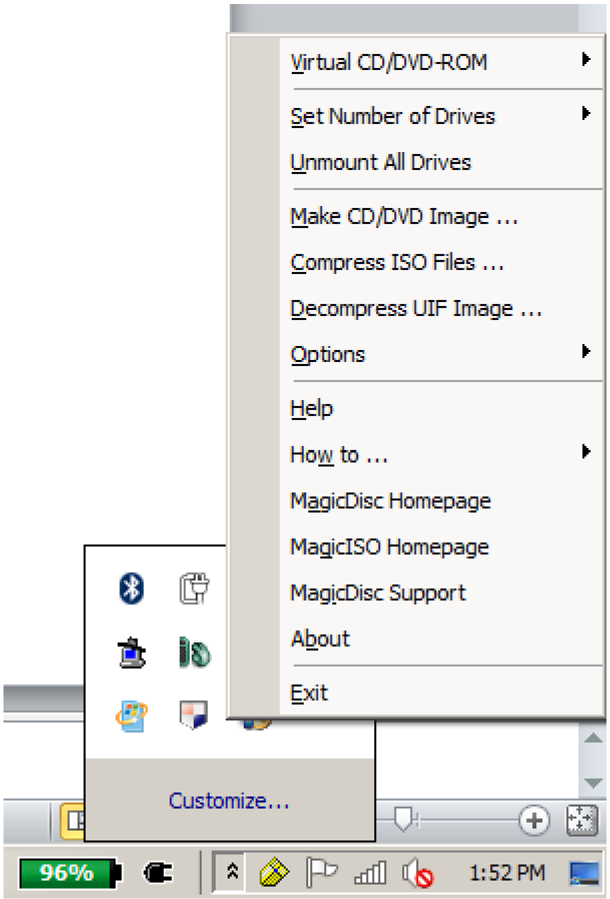
- Double click on the MagicDisc Icon



- MagicDisc will appear on the toolbar



- Browse to files.iso then select “Mount”

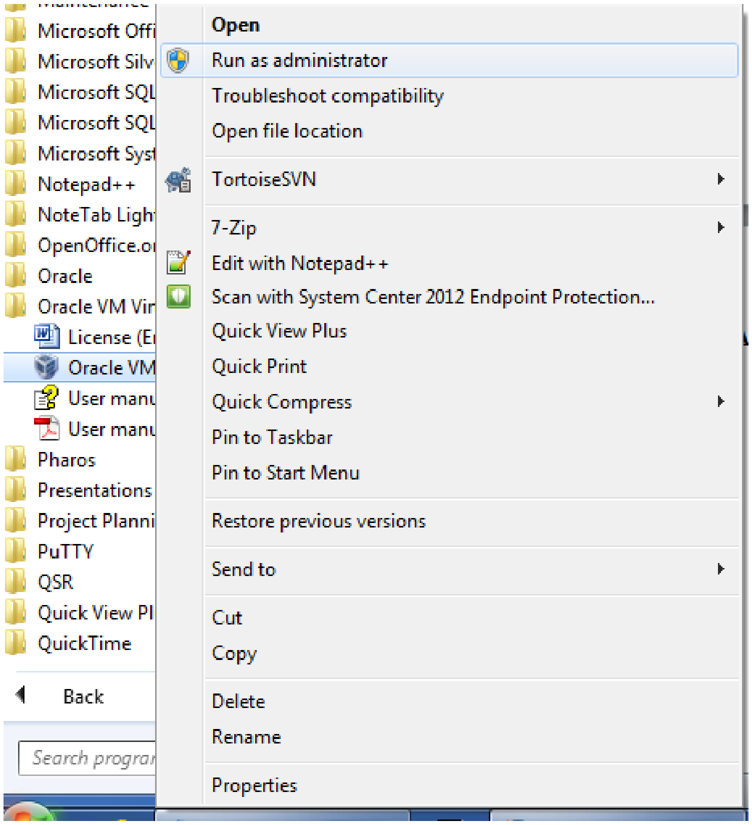


Task Set 4 – Using BitCurator

Note: The BitCurator environment is not running on the lab computers. We will be talking through the tasks listed below. I encourage you to download and install the BitCurator environment and try these tasks on your own. The software and installation instructions are at: http://wiki.bitcurator.net

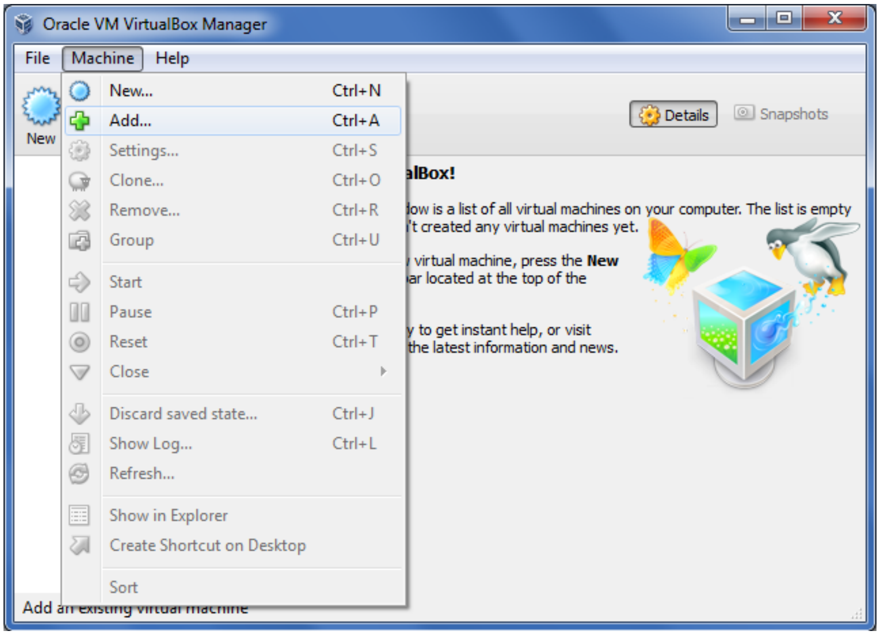
Start up Virtual Box

- Navigate to VirtualBox
- Right-click on the VirtualBox icon and select "Run as Administrator"



Add the BitCurator Virtual Machine

- From the Machine menu, select Add…



lBox!

low is a list of all virtual machines on your computer. The list is empty 't created any virtual machines yet.

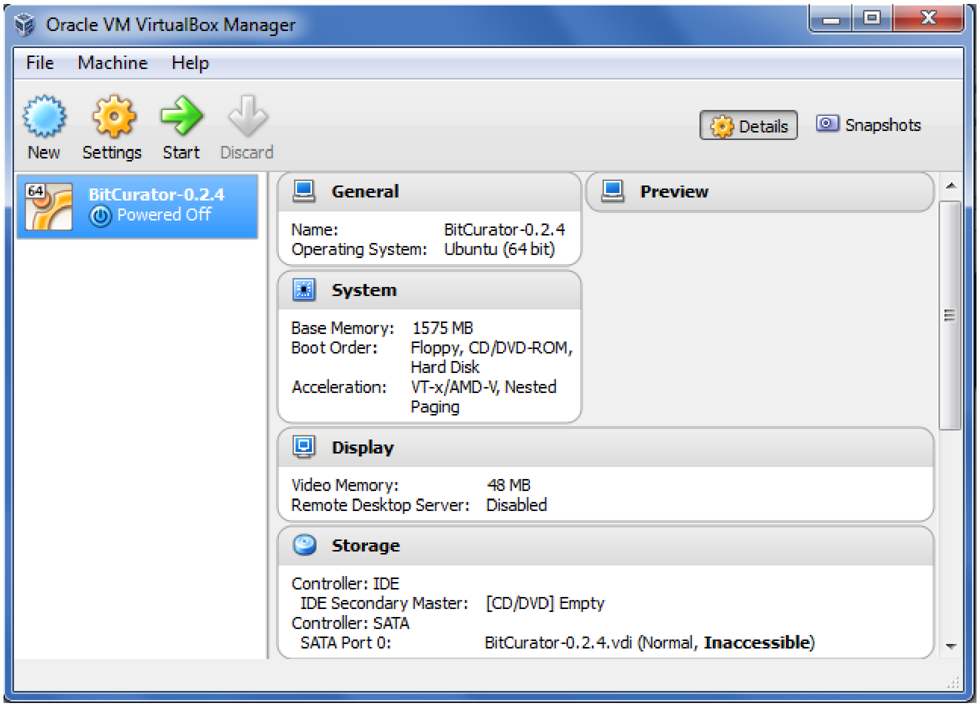
virtual machine, press the **New** ar located at the top of the

y to get instant help, or visit the latest information and news.

Add an existing virtual machine

- Navigate to C:\BitCurator\ and select the BitCurator VM file.
- Click on Open.

Start the BitCurator Virtual Machine



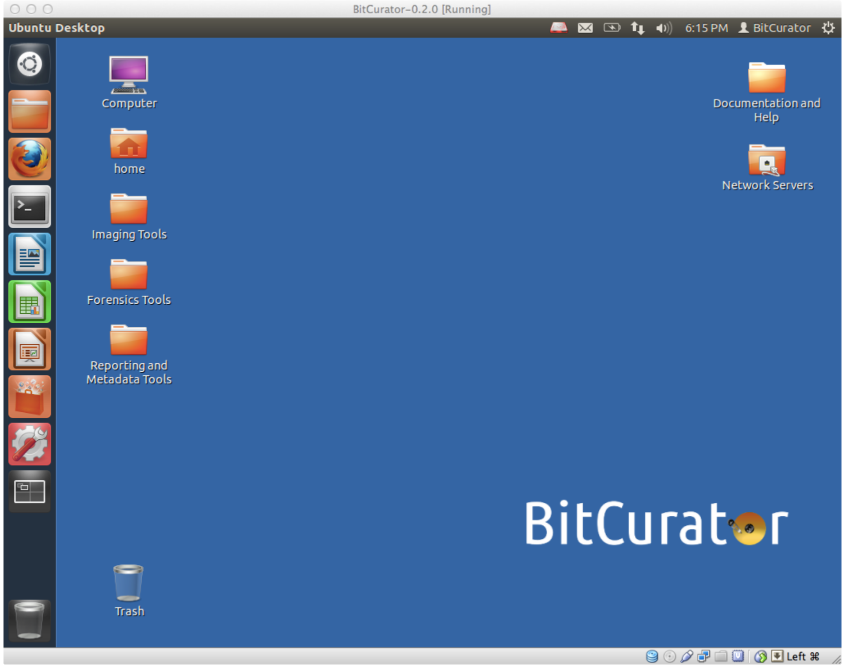
Name: BitCurator-0.2.4
Operating System: Ubuntu (64 bit)

Base Memory: 1575 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Video Memory: 48 MB
Remote Desktop Server: Disabled

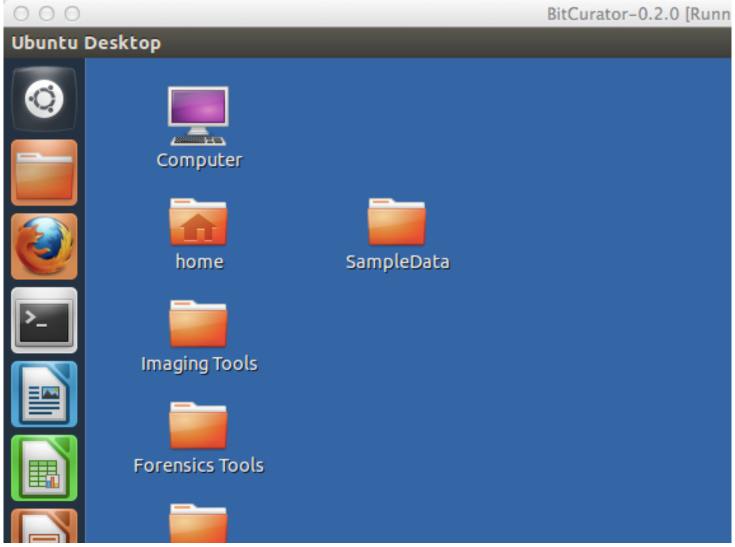
Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: BitCurator-0.2.4.vdi (Normal, **Inaccessible**)

- Clicking on the green "Start" arrow in the Manager screen will start the BitCurator environment. You'll see a startup screen, and then the BitCurator environment will boot and automatically log in.



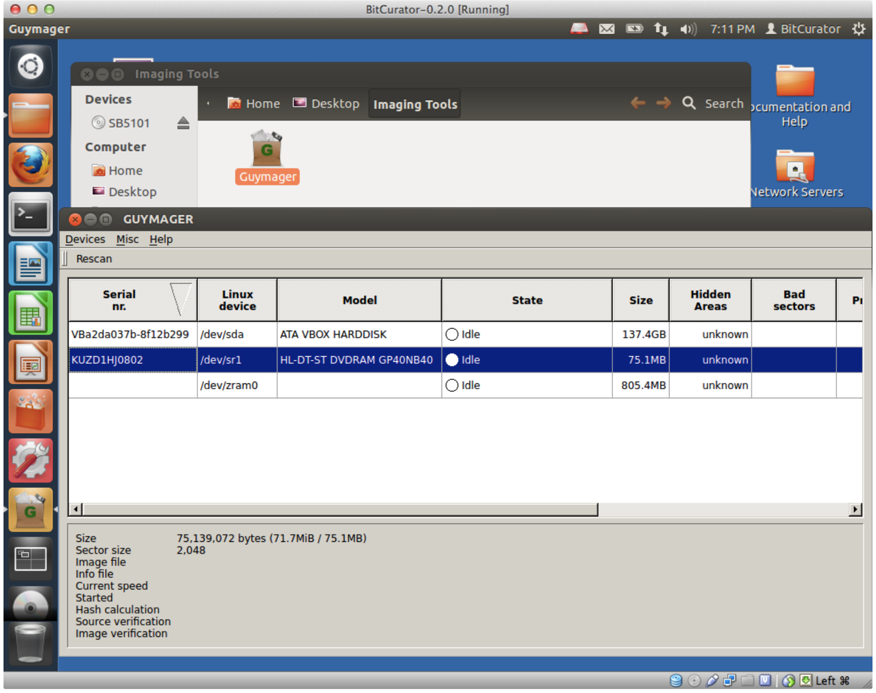
Adding a folder to hold disk images and output data

- Right-click anywhere on the desktop, and select "Create New Folder". A folder named "Untitled Folder" will appear on the Desktop.
- Click on the name and rename it to "SampleData". We'll use this location to store the data for the rest of the exercise.



Imaging a disk

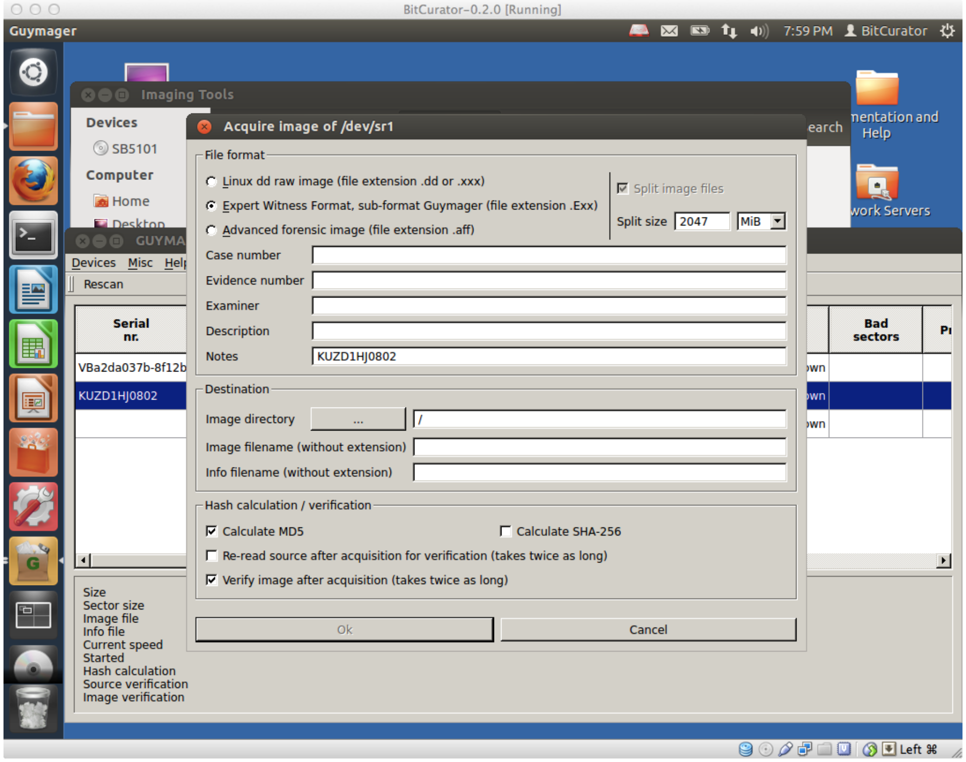
- Make sure that your flash drive is plugged into the computer.
- Double-click on “Imaging Tools” on the Desktop, and then double-click on Guymager. The CD-ROM is selected in the picture above.



Serial nr.	Linux device	Model	State	Size	Hidden Areas	Bad sectors	Pr
VBa2da037b-8f12b299	/dev/sda	ATA VBOX HARDDISK	○ Idle	137.4GB	unknown		
KUZD1HJ0802	/dev/sr1	HL-DT-ST DVDRAM GP40NB40	● Idle	75.1MB	unknown		
	/dev/zram0		○ Idle	805.4MB	unknown		

Size	75,139,072 bytes (71.7MiB / 75.1MB)
Sector size	2,048
Image file	
Info file	
Current speed	
Started	
Hash calculation	
Source verification	
Image verification	

- Right-click on the item that represents the flash drive, and click on “Acquire image” in the menu. You’ll see a new dialog window appear, which will prompt you to enter some acquisition metadata.



Acquire image of /dev/sr1

File format

○ Linux dd raw image (file extension .dd or .xxx)
● Expert Witness Format, sub-format Guymager (file extension .Exx)
○ Advanced forensic image (file extension .aff)

☑ Split image files
Split size 2047 MiB

Case number
Evidence number
Examiner
Description
Notes KUZD1HJ0802

Destination

Image directory ... /
Image filename (without extension)
Info filename (without extension)

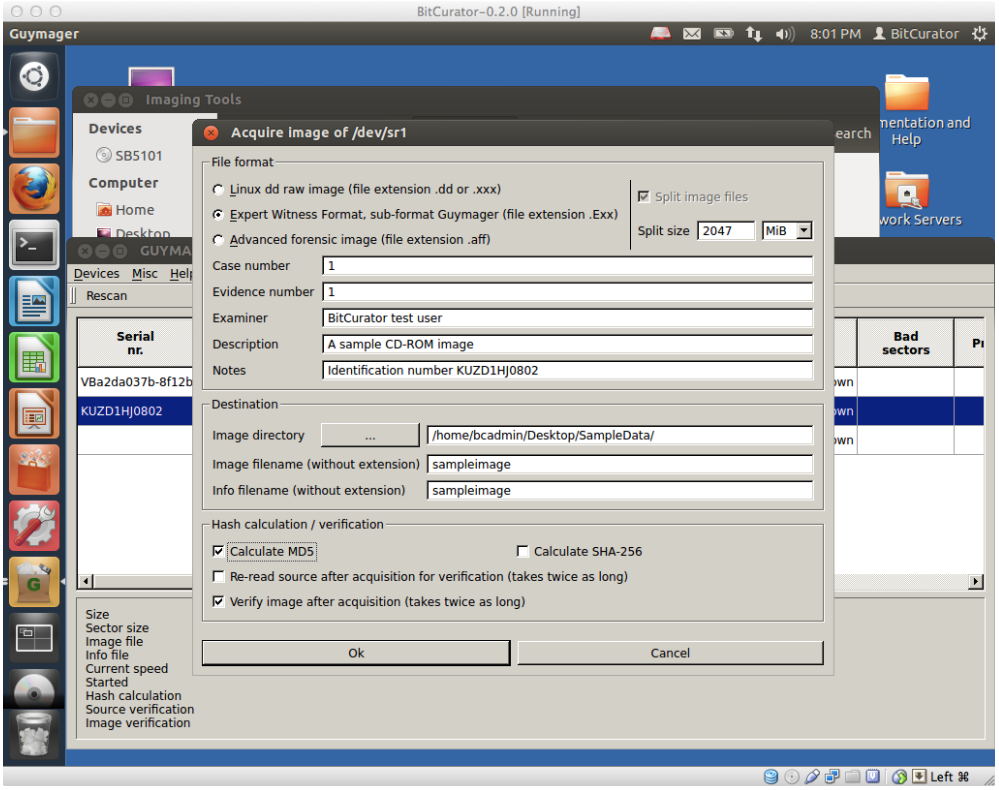
Hash calculation / verification

☑ Calculate MD5 ☐ Calculate SHA-256
☐ Re-read source after acquisition for verification (takes twice as long)
☑ Verify image after acquisition (takes twice as long)

Serial nr.	Bad sectors	Pr
VBa2da037b-8f12b		
KUZD1HJ0802		

Size
Sector size
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification

- Select an image format (the example below uses .e01) and enter some other metadata. For the “Image directory,” select the “SampleData” directory that you created earlier on the desktop, and name the image. Then click “Start”.



Acquire image of /dev/sr1

File format

○ Linux dd raw image (file extension .dd or .xxx)

● Expert Witness Format, sub-format Guymager (file extension .Exx)

○ Advanced forensic image (file extension .aff)

☑ Split image files

Split size 2047 MiB

Case number	1
Evidence number	1
Examiner	BitCurator test user
Description	A sample CD-ROM image
Notes	Identification number KUZD1HJ0802

Destination

Image directory ...	/home/bcadmin/Desktop/SampleData/
Image filename (without extension)	sampleimage
Info filename (without extension)	sampleimage

Hash calculation / verification

☑ Calculate MD5 □ Calculate SHA-256

□ Re-read source after acquisition for verification (takes twice as long)

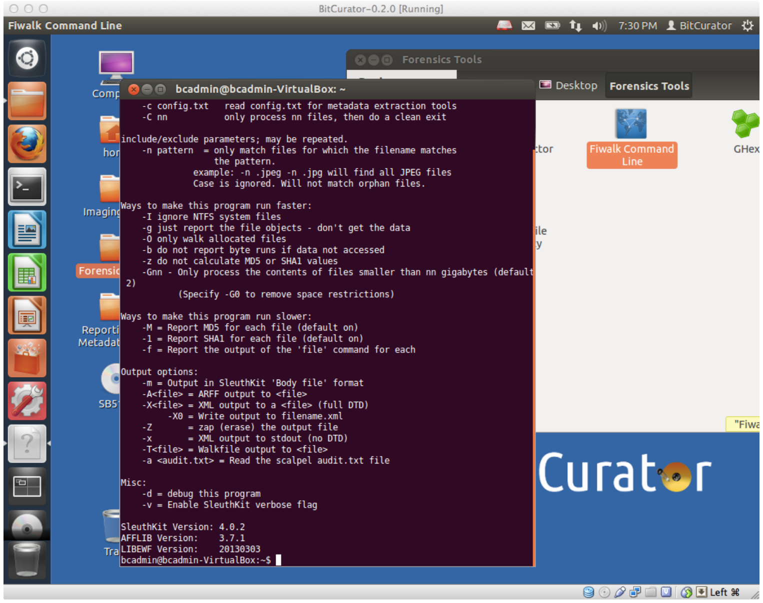
☑ Verify image after acquisition (takes twice as long)

Ok Cancel

- You’ll see the main dialog state change to “Acquisition Running”. Note that the BitCurator environment runs at a resolution of 1024x768 by default. If you wish to see the whole dialog, just make the window bigger. The resolution should resize automatically.
- Cancel the acquisition. We won’t have time to run the whole imaging process in this lab. Normally, you would wait for the acquisition to finish and see an “OK” message in State.
- Once the process has completed, in your SampleData folder, there should be two files: the .E01 image file, and a .info file specific to Guymager.

Producing a DFXML report of the File System Contents

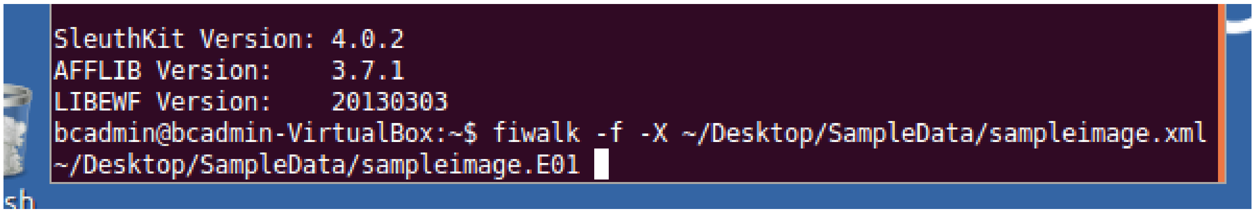
- Double-click on the “Forensics Tools” folder, and then double click on the “Fiwalk Command Line” launcher. You’ll see a terminal pop up and execute the help dialog for fiwalk.



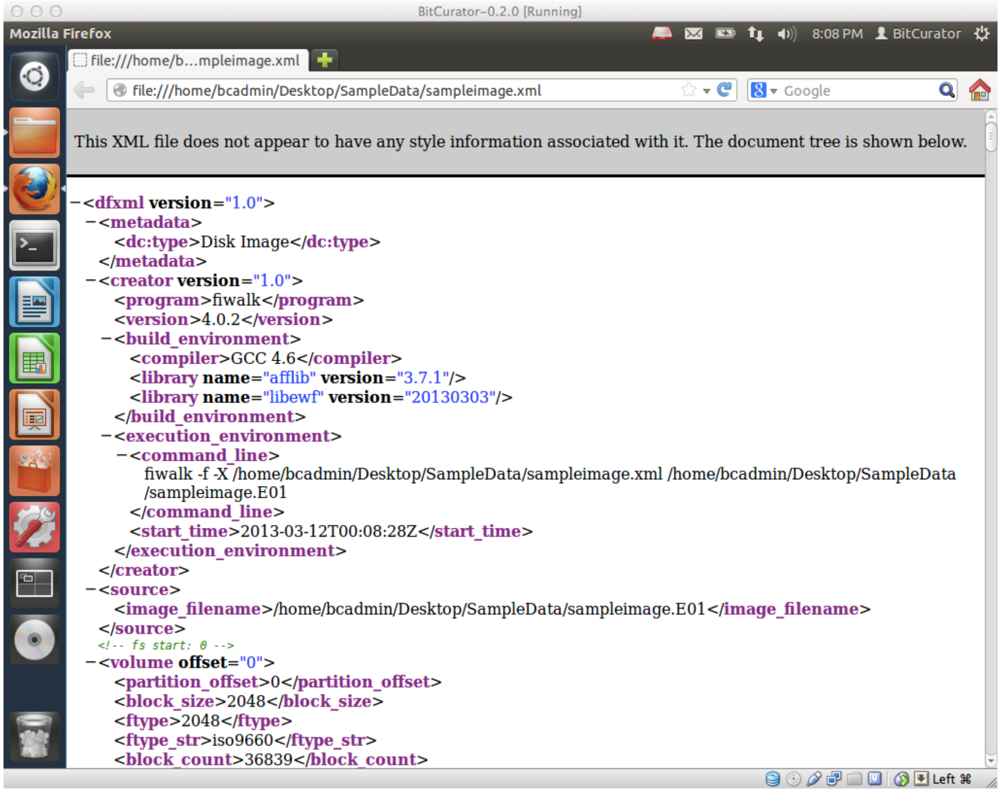
```
    -c config.txt   read config.txt for metadata extraction tools
    -C nn           only process nn files, then do a clean exit

include/exclude parameters; may be repeated.
    -n pattern  = only match files for which the filename matches
                  the pattern.
              example: -n .jpeg -n .jpg will find all JPEG files
              Case is ignored. Will not match orphan files.

Ways to make this program run faster:
    -I ignore NTFS system files
    -g just report the file objects - don't get the data
    -O only walk allocated files
    -b do not report byte runs if data not accessed
    -z do not calculate MD5 or SHA1 values
    -Gnn - Only process the contents of files smaller than nn gigabytes (default
 2)
           (Specify -G0 to remove space restrictions)

Ways to make this program run slower:
    -M = Report MD5 for each file (default on)
    -1 = Report SHA1 for each file (default on)
    -f = Report the output of the 'file' command for each

Output options:
    -m = Output in SleuthKit 'Body file' format
    -A<file> = ARFF output to <file>
    -X<file> = XML output to a <file> (full DTD)
        -X0 = Write output to filename.xml
    -Z       = zap (erase) the output file
    -x       = XML output to stdout (no DTD)
    -T<file> = Walkfile output to <file>
    -a <audit.txt> = Read the scalpel audit.txt file

Misc:
    -d = debug this program
    -v = Enable SleuthKit verbose flag

SleuthKit Version: 4.0.2
AFFLIB Version:    3.7.1
LIBEWF Version:    20130303
bcadmin@bcadmin-VirtualBox:~$
```

The fiwalk program needs to know three things:

1. Whether you want to run “file” to identify the file formats in the file   system (the ‘- f’ option)
2. The name of the DFXML file that will be produced (‘-X’, followed by the file path)
3. The name of the image to process.



```
SleuthKit Version: 4.0.2
AFFLIB Version:    3.7.1
LIBEWF Version:    20130303
bcadmin@bcadmin-VirtualBox:~$ fiwalk -f -X ~/Desktop/SampleData/sampleimage.xml
~/Desktop/SampleData/sampleimage.E01
```

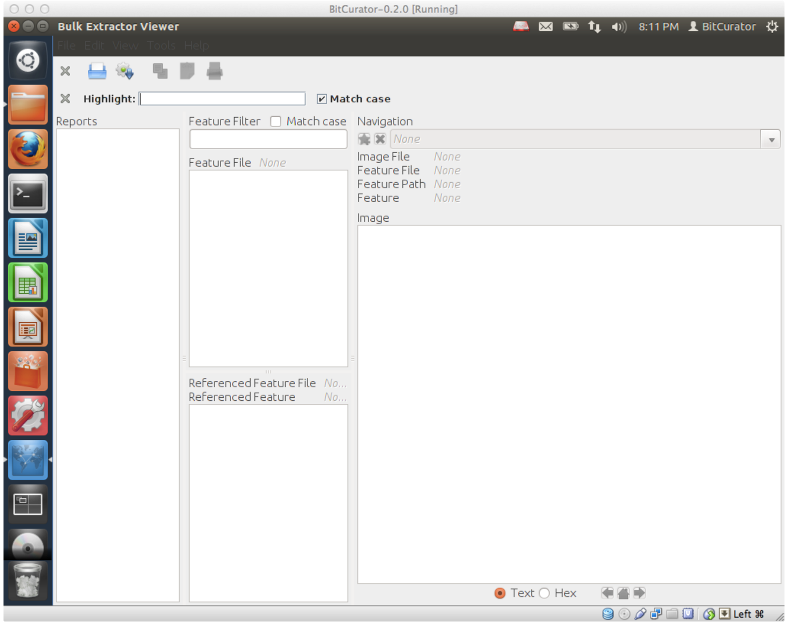

BitCurator-0.2.0 [Running]
Mozilla Firefox
8:08 PM
BitCurator
file:///home/b…mpleimage.xml
file:///home/bcadmin/Desktop/SampleData/sampleimage.xml
Google
Left ⌘

This XML file does not appear to have any style information associated with it. The document tree is shown below.

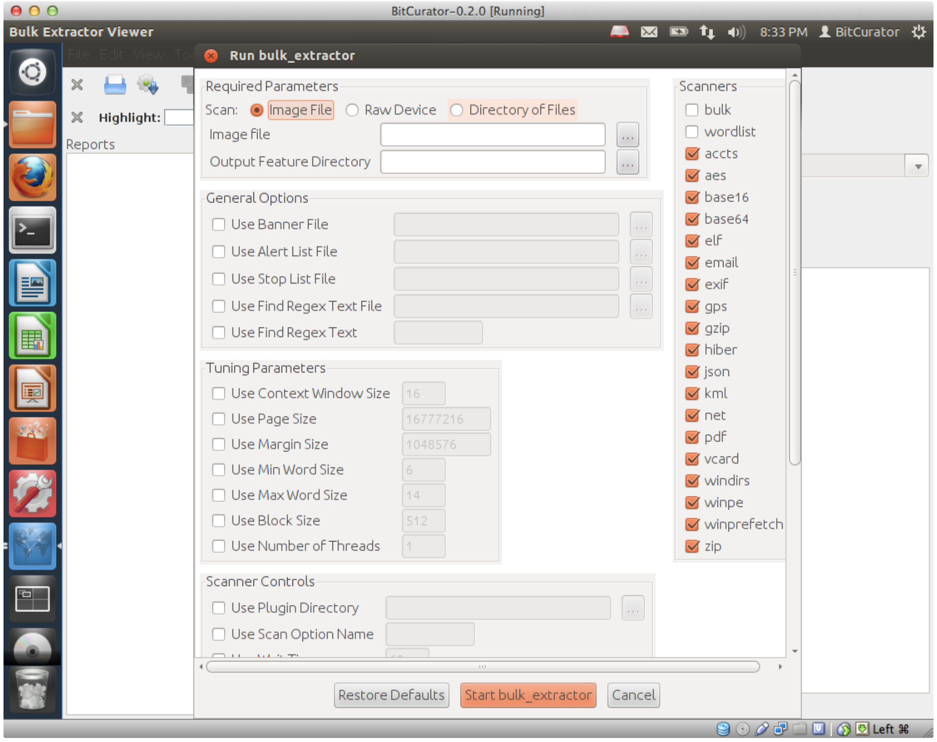
```
−<dfxml version="1.0">
  −<metadata>
      <dc:type>Disk Image</dc:type>
    </metadata>
  −<creator version="1.0">
      <program>fiwalk</program>
      <version>4.0.2</version>
    −<build_environment>
        <compiler>GCC 4.6</compiler>
        <library name="afflib" version="3.7.1"/>
        <library name="libewf" version="20130303"/>
      </build_environment>
    −<execution_environment>
      −<command_line>
          fiwalk -f -X /home/bcadmin/Desktop/SampleData/sampleimage.xml /home/bcadmin/Desktop/SampleData
          /sampleimage.E01
        </command_line>
        <start_time>2013-03-12T00:08:28Z</start_time>
      </execution_environment>
    </creator>
  −<source>
      <image_filename>/home/bcadmin/Desktop/SampleData/sampleimage.E01</image_filename>
    </source>
    <!-- fs start: 0 -->
  −<volume offset="0">
      <partition_offset>0</partition_offset>
      <block_size>2048</block_size>
      <ftype>2048</ftype>
      <ftype_str>iso9660</ftype_str>
      <block_count>36839</block_count>
```

Generating "Feature" (potentially sensitive or personally revealing information) reports with Bulk Extractor

- From the desktop, double-click on "Forensics Tools", and then double-click on the "Bulk Extractor Viewer" icon. This will launch the GUI front-end to Bulk Extractor, a tool to identify various "features" contained within the bitstream extracted from the source media.



- Click on the “Tools” menu in the top of the window, and select “Run Bulk Extractor”. This will bring up a dialog that allows you to select which scanners to run, and where to generate the report directory.



Run bulk_extractor

Required Parameters
Scan: ● Image File ○ Raw Device ○ Directory of Files
Image file [ ] …
Output Feature Directory [ ] …

General Options
□ Use Banner File
□ Use Alert List File
□ Use Stop List File
□ Use Find Regex Text File
□ Use Find Regex Text

Tuning Parameters
□ Use Context Window Size 16
□ Use Page Size 16777216
□ Use Margin Size 1048576
□ Use Min Word Size 6
□ Use Max Word Size 14
□ Use Block Size 512
□ Use Number of Threads 1

Scanner Controls
□ Use Plugin Directory
□ Use Scan Option Name

Scanners
□ bulk
□ wordlist
☑ accts
☑ aes
☑ base16
☑ base64
☑ elf
☑ email
☑ exif
☑ gps
☑ gzip
☑ hiber
☑ json
☑ kml
☑ net
☑ pdf
☑ vcard
☑ windirs
☑ winpe
☑ winprefetch
☑ zip

- Using the “…” icons to the right of the “Image File” and “Output Feature Directory” text boxes, you can select the image file you’ve produced and tell Bulk Extractor to output the report in a new directory “beoutput”, within the SampleData directory you made previously on the desktop.
- You can click on “Start Bulk Extractor” at the bottom of the dialog and then see a new dialog appear, indicating the progress made so far. For large disk images, it may take a while for the process to complete.

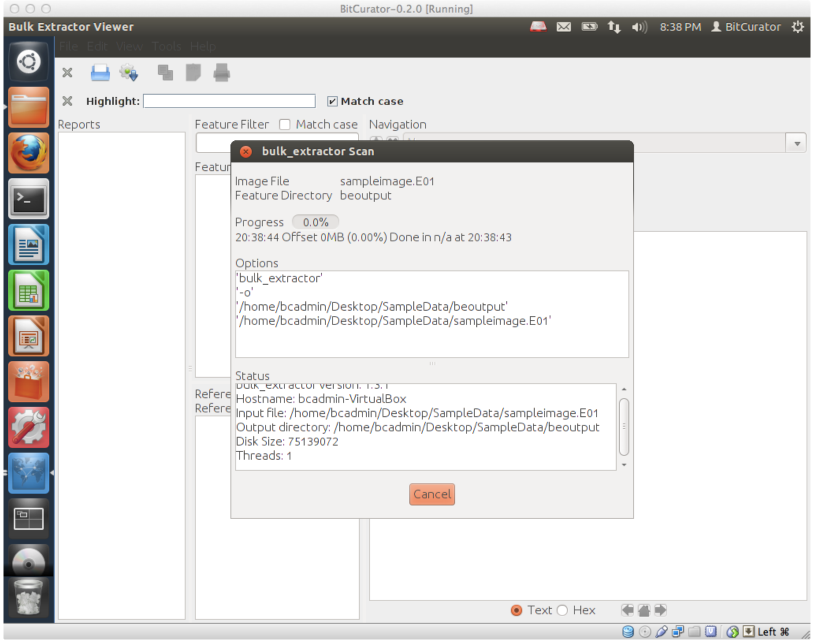


Image File sampleimage.E01
Feature Directory beoutput

Progress 0.0%
20:38:44 Offset 0MB (0.00%) Done in n/a at 20:38:43

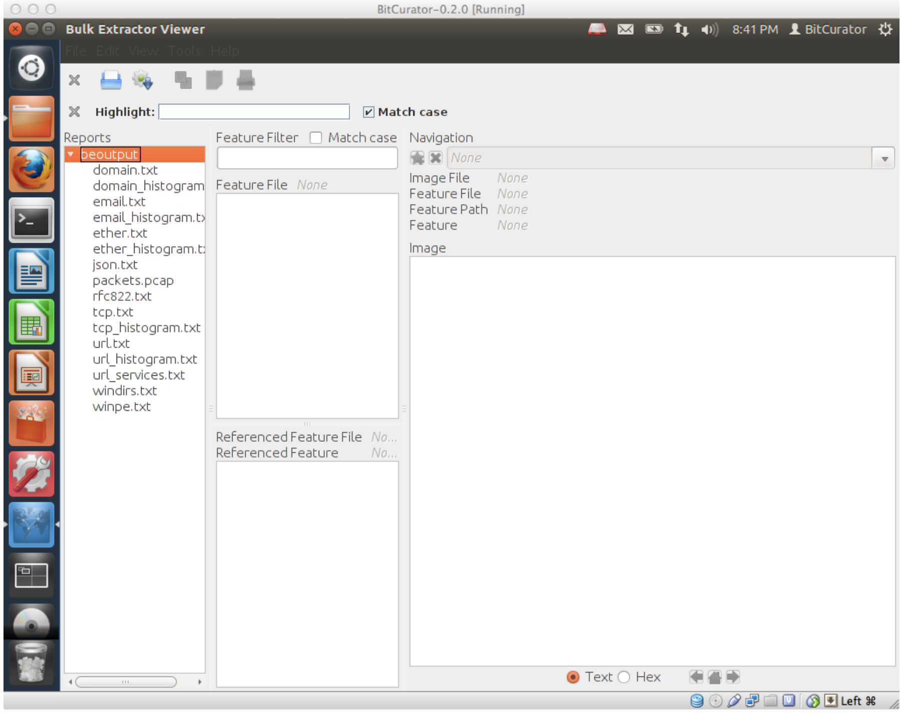
Options

```
'bulk_extractor'
'-o'
'/home/bcadmin/Desktop/SampleData/beoutput'
'/home/bcadmin/Desktop/SampleData/sampleimage.E01'
```

Status

```
bulk_extractor version: 1.3.1
Hostname: bcadmin-VirtualBox
Input file: /home/bcadmin/Desktop/SampleData/sampleimage.E01
Output directory: /home/bcadmin/Desktop/SampleData/beoutput
Disk Size: 75139072
Threads: 1
```

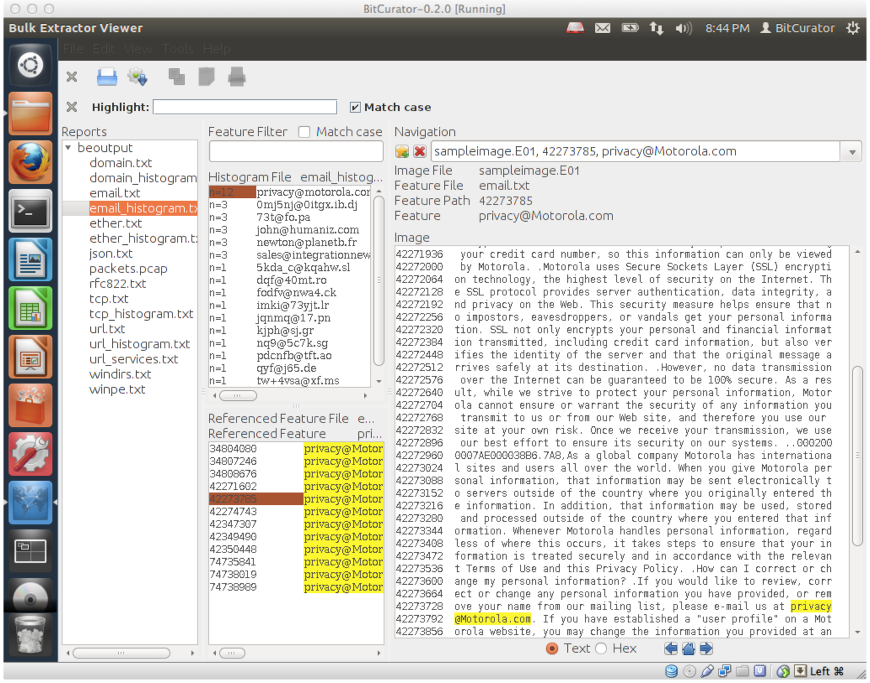
- Once the process has completed, the report directory will be available in the relevant location (in our case, the directory “beoutput” within SampleData). The features identified can also be viewed in the main Bulk Extractor Viewer window, by clicking on the report name in the “Reports” subwindow.



```
beoutput
  domain.txt
  domain_histogram
  email.txt
  email_histogram.t
  ether.txt
  ether_histogram.t
  json.txt
  packets.pcap
  rfc822.txt
  tcp.txt
  tcp_histogram.txt
  url.txt
  url_histogram.txt
  url_services.txt
  windirs.txt
  winpe.txt
```

```
None
Image File    None
Feature File  None
Feature Path  None
Feature       None
```

- Individual features may be examined, for example by selecting the histogram file associated with a particular feature type (in the example above, emails), clicking on a particular instance of a feature in the “Referenced Feature” window, and examining that feature in the Image map on the right.



```
beoutput
  domain.txt
  domain_histogram
  email.txt
  email_histogram.t
  ether.txt
  ether_histogram.t
  json.txt
  packets.pcap
  rfc822.txt
  tcp.txt
  tcp_histogram.txt
  url.txt
  url_histogram.txt
  url_services.txt
  windirs.txt
  winpe.txt
```

```
Histogram File  email_histog...
n=12   privacy@motorola.cor
n=3    0mj5nj@0itgx.ib.dj
n=3    73t@fo.pa
n=3    john@humaniz.com
n=3    newton@planetb.fr
n=3    sales@integrationnew
n=1    5kda_c@kqahw.sl
n=1    dqf@40mt.ro
n=1    fodfv@nwa4.ck
n=1    imki@73yjt.lr
n=1    jqnmq@17.pn
n=1    kjph@sj.gr
n=1    nq9@5c7k.sg
n=1    pdcnfb@tft.ao
n=1    qyf@j65.de
n=1    tw+4vsa@xf.ms
```

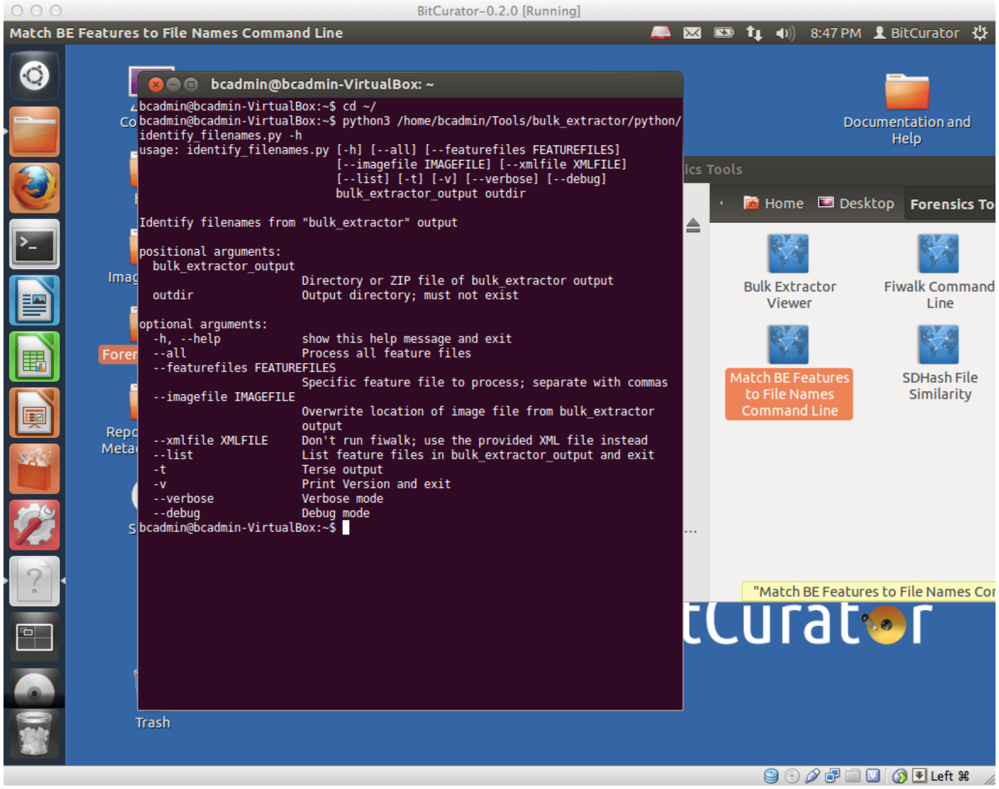
```
Referenced Feature File  e...
Referenced Feature       pri...
34804080      privacy@Motor
34807246      privacy@Motor
34808676      privacy@Motor
42271602      privacy@Motor
42273785      privacy@Motor
42274743      privacy@Motor
42347307      privacy@Motor
42349490      privacy@Motor
42350448      privacy@Motor
74735841      privacy@Motor
74738019      privacy@Motor
74738989      privacy@Motor
```

```
sampleimage.E01, 42273785, privacy@Motorola.com
Image File    sampleimage.E01
Feature File  email.txt
Feature Path  42273785
Feature       privacy@Motorola.com
```

```
42271936   your credit card number, so this information can only be viewed
42272000   by Motorola. .Motorola uses Secure Sockets Layer (SSL) encrypti
42272064  on technology, the highest level of security on the Internet. Th
42272128  e SSL protocol provides server authentication, data integrity, a
42272192  nd privacy on the Web. This security measure helps ensure that n
42272256  o impostors, eavesdroppers, or vandals get your personal informa
42272320  tion. SSL not only encrypts your personal and financial informat
42272384  ion transmitted, including credit card information, but also ver
42272448  ifies the identity of the server and that the original message a
42272512  rrives safely at its destination. .However, no data transmission
42272576   over the Internet can be guaranteed to be 100% secure. As a res
42272640  ult, while we strive to protect your personal information, Motor
42272704  ola cannot ensure or warrant the security of any information you
42272768   transmit to us or from our Web site, and therefore you use our 
42272832  site at your own risk. Once we receive your transmission, we use
42272896   our best effort to ensure its security on our systems. ..000200
42272960  0007AE000038B6.7A8,As a global company Motorola has internationa
42273024  l sites and users all over the world. When you give Motorola per
42273088  sonal information, that information may be sent electronically t
42273152  o servers outside of the country where you originally entered th
42273216  e information. In addition, that information may be used, stored
42273280   and processed outside of the country where you entered that inf
42273344  ormation. Whenever Motorola handles personal information, regard
42273408  less of where this occurs, it takes steps to ensure that your in
42273472  formation is treated securely and in accordance with the relevan
42273536  t Terms of Use and this Privacy Policy. .How can I correct or ch
42273600  ange my personal information? .If you would like to review, corr
42273664  ect or change any personal information you have provided, or rem
42273728  ove your name from our mailing list, please e-mail us at privacy
42273792  @Motorola.com. If you have established a "user profile" on a Mot
42273856  orola website, you may change the information you provided at an
```

Bulk Extractor extracts these features from a disk image by scanning the raw bitstream – not by parsing the filesystem. In order to determine the folders or files where the features appear (or if they appear on an area of the disk not associated with the filesystem), you need to run an additional tool called “Identify File Names.” You can do this by:

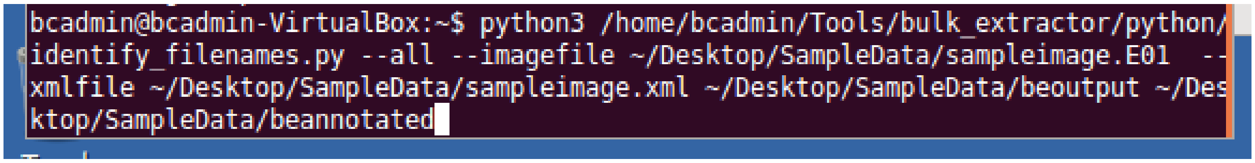
- Returning to the desktop, double-click on “Forensics Tools”, and double clicking on “Match BE Features to File Names Command Line”. You would then see a new terminal pop up.


BitCurator–0.2.0 [Running]
Match BE Features to File Names Command Line
8:47 PM
BitCurator
bcadmin@bcadmin-VirtualBox: ~
Documentation and Help
ics Tools
Home
Desktop
Forensics To
Bulk Extractor Viewer
Fiwalk Command Line
Match BE Features to File Names Command Line
SDHash File Similarity
"Match BE Features to File Names Cor
Trash
Left ⌘

```
bcadmin@bcadmin-VirtualBox:~$ cd ~/
bcadmin@bcadmin-VirtualBox:~$ python3 /home/bcadmin/Tools/bulk_extractor/python/
identify_filenames.py -h
usage: identify_filenames.py [-h] [--all] [--featurefiles FEATUREFILES]
                             [--imagefile IMAGEFILE] [--xmlfile XMLFILE]
                             [--list] [-t] [-v] [--verbose] [--debug]
                             bulk_extractor_output outdir

Identify filenames from "bulk_extractor" output

positional arguments:
  bulk_extractor_output
                        Directory or ZIP file of bulk_extractor output
  outdir                Output directory; must not exist

optional arguments:
  -h, --help            show this help message and exit
  --all                 Process all feature files
  --featurefiles FEATUREFILES
                        Specific feature file to process; separate with commas
  --imagefile IMAGEFILE
                        Overwrite location of image file from bulk_extractor
                        output
  --xmlfile XMLFILE     Don't run fiwalk; use the provided XML file instead
  --list                List feature files in bulk_extractor_output and exit
  -t                    Terse output
  -v                    Print Version and exit
  --verbose             Verbose mode
  --debug               Debug mode
bcadmin@bcadmin-VirtualBox:~$ 
```

Identify Filenames needs to know five things:

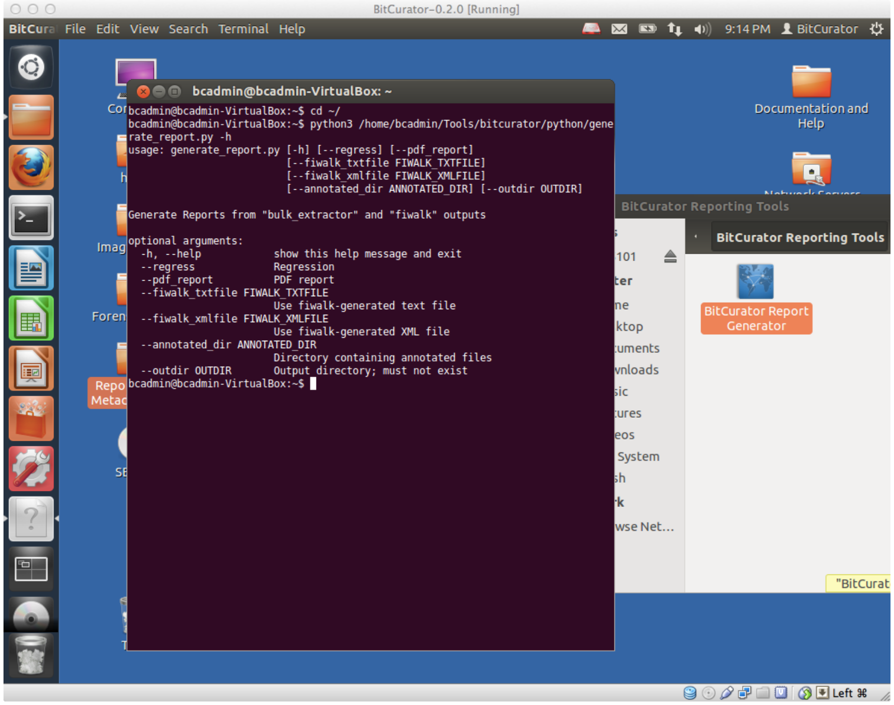
1. Which feature reports to work from (here we’ve used the “all” flag to tell it to use all of them)
2. Where the image file is (“—image file [FILE LOCATION]”)
3. Where the fiwalk output is (“—xmlfile [FILE LOCATION]”)
4. Where the bulk extractor output is (just the location)
5. Where we want to generated the output. In this case, we’re telling it to make a new directory called “beannotated” in our SampleData directory on the desktop.



```
bcadmin@bcadmin-VirtualBox:~$ python3 /home/bcadmin/Tools/bulk_extractor/python/
identify_filenames.py --all --imagefile ~/Desktop/SampleData/sampleimage.E01  --
xmlfile ~/Desktop/SampleData/sampleimage.xml ~/Desktop/SampleData/beoutput ~/Des
ktop/SampleData/beannotated
```

Generating Human-Readable Reports

- Double-click on “Reporting and Metadata Tools” on the desktop, open “BitCurator Reporting Tools”, and double-click on the “BitCurator Report Generator” launcher

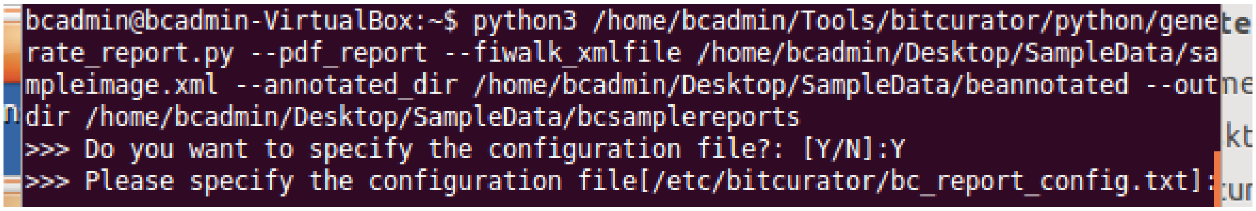

BitCurator-0.2.0 [Running]
BitCura File Edit View Search Terminal Help
9:14 PM BitCurator
bcadmin@bcadmin-VirtualBox: ~
Documentation and Help
BitCurator Reporting Tools
BitCurator Reporting Tools
BitCurator Report Generator
Left ⌘

```
bcadmin@bcadmin-VirtualBox:~$ cd ~/
bcadmin@bcadmin-VirtualBox:~$ python3 /home/bcadmin/Tools/bitcurator/python/gene
rate_report.py -h
usage: generate_report.py [-h] [--regress] [--pdf_report]
                          [--fiwalk_txtfile FIWALK_TXTFILE]
                          [--fiwalk_xmlfile FIWALK_XMLFILE]
                          [--annotated_dir ANNOTATED_DIR] [--outdir OUTDIR]

Generate Reports from "bulk_extractor" and "fiwalk" outputs

optional arguments:
  -h, --help            show this help message and exit
  --regress             Regression
  --pdf_report          PDF report
  --fiwalk_txtfile FIWALK_TXTFILE
                        Use fiwalk-generated text file
  --fiwalk_xmlfile FIWALK_XMLFILE
                        Use fiwalk-generated XML file
  --annotated_dir ANNOTATED_DIR
                        Directory containing annotated files
  --outdir OUTDIR       Output directory; must not exist
bcadmin@bcadmin-VirtualBox:~$ 
```

The “Generate Report” program needs to know about four things:

1. Whether to generate the reports as PDFs (currently the only option), specified by –pdf-report
2. Where the fiwalk output is (“—fiwalk_xmlfile [FILE LOCATION]”)
3. Where the annotated bulk extractor report directory (the one we   generated in the last step) is (“—annotated_dir [DIRECTORY LOCATION]”)
4. Where we want to generated the output. In this case, we’re telling it to make a new directory called “bcsamplereports” in the SampleData directory on the desktop.

There are also a couple prompts for configuration. You can use the defaults by typing “Y” and enter for the first prompt, and simply hitting enter for the second.



```
bcadmin@bcadmin-VirtualBox:~$ python3 /home/bcadmin/Tools/bitcurator/python/gene
rate_report.py --pdf_report --fiwalk_xmlfile /home/bcadmin/Desktop/SampleData/sa
mpleimage.xml --annotated_dir /home/bcadmin/Desktop/SampleData/beannotated --out
dir /home/bcadmin/Desktop/SampleData/bcsamplereports
>>> Do you want to specify the configuration file?: [Y/N]:Y
>>> Please specify the configuration file[/etc/bitcurator/bc_report_config.txt]:
```