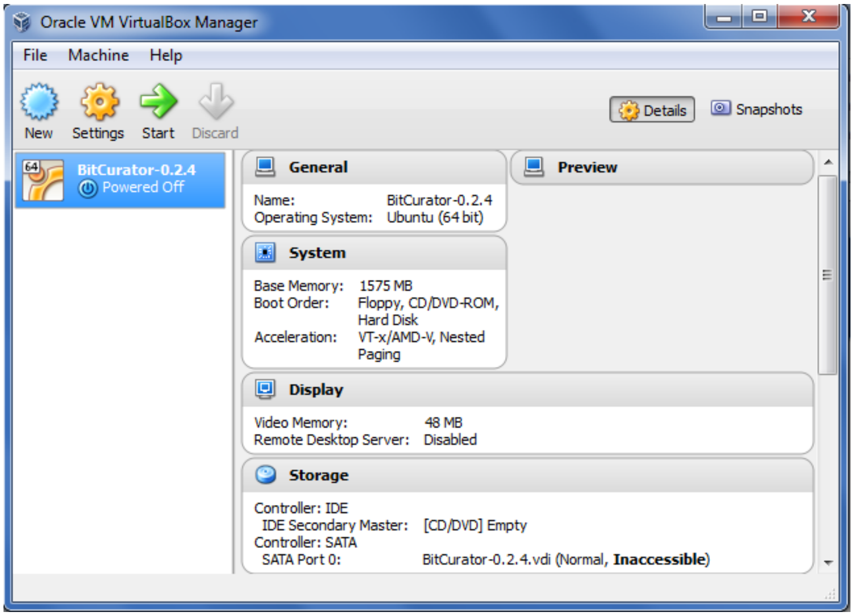
Lab Exercise – Using BitCurator
Lead Instructors: Cal Lee and Kam Woods

Start the BitCurator Virtual Machine

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.



General

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

System

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

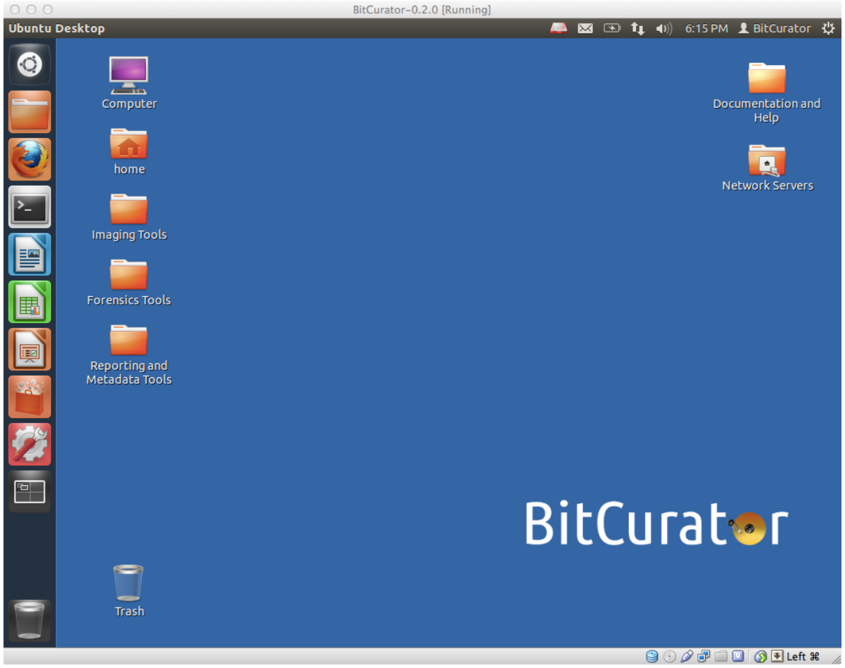
Display

Video Memory: 48 MB
Remote Desktop Server: Disabled

Storage

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

Once the VM has fully booted up, you should see something like this:

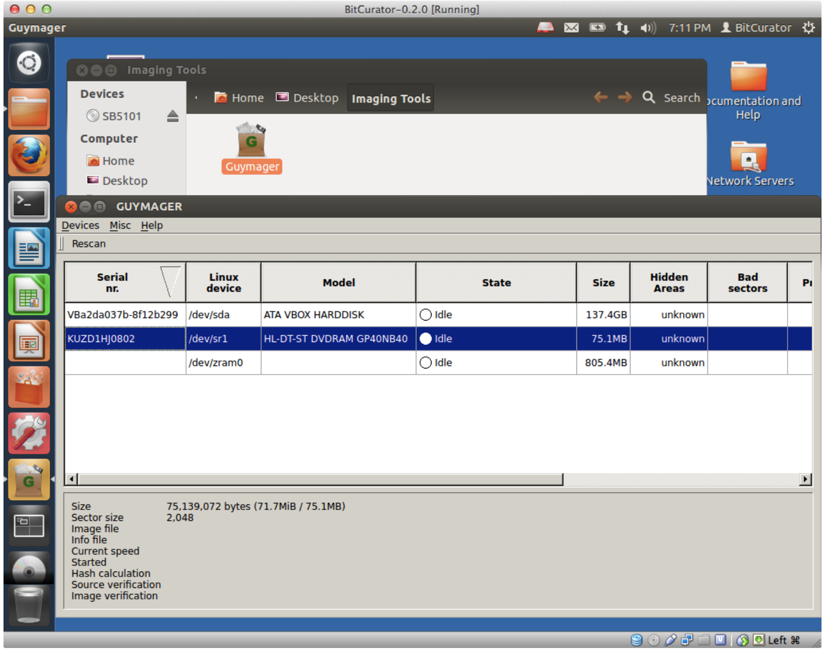


If you see any messages at the top, you can just ignore them.

Imaging a disk

We'll just be looking at the functionality of Guymager. We will **not** be creating any disk images in this lab exercise today.

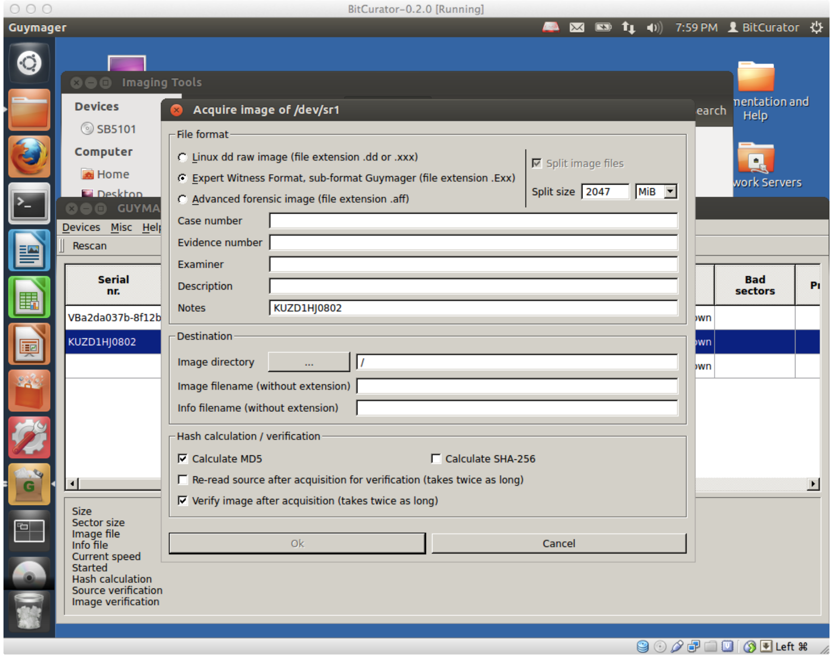
Double-click on "Imaging Tools" on the Desktop, and then double-click on Guymager. Note in the figure below that Guymager is showing three drives and one has been selected.



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 one of the available drives (you may only see one), and click on "Acquire image" in the menu. You'll see a new dialog window that will prompt you to enter some acquisition metadata.



Acquire image of /dev/sr1

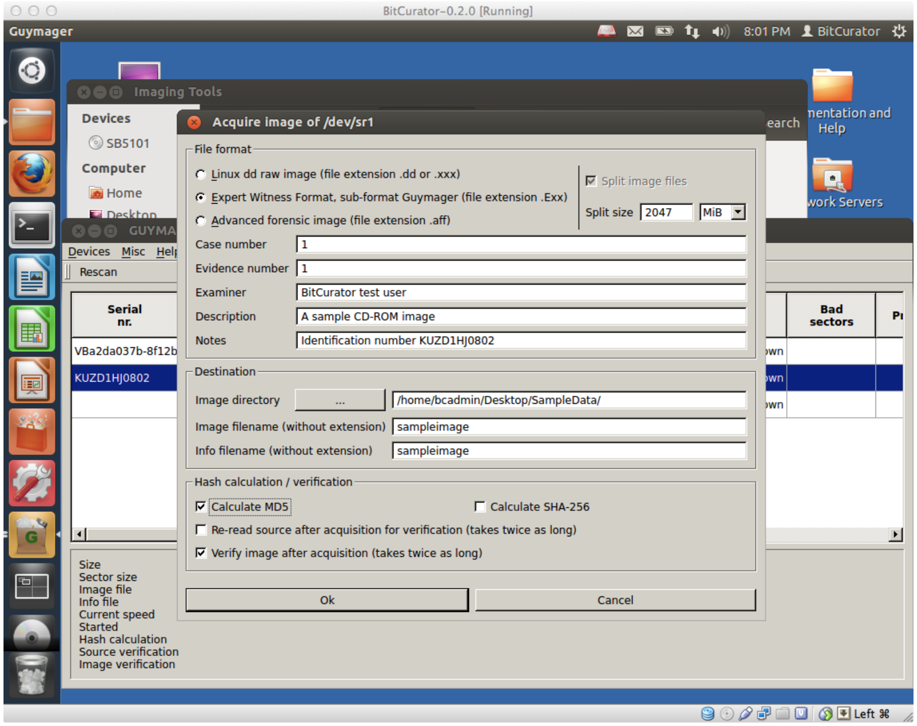
File format
○ Linux dd raw image (file extension .dd or .xxx)
● Expert Witness Format, sub-format Guymager (file extension .Exx)
○ Advanced forensic image (file extension .aff)
☑ Split image files
Split size 2047 MiB

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)

Select an image format (leave it on Expert Witness Format, which is the default) and enter some other metadata. For the "Image directory," select the place for the resulting disk image to be stored (in this case, the "SampleData" directory that you created earlier on the desktop), name the image, and then click "OK."



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

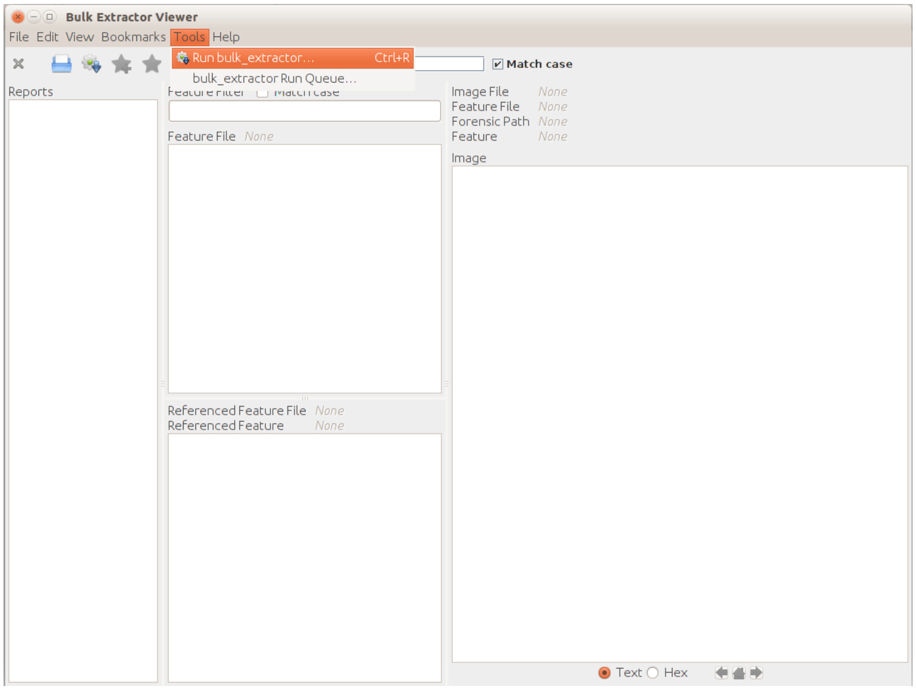
You'll see the main dialog state change to "Acquisition Running". Note that the BitCurator environment runs at a resolution of 1024x768 by default. If you wish to see the whole dialog, just make the window bigger. The resolution should resize automatically.

Cancel the acquisition. As noted above, 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.

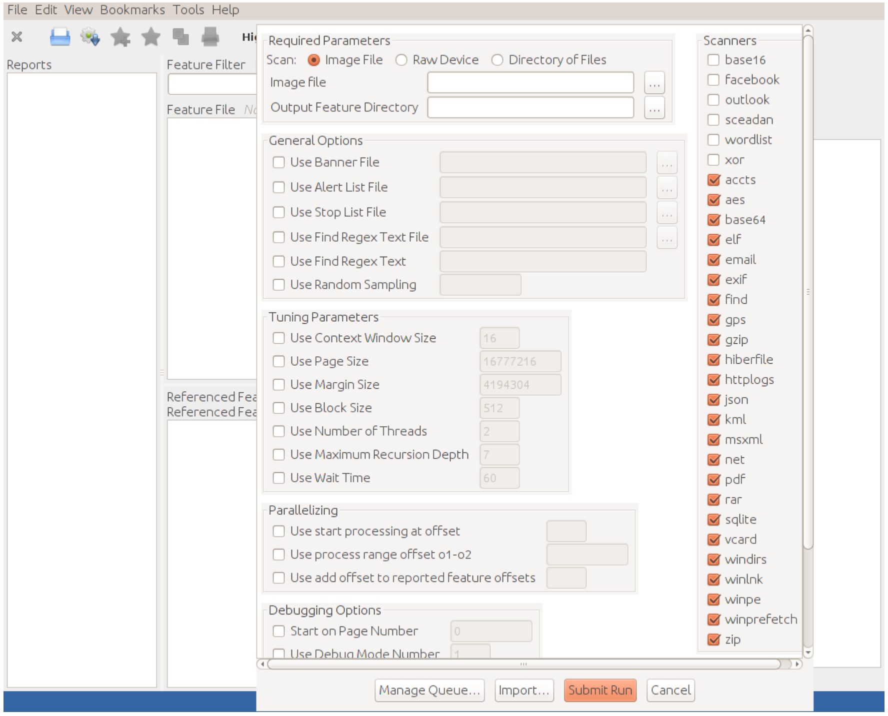
Generating "Feature" (potentially sensitive or personally revealing information) reports with Bulk Extractor

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.



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
□ Use Random Sampling

Tuning Parameters

□ Use Context Window Size 16
□ Use Page Size 16777216
□ Use Margin Size 4194304
□ Use Block Size 512
□ Use Number of Threads 2
□ Use Maximum Recursion Depth 7
□ Use Wait Time 60

Parallelizing

□ Use start processing at offset
□ Use process range offset o1-o2
□ Use add offset to reported feature offsets

Debugging Options

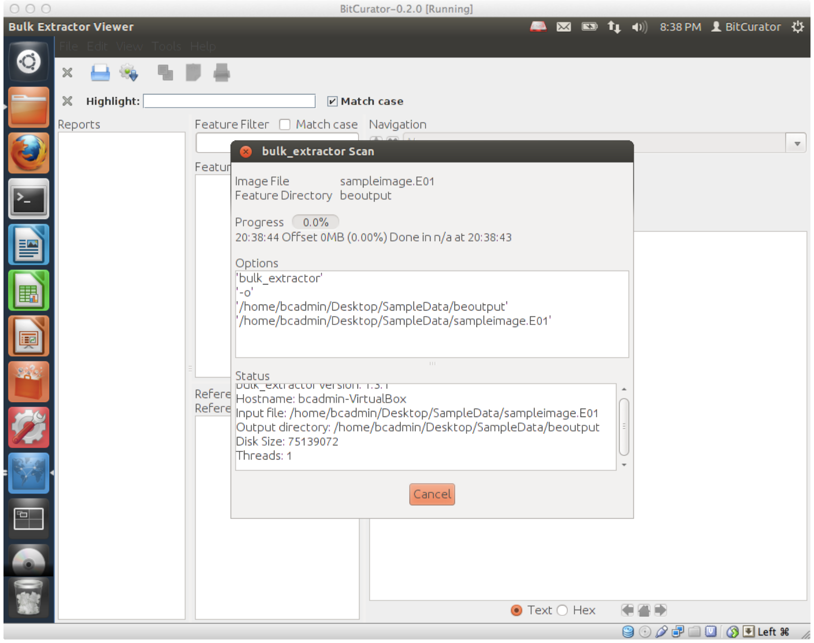
□ Start on Page Number 0
□ Use Debug Mode Number 1

Scanners

□ base16
□ facebook
□ outlook
□ sceadan
□ wordlist
□ xor
☑ accts
☑ aes
☑ base64
☑ elf
☑ email
☑ exif
☑ find
☑ gps
☑ gzip
☑ hiberfile
☑ httplogs
☑ json
☑ kml
☑ msxml
☑ net
☑ pdf
☑ rar
☑ sqlite
☑ vcard
☑ windirs
☑ winlnk
☑ 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.

Click on "Submit Run" at the bottom of the dialog and then see a new dialog appear, indicating the progress made so far.



bulk_extractor Scan

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

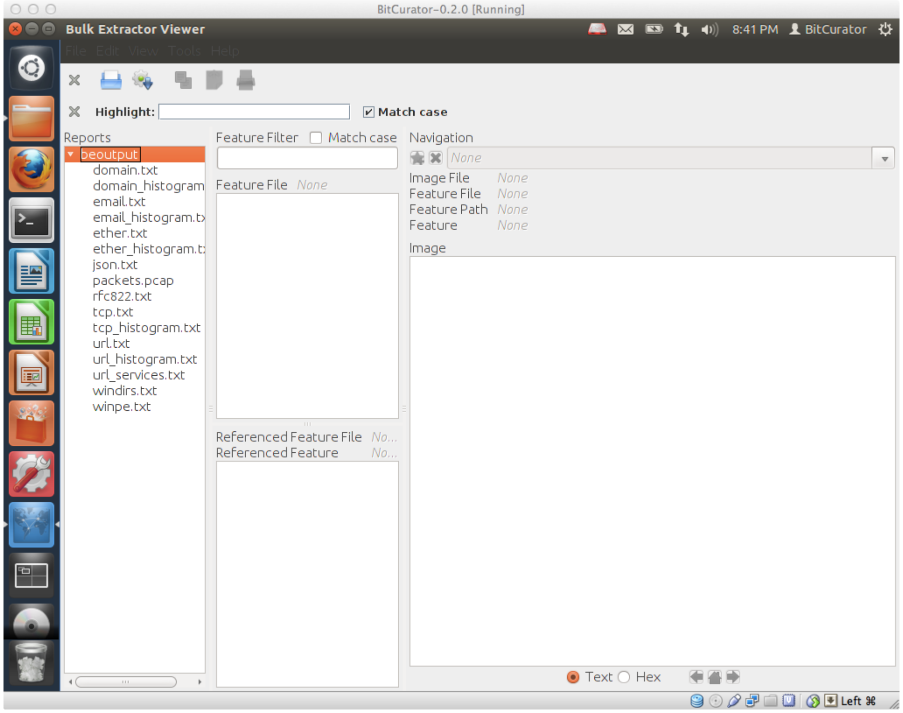
```
'bulk_extractor'
'-o'
'/home/bcadmin/Desktop/SampleData/beoutput'
'/home/bcadmin/Desktop/SampleData/sampleimage.E01'
```

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
```

Cancel

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.



Reports

- 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

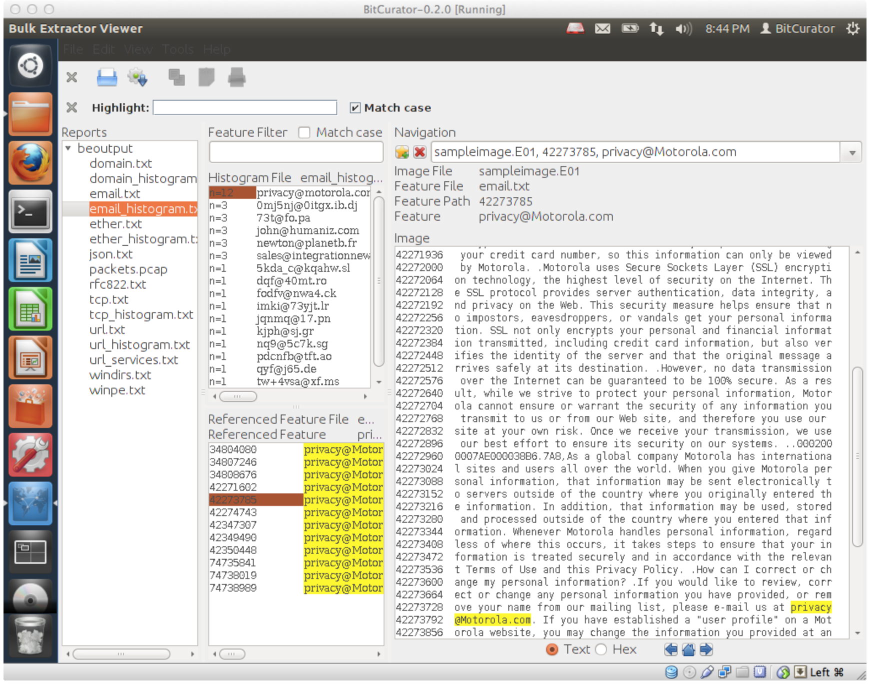
Feature File None

Referenced Feature File No...
Referenced Feature No...

Navigation 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.



Highlight: ☑ Match case

Reports

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

Feature Filter □ Match case

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
```

Navigation

sampleimage.E01, 42273785, privacy@Motorola.com

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

Image

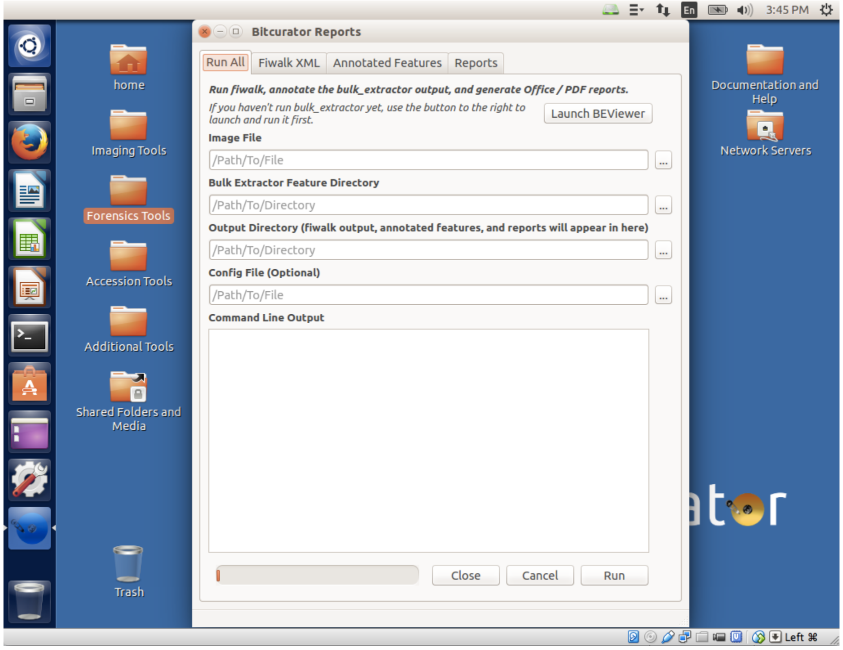
```
42271936   your credit card number, so this information can only be viewed
42272000   by Motorola. .Motorola uses Secure Sockets Layer (SSL) encrypti
42272064  on technology, the highest level of security on the Internet. Th
42272128  e SSL protocol provides server authentication, data integrity, 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
```

● Text ○ Hex

BitCurator Reporting Tool

Bulk Extractor extracts these features from a disk image by scanning the raw bitstream – not by parsing the filesystem. In order to output filesystem information, you need to run a tool called fiwalk. 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 a tool called "Identify File Names." You can also generate various other summaries of the disk's content. You can perform all of these tasks by using the "Run All" tab in the BitCurator Reporting Tool.

Double-click on the "Forensics Tools" folder, and then double click on the "BitCurator Reporting Tool" launcher. You'll see a window pop up that should match the picture shown below.



Bitcurator Reports

Run All | Fiwalk XML | Annotated Features | Reports

Run fiwalk, annotate the bulk_extractor output, and generate Office / PDF reports.

If you haven't run bulk_extractor yet, use the button to the right to launch and run it first. [Launch BEViewer]

Image File
/Path/To/File [...]

Bulk Extractor Feature Directory
/Path/To/Directory [...]

Output Directory (fiwalk output, annotated features, and reports will appear in here)
/Path/To/Directory [...]

Config File (Optional)
/Path/To/File [...]

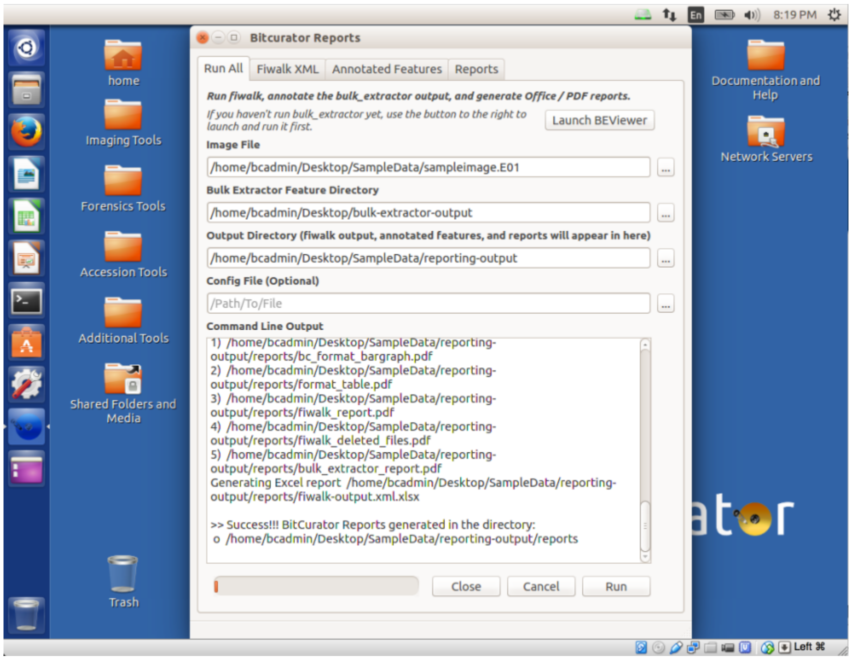
Command Line Output

[Close] [Cancel] [Run]

Click on the box with three dots next to the "Image File" entry, and navigate to the sample image (sampleimage.E01) we created in our SampleData directory on the Desktop earlier. The image file you selected should now appear under the "Image File" entry.

Follow the same process for the “Bulk Extractor Feature Directory” entry. You previously created the “bulk-extractor-output” directory within the “SampleData” directory on the desktop.

Finally, assign an output directory for the reports that will be generated. Note that you do not need to click “Create Folder” when selecting this location. Simply navigate to the desired location (in this case, Desktop/SampleData) and type in the name of the folder you wish to store the reports in. Then, click “Save.” Finally, click “Run.”



Run fiwalk, annotate the bulk_extractor output, and generate Office / PDF reports.

If you haven't run bulk_extractor yet, use the button to the right to launch and run it first.

Image File: /home/bcadmin/Desktop/SampleData/sampleimage.E01

Bulk Extractor Feature Directory: /home/bcadmin/Desktop/bulk-extractor-output

Output Directory (fiwalk output, annotated features, and reports will appear in here): /home/bcadmin/Desktop/SampleData/reporting-output

Config File (Optional): /Path/To/File

Command Line Output

```
1) /home/bcadmin/Desktop/SampleData/reporting-
output/reports/bc_format_bargraph.pdf
2) /home/bcadmin/Desktop/SampleData/reporting-
output/reports/format_table.pdf
3) /home/bcadmin/Desktop/SampleData/reporting-
output/reports/fiwalk_report.pdf
4) /home/bcadmin/Desktop/SampleData/reporting-
output/reports/fiwalk_deleted_files.pdf
5) /home/bcadmin/Desktop/SampleData/reporting-
output/reports/bulk_extractor_report.pdf
Generating Excel report  /home/bcadmin/Desktop/SampleData/reporting-
output/reports/fiwalk-output.xml.xlsx

>> Success!!! BitCurator Reports generated in the directory:
 o  /home/bcadmin/Desktop/SampleData/reporting-output/reports
```

Once the reporting tool is done, you can navigate to the SampleData folder and view the various outputs and reports.