Creating a Disk Image Using Guymager

The BitCurator environment includes Guymager, an open-source, graphical application for creating disk images. Guymager has support for raw dd images, EO1, and AFF image formats. The latter two image formats are commonly used in the digital forensics community and have the ability to incorporate metadata about the original media into the disk image itself.

Step-by-step guide

1. Create a directory in which to store your disk image by opening up Nautilus (the "Home" folder on the top left-hand side of the screen) and right clicking anywhere on the white background. Select "Create New Folder" from the drop-down menu. Name the folder as you see fit; we will use the folder name "diskimages" in this example.

2. Make sure to safely mount the device, enable read-only enforcement, and/or use a write blocker in order to prevent inadvertently writing data back to the disk. The BitCurator environment is set up to enforce read-only access by default.

   Connect the device you wish to image to your computer (USB flash drive, CD-ROM, hard drive, or floppy disk drive).

Note: A device does not need to be mounted in order to be imaged by Guymager, and BitCurator will not mount devices automatically (the icon that appears in the Unity bar on the left indicates that the device is attached, rather than mounted). If you need to examine the contents of the disk before creating the disk image, you can safely mount the device. Simply clicking on the device icon will safely mount (in read-only mode) the readable filesystem(s) on that device.

3. Open Guymager by right-clicking the icon in the "Imaging Tools" folder on the desktop. In the contextual menu, select "Open."

   Figure 1: The contextual menu for opening Guymager.
   
   Figure 2: Guymager prompts for authentication to allow the program root-level rights.

4. Guymager will ask to be run with root rights. When prompted, enter the password associated with the BitCurator user account (usually 'bcadmin').
5. When Guymager launches, it will display a list of all mounted disks on the system. Once again identify the disk you wish to image, right click on its listing, and select "Acquire image".

**Figure 3:** Click on "Acquire image" to begin the imaging process.

6. Clicking on Acquire Image will open the Acquire Image window. In this window you will first select the disk image format you would like to use. The options include Linux dd raw image, Expert Witness Format (.E01), and Advance Forensics image format (.AFF; see Figure 2). An Expert Witness or AFF image will store user-added metadata within the forensically-packaged image.

**Note:** If you choose either Linux dd or Expert Witness format, you have the option to split the image into multiple files, thus making it more easily transferable. So, for example, a 4GB image could be split into four 1GB files, or two 2GB files, etc.

**Figure 4:** Select the image format type and input metadata.
7. After selecting the image format type, fill out the metadata as needed. E01 and AFF images were designed for the digital forensics community, so the fields are labeled for criminal investigation. However, these fields can easily be repurposed for the needs of archivists and curators. For example, an archivist might use the "Case number" field to record an accession number.

8. Next choose the image directory, which in this example would be "/home/bcadmin/diskimages". Note: Guymager is running as the root user, so you want to avoid creating new directories directly through Guymager (thus step #1).

9. Finally, name your disk image and choose which verification options you would like Guymager to perform. Click "OK" to begin the imaging process.

10. Once the imaging process begins you will be taken back to the main Guymager screen in Figure 4, which will now show a progress bar.

11. After Guymager has finished creating the disk image, close Guymager and verify the image by navigating to the directory you created in Step #1. Notice that there are two files, the image itself and an info file (see Figure 3). The info file includes the metadata we input in step 7 along with additional metadata collected during the acquisition process. The imaging process is now complete.

Figure 5: Verify the disk image and metadata.
Related articles

- Creating a Disk Image Using Guymager
- Using Nautilus for Data Triage
- Configuring BitCurator to enable users to authenticate with Active Directory accounts
- Access and Export Files from Disk Images
- Find Potentially Sensitive Information with Bulk Extractor Viewer