

# BitCurator Software: Safely Mounting Drives

Discussion questions to pair with the screencast

<a href="#">Authors</a>	1
<a href="#">Description</a>	1
<a href="#">Learning object type</a>	1
<a href="#">Learning objectives</a>	1
<a href="#">Screencast</a>	2
<a href="#">Discussion Questions</a>	3
<a href="#">Answer Key</a>	4
<a href="#">Tools and Resources Mentioned in This Document</a>	5

## Authors

Cal Lee, Hannah Wang

## Description

These discussion questions can be used to encourage student engagement with the BitCurator screencast, [Safely Mounting Devices](#). The questions can also be used for discussion accompanying a live demonstration, a guided hands-on exercise, or independent exploration of the BitCurator Environment.

## Learning object type

Lesson plan/materials

## Learning objectives

This learning object might be used in a lesson to satisfy the following learning objectives:

## **BitCuratorEdu Learning Object**

- Identify the appropriate tools to: safely acquire born-digital materials from storage media and other modes of transfer; assist in the appraisal of born-digital materials; scan for sensitive information in born-digital materials; and package born-digital materials for preservation and access.

## Screencast

<https://youtu.be/WgjKyawzWOU>

### Discussion Questions

*These discussion questions can be used to encourage student engagement with the BitCurator screencast linked above. The questions can also be used for discussion accompanying a live demonstration, a guided hands-on exercise, or independent exploration of the BitCurator Environment. Video timestamps are included in parentheses, where applicable.*

1. At what point(s) in a digital curation workflow might you expect to use this functionality?
2. What does it mean to “mount” a disk or disk image?
3. How is mounting different from just attaching the device?
4. The video shows mounting an Expert Witness Format (.e01) disk image within the BitCurator environment. Can you mount .e01 files in Windows or MacOS? If not, why not?
5. What software could you use to mount an .e01 file in Windows or MacOS?
6. In what cases would you want to set the USB mount policy to read-only, and in what cases would you want to set the USB mount policy to writeable?

### Answer Key

*These discussion questions can be used to encourage student engagement with the BitCurator screencast linked above. The questions can also be used for discussion accompanying a live demonstration, a guided hands-on exercise, or independent exploration of the BitCurator Environment. The questions **(in bold text)** ask students to analyze the social and technological context of the BitCurator Environment and the tools packaged in the distribution. Example answers are given (in regular text), though some questions are subjective and answers may vary, depending on the knowledge of the student and the scope of the class. Video timestamps are included in parentheses, where applicable.*

#### **At what point(s) in a digital curation workflow might you expect to use this functionality?**

Students would provide a variety of answers to this question. They should identify points in a workflow when one would want to see and possibly copy the contents of a device at the file level but not access any of the underlying data including hidden files and contents of unallocated storage sectors. Note also that mounting a disk image makes the files actionable as files within the operating system, so malicious content (including viruses) can potentially infect the machine. So it's important to consider what point in a workflow is best for exposing the files in this way.

#### **What does it mean to “mount” a disk or disk image?**

When you mount a disk/image, the operating system enables access to the files and directories through the file system on the disk/image. In a Windows environment, you can see that a device has been successfully mounted when a drive letter for that device appears in Explorer (e.g. an attached flash drive might appear as the F: drive). If your OS doesn't support the filesystem on the disk/image, it will not be able to mount it (e.g. Windows won't be able to mount a drive that contains an old Macintosh HFS filesystem).

#### **How is mounting different from just attaching the device?**

If you successfully attach a disk, this means that your computer can access all of the storage sectors on that disk because it has the required hardware and software

## BitCuratorEdu Learning Object

(including device drivers) to do so. You can confirm that a disk is successfully attached by seeing that it appears within the OS disk utility. You should be able to see the attached device using disk imaging software, such as FTK Imager; and you should be able to create an image of the disk, as long as all of the sectors are readable. However, you won't be able to explore the files and directories on the disk unless you also mount it.

### **The video shows mounting an Expert Witness Format (.e01) disk image within the BitCurator environment. Can you mount .e01 files in Windows or MacOS? If not, why not?**

In both Windows (since Windows 8) and MacOS, you mount an ISO disk image by just double-clicking on it. By contrast, EWF is a forensically packaged disk image form that isn't directly supported by either OS.

### **What software could you use to mount an .e01 file in Windows or MacOS?**

You need a third party tool to do this. There are more options for doing so on Windows than on MacOS. For Windows, two popular, free options are OSFMount or FTK Imager.

### **In what cases would you want to set the USB mount policy to read-only, and in what cases would you want to set the USB mount policy to writeable?**

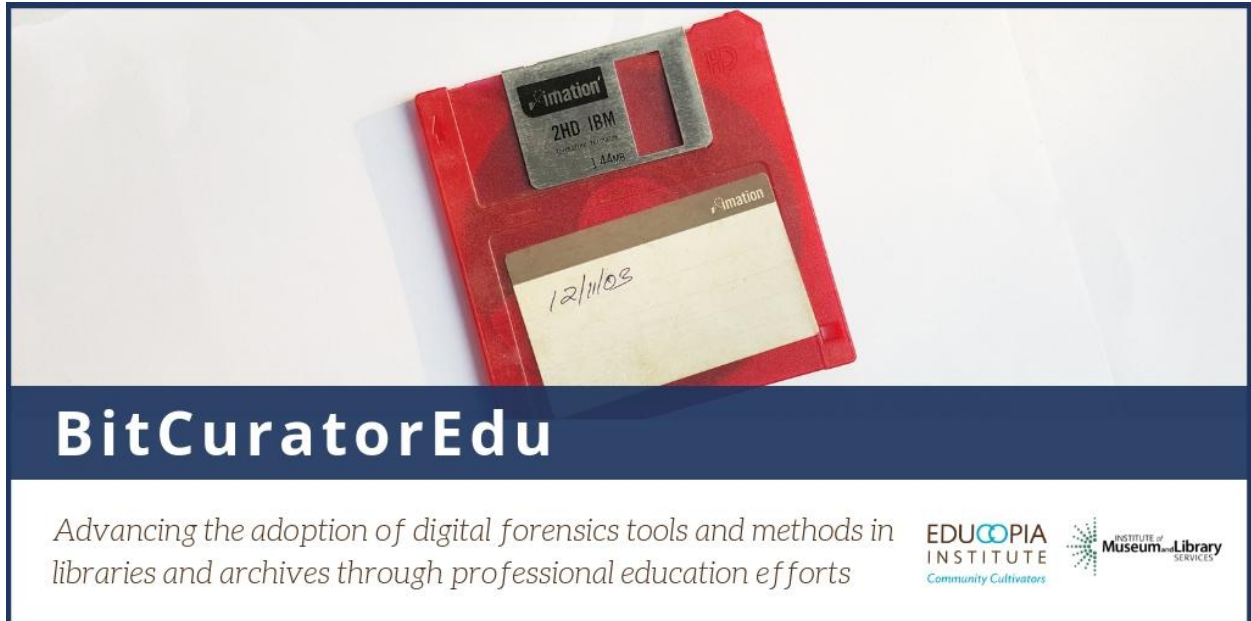
You would want to set it to read-only if the device you're accessing contains primary source materials. You would want to set it to writeable if you're instead using the device as a carrier for moving data from one place to another.

## Tools and Resources Mentioned in This Document

FTK Imager: <https://accessdata.com/product-download/ftk-imager-version-4-5>

OSFMount: <https://www.osforensics.com/tools/mount-disk-images.html>

## BitCuratorEdu Learning Object



This resource was released by the BitCuratorEdu project and is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

*The [BitCuratorEdu project](#) is a three-year effort (2018-2021) funded by the [Institute of Museum and Library Services \(IMLS\)](#) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between [Educofia Institute](#) and the [School of Information and Library Science at the University of North Carolina at Chapel Hill](#), along with the [Council of State Archivists \(CoSA\)](#) and several Masters-level programs in library and information science.*