Securely Wipe A Drive

By
Christopher A. Leonti
Information Technology Support Specialist
College of Ag / Montana Ag Experiment Station
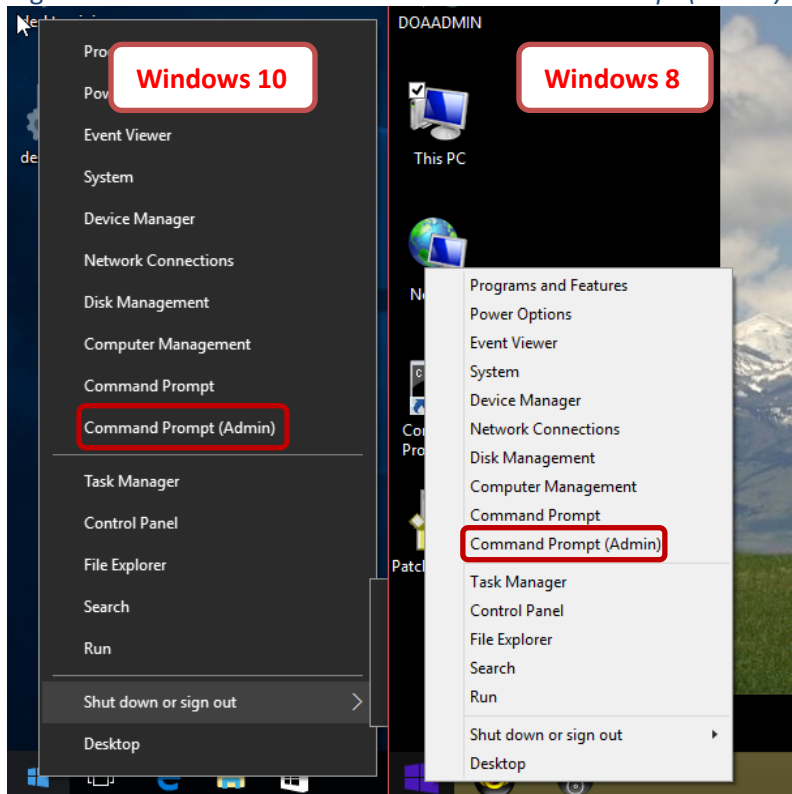Montana State University-Bozeman
http://agriculture.montana.edu/it/

It is common to have drives we need to dispose of and they range from old computer drives, external hard drives, memory cards from tablets/phones or USB thumb drives. You may feel these drives contain nothing important but they often retain sensitive information. It could be student records, research data, personal pictures, web surfing activity, passwords or credit card numbers. This data may be recoverable with the right tools *even if it has been erased*.

Drives need to be securely wiped to ensure data is rendered inaccessible before disposal or giving them to someone else. While an erased or traditionally formatted disk appears empty, data may still be recoverable. This is why tools such as KillDisk, DBAN and File Shredder are often recommended. What many do not realize is that modern versions of Windows include a format option that allows you to securely wipe a drive.
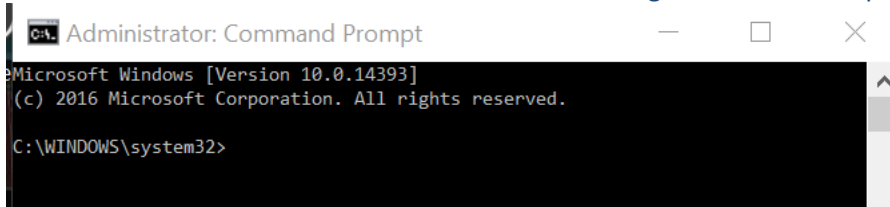
Starting with Windows Vista, Microsoft added the /P feature to the FORMAT command which overwrites every sector of a drive with 0s when formatting. This was enhanced in Windows 8 where the /P parameter overwrites all sectors with random numbers and added the option to overwrite the drive multiple times. Overwriting every sector on a drive multiple times with random information dramatically decreases the chance that any data can be recovered.

Important Note: *Using the information below securely wipes a drive but may not meet the U.S. Department of Defense standard for data removal. If this is a requirement, please use one of the tools noted earlier in this document.*

1. Connect the drive to be securely formatted to a Windows 8 or higher computer.
2. Determine the letter for the drive to be wiped using *This PC* or *Windows Explorer*.
3. Right-Click the START button and click *Command Prompt (Admin)* from the new menu.

4. A black window with white text similar to the following should now be open.
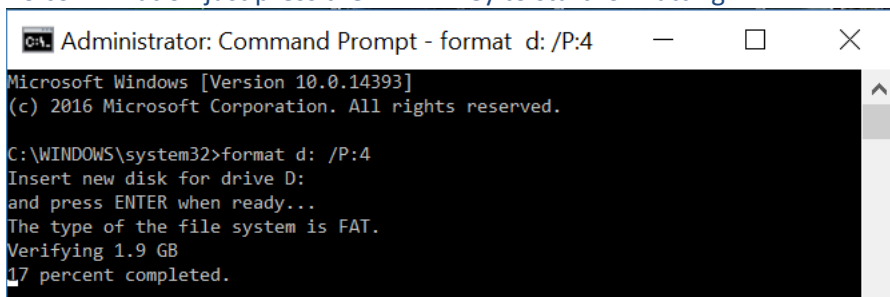

In the window, type the following command followed by the ENTER key (replace <<DRIVELETTER>> with the letter of the drive to securely format):

`Format <<DRIVELETTER>>: /P:4`

WARNING

This next step securely formats a storage device. Ensure the drive letter is correct and that data needed from the drive has been backed up. Once you proceed, there is no chance of recovering information from the drive.

5. If you see a confirmation prompt press Y followed by the ENTER key when ready to start formatting. If there is no confirmation just press the ENTER key to start formatting.
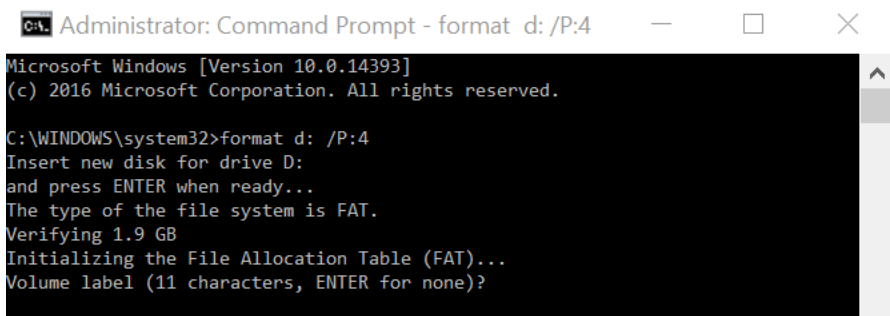

Securely formatting drives can take a long time. The exact length of time varies depending on the size of the drive, speed of the computer and specifications of the drive being formatted. It is common that securely formatting a large hard drive takes more than a full day while a smaller thumb drive may complete in less than an hour. You can leave the format running while you do other work. You can also leave the process running overnight or over a weekend.

6. Once the format has completed, you are asked for a volume label – type one in or press ENTER to leave it blank.

7. Type EXIT and press the ENTER key on the keyboard to close the command prompt window.

You can now dispose of your drive or give it to someone else while being comfortable no data can be recovered from it.