**Question 1: what did you do?**

For this assignment, the tools we downloaded are to help demonstrate how difficult it can be to fully erase data. When you delete a file, many people assume it’s automatically gone. This isn’t the reality – the file continues to exist on your hard drive even after emptying your PC recycle bin. While some find this handy as they can recover files they’ve accidentally removed, from a security standpoint this is actually somewhat concerning.

I have been a long-term user of CCleaner. Once I learned of the program in college, I have always downloaded and kept the program on every computer I’ve owned or operated. Upon setup, I check every box available in the clean options under both Windows and Applications except the Saved Passwords and I tend to alter the settings from the typical one pass deletion to secure deletion. I also enable the cleaning to take place each time I start Windows. In past years, the only offered selection for secure deletion was 3 passes so that was my default setting. More recently this has updated in the program and now I use a complex overwrite selection of 7 passes. I taught myself how to build PC towers when I was in college and I became quite aware that if you are not careful when throwing away old components, like hard drives or USB thumb sticks, people are able to recover your confidential info from these items. I came across Open Box or used items online to purchase for steep discounts and what do you know, people’s files occasionally were still saved on the items for sale.

Recuva was a new program to me. I personally have never needed to try to recover something I’ve deleted before so I’ve never taken the time to research programs offering this ability. This program helps you to restore or recover files that have been deleted. Windows does not overwrite the MFT entry automatically allowing files to be restored. Only once Windows needs the space, does the overwriting happen and make it more challenging to recover a file. Recuva scans the MFT for files marked as deleted and is able to provide a comprehensive list of the files which can be recovered. One thing to note is that as Windows needs the space to save new files, the MFT entries will be overwritten so in order to have a higher chance of Recuva being successful, the sooner you use the tool, the better.

**Question 2: what were the results?**

For this assignment, the test file was named “dilbert\_security.gif”. Per the instructions, I saved this file to my pc, deleted it, and was able to restore it easily from the recycle bin. The next step was the delete it again, and then permanently delete it from the recycle bin. This I also did, however I forgot I still had my usual CCleaner settings on when emptying the recycle bin. When I ran Recuva, it showed a file I had deleted that day but it wasn’t named dilbert\_security anymore. The gif file type was the same and the state in Recuva was listed as ‘Excellent’, but the file was unable to show any preview or be viewed in any program I have. As this is how things should work, I would say CCleaner is a pretty successful option to use for overwriting and destroying data.

I spent some time next then researching how data is stored and then removed from a disk drive. When a disk is essentially full, the space containing deleted files becomes overwritten again and again, right up to the point when Windows (or any operating system) cannot find enough empty space for a file-write action. This is when the message appears to the user that the disk is full with no available space. Completing this assignment enlightened me to how even when files are deleted from a hard drive, anything can easily be restored using free recovery tools or professional forensic software if a user is skilled enough. I would say the public should be made aware as file deletion is a common misconception. Even most tech services claim they can do a quick and simple drive format to protect and delete your data. I’ve since learned even when you delete a file or format a drive, the data does not get immediately destroyed. It simply becomes free space available to be overwritten by new data, such as a new program or a photo, etc. Until the act of using the free space happens, the data remains intact and recoverable.

Researching on CCleaner’s website, there are instructions for wiping the data permanently. To do so, open CCleaner, go to Tools and select Drive Wiper. Then you are able to select which primary drive and wipe that selection. This also handles external hard drives which many people own and for those, you can select the “Entire Drive” option. The wipe process overwrites all the empty space which was previously occupied by your personal data and the overwriting destroys the content in the process.

**Question 3: what did you learn?**

This assignment confirmed my thought that there are some steps you can take to prevent data that’s left behind on old memory storage devices from being stolen. Any PC that is lost, sold or given away can retain old data even after a system reset. These files can range from personal memories or photos to your private documents, banking statements, emails, etc. This goes to show that any data on an old PC or an abandoned hard drive can easily be recovered, this opening yourself up to a lot of risks. I know this as a fact as I have purchased used computer items before and found this data myself unintentionally.

I was further curious if other options remained outside of a specific tool like CCleaner. I discovered that some motherboard BIOS, ie the basic program that controls every aspect of the computer, have a built-in safe erase option which in theory should also work regardless of the hard drive manufacturer. Next time I build a PC or need to tear down an older one for recycling components, I plan to further investigate this option. During one of my jobs working for a government contractor, they had a special high powered magnet tool which they turned on for any computer set to be replaced. This technology may not be available for the general public so if none of the previous options work, there is always the old school method of physically destroying the disk drive using a hammer or other tool.

Another difference I wasn’t aware of is the differences between overwriting data in HDD spinning hard drive compared to a SSD solid state drive. The older technology of the HDD requires multiple overwriting passes. For a SSD, this changes somewhat.

Upon doing some reading, I learned there are basically three stages for SSD: Clear, Purge and Destroy. SSDs work differently as data is stored in cells and those cells have a limited lifespan. Essentially, the cells wear out after multiple large amounts of data is written to them. To protect SSDs, the manufacturers have implemented a feature called “Wear Leveling” that evenly distributes data across cells. This preserves a certain portion of the drive should the cells start to fail. The SSD still is capable of having the entire drive filled with data and then wiped in which a majority of cells will be overwritten and your data will be destroyed.