Sera Hill
CIDM 6341-70

Recuva/CCleaner

What Did I Do?

For this assignment, I downloaded and saved the test image file to my computer. My computer wrote the saved image file to my hard drive and allocated space to store it there. Saving a file means it is broken down into multiple blocks that are then stored on the hard drive. This could mean that the data from the file are stored in different areas of the drive which is then put back together when the file is opened again. I then deleted it and restored it from my recycle bin to make sure that I could still retrieve the test file. By deleting the file, the computer removed the file reference from the file system's directory. This makes the file no longer visible to the user, but the data is still on the disk which is how I am still able to recover it from my recycle bin. Next, I deleted the file again and then permanently deleted the test file from my computer's trash folder. This means my hard drive is marking the previously occupied space as "free", making the space available for new data to be saved there. However, this does not mean that the data is removed, it's just classified as an area that could be overwritten should my drive need that room to store other data. To see if the test file was, in fact, truly deleted from my machine, I used the Recuva software to try and recover the file. Upon the supposedly deleted file's recovery, I saved it back to my computer.

Recuva scanned the hard drive to see if the data from deleted files still existed. The data may not have been overridden already, so the program checks to see if the data blocks are still there and tries to piece it together to form the full file. If the file's meta data has not been corrupted, Recuva could recover that as well, but it's not necessary in the file recovery. Providing the initial scan didn't work, Recuva can also do a more thorough scan that looks for file signatures to identify the lost files.

To try and actually get rid of the test file completely, I used another program called CCleaner and made the necessary adjustments to delete my test file from my computer. CCleaner is able to permanently delete files by performing "secure deletion" or "file shredding" where the data is overwritten multiple times thus making it unrecoverable. CCleaner has different options for overwriting data, and the more times it's overwritten, the

less likely a program like Recuva will be able to find the data. CCleaner also includes an option to overwrite any free space which gets rid of any remaining data from previously deleted files. The metadata is also erased which removes any reference of the file's data on the file system's index. Upon the completion of this program's deletion process, I ran Recuva again to see if I could recover the file once again. Recuva looks for data that may still be on the hard drive, even if it appears to the user that it is completely removed.

What Were the Results?

After running Recuva on my recycle bin, the Dilbert Security gif was recovered; however, I was unable to open the file. The fact that I was unable to open the file after it was recovered means that it was possibly corrupted during the recovery process and may have missing metadata. Missing metatdata doesn't necessarily mean the file will be unusable, but it is important for file accessibility. If some key parts of the data are missing from the recovered file, the recovered data may not be usable at all. However, this may not be true for all files, and if a person wants data permanently gone from their machine, they shouldn't rely on data degradation to protect others from recovering deleted files. Alternatively, a user should not rely on data recovery programs alone to recover their deleted files and should take the necessary precautions when handling important files on their computers. From my results in this assignment, it's easy to see how file corruption can render the file essentially useless.

Recuva was able to find my file despite me "permanently deleting" it from my recycle bin. This is because when you delete files from your computer, they are not immediately deleted, the reference to the file was just removed so the user gets the impression the file itself is gone. The space is marked as free on the hard drive so the user can potentially save over in that space. Until the exact space the file occupied on the hard drive, the file's data still exists and remains recoverable by tools like Recuva. This highlights the importance of overwriting the original file's data to ensure it can't be recovered in the future. The more times the data is overwritten, the less likely it will come up on data recovery tools.

Alternatively, after using CCleaner to get rid of the file, Recuva was unable to recover it at all. This is due to the fact that CCleaner overrides the original data multiple times with random patterns to ensure recovery tools cannot find the original data anymore. This shows us that emptying the recycle bin does not truly permanently delete data, but tools like CCleaner's secure deletion process does.

What Did I Learn?

I learned many things during this assignment that effect computer users in their personal and professional lives. I also realized just how careless I have been in the past with deleting files on my computer or external hard drives. I always thought that once you empty the trash bin on your computer, those files were gone forever. In a way, that made me more aware of what exactly I was deleting, but careless in thinking that they were unrecoverable. This doesn't necessarily mean I've compromised myself entirely, but I have bought new computers without properly destroying the data on my old ones. If I had sold those machines, the next person to use them could potentially use a file recovery tool like Recuva and could have gained access to my information's data that still existed on the computer's hard drive.

I have also been careless with the disposal of flash drives I used to use for school projects in the past. There's not much stopping somebody from taking a found or thrown away flash drive and seeing what files are on there. This is slightly embarrassing because I have held a job position where one of my duties was destroying physical CDs, floppy disks, tapes, etc. with hammers and shredders. I now fully realize why those such actions were necessary in getting rid of those storage devices, even though they had been wiped previously.

All of this highlights the importance of proper data removal or deletion within a company. Companies should utilize tools like Recuva and CCleaner to ensure sensitive information is inaccessible if they truly wanted it deleted. This would help reduce the amount of damage to the company and its data should a security breach occur. On the opposite side of that, should employees accidentally delete files, using something like

Recuva would help recover the deleted files. It can also help companies ensure they are freeing up necessary disk and hard drive space, helping their systems run smoothly.

Using tools like Recuva and CCleaner could be incorporated into a company's Enterprise Information Security Policy to promote better data security and system integrity. This way, companies can respond to incidences where files were deleted maliciously and they could take action to hopefully recover them before it was too late. They can also utilize CCleaner on old machines or drives that are no longer needed to ensure sensitive information can't be recovered by somebody not meant to view those files. It's also important for companies to remain compliant with regulations like GDPR to dispose of customer data. They can also use trainings for these tools with their employees to promote better education and awareness of what happens to files when you delete them, and that it may not be enough to just put unneeded files in the computer's recycle bin.

These tools should be used routinely in a company or even in a personal setting. The amount of time seems to depend on how often you are dealing with secure information. CCleaner recommends to clean your PC once or twice a week if you use your computer everyday for hours at a time (CCleaner Support Community).

In reference to attack surface, utilizing these tools can help reduce attack surface by eliminating potential ways for hackers to access your sensitive information. Instead of either throwing away your old storage devices or computers, you should make sure they are properly wiped so the next person to use your items can't access those files. It can also help prevent data loss vulnerabilities and reduce exposure to data breaches. With proper training and education, employees themselves can take more appropriate actions for getting rid of unneeded files, thus reducing the attack surface in that way as well.

Sera Hill
CIDM 6341-70

References

"CCleaner Support Community." *Ccleaner.com*, 2024, support.ccleaner.com/s/article/how-often-should-you-run-ccleaner-for-windows?language=en_US. Accessed 21 Sept. 2024.

"CCleaner Support Community." *Ccleaner.com*, 2024, support.ccleaner.com/s/article/how-does-recuva-works?language=en_US#:~:text=Regular%20recovery%20process%3A&text=Recuva%20scans%20the%20MFT%20for. Accessed 21 Sept. 2024.