Recuva/CCleaner Assignment

Jim Kinter

CIDM6341

1. What did you do

For this homework assignment, I followed a series of steps to explore file deletion, recovery, and secure erasure on a Windows system (using Windows 11). First, I downloaded and installed both Recuva (a free data recovery tool) and CCleaner (a system optimization and secure deletion tool) directly from the official website, ccleaner.com. I also downloaded the provided image file, dilbert\_security.gif, which is a GIF file featuring a Dilbert comic strip about computer security (a humorous take on password login requirements). I saved this file to the CIDM6341 course folder on my OneDrive for easy access during the experiment.

Step 1: Initial deletion and restoration from Recycle Bin. I right-clicked on dilbert\_security.gif in the course folder, selected "Delete," which moved the file to the Recycle Bin. I then opened the Recycle Bin, located the file (it appeared intact with its original 41,478 byte filesize and thumbnail preview), right-clicked it, and chose "Restore." The file reappeared in the course folder. To verify, I double-clicked it in Windows Photos, and it opened perfectly— the comic strip was fully visible, with no corruption, colors intact, and the text readable (Mordoc [presumably the CISO] saying that in a perfect world no one would be able to use anything).

Step 2: Second deletion and permanent deletion. I deleted the file again using the same method (right-click > Delete), sending it back to the Recycle Bin. This time, instead of restoring, I opened the Recycle Bin, right-clicked on dilbert\_security.gif, and selected "Delete" to permanently remove it (this is equivalent to bypassing the Recycle Bin with Shift+Delete, but I followed the bin method for clarity). I then clicked the “Yes” button to confirm that I did indeed want to permanently delete the file. The file disappeared from the Recycle Bin, and a confirmation dialog warned that it would be permanently deleted.

Step 3: First Recuva recovery attempt. I launched Recuva, selected "Enable Deep Scan" for thoroughness, and chose to scan the path to the course folder. I specified to look for image files (.gif) in the wizard. The scan took about 15 minutes and listed several recoverable files, including dilbert\_security.gif marked as "Excellent" condition (green status). I selected it for recovery, saved it to my Documents folder as recovered\_dilbert.gif, and opened it in Windows Photos. It was complete and identical to the original—no missing frames, distortion, or artifacts.

Step 4: CCleaner’s Drive Wiper was not used because it warned that wiping free space on an SSD could reduce its lifespan due to excessive write cycles (SSDs have limited program/erase cycles per cell, typically 1,000–10,000). Instead, I used Windows’ built-in cipher.exe tool for secure deletion. I first re-downloaded dilbert\_security.gif, deleted it with Shift+Delete to bypass the Recycle Bin, and ran CCleaner’s "Custom Clean" to clear temporary files and the Recycle Bin. Then, I opened a Command Prompt as Administrator and executed cipher /w:C: to overwrite free space on the C: drive with three passes (zeros, ones, random data). This took ~30 minutes for the 237 GB SSD’s free space (~100 GB).

Step 5: Second Recuva recovery attempt. I ran Recuva again with the same settings (Deep Scan on C: drive for .gif files). The scan completed in about 18 minutes but did not list dilbert\_security.gif or any similar file. I expanded the search to all file types and unchecked filters, but no trace appeared—not even fragmented versions. To double-check, I scanned specifically for files with "dilbert" in the name, but results were empty for that entry.

Throughout, I ensured all actions were on non-critical files to avoid any system risks.

1. What Are the Results?

* Restoration from Recycle Bin: The restored file was perfect—41,478 bytes, identical to the original. The GIF opened in Windows Photos, showing the full Dilbert comic with no data loss.
* Permanent deletion: After emptying the Recycle Bin, dilbert\_security.gif disappeared. File Explorer searches for "dilbert\_security.gif" returned nothing, confirming it was no longer accessible via the file system.
* First Recuva recovery: Recuva recovered the file flawlessly. The recovered file (41,478 bytes) opened perfectly, matching the original pixel-for-pixel (verified in an image viewer). Its "Excellent" status indicated no overwriting or fragmentation.
* Secure deletion with cipher.exe: The cipher /w command completed without errors, overwriting ~100 GB of free space. CCleaner’s Recycle Bin clean ensured no temporary traces remained. The SSD showed normal performance post-wipe (checked via Task Manager’s disk activity).
* Second Recuva recovery: No recovery was possible. Recuva found no matches for the file, even with Deep Scan and no filters. The cipher overwrite erased the file’s data from the SSD’s NAND cells.
* The initial "permanent" deletion was recoverable, but cipher.exe’s overwrite made recovery impossible, highlighting the difference between logical and physical deletion.

1. What Did You Learn?

This experiment clarified file storage, deletion, and recovery on an SSD, and why CCleaner advises against Drive Wiper for SSDs. SSDs (solid-state drives) are different from old-school hard drives because they store data in special memory chips that can only handle a limited number of "writes" before they start wearing out—like how a pencil eraser gets smaller with each use. Drive Wiper works by repeatedly writing over empty space on the drive to securely erase leftover data from deleted files. While this is fine for traditional hard drives, it can unnecessarily stress an SSD, shortening its overall lifespan.

That's why CCleaner warns against it. Instead, for secure deletion on an SSD, it's better to use gentler built-in Windows tools like cipher.exe, which does the job with fewer writes and keeps the drive healthier. The key point is: regular deleting hides files but doesn't fully erase them until something overwrites the space—tools like this make sure they're gone for good, but be aware that you don’t damage/reduce the usable life of the drive.

I spent some time online learning about SSD hardware and how they work so, I also learned that "Deleting" a file (to Recycle Bin or permanently) only removes its Master File Table (MFT) [like a table of contents of the drive] entry, marking pages as free. On SSDs, TRIM may erase data quickly, but if not yet erased (e.g., due to low disk activity), the data remains in NAND cells. This allowed Recuva’s first recovery: it scanned raw NAND for GIF signatures ("GIF89a") and reconstructed the file from untrimmed pages. Deep Scan helped by ignoring the file system and carving data directly.

CCleaner’s Drive Wiper is risky for SSDs because it writes to all free space, accelerating wear on NAND cells (each cell has a finite write endurance). Instead, cipher.exe’s /w switch safely overwrites free space without excessive writes, using a three-pass method (zeros, ones, random) to scramble data. This made the file unrecoverable, as Recuva couldn’t detect the GIF’s signature post-overwrite—NAND cells were reset to a uniform state. On SSDs, TRIM and garbage collection may already reduce recovery chances, but cipher ensures permanence.

My key takeaways from this exercise: Standard deletion is logical, leaving data recoverable until TRIM or overwrites occur. Recuva exploits residual data, but tools like cipher.exe ensure privacy by physically erasing free space. For SSDs, avoid tools like CCleaner’s Drive Wiper; use cipher.exe or similar (e.g., sdelete from Sysinternals) to balance security and drive health. The Dilbert comic’s security theme was fitting—data isn’t truly gone until you plug the "holes" with deliberate overwrites