Recuva/CCleaner Report by Masyn Grisel

What did you do?

Before following the instructions provided for this report(which I will list), I researched what the two software’s, Recuva and CCleaner, do and how they work. I did this to gain a better understanding of what the process I was doing would be. Next, I downloaded the “Dilbert\_Security.gif” and opened it to make sure it was working. Next, I deleted the file and restored it by going to my recycling bin and locating the file. Then, I deleted the file again and permanently deleted it by going to my recycling bin. Still following the instructions provided, I ran Recuva and took note of the files recovered. Then, I opened the Dilbert\_Security.gif file to check if it was complete and saved it to my documents directory. Next, I downloaded CCleaner and deleted the Dilbert\_Security.gif, then I ran Recuva again to see if it would find the file. After doing all these steps, I researched the best ways to permanently delete files. I also researched how hackers could recover files that most people would think were deleted.

What are the results?

These are the questions I asked ChatGPT about Recuva and CCleaner and the responses I was given:

Question: What is Recuva?

Response: Recuva is a free data recovery software developed by Piriform, designed to help users recover deleted files from their computers, external hard drives, USB drives, memory cards, and other storage devices. It can retrieve files that have been accidentally deleted or lost due to system crashes, formatting, or other issues.

Recuva supports various file types, including documents, photos, videos, music, and emails. In addition to its file recovery functionality, it also includes a secure deletion feature, which allows users to permanently erase files in a way that makes them unrecoverable. This makes it useful for both data recovery and data destruction tasks.

Question: How does Recuva actually work?

Response: Recuva works by scanning storage devices for files that have been deleted but are still physically present on the disk. When a file is deleted from a computer, it’s not immediately erased. Instead, the system marks the space occupied by the file as available for reuse. Until new data overwrites that space, the original file remains recoverable. Recuva takes advantage of this by searching for and restoring those files.

Here’s a breakdown of how Recuva works:

**1. Scanning the Storage Device**

Recuva offers two types of scans:

* **Quick Scan:** This looks for recently deleted files by scanning the file directory for pointers (references) to deleted files. If the pointers still exist and the files haven’t been overwritten, they can be recovered easily.
* **Deep Scan:** This is a more thorough scan that looks for remnants of deleted files based on file signatures (patterns that identify the file type). It’s more time-consuming but is effective for finding files that might have been deleted some time ago or after significant data writing activity.

**2. Analyzing the File System**

Recuva analyzes the file system (like NTFS, FAT32) to detect deleted files. It checks metadata like file names, sizes, and locations. Even if the directory entry (pointer) is deleted, Recuva can identify files based on the remaining clusters in the file system.

**3. Recovery of Files**

Once it locates deleted files, Recuva shows a list of recoverable files, along with their "recoverability status":

* **Excellent:** The file has not been overwritten and is likely to be fully recoverable.
* **Poor/Medium:** Parts of the file have been overwritten, but some of it may still be recovered.
* **Unrecoverable:** The file has been overwritten or corrupted, making it impossible to recover.

Users can then choose which files to recover and where to save them. It’s recommended not to save recovered files on the same drive they were recovered from, as this can overwrite other deleted data that may still be recoverable.

**4. Secure Overwriting (Optional)**

In addition to recovery, Recuva also offers the option to securely overwrite files, making them unrecoverable by using advanced algorithms (like Gutmann or DoD 5220.22-M) to overwrite the data multiple times.

**Key Features that Aid Recovery:**

* **File Signature Detection:** Even if the file metadata is gone, Recuva can use file signatures to find files by their content. This is especially useful in the deep scan.
* **Raw Data Recovery:** For damaged or formatted drives, Recuva can read raw data and attempt to reconstruct deleted files.
* **Filtering:** Users can filter by file type (e.g., images, documents) or file names to make recovery easier and more focused.

In summary, Recuva works by identifying and restoring data that hasn't been completely overwritten, leveraging the structure of file systems and file signatures to maximize recovery chances.

As you can see, Recuva is possible because files are not immediately erased when deleted, which is something I was not aware of.

Question: What is CCleaner?

Response: **CCleaner** is a system optimization, privacy, and cleaning tool developed by Piriform (now part of Avast). It is designed to help users improve the performance of their computers by removing unwanted files, cleaning up the registry, managing startup programs, and more.

Question: How does CCleaner software work?

Response: CCleaner works by scanning your system for unnecessary or unwanted files and cleaning them to improve performance, free up disk space, and enhance privacy. Here's a breakdown of how it works across its various functions:

**1. File Cleanup**

CCleaner scans for files that are no longer needed by the system, including:

* **Temporary Files:** These are created by applications (e.g., web browsers, Office tools) and the operating system for short-term use. CCleaner identifies and removes these files, freeing up storage.
* **Cache, Cookies, and Browsing History:** CCleaner clears out cached web data, cookies, and browsing history, helping free up space and enhance privacy.
* **System Files:** It removes outdated system files such as Windows Update leftovers, crash dumps, and error logs, which aren't necessary for daily use.

The scanning process can be customized, allowing users to select specific types of files or directories to target. Once the scan is complete, CCleaner presents a list of files for review, and users can delete all or selected items.

**2. Registry Cleaner**

The Windows Registry is a database that stores low-level settings and configurations for the operating system and applications. Over time, invalid or unused entries can accumulate, slowing down the system.

* **Scan for Issues:** CCleaner scans the registry for broken, redundant, or missing entries, such as missing shared DLLs, invalid file paths, unused file extensions, and outdated program settings.
* **Cleaning:** After presenting a list of registry issues, CCleaner offers an option to back up the registry before fixing any issues. This ensures you can restore it if anything goes wrong. After backing up, CCleaner repairs or removes the problematic entries.

**3. Startup Manager**

When many programs start automatically with Windows, it can slow down the boot process and affect system performance. CCleaner helps by:

* **Listing Startup Programs:** It identifies all programs and services that load during startup.
* **Enabling/Disabling:** Users can enable or disable these programs to reduce startup time and improve performance.
* **Prioritizing Programs:** You can decide which programs should start automatically based on necessity.

**4. Uninstall Manager**

CCleaner offers a more detailed alternative to Windows’ built-in uninstaller.

* **Listing Installed Programs:** It shows all installed software, including some that might not be visible in Windows’ standard uninstaller.
* **Removing Programs:** Users can uninstall unwanted programs directly from CCleaner, freeing up system resources and disk space.

**5. Privacy Protection**

CCleaner enhances privacy by removing traces of online activity and usage history from browsers and applications:

* **Browser Cleanup:** It deletes cookies, cache, and history from popular browsers (like Chrome, Firefox, Edge). This not only frees up space but also helps protect against tracking by websites.
* **Application Cleanup:** It also removes usage history from specific programs, ensuring that recent documents, searches, and other activity are erased.

**6. Duplicate File Finder**

CCleaner scans for duplicate files (e.g., copies of documents, images, or other files) that may be taking up unnecessary space.

* **Scanning:** Users can select which folders or drives to scan, and CCleaner presents a list of detected duplicates based on name, size, and content.
* **Deleting:** After reviewing the duplicates, users can select which ones to delete to recover storage space.

**7. Secure File Deletion**

CCleaner offers a feature to **securely delete** files, ensuring that deleted data cannot be recovered using recovery tools:

* **Simple Deletion:** Regular file deletion may leave traces that can be recovered with specialized software.
* **Secure Overwrite:** CCleaner allows users to securely overwrite files using methods like the **Gutmann algorithm** or **DoD 5220.22-M**. These methods overwrite the file with random data multiple times, making recovery impossible.

**8. Software Updater (Pro Version)**

For users with the Pro version, CCleaner scans for outdated software and provides options to update them, helping to keep your system secure and functional with the latest features and security patches.

**9. Drive Wiper**

The Drive Wiper feature allows users to securely wipe entire drives or just free space on a drive to permanently delete files:

* **Wipe Free Space:** This overwrites the free space on your hard drive, preventing recovery of previously deleted files.
* **Wipe Entire Drive:** For situations like selling or decommissioning a computer, users can wipe entire drives to ensure all data is erased.

**How CCleaner Works Technically:**

* **Scanning:** CCleaner uses predefined rules and patterns to identify files, registry entries, and other elements that can be cleaned or optimized. These rules are based on common temporary file locations, browser history formats, and Windows registry structures.
* **Cleaning:** After identifying the data to be cleaned, CCleaner removes or overwrites it, depending on the user's preferences. For file removal, it uses standard file deletion processes. For secure deletion, it overwrites the data with random patterns.
* **Real-time Monitoring (Pro Version):** In the Pro version, CCleaner can monitor the system in real-time, automatically cleaning files when certain conditions are met (e.g., when free disk space drops below a certain threshold).

In summary, CCleaner works by scanning your system for files and settings that can be optimized or deleted, allowing users to improve system performance, free up disk space, and protect privacy. It simplifies routine maintenance tasks, making it easy to keep your system running smoothly.

After researching these tools and how they work, I followed the instructions described at the beginning of this report. Sure enough, the Dilbert\_Security.gif file was restored at first, and I did have to delete it using CCleaner, which caused the file to not show up when I ran Recuva again. This was very eye-opening to me because I would have just deleted it and assumed it was gone.

To conclude my research, I asked ChatGPT two questions, listed below with responses:

Question: What are some ways to permanently delete files?

Response: **Ways to Permanently Delete Files:**

1. **Overwrite with Data (Secure Deletion):** Tools like CCleaner, Eraser, or SDelete overwrite files multiple times with random data, making them unrecoverable.
2. **File Shredders:** Use tools like **File Shredder** or **Secure Eraser** to destroy files by overwriting and deleting them securely.
3. **Wipe Entire Hard Drive:** Tools like **DBAN** or **CCleaner’s Drive Wiper** wipe the entire drive or free space to erase all data permanently.
4. **Physical Destruction:** Destroy the hard drive by drilling holes, shredding, or using a degausser to ensure data is unrecoverable.
5. **Use Built-in OS Tools:**
   * **Windows:** Use **BitLocker** for encryption or the **Cipher Command** to wipe free space.
   * **MacOS:** Use **Disk Utility** to erase free space.
6. **Encrypt Before Deleting:** Encrypt files with tools like **VeraCrypt** before deletion, so even if recovered, the data is unreadable.
7. **Wipe Free Space:** Use tools like **CCleaner** or **SDelete** to overwrite free space after deletion, ensuring no data remnants remain.

For SSDs, ensure **TRIM** is enabled to securely handle deleted data.

Question: How can hackers use files that someone thinks are deleted to hack someone?

Response: Hackers can exploit files that someone thinks are deleted because, in most cases, deletion only removes the file’s reference, not the actual data. Using recovery tools like **Recuva** or **EaseUS Data Recovery**, they can retrieve sensitive information like passwords, financial records, or personal details from these files. This allows them to hack accounts, steal identities, or gather information for targeted attacks. Even remnants like file names or metadata can help them gain further insights into a user's activity or network.

This concluded the results portion of my research.

What did you learn?

I learned a great deal about deleting files permanently and how my understanding of the deletion of files was wrong. In the past, I would assume that, once you delete a file initially, it is unavailable to a hacker. The more research I do on different topic regarding hacking, the more I realize just how little I knew. I believe all businesses should do training and required learning over this material because it could be the difference between a major hack and not. I also learned about specific ways to delete your files permanently. For example, I never knew it was an option to physically destroy your hard drives because it seemed too extreme to me. Going back to the business aspect of this information, I have never been in a job where this type of information was discussed at all. I have been in positions where I had access to sensitive information that was just deleted once. Luckily, we were never hacked at any places I worked at, but it is important to understand the possibilities. What if a competitor wanted to steal information to gain an advantage, and all of your “deleted” files were in the recycling bin? What if all the information needed to take away your personal information was sitting there, and you were not worried because you thought you deleted the information? These are questions I am thinking about more and more now, and I believe that businesses everywhere should further expand their knowledge on how they deal with sensitive information and files.