Fougnigue Sefon

Cybersecurity CIDM 6341

Fall 2023

Recuva/CCleaner report

In a world increasingly reliant on technology, digital file management has become both a challenge and a necessity. This report attempts to uncover the complexities of data deletion and recovery, utilizing two software tools, Recuva and CCleaner. I will assess not only the actions I took but also the underlying mechanisms at play, shedding light on the often misunderstood process of file deletion within computer systems and exploring the tools and techniques that can be employed to ensure the permanent erasure of sensitive data. The first section will provide a comprehensive view of the research process and methodology, the second section will offer insights into the outcomes of my actions, and the last section will present the lessons gained from the experiments.

Section 1: What did I do?

In this experiment, the primary objective was to explore the challenges of data erasure, specifically focusing on two software tools, Recuva and CCleaner. I proceeded to download the free version of Recuva from the official website (https://www.ccleaner.com/recuva/download). Additionally, I downloaded a sample file named "Dilbert\_Security.gif" from WT Class.

The first step involved deleting the "Dilbert\_Security.gif" file and subsequently restoring it from the operating system's recycle bin. This action was performed to demonstrate that the delete function does not permanently erase the data but rather stores it in the recycle bin folder, making it recoverable.

When restored, the image was as good as new, and I was still able to open it with no issue. Following the restore, I once again deleted the image. This time, I also deleted it from the recycle bin. The goal was to permanently delete the file from my computer. To test if my goal was achieved, I used Recuva. Recuva is a data recovery tool designed to retrieve deleted files. When launching it, the interface was user-friendly and accessible. I chose the type of file I was trying to recover, in this case, a picture. The wizard then prompted me with the location from where the file was deleted. I chose “in the recycle bin”. Other options included media cards, documents, and “I am not sure” which would search everywhere on my computer. After that, Recuva performed a scan searching for files that had been deleted but not yet overwritten by new data. Recuva could indeed retrieve the file. Upon retrieval, the state of my file was deemed excellent. After recovering the file, I assessed the completeness of the recovered file. It was fully recovered and the "Dilbert\_Security.gif" was readable. I saved it in my documents. On Recuva, I noticed other files, whose states were deemed unrecoverable, had a comment saying that the file was overwritten. This led me to think that the only way to permanently delete a file was to overwrite it.

The next step in the process was to download and install the CCleaner Professional trial version from the official website (<https://www.ccleaner.com/download>). It is a system optimization and cleaning tool. I ran CCleaner and used it to clean my recycle bin. I then deleted the "Dilbert\_Security.gif" and once it was moved to my recycle bin, ran CCleaner one more time. Subsequently, I executed Recuva once more to determine whether it could locate and recover the file after the use of CCleaner. The file was not recoverable this time.

Section 2: What were the results?

Files that were initially deleted were only being moved to the recycle bin. Once there, they were easily recoverable, even without the use of specialized software. Using Recuva and CCleaner brought more impressive results.

First, we have the Recuva results. Recuva successfully recovered the "Dilbert\_Security.gif" file after its initial deletion. This outcome demonstrates a fundamental concept of data recovery: when a file is deleted from the operating system, it is not entirely erased. Instead, the reference to the file is removed, making it invisible to the user, but the data remains intact on the storage device. Recuva's scanning process, as outlined in Section 1, allows it to locate and reconstruct deleted files. The file was fully reconstructed and recovered. In most cases, when a file is newly deleted and hasn't been significantly overwritten, Recuva can retrieve the entire file.

Then, we have the CCleaner results. Following the installation of CCleaner, we used its secure file deletion feature to clean the recycle bin and permanently erase the "Dilbert\_Security.gif" file. This process involved overwriting the file's data with random characters. As expected, CCleaner's secure deletion function successfully prevented Recuva from locating and recovering the file. This demonstrates the effectiveness of overwriting data to make it irretrievable.

Section 3: What did I learn?

This experiment provided several valuable lessons.

First, I discovered Recuva and CCleaner functionalities. Recuva effectively recovers files that are deleted, while CCleaner offers a secure deletion feature preventing recovery. They are both vital tools for ensuring data security.

Second, I learned a lot about file deletion and recovery mechanisms. Understanding how files are stored and deleted is essential for data security and privacy. Deleting a file removes the file's reference but leaves its data recoverable. The successful recovery of the "Dilbert\_Security.gif" file by Recuva highlights the importance of understanding that, in typical file deletion, data remains on the storage medium until it is overwritten. CCleaner's secure deletion feature effectively prevents data recovery. By overwriting the file's data, it ensures that even specialized data recovery tools like Recuva cannot retrieve the file.

Third, the results could have implications for both individuals and companies. Individuals must recognize that simply deleting files from their computers or storage devices does not guarantee data privacy. This awareness is especially crucial for safeguarding personal information. Even files deleted from the recycle bin can be recoverable if not securely erased. This underscores the need for securely emptying the recycle bin and ensuring comprehensive data protection. One should consider using secure data erasure tools to ensure that confidential information remains so and is not susceptible to unauthorized access. Proper management of the recycle bin will be essential.

Companies handling sensitive customer data, financial records, or proprietary information should implement secure data erasure practices to comply with data protection regulations, such as GDPR or HIPAA. This may include regular data overwriting, secure disposal of storage media, and strict access controls as measures to counter data recovery attempts by unauthorized parties. This ensures that sensitive information, once it has reached the end of its useful life, is thoroughly eradicated. Companies should also put an emphasis on proper training for employees. Staff should be educated on the importance of secure data deletion and provided with the necessary tools and knowledge to do their job securely. Furthermore, these practices should be part of a comprehensive information security policy program. Such a policy should be impartial, covering not only IT aspects but also considering end users who possess common privileges such as Read, Write, Execute, and Delete. It should offer step-by-step procedures as instructions for secure data erasure. Companies, even those less well-versed in data security, can utilize resources like sans.org to access policy templates. Management needs to ensure constant maintenance and modification of these policies and procedures. This ongoing commitment is vital to adapting to evolving threats and technologies and maintaining the highest level of data security. Failure to do so may expose the company to security breaches, regulatory penalties, and damage to its reputation. Thus, a proactive approach to information security is essential for the long-term success and integrity of a company's data management practices.