**Name:** Amarachi Anthony

**Buff Id:** 1130441

**Course:** CIDM 6341(Cybersecurity)

**Assignment**: Recuva/CCleaner

**What Did You Do?**

**Recuva**

I conducted a file recovery test using Recuva to gain a deeper understanding of its internal operations. I began the process by downloading the test file named Dilbert\_security.gif, saved it on my desktop, and then deleted it. After recovering the file from the Recycle Bin, I deleted it again and emptied the bin to make sure it was permanently deleted. Then, I installed Recuva, ran a scan, and successfully recovered the file, demonstrating its strong data recovery capabilities.

Recuva accesses parts of the storage device marked as free space by Windows but still containing deleted files until they are overwritten. When a file is deleted, Windows updates the Master File Table (MFT) to mark it as deleted without immediately erasing it from the system. The space it occupies is now available for new data, but the actual data remains overwritten. Recuva scans the MFT to find deleted files, reads associated metadata, and checks if the data has been overwritten. If the data remains, Recuva can fully recover the file. However, only partial recovery may be possible if some parts have been overwritten.

Recuva supports various file systems used on internal and external storage devices, such as FAT, exFAT, and NTFS. In this test, Recuva located and restored the deleted Dilbert\_security.gif file, showing its ability to recover files not visible to the system.

**CCleaner**

I used CCleaner to thoroughly clean up the files on my system, with the primary intention of permanently removing unwanted files. To test its effectiveness, I deleted a file called Dilbert\_security.gif. My goal was to completely erase the file from the hard drive so that file recovery tools like Recuva could not recover it.

I installed CCleaner, ran the program on my system, and noticed that it successfully cleared out unwanted files, permanently deleting them from the system. This process provides an extra layer of data security by ensuring that sensitive files are completely erased and cannot be retrieved.

Deleting files from a system might seem simple - right-click, select "delete," and then empty the Recycle Bin. Initially, the file is gone for good. However, the truth is different. When a file is deleted, it is not quickly removed from the hard drive. Instead, the operating system marks the space the file used to occupy as available for new data. The file stays on the disk until new data is written over it. This means that programs like Recuva can still recover the deleted file unless overwritten.

CCleaner goes beyond the basic deletion process. It scans through the system's Master File Table (MFT), which is essentially an index of all the files stored on the hard drive. The program identifies the files marked for deletion and securely frees up their space. By doing this, CCleaner ensures that the files are marked as deleted and removed, making it much more difficult (if not impossible) for recovery tools to restore them.

**What were the results?**

**Recuva**

After running a scan with Recuva, I found a list of deleted files, including the test file Dilbert\_security.gif that I had previously deleted. Recuva's scan results indicated that the file was in **"**Excellent**"** condition, with no clusters overwritten by new data. This meant that the file was fully intact and could be successfully recovered without any corruption. The screenshot (see above) illustrates the detailed scan outcome, showing the status of the file as fully recoverable.

This test highlighted Recuva's powerful recovery capabilities. Even though the file had been permanently deleted from the system and was no longer visible through the file explorer, Recuva was able to locate and completely restore it. This emphasizes the importance of understanding that "deleting" a file often only removes its reference in the operating system, leaving the actual data intact on the disk until overwritten.

A screenshot of a computer

Description automatically generated

**CCleaner**

After using CCleaner, the tool efficiently removed 2.05 GB of system clutter, which included residual files such as browser cache, temporary system files, and other unnecessary data. More importantly, CCleaner performed a secure file deletion of the test file Dilbert\_security.gif, ensuring that it was permanently erased from the system. The detailed cleanup report shows that the file was securely overwritten during this process.

To verify the effectiveness of the deletion, I ran another Recuva scan after using CCleaner. This time, the test file was not recoverable. The secure deletion process had successfully overwritten the file's storage sectors, making any attempt to recover it impossible. This demonstrates CCleaner’s effectiveness in ensuring sensitive or unwanted files are deleted and securely wiped from the system, preventing future recovery attempts.

The combined use of both tools showcased how essential it is to perform secure deletion for sensitive files. While Recuva can recover data that has simply been deleted, CCleaner ensures that the deletion is final, safeguarding privacy and data integrity by making the file unrecoverable.

A screenshot of a computer

Description automatically generated

**Recuva after the CCleaner scan**

I used Recuva to attempt to retrieve my deleted Dilbert\_security.gif file. Unfortunately, the Dilbert\_security.gif file was not found among the suggested recovered files, indicating that CCleaner has permanently deleted it from my system, and Recuva was unable to locate and recover the file. Below are the results from Recuva.

A screenshot of a computer

Description automatically generated

**What did I learn?**

**Recuva**

Using Recuva taught me that when a file is deleted, it remains on the hard drive until the space it occupies is overwritten by new data. The more system is used after deletion, the greater the likelihood that space will be reused, making file recovery more complicated. This indicates that the sooner you stop using the system after deleting a file, the higher the chances of successfully recovering it.

I also found out that Recuva provides two types of scans: a regular scan and a deep scan. The deep scan is comprehensive, searching through the system's thousands of files, folders, and entire drives. While this method takes longer, it finds files the regular scan may not detect.

Recuva also allows users to narrow down the scan results by specific areas of interest or by typing the name of a specific file, which helps find data more efficiently.

Another useful feature is that once Recuva has recovered files, you can choose numerous things and access different alternatives via a right-click menu. This gives more flexibility in handling retrieved data and permits for additional steps outside easy recovery.

In terms of security, I realized the critical nature of secure file deletion practices. Tools like Recuva can easily recover deleted files, including sensitive data, unless they are securely overwritten. This is crucial when dealing with confidential information, as regular deletion does not provide sufficient protection from potential data breaches.

**What did I learn?**

**CCleaner**

After using CCleaner, I've discovered that it offers much more than just basic file deletion. Upgrading to the professional version revealed that CCleaner also provides robust antivirus capabilities, adding an extra layer of security to my system. Its functionality extends beyond file cleanup and includes advanced features that enhance system security, making you feel informed and knowledgeable. Using CCleaner, I realized the importance of regularly running secure cleanup operations, especially in scenarios involving sensitive data. The tool offers much more than basic file deletion by securely wiping data from the system.

CCleaner's built-in web browser effectively shields against unwanted ads, malware, phishing attempts, and malicious downloads. This browser also helps to block irritating pop-ups and reduce excessive browser cache accumulation. Notably, the browser is built on Chromium, an open-source project from Google, and is exclusively available for the Microsoft Windows operating system.

CCleaner's seamless integration of security tools and system maintenance capabilities showcases its versatility. It serves as a powerful cleanup tool and provides a comprehensive solution for optimizing and safeguarding systems.

**How Recuva and CCleaner Inform a Security Program**

Recuva and CCleaner both play essential roles in a security program. Recuva can be used regularly to find potentially recoverable files on a system, which allows one to determine if sensitive data is still at risk after deletion. This can prompt system administrators to use secure deletion methods or adjust data retention policies to reduce risks.

CCleaner complements Recuva by ensuring that data is permanently removed after deletion. Regular use of CCleaner helps keep the system clean by securely erasing temporary files, cache data, and sensitive information, making it a crucial tool for data security. Incorporating these tools into a regular maintenance schedule can help organizations protect their systems from unintentional data recovery or leaks.