**RECUVA/CCLEANER**

Adrian Varela

WTAMU

CIDM 6341-70: Current Issues In Cybersecurity

Professor Murray Jennex

February 12, 2023

WIRELESS SURVEY

WHAT DID YOU DO

First thing I had to do for this exercise to download Recuva was utilize my Windows Laptop. Unfortunately, Recuva does not work well with Macbooks and this led to my first discovery. I followed the instructions step by step ensuring I downloaded the file of Dilbert.gif to my device. I ensured to store it through my hard drive to view the file through the recycle bin and deleted the file. Once I started and downloaded the data recovery tool, Recuva I had the opportunity to begin my scan for the deleted file of Dilbert.gif. When installing I had to answer what File Type I wanted, I chose all files. I then had to select the file location so, I chose the option of “I’m not sure”. Then the tool was scanning through all seven of my file drives retrieving all deleted files. It then moved to stage two of analyzing damaged data and ended with stage three analyzing file contents.

WHAT WERE THE RESULTS

The results of the Recuva software were very interesting to see all of the files that I thought I had once deleted. Through the results there were over 5,000 files found in less than 30 seconds. This would have taken me a longer time if it was not for the advanced mode search. I had the opportunity to look for the Dilbert.gif file once I choose the correct drive I wanted and the file type. I modified the content by clicking the top tab of date to show the files from newest to oldest. I found the Dilbert.gif file and selected the folder location. Once recovered, I found that the file was reorganized through encryption and just had what looked like a binary code on the file. This led me to test it with a text file. I used notepad and deleted this filed and recovered it utilizing the same steps. The result was different though, it was the exact file that I had deleted.

WHAT DID YOU LEARN

My results for this portion of the exercise taught me first, that files if stored on a hard drive are never fully deleted. This can be useful for a company if people are trying to keep information from their employer by deleting certain files. These files can be retrieved through software. These files are stored permanently on the hard drive for which it is selected and can be recovered easily with these tools. I found out that the delete function only frees up the space that the certain file took. This shows that the file is still located on the hard drive.

Another piece of information I found useful for the Recuva tool was that although the picture was not recovered exactly the same only a portion of it was retrieved. The retrieved information was the encryption of the photo used. When experimenting with the text file I created, Recuva fully recovered the text and the information on the file.

CCleaner

WHAT DID YOU DO

When beginning with the CCleaner I had to utilize the Wizard to download the software. CCleaner analyzed and extracted the files and data from my computer to notify me of what could be cleaned out. Once the software was running, I then searched through tools to find the Dilbert.gif file. Once the file was found I right clicked the file, and the CCleaner gave me the option to wipe this file. Once deleted the I went back to Recuva where I refreshed my scan to attempt to find the file once again.

WHAT WERE THE RESULTS

The results for the Dilbert.gif file was nowhere to be found. I then, looked through all the drives utilizing the Recuva software and again the same result was the file was no longer there. I attempted the same deletion on a text file. This again proved that the file was no longer on the drive or any of the other seven drives as well.

WHAT DID YOU LEARN

These exercises gave a huge amount of information when it comes to the difference from deleting and wiping files. Through CCleaner the software wipes the files that have been stored on the drive. This makes the file no longer able to exist through any recovery setting. When Recuva was able to retrieve the files through the previous exercise it was because the files were just deleted. This allows the files to still exist but, no longer take up space in the drive. I was astounded that I found files from 2018 that were not wiped but still able to recover using the Recuva tool. This also help me understand that when it comes to people attempting to be malicious it is easily proven if someone wipes a file versus just accidently deletes one. This shows the complexity it takes to erase files through a company’s device.