Slacker Tool Evaluation

Contents

[Introduction 3](#_Toc43034020)

[Installation 3](#_Toc43034021)

[Using Slacker.exe 3](#_Toc43034022)

[Conclusions 3](#_Toc43034023)

# Introduction

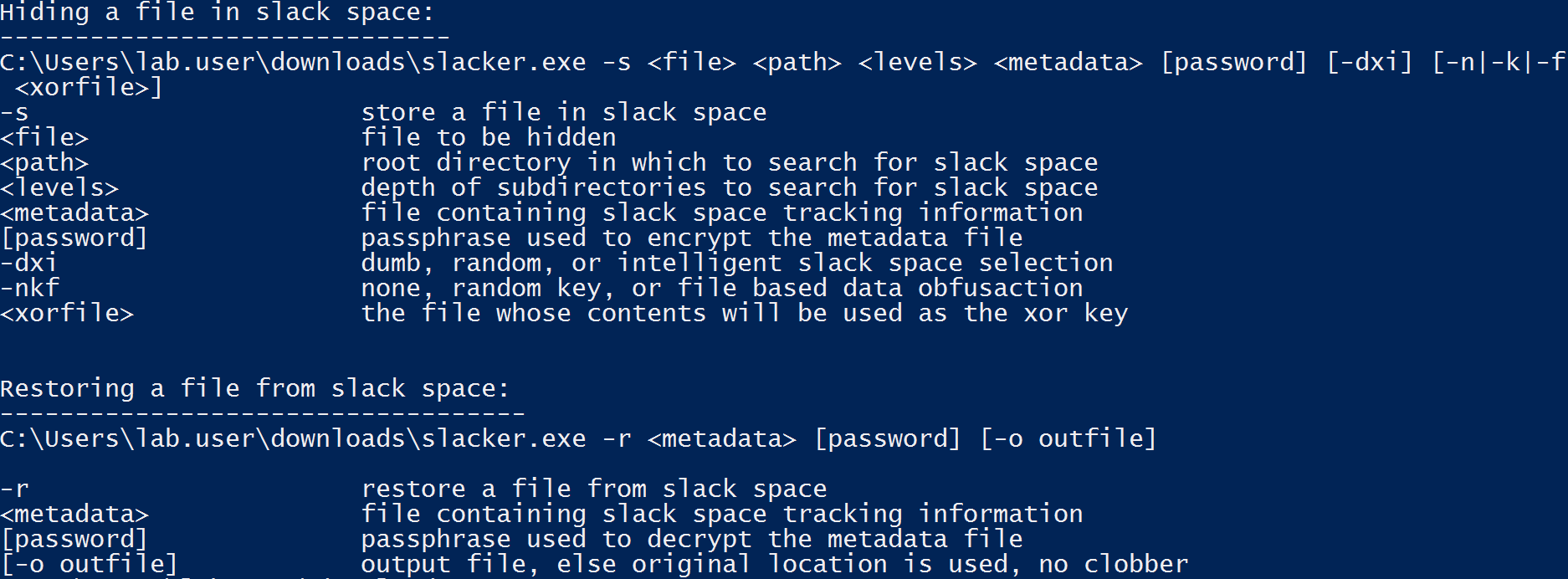
Slacker.exe is a tool that allows users to hide files within the slack space that is inherent to modern NTFS file systems. Slack space is unused space in a file that occurs due to the design of modern hard drives. Since most drives have set cluster sizes of about four kilobytes, any file that does not use 100% of that space will have remaining, empty space that is inaccessible using traditional file exploring software. Storing files in slackspace can be a clever avoidance technique to hide critical files while you are in the process of performing an attack. While it may have once been a more powerful anti-forensic technique, most modern forensic tools can perform slack space analysis. Slacker does use symmetric encryption measures to protect some of it’s data making this type of analysis harder.

# Installation

Installing slacker.exe is a fairly simple process. As a standalone executable, the only steps needed are to download the tool and browse to it’s directory using a command line too like PowerShell or cmd.exe. There are multiple places where this tool can be found on the internet, but I chose to download it from a repistory of forensic tools maintained on github by the user codejanus. You can find the repository containing slacker.exe at the following address: <https://github.com/codejanus/ToolSuite>

In order to ensure that there would be enough files on my virtual machines disk for Slacker to work properly, I first transferred over a number of pictures, documents, and music files from my own personal computer into the VM environment. I also installed several programs that would be typical on an average users PC, each of which would have created their own files on the disk.

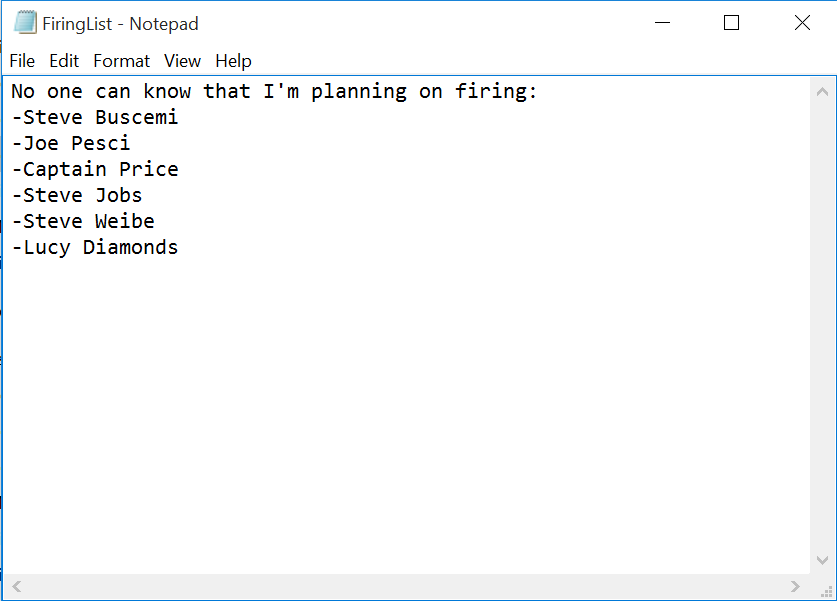
# Using Slacker.exe

Slacker has two basic modes of operation, one for writing files to slack space and another that reads the file back out form this space and saves it to a user specified location on disk. As a command line tool, it has no user interface and must be run using a tool such as PowerShell or cmd.exe as previously mentioned.

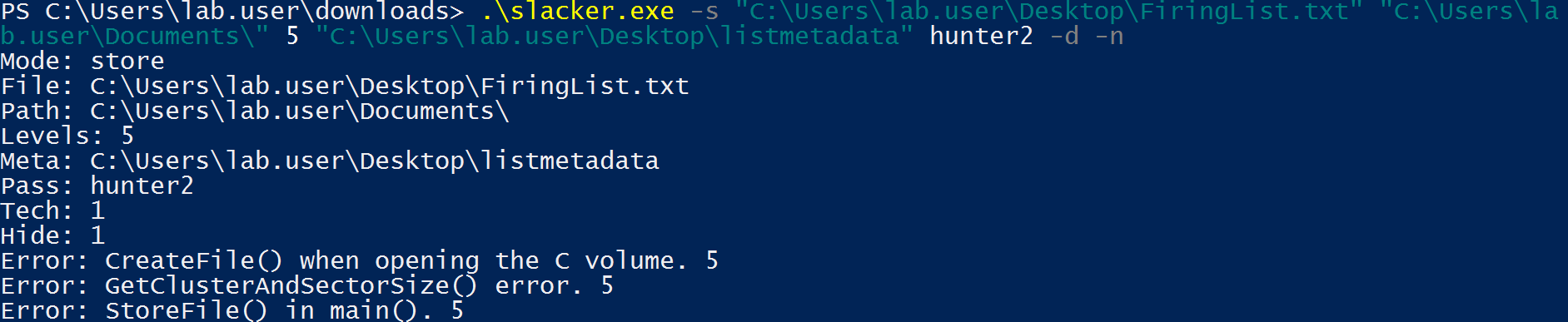
*Fig. 1. The Man Page for Slacker.exe*

The basic procedure for using slacker is to first run the command using the -s argument. This allows you to specify a file to be hidden, the root directory whose slack space you want to have the file stored, where the file storing the metadata needed to retrieve this file should be kept, a password to protect this file, as well as some options regarding how slacker should attempt to utilize the slack space that it has available. Once you have written a file using this method, you simply call slacker with the -r argument, allowing you to specify which metadata file you want to use to retrieve the data, the password associated with that file, and the location where you want the file to be saved.

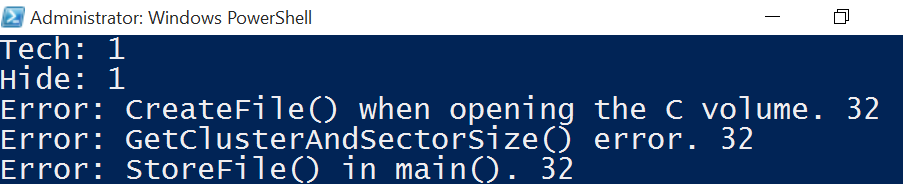
For this reason, the investigation process for this tool at this moment will be relatively short. I am still waiting to receive access to proper forensics tools from Champlain College professors, and as such cannot perform the slack space analysis that would be required to understand the difference between the various options provided. Without any ability to view the slack space there is no way for me to know what the difference between “Dumb” and “Intelligent” slack space selection looks like. I will return to this evaluation once access to those tools has been granted.

I began by choosing what file I wanted to hide. Given the limited amount of free slack space likely available on this PC, I instead decided to hide a text file containing a fake list of employees in the company who I planned to fire. I called this file “FiringList.txt”

*Fig. 2. The contents of FiringList.txt before being stored in slack space.*

With the file created, the next step was to store it in the Slack Space. I created the file on the desktop so that I could attempt to store it within the slack space of the files within the Documents folder on the PC. My first attempt at performing this procedure used the command shown below, resulting in an error where slacker was unable to access files on the C:\ volume

*Fig. 3. The first slacker command attempted along with the resulting error message*

After receiving this error I figured that slacker may require to have administrator permissions in order to run. I restarted my PowerShell session as an administrator, and attempted to run the same command again. I received the same error.

*Fig. 4. The same error message displayed in an administrator powershell window*

Troubleshooting on the web mentioned that this error could occur in cases where the folders in question had been set to read only. Curious to see if that was the case, I checked the properties of both the Desktop and Documents folder to find that the “Read-Only” flag had been set to on for both folders. After toggling these off, I attempted to run the command again and again received the same error. I also attempted to run the program targeting the root C:\ folder as the target for slack space, thinking maybe there was just not enough available for the tool to work. Again, I received an error. I then considered that this may be an issue caused by the nature of VMWare’s virtual hard disk system. For this reason, I attempted to run Slacker on my own personal desktop system. I ran into the same errors there, even after setting both my desktop and documents folder to be not read only and running the command as an administrator.

Further investigation showed that it was impossible to toggle folders to read only within Windows 10. This was likely due to some security feature within the operating system. I attempted to remediate the problem using several different trouble shooting steps, including removing the “SYSTEM” user as a folder owner, disabling Microsoft’s folder protection, and making myself the owner of the entire C:\ drive to no avail. It seems likely that some step this tool performs has since been flagged as suspicious activity and is blocked by Microsoft in it’s most recent operating system. Further analysis is required.

# Conclusions

While Slacker seems like it would be an interesting and useful tool, I was unable to get a working build of it to run either in my virtual windows 10 environment or on my live desktop PC. For this reason I will have to label it as impossible to complete for now until I can get access to a wider range of operating systems to test the tool on.