Submit

**Part 1 - Project**

1. Paste a **clickable**link to your public GitHub repo: <https://github.com/S541931/df-mod2-forensic-copy>
2. Tell us about your project: In this project we will be practicing the creation of forensically sound copies. To start I will create some evidence and place it in an Evidence Folder inside the GitHub Repository, df-mod2-forensic-copy Folder. Through a script ran in VS Codes PowerShell Terminal I collected the SHA256 Hash Values. After creating the Evidence, I then found the SHA256 Hash Values in VS Code PowerShell. Then I made a copy of the Evidence Folder in the Windows File Explorer. I then used the same method to find the SHA256 Hash Values of the copied files. I used the search(Ctrl + F) in the files to guarantee the Hash Values match.
3. About how long did you spend on this module: About 5 to 6 Hours.
4. In general, how did it go: Well, I had no issues on the Project.
5. What was the most difficult part: It’s not a part of this module but I’m slightly worried about automation with PowerShell, I think I’ll research it a bit before next week.
6. What was most interesting: I found the Hash Values really interesting, so I researched them beyond the book before the Discussion.
7. Did you do the optional bonus (y/n). How did it go - or why not? No, I did not adjust the 001 case script to reduce manual work.

**Part 2 - Self Assessment**

From the Module Overview, paste the numbered list of module objectives and assess your ability on each as "Highly proficient", "Proficient", or "Not Proficient":

Module Objectives:

* 1. Describe how to acquire and preserve digital evidence using free tools. L01, L02: Proficient.
  2. Describe how to verify the integrity of forensic evidence using hashing techniques. L01, L02: Highly proficient.
  3. Demonstrate hashing techniques to replicate and verify evidence files. L03, L05: Highly proficient.