**Project #1 Grading Rubric:**

The grading rubric that will be used to grade each disk image will be based on the following criteria:

|  |  |  |
| --- | --- | --- |
| Activity | % | Points |
| Number and type of partitions specified? | 5% | 10 |
| File status, filename, extension, attributes, and file sizes specified? | 10% | 19 |
| Was the byte offset for each file specified? | 15% | 30 |
| Was a File Allocation Table provided? | 10% | 20 |
| Were all files recovered from each partition? | 25% | 50 |
| Where hiding methods specified? | 15% | 30 |
| Describe what tools or applications were used to hide data | 5% | 10 |
| Describe the ultimate objective of users of the laptop | 5% | 9 |
| Describe the process used to find malicious content in the Lure challenge | 10% | 19 |
|  | 100% | 197 |

Note: Excellent work! You recovered all the files and provided a very thorough analysis of the partitions, provided the techniques and tools that were used to hide data. I would only add more details on the heist (When and where did the malicious actors were to meet). This information can be found in the recovered Plan table (You are supposed to change the extension to the xls to see to content). Also, the file from the Lure challenge is rather to be called malicious because of the suspicious activity. The count number for Mystery.zip file is 258, not 640.