## Questions:

Answer the questions below using xxd (or other hex viewer only), dd, file and stat commands. For each question, include a screenshot as appropriate. You are not to use automated tools for this assignment. We’ll do that later.

1. What is the physical size, MD5 and SHA-1 Hash of the partition? Answer the question and include a screenshot of the commands used and their output.
2. At what hexadecimal offset does the Volume Boot Record begin and what is the file system? Answer the question and include a screenshot showing this location in xxd.
3. At what hexadecimal offset does the first File Allocation Table begin? Answer the question and include a screenshot showing this location in xxd.
4. At what hexadecimal offset does the second File Allocation Table begin? Answer the question and include a screenshot showing this location in xxd.
5. At what hexadecimal offset does the root directory? Answer the question and include a screenshot showing this location in xxd.
6. How many files are on the partition (deleted or undeleted files)? How many are deleted? How can you tell they are deleted?
7. Complete the table below. List the file names, types, physical and logical sizes, and starting logical cluster below for each deleted file. For each file you are recovering, include a screenshot of xxd showing the root directory with the bytes highlighted that you are converting to determine the size of the file.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| File name | File Type | Logical Size | Physical Size | Starting Offset |
| file1.png | PNG | 73380 | 73728 | 0x4400 |
| ? | ? | ? | ? | 0x16400 |
| file3.jpg | JPG | 53996 | 54272 | 0x21600 |
| ? | ? | ? | ? | 0x2EA00 |
| file5.txt | Text file | 37591 | 37888 | 0x37200 |

1. Use dd to recover deleted files and sha1sum to hash the files only. Copy and paste the calculated hashes in the second column for the recovered files. The hashes for the allocated files have been provided for you along with the first four bytes of the deleted files so you can check your work.

|  |  |
| --- | --- |
| File name | Sha1 hash |
| file1.jpg | 98652815708b00e377043c6587c545e52cc42e50 |
| ? | f1a0 (the first four bytes)  |
| file3.jpg | d6b5b17969b086bf6a329fbb1dc1a5b54c468785 |
| ? | 00ba (the first four bytes) |
| file5.txt | 0b4290da0b0b7d4d9babce8bf76bf9900f9247bd |

1. Why are there two entries in the root directory for each file? Be specific in your answer. This should not be answered with just a sentence or two.
2. Why is the physical size of a file usually greater than or equal to the logical size of the file? Be specific in your answer. This should not be answered with just a sentence or two.
3. Open the files you recovered and Include screen shots of their content below. You should be able to resize them in Word.

## <INSERT YOUR IMAGES HERE>