**Question #1: *What are the sizes of the files you created? Fill out the below table with this data.***

|  |  |  |
| --- | --- | --- |
| **File name** | **File content** | **File size (bytes)** |
| file1 | First file created | 19 |
| file2 | Second file created | 20 |
| file3 | Third file | 11 |

**Question #2: *Fill out the below table with any output the strings command provides. (Some of the table is filled out for you.)***

|  |  |
| --- | --- |
| **Offset** | **String** |
| 6034 | file1 |
| 6044 | file2 |
| 6054 | file3 |
| 9800 | First file created |
| 9c00 | Second file created |
| A000 | Third file |
|  |  |
|  |  |
|  |  |

**Question #3: *Fill out the below table with the data found in the disk image, with the offset of each piece of data.***

|  |  |
| --- | --- |
| **Offset** | **String** |
| 6034 | File1 |
| 6044 | File2 |
| 6054 | File3 |
| 9800 | First file created |
| 9c00 | Second file created |
| A000 | Third file |
|  |  |
|  |  |
|  |  |

**Question #4: *What do you observe? Is this what you expected to see? What security problems, if any, are implied by your observations?***

|  |
| --- |
| None of the files were missing, including File2 which is what I removed in the previous step. I definitely did not expect that to happen I thought the table wouldn’t have File2 and file3 would take the offset (6044). I would be concerned that if I deleted a file that another hostile actor could find a file that I didn’t think existed anymore. |

**Question #5: *What is the decimal offset into the disk, to the point where*** file2 ***begins?***

|  |
| --- |
| 39936 |

**Question #6: *Were you able to restore the file?***

|  |
| --- |
| Yes the contents of rfile2 contained “Second file created” |

**Question #7: *What do you observe? Fill out the below table with the output of the strings command.***

|  |  |
| --- | --- |
| **Offset** | **String** |
| 6034 | File1 |
| 6044 | 0000 |
| 6054 | 00003 |
| 9800 | First file created |
| 9c00 | Second file created |
|  |  |
|  |  |
|  |  |
|  |  |

**Question #8: *What do you observe? Fill out the below table with the output of the above command.***

|  |  |
| --- | --- |
| **Offset** | **String** |
| 14168 | First file created |
| 14568 | Second file created |
|  |  |

**Question #9: *Which inode number was associated with file1? Which inode number was associated with file3?***

**File1: *64***

**File3: *66***

**Question #10*: Try to recover file3 and compare with the results from your attempt to recover file1.***

|  |
| --- |
| When undeleting it refers to the file as ‘0’ where as when restoring the file1 it said ‘file1’ there are also no results when you try to ‘cat rfile3’ |

**Question #11*: Go back to some steps in this lab and experiment. Try to do something differently, or otherwise explore. Explain what you did here:***

|  |
| --- |
| I went back and tried to shred a file that was already removed using rm then restored. It didn’t seem to affect the recoverability of the file after it had been shredded the second time. One thing I was wondering is how I could get files from my myfs.img mount onto the ntfs.img to “break” it, but I didn’t have any luck with that. |