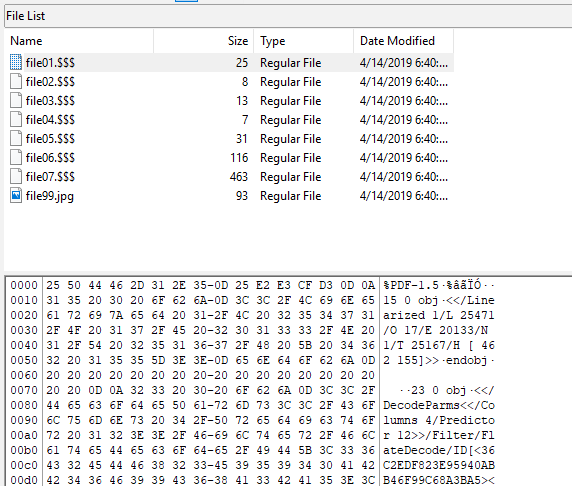
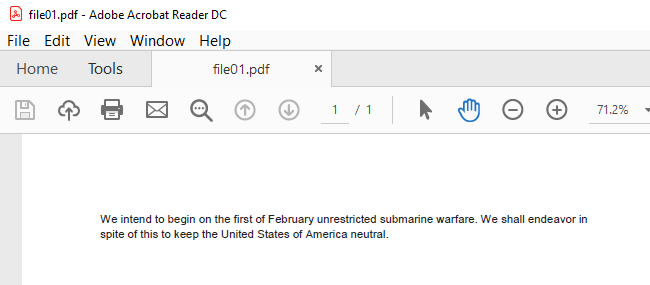
**Report for Lab – Forensics**

Lu Lin, Columbus State University

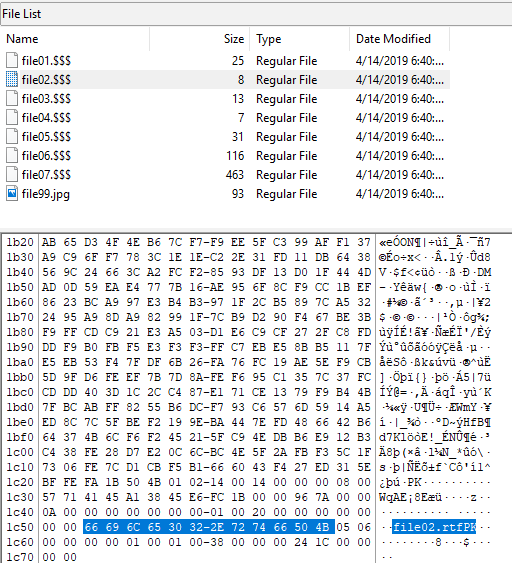
At the very first of this lab assignment, I download and unzip the given m4-file00 file, and then inspect file01 to file 07 through FTK Imager under Hex View.

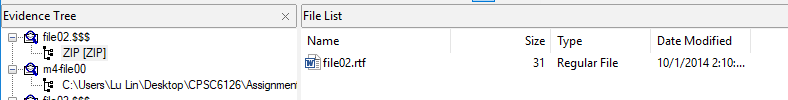
1. As we can see, file01 is a PDF file, it is recovered as follows:

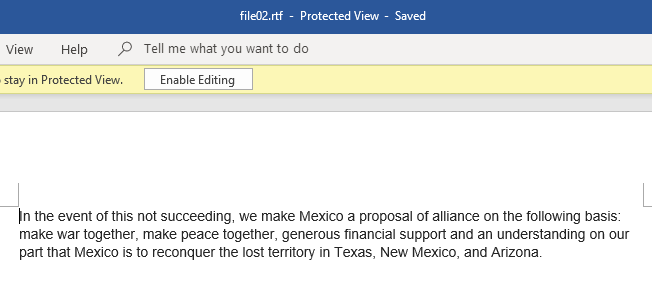




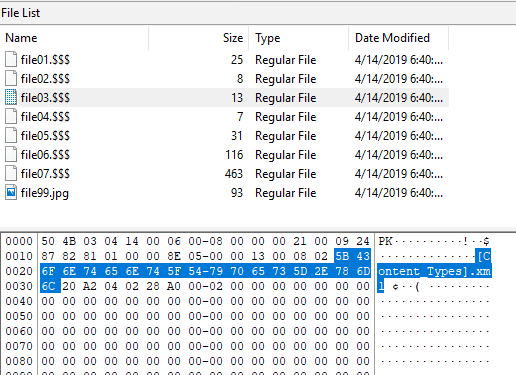
1. From Hex info file02 may contain some rtf file; after covering I find out it is file02.zip which contains one file: file02.rtf

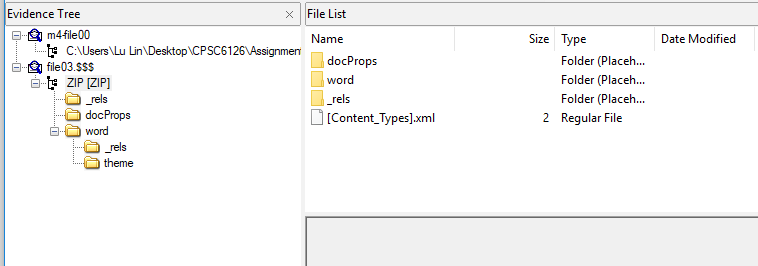




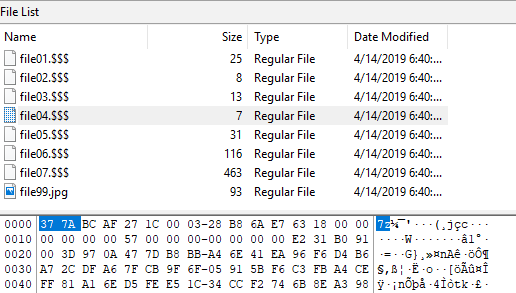


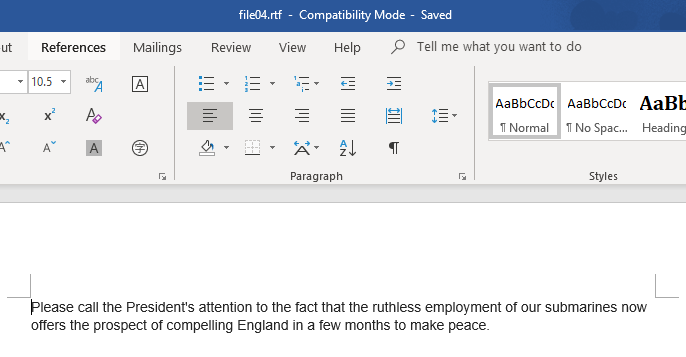
1. Similarly, the third file is file03.zip, which contains the following xml files:



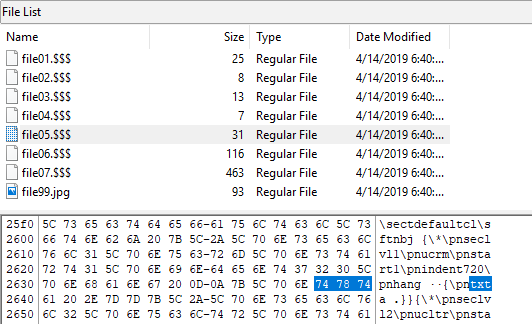


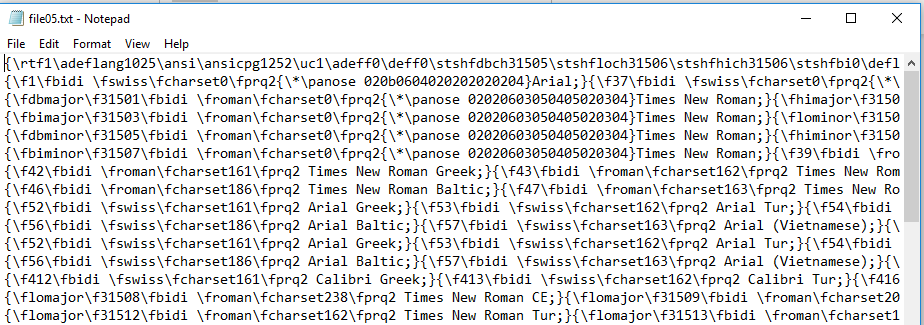
1. The fourth file is file04.7z, which contains file04.rtf as follows:



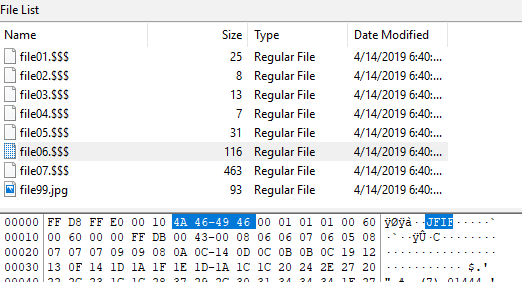


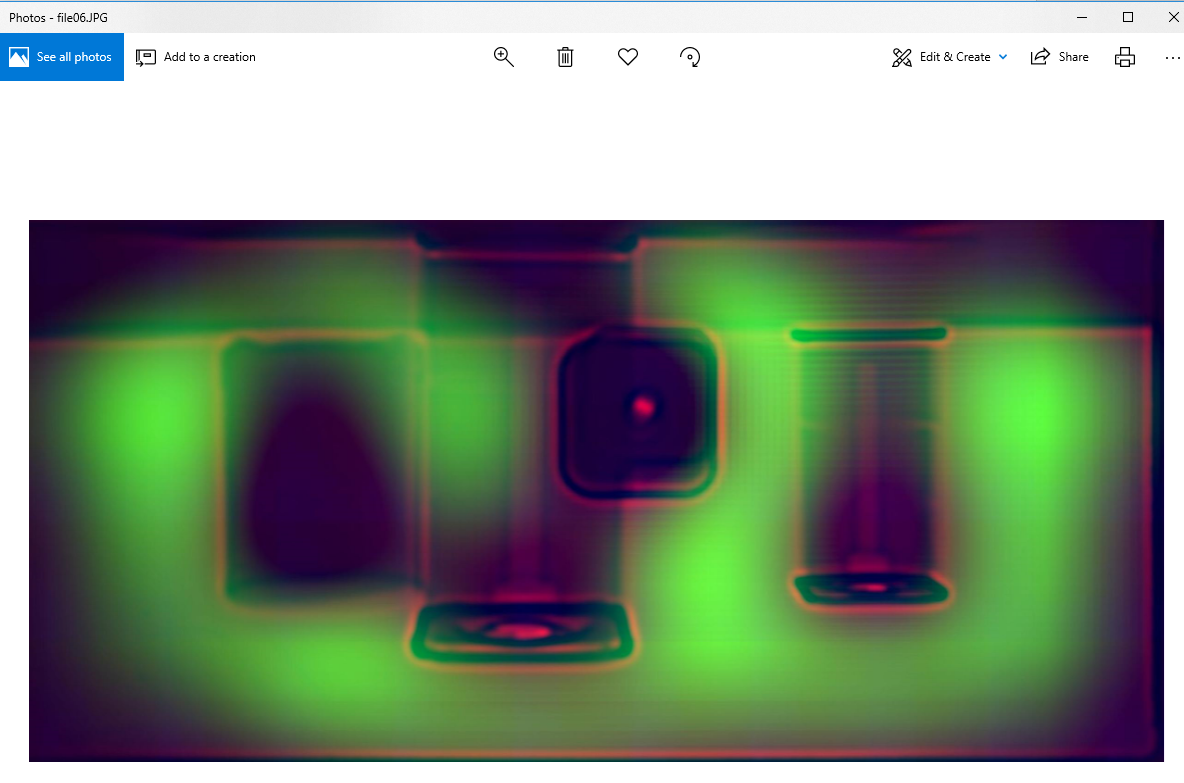
1. The fifth file is file05.txt, its content is as follows:



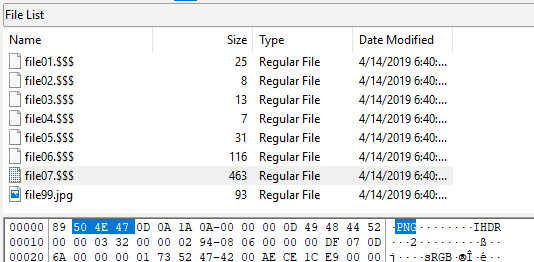


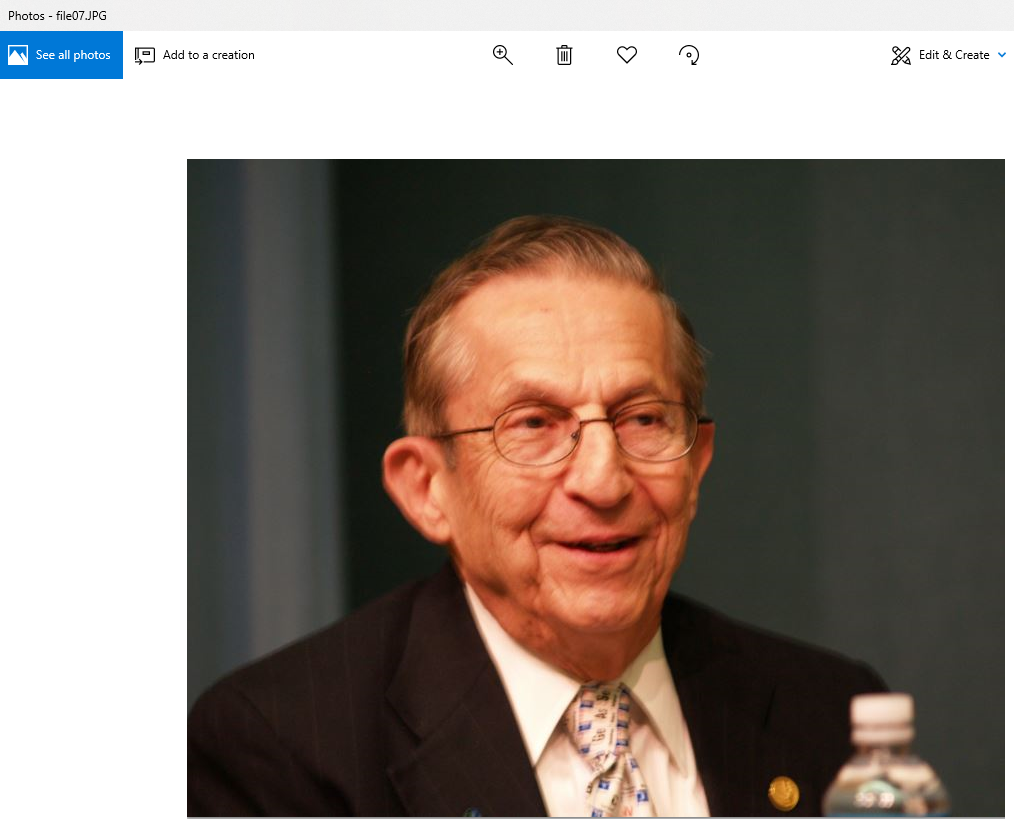
1. The sixth file is file06.JPG as following:



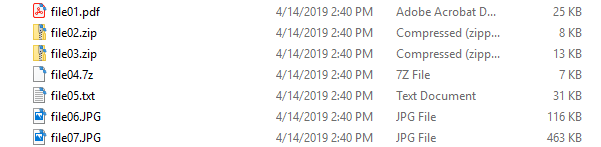


1. The seventh file is file07.JPG:





1. To sum up, the file01-07 are listed as follows:



1. As for file99.jpg, through inspecting the Hex info, I realize there is hidden file/files. After recovering, I find out it is file99.rar, and file99.rar contains one file: secret.txt, its content is as following:

