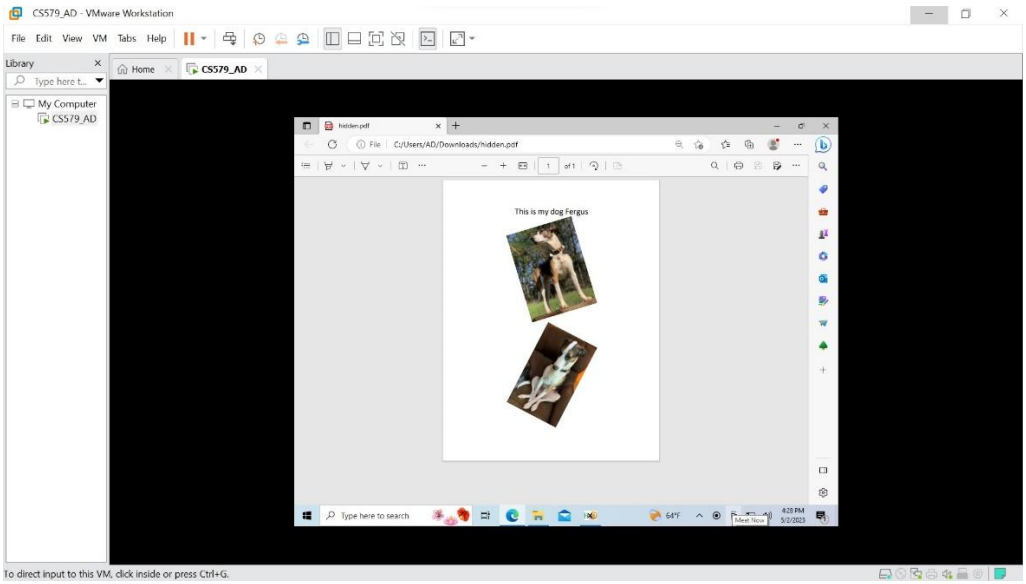
Fergus File Carving

The displayed image taken from canvas or box was as follows:

The hidden file was as follows:

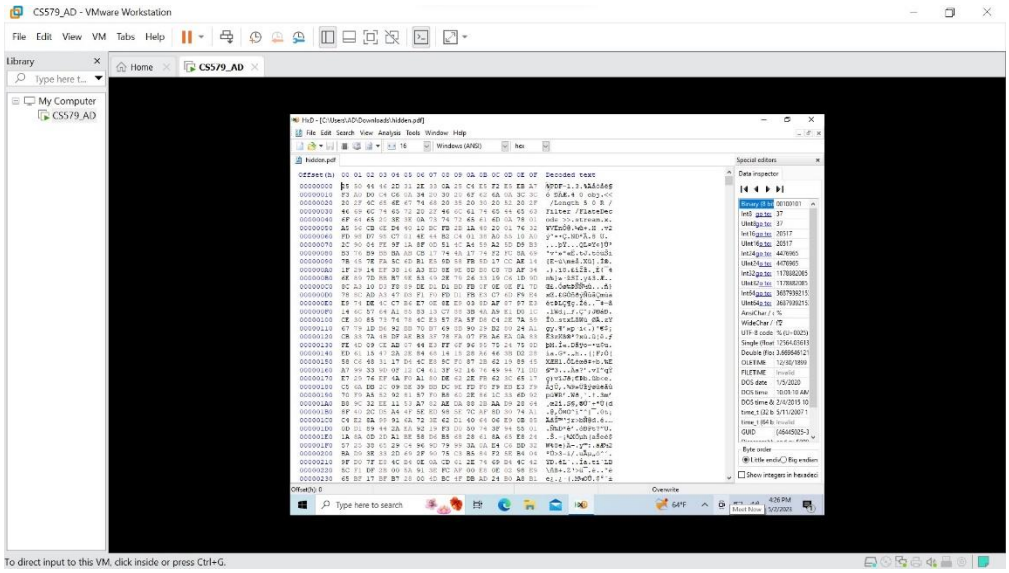


We downloaded the display image from Canvas and opened the HxD Hex Editor to view the Hex value of the display image. According to Gary Kessler's File Signatures Table, we were able to find the headers and trailers for a “JPEG” file which were “FF D8” and “FF D9” respectively.

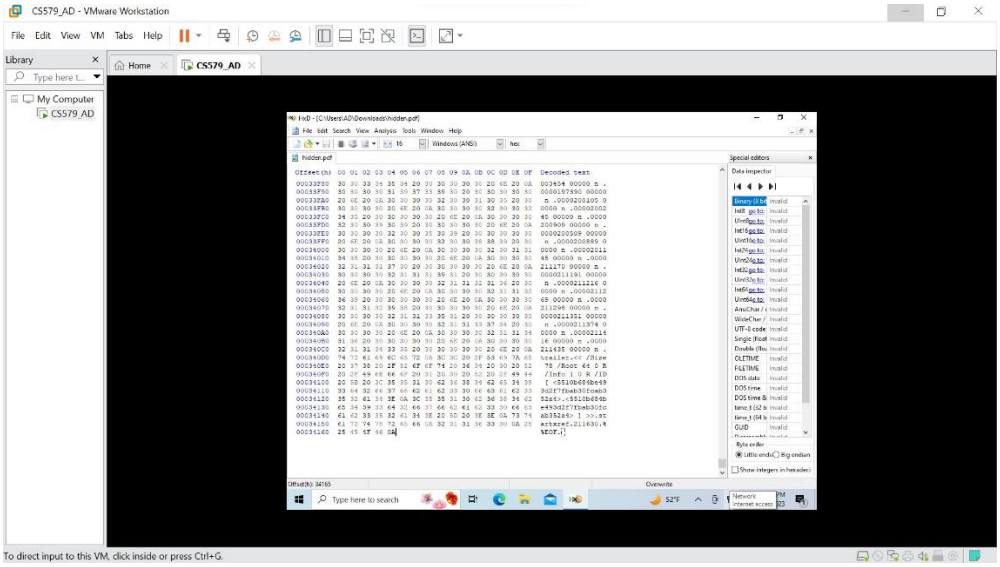
Moving ahead, we searched for those two hex values to match the start and end point of the display image. FF D8 was the first hex value for that image and FF D9 was located somewhere in middle of the hex values.

Upon checking the first instance of FF D9, we came to know about the presence of hidden files in the display image. So, we selected all the hex values after FF D9 till the end of that file and copied it in a new file.

Below is a screenshot of the hex value for the newly carved file:



Headers of Carved File



Trailers of Carved File

After viewing the hex values of the carved file, we began to examine its headers and trailers to determine the type of file extension that it consisted of. The header of that file was “25 50” and the trailer value was “0A 25 25 45 4F 46 0A”. We searched for these hex values in Gary Kessler's File Signatures Table and found out that it corresponded to a file with an extension “.pdf”.

We saved the copied hex values into a directory as a .pdf file. We opened the pdf file to view the carved output and reported the results. During this process we made a note of the file sizes of the display image and the carved output file which were 512 kb and 208 kb respectively.