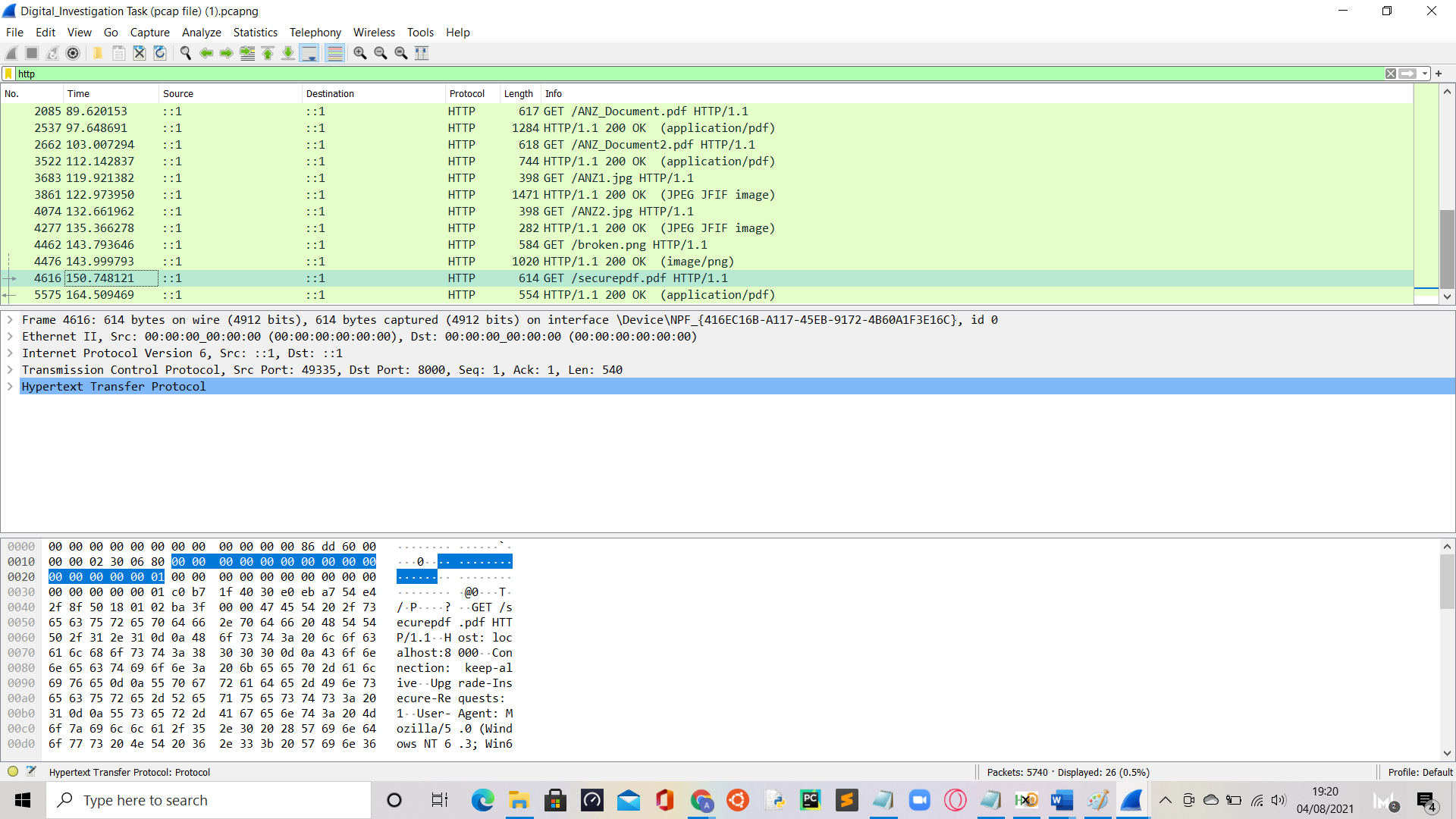
**Packet Capture Analysis:**

I have analysed the provided packet capture file using the free network analysis tool Wireshark.

I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.

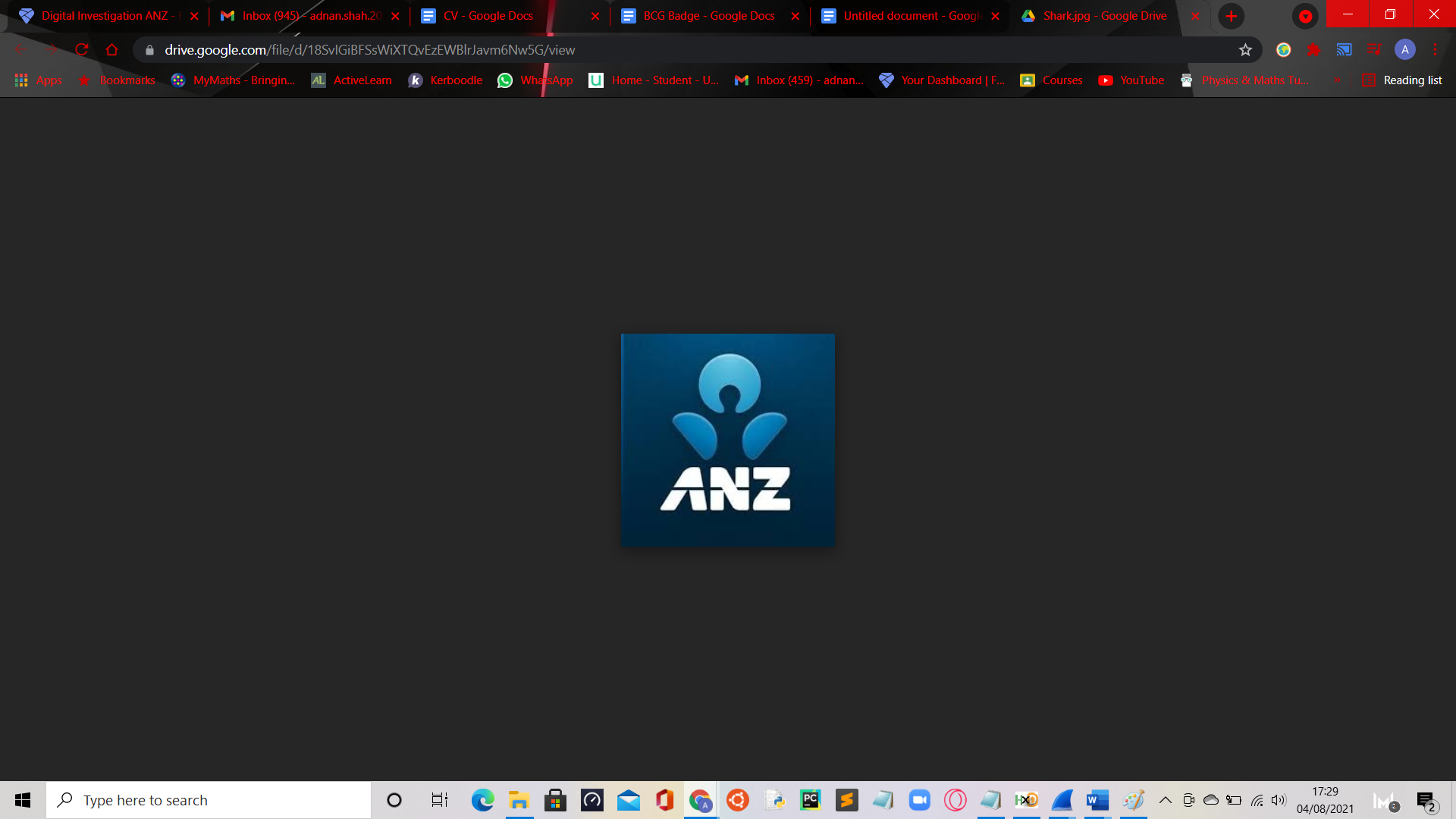
This view ;let me see some interesting ‘http GET requests, which indicate that the user specifically requests information, including one for hackers.jpg.



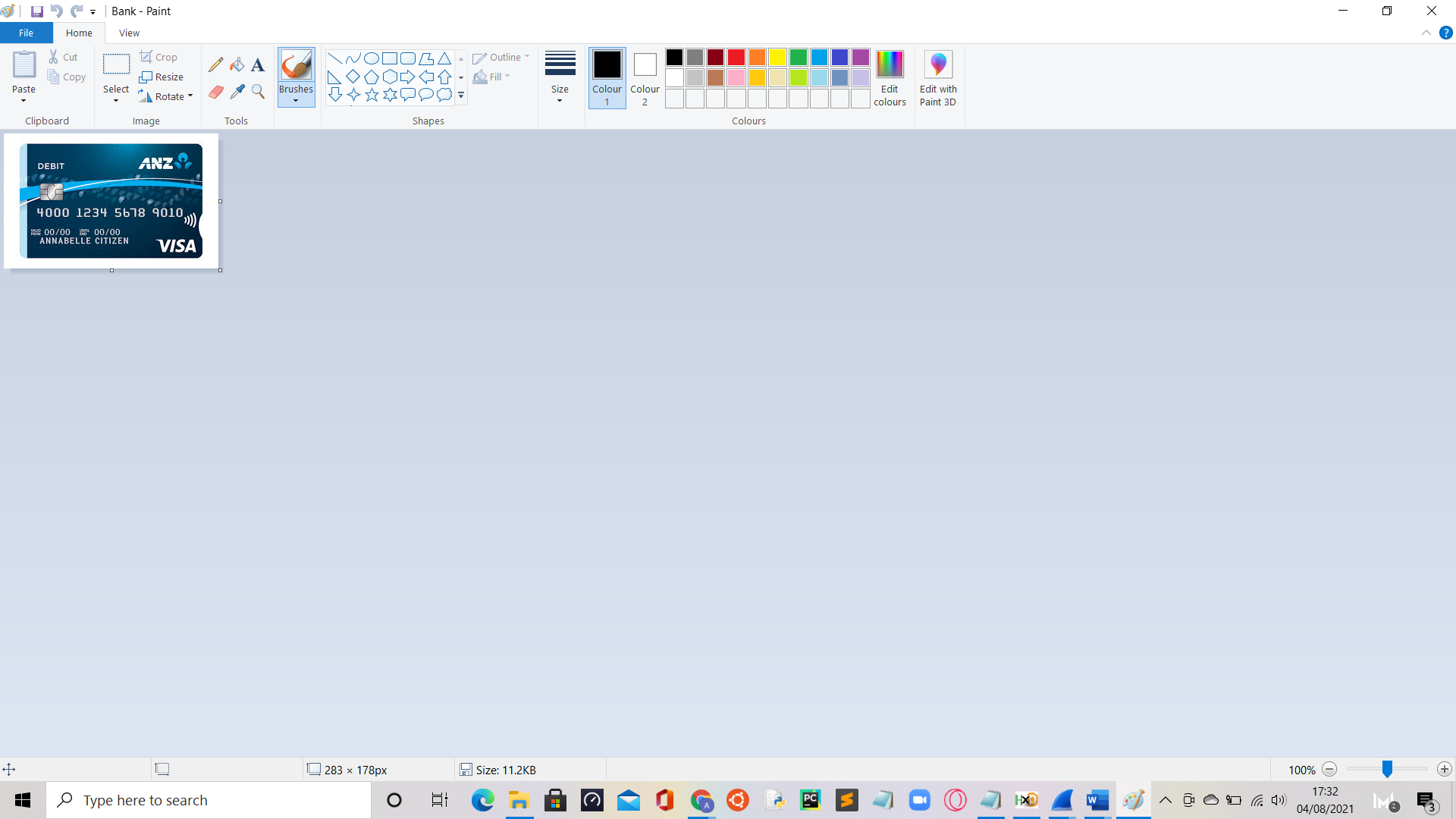
To investigate this image download further, I viewed its TCP stream to see what I could find. Looking through the data in the TCP stream showed that this get request actually downloaded 2 images, as the data contained 2 headers and 2 footers for a .jpg image. The header/footer is FFD8 - FFD9 in hex and the images are also recognizable in ASCII by the string ‘JFIF’ near the beginning.

**Sub-Task 1:**

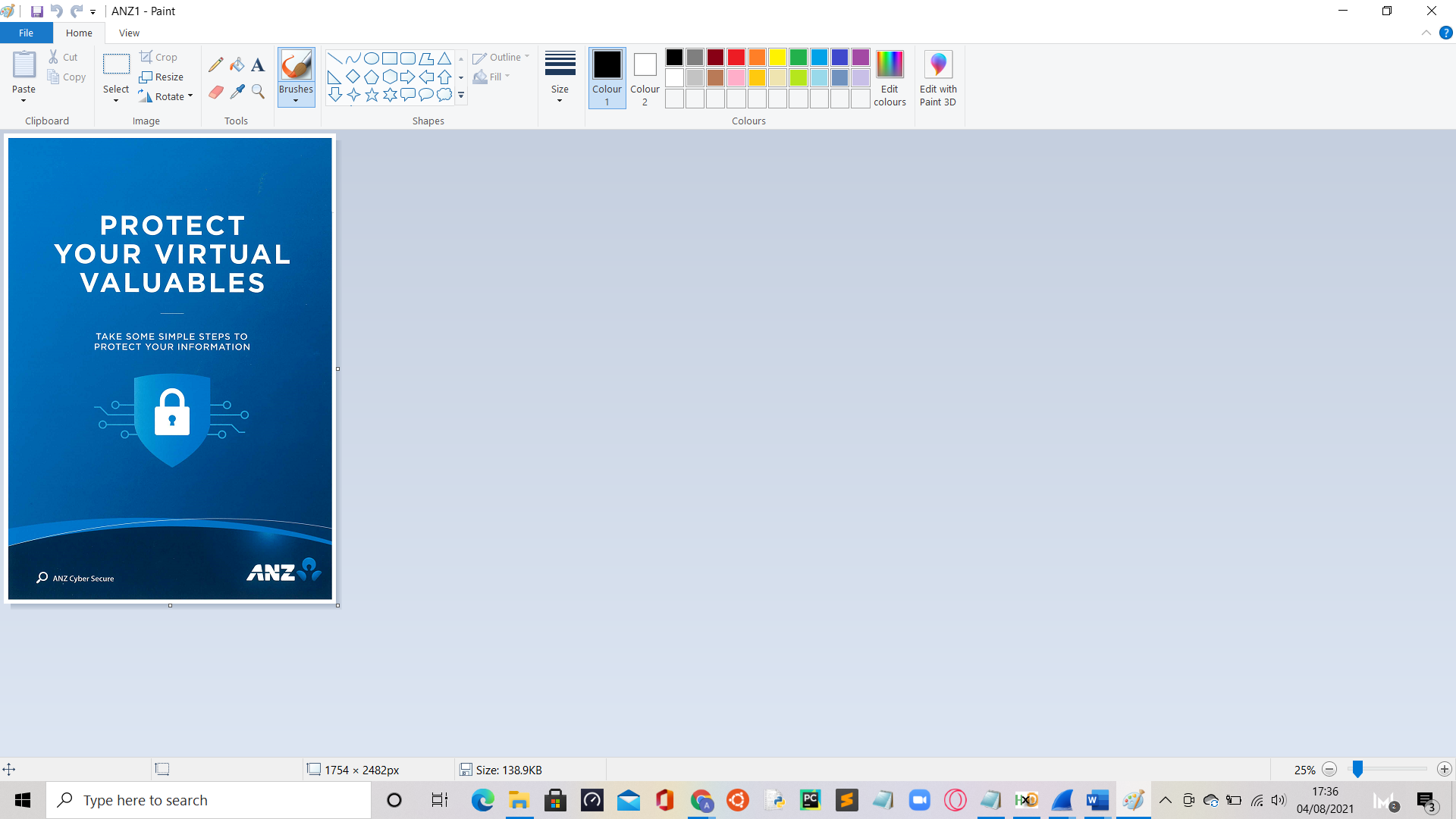
The next step taken was carving out the images from the tcp stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor HxD. I then saved the file as a jpg and opened it in the Paint software, resulting in the image below:

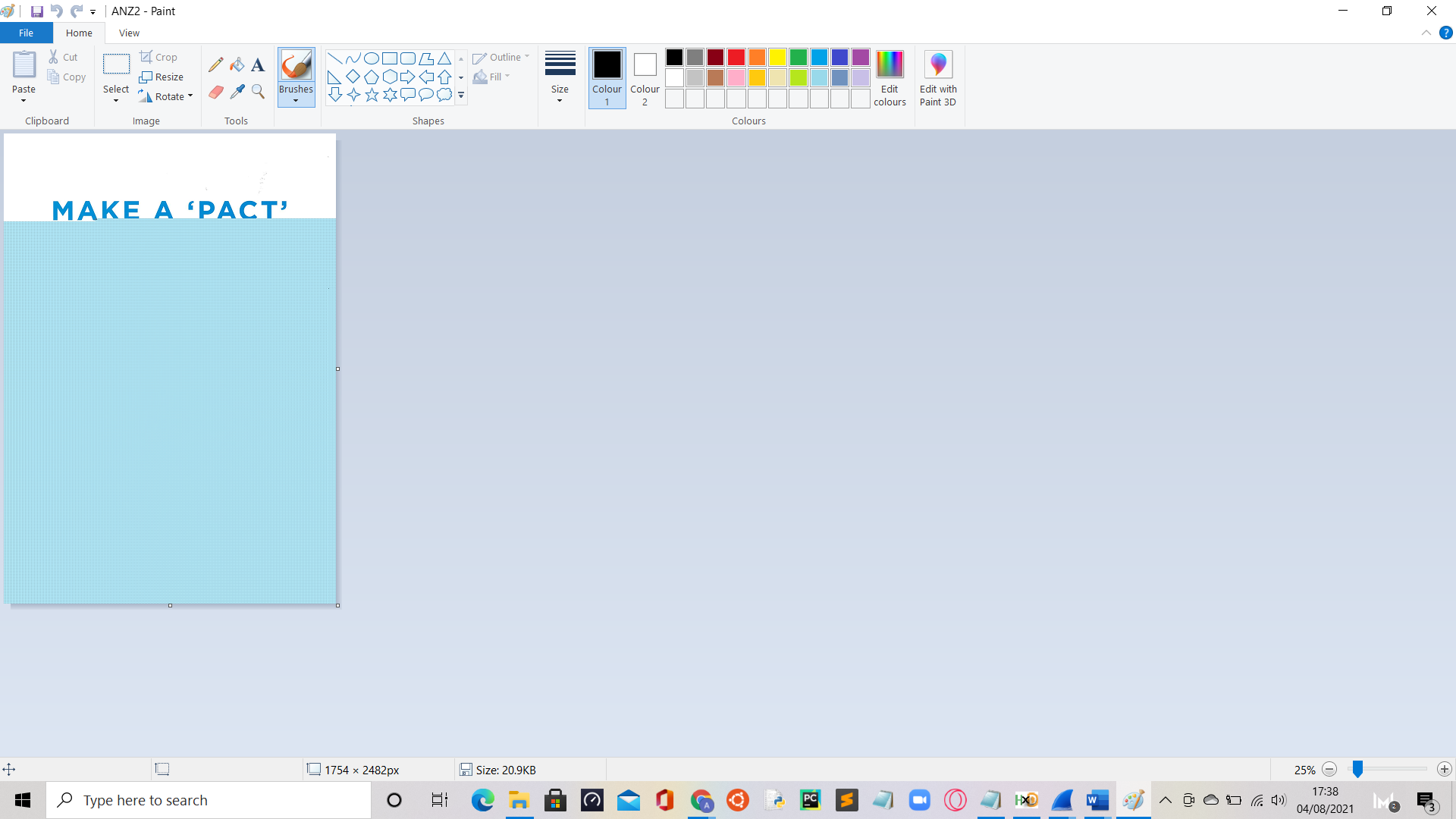


I followed the same process for the 2nd image

****

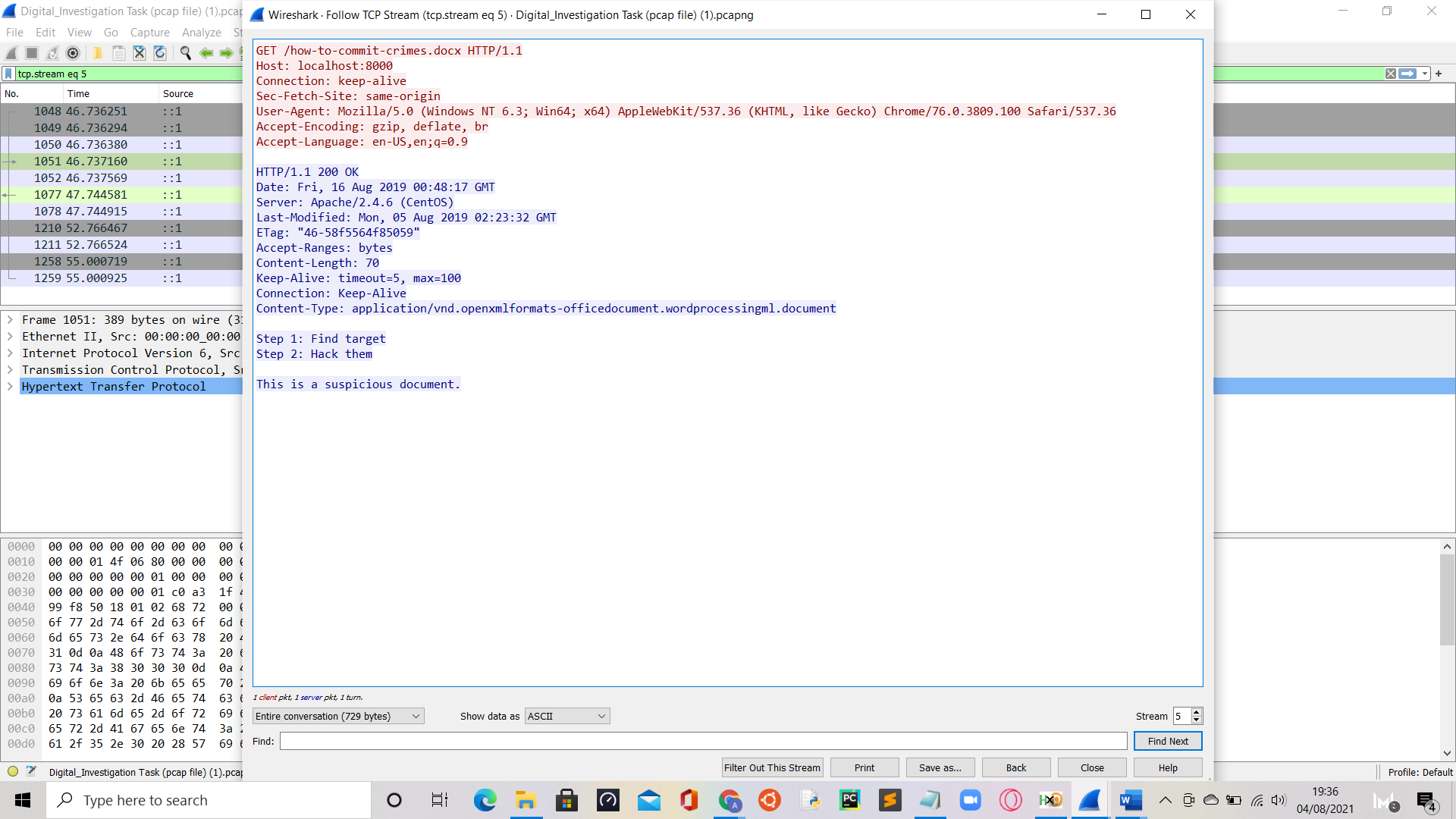
**Sub-Task 2:**

****

****

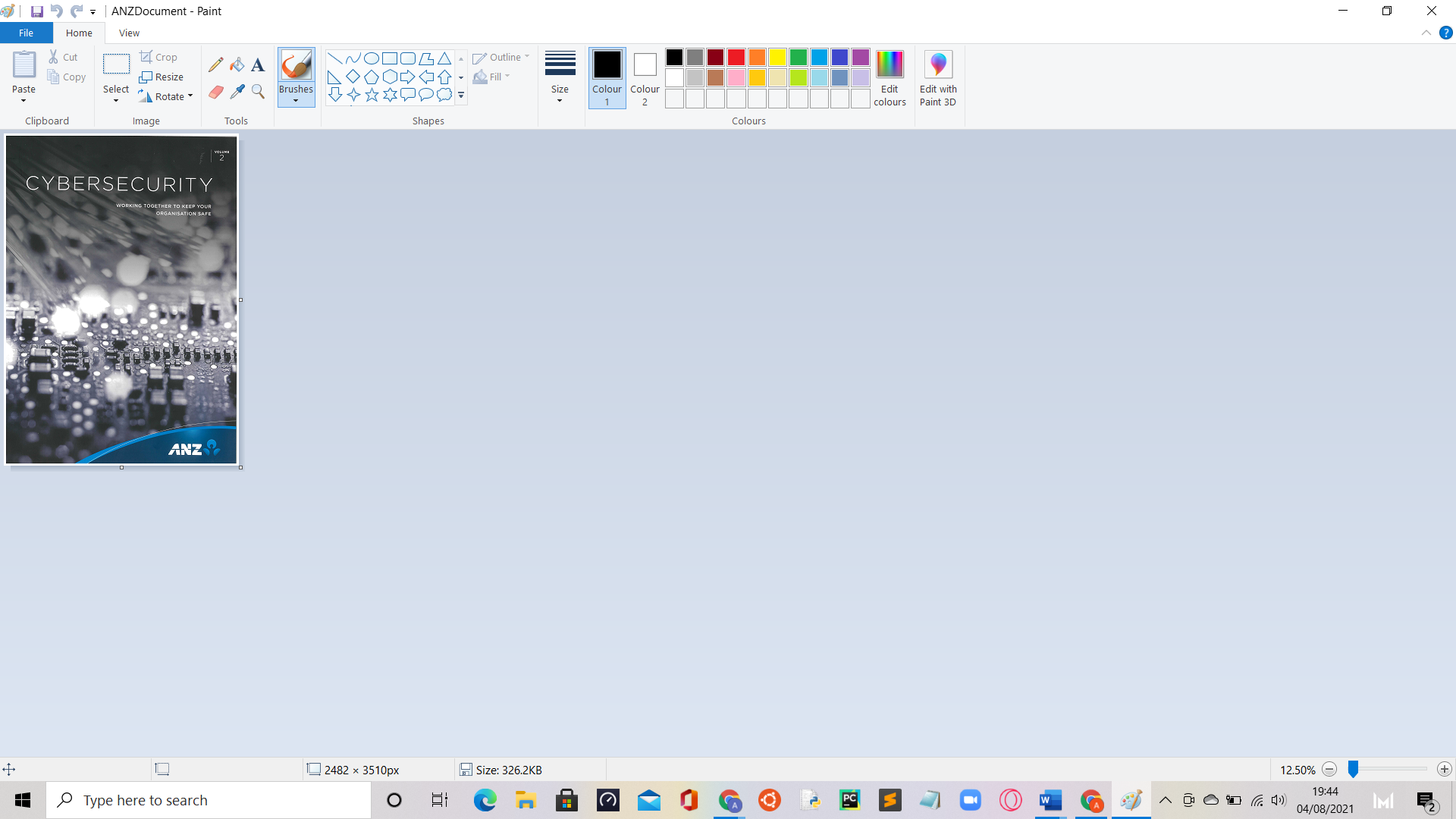
The 2nd image seems to be more covered than the 1st image. Two different posters, possibly related posters since the sentence ‘make a pact’ seems like a slogan for the @Anz company. However, the 2nd image seems like it has been corrupted.

**Sub-Task 3:**

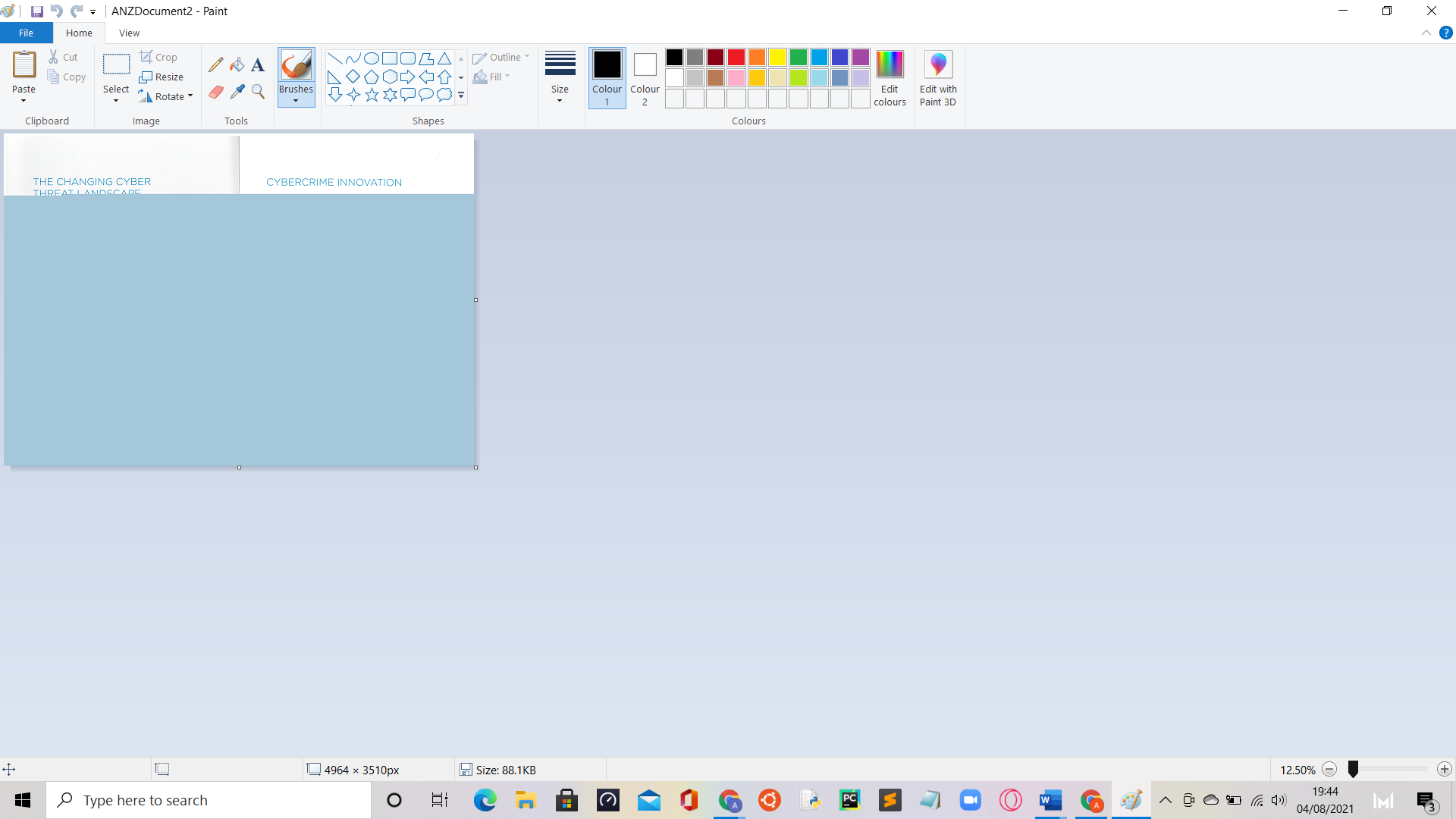


**Sub-Task 4:**

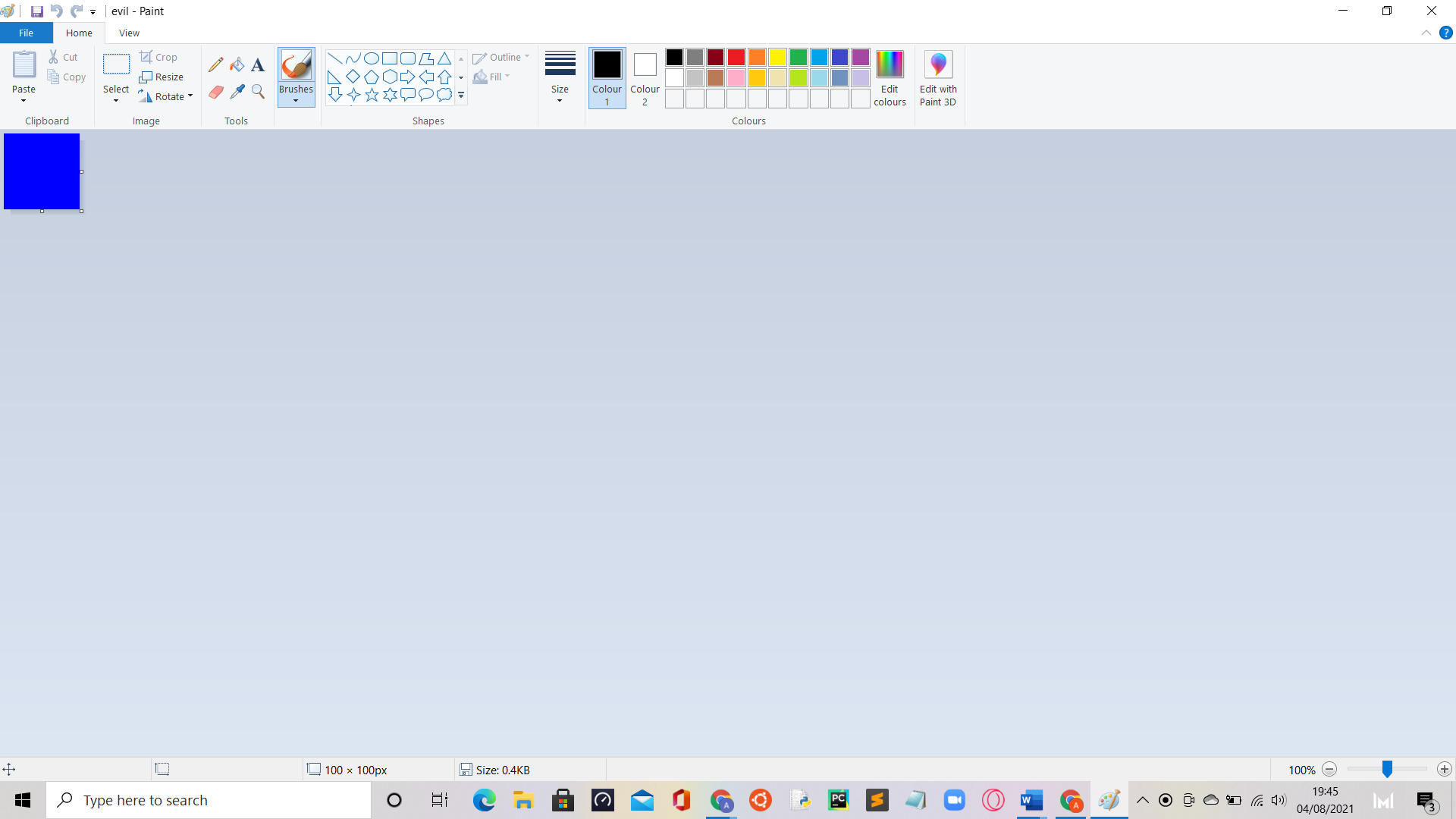
ANZDocument:



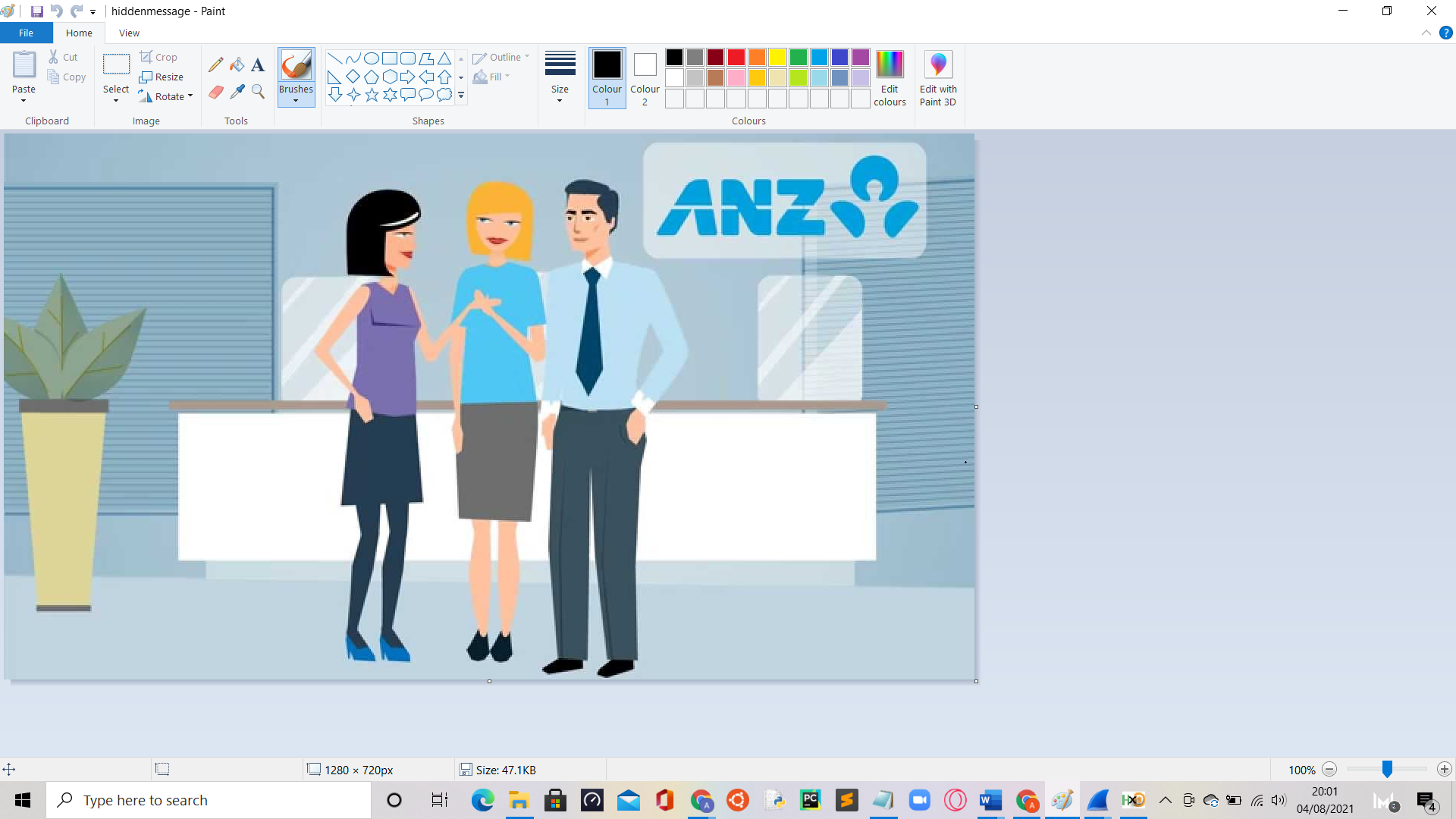
ANZDocument2:



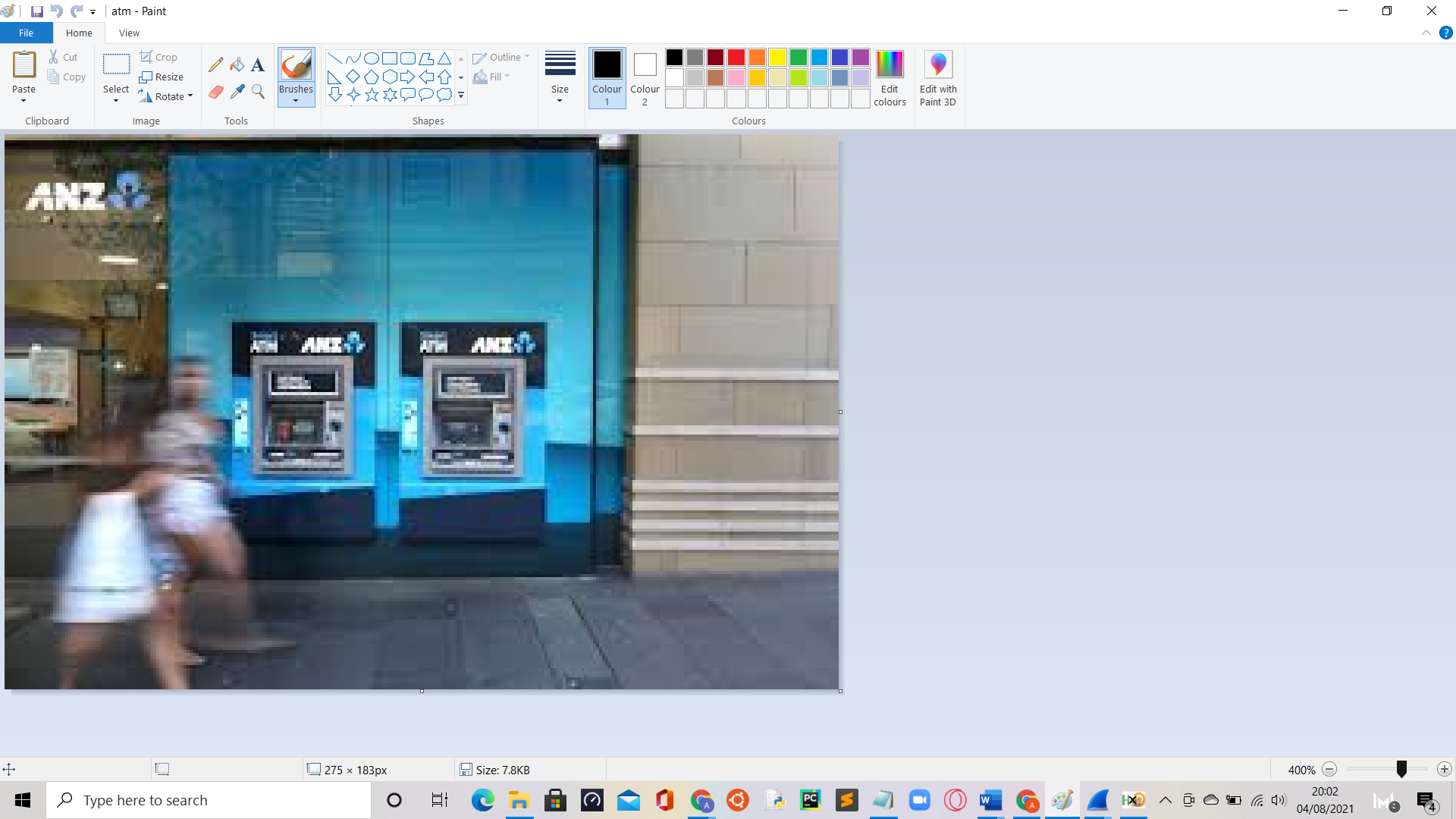
Evil:



**Sub-Task 5:**



**Sub-Task 6:**

****

This shows the atms at an Anz facility/bank location. This could be an attempt by hackers to steal the pin code of anz users.

**Sub-Task 7 & 8:**

The Broken.png could not be opened, as it is a corrupted file. The securepdf.pdf file can be opened, but unfortunately it’s encrypted, so I personally cannot open the file.