|  |
| --- |
|  |

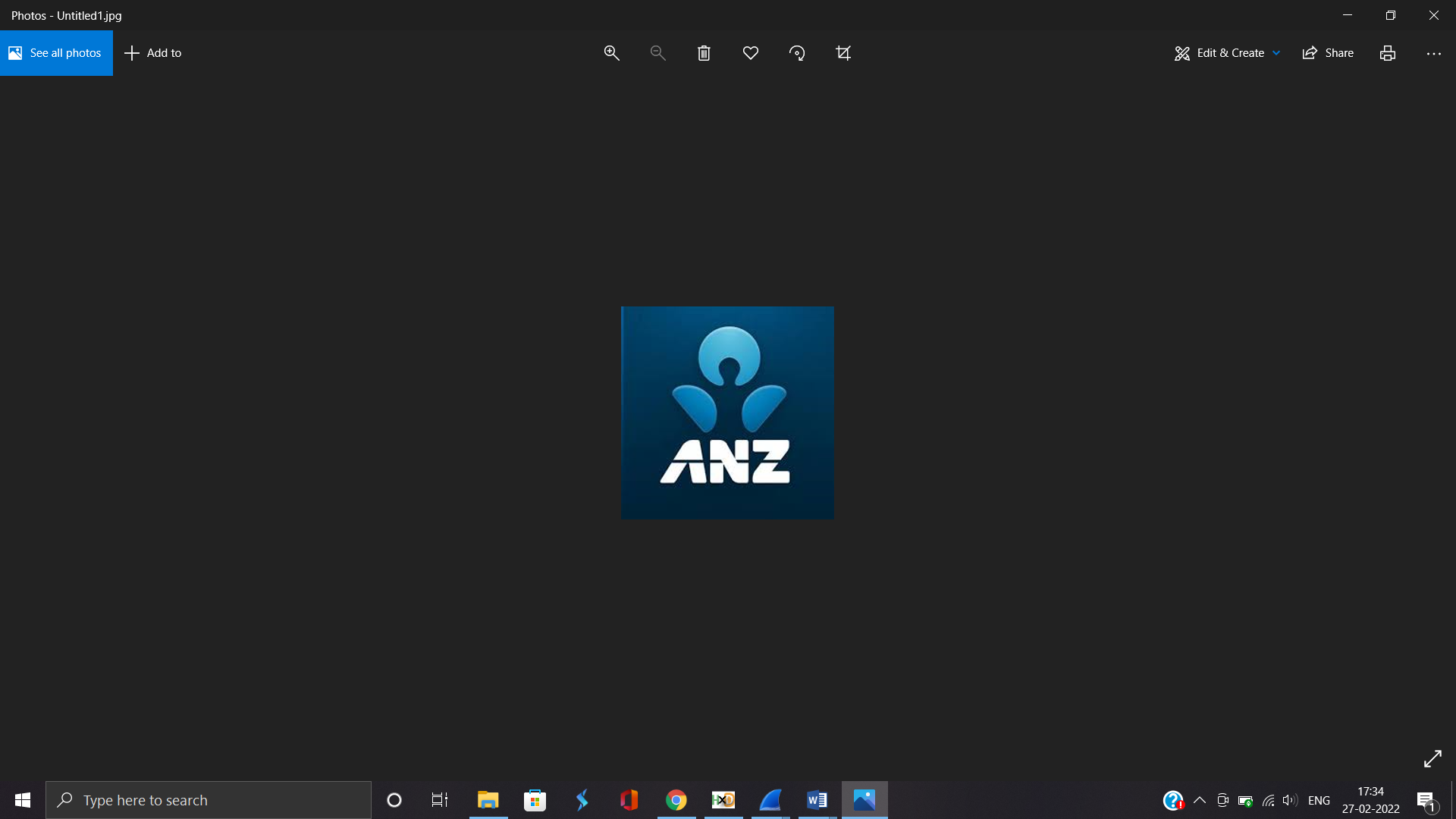
I have analyzed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.

**Sub-task 1:**

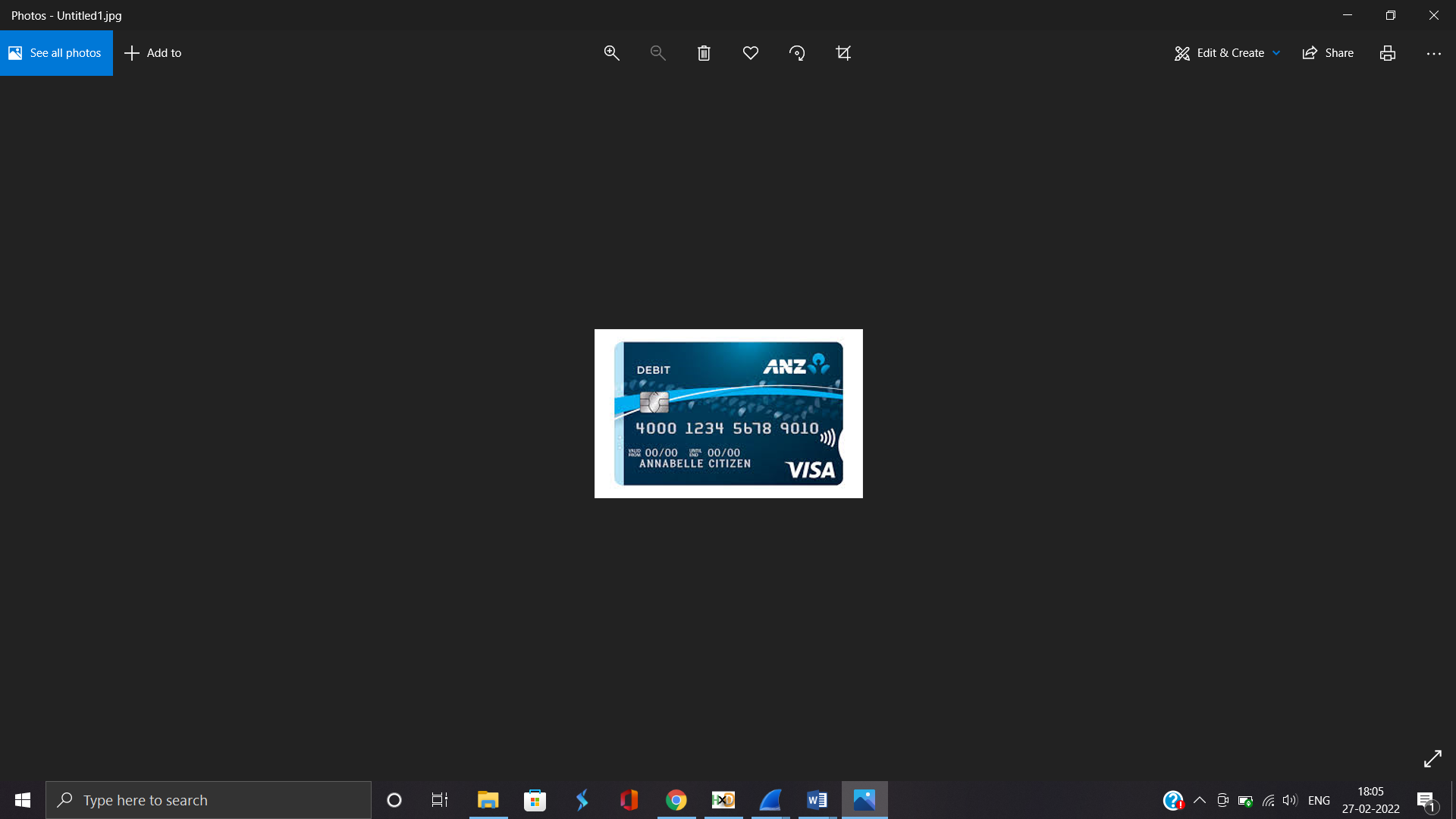
To find both images anz-logo.jpg and bank-card.jpg that show up in the user’s network traffic, we have to follow these steps-

* First of all, filter the packets using http.
* Then find the GET request of the images and then follow on TCP steam using right-click on the image.
* Then to look data of image in hex format, we have to choose to Show data as ‘Raw’.
* Then as we know signature of Jpg file is ddf8 and ddf9, we copied all the data in between those signature and then pasted it in HxD to save it as Jpg image resulting in the image.

*Bank-logo.jpg*



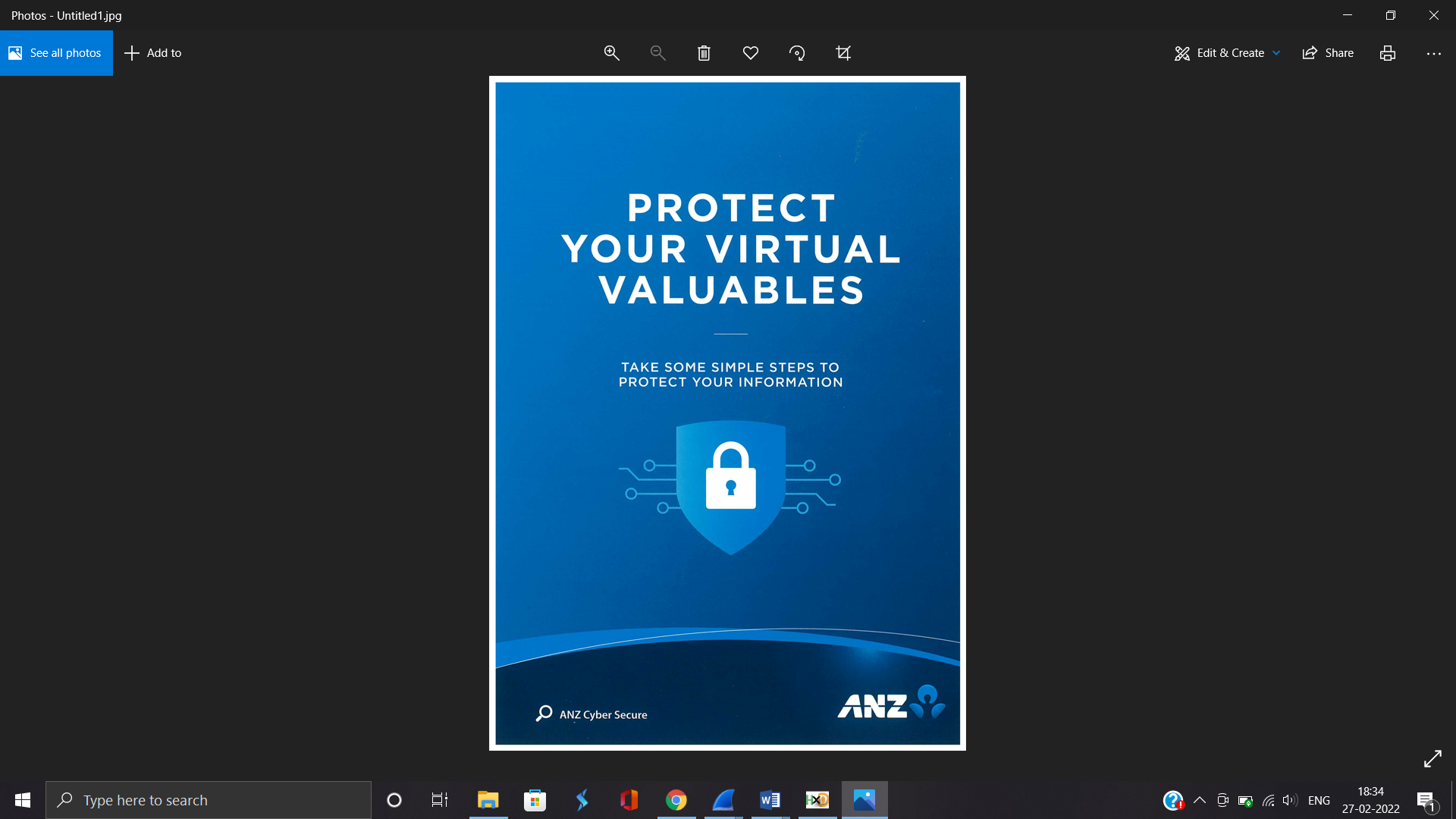
*Bank-card.jpg*



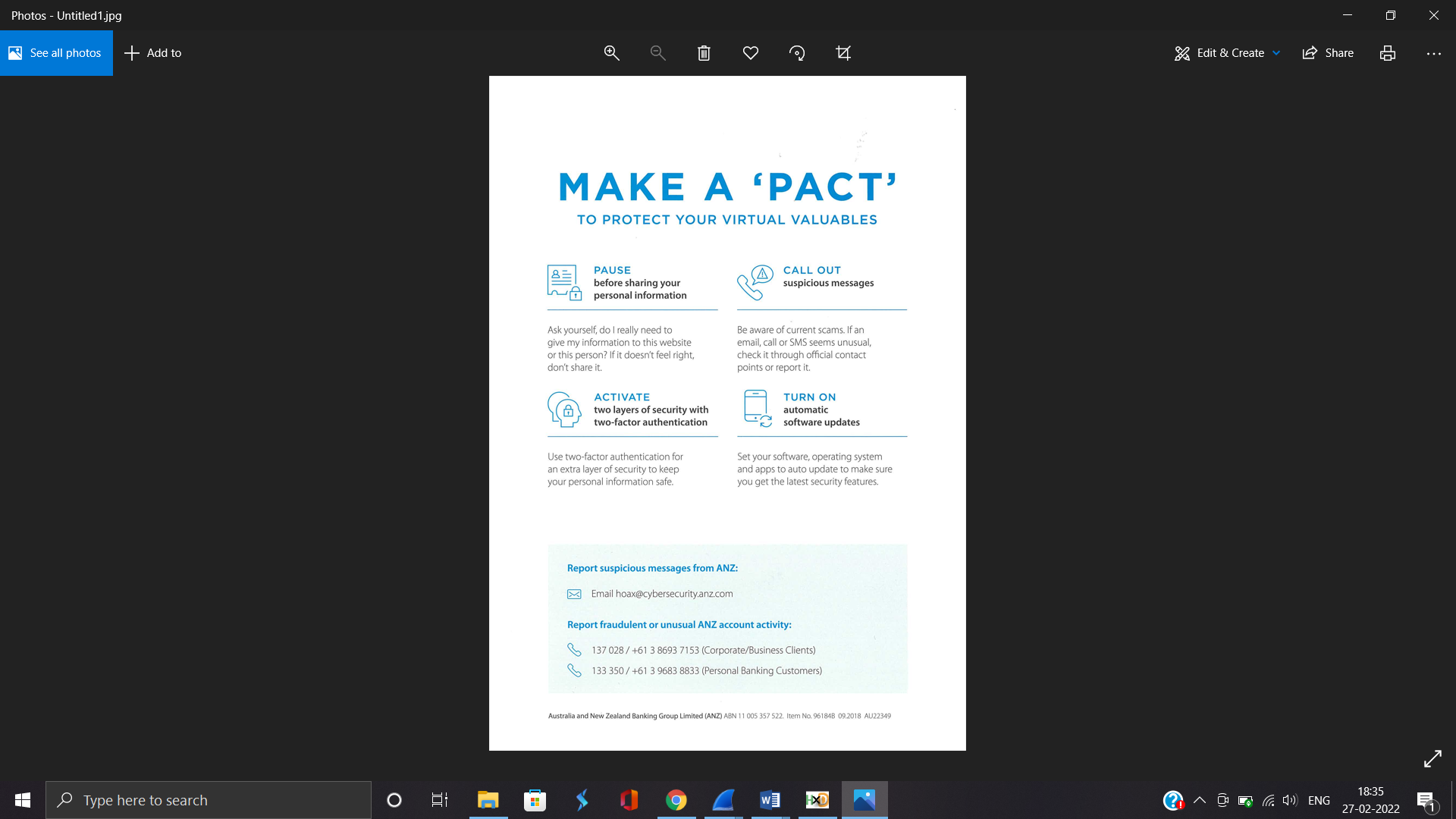
**Sub-task 2:**

* *Using the same above steps we are able to get these images i.e. follow tcp steam,raw,ddf8, copy and paste HxD ,save in jpg image.*
* *We found different messages after the images*

*ANZ1.img- “You’ve found a hidden message in this file! Include it in your write up.”*



*ANZ2.img- “You’ve found a hidden message in this file! Images are sometimes more than they appear.”*



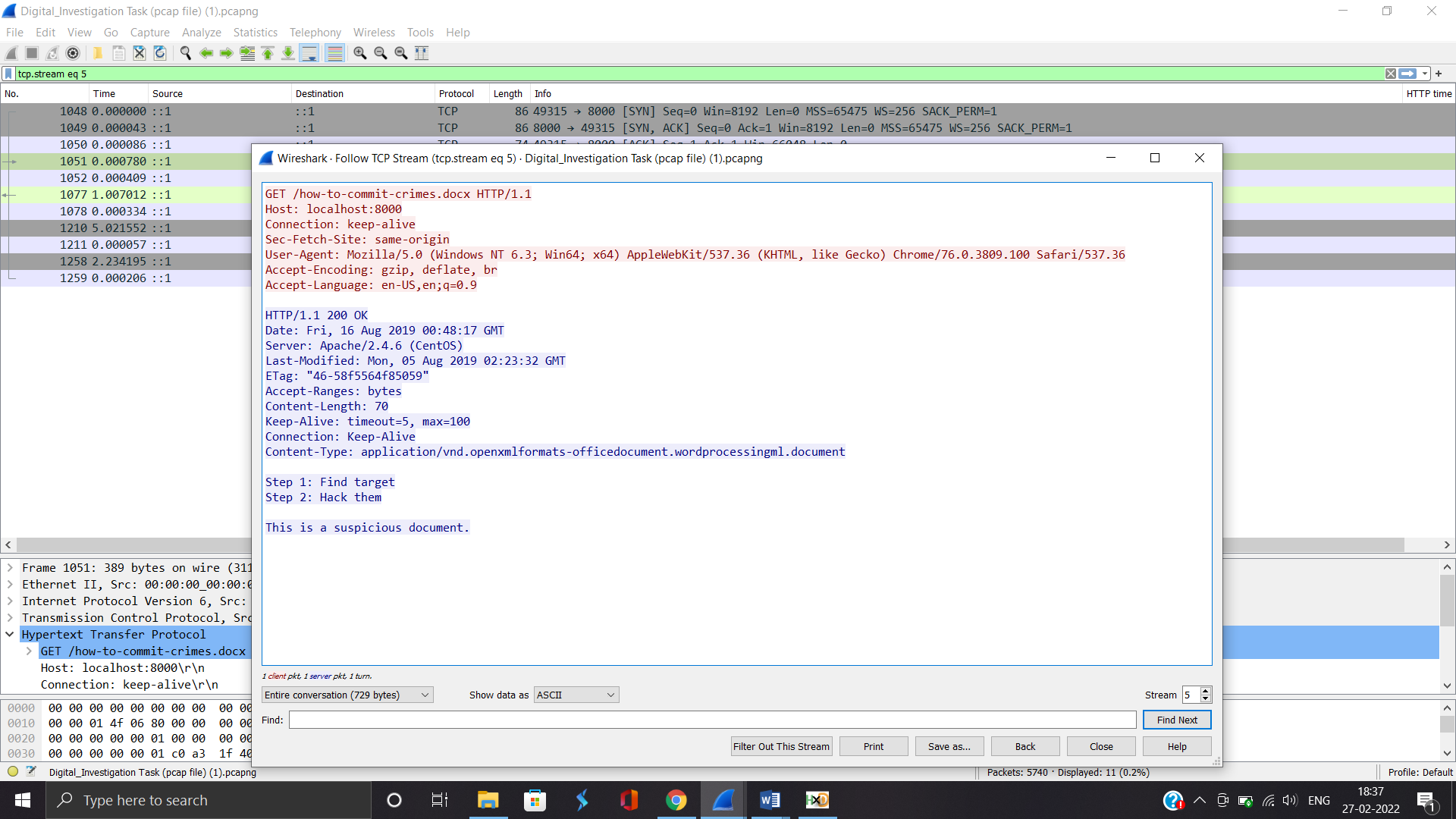
**Sub-task 3:**

* *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*

*Step 1: Find target*

*Step 2: Hack them*

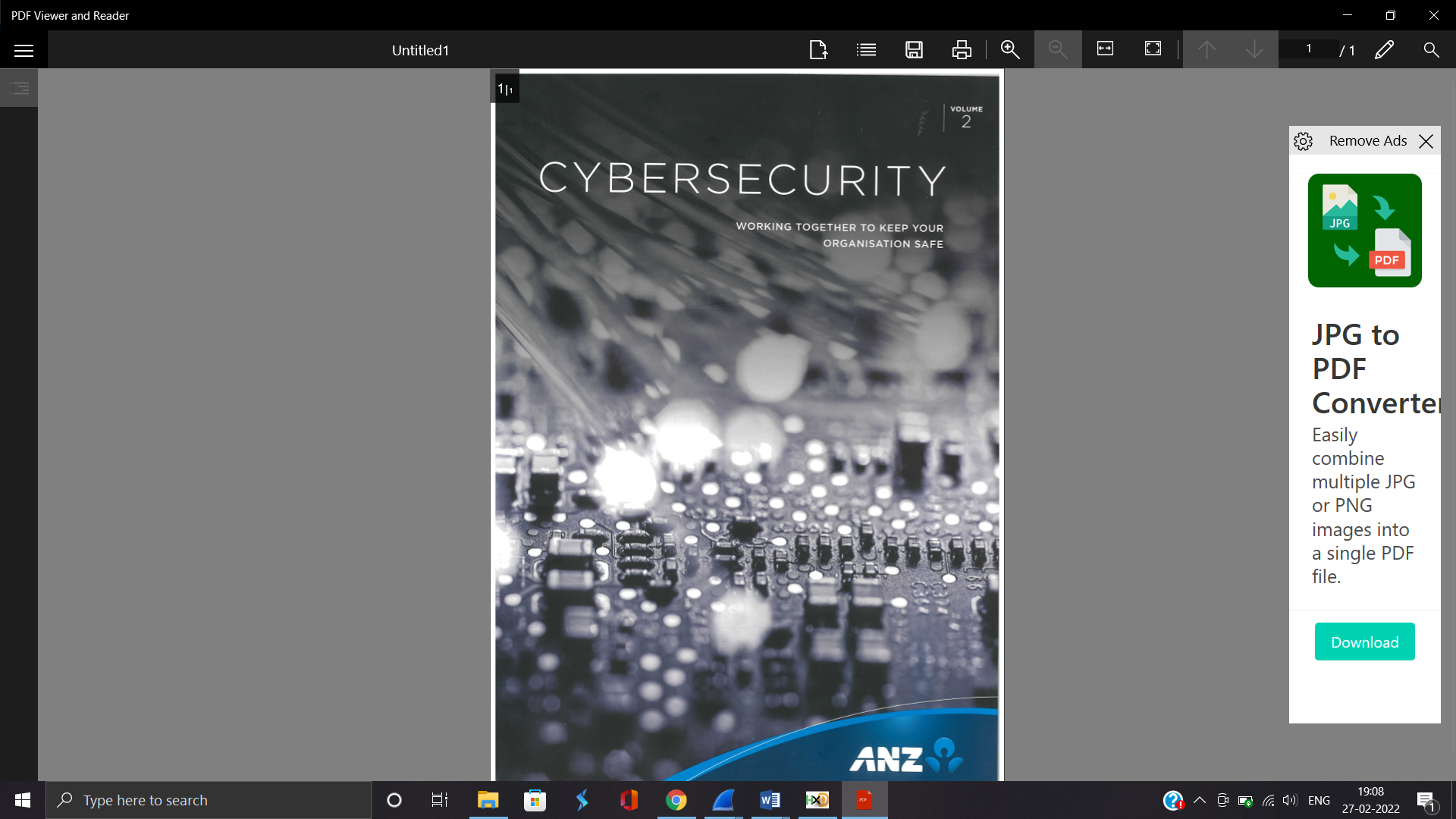
*This is a suspicious document.*



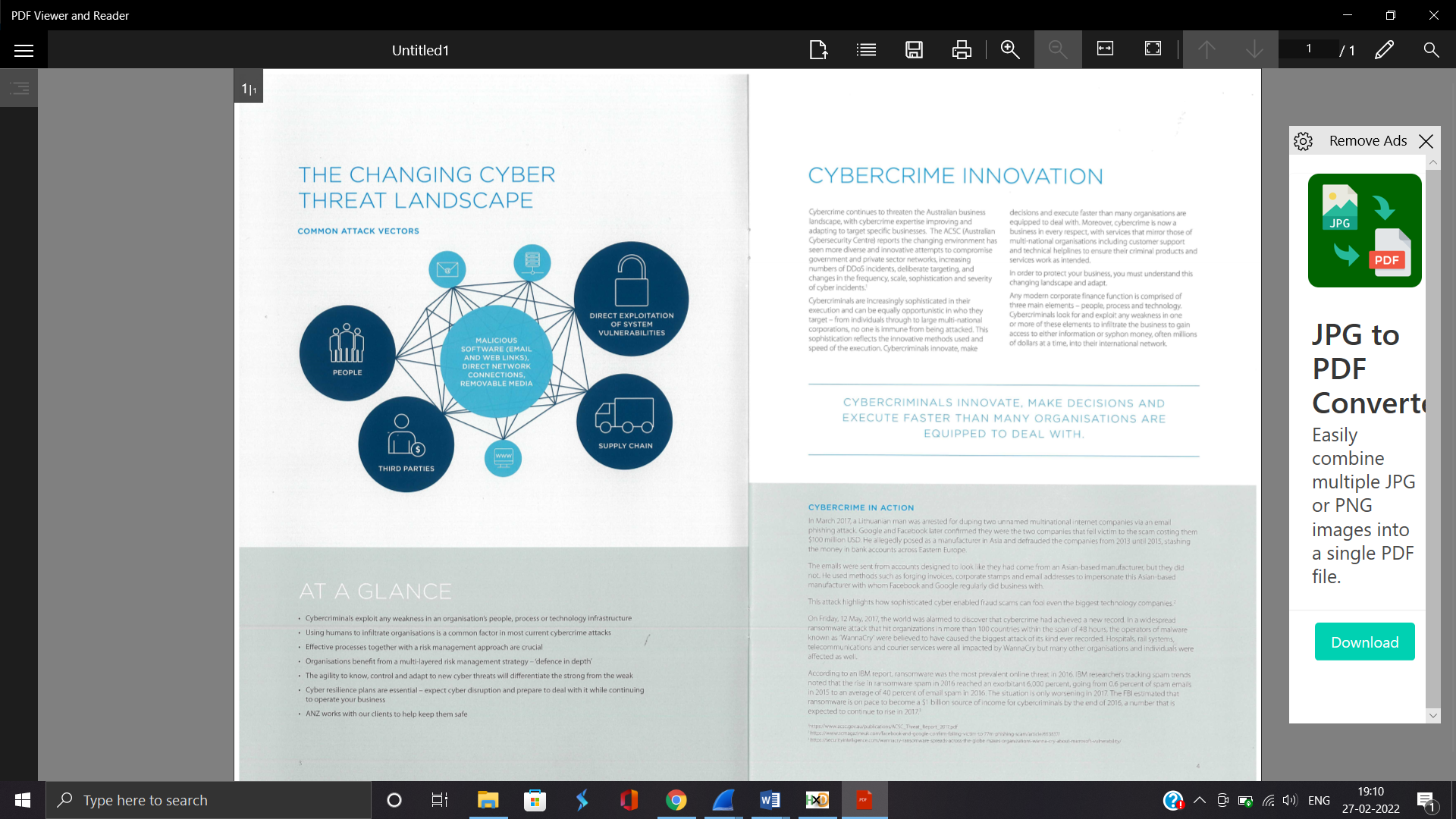
**Sub-task 4:**

* *The user accessed 3 pdf documents: ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf*
* *First we will follow same process as in image same.*
* *In order to view the pdf’s we have to look for pdf signature i.e. 25 50 44 46 2D in raw format then paste those in between to HxD and save it in pdf file to look for data inside them.*

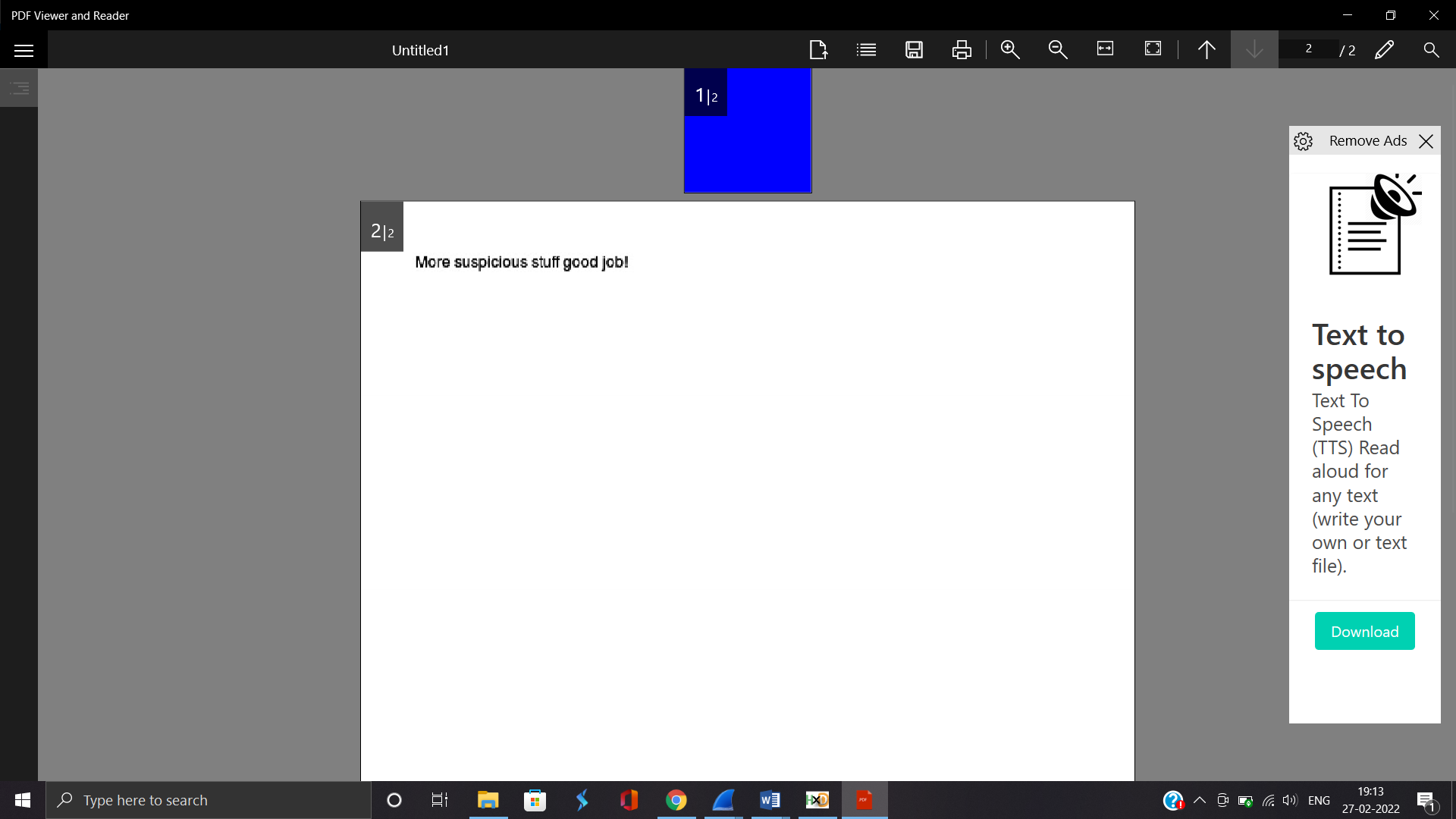
*ANZ\_document.pdf*



*ANZ\_document2.pdf*

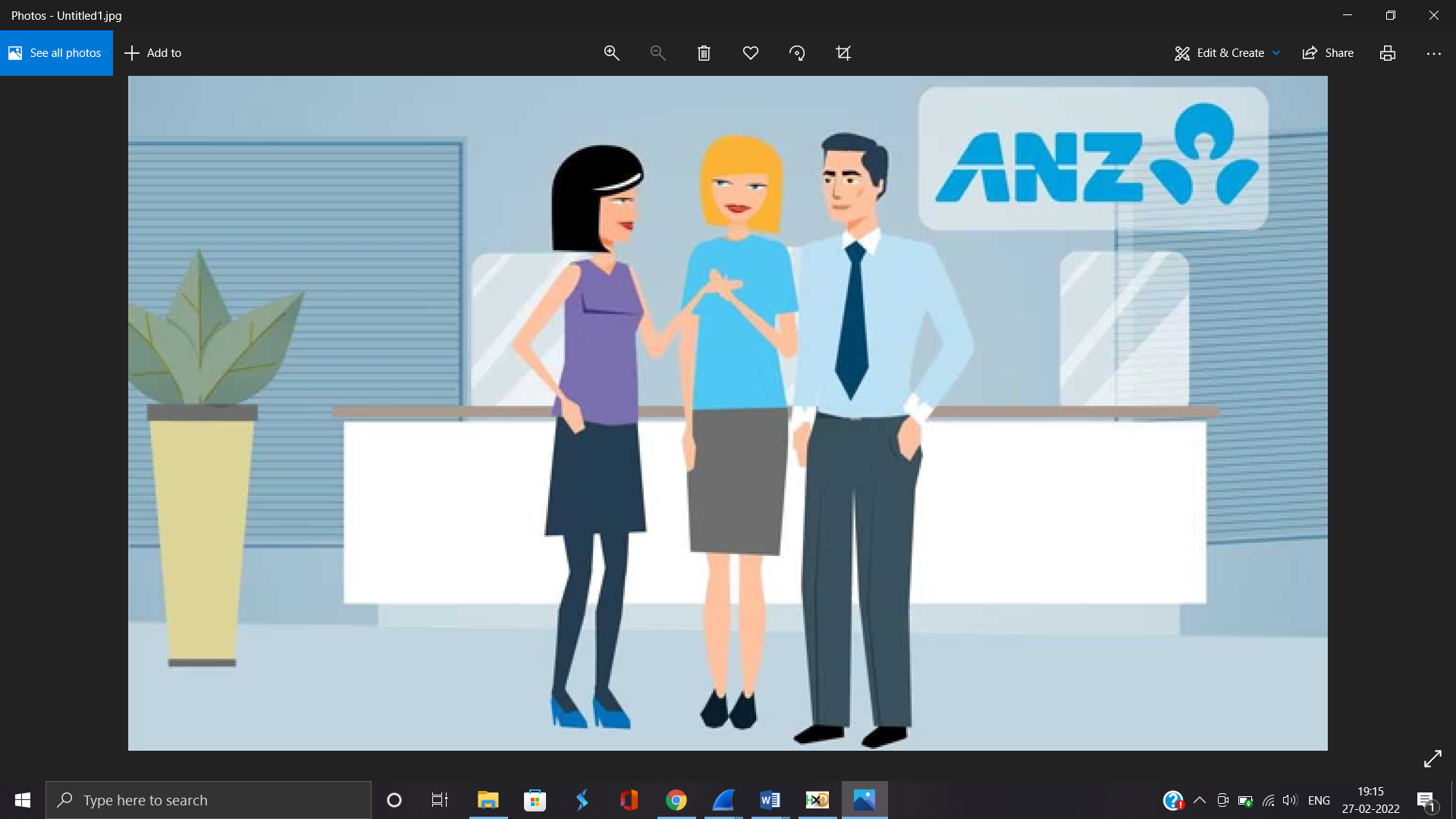


*Evil.pdf*



**Sub-task 5:**

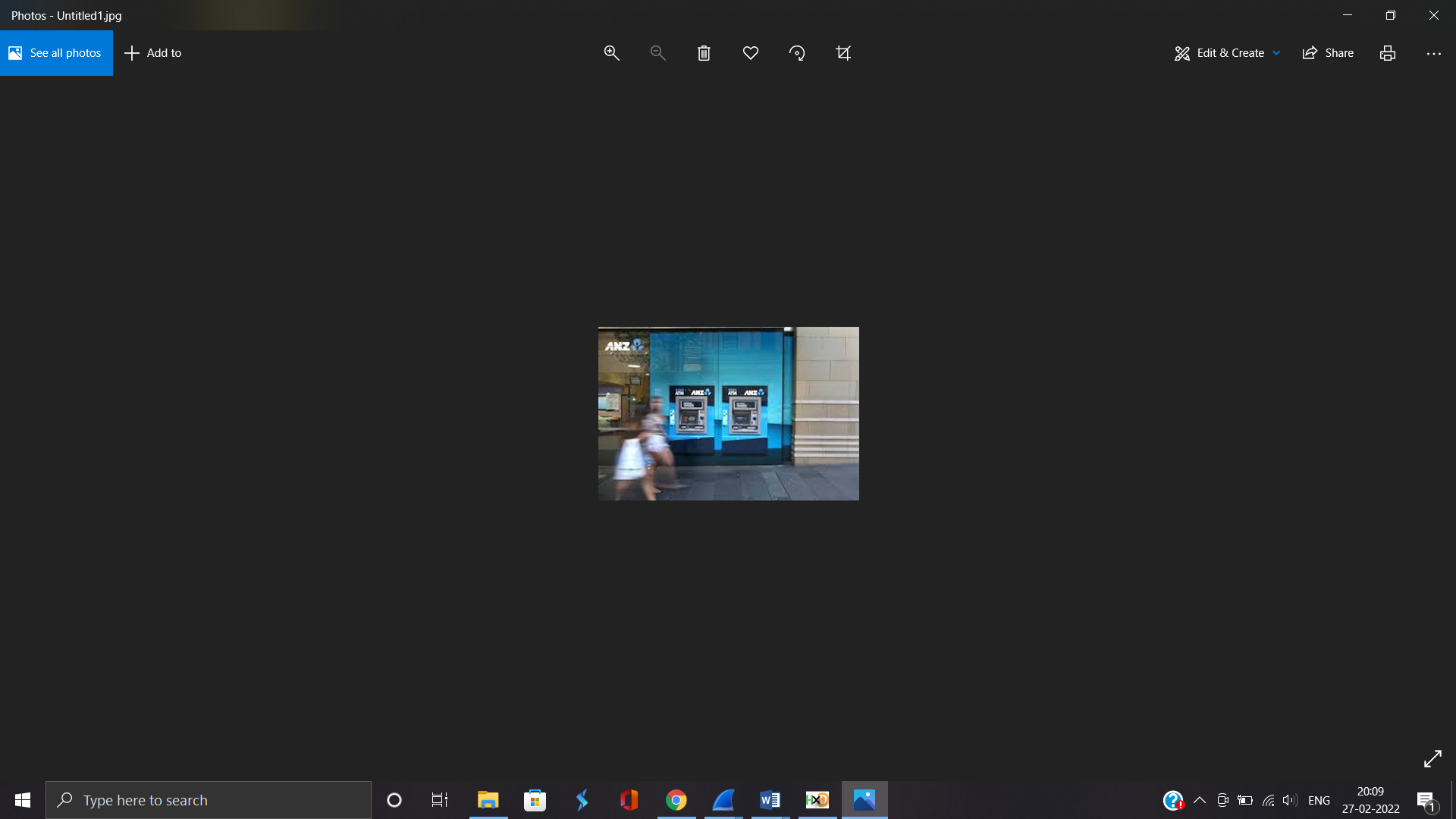
* *The user also accessed a file called "hiddenmessage2.txt"*
* *First, we will follow same steps till follow tcp steam.*
* *In which we saw that this txt file was having same file signature that of jpg.*
* *After which we proceeded with same steps of jpg of which we got this image.*



**Sub-task 6:**

* *The user accessed an image called "atm-image.jpg"*
* *Following same steps of jpg as in Task 1, we got to know that there are multiple ddf8 and ddf9 signature of jpg.*
* *I tried extracting both sets of data, and got two different images.*

*First Image:*

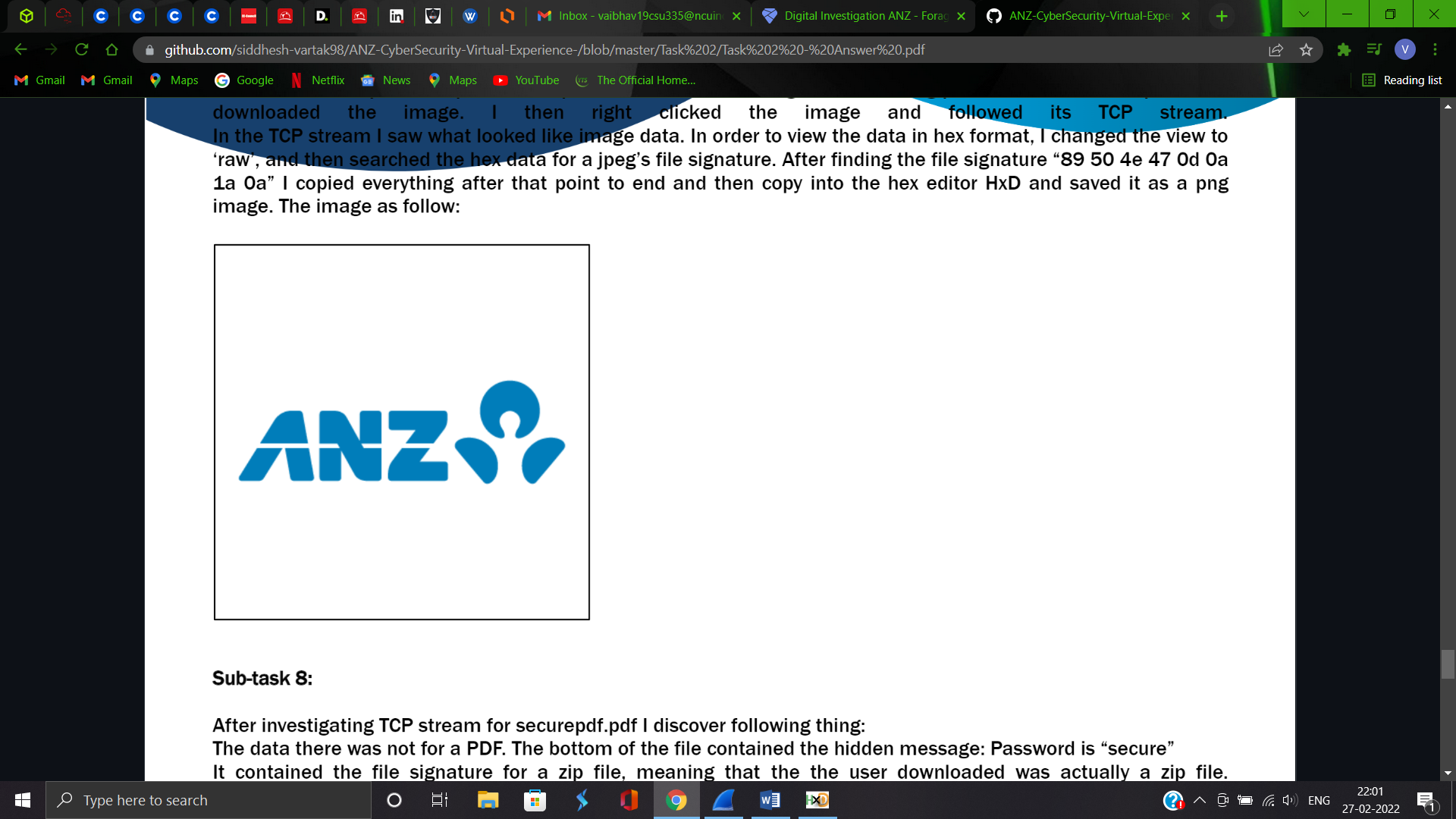


*Second Image:*

****

**Sub-task 7:**

* *The network traffic shows that the user accessed the image "broken.png"*
* *We first filtered the packet to http packets only, then opened the image broken.png using follow tcp steam method.*
* *In this type we have png image so our signature would be e “89 50 4e 47 0d 0a 1a 0a”*
* *I copied everything after that point to end and then copy into the hex editor HxD and saved it as a png image.*
* *The image as follow:*



**Sub-task 8:**

* *The user accessed one more document called securepdf.pdf*
* *The data there was not for a PDF. The bottom of the file contained the hidden message: Password is “secure” it contained the file signature for a zip file, meaning that the user downloaded was actually a zip file.*
* *So I copied the hex of the zip file into HxD and saved it as a zip file. I opened this zip file, and found it contained a pdf file called rawpdf.pdf.*
* *When opened, the pdf prompted for a password.*
* *The password „secure‟ shown in the tcp stream worked and the PDF opened.*
* *It was the first two pages to a guide for internet banking.*

