|  |
| --- |
|  |

**Provide a report on your findings from the pcap file and outline what processes / the steps you followed to achieve this. Here are each of your sub-tasks with additional instructions. Please record your findings under each sub-task title.**

**Sub-task 1:**

* *Firstly I applied a filter http to filter out http traffic and got to know that the user requested a .jpg file extension directly.*
* *So I right clicked on the link and followed the TCP stream and converted the data into raw format.*
* *So that I could see "ffd8” at the top and “ffd9” at the bottom.*
* *I copied this raw data into hex editor and saved it as a JPG file with .jpg extension and the resulting image is as follows:*

**

*Bank-logo.jpg*

**

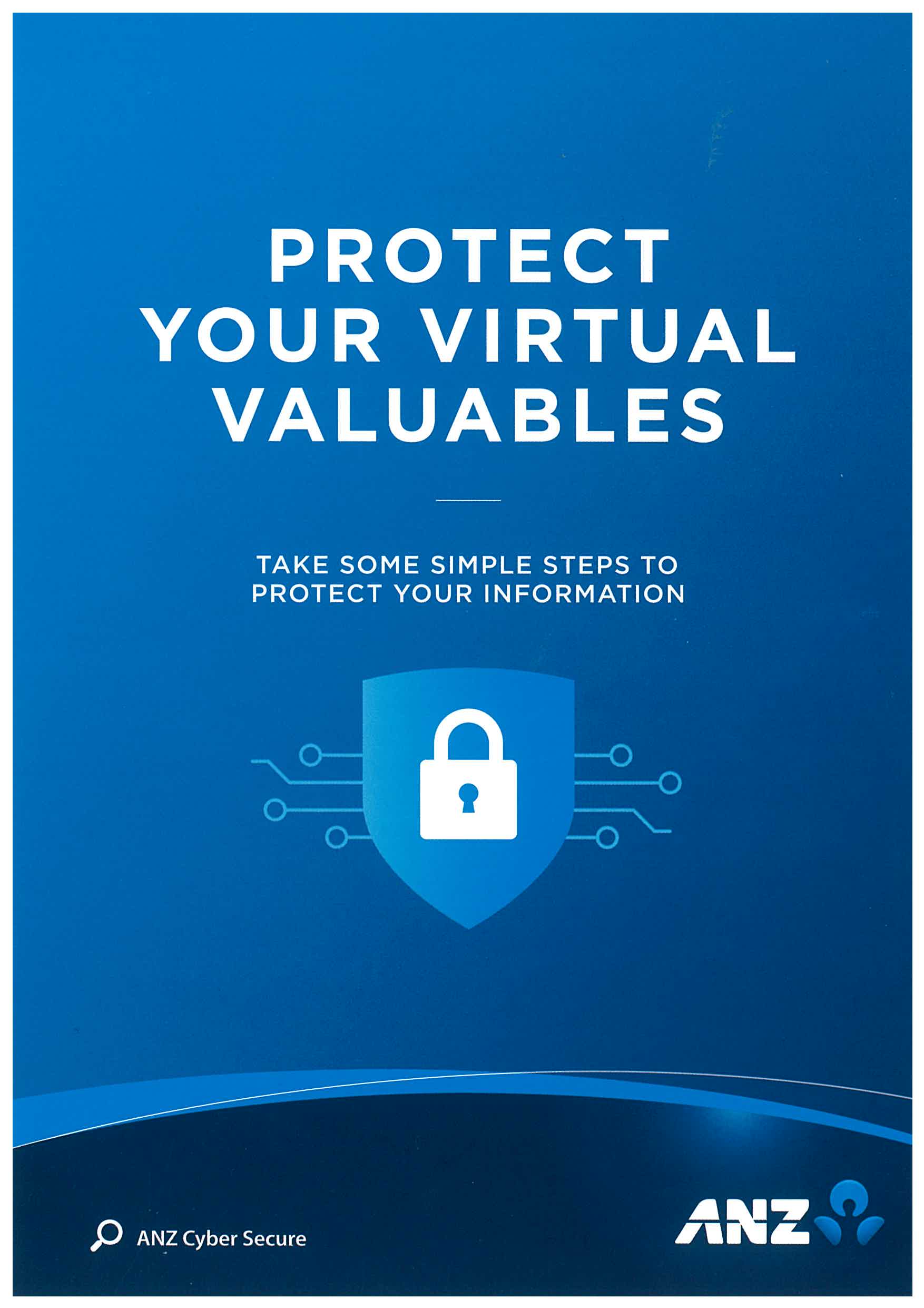
*Bank-card.jpg*

**Sub-task 2:**

* *I followed the same process as I did for top images I followed the TCP stream and copied the raw data to a hex editor and saved the file as a jpg.*
* *But I also found a hidden message when converting the hex value which read:*

***“You've found a hidden message in this file! Include it in your write up.”***

* *The resulting image was as follows:*

**

* *There were two hidden messages attached with these two images. The other hidden message was:*

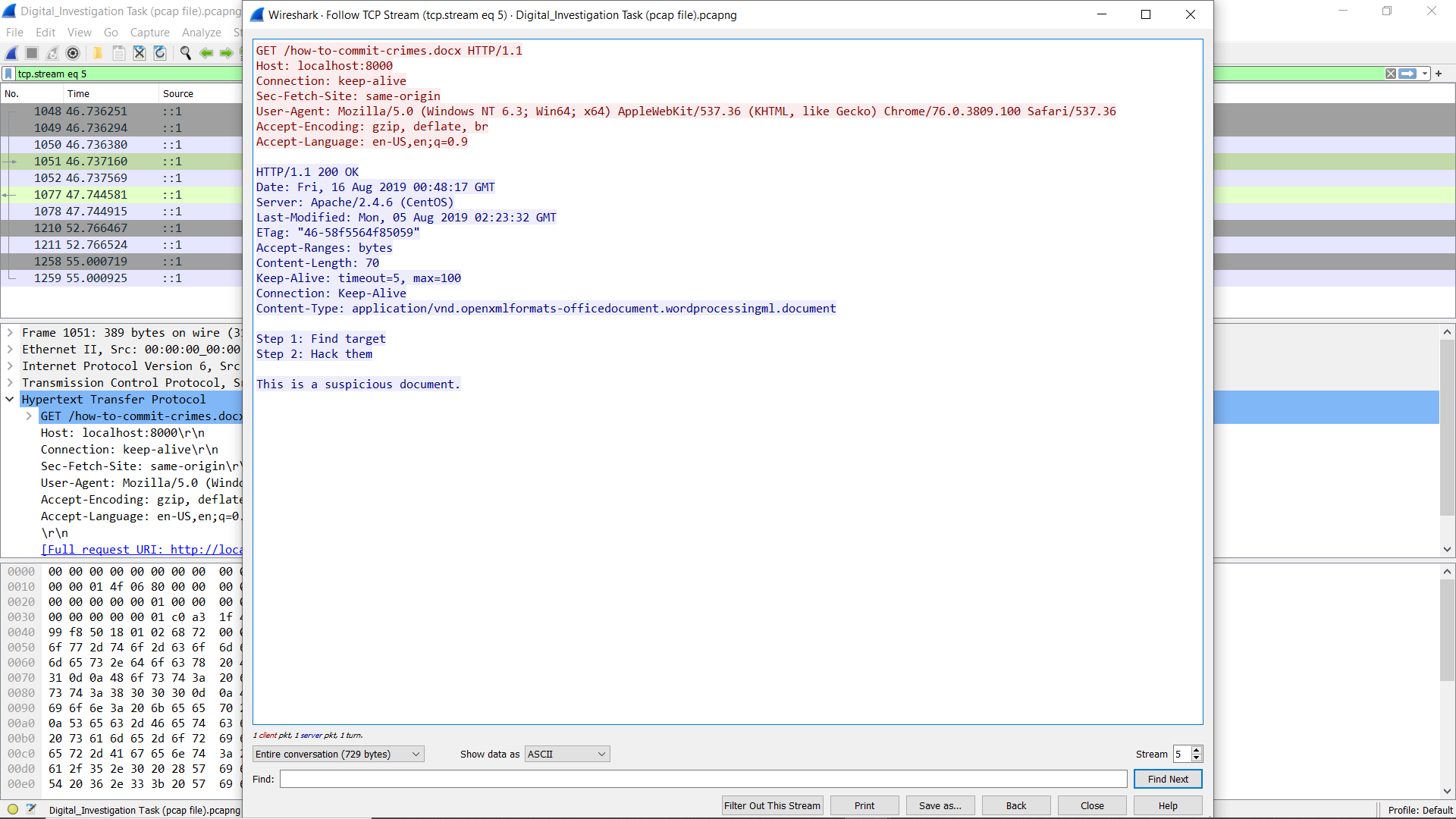
***“You've found the hidden message!***

***Images are sometimes more than they appear.”***

******

**Sub-task 3:**

* *In order to reveal the contents of the document, I had view the TCP stream of the http get request for the file. The document contents were visible in the ASCII view. The document attached below :*

**

**Sub-task 4:**

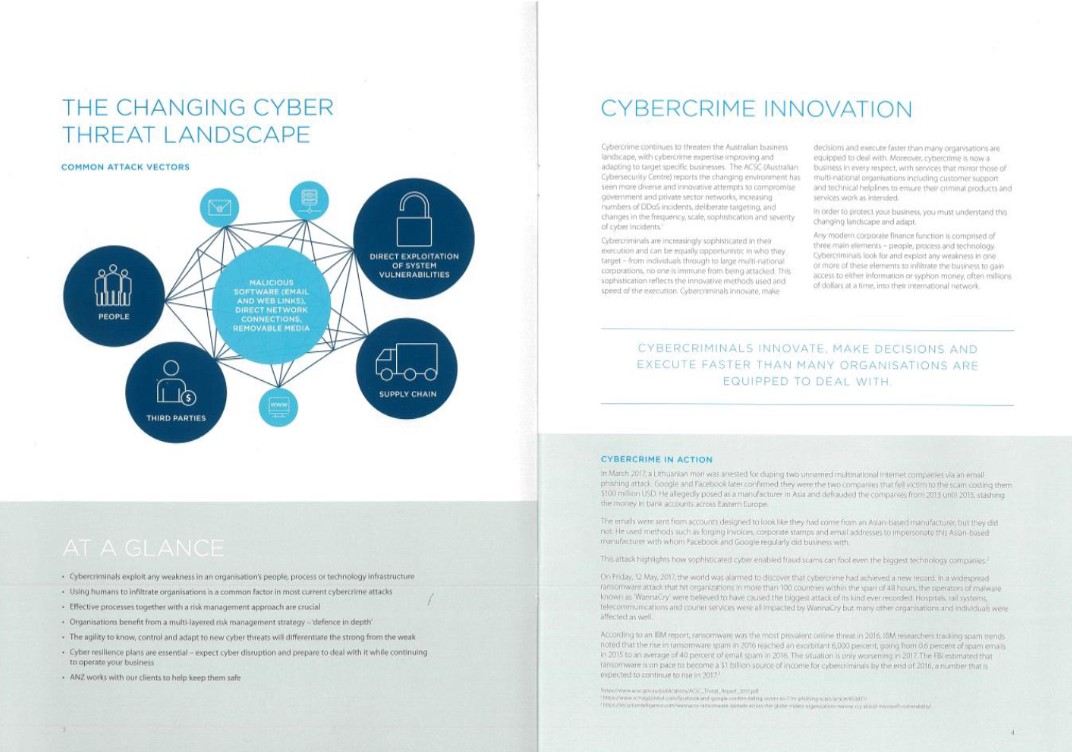
* *I followed the TCP stream for this as usual and I found the pdf file signature which was hex value*

25 50 44 46

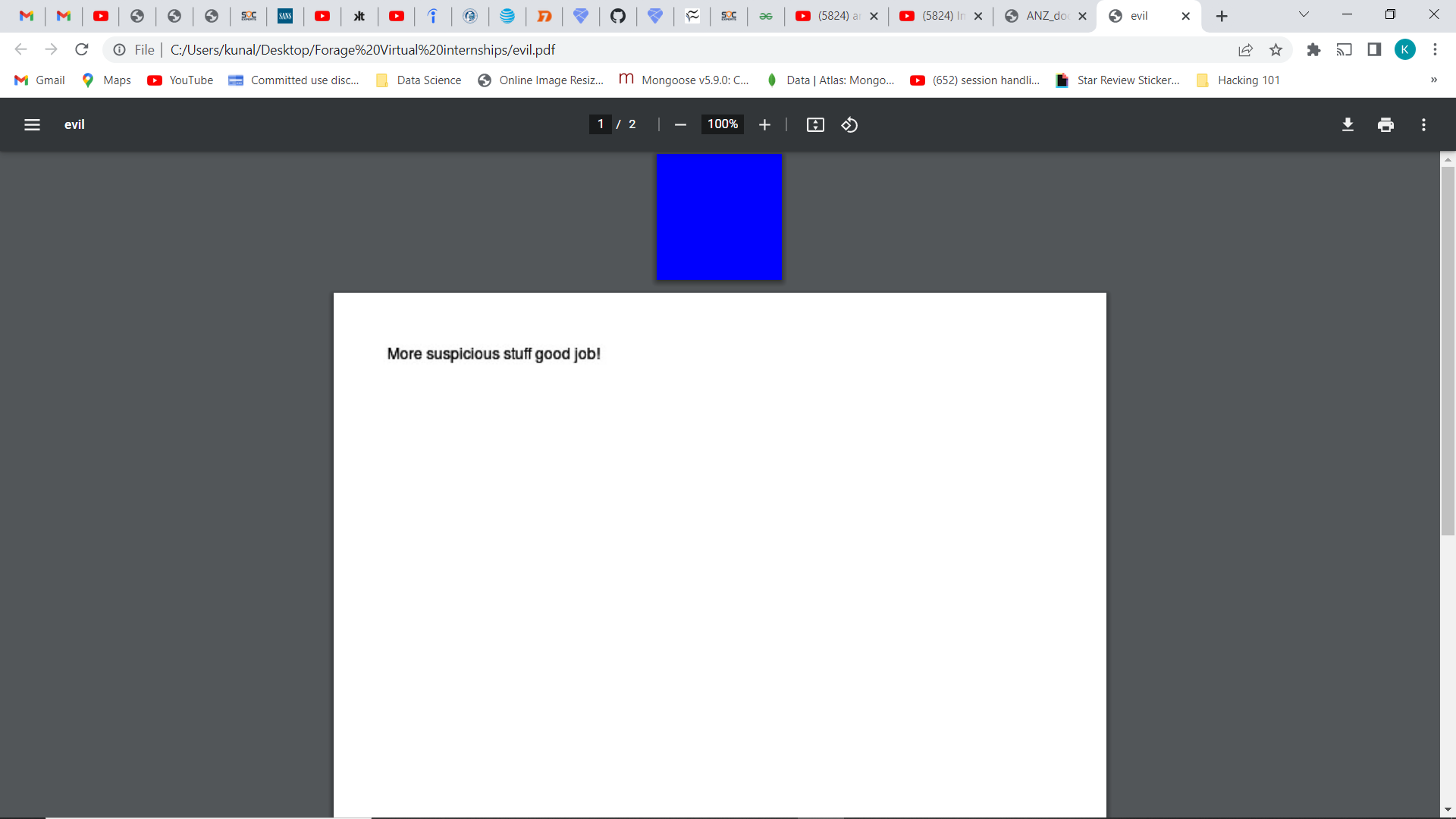
* *The screenshot of the pdf file is attached below:*

**

*ANZ\_document.pdf (extracted image)*

**

*ANZ\_document2.pdf (Extracted image)*

**

*Evil.pdf (Extracted image)*

**Sub-task 5:**

* *The hiddemessage2.txt file after following the TCP stream discovered to be a jpg file so I dumbed the raw data into hex editor and saved it as jpg file.*
* *Below is the attached jpg file:*

**

**Sub-task 6:**

* *I viewed TCP stream as usual when investigating this traffic I found two sets of jpeg file signatures.*
* *So I right clicked on the link and followed the TCP stream and converted the data into raw format.*
* *So that I could see "ffd8” at the top and “ffd9” at the bottom.*
* *I copied this raw data into hex editor and saved it as a JPG file with .jpg extension and the resulting image is as follows:*

**First Image:**

****

**Second Image:**

****

**“Here single get request downloaded two images.”**

**Sub-task 7:**

* *I filtered the http traffic and followed the TCP stream for the .png file and found the signature and dumped all the raw data into hex editor and saved the file as png.*
* *Below is the image:*

**

**Sub-task 8:**

* *After investigating and following the TCP stream I discovered that the ASCII view contained a secret message at the bottom which was password is “secure”.*
* *It contained signature of a zip file the user had actually downloaded the zip file.*
* *I opened the zip file it contained a pdf file named rawpdf.pdf its password was “secure”.*
* *The pdf content was first two pages of banking guide.*
* *The image is below:*