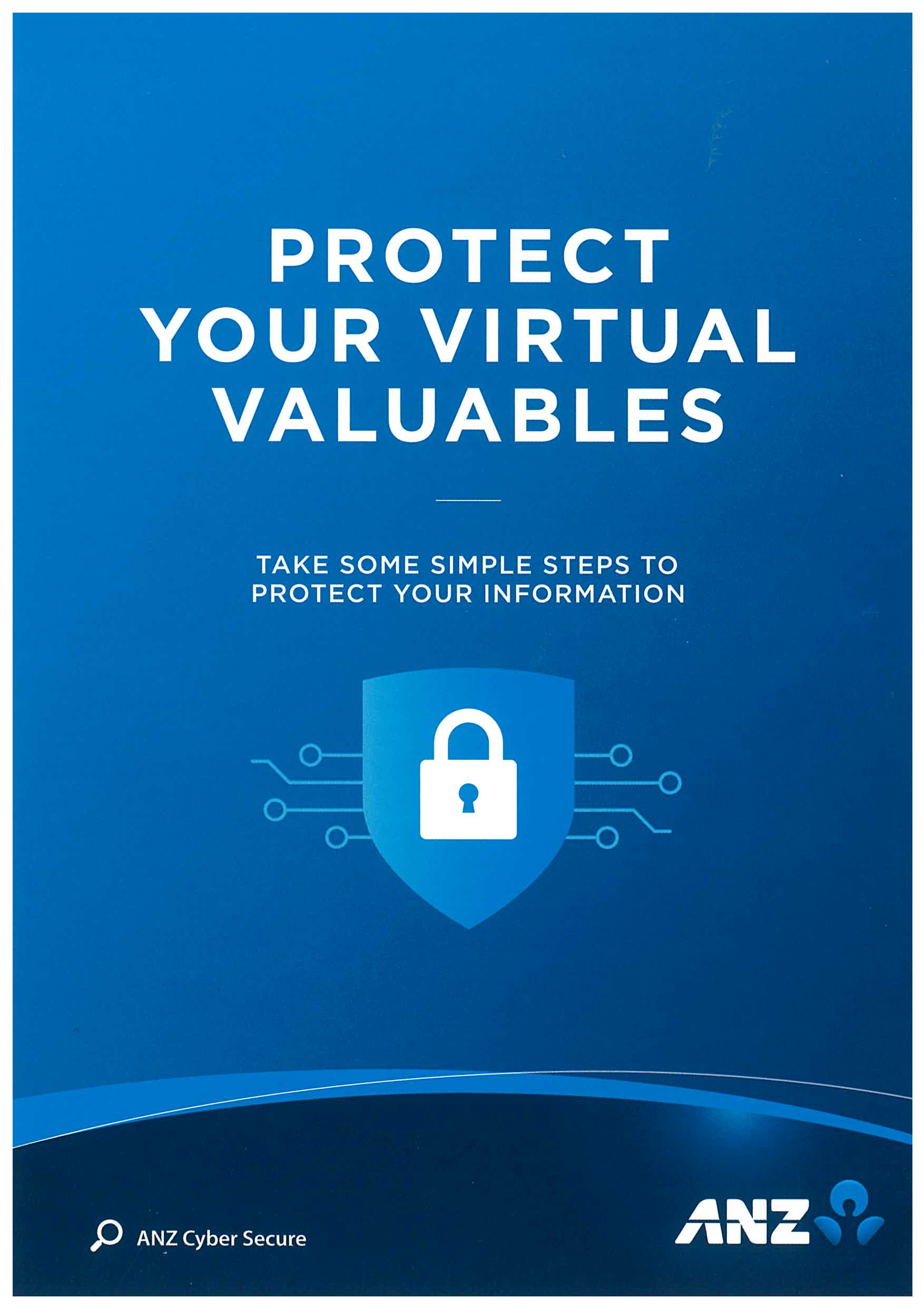
|  |
| --- |
|  |

**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:**

* *anz-logo.jpg and bank-card.jpg are two images that show up in the user’s network traffic.*
* *Extract these images from the pcap file and attach them to your report.*
* **

**Sub-task 2:**

* *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
* *Extract the images, include them and mention what is different about them in your report.*
* *I followed the same process to extract these images as I did in sub-task 1, which was to view the TCP stream, identify the images hex data, then copy and save that as a jpg file.*
* **

**

1. *The first image had the message in the network traffic that said “You've found a hidden message in this file! Include it in your write up.”*
2. *The first image had the message in the network traffic that said “You've found the hidden message!*

*Images are sometimes more than they appear.”*

**Sub-task 3:**

* *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
* *Find the contents of this file and include it in your report.*
* *In order to find the contents of the document, I had to view the TCP stream of the http get request for the file. The documents contents were visible in the ascii view.*

Step 1: Find target

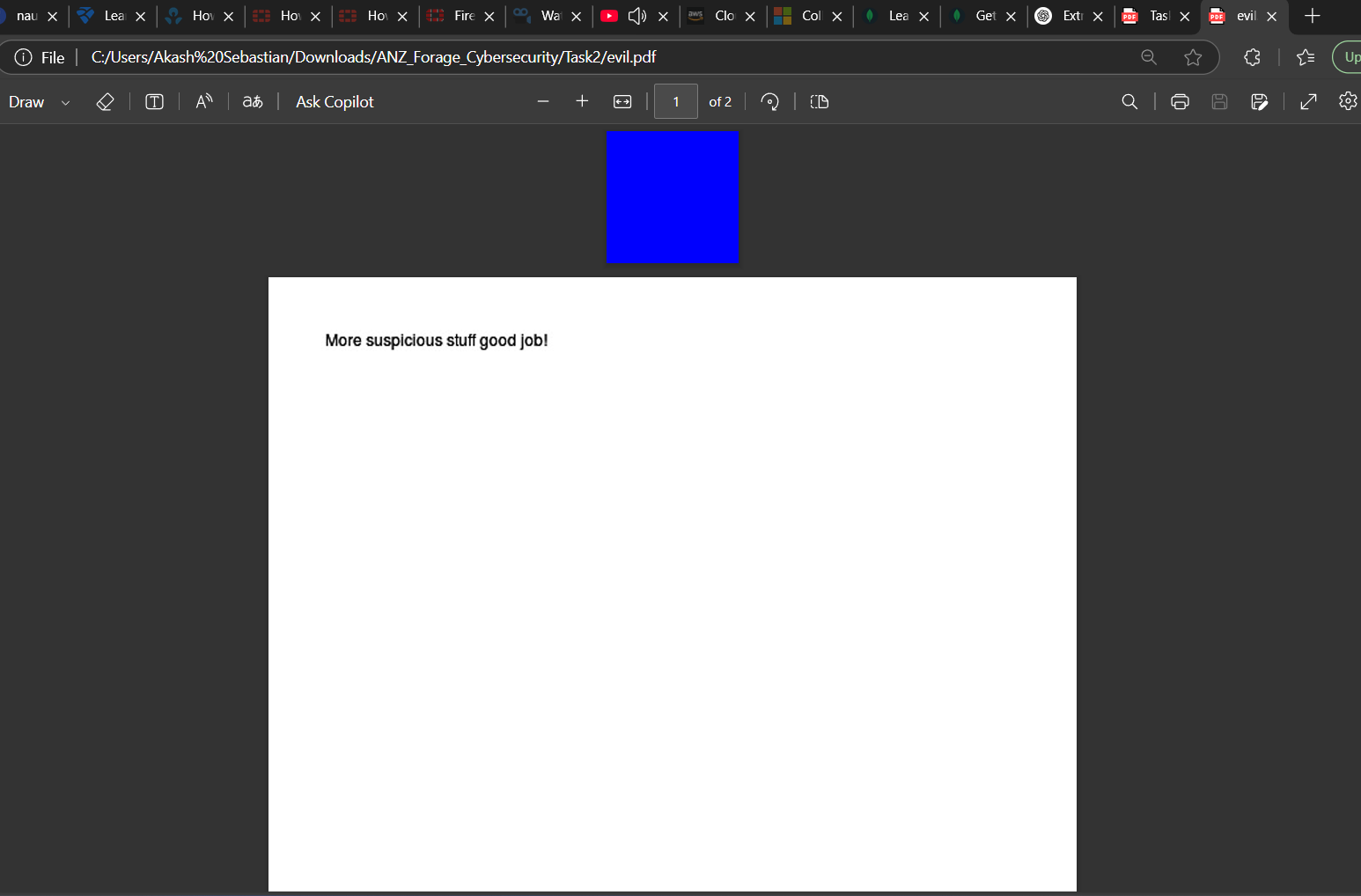
Step 2: Hack them

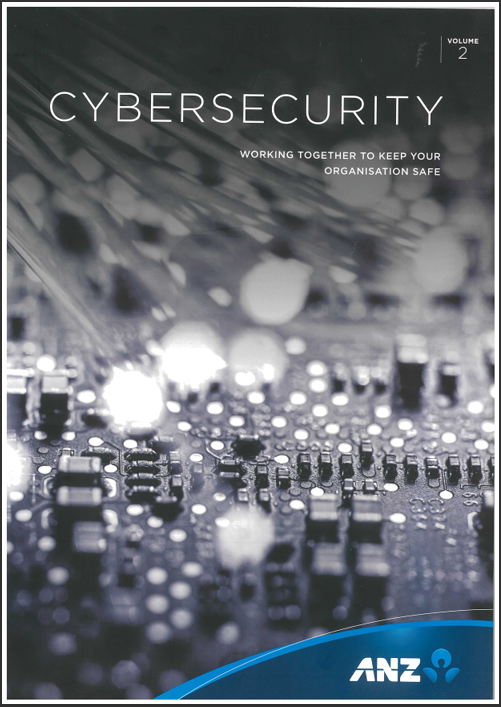
This is a suspicious document.

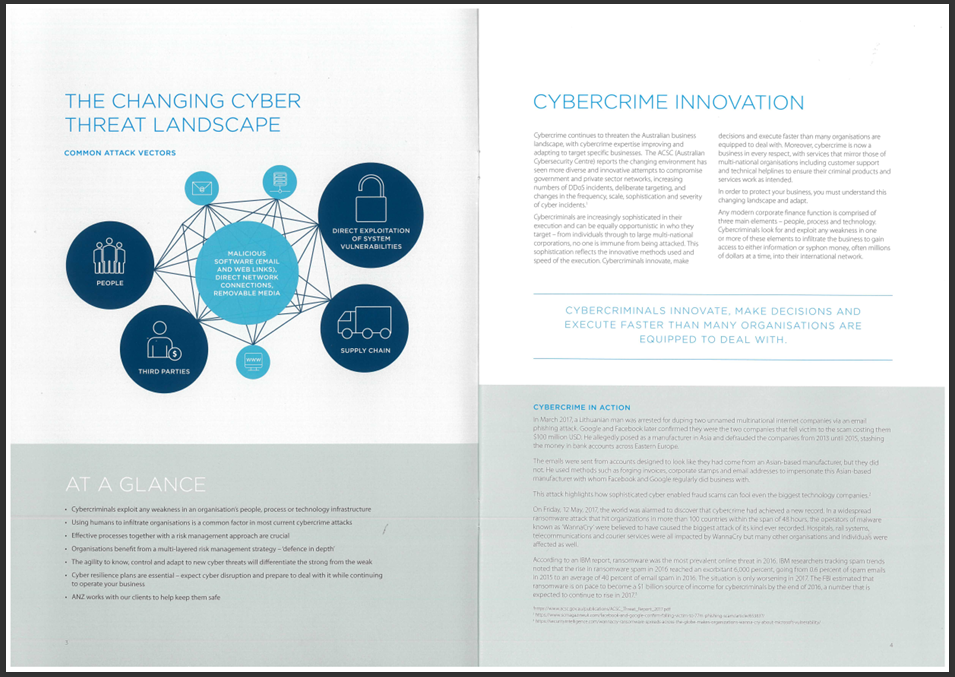
**Sub-task 4:**

* *The user accessed 3 pdf documents: ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf*
* *Extract and view these documents. Include images of them in your report.*

*In order to view these PDF’s I viewed the TCP stream as usual, and found the file signature for a PDF, which was the hex data “25 50 44 46”. I noticed in the ascii view that the PDF data went until the very end of the TCP stream, so I copied all the hex date from the file signature onwards into HxD and saved it as a pdf file.*

**

**

**

**Sub-task 5:**

* *The user also accessed a file called "hiddenmessage2.txt"*
* *What is the contents of this file? Include it in your report*
* *I viewed the TCP stream of this file, and noticed that instead of being plain text it was encoded data and when viewed as hex it had the same file signature as a jpg image. So I copied and saved the hex data with HxD as I have for other images, and discovered that the text file was actually this image*

**

**Sub-task 6:**

* *The user accessed an image called "atm-image.jpg"*
* *Identify what is different about this traffic and include everything in your report.*

****

****

**Sub-task 7:**

* *The network traffic shows that the user accessed the image "broken.png"*
* *Extract and include the image in your report.*

*The TCP stream for the broken.png traffic did not show any file signature for a png image. So while viewing the ascii form of the data, I recognized that the data was encoded in base64. Decrypting the base64 with an online tool resulted in png image data, which I copied into the “decoded text” section of HxD and saved as a png file.*

**

**Sub-task 8:**

* *The user accessed one more document called securepdf.pdf*
* *Access this document include an image of the pdf in your report. Detail the steps to access it.*

**After investigating the TCP stream for securepdf.pdf I discovered three things:**

**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 what 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.**