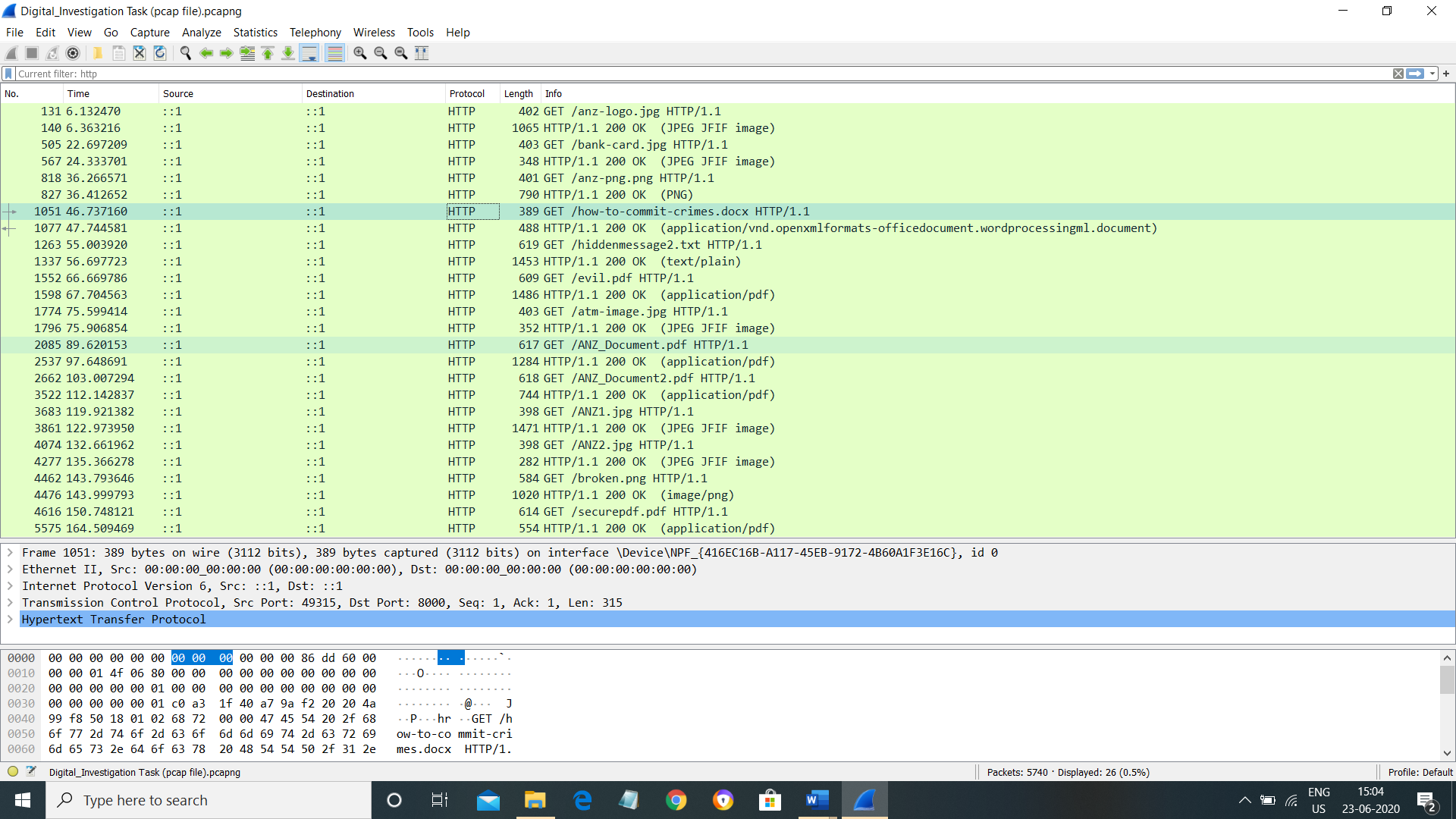
|  |
| --- |
|  |

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

**Sub-task 1:**

I have analyzed the provided packet capture file using the free network analysis tool ‘**Wireshark’**. I filtered out only the ‘http’ packets by typing ‘http’ in the ‘filter’ field to ease out the process of analyzing the packets as shown in the image below:



**(pcap file after applying the ‘http’ filter)**

To investigate this image download further, I viewed the TCP stream for **anz-logo.jpg** to see what I could find. The header/footer is **FFD8 – FFD9** in hex and the image is also recognizable in ASCII by the string ‘**JFIF**’ near the start.

The next step taken was extracting 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 program ‘**HxD**’. I then saved the file as a jpg and opened it, resulting in the image below:



**(anz-logo.jpg)**

I followed to same process as above but this time following the TCP stream of **bank-card.jpg** and the resulting image is as below.



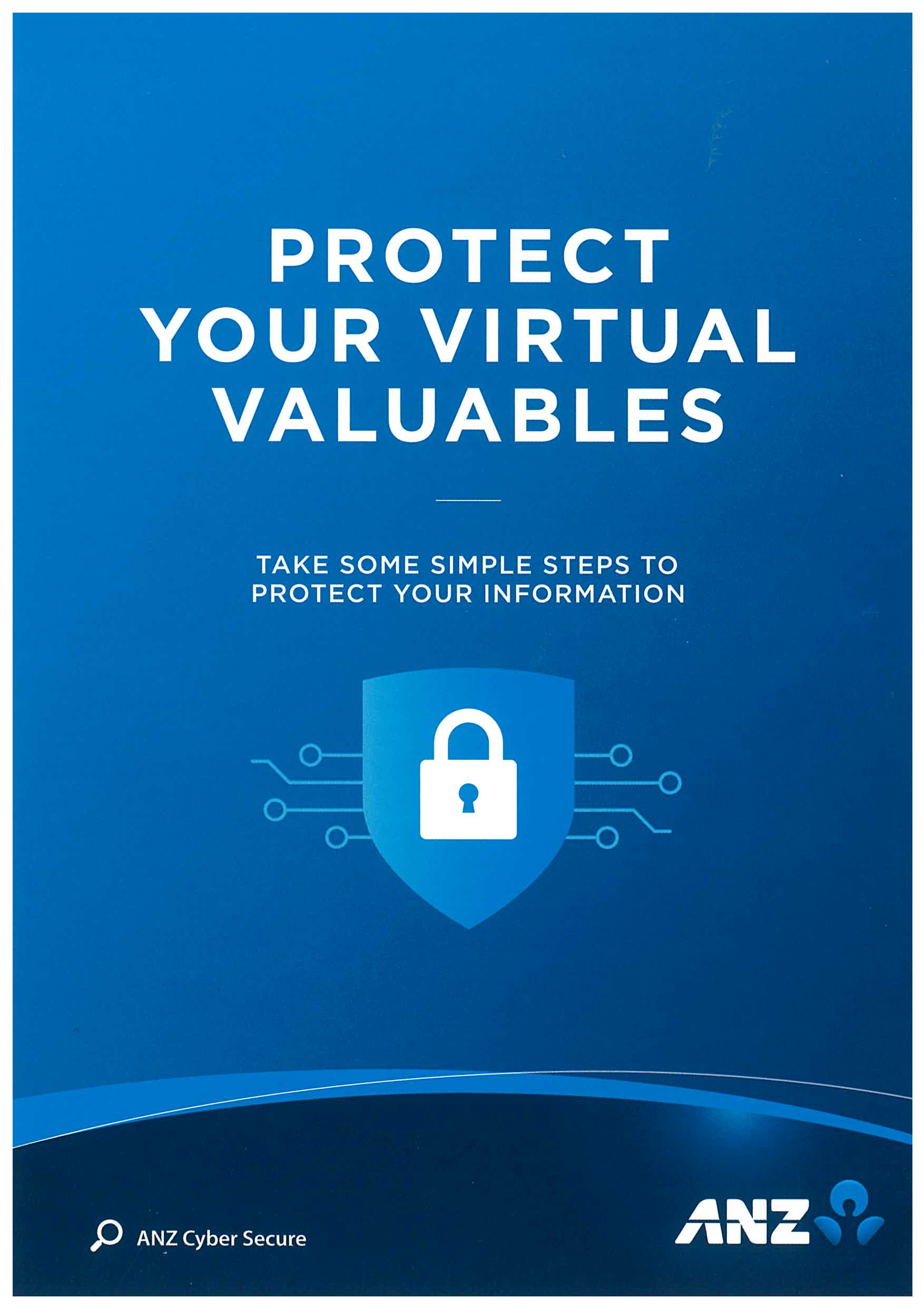
**(bank-card.jpg)**

**Sub-task 2:**

To investigate this image download, I viewed the TCP stream for **ANZ1.jpg** to see what I could find. The header/footer is **FFD8 – FFD9** in hex and the image is also recognizable in ASCII by the string ‘**JFIF**’ near the start.

The next step taken was extracting the images from the TCP stream, which I did by taking all the hex from FFD8 to FFD9. Starting from the first occurrence of **FFD8** till the last occurrence of **FFD9**, the hex was copied and pasted into the hex editor program ‘**HxD**’. I then saved the file as a jpg and opened it, resulting in the image below.

While viewing the TCP stream of **ANZ1.jpg** in ASCII view, I scrolled down to the end of the file and there was a line of text that said **“ You've found a hidden message in this file! Include it in your write up.”**



**(ANZ1.jpg)**

I followed to same process as above but this time following the TCP stream of **ANZ2.jpg** and the resulting image is as below.



**(ANZ2.jpg)**

While viewing the TCP stream of **ANZ2.jpg** in ASCII view, I scrolled down to the end of the file and there was a line of text that said **“You've found the hidden message! Images are sometimes more than they appear.”**

**Sub-task 3:**

To investigate the document that was downloaded, I viewed the TCP stream of **“how-to-commit-crimes.docx**”. In the ASCII view, I was able to see the following suspicious content of the document:

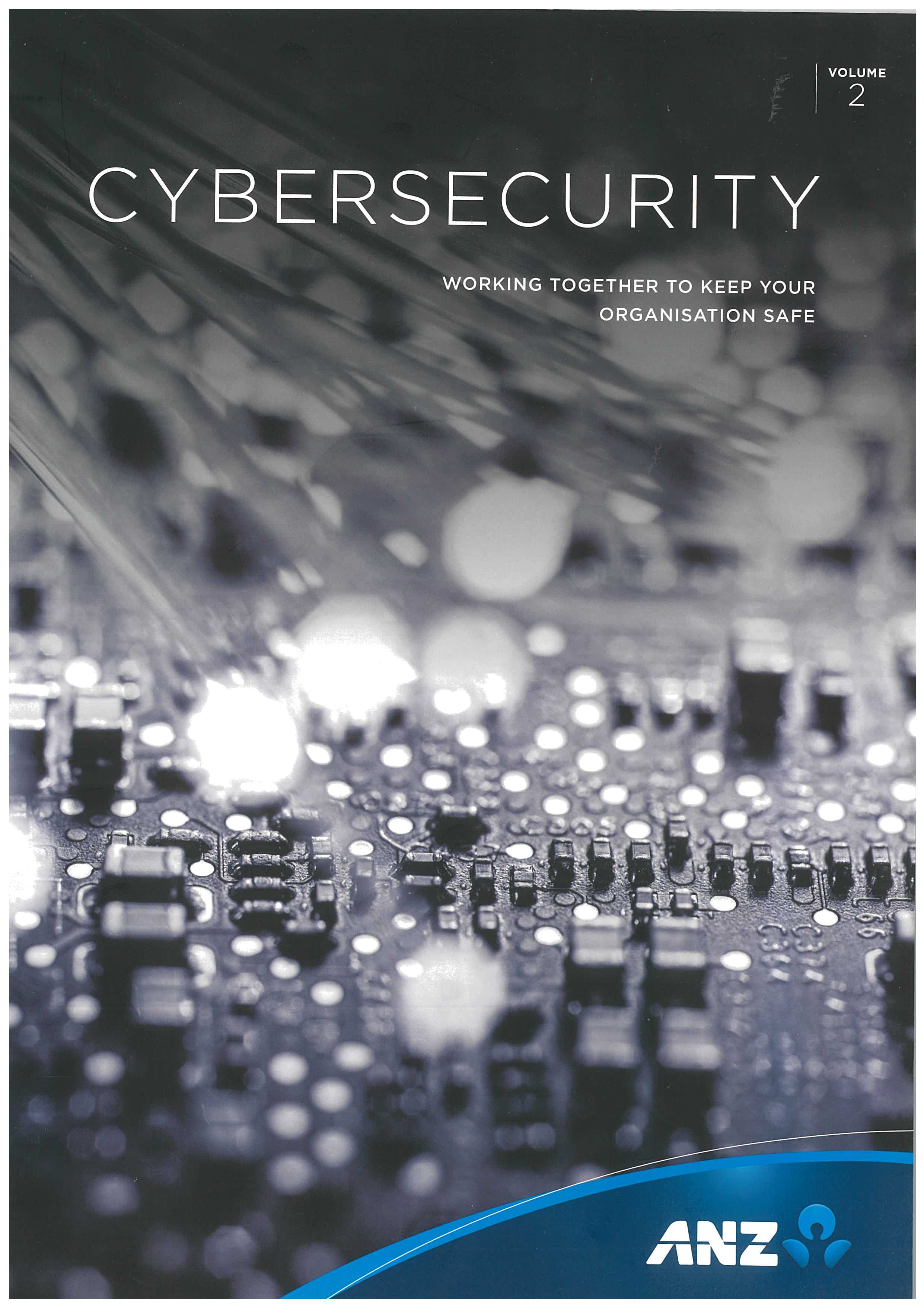
Step 1: Find target

Step 2: Hack them

This is a suspicious document.

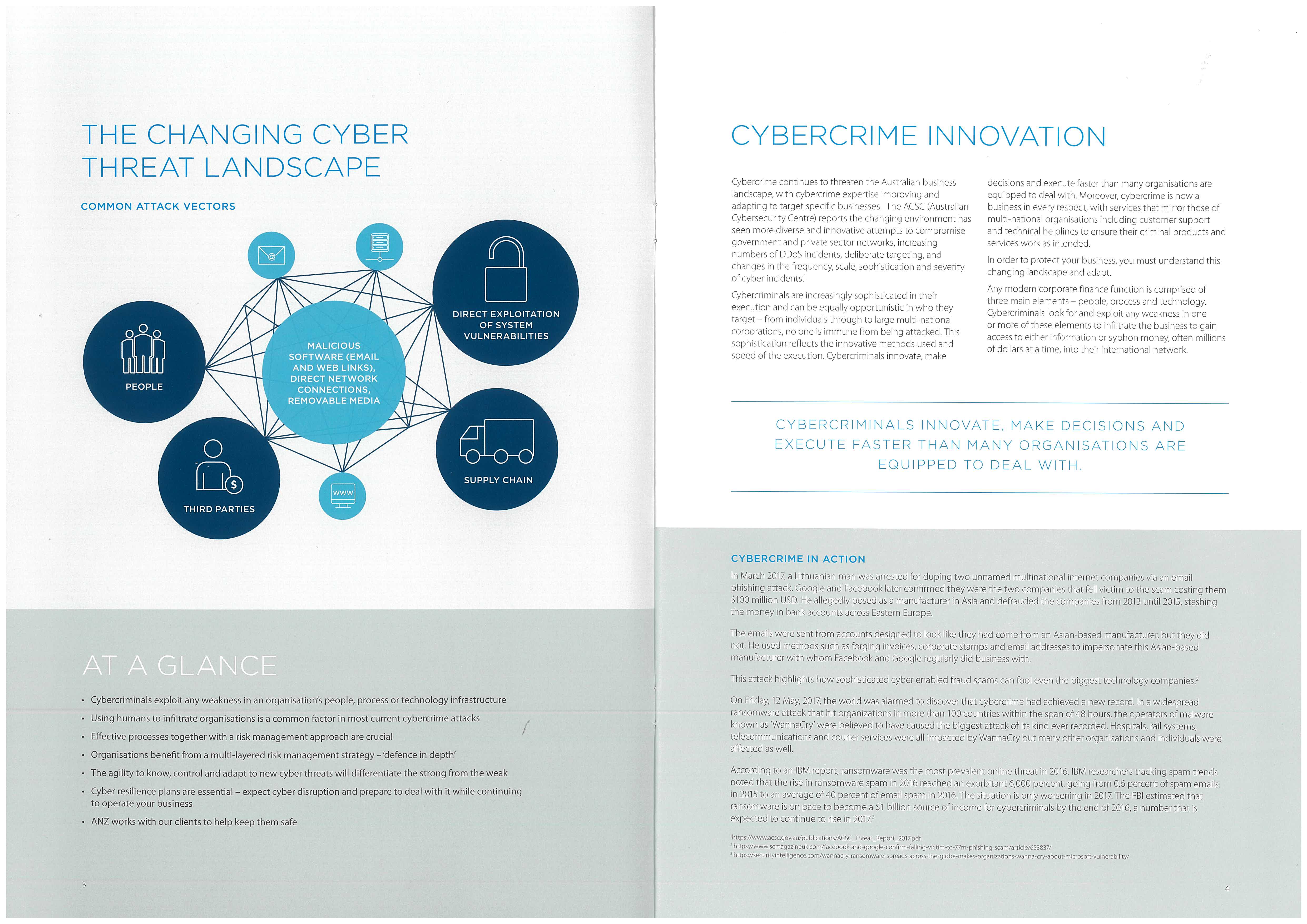
**Sub-task 4:**

To investigate the pdf that was downloaded, I viewed the TCP stream of **ANZ\_Document.pdf**. In the hex view, I searched for the pdf file signature  **“25 50 44 46 2d”** and copied the hex starting from this signature till the end and pasted it into the hex editor program ‘**HxD**’. I then saved the file as a **pdf** and viewed it. The following image was found in the pdf:



**(Image from ANZ\_Document.pdf)**

I followed to same process as above but this time following the TCP stream of **ANZ\_Document2.pdf** and the following image was found in the pdf:

**

**(Image from ANZ\_Document2.pdf)**

I followed to same process as above but this time following the TCP stream of **evil.pdf** and the following images were found in the pdf:



**(Image from evil.pdf)**



**(Image from evil.pdf)**

**Sub-task 5:**

To investigate the text file downloaded, I followed the TCP stream of **hiddentextmessage2.txt.** The string ‘**JFIF**’ near the start indicated that it was an image(.jpg). I switched to the hex(raw) view. The next step taken was extracting the image from the TCP stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program ‘**HxD**’. I then saved the file as a jpg and opened it, resulting in the image below:

**

**(image obtained from hiddentextmessage2.txt)**

**Sub-task 6:**

To investigate the image downloaded, I followed the TCP stream of **atm-image.jpg** to see what I could find. The string ‘**JFIF**’ appeared twice in the ASCII view of the TCP stream which indicated that there were two images. I switched to the hex (raw) view. The next step taken was extracting 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 program ‘**HxD**’. I then saved the file as a jpg and opened it, resulting in the image below:



**(image from atm-image.jpg file)**

I followed the same process to find the other image and the following image was found:



**(image from atm-image.jpg file)**

**Sub-task 7:**

To investigate the image downloaded, I followed the TCP stream to see what I could find. There was no header named **PNG** in the start of the TCP stream. I scrolled down to the bottom and found ‘==’ which indicated that it might be some padding. Instantly, I realised that it might be **base64 encoded**. I copied the text and **decoded** the base64 encoded text and I could see the **PNG** header. The corresponding hex data (starting from the PNG file signature - **89 50 4E 47 0D 0A 1A 0A**) was copied and pasted in the hex editor **HxD**. The file was saved as **broken.png** and the following image was obtained:



**(broken.png)**

**Sub-task 8:**

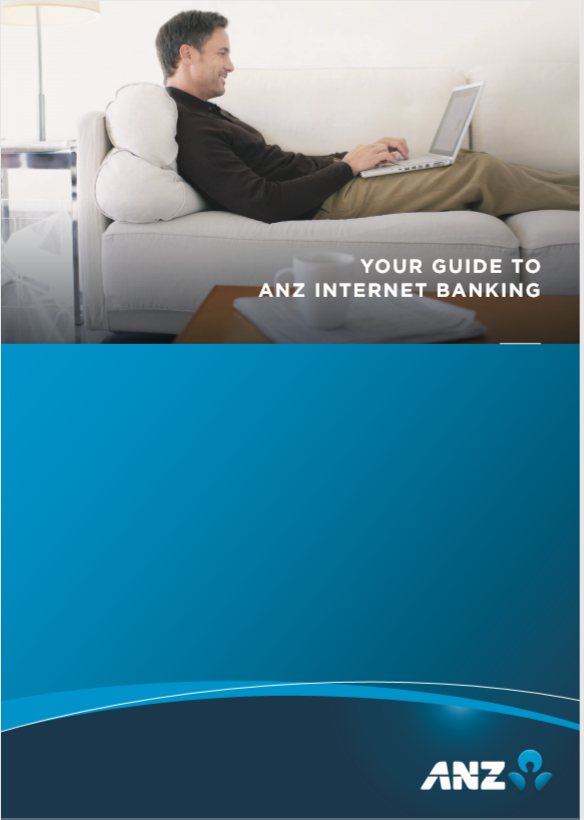
To investigate the pdf downloaded, I followed the TCP stream of **securepdf.pdf** to see what I could find. I header was shown as ‘**PK….’**.

I then searched for the file signature of **zip files** - “**50 4b 03 04”.** I copied the hex from this signature till the end and pasted it in the hex editor (**HxD).**  I then saved the file as **securepdf.zip.** Next step was to extract the contents of the zip file. After extracting, a pdf called ‘**rawpdf.pdf’** was obtained but it was **password protected.**

I then searched in the ASCII view of the TCP stream for **securepdf.pdf**  in ‘wireshark’ and in the end of the file, I found the following text:

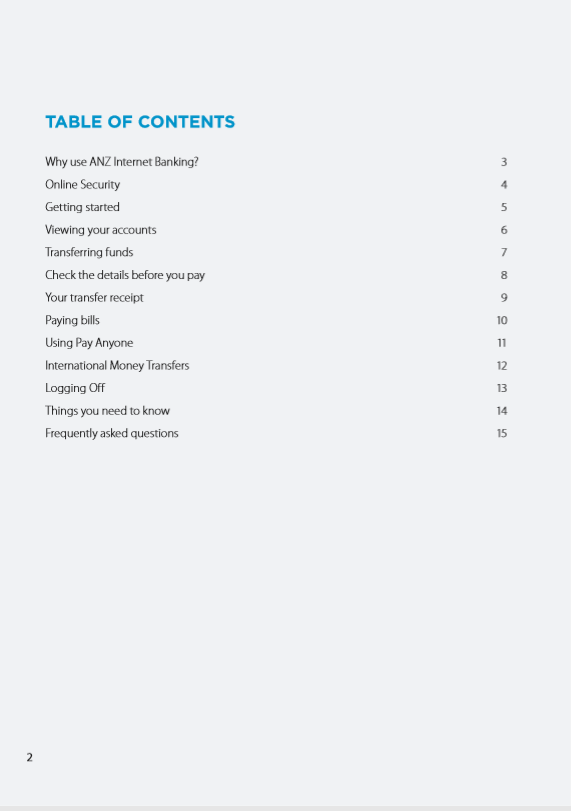
Password is "secure"

I have successfully obtained the **password** for the pdf as well. I entered the password in the pdf that was obtained by extracting the zip file and I was able to view the contents of the pdf. The following were obtained:



**(image from rawpdf.pdf)**

The second page of the pdf was:



**(image from rawpdf.pdf)**

**Additional information:**

By analysing the TCP packets in wireshark, I found another png image called **anz-png.png** which was not asked for in any of the sub tasks. By following the TCP stream and viewing the hex(raw) data I was able to find the file signature of **PNG** in the hex view. I copied the data starting from the file signature **89 50 4E 47 0D 0A 1A 0A**  and pasted it in the hex editor **HxD.** I saved the file as anz-png.png and the following image was obtained:

