|  |
| --- |
|  |

**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 users 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.*

**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.*

**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.*

**Sub-task 5:**

* *The user also accessed a file called "hiddenmessage2.txt"*
* *What is the contents of this file? Include it in your report*

**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.*

**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.*

**Packet Capture Analysis:**

* The provided pcap file was analyzed using wireshark.
* As filter, ”http” was put to see only HTTP packets.

**Sub Task 1 :**

****

To investigate the anz-logo jpeg image further, I viewed it’s TCP stream. From the TCP stream, I copied all the hex from FFD8 to FFD9 (Header and Footer of jpg), to the hex editor program HxD. I then saved the file as a jpg, resulting in the image above.

The same procedure was done for the bank-card image as well, shown below:



**Sub Task 2 :**

The stream for the images ANZ-1.jpg and ANZ-2.jpg are different because they include incomplete streams of data, containing multiple headers and footers denoting the fact that this image was attempted to be downloaded multiple times. By doing the same procedure as told above in task 1, we obtain some parts of the image as shown:

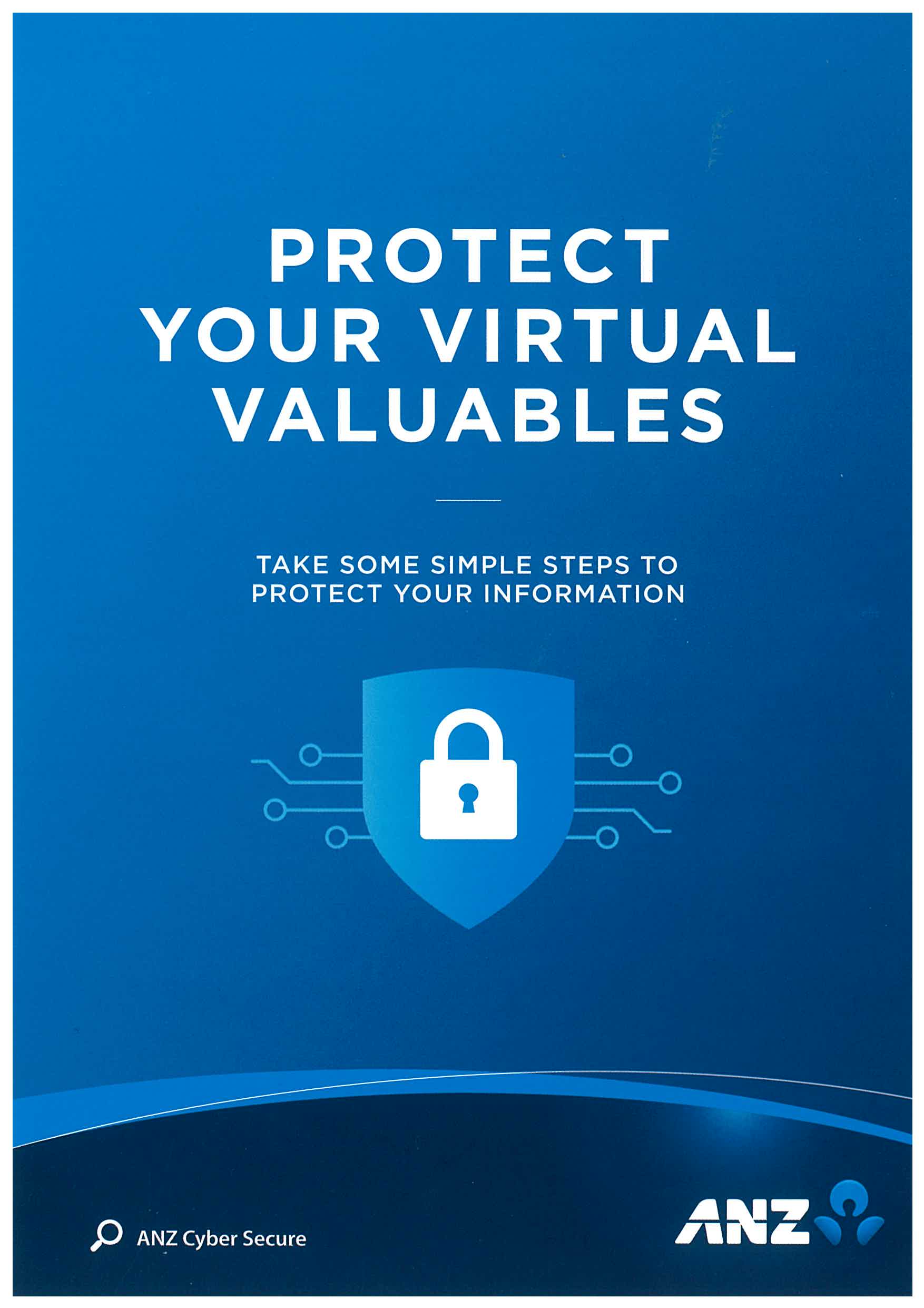
task2(1)

*ANZ-1 (partial)*

*task2(2)*

*ANZ-2 (Partial)*

By exporting them through wireshark however, we obtain the complete images:



ANZ-1 (complete)



ANZ-2 (Complete)

**Sub Task 3 :**

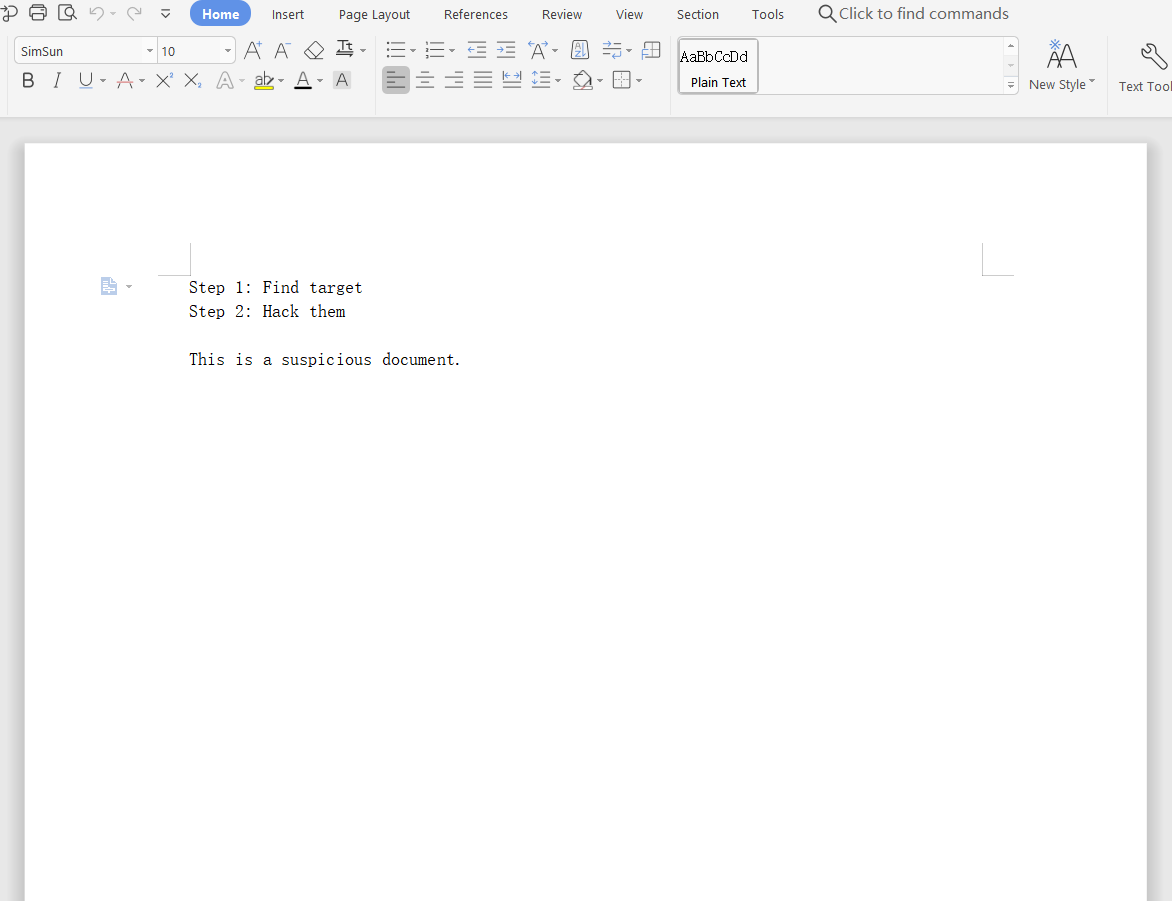
The docx file ‘how-to-commit-crimes’ was obtained by exporting from wireshark content being:

Step 1: Find target

Step 2: Hack them

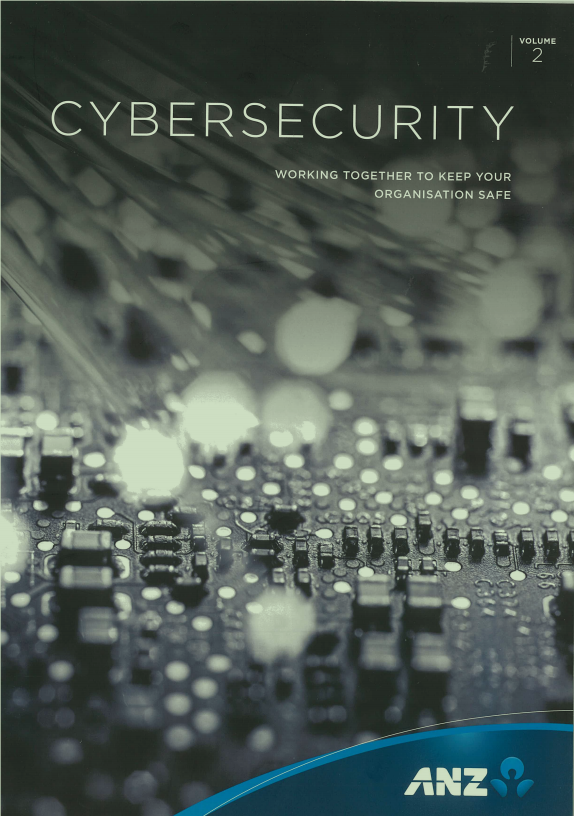
This is a suspicious document.

The image of which is shown below:

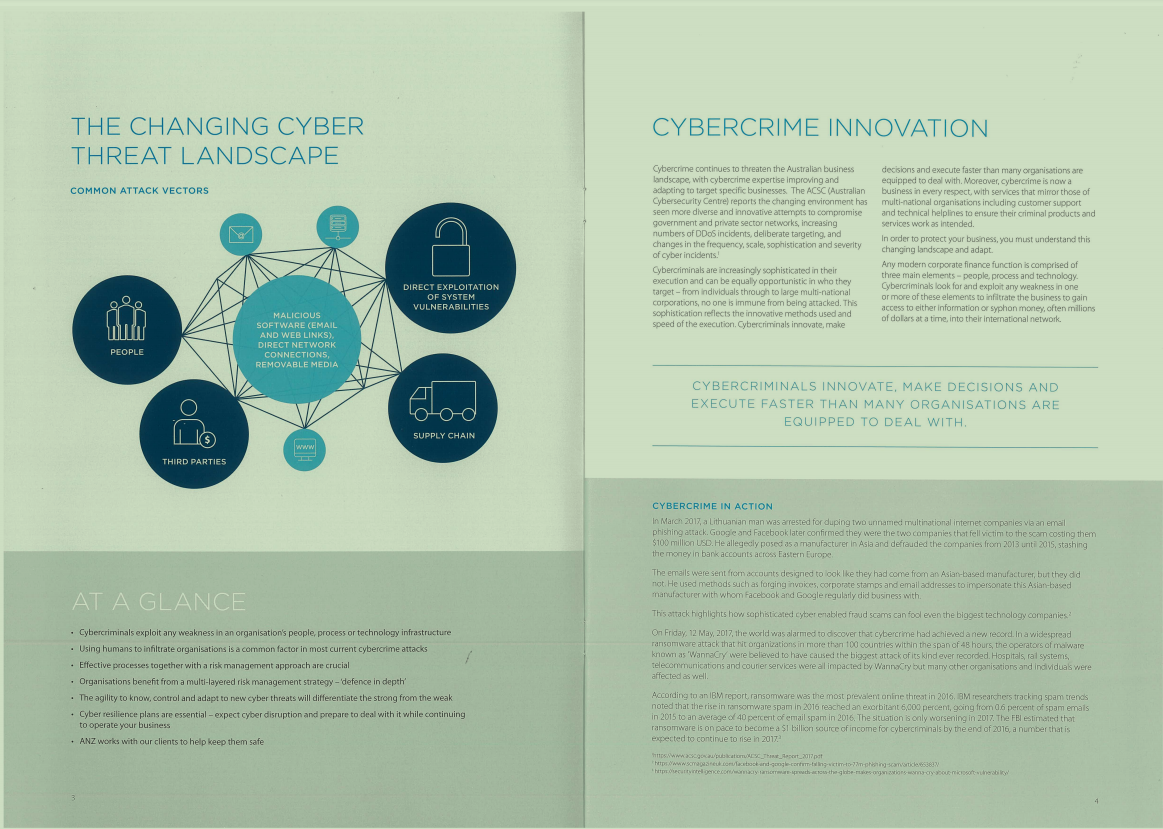


**Sub Task 4 :**

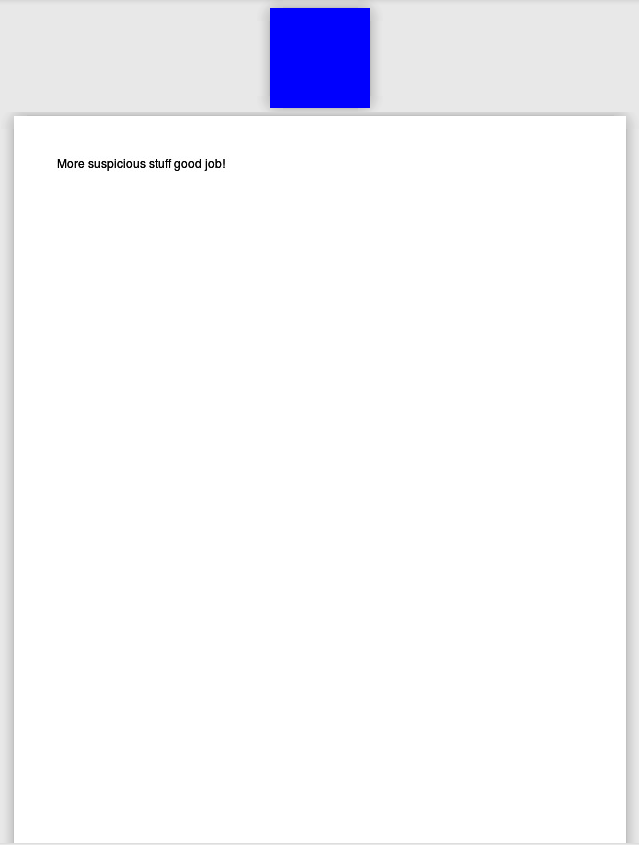
We can obtain the three pdf’s using wireshark, either by directly exporting them, or by inputting its hex signature (255044462d) and then using HxD to save as pdf. The images of the documents after obtaining them are shown below:



ANZ\_document\_1



ANZ\_document\_2



Screen Capture of evil.pdf

**Sub Task 5 :**

Included in the network stream was ‘hiddenmessage2.txt’, which when exported directly via wireshark gives out a bunch of characters in iso-8859 format.

After viewing the TCP stream, we see the plain text message contains the hex code with three jpg headers and 1 jpg footer. Ignoring the first 2 headers, and only copying the hex contents between the last header and footer we obtain the hidden image as shown below:



**Sub Task 6 :**

Directly exporting ‘atm-image’ through wireshark will give only the first image as shown below:



Opening the file’s TCP stream however, I saw that there is one more image hidden after the first image, and copying only that to HxD and saving it we obtain the hidden image:



**Sub Task 7:**

I tried to extract the image from the file ‘broken.png’ but, couldn’t as the stream was incomplete data.



(transparent anz-png)

**Sub Task 8:**

After opening the TCP stream of the ‘securepdf’ file, it is apparent that it is a file in zip format due to the iso-8859 stream showing PK.. (signature of zip).

From the ASCII we can also obtain the password of the zip which is ‘secure’.

Copying the hex from the stream to HxD and then saving the file as zip, we obtain the zip file, which when extracted with the pasword ‘secure’, gives the pdf (shown as images):

