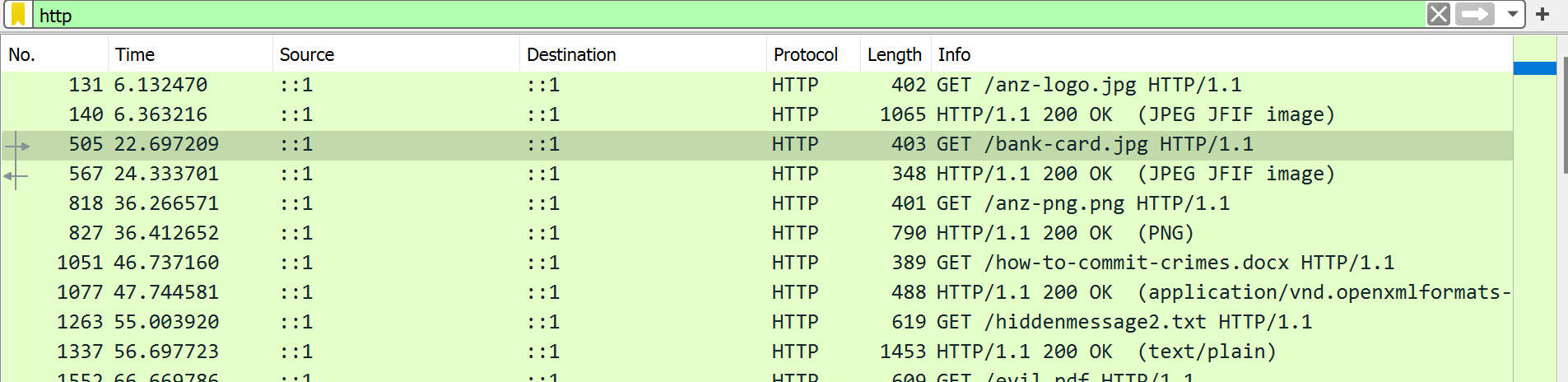
|  |
| --- |
|  |

**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.*

I have analyzed the provided packet capture (PCAP) 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.   
  
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including one for anz-logo.jpg and bank-card.jpg.

To investigate this image download further, I viewed its TCP stream to see what I could find.  
Looking through the data in the TCP stream showed that this get request actually downloaded two images separately as there are two separate files for .jpg images. We then open the raw files of the respective images and search for the .jpg files by typing in the header/footer hex value which is FFD8-FFD9.

The next step taken was carving out 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.



*Fig: anz-logo.jpeg*



*Fig: bank-card.jpeg*

**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 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.   
  
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including one for ANZ1.jpg and ANZ2.jpg

To investigate this image download further, I viewed its TCP stream to see what I could find.  
Looking through the data in the TCP stream showed that this get request actually downloaded two images separately as there are two separate files for .jpg images. We then open the raw files of the respective images and search for the .jpg files by typing in the header/footer hex value which is FFD8-FFD9.

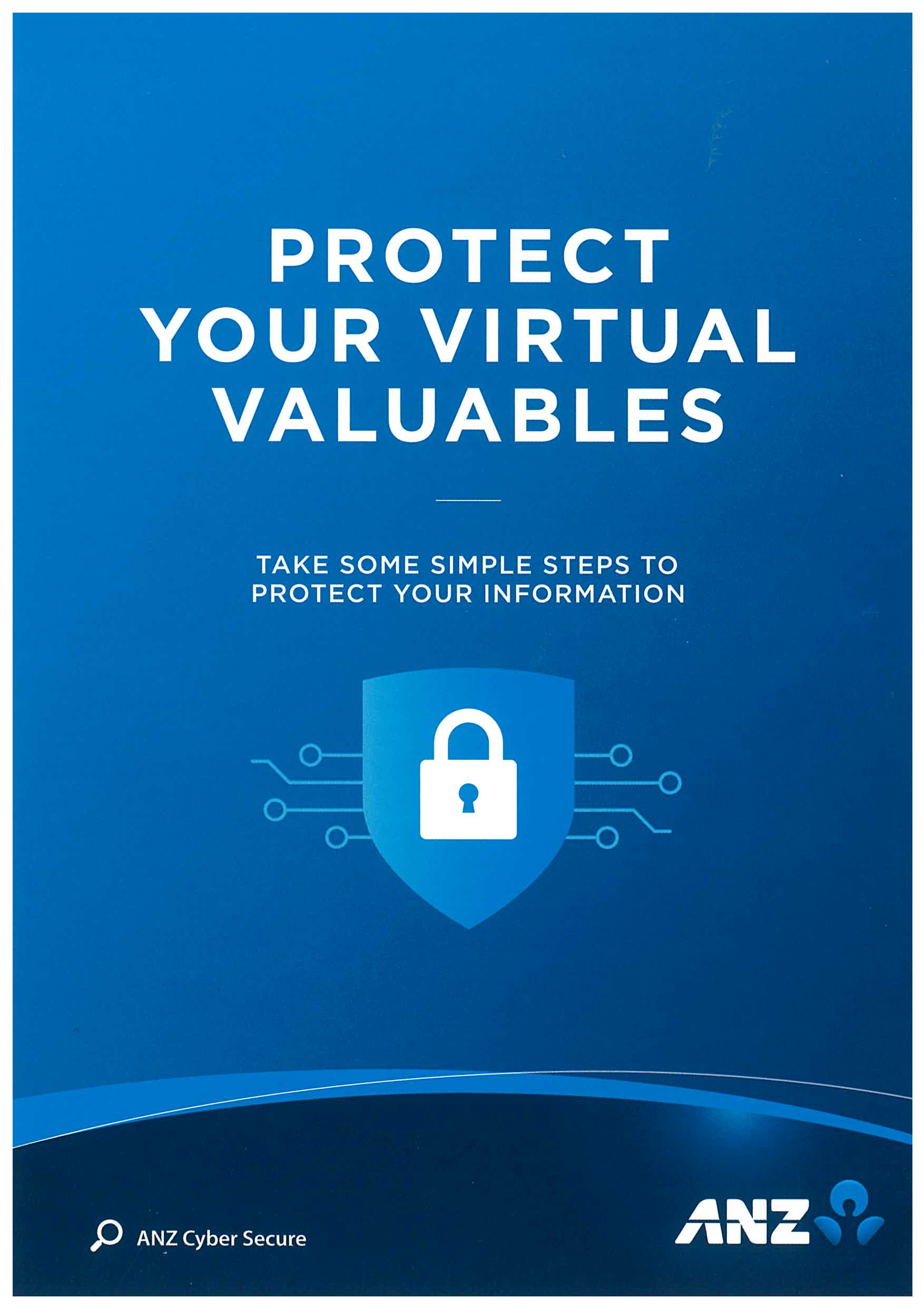
The next step taken was carving out the images from the TCP stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program HxD. I then saved the file as a jpg and opened it, resulting in the images below.

In the ASCII file of ANZ1.jpg file, when we scroll down to the end of the file, we find a hidden message stating:

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

While in the ASCII file of ANZ2.jpg file, when we scroll down to the end of the file, we find a hidden message stating:

**“You've found the hidden message! Images are sometimes more than they appear.”**

****

**

*Fig: ANZ1.jpg (resized for the report) Fig: ANZ2.jpg (resized for the report.)*

**Sub-task 3:**

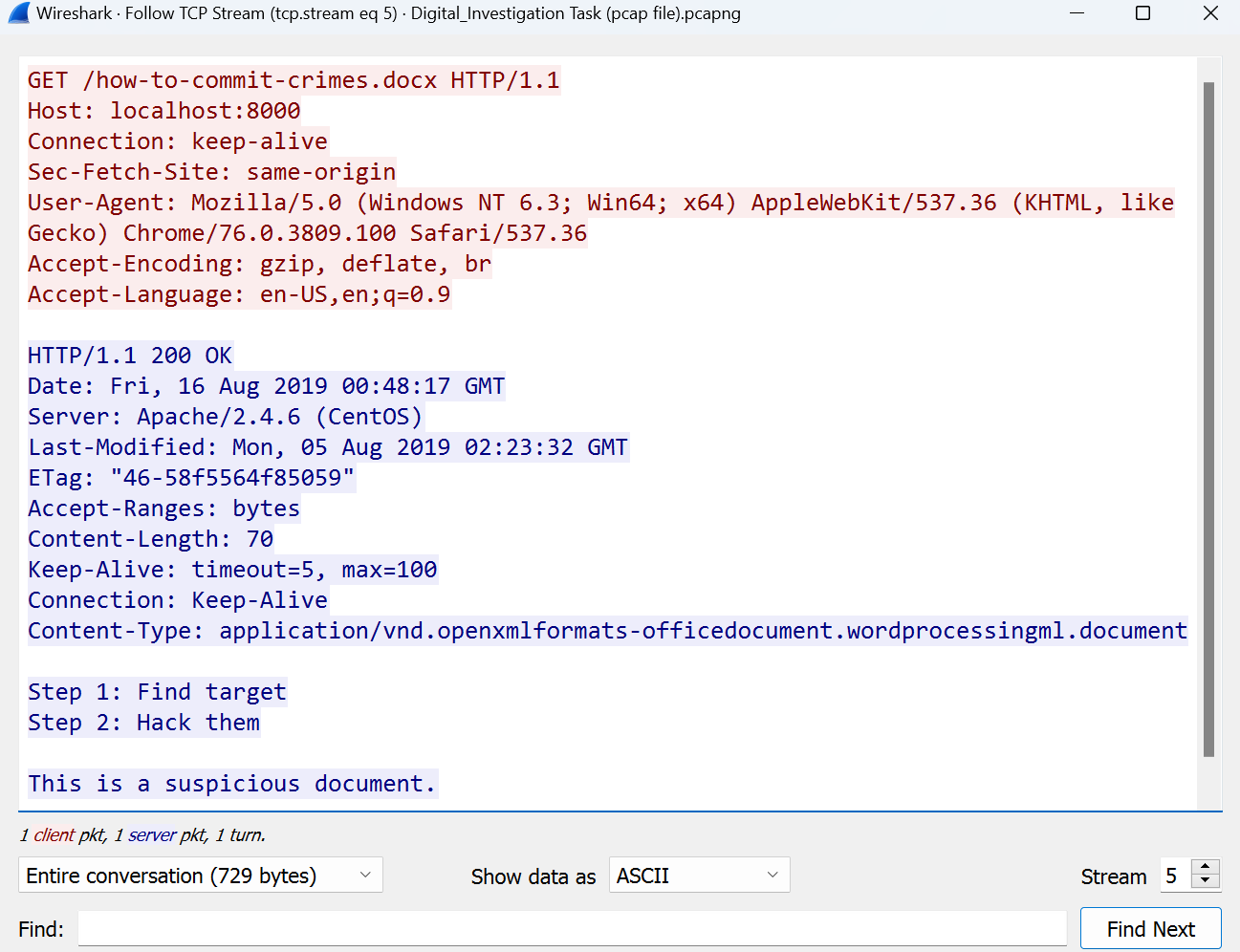
* *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
* *Find the contents of this file and include it in your report.*

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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including one for how-to-commit-crimes.docx.

To investigate this image download further, I viewed its TCP stream to see what I could find.  
Looking through the data in the TCP stream showed that this get request downloaded a suspicious document called “how-to-commit-crimes.docx”. We then open the ASCII files of the document in which we find the contents of the file written as:

1. Step 1: Find target
2. Step 2: Hack them

This is a suspicious document.



*Fig: ASCII view of “how-to-commit-crimes.docx” file*

**Sub-task 4:**

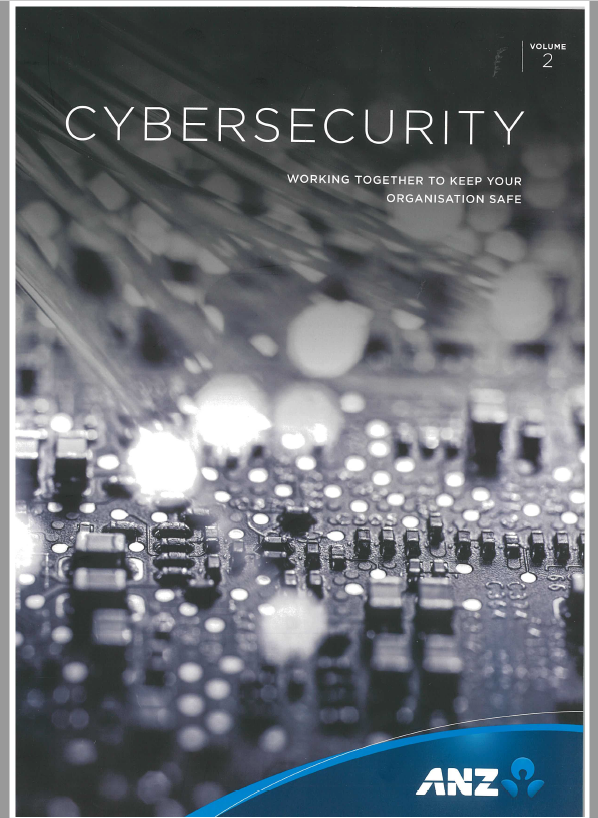
* *The user accessed 3 pdf documents:* *ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf*
* *Extract and view these documents. Include images of them in your report.*

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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including the ones for ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf.

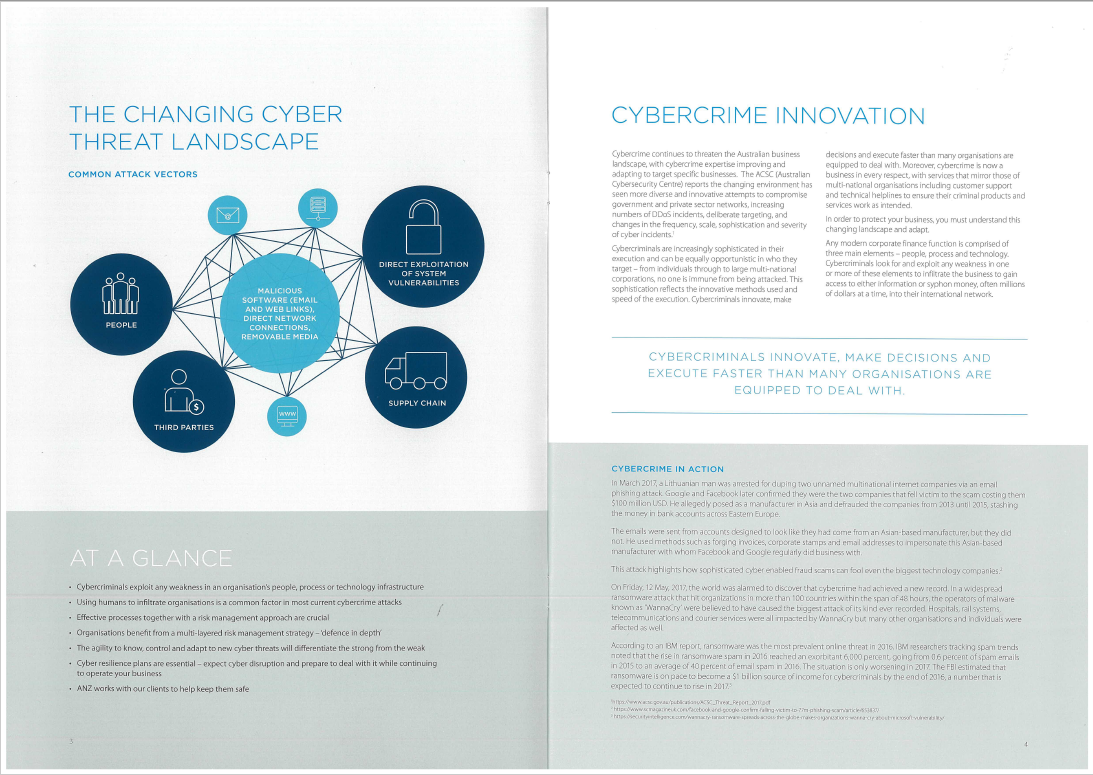
To investigate this image download further, I viewed its TCP stream of each file separately to see what I could find. Looking through the data in the TCP stream showed that the user accessed all three suspicious PDFs. We then move onto the Hex view of files one at a time and type in the file signature value of PDF file in the Find dialogue box which is “25 50 44 46”. We copy the Hex data all the way to the end of the file. The copied data is then copied into the HxD 64 editor and is saved as a pdf file.

The above procedure is repeated for the other two succeeding files.

The images of the extracted PDF files are attached below

**

*Fig: Image of ANZ\_Document.pdf*

**

*Fig: Image of ANZ\_Document2.pdf*

**

*Fig: Image of evil.pdf*

**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 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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including hiddenmessage2.txt.

When I looked at the TCP stream of this file, I saw that it contained encoded data rather than plain text, and when I looked at it as hex, it had the same file signature as a jpg image. I followed the same procedure of extracting a .jpg file as in the above subtasks.

The text file turned out to be this image (resized) after I copied and saved the hex data using HxD like I had done for other images.



*Fig: hiddenmessage.txt extracted 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.*

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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including atm-image.jpg.

When I looked at the TCP stream of this file, I saw that it contained hex values of two sets of .jpg files rather than one. I followed the same procedure of extracting a .jpg file as in the above subtasks.

The following two images (resized) were extracted from atm-image.jpg, after I copied and saved the hex data using HxD like I had done for other images.

*Fig: Images extracted from atm-image.jpg*

**Sub-task 7:**

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

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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including broken.png.

When I looked at the TCP stream of this file, I saw that it There was no file signature for a png image in the TCP stream for the broken.png transmission. So, while looking at the data in its ascii form, I realised that it had been base64 encoded. I pasted the png image data into the "decoded text" part of HxD and saved it as a png file after using a web tool to decrypt the base64.

**

*Fig: Image extracted from broken.png*

**Sub-task 8:**

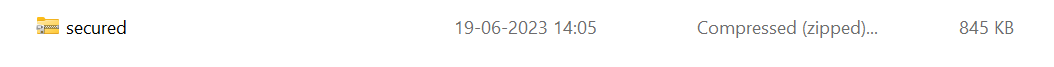
* *The user accessed one more document called securepdf.pdf*
* *Access this document include an image of the pdf in your report. Detail the steps to access it.*

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.   
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including securepdf.pdf.

Upon investigating the hex data it was found that securepdf.pdf was:

1. There was no PDF-compatible data there.
2. The hidden message "Password is "secure" was written at the bottom of the file.
3. It had a zip file's file signature, indicating that what the user had downloaded was in fact a zip file.

I then copied the zip file's hex into HxD and saved it there. When I opened the zip file, I discovered a PDF file named rawpdf.pdf within. The document requested a password when it was opened. The PDF opened after the password "secure" displayed in the TCP stream was successful. It was the first two pages of an instruction manual for online banking.







*Fig: PDF extracted from securepdf.pdf zip file.*