Packet Capture Analysis:

I have analysed the provided packet capture file using Wireshark.
I filtered the network traffic to only see HTTP requests information. This allowed me to see http GET requests.

Sub-task 1:

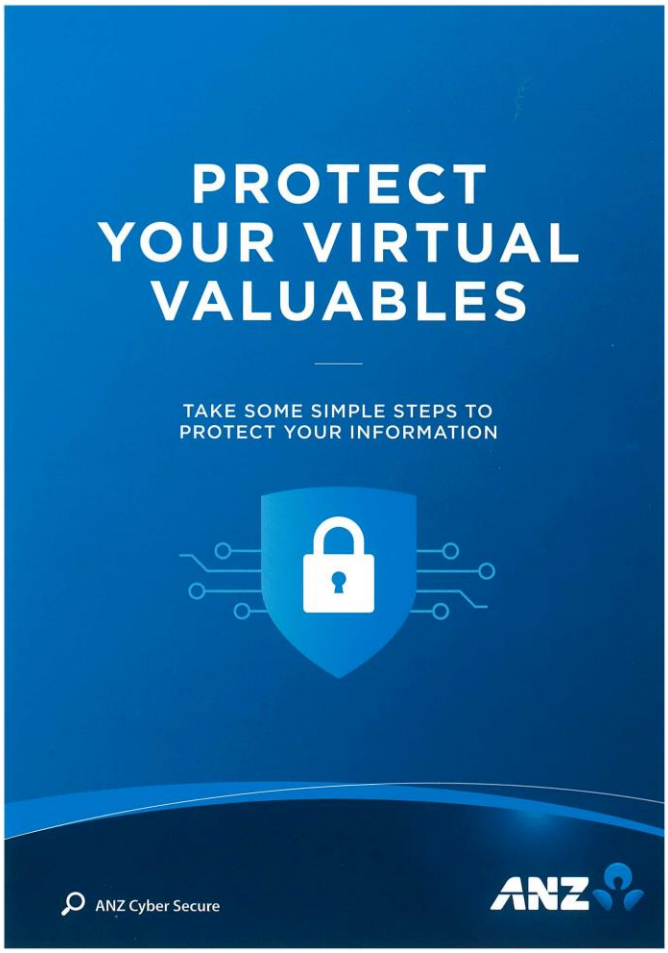
anz-logo.jpg and bank-card.jpg are two images that show up in the users network traffic, I viewed the TCP stream of the images.
The data there contained header for jpeg , which is FFD8.
I viewed the data in raw format and copied all the data between ffd8-ffd9.
Then I saved the copied into HxD and saved them in .jpeg format to obtain both the images.

Anz-logo.jpg

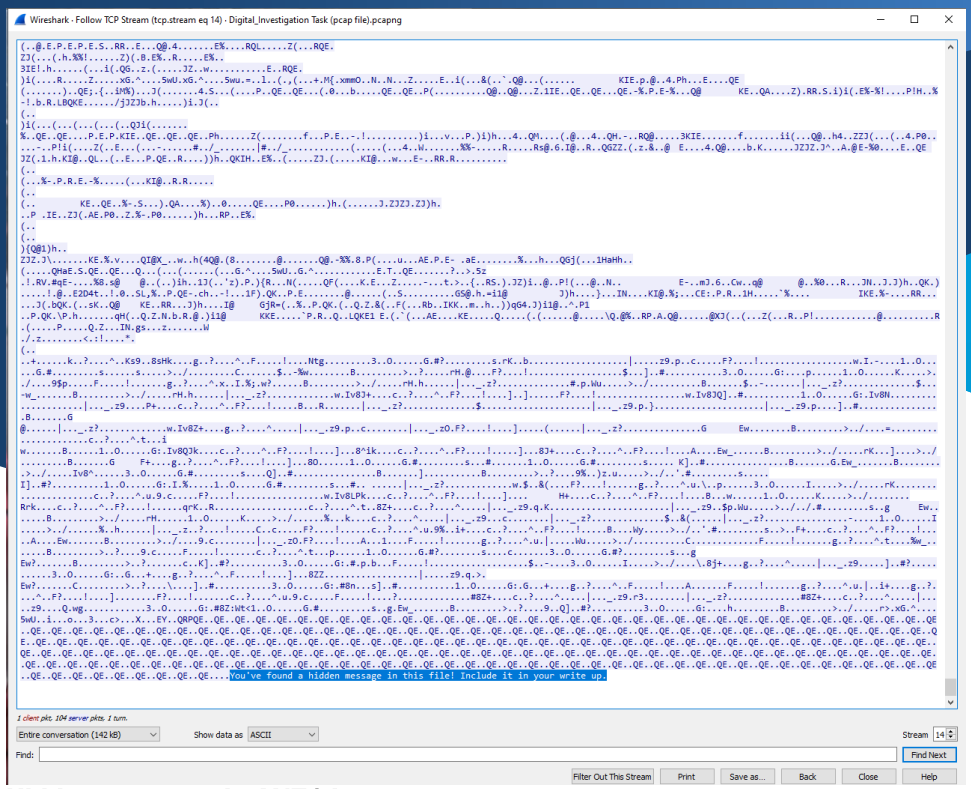
Bank-card.jpg

Sub-task 2:

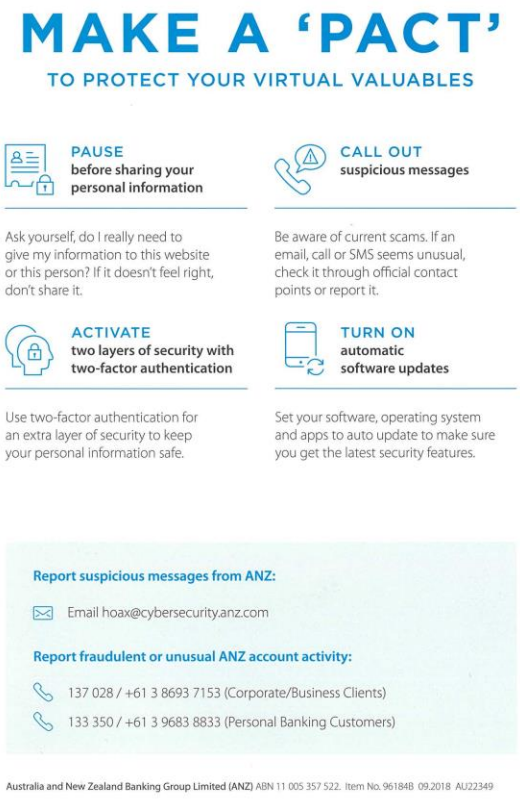
Upon viewing the TCP stream of the two imgaes ANZ1.jpg and ANZ2.jpg in ASCII format, I found that there is a hidden message at the bottom for both the files.
The hidden message in ANZ1.jpg was "You've found a hidden message in this file! Include it in your write up."
The hidden message in ANZ2.jpg was "You've found the hidden message! Images are sometimes more than they appear."
Then I viewed the data in raw format and copied everything between ffd8-ffd9 and saved it in HxD in .jpeg format to extract both the images.



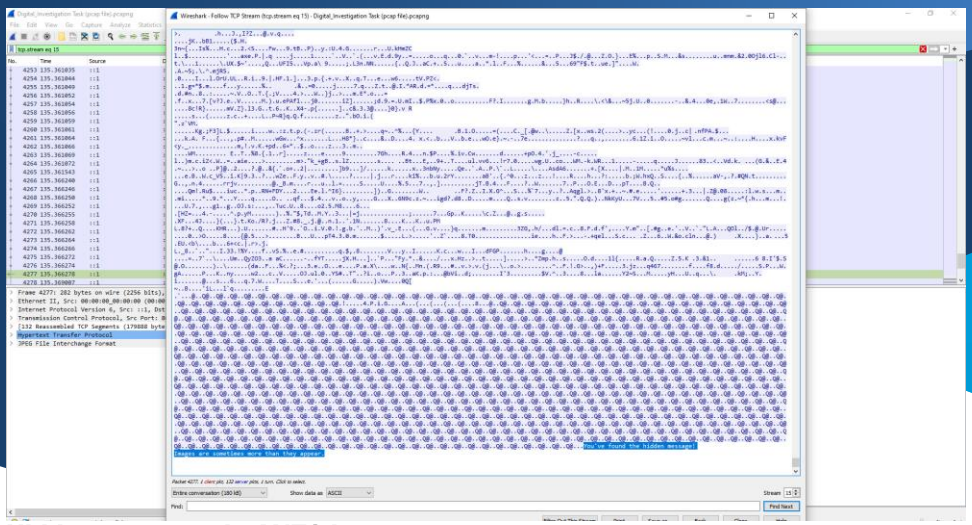
ANZ1.jpg



Hidden message in ANZ1.jpg



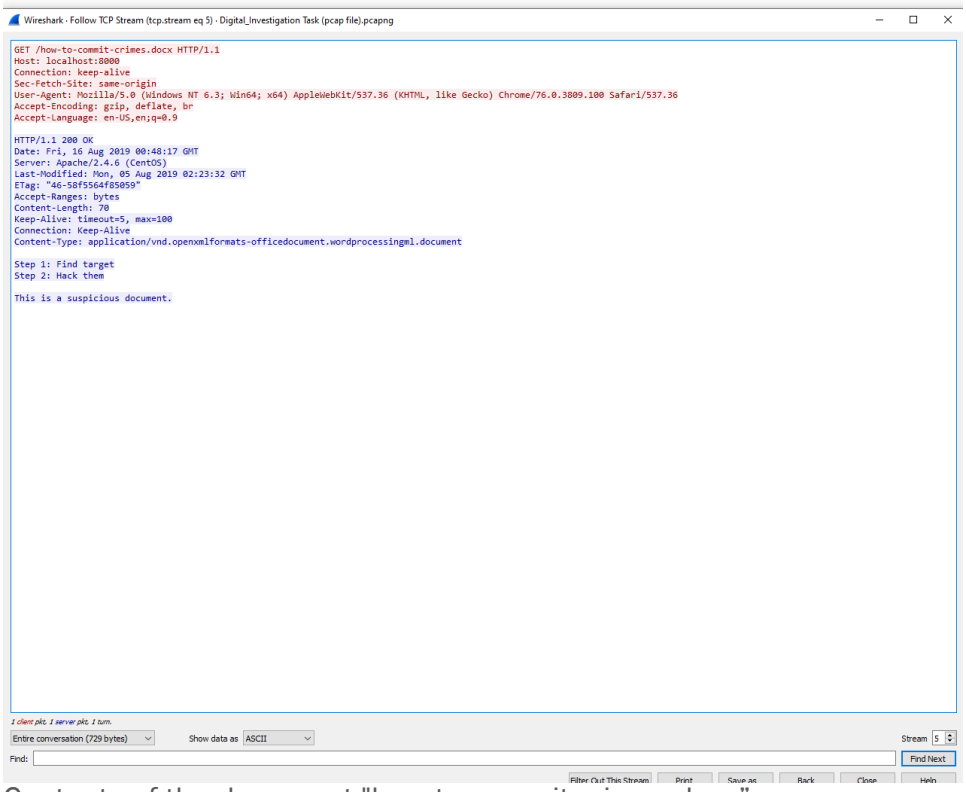
ANZ2.jpg



Hidden message in ANZ2.jpg

Sub-task 3:

Upon viewing the TCP stream of the document “how-to-commit-crimes.docx” in ASCII format, I was able to see the contents of the document.



Contents of the document "how-to-commit-crimes.docx”

Sub-task 4:

I opened the TCP stream of the three PDF’s ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf and found out that the file signature was for a pdf, which is “25 50 44 46”.
I copied all the hex data from the file signature onwards and saved it in .pdf format in HxD.

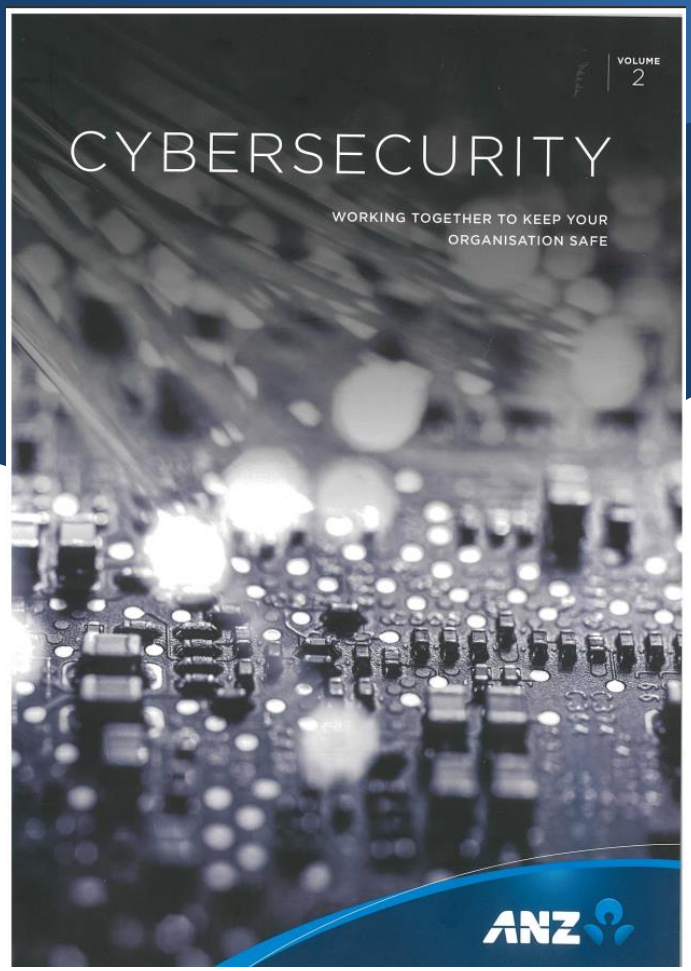


Image of ANZ_document.pdf

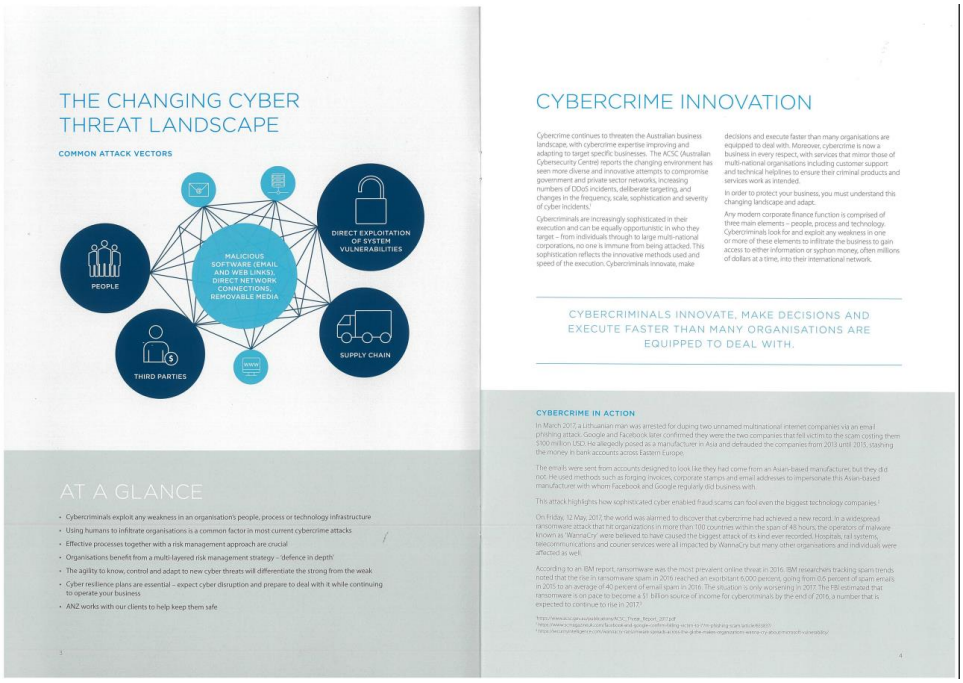


Image of ANZ_document2.pdf

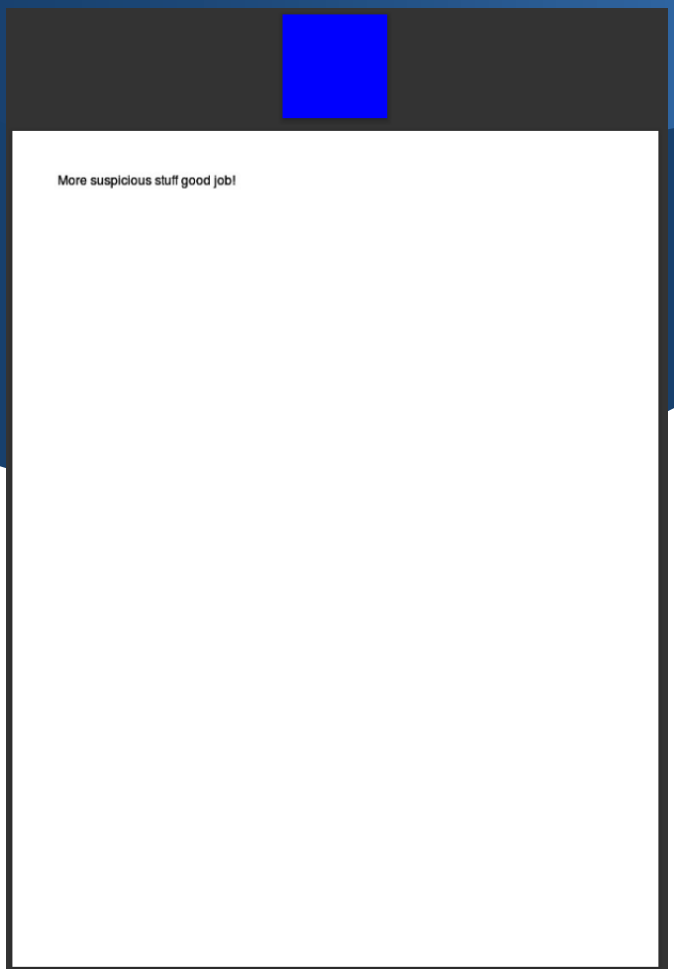
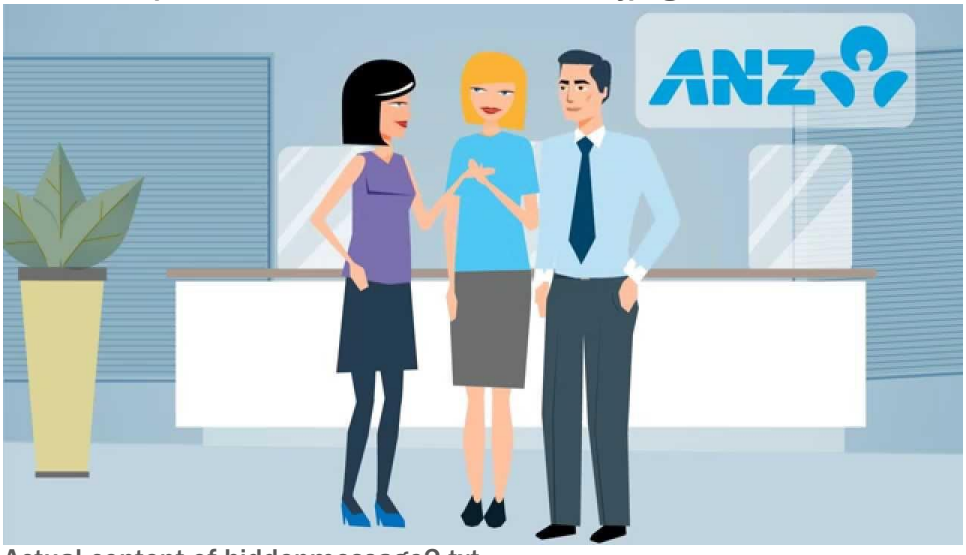


Image of evil.pdf

Sub-task 5:

I opened the TCP stream for "hiddenmessage2.txt" and viewed it as hex. I found out that the file signature is same as that of a jpeg file.So, the text file"hiddenmessage2.txt" was actually an image. Hence, I copied and saved the data in HxD in jpeg format.



Actual content of hiddenmessage2.txt

Sub-task 6:

I opened the TCP stream for "atm-image.jpg" and found out that there are two sets of file signature same as that of a jpeg file.
I opened the TCP stream in raw format and tried extracting both sets of data and I was able to get two different images.

1st Image

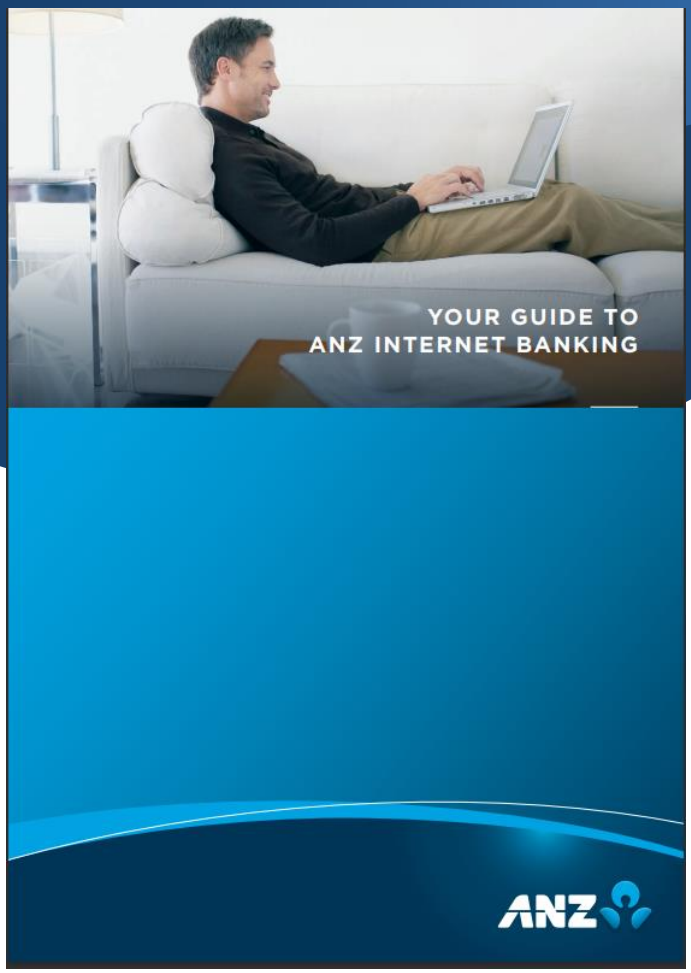
2nd Image

Sub-task 7:

Upon viewing the TCP stream for "broken.png" in raw format, I discovered that the file signature was “80 50 4e 47 0d 0a” which is the file signature for a png.
I copied everything following that signature and saved it in .png format in HxD editor to obtain the image.

Sub-task 8:

I opened the TCP stream for "securepdf.pdf" in ASCII format and found out that at the bottom there was a message "Password is Secure". This indicated that the file was actually a ZIP file.
So, I opened the data in raw format and found the file signature for a ZIP file which is "504B0304".
Hence , I copied everything following that signature and saved it in .rar format in HxD editor.
After extracting the ZIP file using the password "Secure", I was able to extract the content of the zip file file which was a pdf containing two pages.



1st page of the extracted pdf

TABLE OF CONTENTS

2nd page of the extracted pdf