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.*

To find the images the user accessed called anz-logo.jpg and bank-card.jpg I followed the following process for both images:

First I filtered the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image. I then right clicked the image and followed its TCP stream.
In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the view to 'raw', and then searched the hex data for a jpeg's file signature.

After finding the file signature "FFD8" the top, and the file footer "FFD9" at the bottom, I copied everything between those two points into the hex editor HxD and saved it as a jpg image.

This was the image I found for anz-logo.jpg:

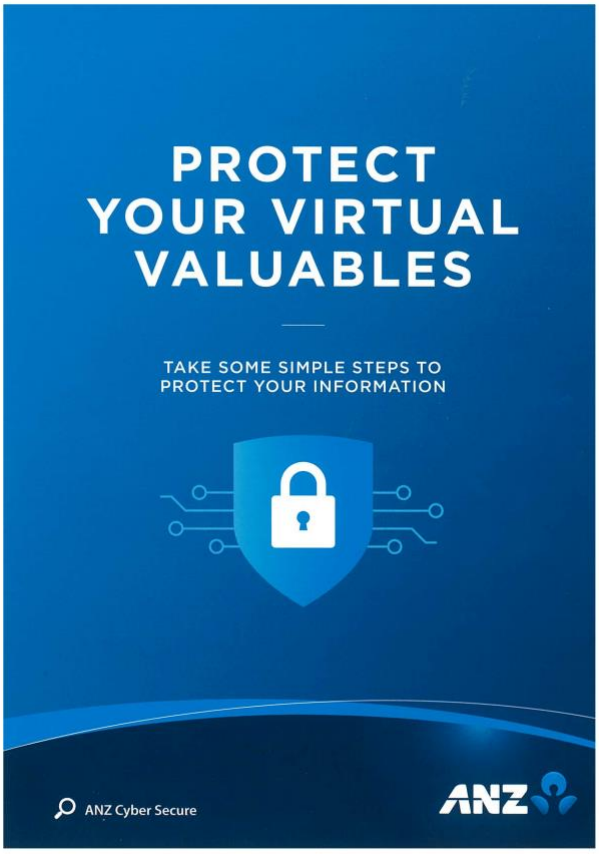
This was the image I found for bank-card.jpg:


**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.

The image for ANZ1.jpg (Resized for report):




The difference in the network traffic for this images download I discovered was a hidden message in the data after the end of the image.

The message said “You've found a hidden message in this file! Include it in your write up.”

The image for ANZ2 (also resized):


This network traffic also had a message hidden in the same way.

It was “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.

The full document contained the message:
"Step 1: Find target
Step 2: Hack them

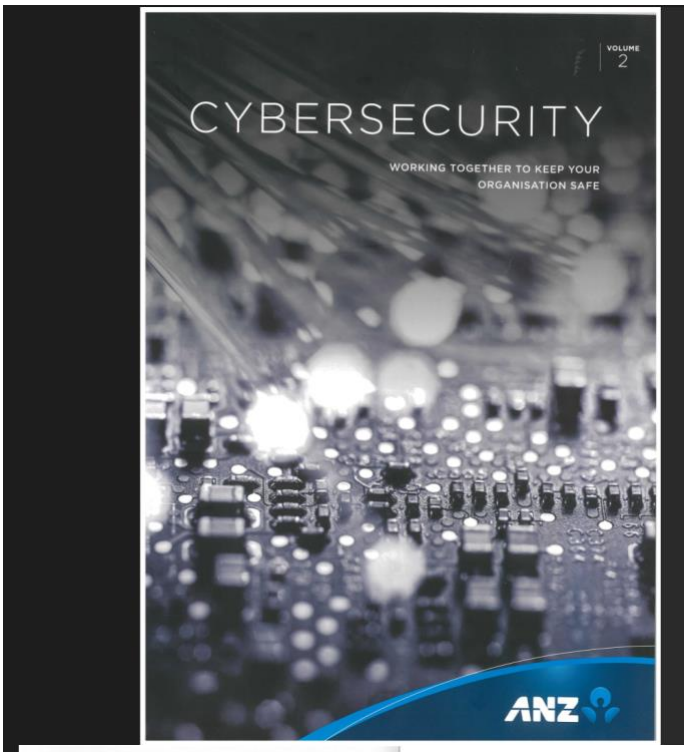
This is a suspicious document.
"

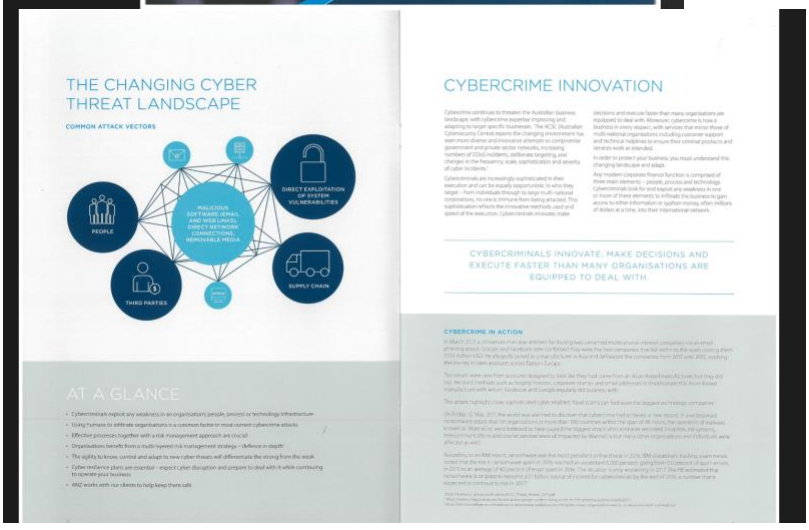
**Sub-task 4:**

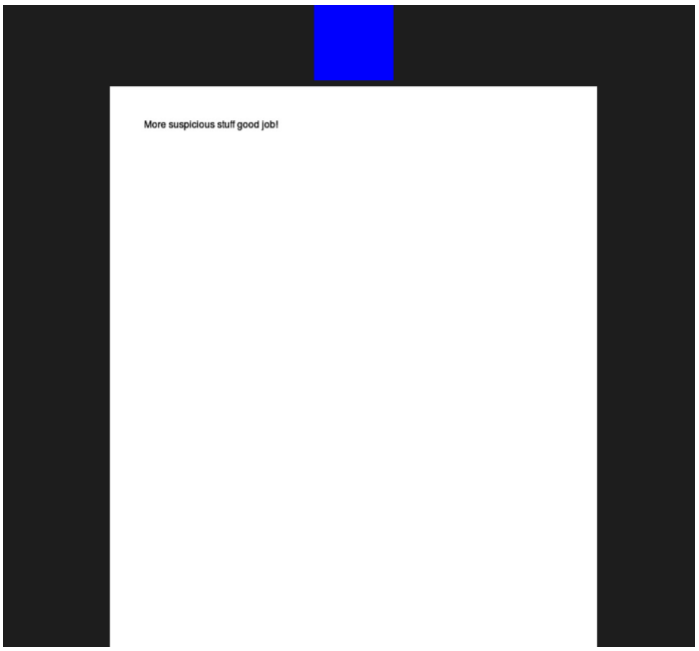
- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *Extract and view these documents. Include images of them in your report.*

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.

The same process worked for all three files:


VOLUME
2
CYBERSECURITY
WORKING TOGETHER TO KEEP YOUR ORGANISATION SAFE
ANZ


THE CHANGING CYBER THREAT LANDSCAPE
COMMON ATTACK VECTORS
PEOPLE
DIRECT EXPLOITATION OF SYSTEM VULNERABILITIES
THIRD PARTIES
SUPPLY CHAIN
AT A GLANCE
CYBERCRIME INNOVATION
CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.
CYBERCRIME IN ACTION




**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 (resized):


**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 viewed the TCP stream as normal when investigating this traffic, and found two sets of jpeg file signatures instead of one like in the previous tasks.
I tried extracting both sets of data, and got two different images.

The first image:

The second image:


So the thing that is different about this traffic is that a single GET request performed by the user downloaded two images.

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.

That resulted in this image:

Sub-task 8:

- *The user accessed one more document called securepdf.pdf*
- *Access this document and 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.


YOUR GUIDE TO
ANZ INTERNET BANKING
TABLE OF CONTENTS
Why use ANZ Internet Banking? 3
Online Security 4
Getting started 5
Viewing your accounts 6
Transferring funds 7
Check the details before you pay 8
Your transfer receipt 9
Paying bills 10
Using Pay Anyone 11
International Money Transfers 12
Logging Off 13
Things you need to know 14
Frequently asked questions 15
2