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.*

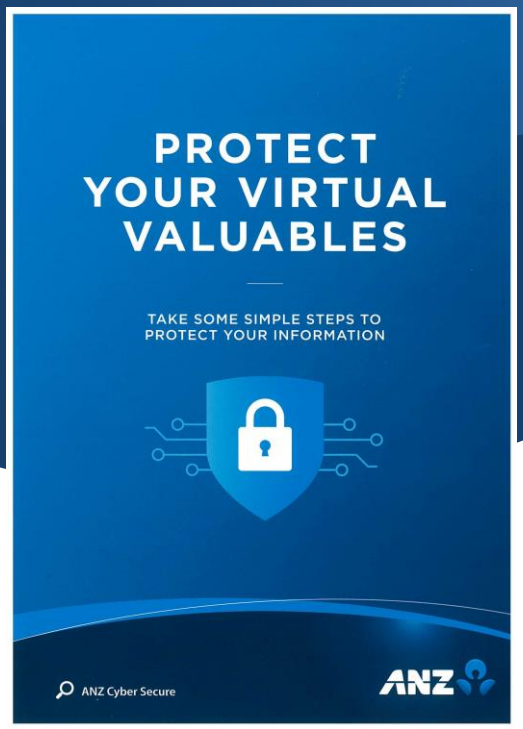
First I filtered the packets using http and look for GET request, right click and follow TCP stream. Apply the filter to RAW from ASCII. Search for"FFD8". Copy the line starting with ffd8 till ffd9. Now open the HxD app and save the file as jpg.

anz-logo.jpg

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.*



anz1.jpg

anz2.jpg

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.*

```
GET /how-to-commit-crimes.docx HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:48:17 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 05 Aug 2019 02:23:32 GMT
ETag: "46-58f5564f85059"
Accept-Ranges: bytes
Content-Length: 70
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

Step 1: Find target
Step 2: Hack them

This is a suspicious document.
```

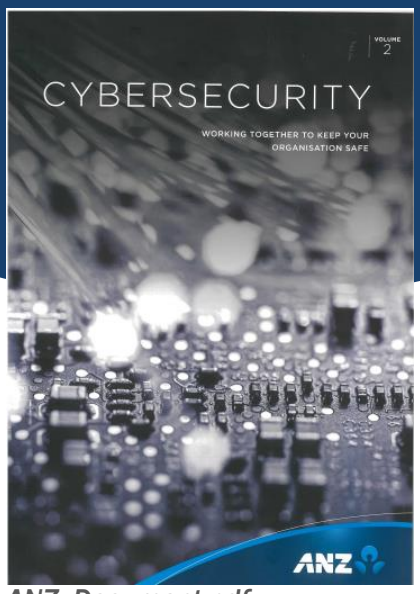
Step 1: Find target
Step 2: Hack them
This is a suspicious file

Sub-task 4:

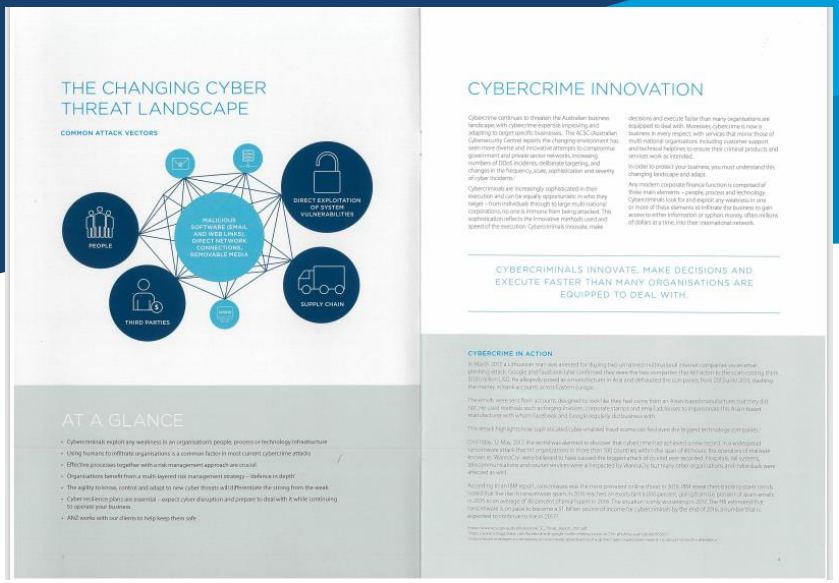
- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *Extract and view these documents. Include images of them in your report.*

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:



ANZ_Document.pdf



ANZ_Document2.pdf

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 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

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.*

Image1:

Image2:

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

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.*

  At the end of packet there is a line “password is secure “meaning that the file is not a pdf but a zip. Find the file signature for a zip file and then save in hex-editor. Open the zip file with the given password to get a 2 page pdf