|  |
| --- |
|  |

**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.*

*I filtered HTTP traffic in Wireshark to locate GET requests for the images. By following the TCP stream, I identified the JPEG file signatures (FFD8 header and FFD9 footer). I copied the hex data between these markers and saved it as JPG using HxD.*

**

**

**Sub-task 2:**

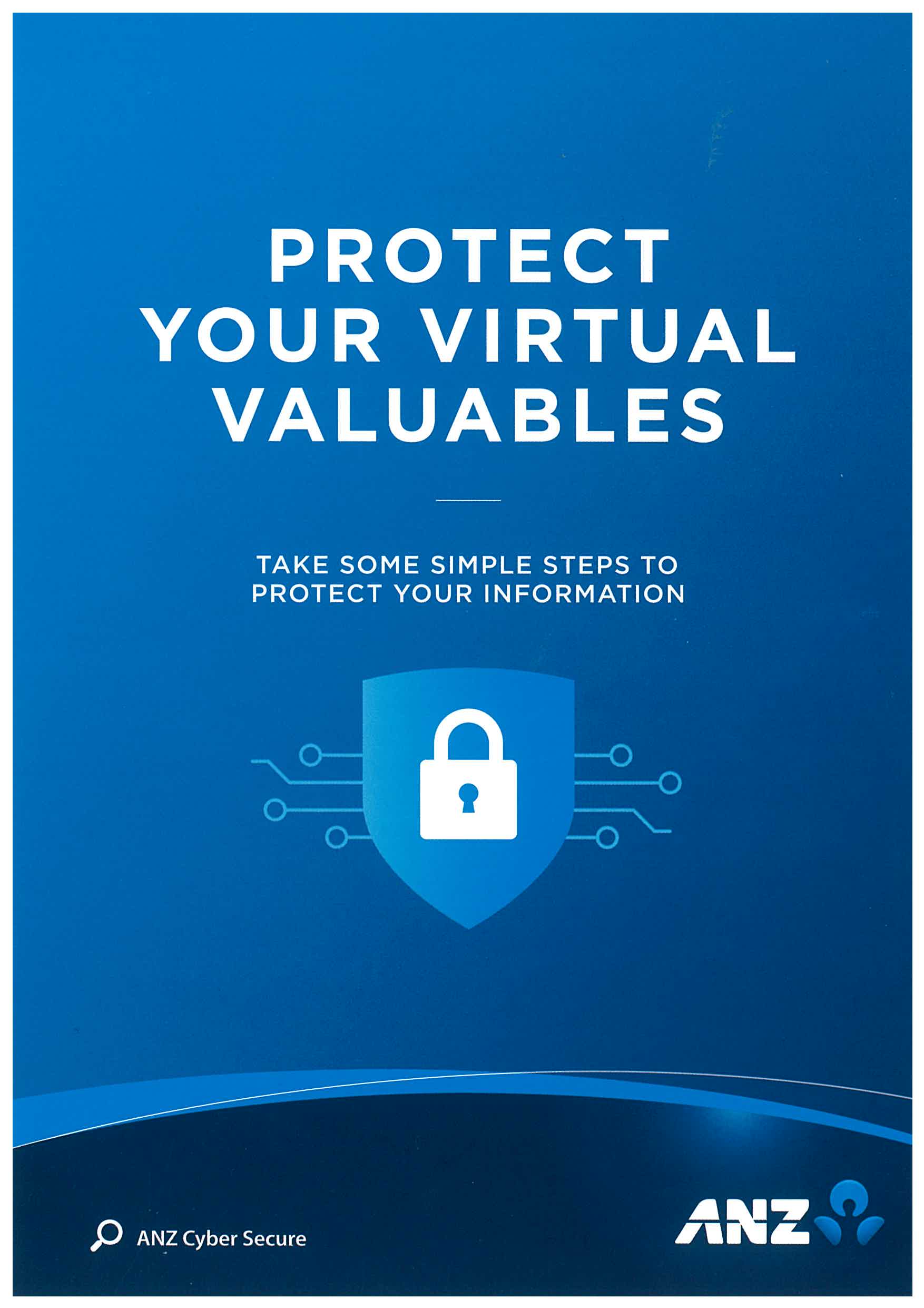
* *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
* *Extract the images, include them and mention what is different about them in your report.*

*I repeated the same extraction process as Sub-task 1.*

*ON ANZ1:*

*The image included a hidden message:*

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

**

*FOR ANZ2.jpg*

*The image also included a hidden message:*

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

**

**Sub-task 3:**

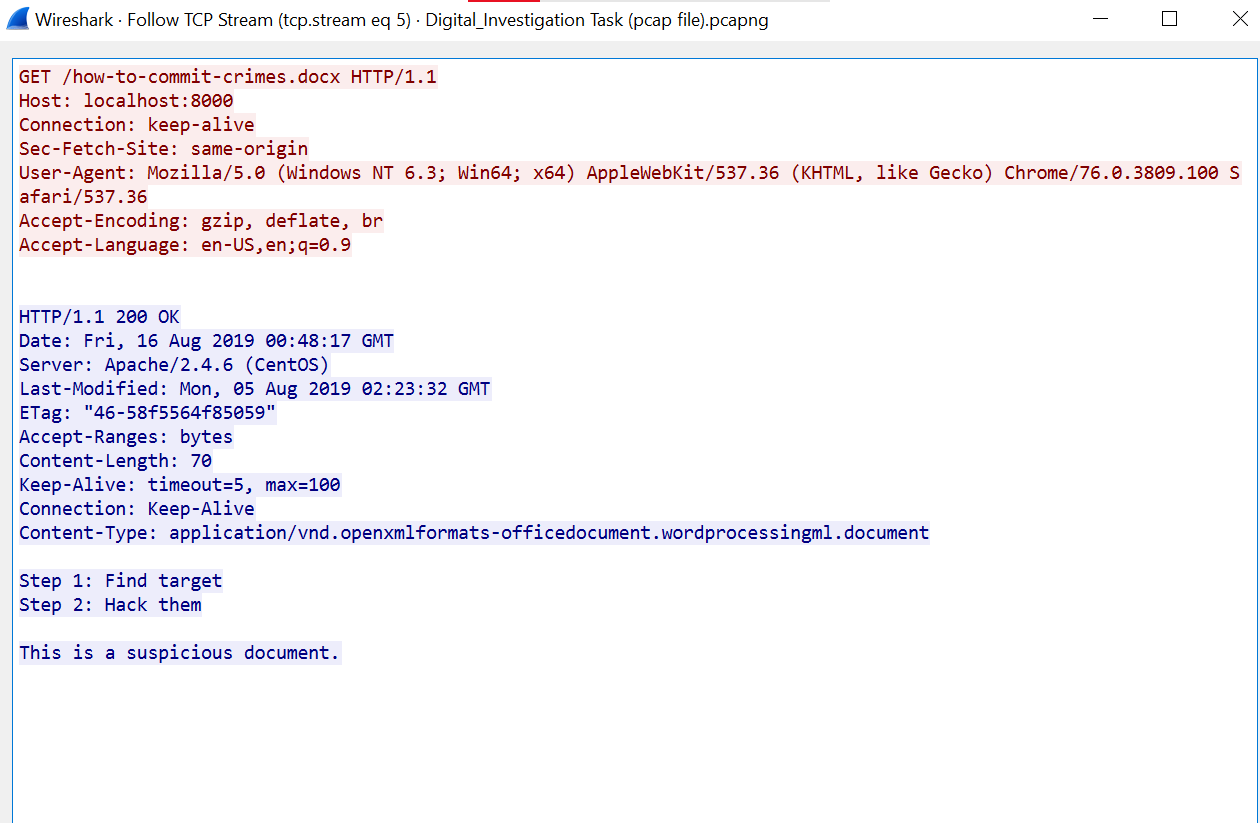
* *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
* *Find the contents of this file and include it in your report.*

*I analyzed the TCP stream for how-to-commit-crimes.docx. The HTTP request showed a user agent for Chrome on Windows. The document’s plaintext content included (in ASCII mode) :*

*Step 1: Find target*

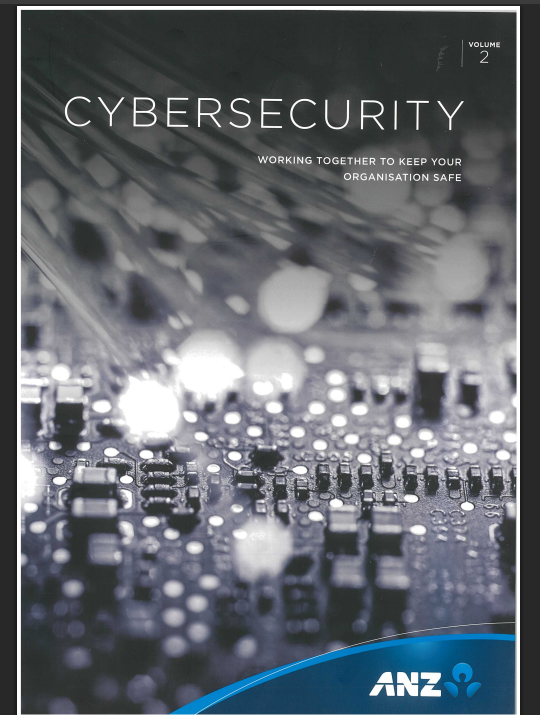
*Step 2: Hack them*

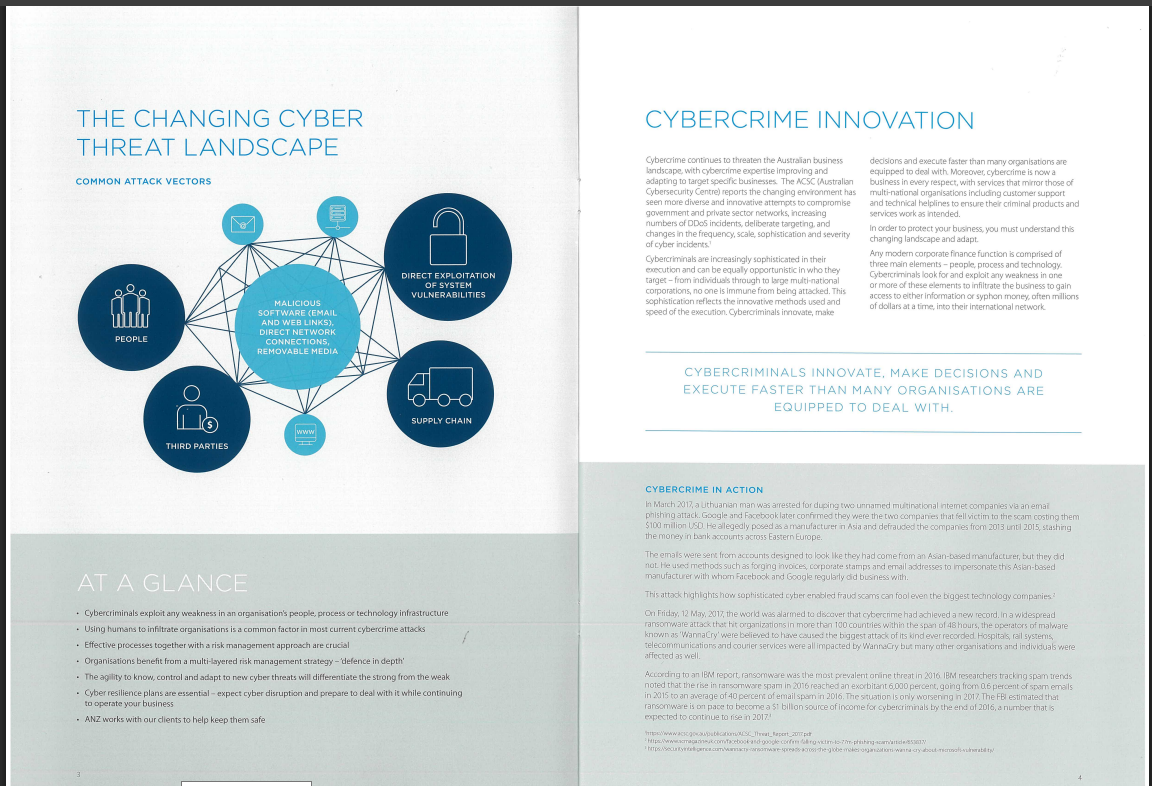
*This is a suspicious document*

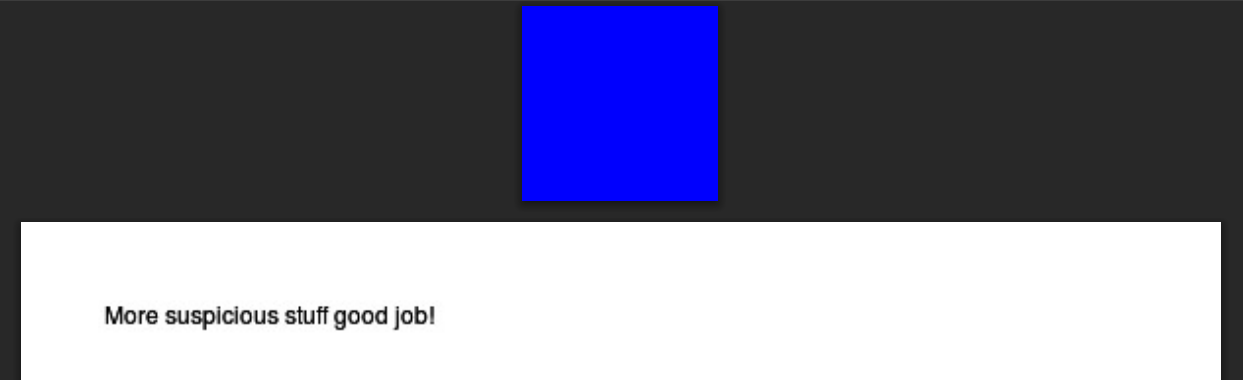


**Sub-task 4:**

* *The user accessed 3 pdf documents: ANZ\_Document1.pdf, ANZ\_Document2.pdf, evil.pdf*
* *Extract and view these documents. Include images of them in your report.*

**

**

**

*I searched for PDF signatures (25 50 44 46) in hex data. Copying from the signature to the end of the stream, I saved three files: ANZ\_document.pdf, ANZ\_document2.pdf, and 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*

*A file initially appearing as text contained JPEG hex signatures. Saving it as a JPG revealed hidden image content, showing how files can mask their true formats.*

**

**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.*

*A single GET request contained two JPEG signatures. Extracting both gave two images: one ANZ-related and another sourced from shutterstock.com (ID: 567329461).*

**

**

*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.*

*To find the images the user accessed called broken.png 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 “89 50 4e 47 0d 0a 1a 0a” I copied everything after that point to end and then copy into the hex editor HxD and saved it as a png image*

**

**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.*

**After investigating TCP stream for securepdf.pdf I discover following thing: 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 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**

****