**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 locate the images "anz-logo.jpg" and "bank-card.jpg" that the user accessed, I followed a systematic process for both images:

Initially, I filtered the packet capture specifically for HTTP traffic, narrowing down the search to focus on relevant data. Within the remaining packets, I scanned for the specific GET request responsible for fetching each image. Upon locating the relevant packet, I right-clicked on the image and proceeded to examine its TCP stream.

Within the TCP stream, I encountered what appeared to be image data. To further analyze the data, I adjusted the view to "raw," enabling me to inspect the hexadecimal representation of the image. My objective was to identify the JPEG file signature within the hexadecimal data.

Upon successfully identifying the JPEG file signature markers, namely "FFD8" at the beginning and "FFD9" at the end, I isolated the hexadecimal data corresponding to the image content. Utilizing a hex editor software like HxD, I extracted the segment between these markers and saved it as a JPG image file.

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

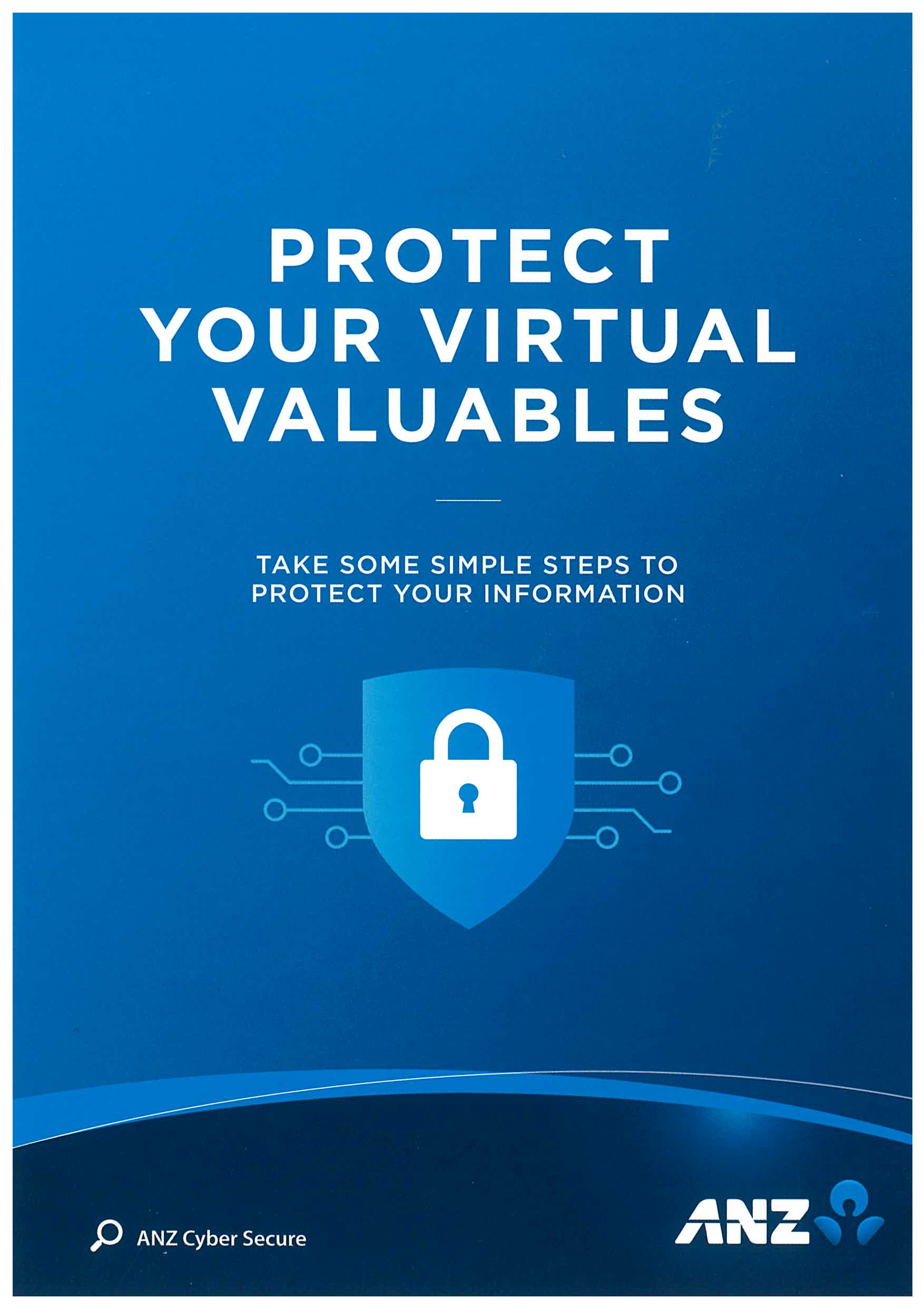


This is the image I found for bank-card.jpg:



**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 **

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   
  
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

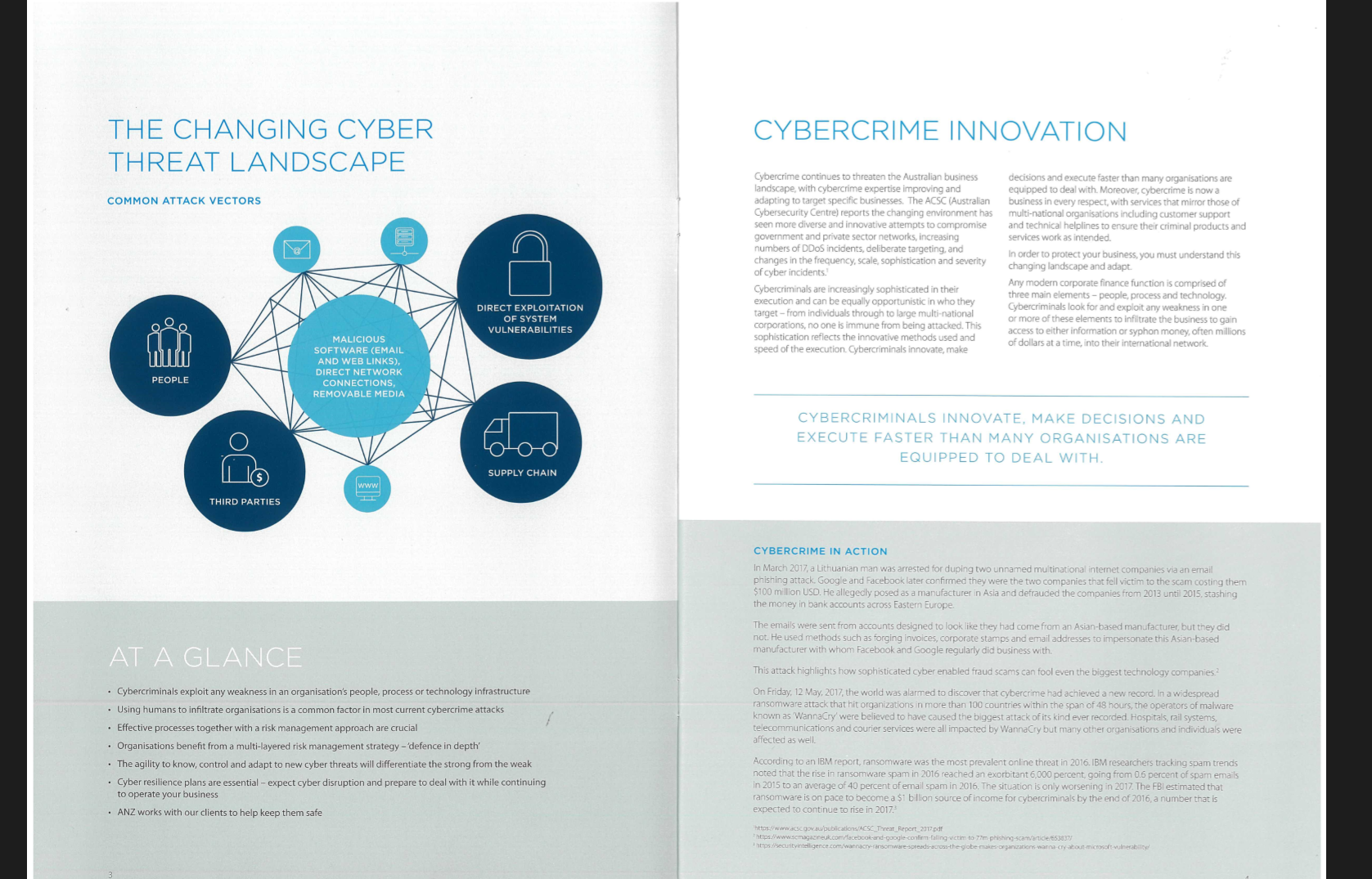
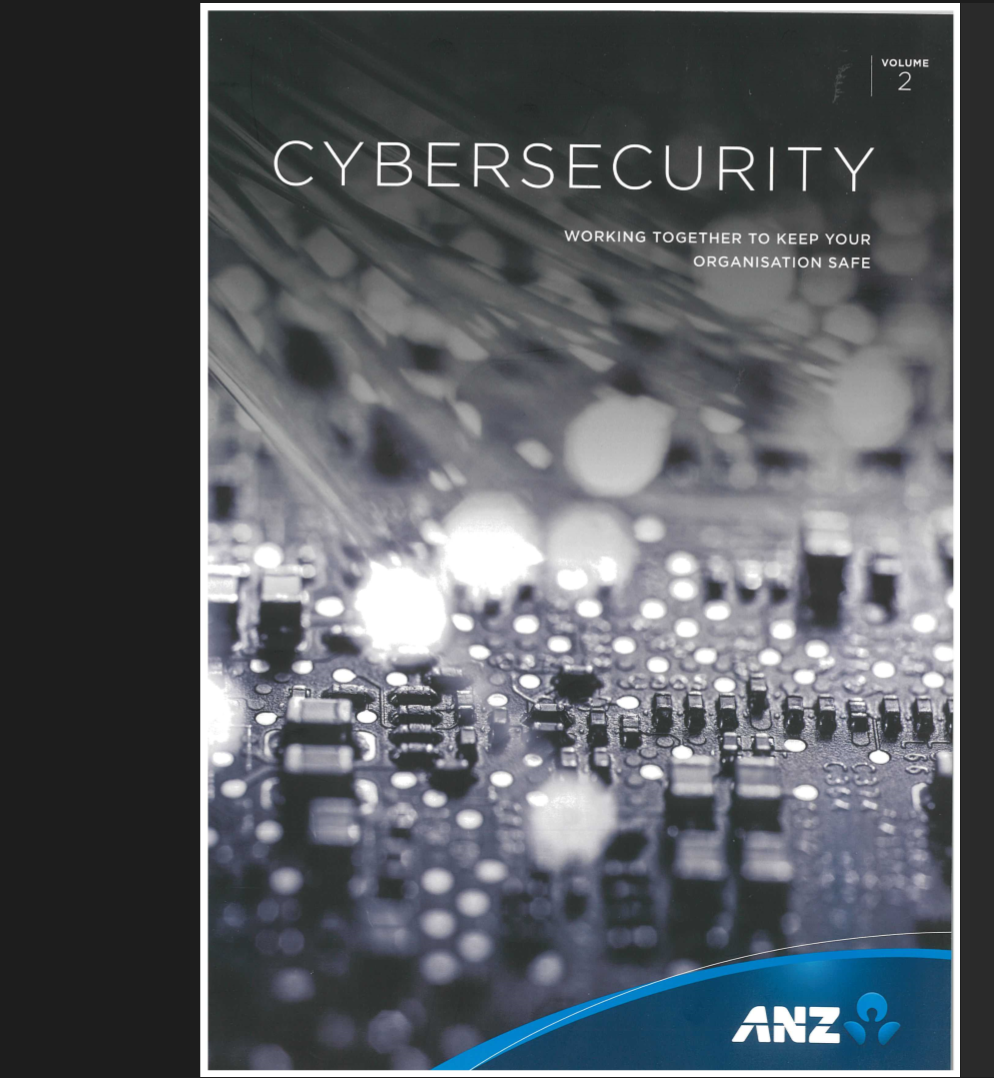
This is a suspicious document.

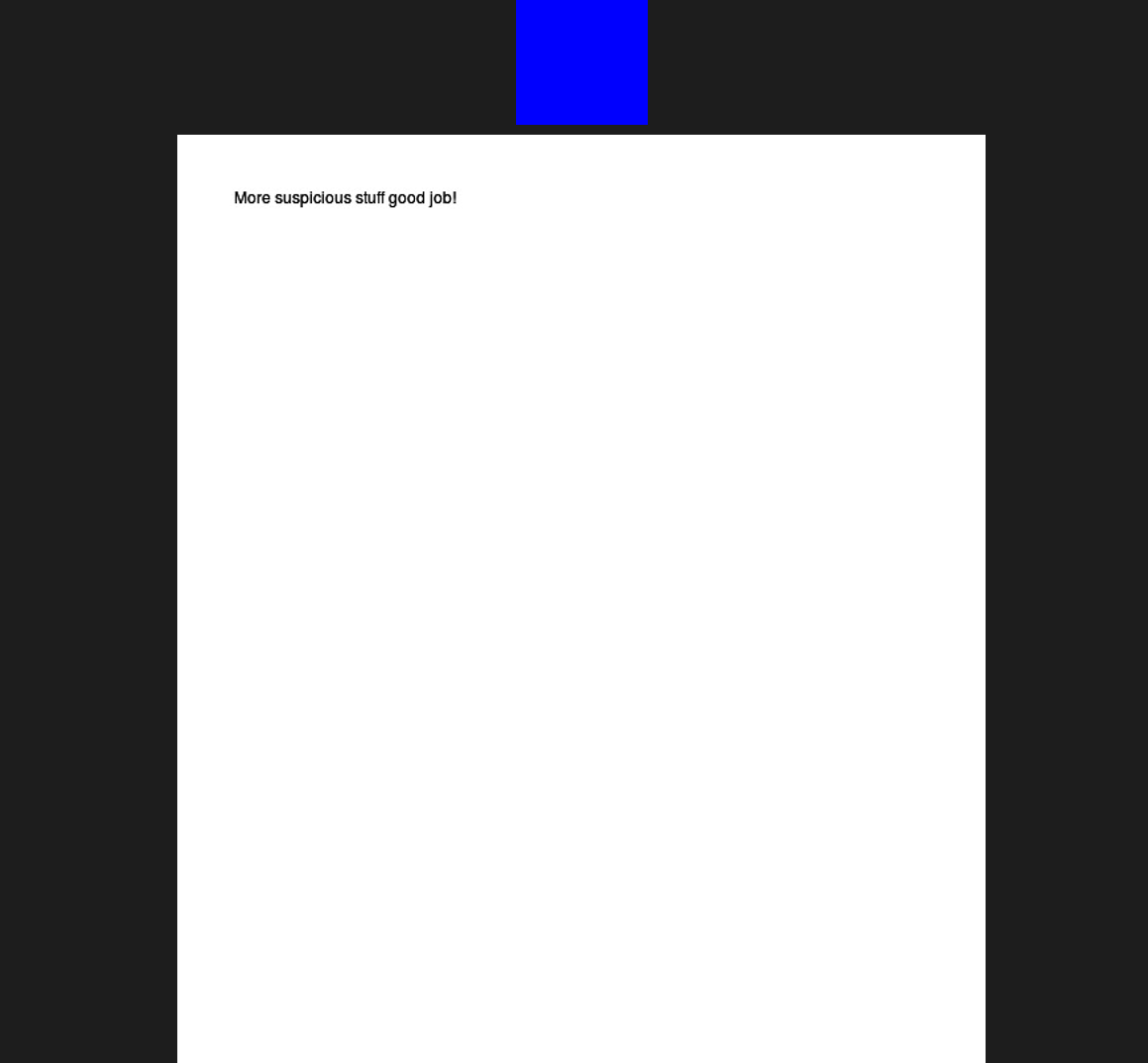
“

**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.*

To access the PDF files, I followed a similar procedure to the one used for images. First, I examined the TCP stream, searching for the distinctive PDF file signature, identified by the hexadecimal data "25 50 44 46." Once located, I observed that the PDF data extended to the end of the TCP stream, as indicated by the ASCII view.

Based on this observation, I copied all hexadecimal data from the PDF file signature onward into HxD. Then, I saved this extracted data as a PDF file. This method proved effective for all three PDF files, allowing for their successful retrieval and preservation as PDF documents.  
  


**

**Sub-task 5:**

* *The user also accessed a file called "hiddenmessage2.txt"*
* *What is the contents of this file? Include it in your report*

Upon inspecting the TCP stream of the file, I observed that rather than containing plain text, it was encoded data. Upon further examination in hexadecimal format, I noticed that it exhibited the same file signature as a JPG image.

Subsequently, I proceeded to copy and save the hexadecimal data using HxD, employing the same method I've utilized for other images. Surprisingly, upon doing so, I discovered that the purported text file was, in fact, an

image file.

**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.*

While examining the TCP stream in the course of my investigation, I encountered an unusual occurrence. Instead of the expected single set of JPEG file signatures, I observed two distinct sets within the stream.

Given this discovery, I opted to extract both sets of data, resulting in the retrieval of two separate images. This deviation from the norm presented a unique challenge, requiring careful handling to ensure accurate extraction and analysis of the image content.  
  
The first image:



The second image:



**Sub-task 7:**

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

Upon examining the TCP stream associated with the "broken.png" traffic, I didn't observe any recognizable file signature indicative of a PNG image. Realizing this, I shifted my focus to analyzing the ASCII representation of the data.

Upon closer inspection, I identified that the data was encoded in Base64 format. To decode it, I utilized an online Base64 decoding tool, which successfully decrypted the Base64-encoded data, revealing PNG image content.

Once the data was decoded, I copied the decoded text into the designated section within the HxD hex editor software. From there, I saved the extracted content as a PNG file.

The 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.*

Upon examining the TCP stream for "securepdf.pdf," I made several notable discoveries:

The data within the TCP stream did not correspond to a PDF file as expected. Instead, it revealed an unexpected content format.

At the conclusion of the file, I uncovered a concealed message indicating the presence of a password: "Password is 'secure'."

Interestingly, the file signature embedded within the data matched that of a zip file, suggesting that the content was, in fact, a compressed archive.

Subsequently, I proceeded to extract the hexadecimal representation of the zip file and transferred it to HxD for further analysis. Saving this data as a zip file, I proceeded to unzip it and found a PDF file named "rawpdf.pdf" within. Attempting to access this PDF file prompted a password request.

Fortunately, recalling the password provided in the TCP stream, namely 'secure,' I entered it, granting access to the PDF. Within the PDF, I discovered the initial pages of a guide for internet banking.

