|  |
| --- |
|  |

Packet Capture Analysis:

Analyzing a packet capture from a network provided to me. I filtered it to HTTP traffic to look at the contents of the HTTP packet.  
A screenshot of a computer

Description automatically generated

**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 look at the images the user accessed named anz-logo.jpg and bank-card.jpg, I right-click on it and followed TCP stream. The raw data string is too long, so I created a simple script that will automate the process of getting the raw data between the first hex (FFD8) and the last hex (FFD9), my script then will output it in a text file. This is the script I used:

A screenshot of a computer program

Description automatically generated

This is how the program works:



And voila here is the extracted hex data:

A screenshot of a computer screen

Description automatically generated

I copied and pasted it to my hex editor and saved it as JPG file format to view the data and this is what I found:

anz\_logo.jpg

A blue and white logo

Description automatically generated

bank-card.jpg

A blue credit card with white text and blue background

Description automatically generated

**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.*

Same method applies when extracting images, after performing the previous steps, these are the images I found:

ANZ1.jpg ANZ2.jpg

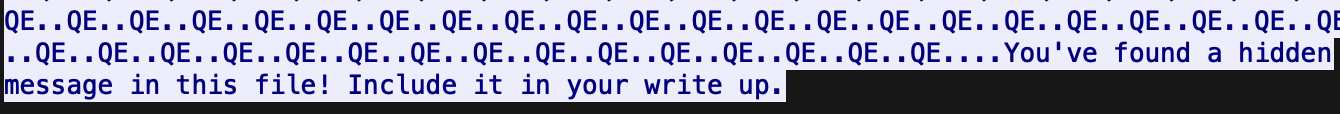
A close-up of a document

Description automatically generatedA blue cover with a blue shield and a white logo

Description automatically generated

**I saw messages at the end of these hex data:**

* **ANZ1.jpg**

****

* **ANZ2.jpg**

**A screen shot of a computer screen

Description automatically generated**

**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 checked this specific traffic and found this:

A screenshot of a computer screen

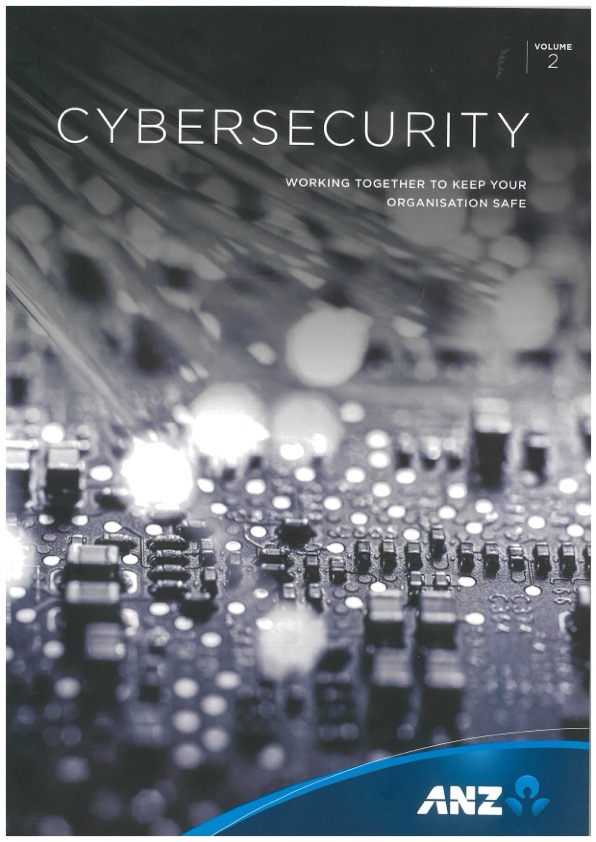
Description automatically generated

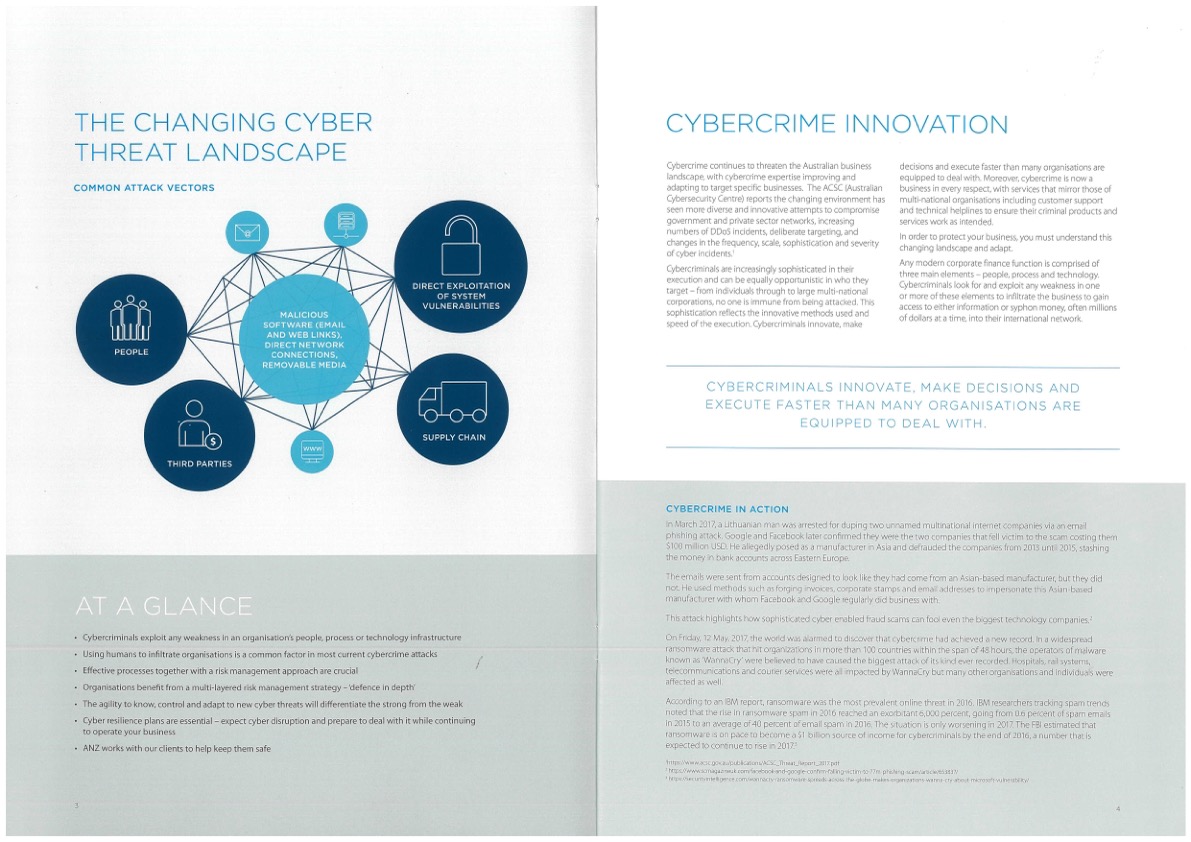
**Sub-task 4:**

* *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.*

This time I did it differently, I utilized the search function on wireshark and put the hex data on raw. I searched for “25504446” since it is a pdf file signature, I copied and pasted from 25504446 until the end of the hex data. I did it to all these pdf files and here are the results:

ANZ\_Document.pdf ANZ\_Document2.pdf



****

**evil.pdf**

**A blue square on a black background

Description automatically generated**

**Sub-task 5:**

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

For this one I can’t find the txt signature file, so I tried typing ffd8 and it worked, I believe this is a jpg file hidden in a txt file, I found this image:

A group of people standing together

Description automatically generated

**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 noticed there are 2 FFD8 in the hex value, leaving me puzzled, so I tried breaking it into 2 and yes I found 2 photos. Here are the photos I gathered:**

**atm-image.jpg atm\_image2.jpg**

**A group of people walking past a storefront

Description automatically generatedA person wearing a mask and holding a crowbar

Description automatically generated**

**Sub-task 7:**

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

A blue logo on a black background

Description automatically generatedI’ll be honest but this is the section I kind of struggled, so I pasted the ASCII data to chatgpt and was informed that this is a base64 encoding. I looked online for a base64 conversion tool and the result I have is this 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*
  + I tried looking at the packet and it is not a pdf file since it is not finding the pdf signature, so again I posted this hex value to chatgpt and I was told that this was a zip file.
  + I looked for online tool that can convert this hex to zip file.
  + After I did that, the zip file was reconstructed, but I was asked for a password.
  + I looked at the ASCII data of the packet and looked at the very bottom and found this:

A close-up of a computer screen

Description automatically generated

* + I went back to the file and put “secure” as the password and yes it gave me a pdf file called rawpdf.pdf. I opened it and I was presented with 2 pages of pdf. Here is the image:

A person using a computer on a couch

Description automatically generated