|  |
| --- |
|  |

**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.**

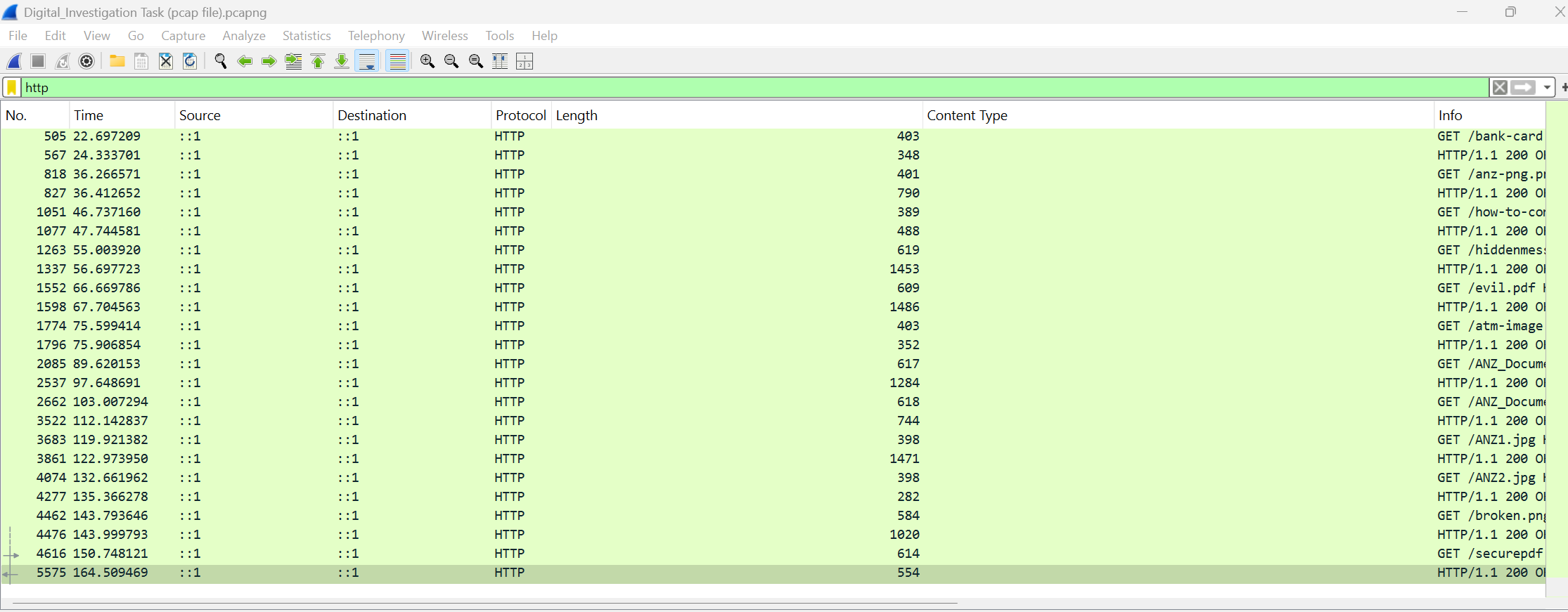
Here is the background information on your task Suspicious network activity has been detected coming from a user on the ANZ network. A laptop has been flagged up on our security systems due to suspicious internet traffic, and we need you to investigate the network traffic in order to establish what the user accessed and downloaded. Your task is to examine their network activity and gather what information you can on what images they viewed and what files they accessed. You have been provided with a packet capture file (pcap) containing all their recent network activity. There may be a number of artifacts contained within the packet capture file, and you will be expected to identify and report as many as possible. You must provide a report on everything you found, and document what processes / steps you followed to achieve this.

**Analysis**

***All the traffic is between loop aaddress ::1, implying a local proxy environment.***

***The activies use http allowing full inspection the comunication.***

***The files accessed or downloaded include* (.jpg, .png), PDFs, DOCX documents, and plain text.**



*File export*

**Go to File → Export Objects → HTTP** This opens a window listing all HTTP-transferred files (like .jpg, .png, .pdf, .docx, etc.).

But for deeper inspection, the **Follow TCP** Stream have been used to recontruct raw.

**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.*

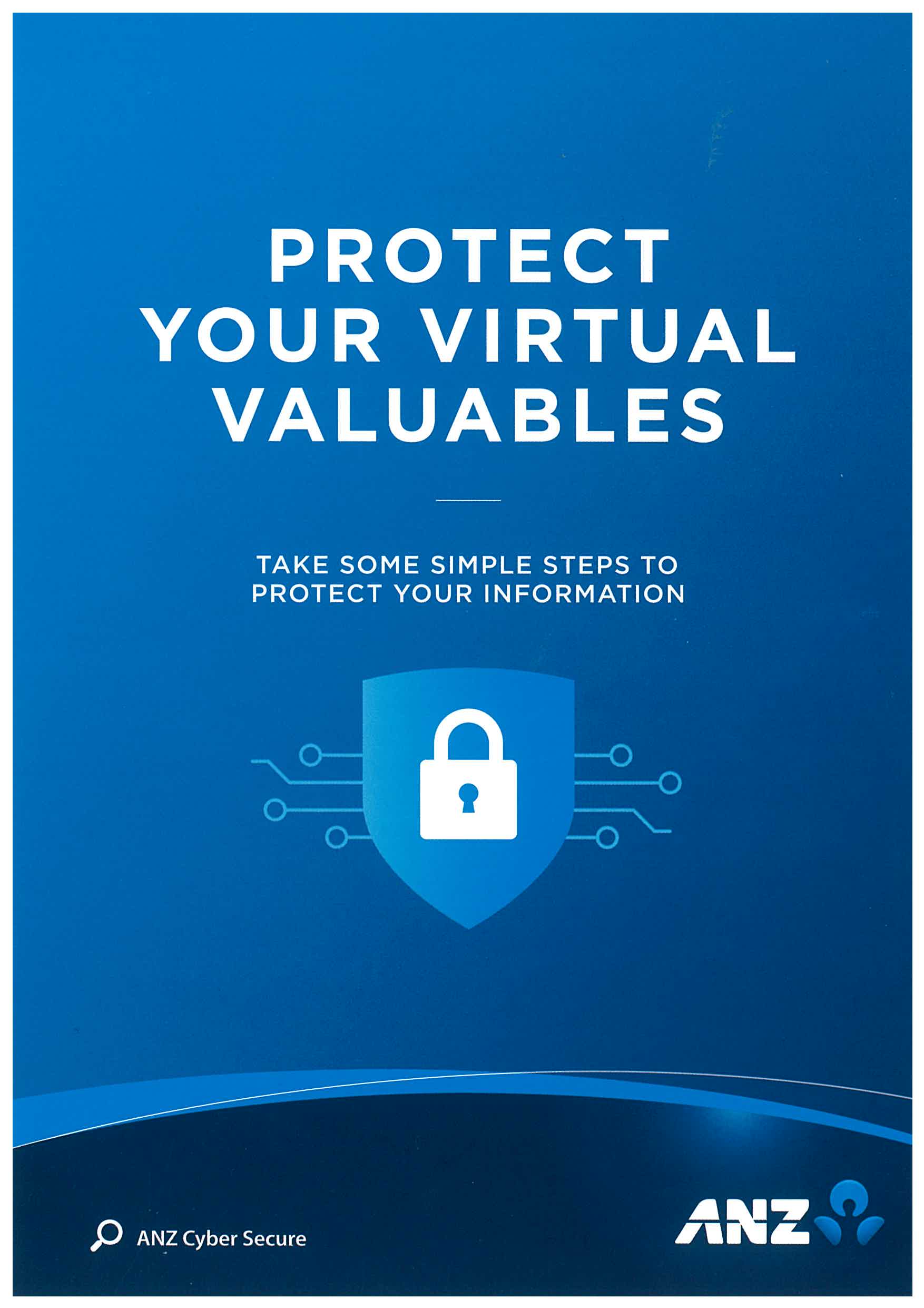


**Sub-task 2:**

* *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.*

*Differences between the images ANZ1.jpg" and "ANZ2.jpg"*

*ANZ1.jpg*

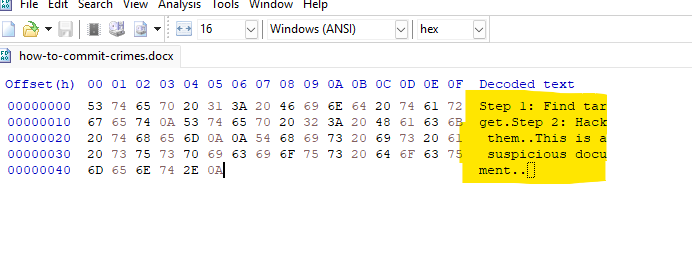


**Sub-task 3:**

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

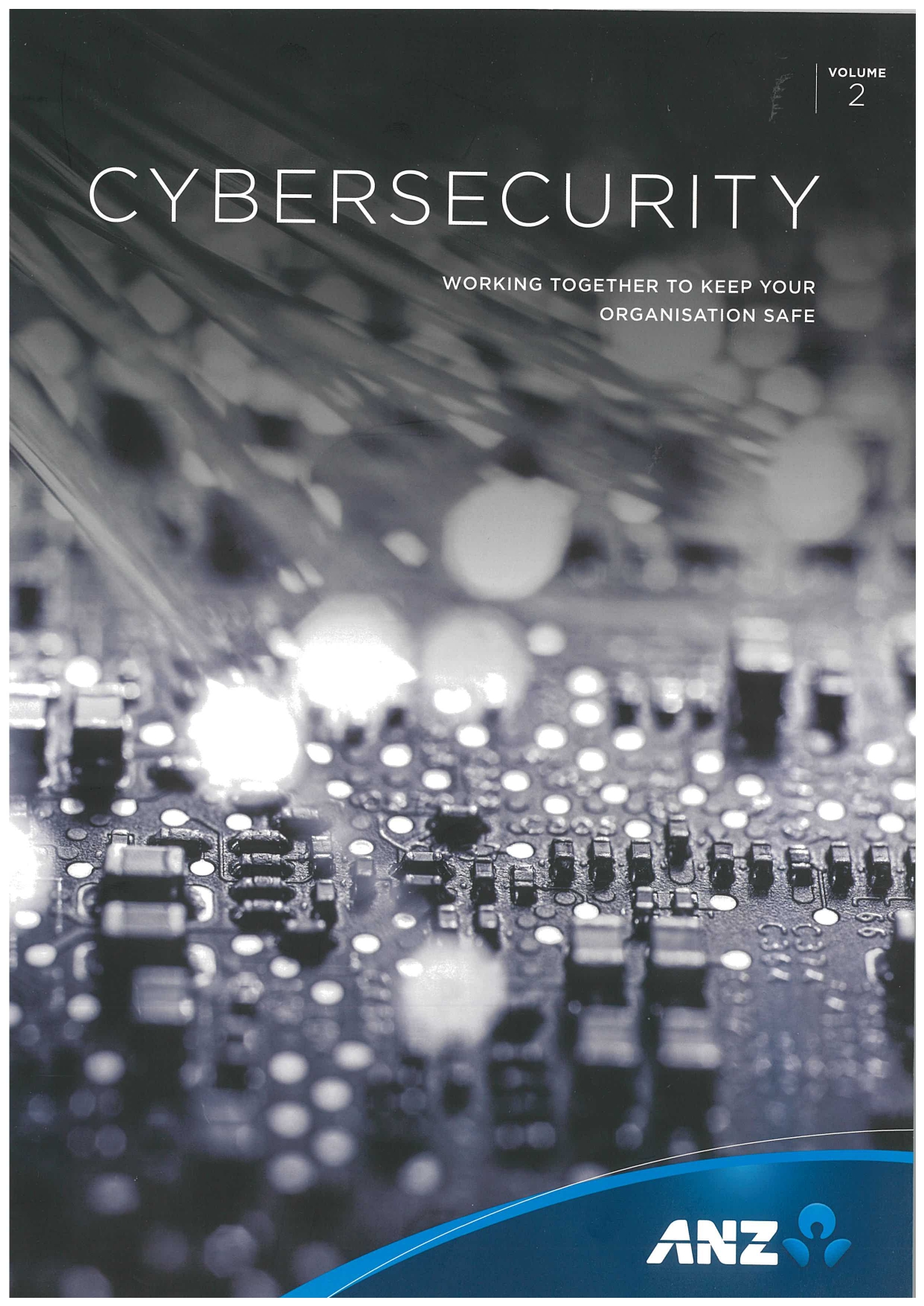
As word can’t open the file file I’ve use HxD to read it.

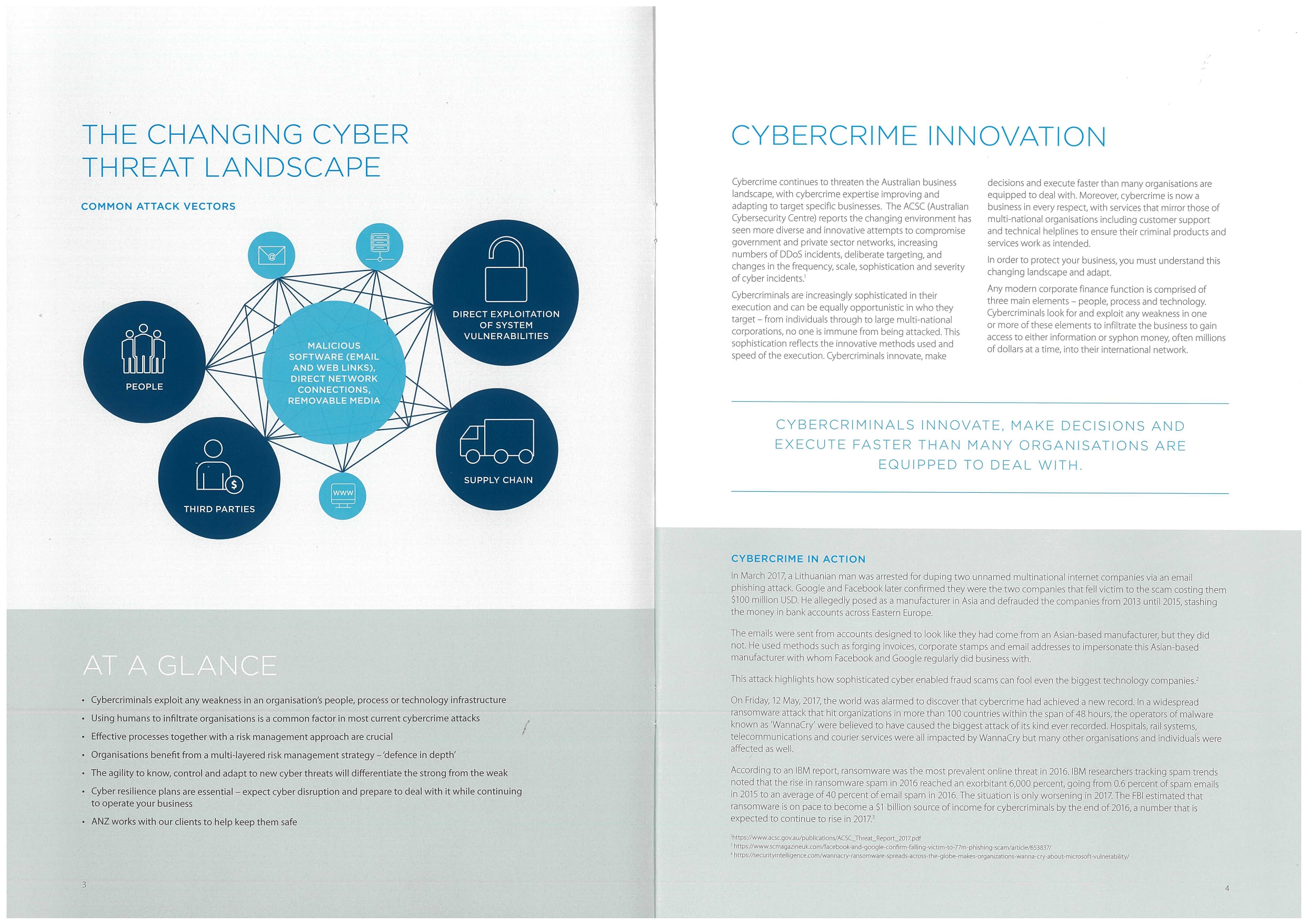
Below the the results.



**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.*







**Sub-task 5:**

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

The file hiddenmessage2.jpg was recovered via HTTP and analyzed using CyberChef’s Extract Files operation. At offset 0x350, a new image file was discovered: extracted\_at\_0x350.jpg. This image depicts three individuals standing in front of an ANZ bank sign and is likely the intended hidden content. This layered concealment technique illustrates practical steganography using embedded JPEG structures.



**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.*

The image *atm-image.jpg* was accessed via HTTP from a local server (localhost:8000). The traffic used TCP and was segmented into 7 reassembled packets totaling 13,238 bytes. The HTTP response indicated a successful transfer (200 OK) from an Apache/2.4.6 (CentOS) server. The use of a non-standard port and local URI suggests this traffic was generated in a controlled or simulated

environment, possibly for forensic analysis. The image was identified as a JPEG file with a content length of 12,950 bytes.



**Sub-task 7:**

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

**Investigation Process**

* 1. Captured HTTP traffic showed a **GET request for broken.png** served from a **local server (localhost:8000)** using the IPv6 loopback address.
  2. The response included standard HTTP headers indicating a **Content-Type: image/png** with a **Content-Length of 16,102 bytes**.
  3. Upon extracting the file from the TCP stream, the resulting .png file **failed to open** in conventional viewers—suggesting corruption or intentional obfuscation.

**Hex Analysis**

A **hex editor (HxD)** revealed that the file contained a valid HTTP response but no immediately readable PNG image data.

After scrolling through the hex, the PNG signature (89 50 4E 47 0D 0A 1A 0A) was located, confirming the presence of embedded image data.

**Extraction**

Using **CyberChef**, the PNG hex segment was isolated and converted:

Applied operations: "From Hexdump" → "To Base64" → "From Base64" → "Save File" (as broken.png).

The exported file opened successfully, displaying the originally hidden image.

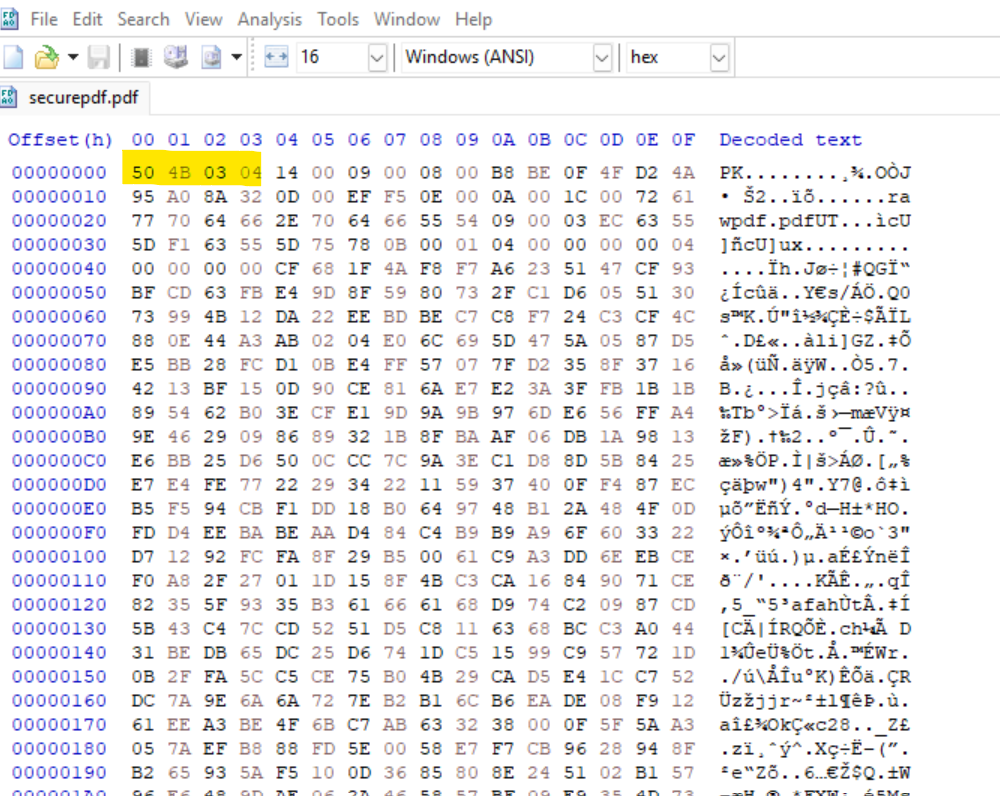
**Conclusion**

The image was embedded in a textual hex dump and disguised with misleading headers and filler bytes, requiring manual carving and decoding.



**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.*



The file securepdf.pdf was captured in HTTP traffic.

Upon inspection in HxD, it was revealed to be a **ZIP archive (with ZIP archive HEX Signature 50 4B 03 04 )** in disguise (application/zip), not a true PDF.

**Extraction**

**Oneìce noticed that the securepdf.pdf was a ZIP archived I’ve saved the file as a .ZIP (securepdf.zip) and then tried to unzip it and then found out that there was a password protected pdf file in that archive named rawpdf.pdf**

