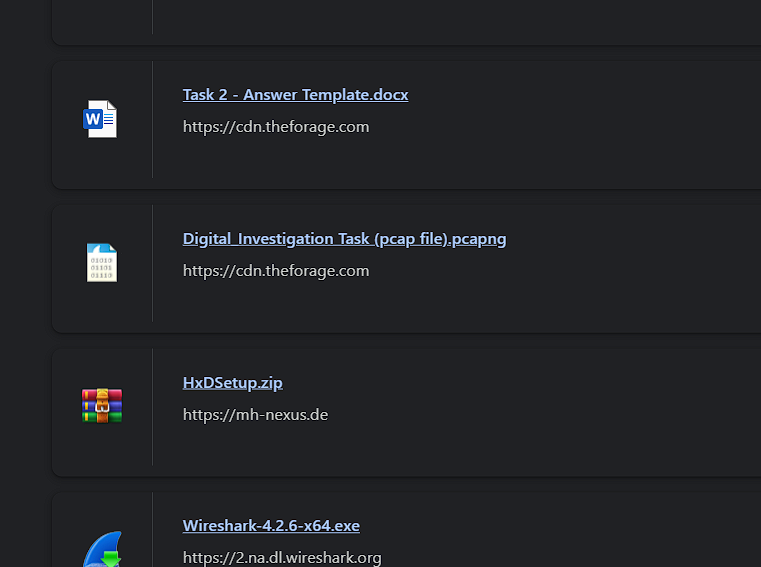
|  |
| --- |
|  |

**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.**

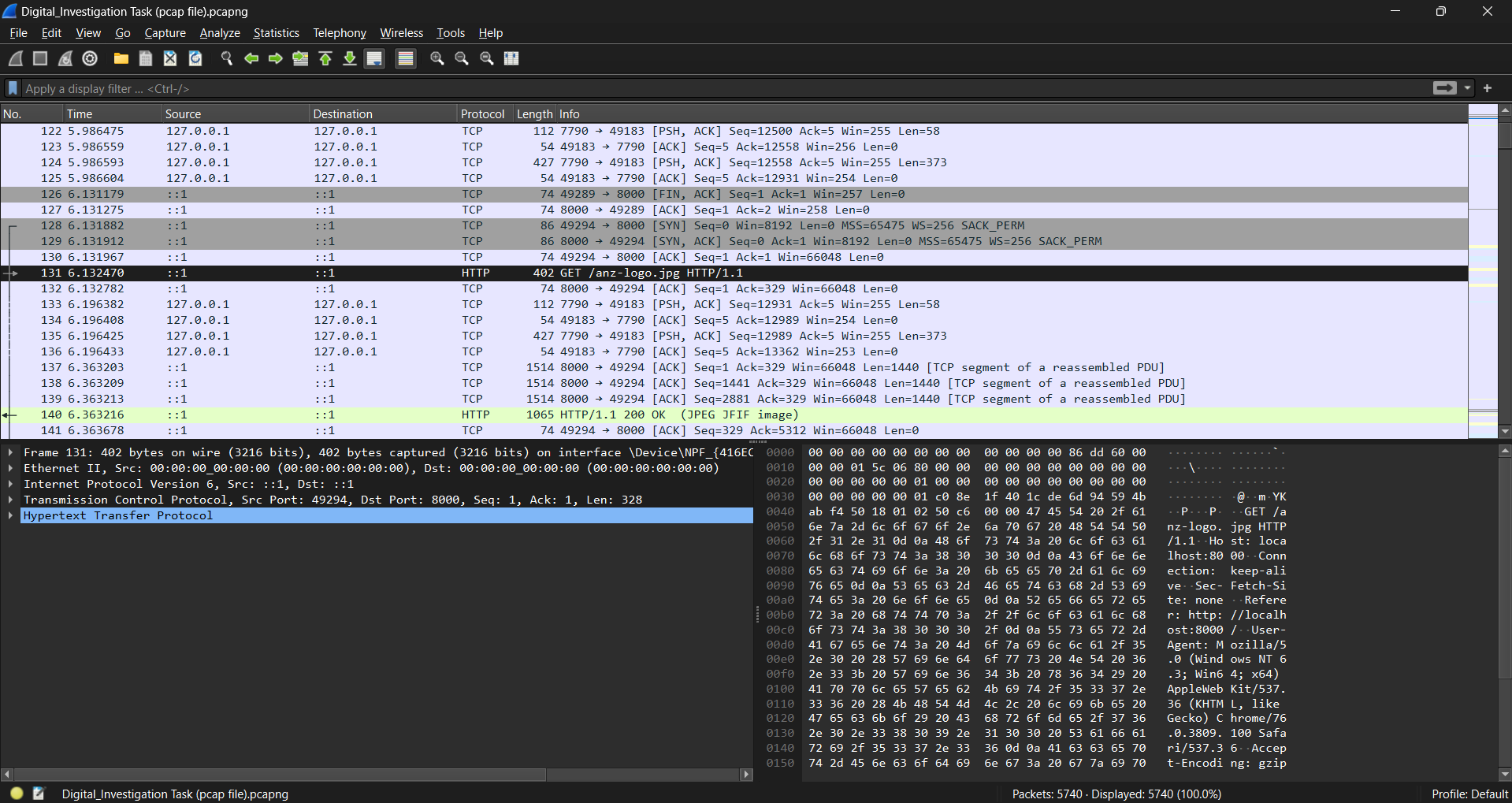
**Sub-task 1:**

Step 01 : I downloaded the pcap file, then I opened it using wireshark which is already installed in my laptop as shown in the image 1.0 .



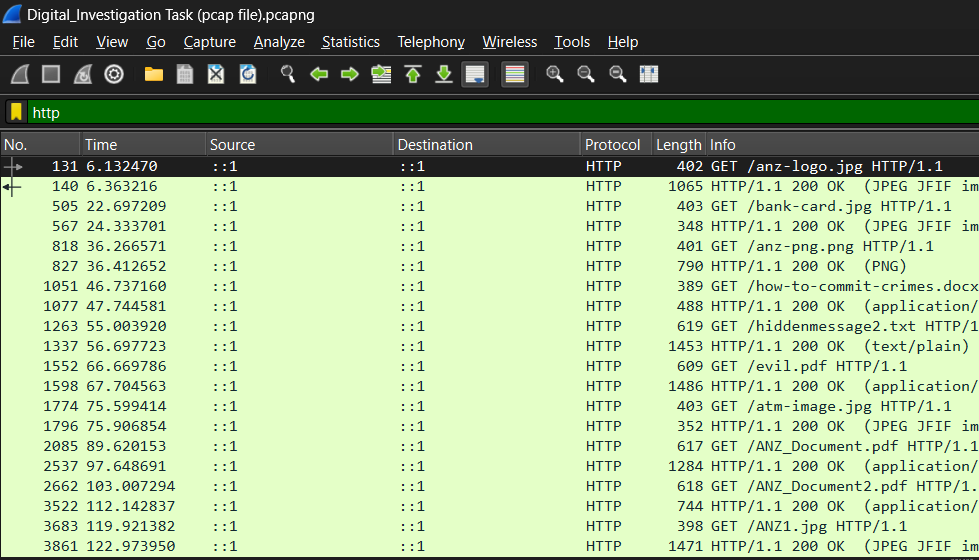
1.0

Step 02 : The interface will look like the image 1.1 .



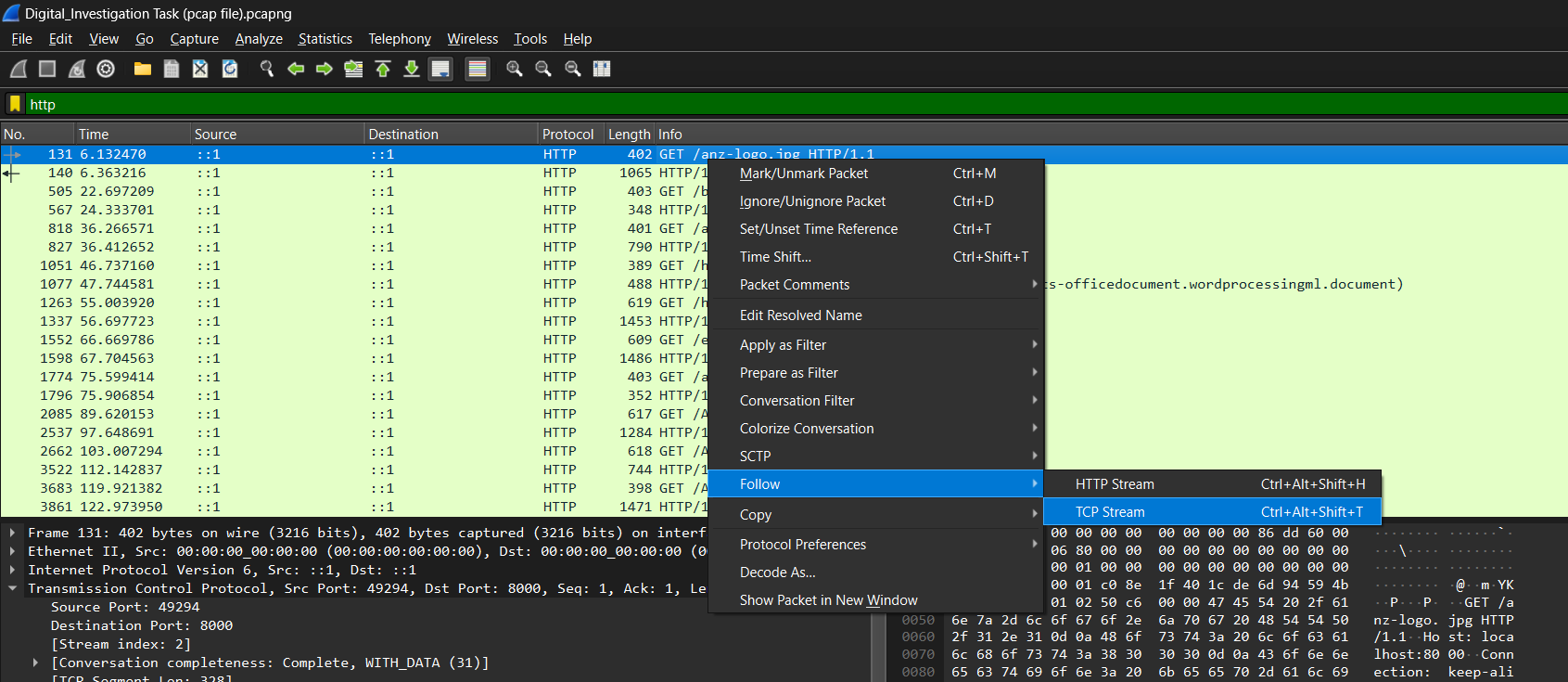
1.1

Step 03: Searched “http” in the search box as show in the image 1.2 .



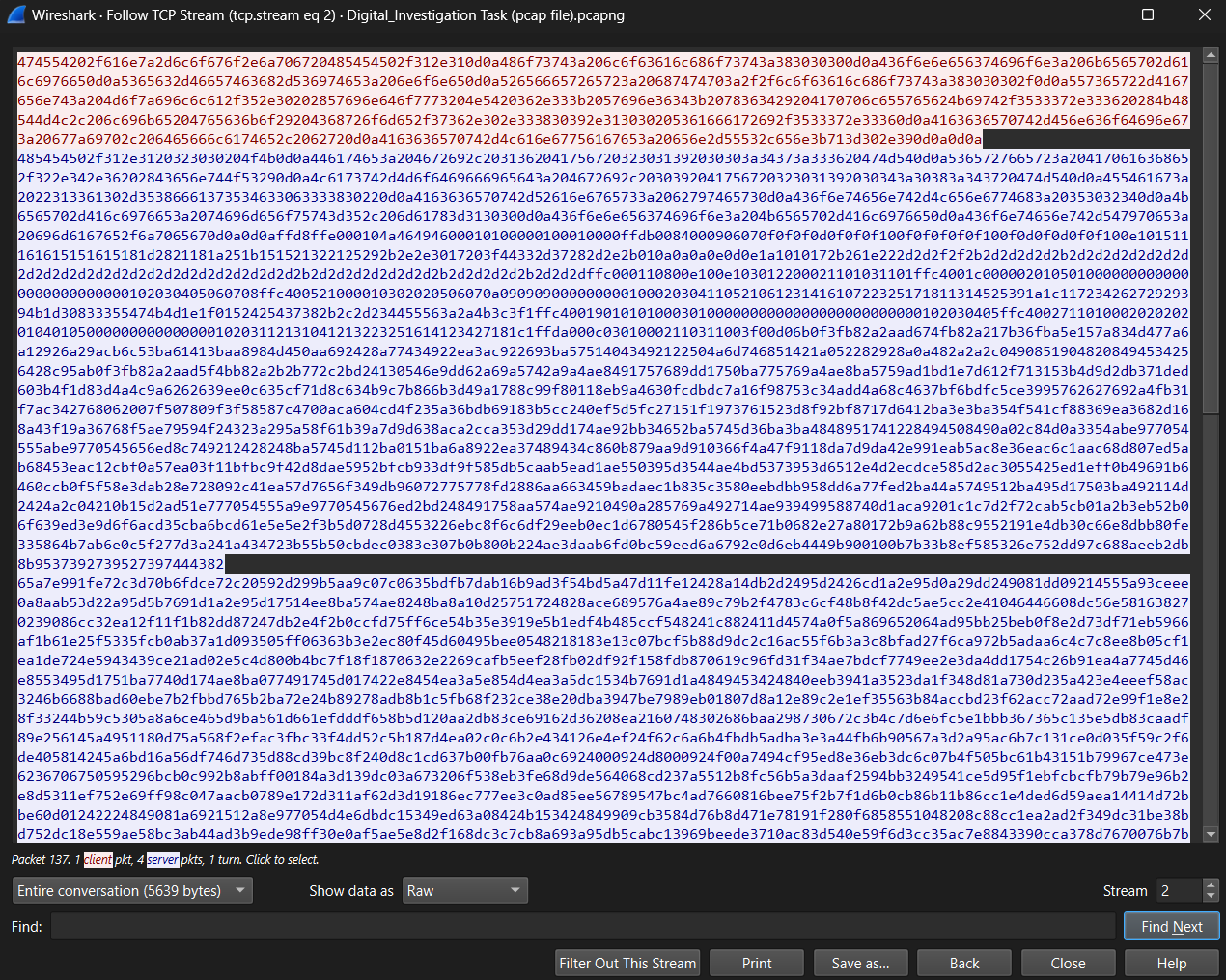
1.2

Step 04: Right click on the anz-logo.jpg as shown in the image 1.3 .



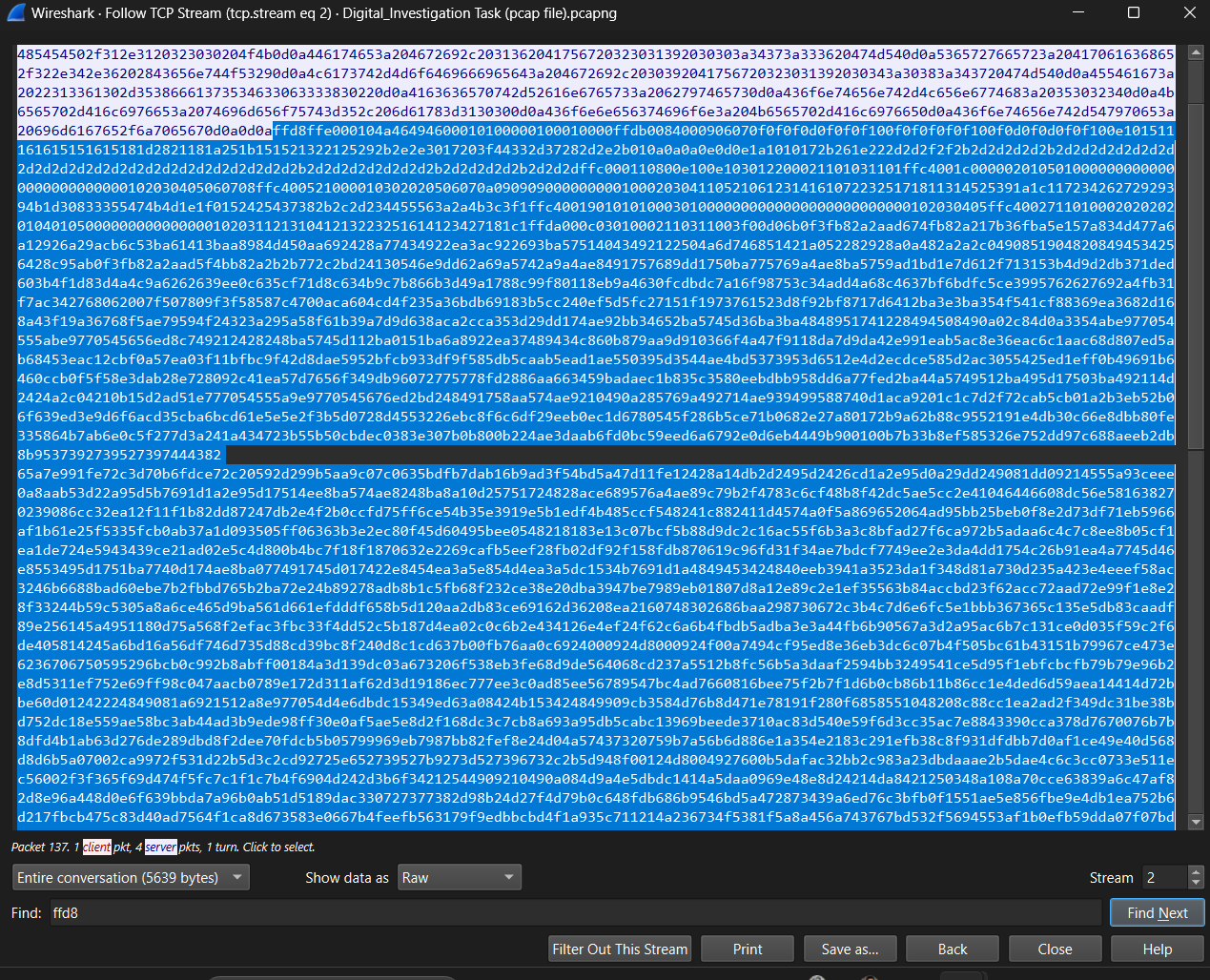
1.3

Step 05: After doing this you will get a box like this 1.4 .

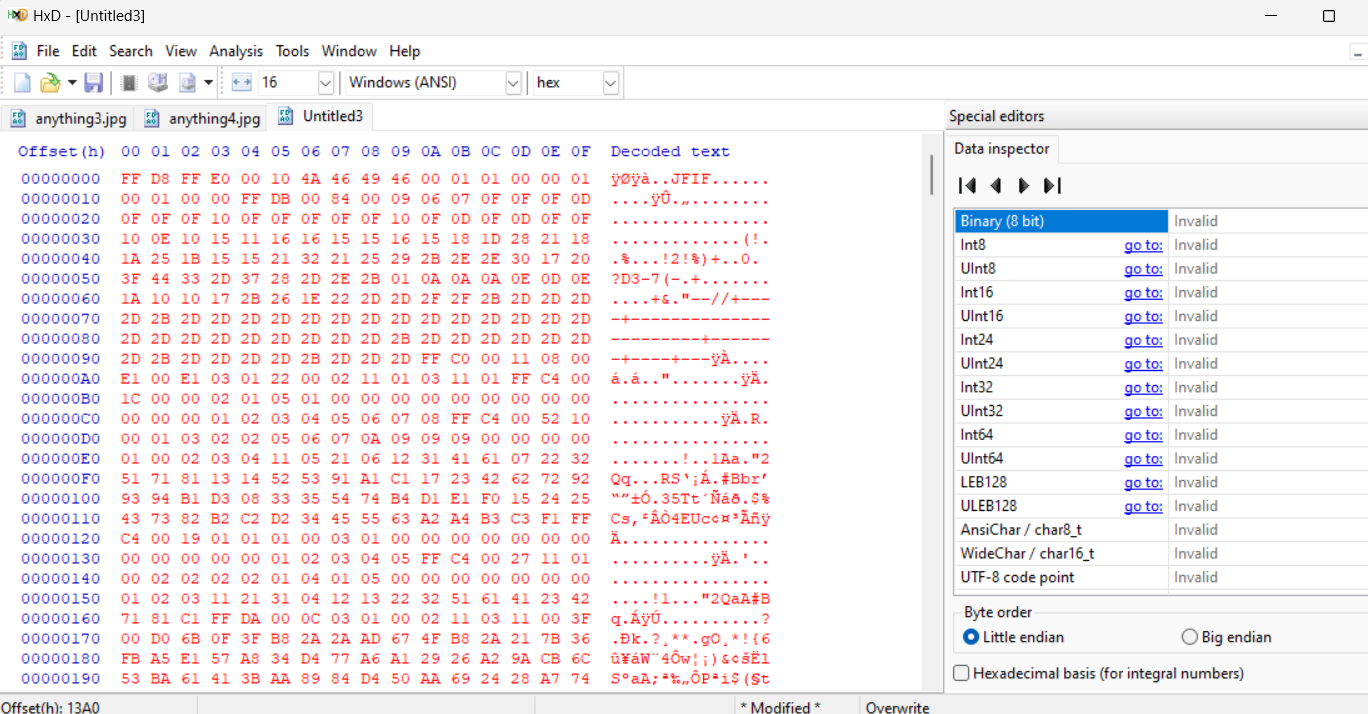


1.4

Step 06: Copy the text which is shown in the box starting from “ffd8” to “ffd9” which is the unique code representing the image and paste it in the hex editor tool like shown in the image 1.5 & 1.6 .



1.5



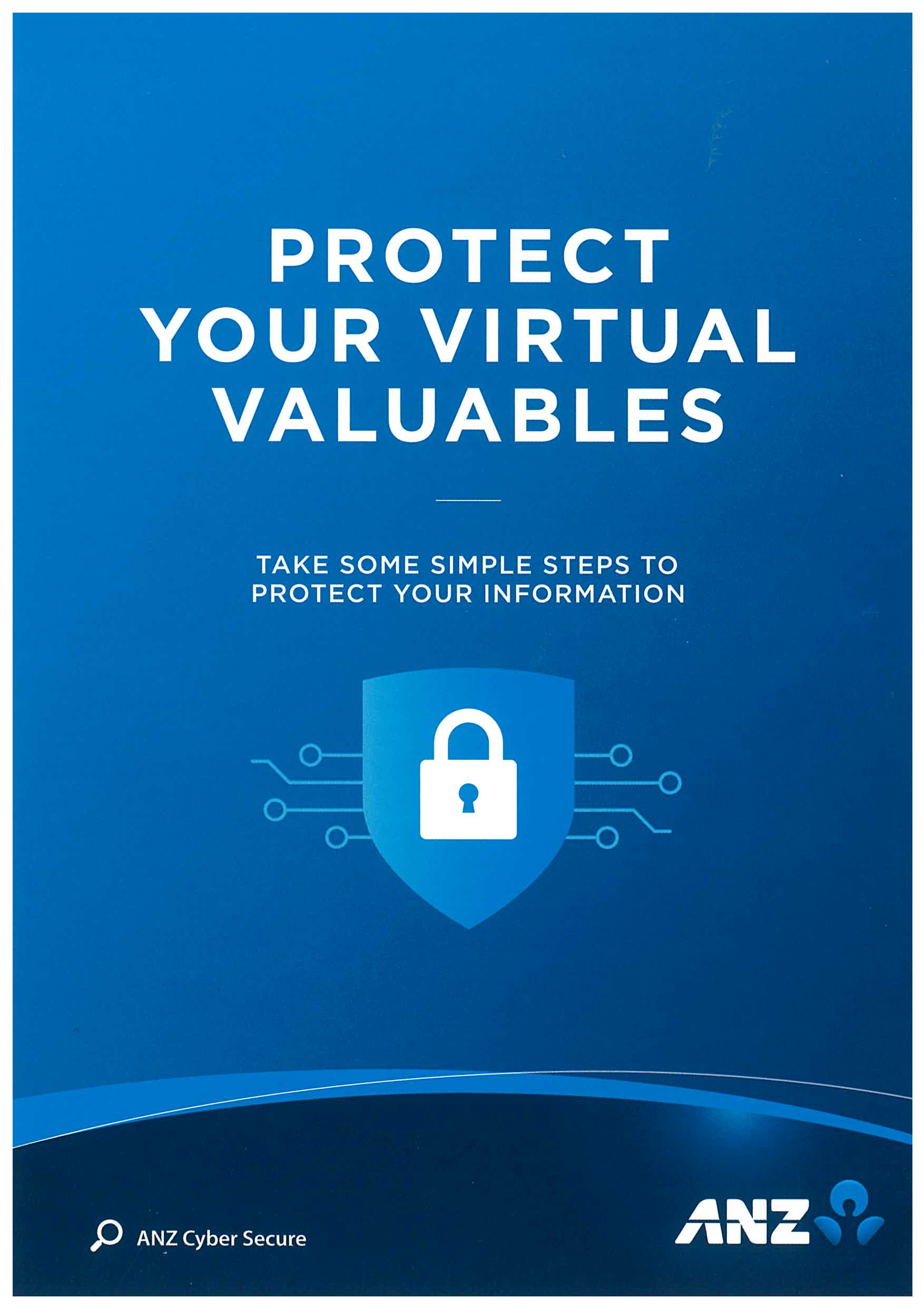
1.6

Step 07: Save the file in the “.jpg” format, and you got the images.(Note: Same process for 2nd image also)

**

**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.*

****

**The above are the two images which I had found**

**The difference between the 1st and the 2nd image is, in the first image “**You've found a hidden message in this file! Include it in your write up.**” Is found and in the 2nd image “**You've found the hidden message! Images are sometimes more than they appear.**” in the ASCII value.**

**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..*

**The content I found is:**

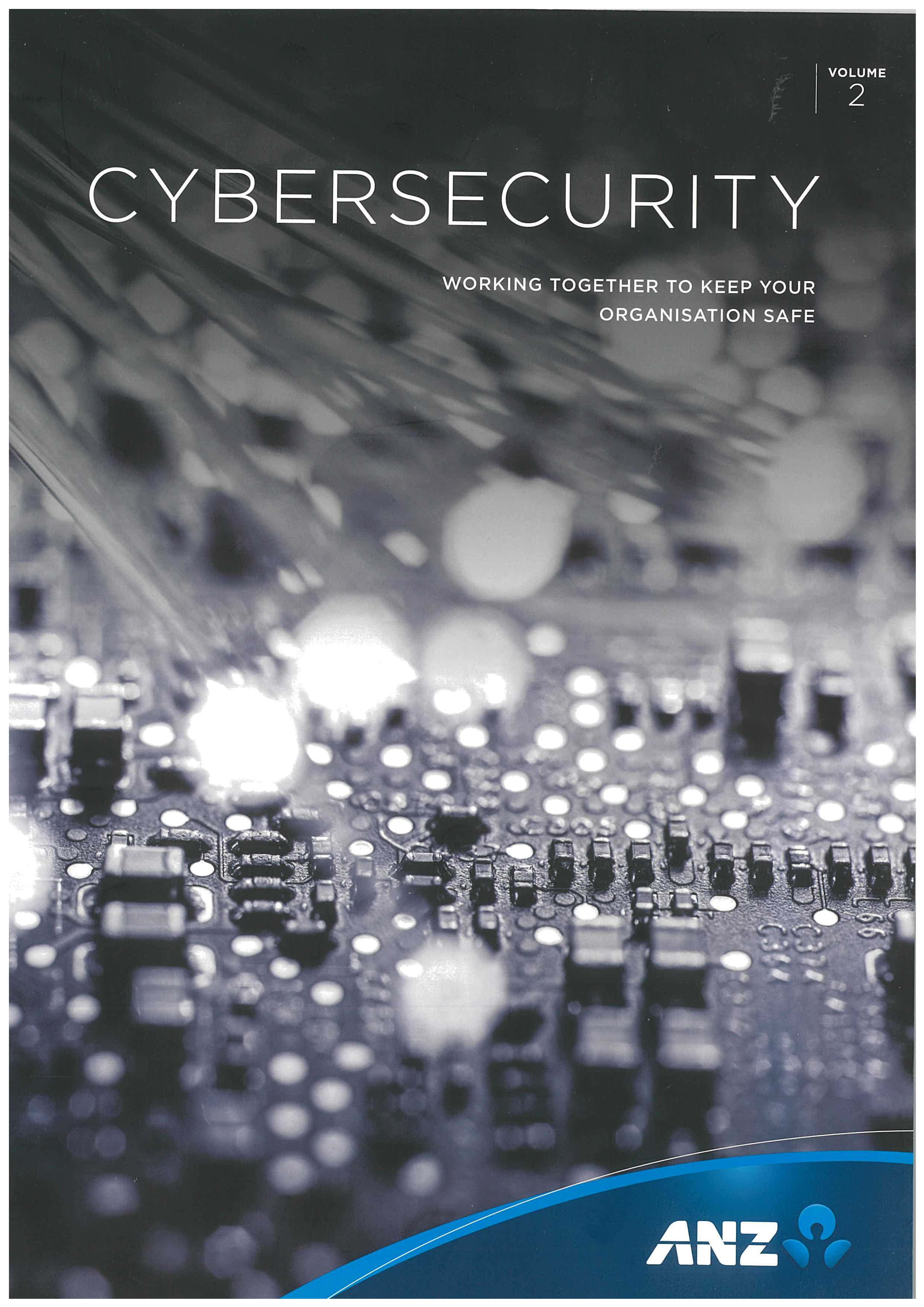
Step 1: Find target

Step 2: Hack them

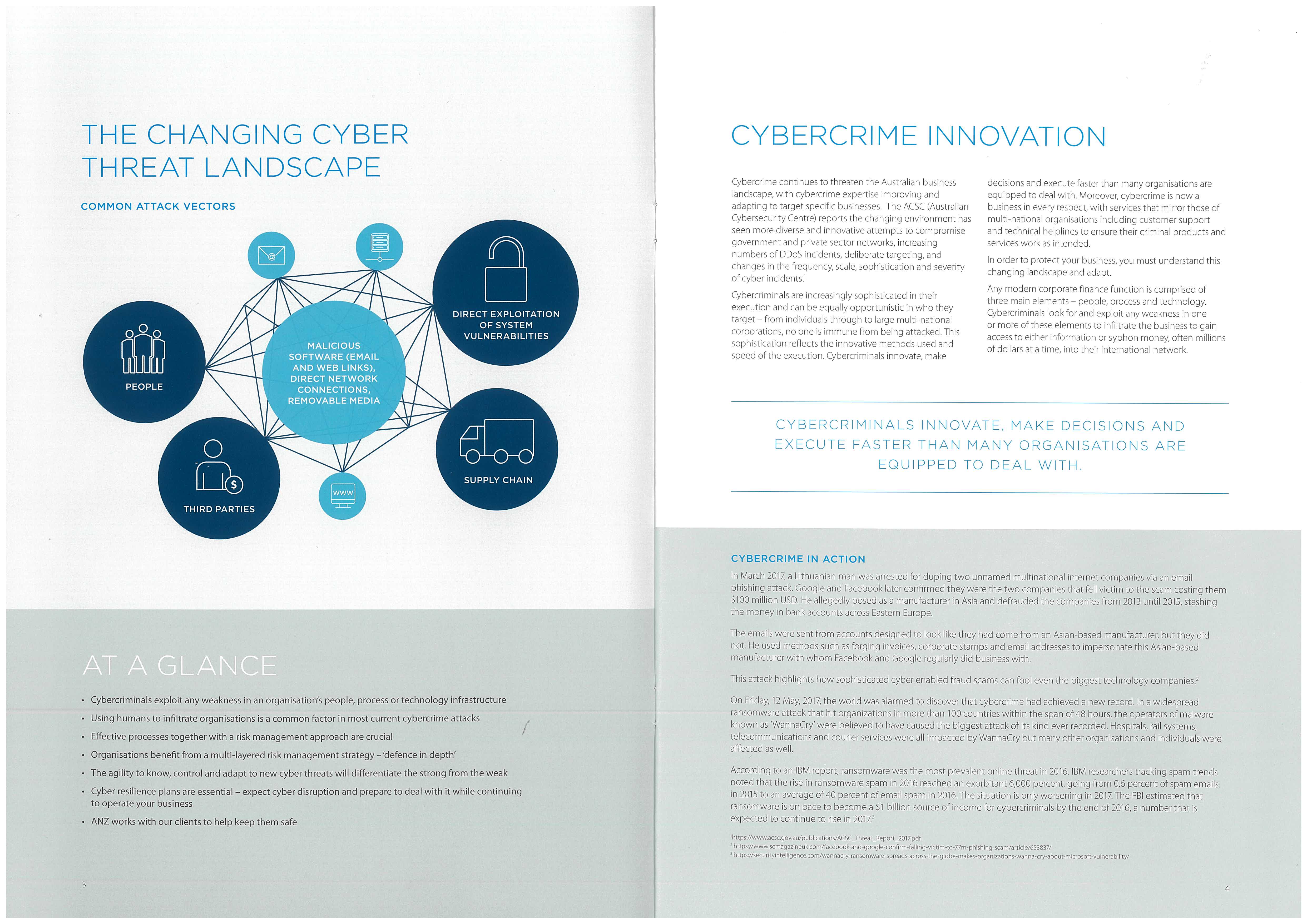
This is a suspicious document.

**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.*



*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*

**

**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 difference in this traffic I found is there is 2 images in a single traffic one after the another, the 2 images are given above.**

**Sub-task 7:**

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

****

**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.*

**A TCP stream analysis of the file 'securepdf.pdf' revealed unexpected content. Instead of PDF data, the file's footer contained a hidden message: "Password is 'secure'."**

**Further examination showed a ZIP file signature within the data, indicating the downloaded file was actually a ZIP archive disguised as a PDF.**

**The extracted ZIP file included a PDF named 'rawpdf.pdf'. Opening this PDF required a password, which was successfully provided using the 'secure' password found in the TCP stream. The PDF content was identified as the initial two pages of an internet banking guide.**

****