|  |
| --- |
|  |

Steps to view the required files –

1. Uplaod the pcap file into wireshark
2. Filter the HTTP packets for analysis
3. View each png , pdf required by selecting Follow when you right click on the HTTP packet
4. Select TCP stream to the data
5. Convert ASCII to raw
6. Select the hexdata and paste it in HxD
7. Save the file with the required extension

**Sub-task 1:**

For the first task search for FFD8 and FFD9 to view the image .

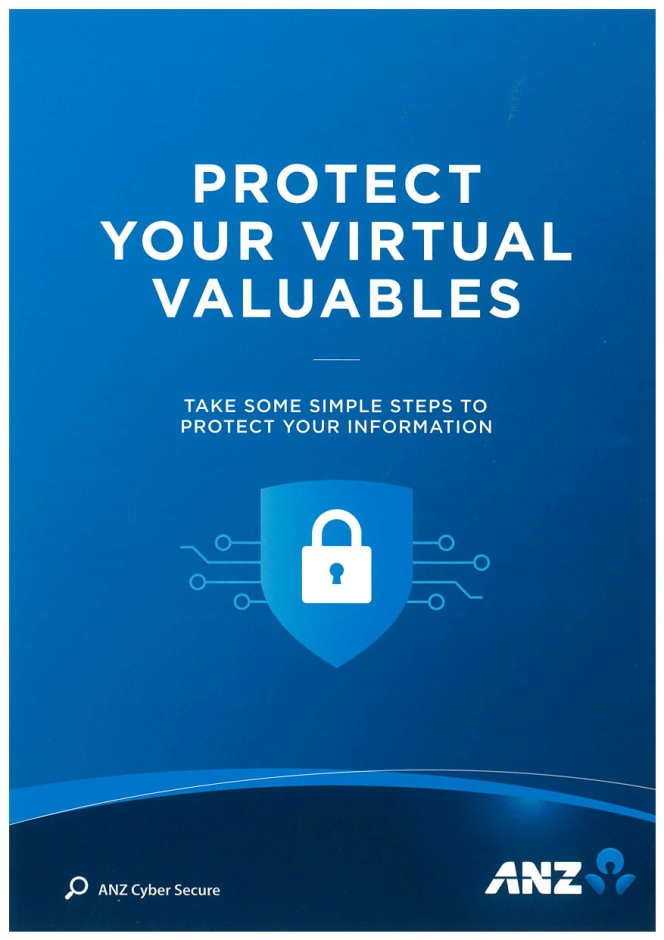
**

*Bank-logo.jpg*

**

*Bank-card.jpg*

**Sub-task 2:**

**

*ANZ1.jpg*

At the end of the network traffic if observed carefully there was a message – “You’ve found a hidden message in this file ! Include it in your write up.”

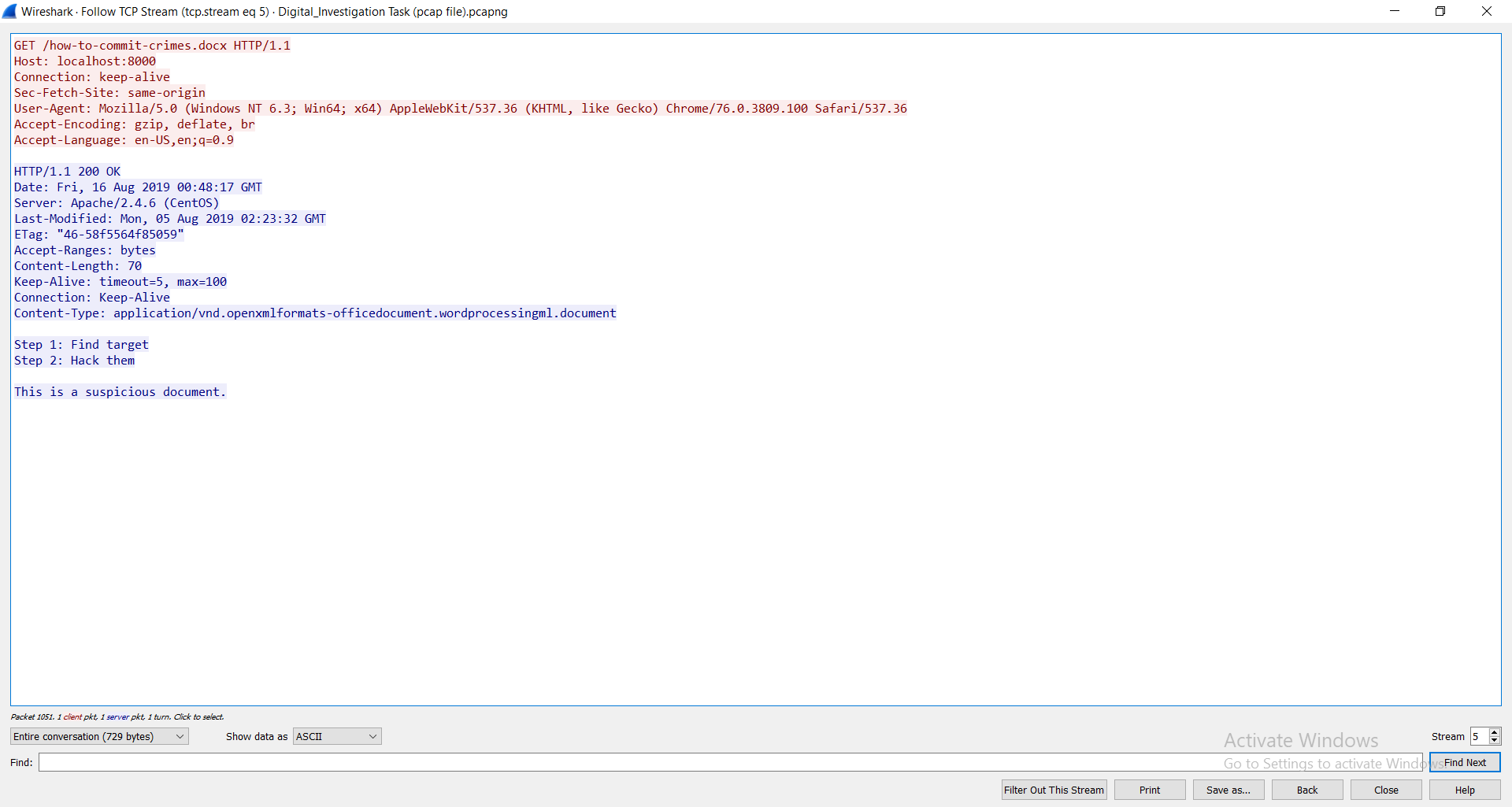
**

*ANZ2.jpg*

At the end of the network traffic if observed carefully there was a message – “ You’ve found the hidden message !Images are sometimes more than they appear .”

**Sub-task 3:**

Whatever was required in directly present in the ASCII format

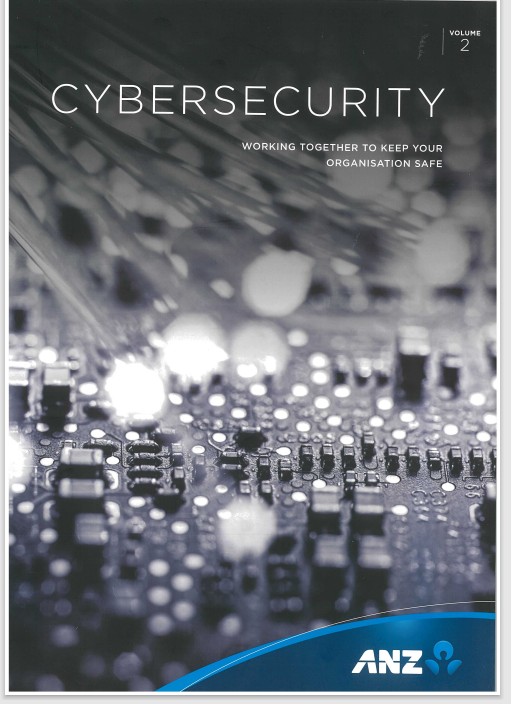
**

**Sub-task 4:**

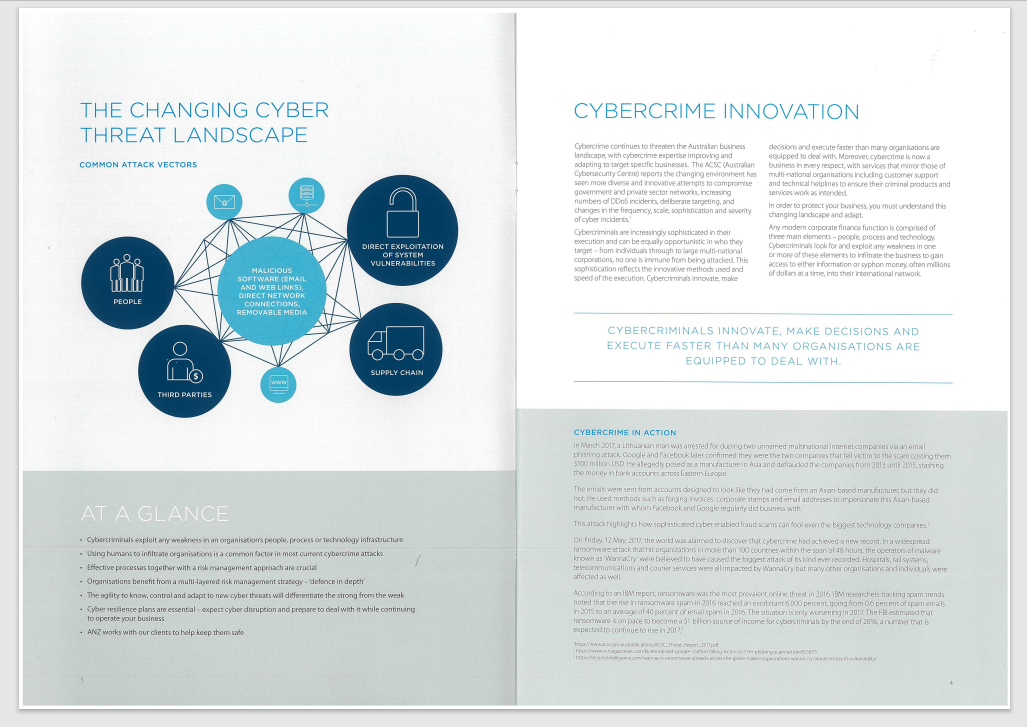
If we follow the above steps and save each of them as a pdf we get the following images in pdf.

****

*Evil.pdf*

**

*ANZ\_document.pdf*

**

*ANZ\_document2.pdf*

**Sub-task 5:**

The text in this was encoded and although it says it is a text file , it is an image as seen below **.**

****

**Sub-task 6:**

If we analyze the raw data there are FFD8 and FFD9 . If we paste both of them in HxD we get two different images as seen below .

****

****

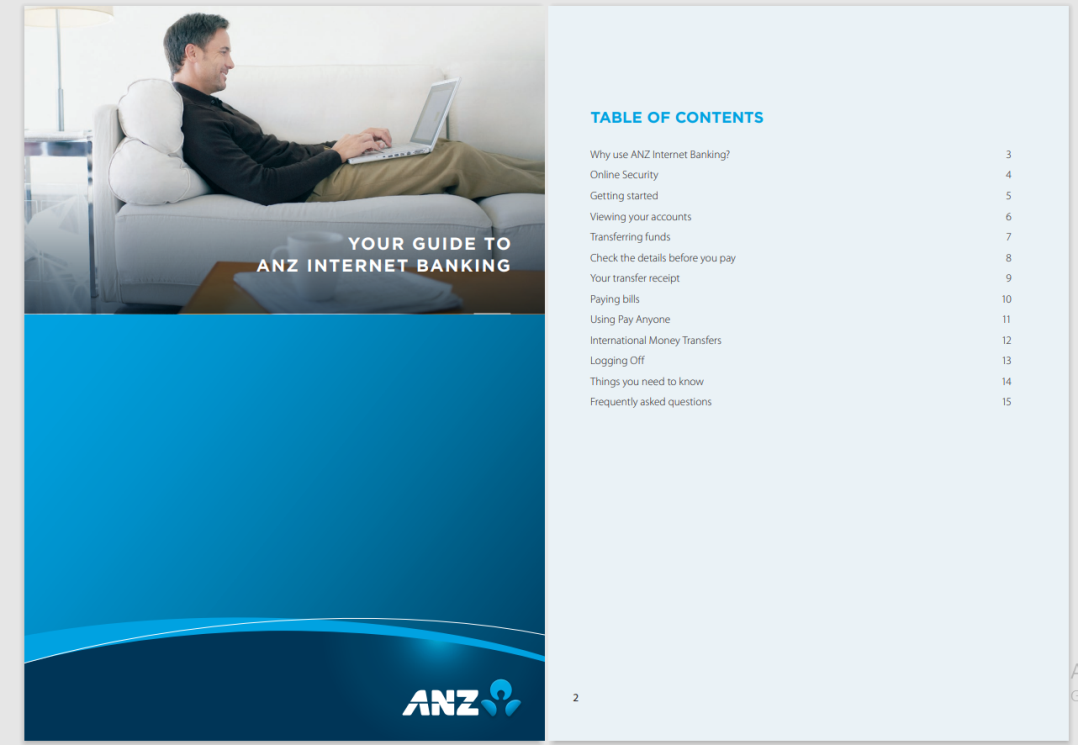
**Sub-task 7:**

If we get the hex value of a jpeg file we can look for it in the TCP data stream and get the hex data to retrieve the image



**Sub-task 8:**

The password is given at the end of the ASCII format , when we extract the zip file from the hex data we see there is a pdf named rawpdf.pdf and when we try to open it it asks for a password which is secure as mentioned in the ASCII data . The pdf contains the following two pages .

****