|  |
| --- |
|  |

**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:**

* *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.*
* **
* **
* *They are not complete images . Something is being hidden in this images for some malicious intent.*

**Sub-task 3:**

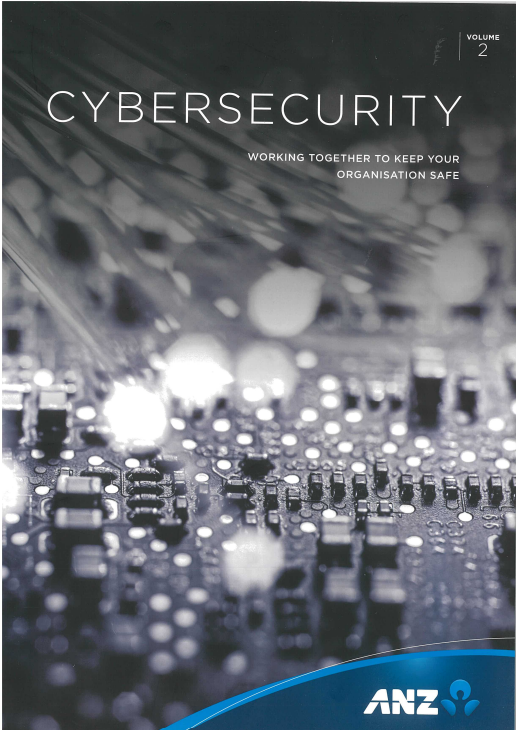
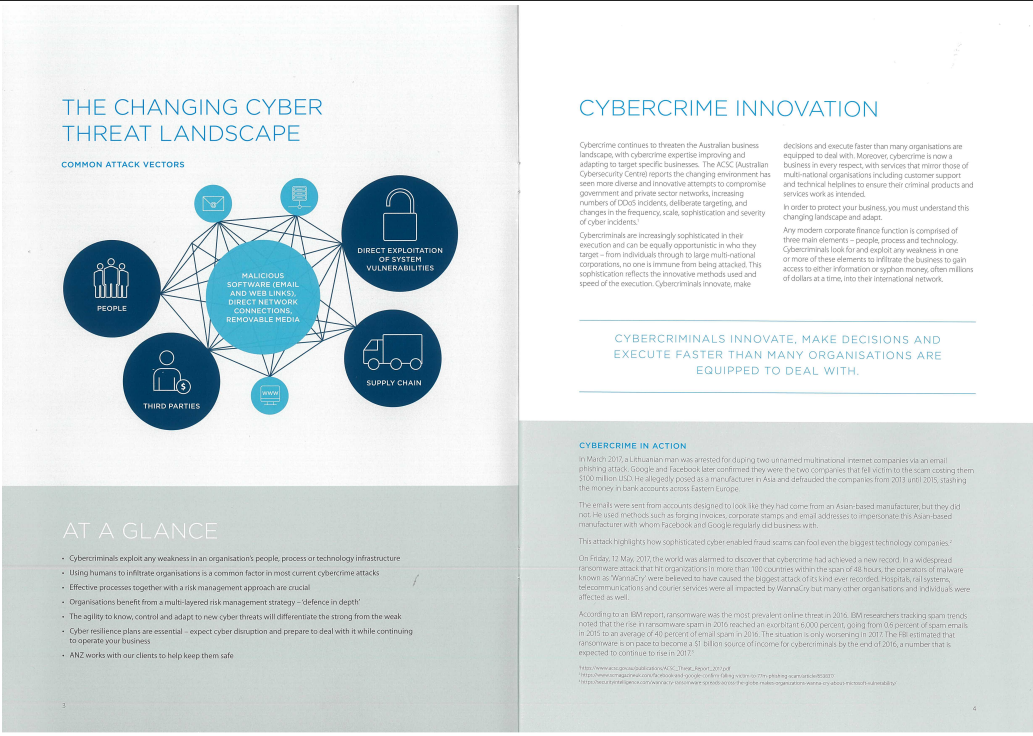
* *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
* *Find the contents of this file and include it in your report.*

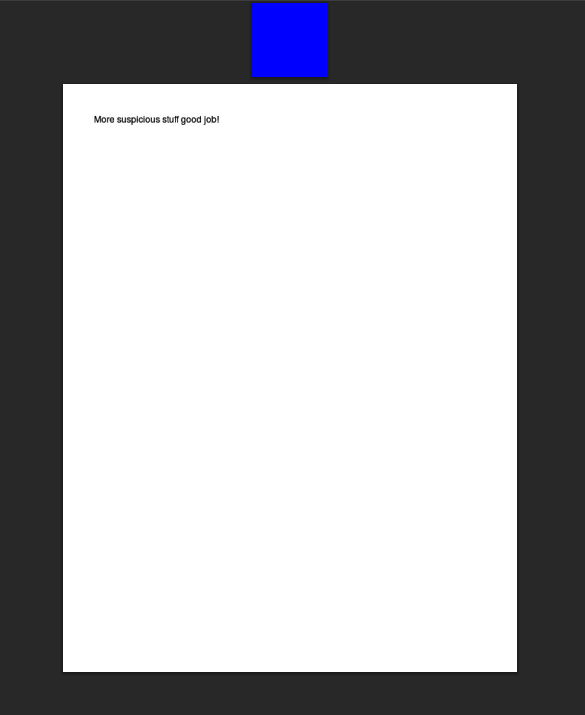
Step 1: Find target

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.*
* **
* **

**

**Sub-task 5:**

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

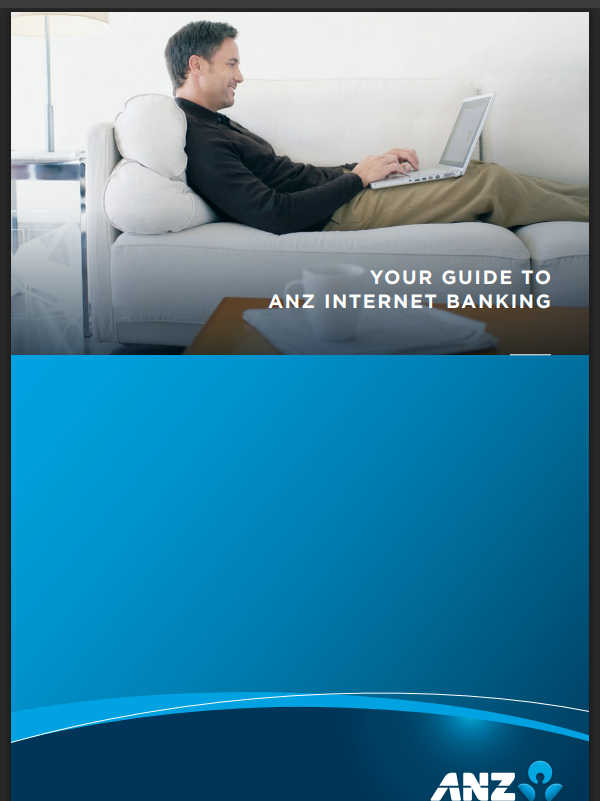
**Sub-task 6:**

* *The user accessed an image called "atm-image.jpg"*
* *Identify what is different about this traffic and include everything in your report.*
* **
* *The image is blurry and it seems the quality has been made like this so that the faces cannot be identified, maybe because they were involved in some security threat or due to some security reasons.*

**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.*
* **
* **
* **Okay so this was the most difficult task of all first**
* **I copied all of the hex and saved it as zip**
* **Then I opened it , there was a pdf called rawpdf , I opened it and password was required**
* **Then I again went to the hex but this time I changed the format to ascii and at the last the password as written “secure” I entered the password and viola I completed all the tasks**