|  |
| --- |
|  |

**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.*



**ANZ1.jpeg ANZ2.jpeg**

Difference:

* ANZ1.jpeg follows the colour scheme of ANZ1.jpeg , ANZ2.jpeg doesn’t .
* ANZ2.jpeg has a text “MAKE A PACT”, ANZ1.jpeg doesnot have any text written on it.

**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.*

*Following is the content:*

Step 1: Find target

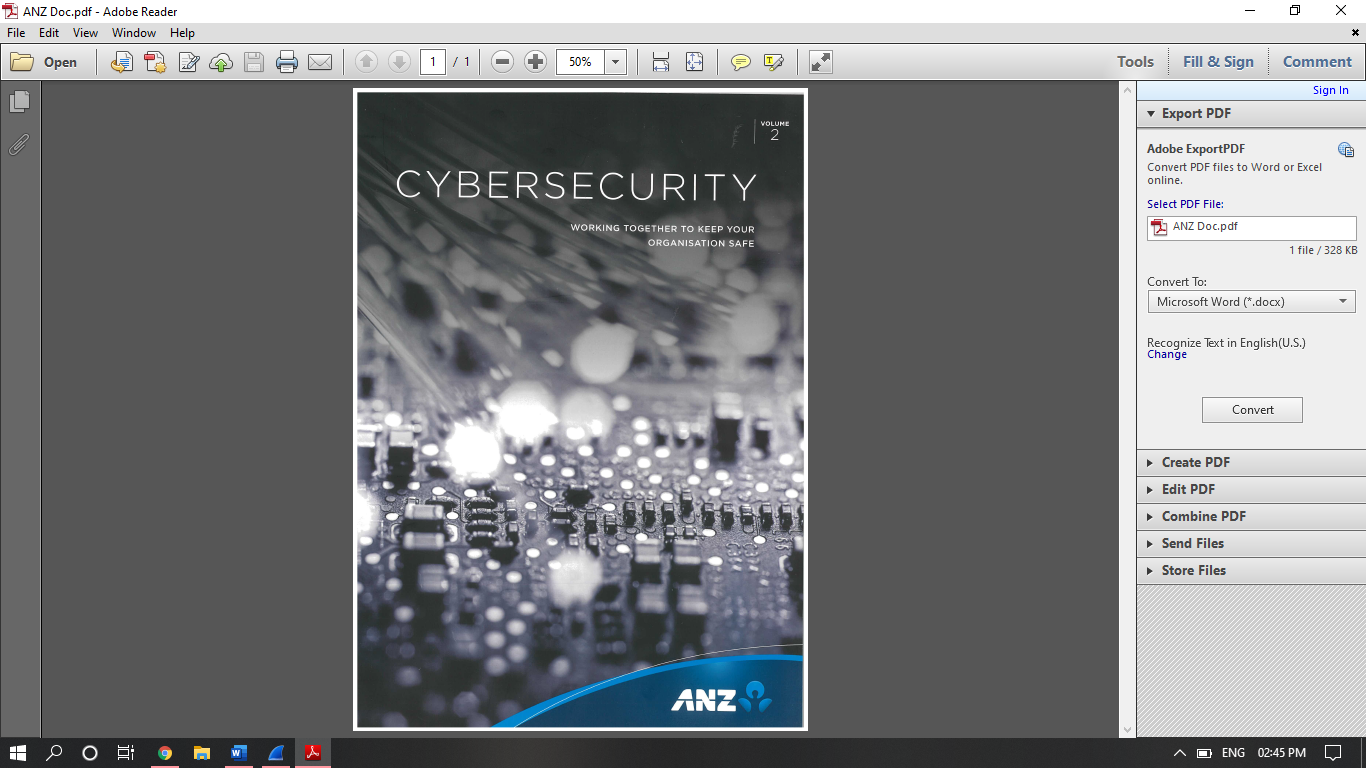
Step 2: Hack them

This is a suspicious document.

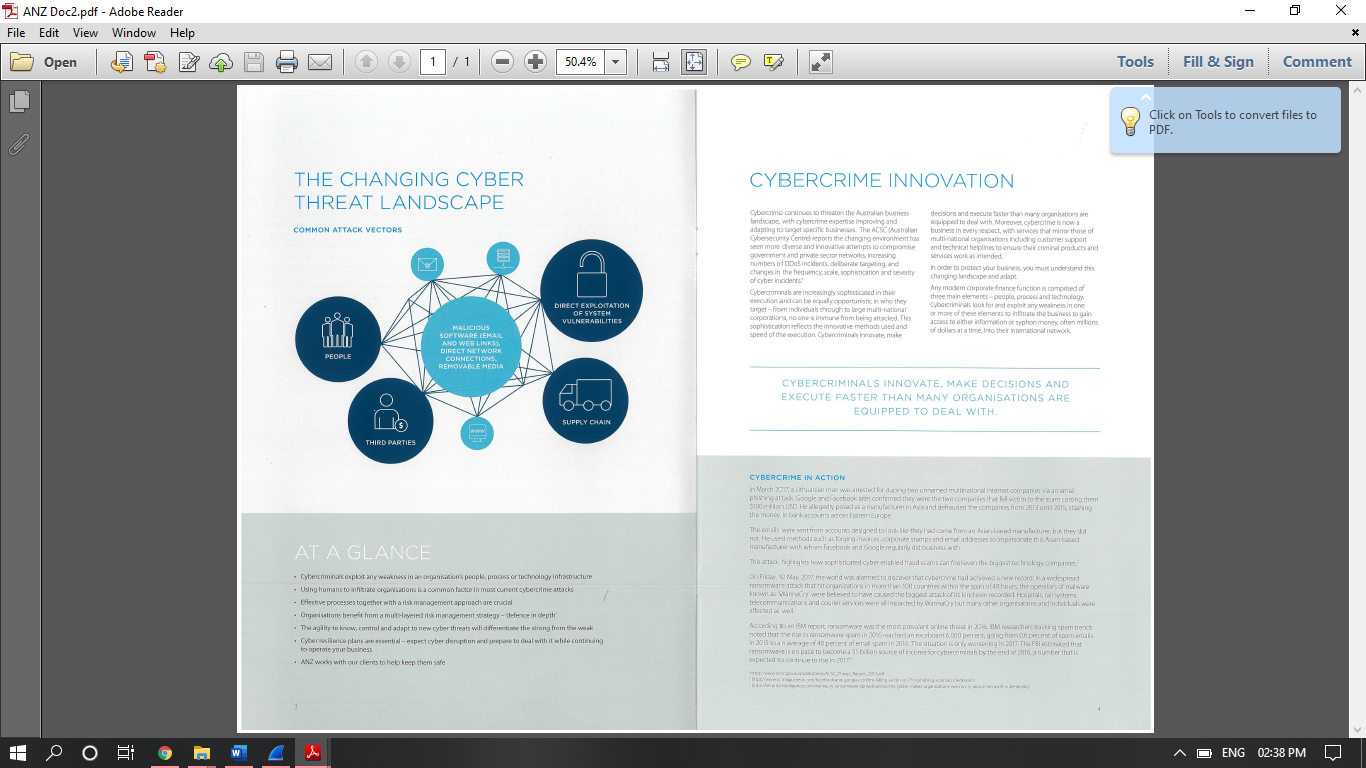
**Sub-task 4:**

* *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.*

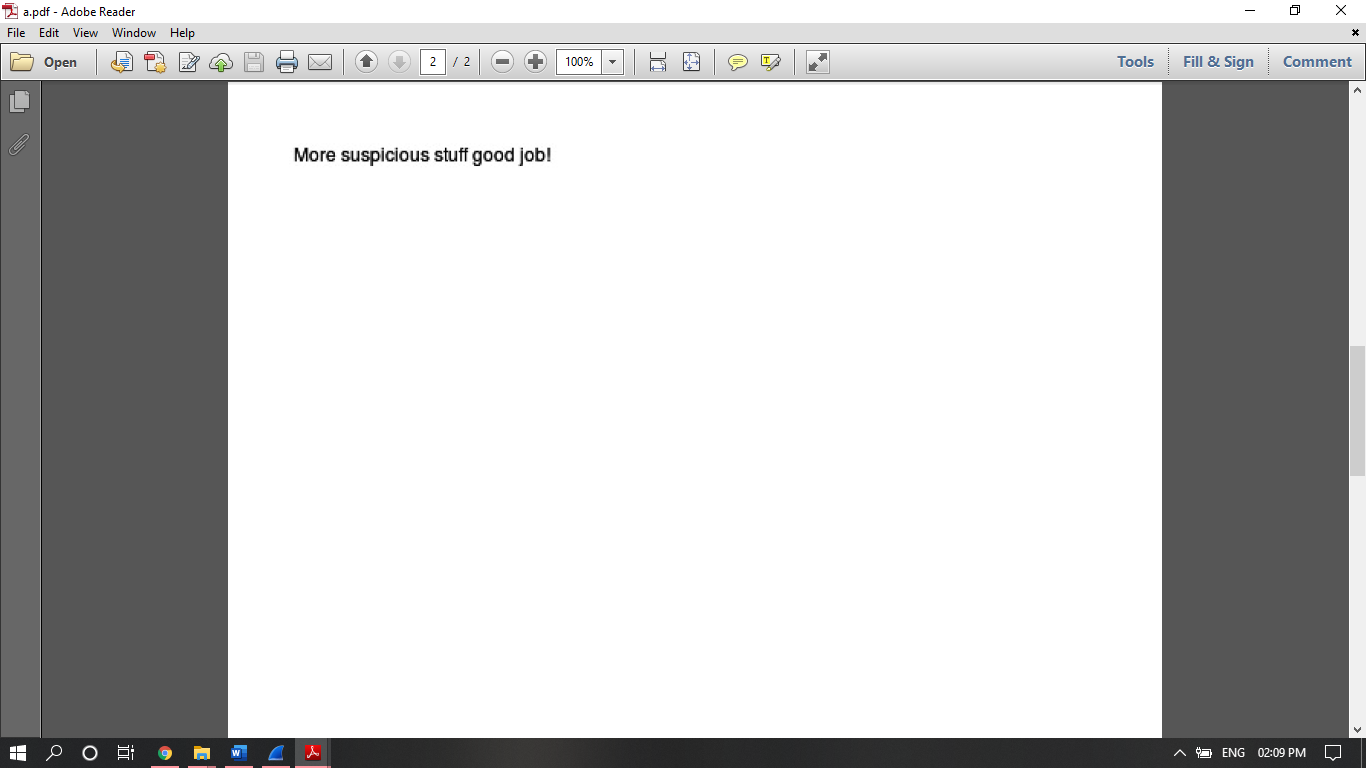
*ANZ\_Document.pdf:*

**

*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*

*Following is the content of the file:*



**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.*



* *It seems that the picture was clicked in a hurry, could be used for malicious activities.*

**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.*

