A blue and white logo

Description automatically generated with medium confidence

**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.*

**Solution:**

I was able to extract anz-logo.jpg and bank-card.jpg from the pcap file. The steps to do this was as below:

1. Open the .pcap file in wireshark
2. Filter the traffic to isolate “http” packets
3. Locate the packets which correspond to “anz-logo.jpg”. Right-click on it and select “Follow > TCP Stream”
4. You will see a new window open with the packet contents, by default in ASCII. Notice that the Content-Type that shows up here is “image/jpeg”. To change the format, change the format at the field “Show data as” to any of your desire. Here, we will change the format to “RAW”.
5. Since this is a jpeg / jpg file, search for the start of the image parameters, it starts with the string “FFD8” and ends with the string “FFD9”. Highlight the contents between the start and end strings and copy them.
6. Open HxD editor and create a new file.
7. Paste the copied contents.
8. Save this file with .jpg format
9. Steps 3 to 8 apply for the file “blank-card.jpg” as well.

|  |  |
| --- | --- |
| Evidence 1: anz-logo.jpg | Evidence 2: bank-card.jpg |

**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.*

Solution:

I was able to extract ANZ1.jpg from the pcap file. Here, it appears that there is multiple jpg signature start and end strings. This could mean this is an edited image, multiple images could have been layered on this image. The image is essentially a poster talking about “steps to protect information.” The same applies to ANZ2.jpg

|  |
| --- |
| Evidence 3: ANZ1.jpg |
| Evidence 4: ANZ2.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.*

I was able to extract how-to-commit-crimes.docx from the pcap file. The steps to do this was as below:

1. Open the .pcap file in wireshark
2. Filter the traffic to isolate “http” packets
3. Locate the packets which correspond to “how-to-commit-crimes.docx”. Right-click on it and select “Follow > TCP Stream”
4. You will see a new window open with the packet contents, by default in ASCII. Notice that the Content-Type that shows up here is “application/vnd.openxmlformats-officedocument.wordprocessingml.document”. To change the format, change the format at the field “Show data as” to any of your desire. Here, we will change the format to “RAW”.
5. Since this is a docx file, search for the start of the image parameters, it starts with the string “50 4B 03 04”. Highlight the contents between the start and end strings and copy them.
6. Open HxD editor and create a new file.
7. Paste the copied contents.
8. Save this file with .docx format

Contents of the document (Evidence 5: how-to-commit-crimes.docx)

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.*

I was able to extract *ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf* from the pcap file. The steps to do this was as below:

1. Open the .pcap file in wireshark
2. Filter the traffic to isolate “http” packets
3. Locate the packets which correspond to “ANZ\_Document.pdf”. Right-click on it and select “Follow > TCP Stream”
4. You will see a new window open with the packet contents, by default in ASCII. Notice that the Content-Type that shows up here is “application/pdf”. To change the format, change the format at the field “Show data as” to any of your desire. Here, we will change the format to “RAW”.
5. Since this is a pdf file, search for the start of the image parameters, it starts with the string “25 50 44 46”. Highlight the contents between the start and end strings and copy them.
6. Open HxD editor and create a new file.
7. Paste the copied contents.
8. Save this file with .pdf format
9. Steps 3 to 8 can be repeated for ANZ\_Document2.pdf and evil.pdf

|  |
| --- |
| Evidence 6: ANZ\_Document.pdf |
| Evidence 7: ANZ\_Document2.pdf |
| Evidence 8: 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*

I was able to extract hiddenmessage2.txt from the pcap file. The steps to do this was as below:

1. Open the .pcap file in wireshark
2. Filter the traffic to isolate “http” packets
3. Locate the packets which correspond to “hiddenmessage2.txt”. Right-click on it and select “Follow > TCP Stream”
4. You will see a new window open with the packet contents, by default in ASCII. Notice that the Content-Type that shows up here is “text/plain”. To change the format, change the format at the field “Show data as” to any of your desire. Here, we will change the format to “RAW”.
5. Since this is a pdf file, search for the start of the image parameters, it starts with the hex string of the text in the file. Highlight the contents between the start and end strings and copy them.
6. Open HxD editor and create a new file.
7. Paste the copied contents.
8. Save this file with .txt format
9. However, this file has signature parameters of a jpg file. The output is as below

|  |
| --- |
| Evidence 9: hiddenmessage2.txt |

**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.*

I was able to extract hiddenmessage2.txt from the pcap file. The steps to do this was exactly as Sub-task 1:

This traffic had two signatures of jpg file, the image was extracted collectively, provided below. This seems to be an image of the ANZ atm.

|  |
| --- |
| Evidence 10: atm-image.jpg |

**Sub-task 7:**

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

I was able to extract broken.png from the pcap file. The steps to do this was exactly as Sub-task 1, with the change that the signature will be of the png file (89 50 4E 47 0D 0A 1A 0A). The file appears to be broken.

|  |
| --- |
| Evidence 11: broken.png |

**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.*

I was able to extract securepdf.pdf from the pcap file. The thing to note here is that the raw file had no pdf signatures, so it was possible that the extension has been changed. I tried different signatures, and the signature for zip file worked. The password was found in the ASCII format, right at the bottom.

1. Open the .pcap file in wireshark
2. Filter the traffic to isolate “http” packets
3. Locate the packets which correspond to “securepdf.pdf”. Right-click on it and select “Follow > TCP Stream”
4. You will see a new window open with the packet contents, by default in ASCII. Notice that the Content-Type that shows up here is “application/pdf”. To change the format, change the format at the field “Show data as” to any of your desire. Here, we will change the format to “RAW”.
5. Here, the signature for pdf file is not found, but signature for zip file was found. Search for the start of the image parameters, it starts with the hex string “50 4B 03 04”. Highlight the contents between the start and end strings and copy them.
6. Open HxD editor and create a new file.
7. Paste the copied contents.
8. Save this file with .zip format
9. For the password, open the file in ASCII via wireshark at step 4.

|  |
| --- |
| A picture containing text, font, line, screenshot  Description automatically generated  Evidence 12: Password of securepdf.pdf |
| A person lying on a couch using a computer  Description automatically generated with medium confidence  Evidence 12: securepdf.pdf |
| A screenshot of a computer  Description automatically generated with low confidence  Evidence 12: securepdf.pdf |