Analyzed the provided packet capture file using the free network analysis tool Wireshark.

It let me see some interesting http GET requests, which indicate that the user specifically requests information.

1:

Filtered the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image , then right clicked the image and followed its TCP stream in which I saw what looked like image data.

After finding the file signature "FFD8" the top, and the file footer "FFD9" at the bottom, I copied everything between those two points into the hex editor HxD and saved it as a jpg image.

2:

Similar to step 1 , which was to view the TCP stream, identify the images hex data, then copy and save that as a jpg file I repeated in same way
The difference in the network traffic for this images download I discovered was a hidden message in the data after the end of the image.
Which says "You've found a hidden message in this file! Include it in your write up."

This network traffic also had a message hidden in the same way.
It was "You've found the hidden message!"

3:

To find the contents of the document, I had to view the TCP stream of the http get request for the file. The documents contents were visible in the ASCII view and hence convert it accordingly.

4:

To view these PDF‟s I repeated the process and found the file signature for a PDF, which was the hex data “25 50 44 46”. I copied all the hex date from the file signature onwards into HxD and saved it as a pdf file and it worked for all three files.

5:

Viewed the TCP stream of this file, and noticed that instead of being plain text it was encoded data and when viewed as hex it had the same file signature as a jpg image. So I copied and saved the hex data with HxD and found that the text file was actually an image flie.

6:

Viewed the TCP stream as normal when investigating this traffic, and found two sets of jpeg file signatures. In the TCP stream I saw what looked like image data. Eventually it seems me as the same process might work as what I have done in step 1. So I repeated step 1 on finding the file signature “FFD8” the top, and the file footer “FFD9” at the bottom and then tried extracting both sets of data, and got two different images.

So the thing that is different about this traffic is that a single GET request performed by the user downloaded two images.