|  |
| --- |
|  |

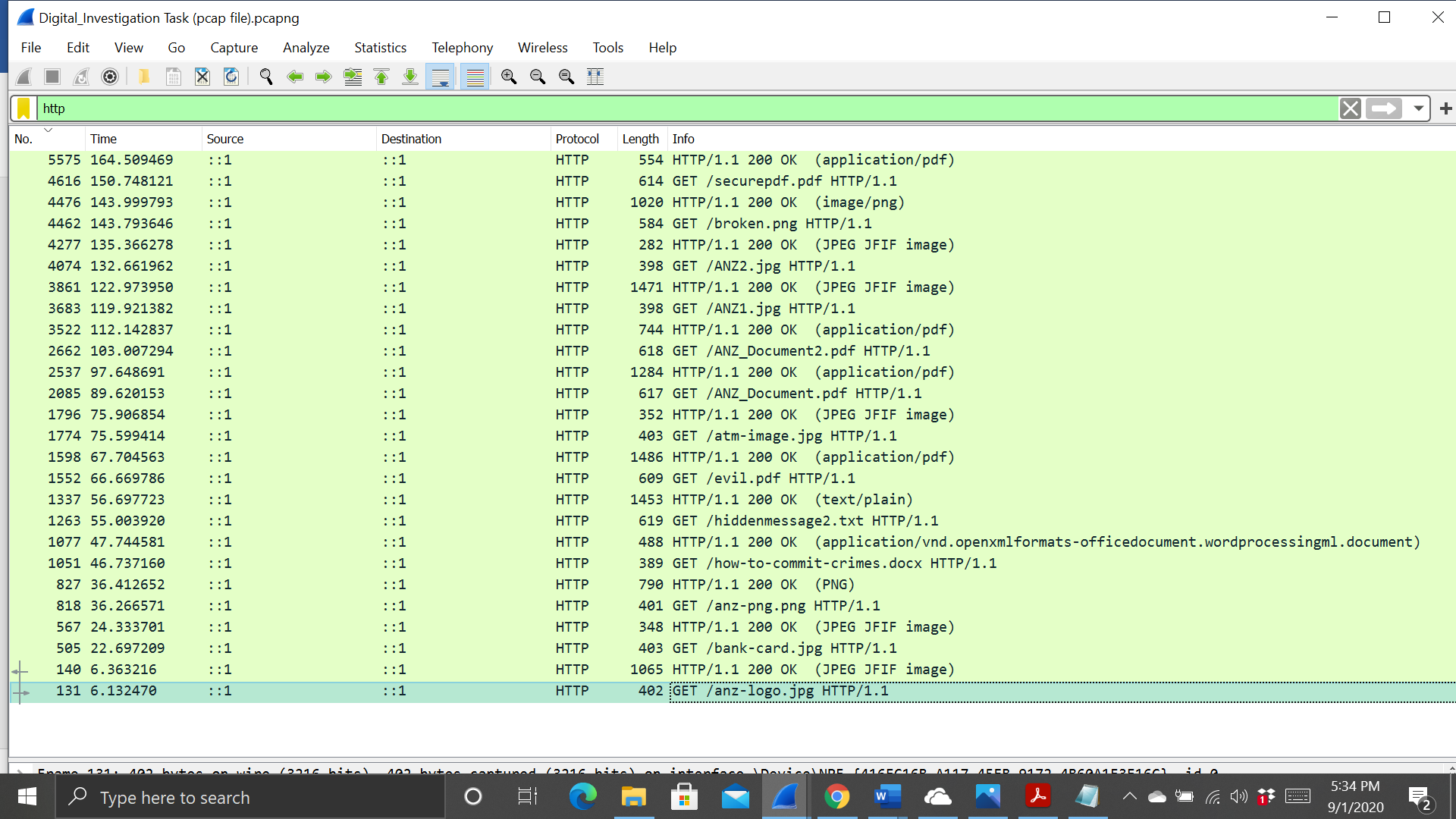
**Provide a report on your findings from the pcap file and outline what processes / the steps you followed to achieve this. Here are each of your sub-tasks with additional instructions. Please record your findings under each sub-task title.**

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.*

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including anz-logo.jpg and bank-card.jpg



To investigate this images , I viewed its TCP stream to see what I could find. The data is in the ASCII format so I changed it to RAW. Then I searched for the jpeg hexadecimal file signature “FFD8” in the search bar at the bottom. This shows where the data for the image begins. Then I searched for the file footer of jpeg “FFD9” will show the image data ends.   
  
The next step taken was carving out the images from the tcp stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program HxD. I then saved the file as a jpg and opened it, resulting in the image below.



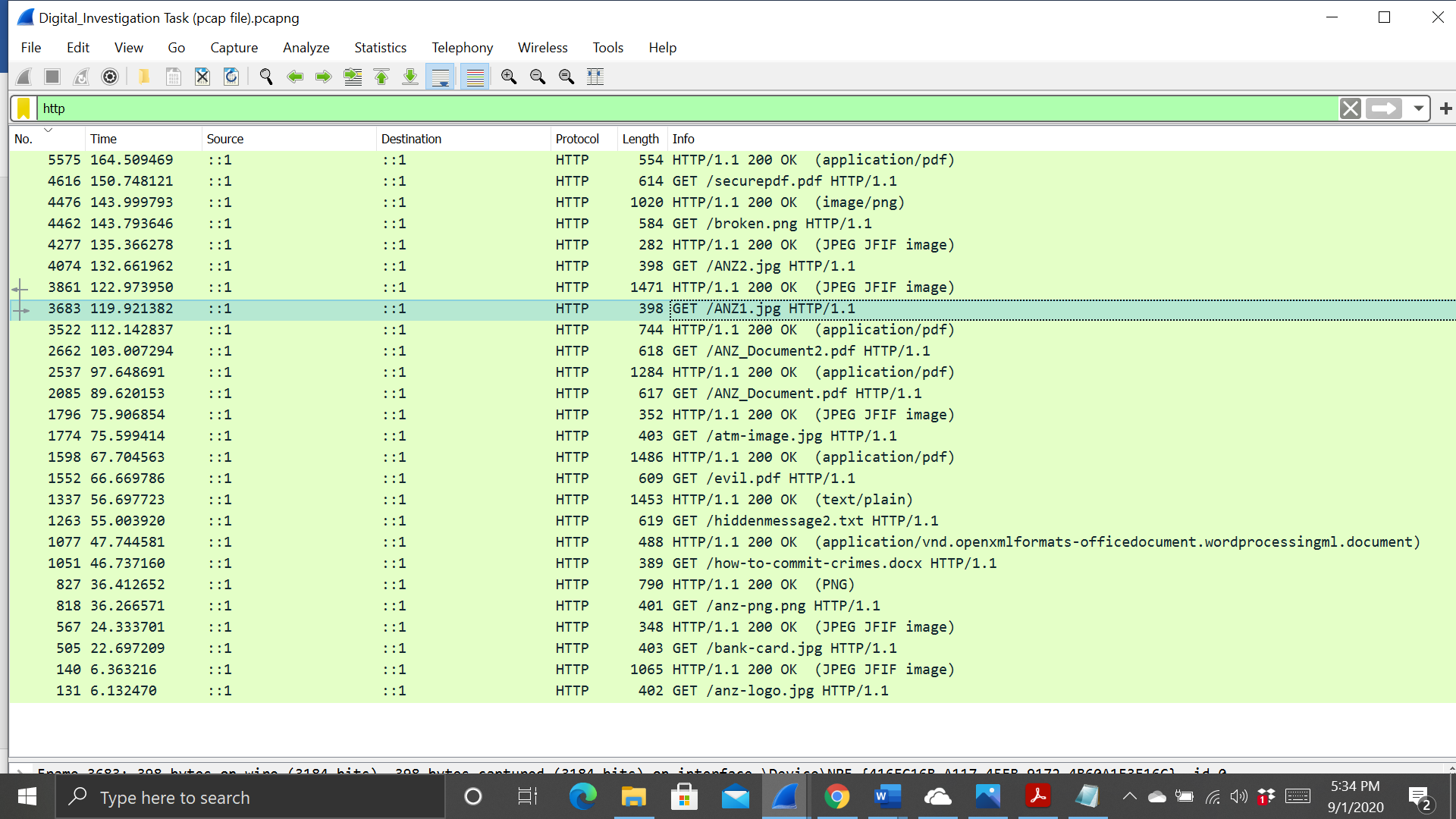


Sub-task 2:

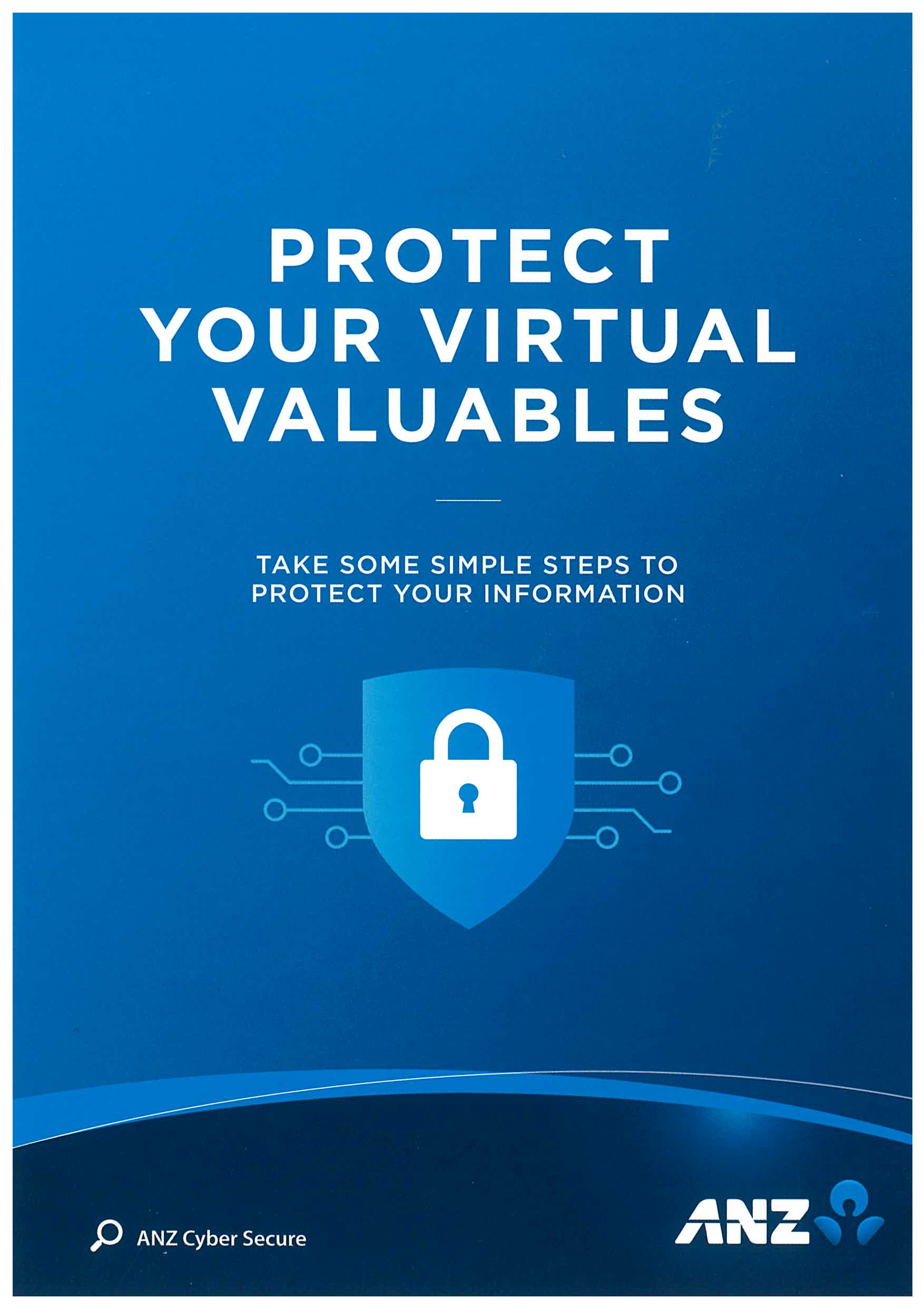
* *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
* *Extract the images, include them and mention what is different about them in your report*

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including ANZ1.jpg and ANZ2.jpg



To investigate this images , I viewed its TCP stream to see what I could find. The data is in the ASCII format so I changed it to RAW. Then I searched for the jpeg hexadecimal file signature “FFD8” in the search bar at the bottom. This shows where the data for the image begins. Then I searched for the file footer of jpeg “FFD9” will show the image data ends.   
  
The next step taken was carving out the images from the tcp stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program HxD. I then saved the file as a jpg and opened it, resulting in the image below.



This Image shows ANZ Cyber secure, it provides some information about protecting information in simple steps.



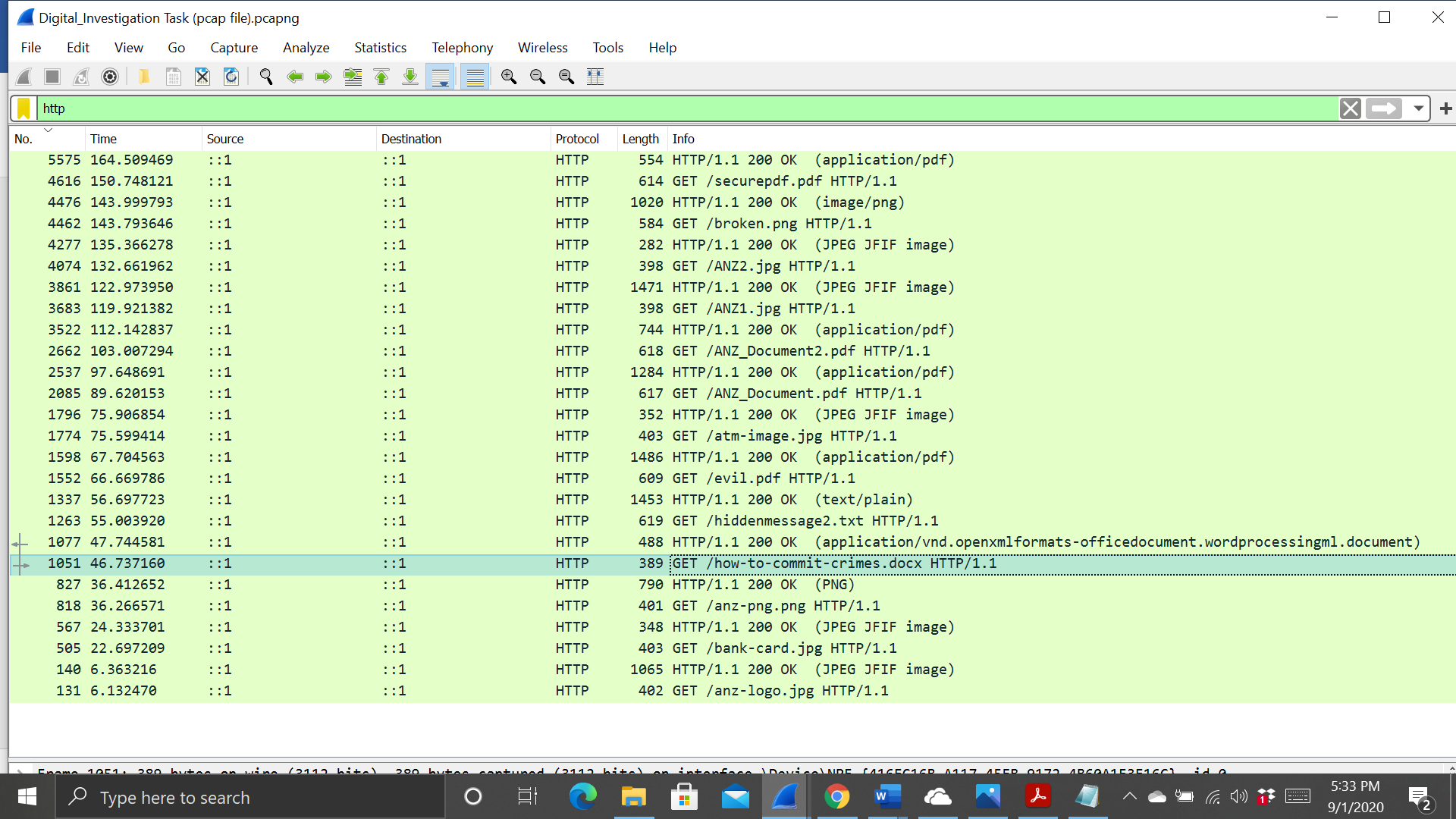
This image provide some useful information on how to protect from threat and provide email and contact number to ANZ if find any suspicious thing.

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.*

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including how-to-commit-crime.docx



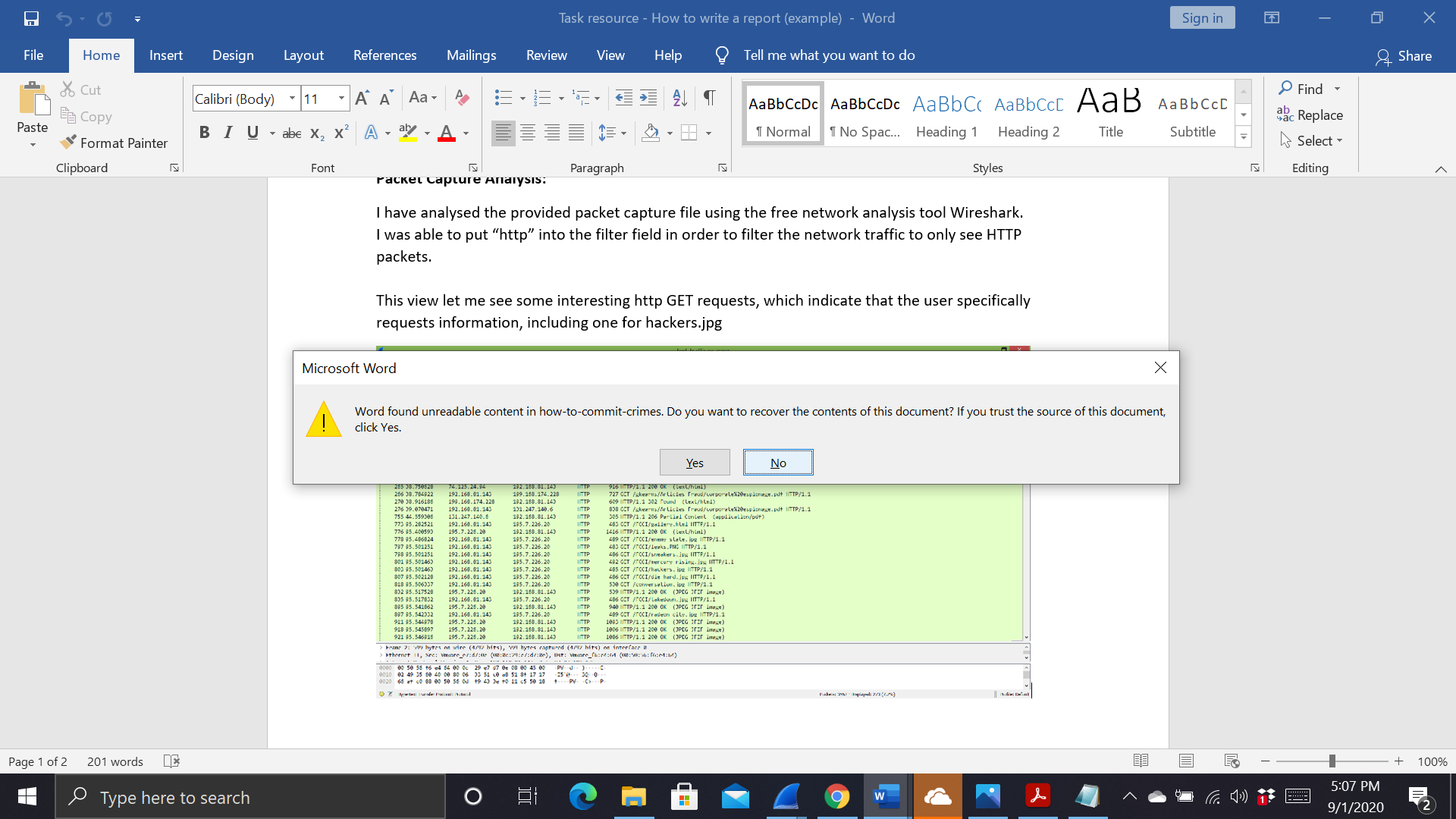
To investigate this document, I had to view the TCP stream of the http get request for the file. The documents contents were visible in the ascii view.

The full document contained the message:  
“Step 1: Find target

Step 2: Hack them

This is a suspicious document.

“

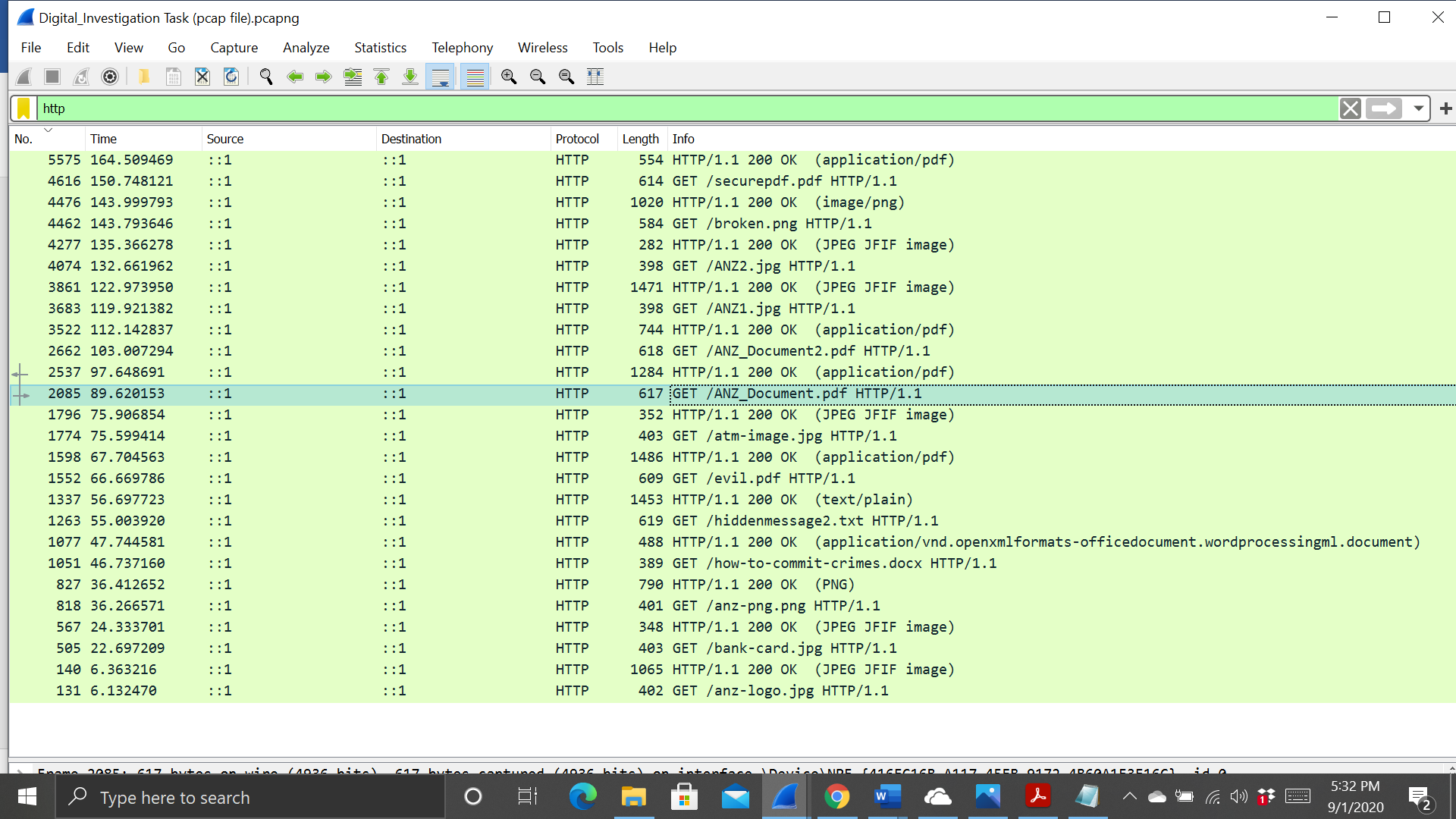


Sub-task 4:

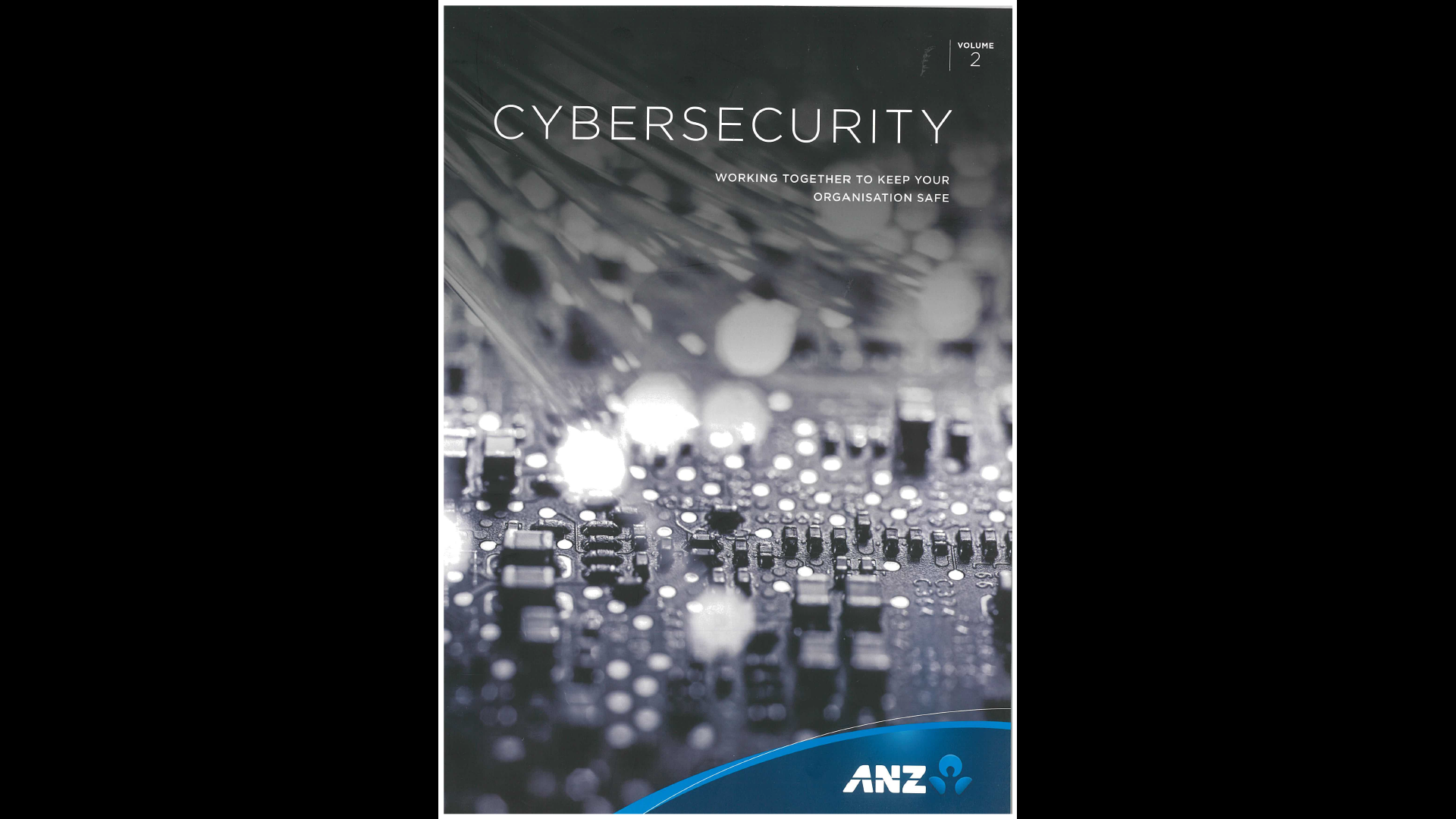
* *The user accessed 3 pdf documents: ANZ\_Document.pdf, ANZ\_Document2.pdf, evil.pdf*
* *Extract and view these documents. Include images of them in your report.*

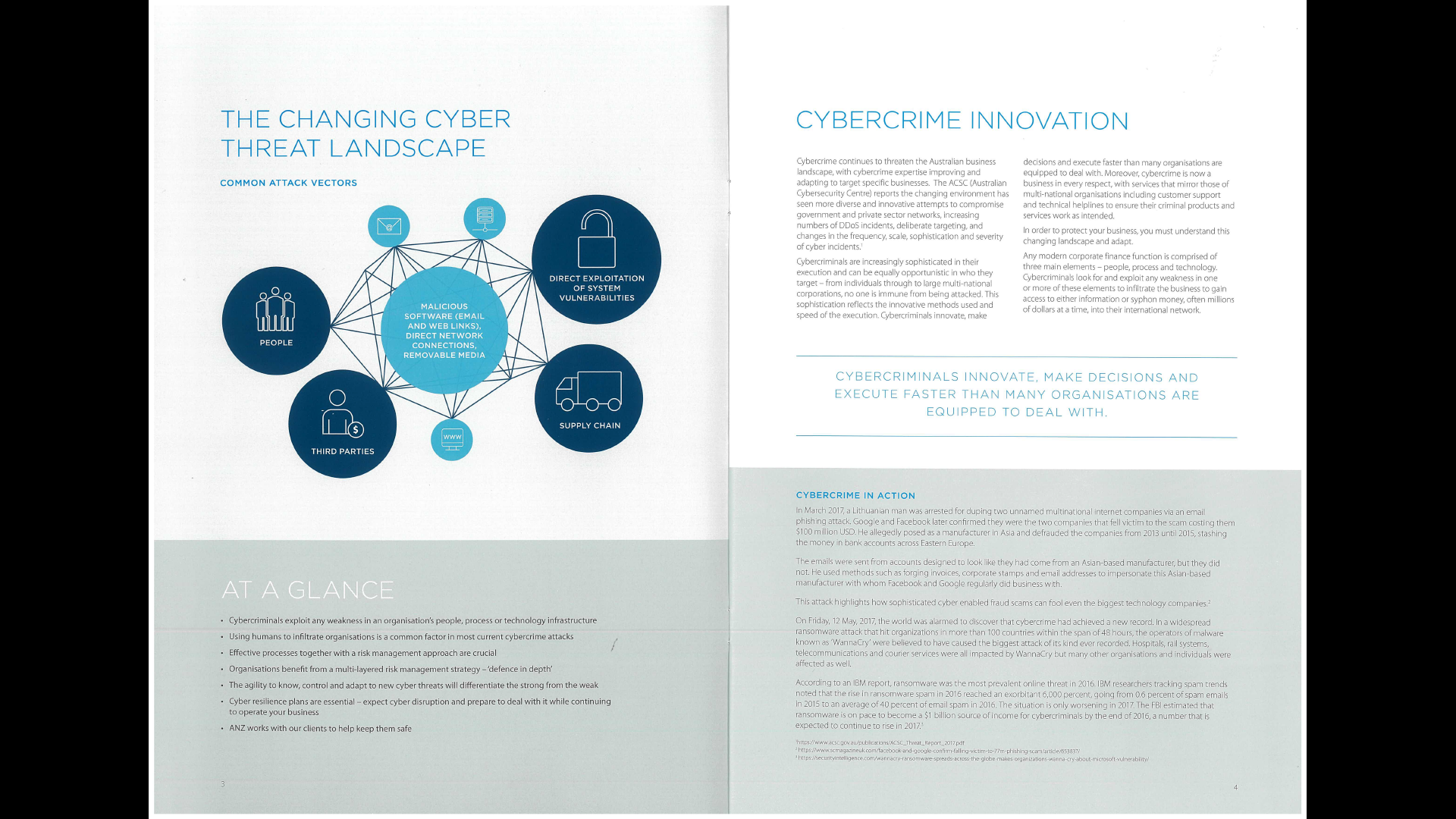
Packet Capture Analysis:

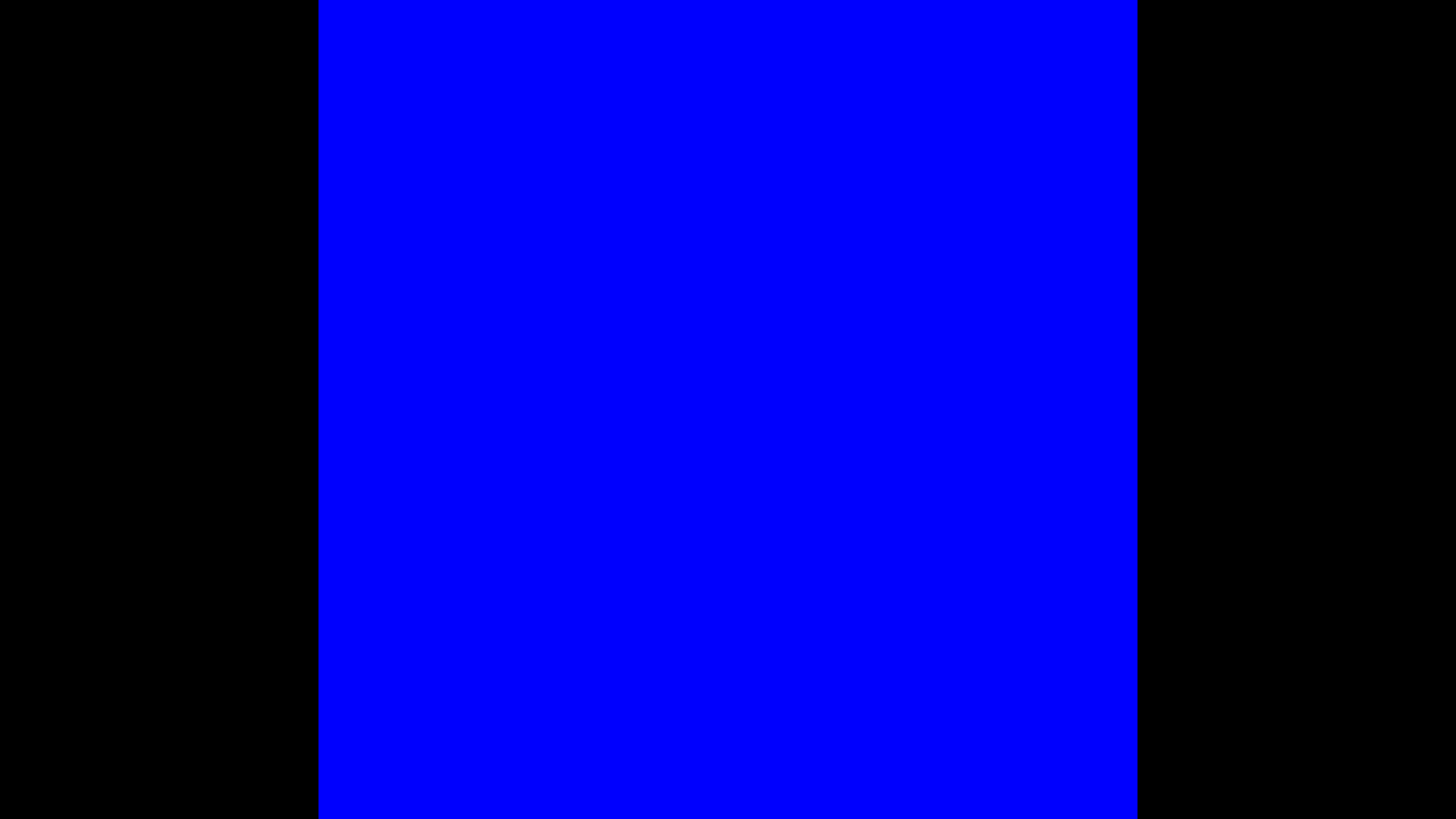
I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including ANZ\_Document.pdf, ANZ\_Document2.pdf and evil.pdf

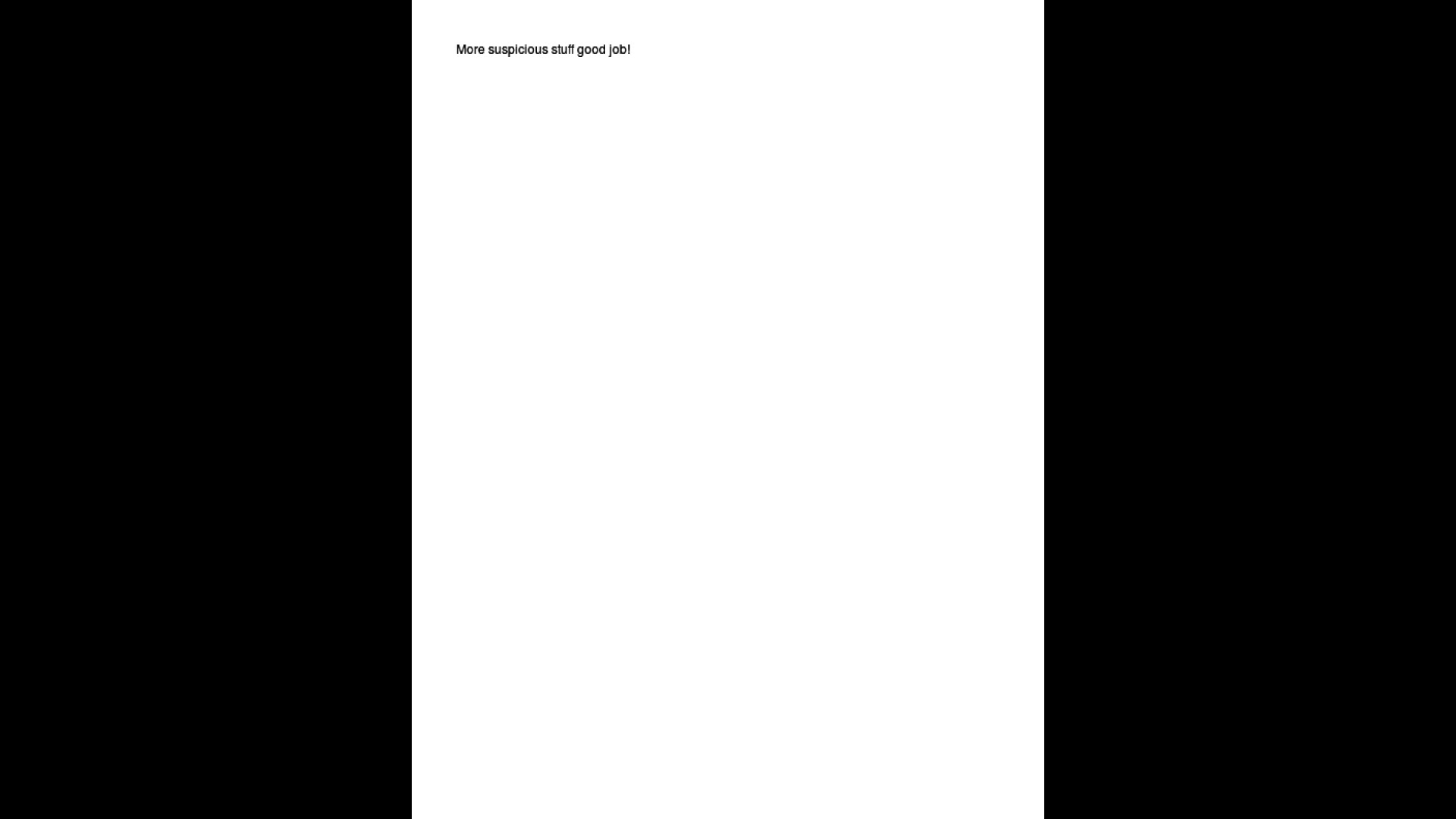


To investigate these PDF’s I viewed the TCP stream as usual, the file signature for a PDF which is “25 50 44 46”. I noticed in the ascii view that the PDF data went until the very end of the TCP stream, so I copied all the hex date from the file signature onwards into HxD and saved it as a pdf file.







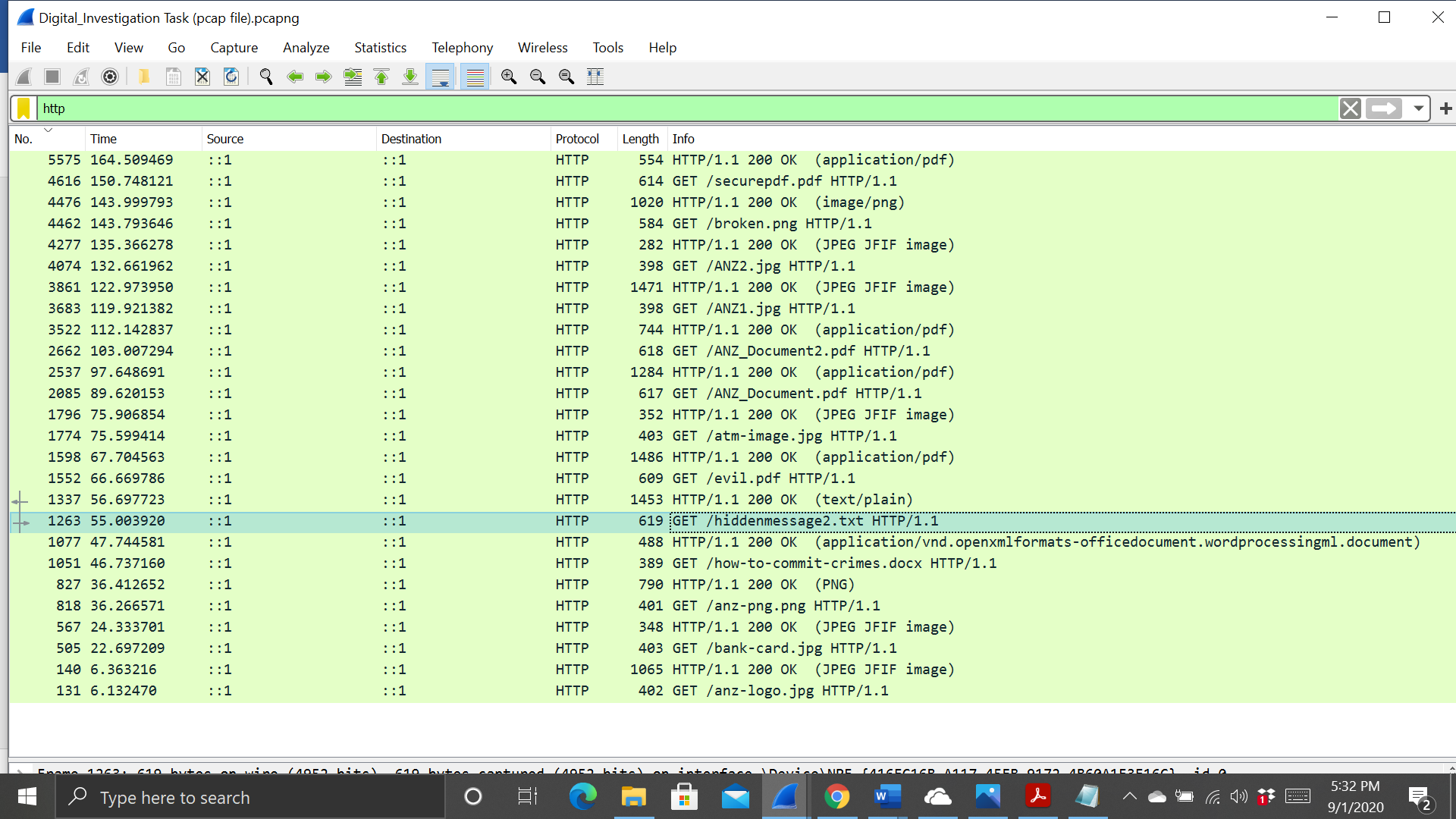


Sub-task 5:

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

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including hiddenmessage2.txt



To investigate this text file , the file was actually in jpg format but it as given .txt extension, while searching in search bar I found the header of jpg file “FFD8” and footer “FFd9”, then I copied the data into HxD editor and saved the image as hiddenmessage2.jpg.

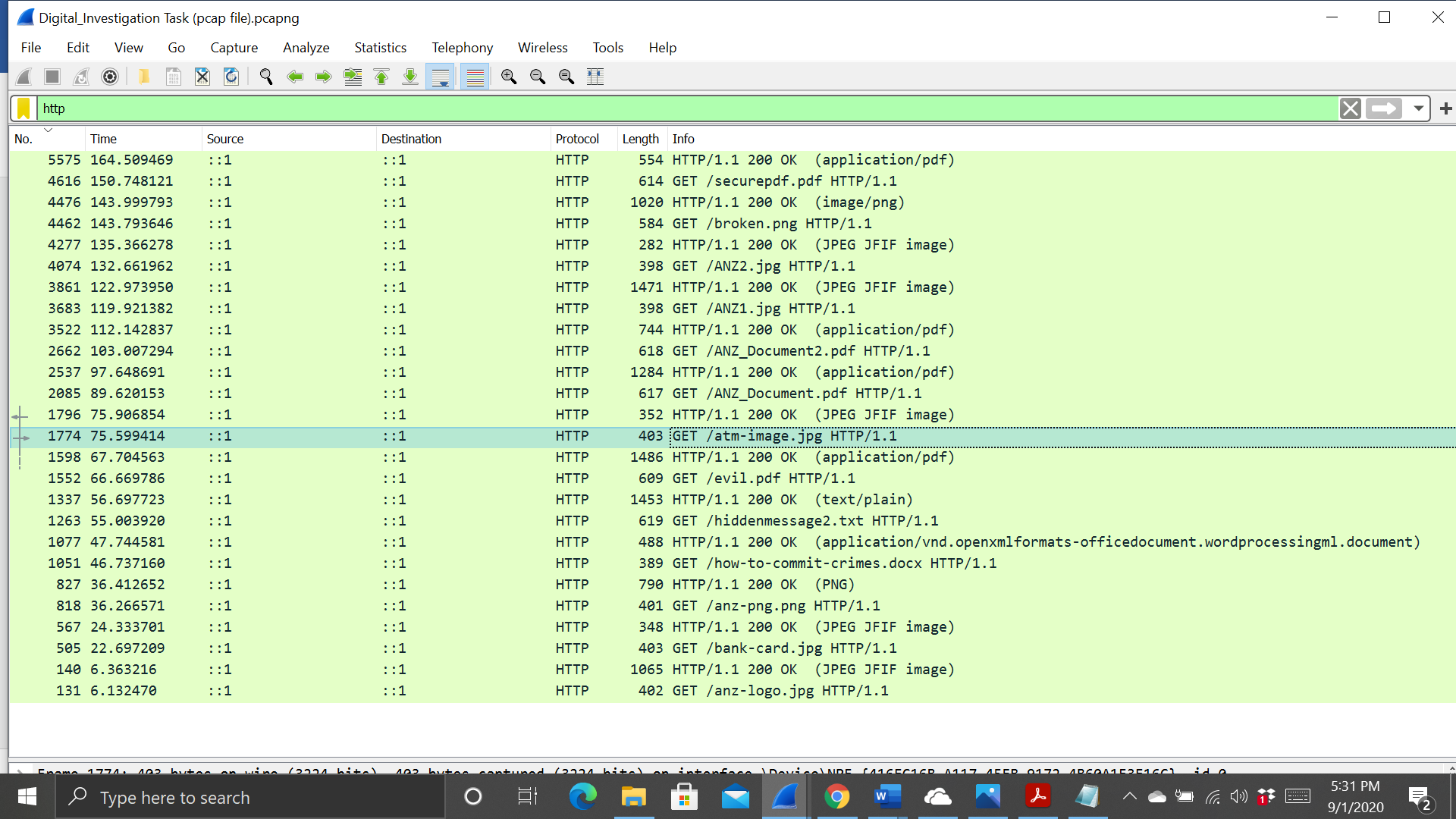


Sub-task 6:

* *The user accessed an image called "atm-image.jpg"*
* *Identify what is different about this traffic and include everything in your report.*

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including atm-image.jpg



To investigate this image , I viewed its TCP stream to see what I could find. The data is in the ASCII format so I changed it to RAW. Then I searched for the jpeg hexadecimal file signature “FFD8” in the search bar at the bottom. This shows where the data for the image begins. Then I searched for the file footer of jpeg “FFD9” will show the image data ends.   
  
The next step taken was carving out the images from the tcp stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program HxD. But I found two header while searching the header then I saved the both file as a jpg and opened it, resulting in the images below.



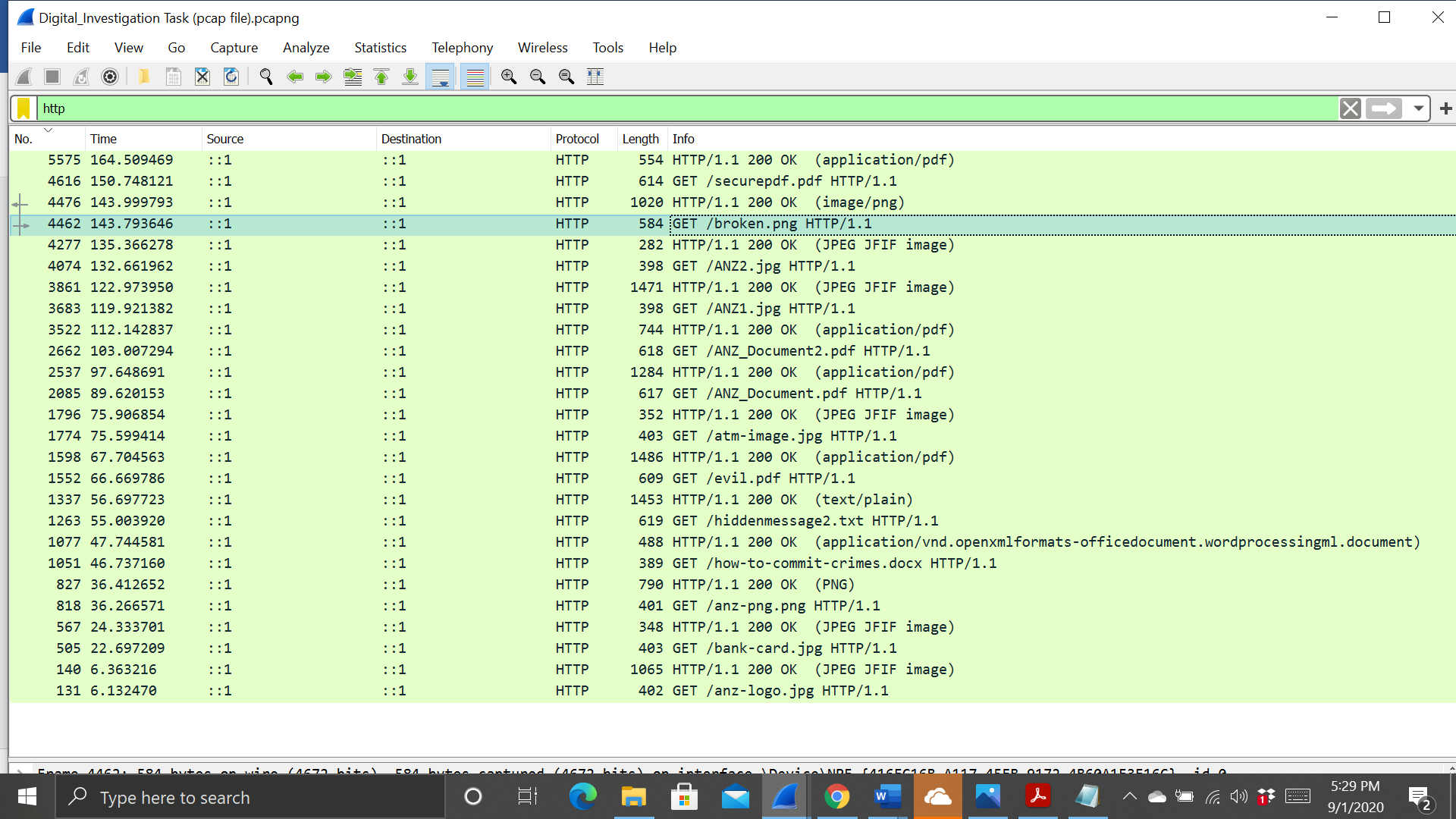


Sub-task 7:

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

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http requests, which indicate that the user specifically requests information, including broken.png



To investigate this image , I used the following steps first I selected the file or packet then I clicked on the file > Export object > HTTP. Wireshark has the ability to export files from HTTP. Then I selected the specific and saved it.

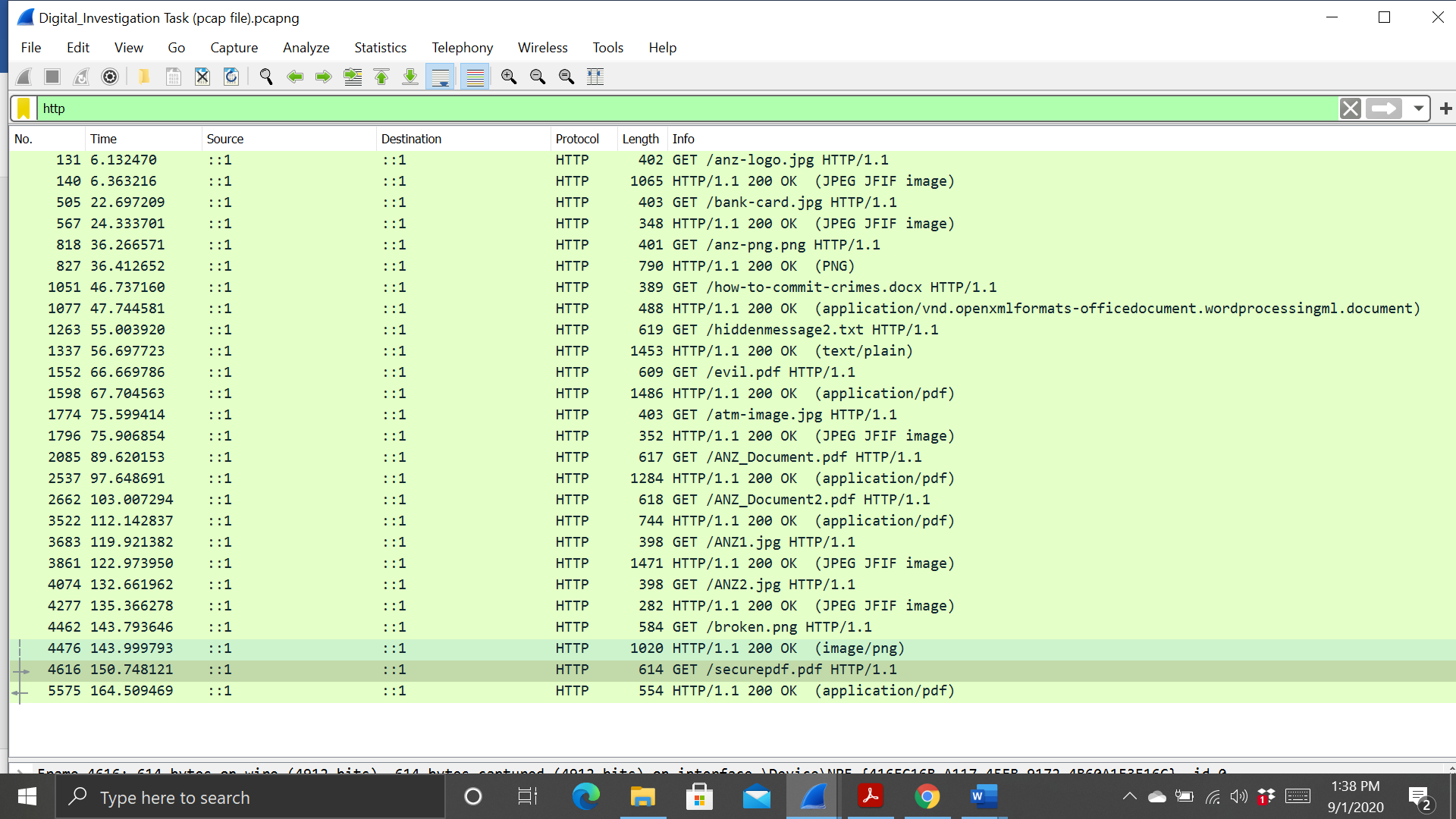


Sub-task 8:

* *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.*

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark.   
I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.   
  
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including securepdf.pdf



To investigate this pdf , The data there was not for a PDF. At the top of the file it shows rawpdf.pdf and at the bottom of the file which is ASCII format contained the message - Password is “secure” It contained the file signature for a zip file, means it is a zip file.  
  
So I copied the hex of the zip file into HxD and saved it as a zip file. I opened this zip file, and found it contained a pdf file called rawpdf.pdf. When opened, the pdf prompted for a password. The password ‘secure’ shown in the tcp stream worked. It was the first two pages to a guide for internet banking.

