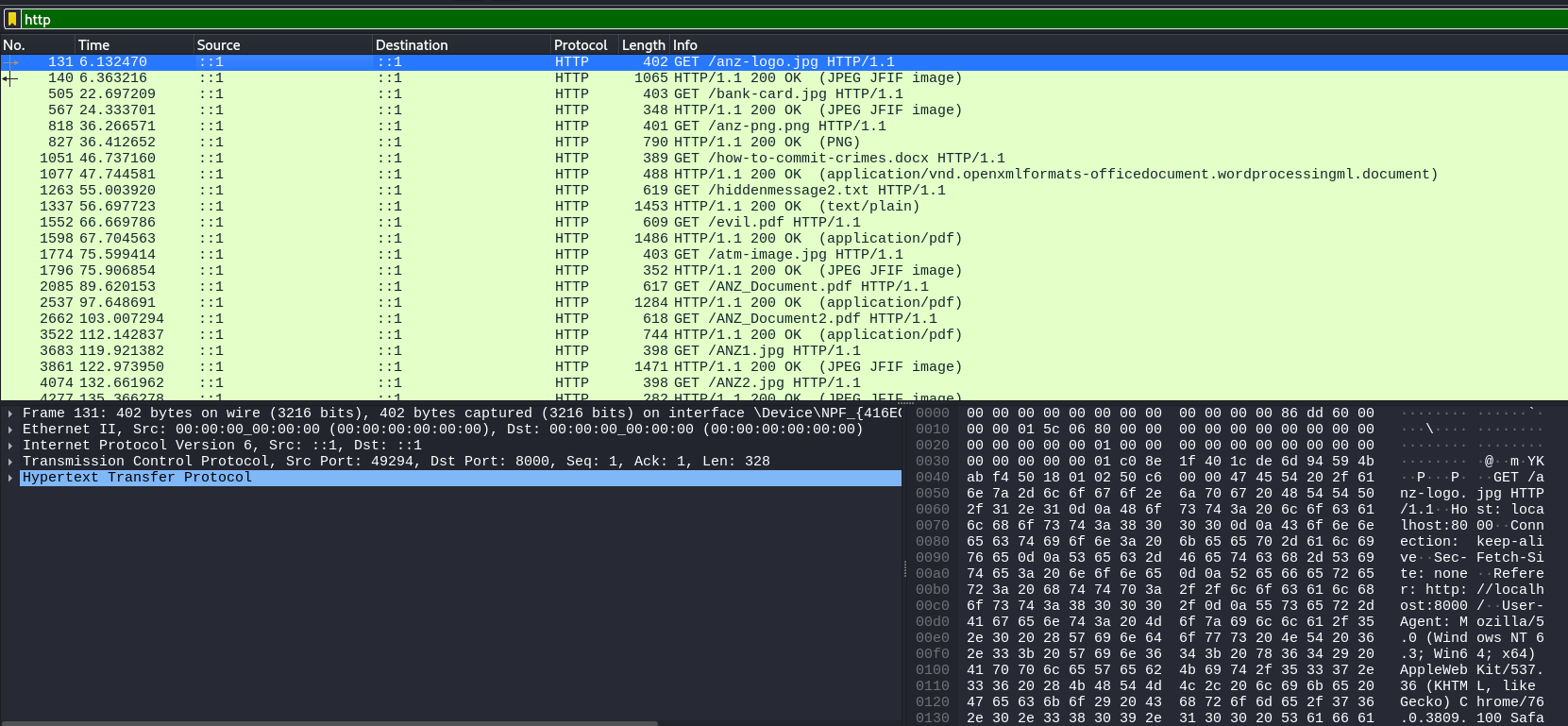
**Packet Capture Analysis: -**



1.) Found ***anz-logo.jpg***, extracted by following TCP stream of GET parameter of file then searching for file signature for jpg, which begins with – **FFD8** and ends with – **FFD9**



Then Used a hex editor (here HX Hex Editor) – pasting the hex values in a new file and saving it as “.jpg” extension, fetched the file which is readable by any photo viewer application

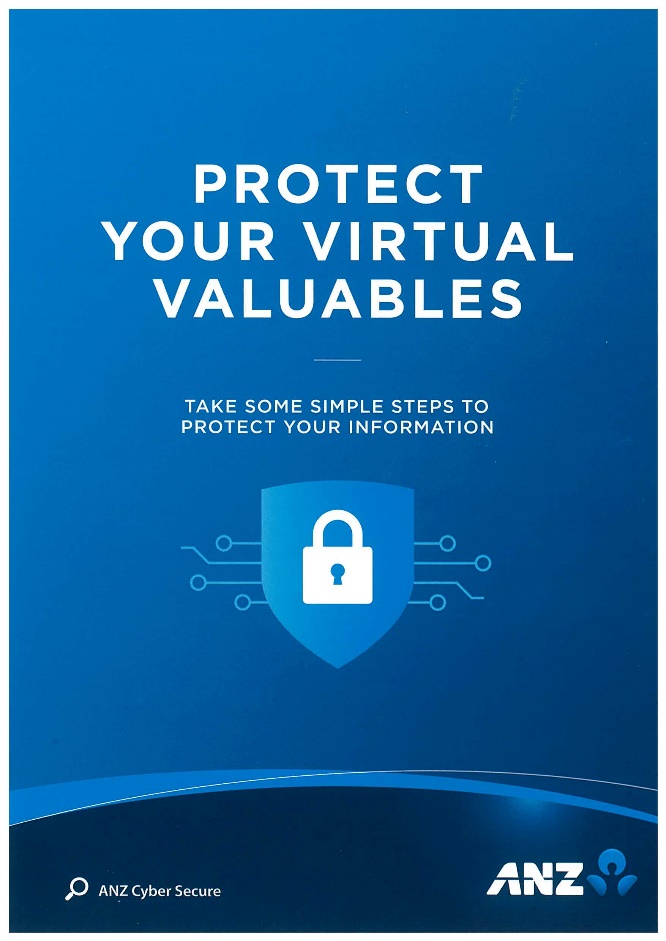


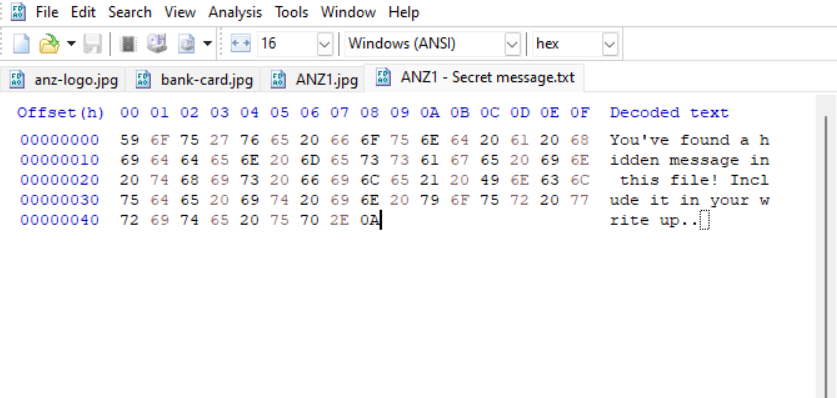
With same methods found other jpg files, all files are listed below: -

***Bank-card.jpg***



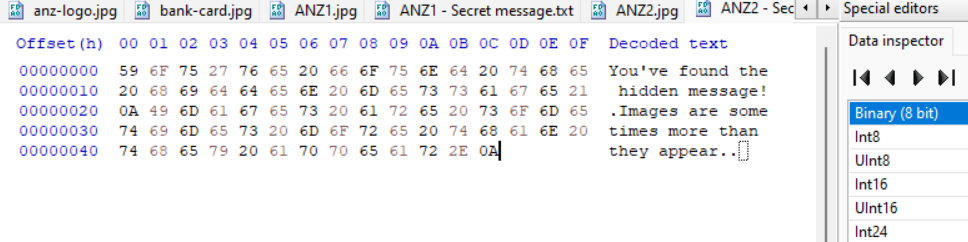
***ANZ1.jpg*** – While following TCP stream, there was some extra data at the end





***ANZ2.jpg*** – it also has similar hidden data in the end of the stream

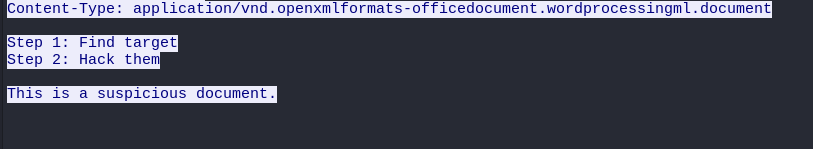




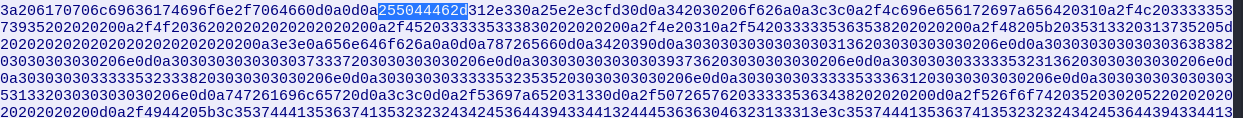
***Atm-image.jpg*** – Nothing Seems different for this stream/traffic

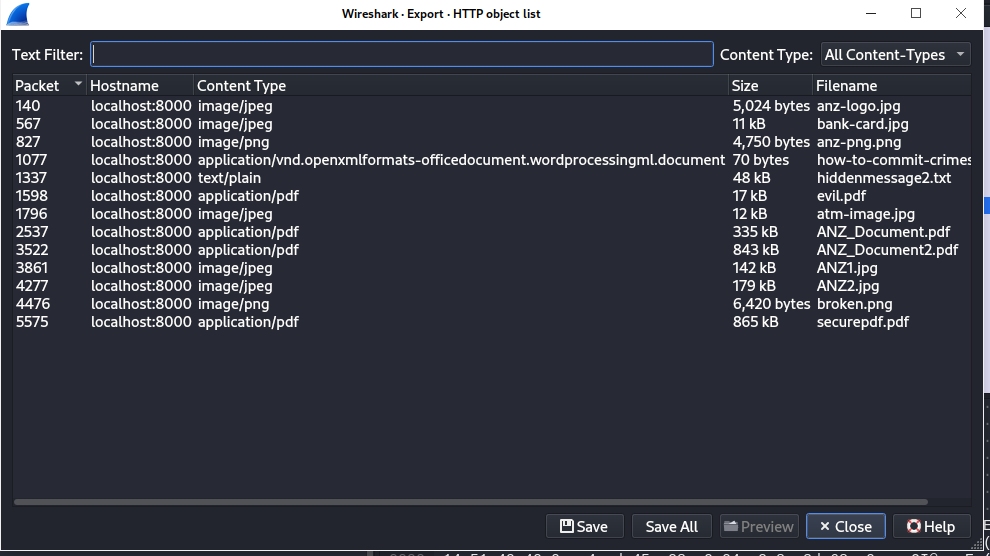


There is an office document file found during analysis named - ***how-to-commit-crimes.docx*** *–* content of files can be directly viewed in Wireshark, docx have file signature - **50 4B 03 04**

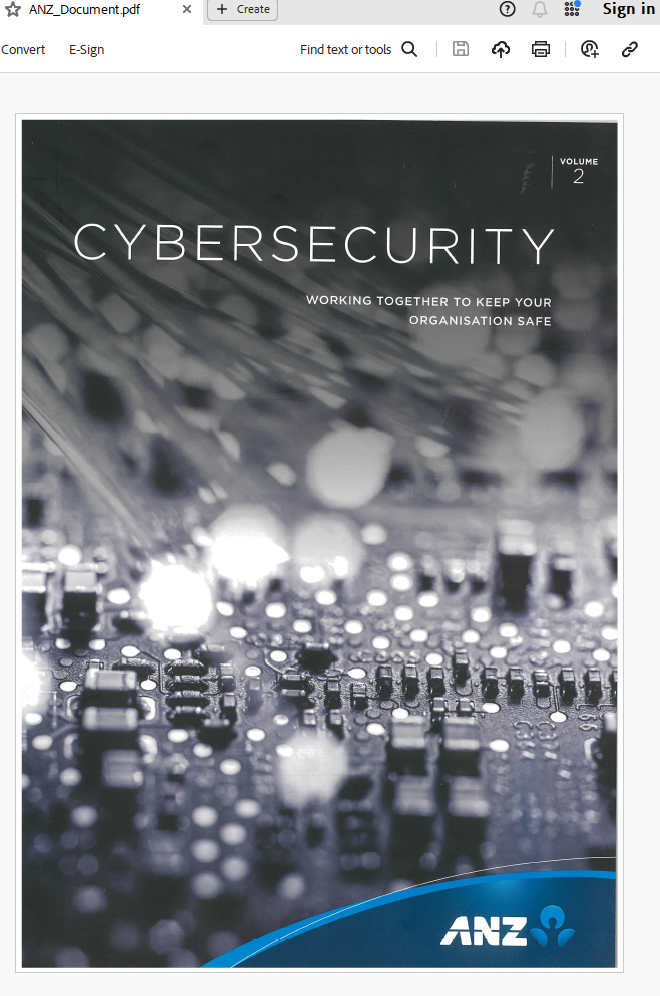


Now there are some PDF files (signatures to look for - **25 50 44 46 2D**), in Wireshark these kinds of large files can easily be extracted from **File -> Export Object -> HTTP**

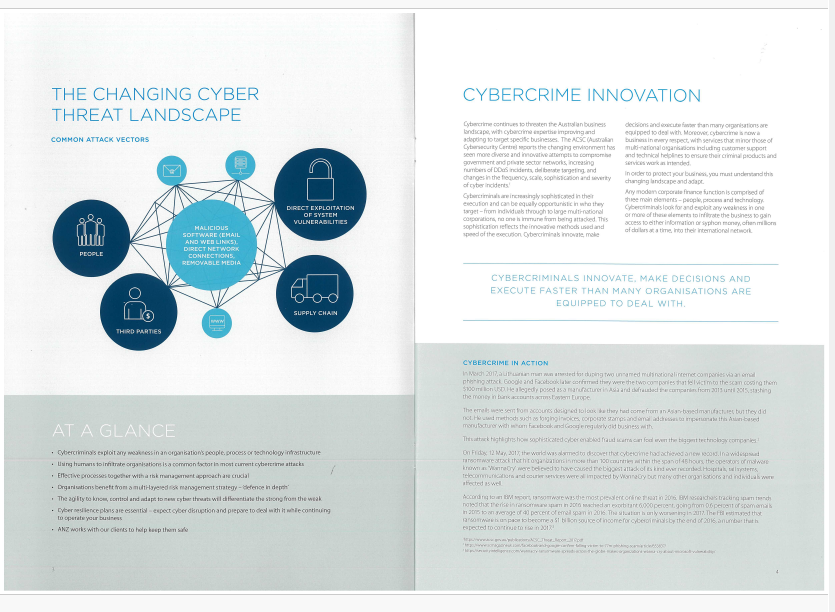




Extracting ***ANZ\_Document.pdf***



Same method Extracting ***ANZ\_Document2.pdf***



For ***Evil.pdf***

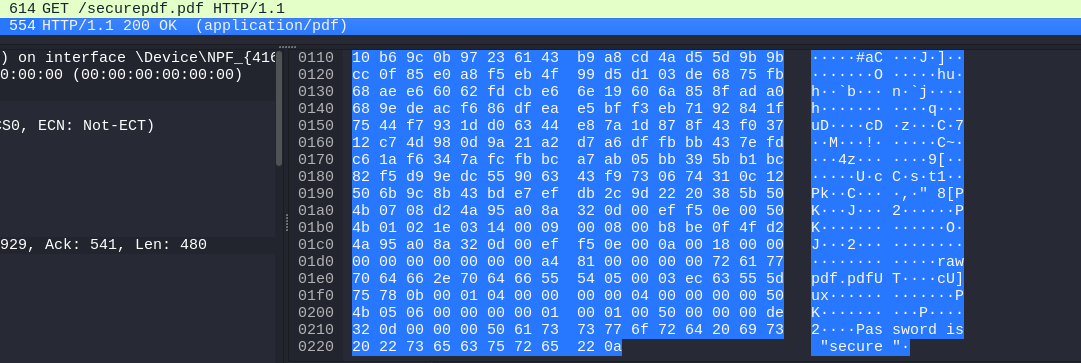


For file – ***securepdf.pdf***

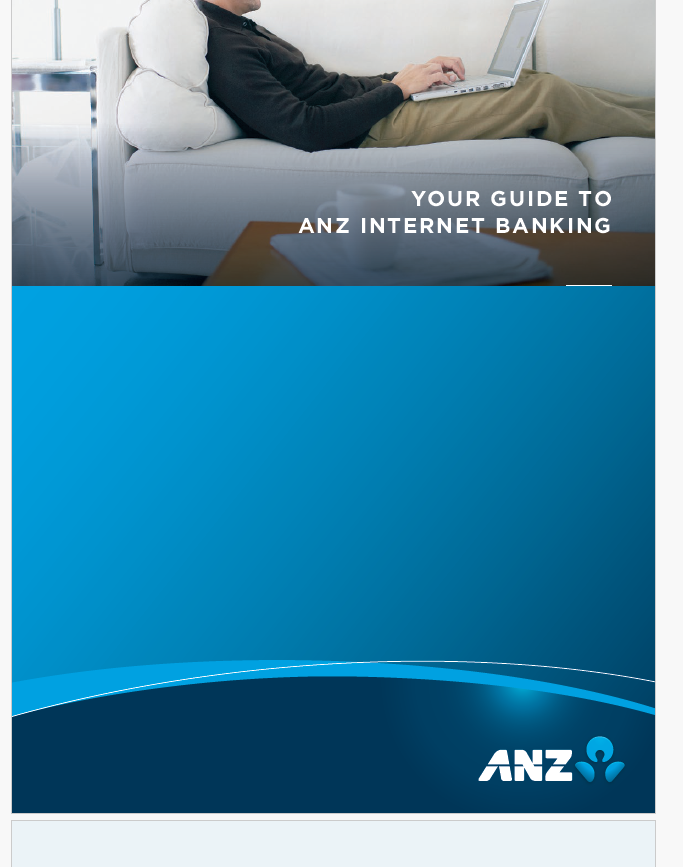
Shows garbage data, upon inspecting

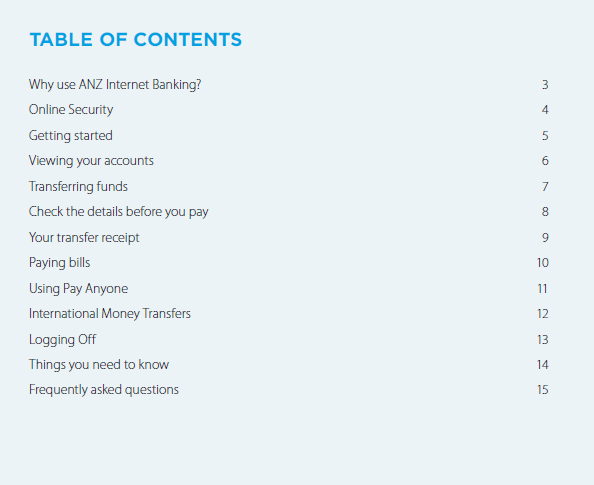


It’s a Zip archive need to be extracted, which is showing a password is needed to extracted which we can see in Http response for the get request – password is - ‘secure’



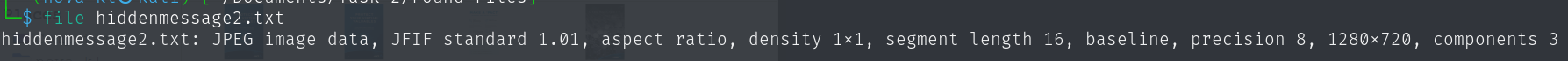
Upon extracting it





Same way extracted a text file – ***Hiddenmessage2.txt***

Although Opening file outputs garbage data, so executed file command to check if actually a txt file



Shows it’s a jpeg file, just changed the extension to ‘.jpeg’ – can be read by any photo viewer application

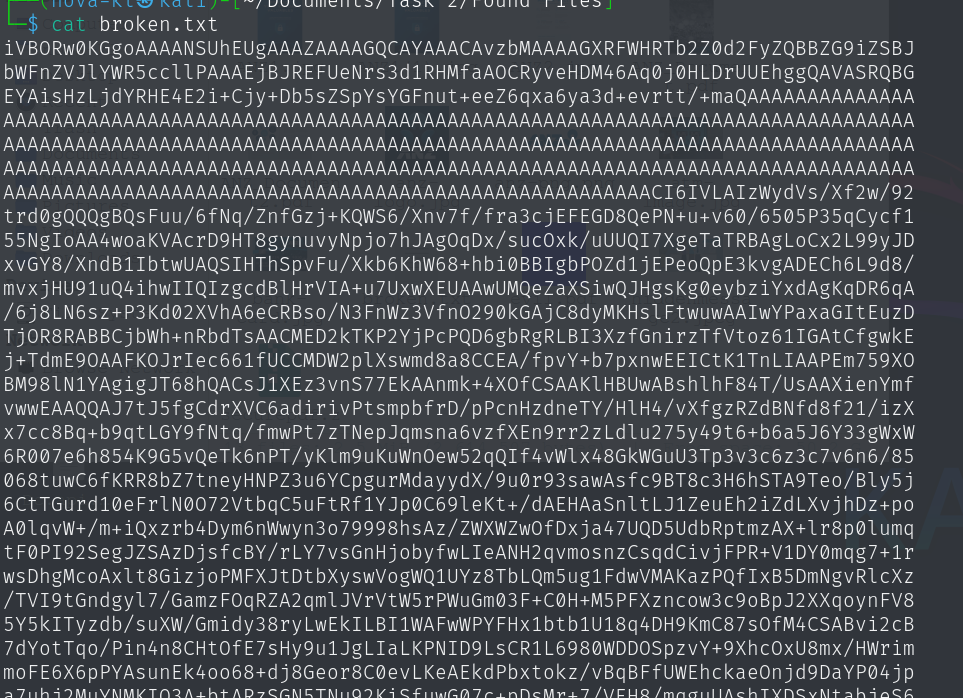


Found a PNG file – ***Broken.png***, which seems to be corrupted – (signature - **89 50 4E 47 0D 0A 1A 0A**)

File command shows it’s an ASCII text file



Renamed it to – ‘.txt’ extension and found that it’s **base64 encoded string** we can decode and view it with an online – base64 to image converter



Used following site - <https://base64.guru/converter/decode/image>

