1. Open the pcap file:

A screenshot of a computer

Description automatically generated

1. Find a FTP session:

A screenshot of a computer

Description automatically generated

1. Under File->Export Objects->FTP-DATA, save the FTP file:

A screenshot of a computer

Description automatically generated

1. Extract the ZIP file:

A screenshot of a computer

Description automatically generated

1. Use hexeditor to open the file extracted:

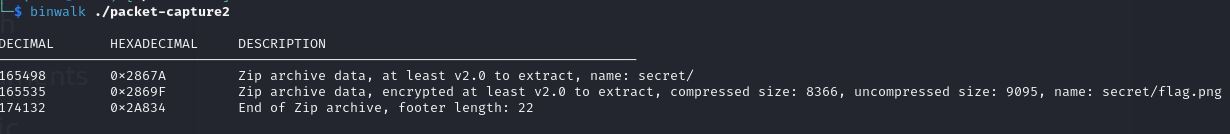
A screenshot of a computer

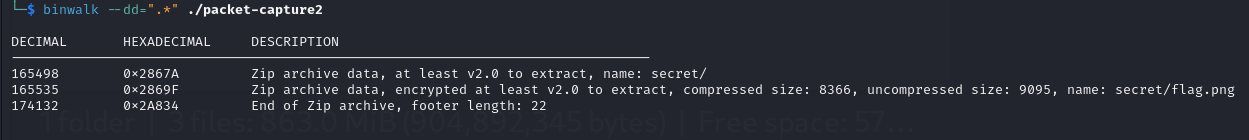
Description automatically generated

1. From the header FF D8 we can get to know, it’s a JPEG file but it’s corrupted ([List of file signatures - Wikipedia](https://en.wikipedia.org/wiki/List_of_file_signatures)), Fix the JPEG file (Change “DC E0” to “FF FF”), we can see an image but not a flag:

A group of men in a city

Description automatically generated

1. Use binwalk to check the fixed JPEG, there is ZIP file embedded:
2. Extract the ZIP file:



A screenshot of a computer

Description automatically generated

1. Try to extract folder “secret”, but need password:

A screenshot of a computer

Description automatically generated

1. Remember the image we got from previous steps, it shows “19991220”, try to input this as password, we can get the flag:

A black and white text

Description automatically generated

Flag: MOCSCTF{Y0u\_f1nd\_th3\_1ns1gh7!}