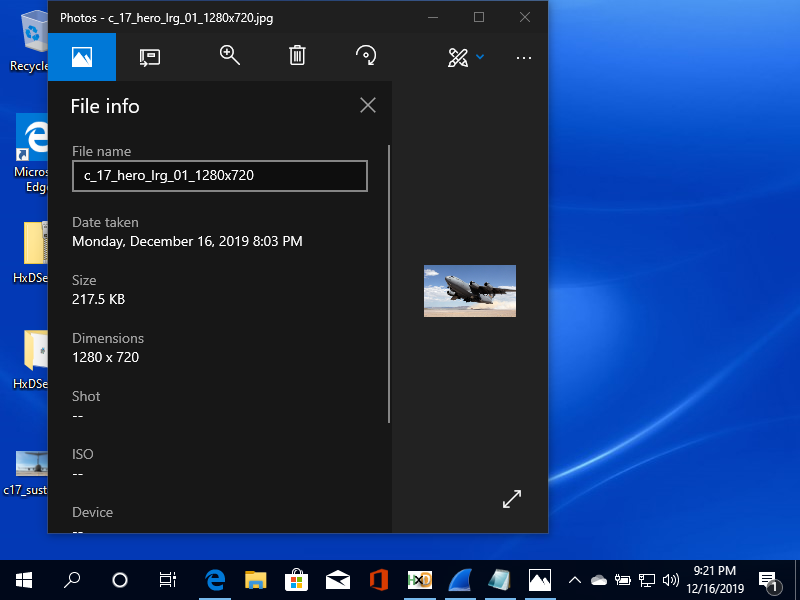
Yung Nguyen

CECS 378

Lab 8

* Part 1
  + 1. OS Type - Mac OS
  + 2. OS Version - Mac OS X 10.14.6, build 18G1012 (Darwin 18.7.0)
  + 3. Type of Web browser - Mozilla/Safari
  + 4. Web browser version - 5.0/13.0.3
  + 5. Hosting Web Address - www.boeing.com
  + 6. Date and Time of transfer - Dec 1, 2019 23:09:13.872796000 Pacific Standard Time
  + 7. Frame # from GET to Received Image - 2195 -> 2639
  + 8. Source IP Address of the server - Apple\_d3:49:68 (d0:03:4b:d3:49:68)
  + 9. Port # used for the transfer (server) - 80
  + 10. Destination IP Address of the client and port - Apple\_d3:49:68 (d0:03:4b:d3:49:68); port: 62698
  + 11. Port # used for the transfer (client) - 62698
* Part 2
  + 1. Type of image you are looking for- a .jpg image file
  + 2. File Signature of image - FF D8 FF E1 00
  + 3. Type of traffic protocol - Hypertext Transfer Protocol
  + 4. Why were you able to carve out the image?
    - WireShark lets you intercept data over the network and reassemble it in its original form, including attached image files in emails. This is done using its “Capture” function. It records all the data regarding communications between the host and the server (whatever you are trying to request from the server), in this case, in packet #2195, from the .pcap file (the entire session), where the image file is requested from boeing (host) and it returns it in the packet #2639. That image is what I was looking for. All I did was tell Wireshark to find the image (HTTP Protocol) which was the specific data section in Hex of the .pcap file, and export it to my computer. The image should be the same as the original image because it is the original image.
  + 5. Size of the image file (Include a screenshot)
    - 217.5 KB



* + 6. Hash the image file. Does it match the hashes provided? Explain either way
    - It does match the hashes provided because like I have explained, the image I extracted IS the original image sent by the server to the client. WireShark simply “captured” all data, the original data, of the entire session of the client with different hosts in the .pcap file. And the image is one of those data captured.