Assignment & Instructions

For all and each question, please Label your answer with the question (e.g. Part I – (1-3) or Part III (2))

along with the instructions that are being asked. In this lab you should be looking for specific pieces of

information

* You are to find the following image.

A picture containing sky, plane, runway, outdoor

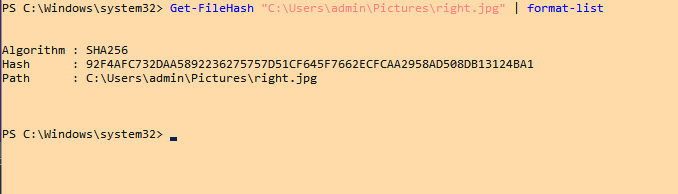
Description automatically generatedA large airplane on a runway

Description automatically generated with low confidence

Part 1 for eagle\_gallery\_lrg\_07\_960.jpg

1. Windows
2. NT 10.0 x64
3. Mozilla Firefox
4. 88.0
5. www.boeing.com
6. Sun, 02 May 2021; 21:41:08 GMT
7. 2862
8. 130.76.22.18
9. 80
10. 172.16.46.2
11. 49789

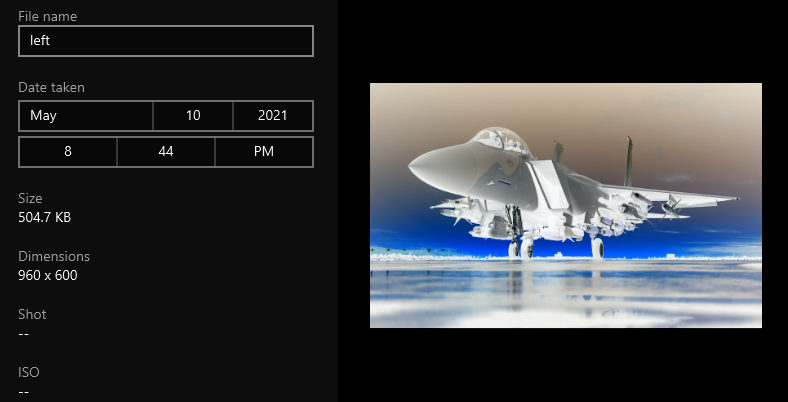
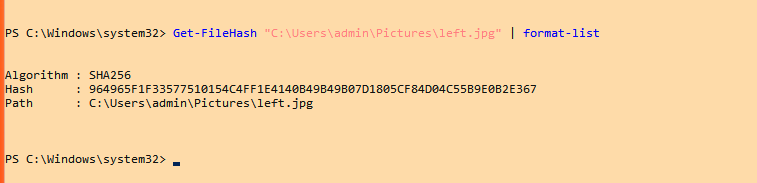
Part 2

1. JPEG
2. Ff d8 ff e1
3. HTTP
4. I am able to carve out this image because it is an HTTP protocol, which fetches the resources from the server the picture was downloaded. However, the protocol is not encrypted, and therefore the get requests and the HTTP response are in plaintext, which makes it easy for us to view the information that we carved out of the image. (This is contrast to HTTPS, which is encrypted.) With wireshark, all we do is hupload the pcapng file into the program, and it splits the file into a structure that can be read easily. The pcapng file already included the monitoring information of the HTTP requests and response, which is why we could see it in a nice format, where we could extract information. This is most notable in the source port number for the http request, which is port 80, enabling data transmission in plain text, aforementioned.
5. 
6.  It matches because I downloaded it from the same server where the file was requested from
7. ok

Part 1 for f15\_gallery\_med\_04\_960x600.jpg

1. Windows
2. NT 10.0 x64
3. Mozilla Firefox
4. 88.0
5. [www.boeing.com](http://www.boeing.com)
6. Sun, 02 May 2021, 21:41:55 GMT
7. 6659
8. 130.76.22.19
9. 80
10. 172.16.46.2
11. 49785

Part 2

1. Jpeg
2. Ff d8 ff e1
3. HTTP
4. Same as the other one, I am able to carve out this image because it is an HTTP protocol, which fetches the resources from the server the picture was downloaded. However, the protocol is not encrypted, and therefore the get requests and the HTTP response are in plaintext, which makes it easy for us to view the information that we carved out of the image. (This is contrast to HTTPS, which is encrypted.) With wireshark, all we do is hupload the pcapng file into the program, and it splits the file into a structure that can be read easily. The pcapng file already included the monitoring information of the HTTP requests and response, which is why we could see it in a nice format, where we could extract information. This is most notable in the source port number for the http request, which is port 80, enabling data transmission in plain text, aforementioned.
5. 
6.  Yes, they match, because I downloaded straight from the same server that made the original HTTP request
7. Ok