# Lab 2 - Wireshark Part 2

|  |
| --- |
| * This is an individual assignment, and worth 5 points. * The due date is Friday midnight (10/11). It will be graded as pass/fail (5 or 0 points). * Change the file name following the naming convention (e.g., Lab2-AhS.docx). |

Open the file “**LittlePrince\_ghi.pcap**” with **WireShark** and answer the following questions. You may want to use **NetworkMiner** for a summary of the analyses.

You can install **NetworkMiner** after unzipping the file and clicking on \*.exe.

Download: <https://www.netresec.com/?page=Networkminer>

1. How many DNS queries (not query response) were made?

2

1. How many TCP streams were created in this file?

6

1. What are the first and last frame numbers involved in uploading "LittlePrince.txt"?

Frame 6 and Frame 18

1. How many TCP segments were used in uploading "LittlePrince.txt"?

10

1. What is the host name where "LittlePrince.txt" was uploaded to?

[Request URI: /wireshark\_project.php]

1. What are the IP addresses of the servers involved in this file?

31.170.162.223 and 192.168.1.66

1. Follow a TCP or HTTP stream of "LittlePrince.txt" that was uploaded to the server. Screen capture part of the content of the text file.

