# Lab 2 - Wireshark Part 2

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

Open the file “**LittlePrince\_ghi.pcap**” with **WireShark** and answer the following questions. You need to use **NetworkMiner** for a few questions.

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?

**Ans: 2**

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

**Ans: 6**

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

**Ans: First 33, Last 382**

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

**Ans: 238**

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

**Ans: Ghi.site90.com**

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

**Ans: 31.170.160.65, 31.170.162.223, 74.125.65.102**

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.

**Ans: Check for following Picture Below**

