Lab 2 - Wireshark Part 2 (in class)

- This is an in-class individual assignment, and worth 2 points.
- The due date is the next day midnight. It will be graded as pass/fail (2 or 0 points).
- Change the file name following the naming convention.

Open the file "**LittlePrince_ghi.pcap**" with **WireShark** and answer the following questions. You need to use **NetworkMiner** for some of the questions.

For Mac users: If you cannot install **NetworkMiner** on your computer, switch into Proxmox. On the Proxmox server, use Windows Server and download NetworkMiner. Wireshark is already available.

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

2. How many HTTP sessions were created in this file?
   - 8

3. What are the first and last frame numbers involved in uploading "LittlePrince.txt"?
   - 9 and 33

4. How many TCP segments were used in uploading "LittlePrince.txt"?
   - 2 TCP segments

5. What is the host name where "LittlePrince.txt" was uploaded to?
   - ghi.site90.com

6. What is the IP address of the servers involved in this file?
   - 31.170.162.223

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