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

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

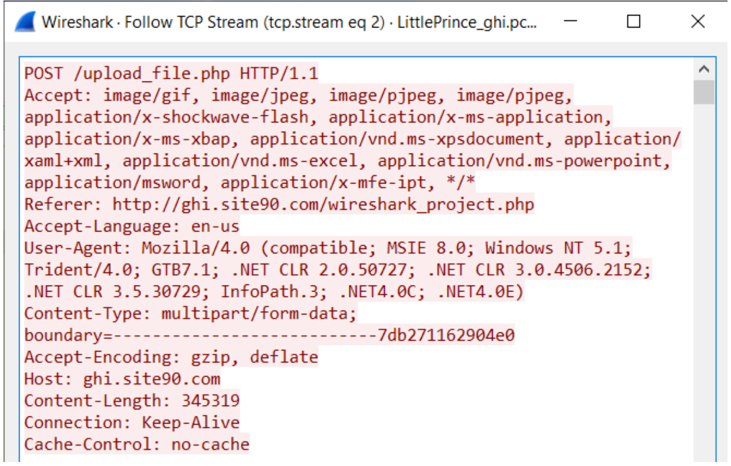
3. What are the first and last frame numbers involved in uploading "LittlePrince.txt"?
   First 9 & Last 33

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

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.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · LittlePrince_ghi.pc...

```
POST /upload_file.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg,
application/x-shockwave-flash, application/x-ms-application,
application/x-ms-xbap, application/vnd.ms-xpsdocument, application/
xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, application/x-mfe-ipt, */*
Referer: http://ghi.site90.com/wireshark_project.php
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; GTB7.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152;
.NET CLR 3.5.30729; InfoPath.3; .NET4.0C; .NET4.0E)
Content-Type: multipart/form-data;
boundary=---------------------------7db271162904e0
Accept-Encoding: gzip, deflate
Host: ghi.site90.com
Content-Length: 345319
Connection: Keep-Alive
Cache-Control: no-cache
```