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?
   There are 2 DNS queries

2. How many TCP streams were created in this file?
   There are 6 TCP streams created in this file

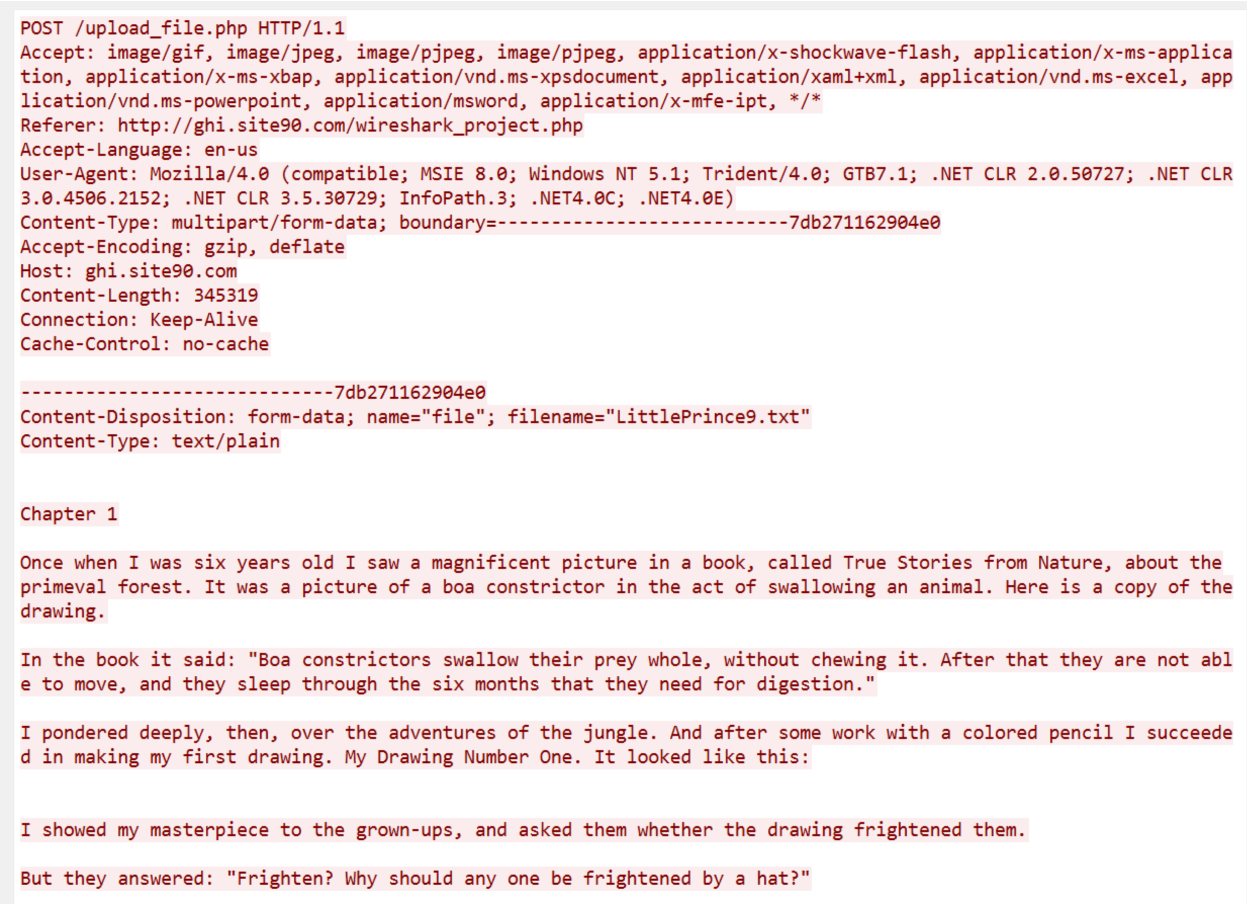
3. What are the first and last frame numbers involved in uploading "LittlePrince.txt"?
   33 and 382

4. How many TCP segments were used in uploading "LittlePrince.txt"?
   377

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

6. What are the IP addresses of the servers involved in this file?
   192.168.1.66 and 1367 31.170.162.223

7. 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.



```
POST /upload_file.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-applica
tion, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, app
lication/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

-----------------------------7db271162904e0
Content-Disposition: form-data; name="file"; filename="LittlePrince9.txt"
Content-Type: text/plain


Chapter 1

Once when I was six years old I saw a magnificent picture in a book, called True Stories from Nature, about the
primeval forest. It was a picture of a boa constrictor in the act of swallowing an animal. Here is a copy of the
drawing.

In the book it said: "Boa constrictors swallow their prey whole, without chewing it. After that they are not abl
e to move, and they sleep through the six months that they need for digestion."

I pondered deeply, then, over the adventures of the jungle. And after some work with a colored pencil I succeede
d in making my first drawing. My Drawing Number One. It looked like this:


I showed my masterpiece to the grown-ups, and asked them whether the drawing frightened them.

But they answered: "Frighten? Why should any one be frightened by a hat?"
```