Lab 2 - Wireshark Part 2

- This is an individual assignment, and worth 5 points.
- The due date is Friday midnight (9/22). 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 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 DNS queries

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

There is a total of 6 TCP streams but their Stream IDs are listed from 0-5.

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

First: 33
Last: 382

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

238

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

Host: ghi.site90.com\r\n

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

   - Server
     - 31.170.162.223

- 31.170.160.223

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.

Wireshark · Follow TCP Stream (tcp.stream eq 2) · LittlePrince_ghi(1).pcap

```
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-p
ord, 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 able 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 succeeded 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?"

My drawing was not a picture of a hat. It was a picture of a boa constrictor digesting an elephant. But since the grown-ups were not able to understand it, I made another drawing: I drew the inside of the boa constrictor, so that the grown-u
hey always need to have things explained. My Drawing Number Two looked like this:


The grown-ups' response, this time, was to advise me to lay aside my drawings of boa constrictors, whether from the inside or the outside, and devote myself instead to geography, history, arithmetic and grammar. That is why, at the age of si
ve been a magnificent career as a painter. I had been disheartened by the failure of my Drawing Number One and my Drawing Number Two. Grown-ups never understand anything by themselves, and it is tiresome for children to be always and forever
.

So then I chose another profession, and learned to pilot airplanes. I have flown a little over all parts of the world; and it is true that geography has been very useful to me. At a glance I can distinguish China from Arizona. If one gets lo
ledge is valuable.

In the course of this life I have had a great many encounters with a great many people who have been concerned with matters of consequence. I have lived a great deal among grown-ups. I have seen them intimately, close at hand. And that hasn'
of them.

Whenever I met one of them who seemed to me at all clear-sighted, I tried the experiment of showing him my Drawing Number One, which I have always kept. I would try to find out, so, if this was a person of true understanding. But, whoever it
ways say:

"That is a hat."

Then I would never talk to that person about boa constrictors, or primeval forests, or stars. I would bring myself down to his level. I would talk to him about bridge, and golf, and politics, and neckties. And the grown-up would be greatly p
sensible man.

To Main PageTo Table of ContentsNext ChapterPrevious Chapter

-------------

Chapter 2
```

238 client pkts, 1 server pkt, 1 turn.

Entire conversation (346 kB) Show data as ASCII

Find: