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 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?
   Answer: 2 queries

2. How many TCP streams were created in this file?
   Answer: 6 total streams or conversations

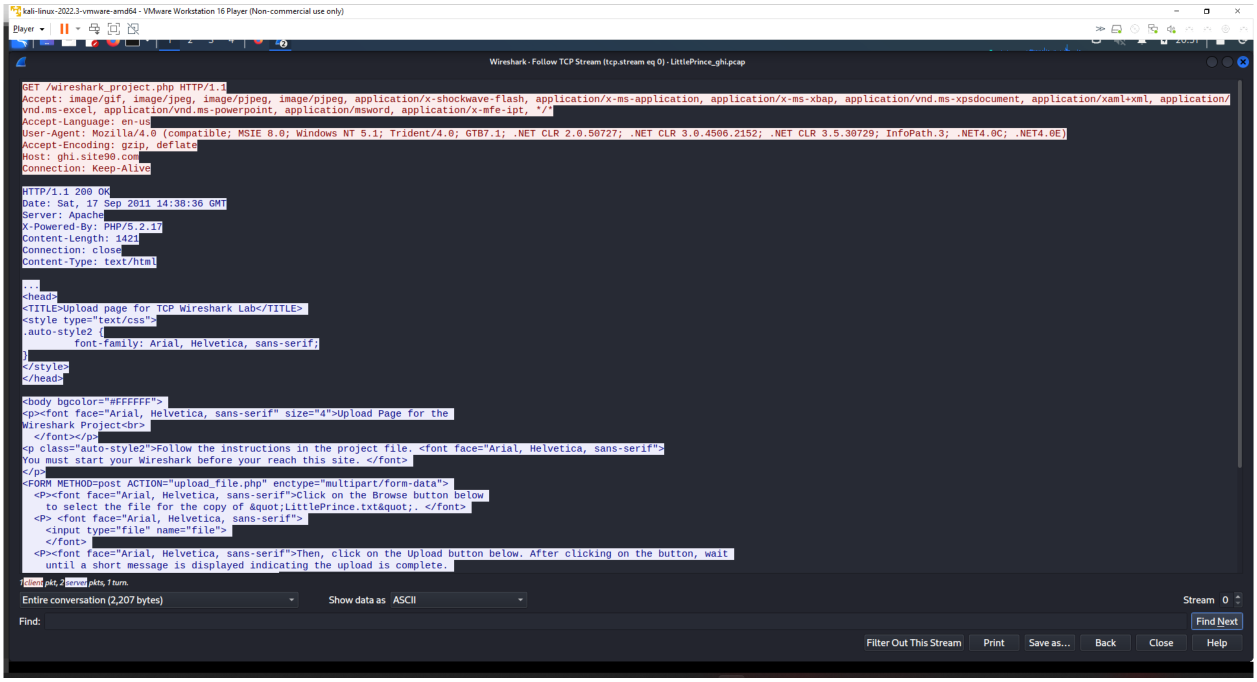
3. What are the first and last frame numbers involved in uploading "LittlePrince.txt"?
   Answer: Starts at 40, ends at 382 using the filter and using (frame contains "little prince")

4. How many TCP segments were used in uploading "LittlePrince.txt"?
   Answer: 238 I think. There were a lot and I tried to count them and that's what I came to.

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

6. What are the IP addresses of the servers involved in this file?
   Answer: 31.170.162.233
   Answer: 31.170.160.65

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.


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Wireshark · Follow TCP Stream (tcp.stream eq 0) · LittlePrince_ghi.pcap
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
GET /wireshark_project.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, */*
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)
Accept-Encoding: gzip, deflate
Host: ghi.site90.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 17 Sep 2011 14:38:36 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 1421
Connection: close
Content-Type: text/html

...
<head>
<TITLE>Upload page for TCP Wireshark Lab</TITLE>
<style type="text/css">
.auto-style2 {
         font-family: Arial, Helvetica, sans-serif;
}
</style>
</head>

<body bgcolor="#FFFFFF">
<p><font face="Arial, Helvetica, sans-serif" size="4">Upload Page for the
Wireshark Project<br>
  </font></p>
<p class="auto-style2">Follow the instructions in the project file. <font face="Arial, Helvetica, sans-serif">
You must start your Wireshark before your reach this site. </font>
</p>
<FORM METHOD=post ACTION="upload_file.php" enctype="multipart/form-data">
  <P><font face="Arial, Helvetica, sans-serif">Click on the Browse button below
    to select the file for the copy of &quot;LittlePrince.txt&quot;. </font>
  <P> <font face="Arial, Helvetica, sans-serif">
    <input type="file" name="file">
    </font>
  <P><font face="Arial, Helvetica, sans-serif">Then, click on the Upload button below. After clicking on the button, wait
    until a short message is displayed indicating the upload is complete.
```

1 client pkt, 2 server pkts, 1 turn.

Entire conversation (2,207 bytes) Show data as ASCII Stream 0

Find: