# Mohammed Al Madhi

# CIS 480

# FALL 2020

# Lab 2 - Wireshark Part 2 (in class)

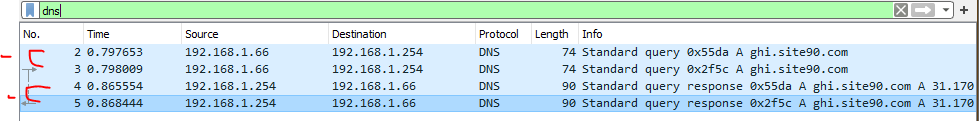
|  |
| --- |
| * This is an in-class individual assignment, and worth 2 points. * The due date is the next day midnight. It will be graded as pass/fail (2 or 0 points). * Change the file name following the naming convention. |

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.

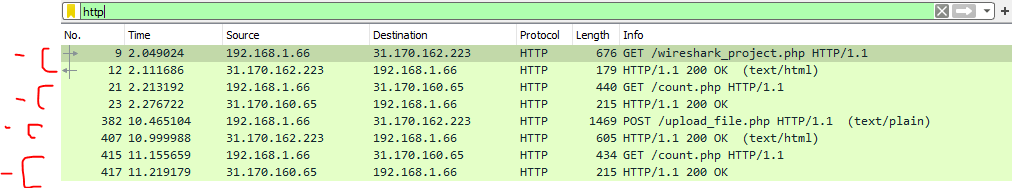
1. How many DNS query was made? How many DNS query were made? In the DNS queries, we get the private IP address as the destination? Can you explain why?

**There are two dns query’s, the the first the host contacts the gatewat, then the gateway contacts the DNS server which then it will return to the gateway, and gateway sends it back to us ot to the IP of the source.**



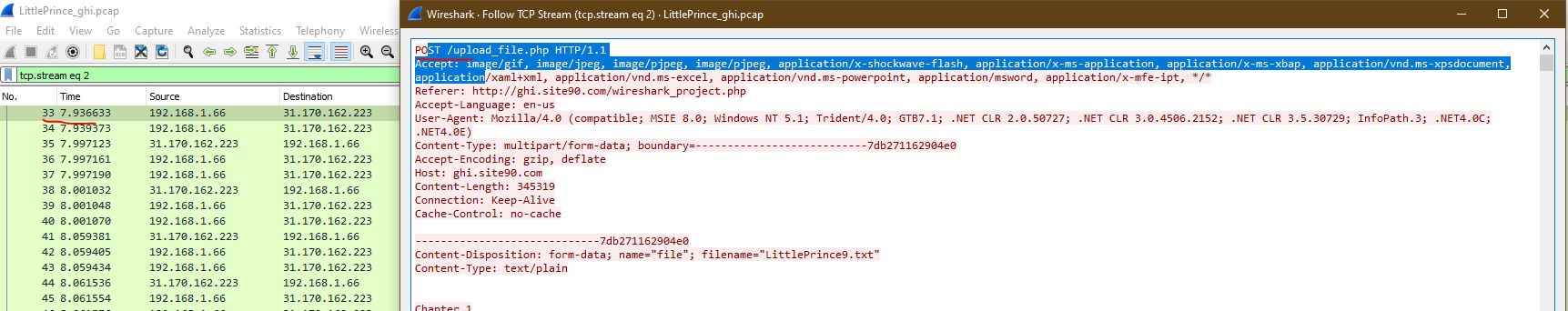
1. How many HTTP sessions were created in this file?

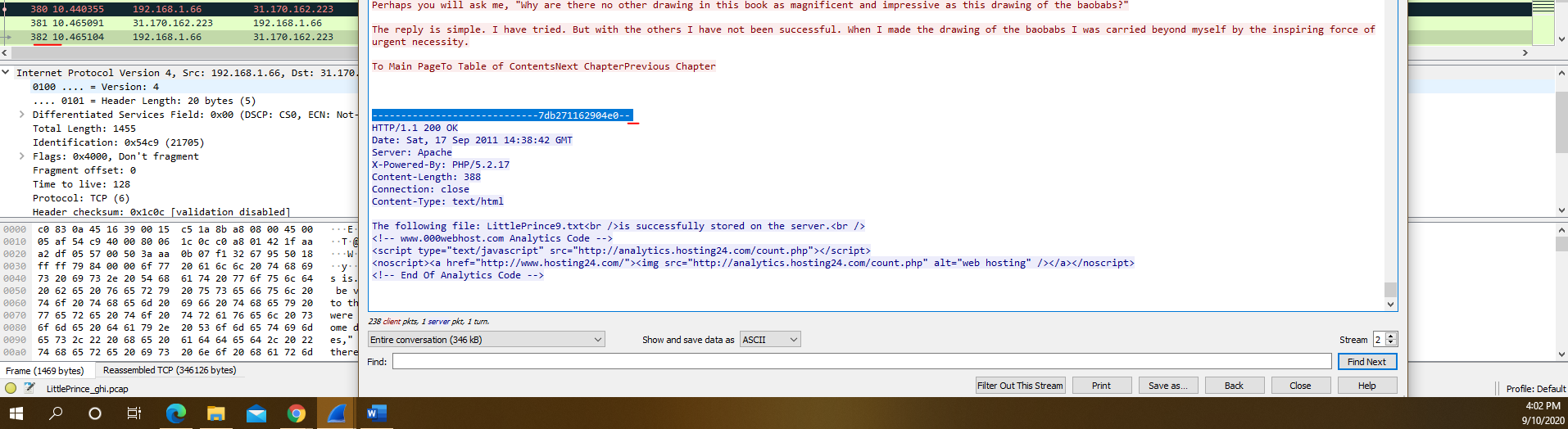
**There are four HTTP sessions created.**



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

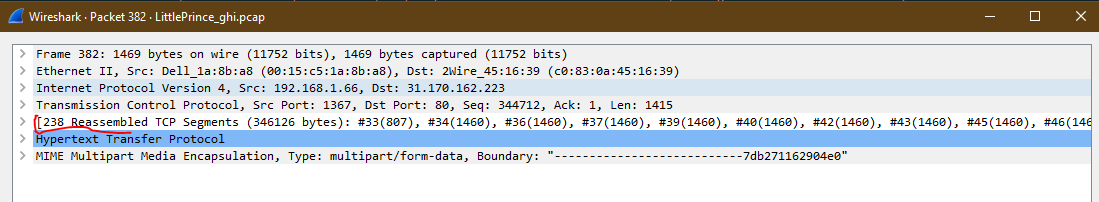
**When I clicked the word “POST” 33 was the first frame and the last was 382.**





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

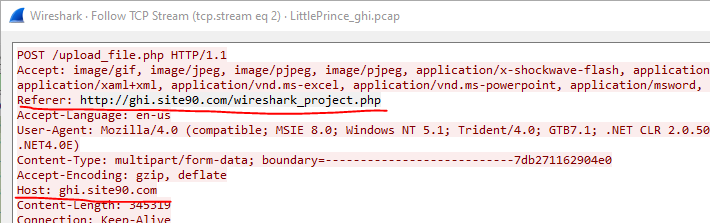
**238**



1. What is the host name where "LittlePrince.txt" was uploded to?

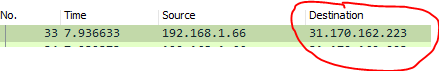
**HOST: ghi.site90.com**

**Reference:** [**http://ghi.site90.com/wireshark\_project.php**](http://ghi.site90.com/wireshark_project.php)



1. What is the IP address of the servers involved in this file?

**31.170.162.223**



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

