Lab 1: Wireshark Packet Capture

+ Take as many screen pictures as possible and insert into your answer sheet
+ Return your answer in pdf or docfile with file name likes this

GROUP-CODE-NAME-wireshark01
Ex: SE0709- SE02436-Linhlm--wireshark01

Question 1: Turn the cmd program in Windows by going to Start, Run and type cmd in the pop-up window, press enter. Type command tracert www.cnn.comand see the result.
- What is the "tracert" command? What is the meaning of output?

Question 2:
1) Start up your web browser.
2) Start up the Wireshark.
3) Enter the following to your browser http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html. Your browser should display the very simple, one-line HTML file.
4) Stop Wireshark packet capture.

Answer following questions:
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

2. What languages (if any) does your browser indicate that it can accept to the server ?

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server ?

4. What is the status code returned from the server to your browser ?

5. When was the HTML file that you are retrieving last modified at the server?

6. How many bytes of content are being returned to your browser?

7. Find the "GET http" message that connect your computer to http://gaia.cs.umass.edu

Note: Highlight the clue of each your answers.