

**Experimental Report**

|  |  |
| --- | --- |
| **Course**: | Computer Networking |
| **Semester**: | 2nd semester of the academic year **2020-2021** |
| **Major**: | Software Engineering |
| **Class**: | 2019 |
| **Student Name**: | 吴嘉诚 |
| **Student ID:** | 222019321062111 |
| **Teacher:** | Zheng Yang (杨铮) |

**School of Computer and Information Science**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | | Wireshark Lab: HTTP | | | |
| Date | | 2021/5/8 | Type | | □Confirmatory  √ Design  √ Comprehensive |
| 1. **Objectives & Requirements**   **Master how to analyze HTTP packets using the Wireshark packet capture tool**   * The Basic HTTP GET/response interaction * The HTTP CONDITIONAL GET/response interaction * Retrieving Long Documents * HTML Documents with Embedded Objects * HTTP Authentication | | | | | |
| 1. **Experimental environment (**platform and software**)**  * Ubuntu + Wireshark | | | | | |
| 1. **Experimental content and design** (Main Content, Procedure, Codes and Results) 2. **The Basic HTTP GET/response interaction**  * Following the instructions and I got:   2021-05-09 15-44-42 的屏幕截图  2021-05-09 15-42-36 的屏幕截图   * **Question answering:**  1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?   **So my browser runs v1.1:**    **The server runs v1.1 too:**     1. What languages (if any) does your browser indicate that it can accept to the server?   **Chinese(CN,TW,HK), English(US, )**     1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?   **My IP is 10.124.109.45, and the server’s is 128.119.245.12**     1. What is the status code returned from the server to your browser?   **The status code is 200, means OK**     1. When was the HTML file that you are retrieving last modified at the server?   **2021/5/9 05:59:01 GMT**     1. How many bytes of content are being returned to your browser?   **128Byte**     1. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.   **User-Agent: The information about the agent**    **Server: The information about the server**     1. **The HTTP CONDITIONAL GET/response interaction**  * **Clear browser cache**   **2021-05-09 16-28-50 的屏幕截图**   * **Finally got this:**      * **Question answering:**  1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?   **No**   1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?   **For the first response, yes. As i can see the html contents from the packet:**  **But in the second response, it didn’t explicitly return the content. Because i didn’t find the contents.**   1. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?   **Yes:**    **It follows some date information, It is same as the date of “Last-Modified”**   1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.   **304 Not Modified**     1. Retrieving Long Documents  * Tried twice and get two results:        * **Question answering**  1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?   **2(But the second is to get an icon as discussed before)**  **No.793(848 for the second result)**   1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?   **No.793**   1. What is the status code and phrase in the response?   **200 OK\r\n**   1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?   **Here is 4 segments:**     1. **HTML Documents with Embedded Objects**  * **Results:**      * **Problem answering**  1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?   **4 GET request**  **Three to 128.119.245.32 AND one to 178.79.137.164**   1. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.   **(Ignore the GET request for the favicon)**  **In parallel. We can see the GET requests don’t wait for the previous GET’s response. They are sent immediately.**   1. **HTTP Authentication**  * **Results:**      * **Problem answering**  1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?   **401 Unauthorized**   1. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?   **Authorization field, which contains our encoded username and password**     * **Decode result:** | | | | | |
| 1. **Analysis and discussion of experiment results**（Analysis of experimental results, and summary of gains and the existing problems）  * **Known a lot about the procedures of packets transferring of HTTP** * **Learned much about the HTTP Authentication Schemes from the given website. I’m really interested in it.** * **Existing problem**  1. Why it can be different result for task3? Because of my own network connection? | | | | | |
| Comments & Evaluation | Content & Design (A-E) | | |  | |
| Procedure & Codes (A-E) | | |  | |
| Results (A-E) | | |  | |
| Analysis & Discussion (A-E) | | |  | |
| Score (A-E):  Feedback comments: | | | | |