

**Lab report**

|  |  |
| --- | --- |
| **Course**: | Computer Networking |
| **Semester**: | 2nd semester of the academic year **2022-2023** |
| **Major**: | Software Engineering |
| **Class**: | 软件工程（中外）1班 |
| **Student Name**: | 朱昊 |
| **Student ID:** | 222022321062008 |
| **Teacher:** | Chunming Wu (吴春明) |

**School of Computer and Information Science**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | | HTTP、TCP | | | |
| Date | |  | Type | | □Confirmatory  √ Design  √ Comprehensive |
| 1. **Objective & Requirements**   1. Learning to use Wireshark to capture packets  2. Understanding HTTP packet content  3.Capturing TCP packets with wireshark | | | | | |
| 1. **Result analysis and discussion**（Analysis of experimental results and summing up the harvest and the existing problems）   **HTTP实验：**  HTTP请求报文结构如下：  抓包结果如下：   1. 你的浏览器使用的HTTP版本是1.0还是1.1？     如上图所示，我的HTTP版本是1.1   1. 你的浏览器指定服务器使用的语言类型是什么？     如上图所示，使用的语言类型是中文和英文   1. 你的计算机IP地址是多少？     如上图所示，本机ip为10.135.121.195   1. 从服务器返回的状态码是多少？     如上图所示，返回的状态码是200 OK，表示请求成功   1. 你从服务器获取最后更新的HTML代码是什么时候的？     如上图所示，最后一次修改在2024年五月八日   1. 从服务器返回了多少字节的数据？     如上图所示，一共返回了128个字节  8、检查内容窗口里的第一个HTTP GET请求，是否看到“IF-MODIFIED-SINCE”信息？    如上图所示，在第一个HTTP GET请求中有看到IF-MODIFIED-SINCE信息  9、检查内容窗口里服务器的响应，服务器是否明确的返回了文件内容？    如上图所示，服务器返回了文件内容，但是第四个get请求的响应报文中得到的。  10、检查第二个HTTP GET请求，是否看到了“IF-MODIFIED-SINCE”，如果有的话，跟在后面的是什么信息？    如上图所示，可以看到IF-MODIFIED-SINCE信息，跟在后面的是 时间信息   1. 服务器响应第二个HTTP GET的信息是什么？服务器是否返回了文件内容？请解释为什么会出现这种状态。     如上图所示，没有返回文件内容    如上图所示如果有If-Modified-Since，则会与当前服务器上相关资源最后一次修改时间进行对比，如果相同则返回304（资源可访问，但没修改），否则加载最新数据，浏览器再缓存起来。这样减少网络数据传输和服务器压力。  在第二次的请求报文中和响应报文中可以看到如下两图所示的时间      所以两者的时间是相同的，所以不会返回数据     1. 你的浏览器发送了多少个HTTP GET请求？   如上图所示，发送了四个get请求   1. 服务器响应这个消息发送了多少个包含数据的TCP片段？   没有发现发送TCP片段   1. 服务器响应这个请求的状态码和短语是什么？   有200，ok 也有304，Not Modified   1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?     在本次抓包实验中，只需要一个响应报文就携带了全部网页内容。     1. 浏览器发出多少个HTTP GET请求？这些get请求被发送到哪里？   如下图所示，发送了3个HTTP GET请求，这些请求被发送到IP地址为128.119.245.12的DNS服务器上。     1. 浏览器下载两个图片是并行还是串行的？请解释。   并行的，因为在第一个图片下载结束前，第二个图片就开始下载了   1. 服务器对最初的HTTP GET消息响应是什么？   如下图所示：401 unauthorized     1. 浏览器是什么时候发送第二条HTTP GET消息的？包含在里面新的字段是什么？   如下图所示，最新字段是Authorization,里面有用户名和密码    **TCP实验：**  1.What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?    如图所示：源IP为172.18.3.185 源端口：50203  2.What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?  从第一问的图片中也可以看出，目的IP为128.119.245.12，目的端口是80  3.What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?  仍然是源IP为172.18.3.185 源端口：50203  4.What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?    由上图可知，Sequence number是0，flags是0x002  5.What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?    由上图可知，sequence number是0，acknowledgement字段的值为1，代表接收方想接受序号为1的TCP报文段，flags=0x012.   1. What is the sequence number of the TCP segment containing the HTTP POST command?   包含HTTP POST命令的TCP段的序号是多少？（如果要找到POST命令，需要在数据包内容域里查找）。    由上图可见，右边数据有POST，左边显示sequence number是1   1. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?     由上图可见，前六个发送方发送的TCP报文段的序号分别为1，1201，2401，3601，4801，6001  六个数据包的发送时间分别是：16.419211，16.419214，16.671860，16.671873，16.671875，16.671877  六个数据包的接受时间分别是： ，16.671726， ，16.924344， ，16.924389  RTT：0.252512000，0.252471000，0.252467000  8.What is the length of each of the first six TCP segments?  前六个数据段长度分别为：1200，1200，1200，1200，1200，1200  9.What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?  最小可用接收缓冲区大小为34048字节，传送缓冲区大小没有变  10.Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?  在抓取的包中，是否有重传的数据段？为什么？    如上图所示，有重传的TCP报文段，因为发送方接受到了超过三个相同的ACK确认，所以启动立即重传。  11.How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).  通常一个ACK报文段确认了两个接收方发送的报文段，也就是2400字节的数据。  12.What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.  从所抓取的数据中，计算TCP传输的吞吐量（单位时间内传输的字节数）是多少？  由于吞吐量=总数据量/总传输时间    如上图所示，最后一个接收方向发送方发送的TCP数据报的ACK=153037，此时时间是20.117252  而上图显示，TCP建立时，接收方向发送方发送ACKSYN时的时间为16.418299  所以吞吐量为 153037/20.117252-16.418299=153037/3.698953=40.40337774297213KB/S  13.Use the *Time-Sequence-Graph(Stevens*) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP’s slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we’ve studied in the text.    如上图所示，竖着的红圈代表着慢启动阶段，横着的红圈代表着拥塞避免阶段。 | | | | | |
| Comments & Evaluation | Content & Design (A-E) | | |  | |
| Procedure & Codes (A-E) | | |  | |
| Results (A-E) | | |  | |
| Analysis & Discussion (A-E) | | |  | |
| Score (A-E):  Feedback comments: | | | | |