

**计算机网络**

**课程实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 利用Wireshark进行协议分析 | | | | | |
| 姓名 | 许坤彬 | | 院系 | 计算学部 | | |
| 班级 | 2203103 | | 学号 | 2022114586 | | |
| 任课教师 | 聂兰顺 | | 指导教师 | 聂兰顺 | | |
| 实验地点 | G001 | | 实验时间 | 2024/10/24 | | |
| 实验课表现 | 出勤、表现得分(10) |  | 实验报告  得分(40) |  | 实验总分 |  |
| 操作结果得分(50) |  |
| 教师评语 | | | | | | |
|  | | | | | | |

****

|  |
| --- |
| 实验目的： |
| 熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以及报文交换的情况。 |
| 实验内容： |
| 1) 学习 Wireshark 的使用  2) 利用 Wireshark 分析 HTTP 协议  3) 利用 Wireshark 分析 TCP 协议  4) 利用 Wireshark 分析 IP 协议  5) 利用 Wireshark 分析 Ethernet 数据帧  6）选做内容：  a) 利用 Wireshark 分析 DNS 协议  b) 利用 Wireshark 分析 UDP 协议  c) 利用 Wireshark 分析 ARP 协议 |
| 实验过程： |
| 1. 学习使用Wireshark 2. 首先启动Wireshark软件，选择捕获菜单下的选项。      1. 在这里选择无线网卡WLAN，随后点击开始。 2. 打开浏览器，输入一个网页。在这里我们选择<http://www.arnc2024.cn/hello.html>，这个网页是我个人使用nginx部署在阿里云服务器上的一个用于实验测试的HTML。在浏览器得到全部网页内容之后，停止捕获，在内容过滤器中输入HTTP，可以过滤得到HTTP协议相关的捕获信息。     点击第一条信息，可以在下方依次看到以太网帧、 IP 数据报、 TCP 报文段、以及 HTTP 报文首部信息。   1. HTTP分析 2. HTTP GET/response交互   按照上面的方法，现在wireshark中打开捕获信息，随后在浏览器中打开<http://hitgs.hit.ediu.cn/news>，出现内容后停止信息捕获，并通过过滤器筛选HTTP相关信息。通过查看HTTP报文和IP报文中的相关内容可以得到指导书中问题的答案。    2． HTTP 条件 GET/response交互  首先清空浏览器的缓存，随后输入URL：<http://hitgs.hit.edu.cn/news>，访问一次，在得到服务器返回的内容后，点击浏览器的刷新按钮，再次进行访问，使用wireshark进行分组捕获。随后停止wireshark的分组俘获，在过滤筛选处输入http，在列表中寻找对应的HTTP报文。   1. TCP分析   首先访问<http://gaia.cs.umass.edu/Wireshark-labs/alice.txt>网页，得到文本，并且右键将文本保存到电脑上    随后打开https://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，先输入文件路径，随后打开Wireshark开始分组俘获，再点击上传，上传完毕，贺词信息出现在浏览器中之后，再停止俘获。 |
| 实验结果： |
| 一、wireshark使用  二、HTTP分析  1. HTTP GET/response交互  （1）浏览器运行的是HTTP 1.1    （2）浏览器向服务器指出能够接受语言版本为zh\_CN，即简体中文。    （3）我的计算机IP地址为172.20.233.126，服务器的IP地址为219.217.2226.25    （4）服务器为我返回的状态代码为200    2. HTTP 条件 GET/response交互  在这一部分中，我使用网站<http://hitgs.hit.edu.cn/news>的时候，无论如何发送、重复几次都无法发送出带有If-modified-since的请求头，并且无法接收到304，我猜测这个网站本身就没有提供last-modified字段，所以无法完成这个实验的验证。因此，在这里我们将使用的网站切换为<http://www.arnc2024.cn/hello.html>，这个网站是我自己使用nginx部署到阿里云服务器上的，会在返回的HTTP报文中增加last-modified字段。能够完成本实验的验证。   1. 第一次发送给服务器的请求中没有IF-MODIFIED-SINCE 2. 第一次服务器响应的报文返回了文件内容，因为返回的状态码为200     （3）较晚的HTTP GET请求中包含了IF-MODIFIED-SINCE字段，字段后面跟着的内容是本地缓存中所存储的上次HTTP报文返回的Last-Modified字段  （4）较晚的HTTP GET请求的响应HTTP状态编码为304，没有返回文件内容。     1. TCP分析   1. 上传文件    2. 浏览追踪信息  （1）向gaia.cs.umass.edu服务器发送文件的客户端主机的IP地址是172.20.233.126，端口号为61184。  （2） gaia.cs.umass.edu服务器的IP地址是183.240.139.243，用来发送和接受TCP报文的端口号是20058。    3. TCP基础  （1）SYN报文段的序号是403855647，在该报文段中使用flag的低两位来标注SYN报文段（第二位若为1则为SYN报文段）。    （2）SYNACK的报文段序号是2710228023，通过使用Syn和Ack两位来用来标注SYN ACK。      （3）tcp三次握手的过程    （4）包含了HTTP POST命令的TCP报文段序号是    （5）第六个报文段的序号是    它的发送时间是  （6）前6个TCP报文段的长度 |
| 问题讨论： |
|  |
| 心得体会： |
| 结合实验过程和结果给出实验的体会和收获。 |