

**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 | 朱明彦 | | 院系 | 计算机科学与技术学院 | | |
| 班级 | 1603109 | | 学号 | 1160300314 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 格物213 | | 实验时间 | 2018/11/17 | | |
| 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   **选做内容：**   * 1. 利用Wireshark分析DNS协议   2. 利用Wireshark分析UDP协议   3. 利用Wireshark分析ARP协议 |
| 实验过程： |
| 以文字描述、实验结果截图等形式阐述实验过程，必要时可附相应的代码截图或以附件形式提交。  在本次实验中，共使用了两台不同的电脑进行实验，其IP地址分别是：   1. Windows 10 主机：172.20.85.207      1. Ubuntu 16.04 主机：172.20.145.140   **（一）Wireshark的使用**  在Wireshark的使用环节，选择Ubuntu的无线网卡进行分组捕获，并访问<http://www.hit.edu.cn>。在完整的页面加载完成后，结束分组捕获。在这一段时间Wireshark捕获了本机所有利用该无线网卡与其他网络实体进行交换的报文，具体文件见1.pcapng.gz，实验结果的分析见**实验结果**部分。  **（二）HTTP分析**  1) HTTP GET/response交互  在Wireshark显示过滤部分输入“HTTP”即仅显示捕获的HTTP报文，开始捕获后访问<http://hitgs.hit.edu.cn/>，在加载完全部页面后停止分组捕获。在这一段时间，Wireshark捕获的全部分组见2\_http\_with\_buffer.pcapng.gz，实验结果的分析见实验结果部分。  2)HTTP 条件 GET/response交互  首先将浏览器内的所有缓存清空。  启动Wireshark分组捕获，访问<http://hitgs.hit.edu.cn/>，在加载完全部页面后，重新刷新页面；在刷新页面后，停止Wireshark分组捕获。在这一段时间Wireshark捕获的全部报文，见文件2\_http\_without\_buffer.pcapng.gz，实验结果的分析见**实验结果**部分。  **（三）TCP分析**  1. 访问<http://gaia.cs.umass.edu/wireshark-labs/alice.txt>，获得alice.txt文件。再打开<http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>，选择好本地alice.txt文件的位置，开始Wireshark分组捕获后，点击”Upload alice.txt file”按钮；在文件上传完毕后，停止Wireshark分组捕获。  2. 在这一段时间内Wireshark捕获的分组见3\_tcp.pcapng.gz，在筛选规则中选择“tcp”部分，进行分析，具体分析见**实验结果**部分。  **（四）IP分析**  1. 使用pingplotter进行实验，启动Wireshark开始分组捕获，首先发送一系列56字节的包；再发送一系列2000字节的包；再发送一系列3500字节的包，然后停止Wireshark捕获。  2. 在这段时间捕获的数据包见文件4\_ip.gz.pcapng.gz，具体结果分析见**实验结果**部分。  **（五）抓取ARP数据包**  1. 利用arp查看本机的ARP缓存表  2. 开始Wireshark分组捕获，在命令行中输入：ping 192.168.45.95  3. ping通之后利用停止Wireshark捕获，这段时间捕获的分组见5\_arp.pcapng.gz，具体结果分析见**实验结果**部分。  **（六）抓取UDP数据包**  启动Wireshark分组捕获，利用QQ给好友发送消息，消息发送结束后，停止分组捕获；这段时间捕获的报文分组见6\_udp.pcapng.gz，具体结果分析见**实验结果**部分。  **（七）利用Wireshark进行DNS协议分析**  首先清空dns缓存，在浏览器中访问<http://www.google.com.hk/>，进行Wireshark抓包，这段时间抓取的分组见7\_dns.pcapng.gz，具体的结果分析见**实验结果**部分。 |
| 实验结果： |
| 采用演示截图、文字说明等方式，给出本次实验的实验结果。  **（一）Wireshark的使用**  图见下页  可以看到，经过过滤后的第一条HTTP报文，即为向[www.hit.edu.cn](http://www.hit.edu.cn/)发送HTTP GET报文。可以看到分装在tcp段中的HTTP请求报文，相关信息见图片。    （二）HTTP分析  1) HTTP GET/response交互  利用Wireshark打开2\_http\_with\_buffer.pcapng.gz，捕获分组的截图如下    思考问题  1. 浏览器运行的协议为HTTP/1.1；访问的服务器运行的HTTP协议版本号同为HTTP/1.1。  2. 浏览器向服务器指明其可以接收的对象为  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  3. 本机ip地址为 **172.20.45.140**（Ubuntu 主机ip地址）  服务器<http://hitgs.hit.edu.cn的ip>地址为**219.217.226.25**  4. 服务器向本机浏览器返回的状态码为**200。**  2) HTTP条件GET/response交互 |
| 问题讨论： |
| 对实验过程中的思考问题进行讨论或回答。 |
| 心得体会： |
| 结合实验过程和结果给出实验的体会和收获。 |