**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机网络**

**实验项目名称： 实验三 数据包抓取与分析**

**学院： 计算机与软件学院**

**专业： 计算机科学与技术**

**指导教师： 崔来中**

**报告人：张博智 学号：2023150159 班级： 计科2班**

**实验时间： 2025年4月1日**

**实验报告提交时间： 2025年4月6日**

**教务部制**

|  |  |  |
| --- | --- | --- |
| **实验目的：**  学习安装、使用协议分析软件，掌握基本的数据报捕获、过滤和协议的分析技巧，能对抓取数据包进行分析。  **实验内容：**  协议分析软件的安装和使用、学会抓取数据包的方法并对对抓取数据包进行分析  **实验环境和要求:**  使用Windows操作系统；Internet连接  抓包软件Wireshark。 | | |
| 方法、步骤：  **1.在网址http://wiki.wireshark.org/CaptureSetup/NetworkMedia.处下载最新版的wireshark并安装：**    **2.wireshark是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你需要选择一个网卡。**    **3.** **WireShark 主要分为这几个界面：**  **Display Filter(显示过滤器)，用于过滤**  **Packet List Pane(封包列表)，显示捕获到的封包，有源地址和目标地址，端口号。颜色不同，代表3. Packet Details Pane(封包详细信息),显示封包中的字段**  **Dissector Pane(16进制数据)**  **Miscellanous(地址栏，杂项)**    **4.** **过滤器会帮助我们在大量的数据中迅速找到我们需要的信息。**    **5.** **这个面板是我们最重要的，用来查看协议中的每一个字段**  **-Frame:物理层的数据帧概况**  **-Ethernetl:数据链路层以太网帧头部信息**  **-Internet Protocol Version 4:互联网层|P包头部信息**  **-Transmission Control Protocol:传输层T的数据段头部信息，此处是TCP- Hypertext Transfer Protocol:应用层的信息，此处是HTTP协议**    **6.** **从下图可以看到wireshark捕获到的TCP包中的每个字段** | | |
| 实验过程及内容：  （ps:由于ppt提供的两个关于深大的网址无法打开，本实验用校园网网址进行代替）  **一、tcp分析**  **网址1：www1.szu.edu.cn--三次握手**  客户端发送连接请求    服务器端接收连接请求    客户端确认    **网址1：www1.szu.edu.cn—四次挥手**  服务端确认断开连接（**在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求**）    客户端发送ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。    客户端已确认信息全部发送完毕，确认断开连接    服务器确认断开连接    **网址2：www.youku.com --三次握手**  客户端发送连接请求    服务器端接收连接请求    客户端确认    **网址2：www.youku.com –四次挥手（三次）**  客户端确认断开连接    当被动关闭方（此处是优酷服务器服务器）在tcp挥手过程中，如果“**没有数据要发送**”，同时“**没有开启TCP\_\_QUICKACK**”（默认没有开启，等于是在使用tcp延迟确认机制），那么第二次和第三次挥手就会合并传输，这样就出现了三次挥手。    客户端确认断开连接    **网址3：www.sina.com.cn --三次握手**  客户端发送连接请求    服务器端确认连接请求    客户端确认    **网址3：www.sina.com.cn –四次挥手（在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求）**  服务器端向客户端发送确认断开连接的请求    客户端发送ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。    客户端已确认信息全部发送完毕，确认断开连接    服务器确认断开连接    **二、三个网址的udp和dns协议分析**  在控制面板中可以找到自己当前网卡的DNS服务器的IP地址（**在后续抓包过程可以发现确实是把域名发送到了该IP地址对应的DNS服务器**）：      **网址1：www1.szu.edu.cn**    **由图可知：**  **该数据包的源端口=53，目的端口=61380**  **长度=199，校验码=0x676f**  **需要转换的网址是：www1.szu.edu.cn**  **IP地址是：210.39.4.1**  **网址2：www.youku.com**    **由图可知**  **该数据包的源端口（DNS服务器）=53，目的端口=61342**  **长度=492，校验码=0xd67**  **需要转换的网址是：**[**www.youku..com**](http://www.youku..com)  **IP地址：106.11.43.215**  **网址3：**[**www.sina.com.cn**](http://www.sina.com.cn)    **由图可知**  **该数据包的源端口（DNS服务器）=53，目的端口=49316**  **长度=511，校验码=0x5e55**  **需要转换的网址是：www.sina.com.cn**  **IP地址有：**    **DNS系统还支持基于地理位置的域名解析，可以将域名解析成距离用户地理位置最近的服务器地址，加快用户访问速度。**  **三、三个网站的HTTP协议分析**  **网址1：www1.szu.edu.cn**  首先通过控制台给对应网址发送数据包：    通过http流，可以看到客户端向服务器发送的信息，和校园网服务器响应的信息      **网址2：www.youku.com**  首先通过控制台给对应网址发送数据包：    通过http流，可以看到客户端向服务器发送的信息，和优酷服务器响应的信息      **网址3：**[**www.sina.com.cn**](http://www.sina.com.cn)  首先通过控制台给对应网址发送数据包：    通过http流，可以看到客户端向服务器发送的信息，和优酷服务器响应的信息 |
| 实验分析：  **TCP连接管理**  三次握手：客户端发送SYN，服务端响应SYN+ACK，客户端确认ACK，成功建立连接。  四次挥手：主动关闭方发送FIN，接收方ACK确认；接收方发送FIN，主动方ACK确认后释放连接。  观察到部分场景因延迟确认机制导致挥手步骤合并为三次（FIN+ACK合并）。  **DNS协议分析**  响应中包含域名对应的IP地址（如www1.szu.edu.cn解析为210.39.4.1）。  支持基于地理位置的解析，返回距离用户最近的服务器IP。  **HTTP协议解析**  响应包含状态码（如200 OK）、响应头和HTML内容。  观察到HTTPS流量因加密无法直接解析明文内容。 |

|  |
| --- |
|  |

深圳大学学生实验报告用纸

|  |
| --- |
| 实验结论：  **工具掌握**：熟练使用Wireshark进行数据包捕获、过滤及分层解析，验证了网络协议的分层结构（物理层→应用层）。  **协议理解：**  TCP通过三次握手确保可靠连接，四次挥手实现有序断开。  DNS通过UDP实现高效域名解析，支持负载均衡与地理位置优化。  HTTP/HTTPS协议在应用层实现客户端与服务器的请求-响应交互。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。