《网络与通信》课程实验报告

实验三：数据包结构分析

姓名	李昀哲	院系	计算机学院	学号	20123101
任课教师	刘通		指导教师	刘通	
实验地点	计 708		实验时间	2022.10.14	
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)					

实验目的：

1. 了解 Sniffer 的工作原理，掌握 Sniffer 抓包、记录和分析数据包的方法；
2. 在这个实验中，你将使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验内容：

使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验要求：（学生对预习要求的回答）（10 分）　得分：

- 常用的抓包工具

  Fiddler 抓包工具、Charles 抓包工具、Firebug 抓包工具、httpwatch 抓包工具、Wireshark抓包工具、SmartSniff 抓包工具。

实验过程中遇到的问题如何解决的？（10 分）　得分：

问题 1：不明确软件的使用过程和方法

结合 WireShark 官方 Document 以及课上所学知识，逐步上手尝试熟悉使用

问题 2：不清楚如何筛选出自己想要的抓取到的数据包

使用软件中的“过滤语法”，具体语法包括：

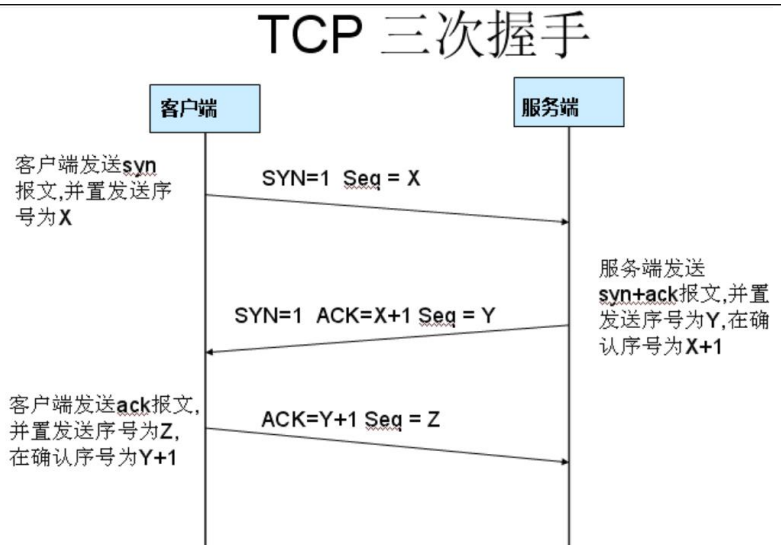
1. 比较操作符，如==, !=, >, <等；
2. 协议过滤，如：tcp, http, icmp 等；
3. Ip 过滤，如：ip.src == ....., ip.dst == ....., ip.addr == .....；
4. 端口过滤，如 tcp.port, tcp.srcport, tcp.dstport；

问题 3：文档中提到的 TCP 三次握手并不了解（可能后续会学），这里简要了解了一下

Step1：客户端发送一个 SYN=1，ACK=0 标志的数据包给服务端，请求进行连接，这是第一次握手；

Step2：服务端收到请求并且允许连接的话，就会发送一个 SYN=1，ACK=1 标志的数据包给发送端，告诉它，可以通讯了，并且让客户端发送一个确认数据包，这是第二次握手；

Step3：服务端发送一个 SYN=0，ACK=1 的数据包给客户端端，告诉它连接已被确认，这就是第三次握手。TCP 连接建立，开始通讯。



本次实验的体会（结论）（10 分） | 得分：

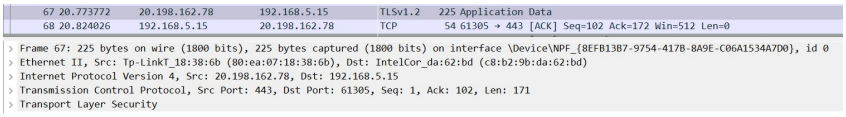
本次实验中了解了 wireshark 的工作原理，掌握 wireshark 抓包、记录和分析数据包的方法，通过软件的使用，对各个层次有了更清晰的了解，也对数据包中各层协议的格式有了直观的认识，为理论课的学习增添了实践的尝试。同时在学习软件过程中，了解到了 TCP 三次握手，也通过网络进行了检索和学习。

思考题：（10 分）

思考题 1：（4 分） | 得分：

写出捕获的数据包格式。

选择其中一例进行分析：



总览：

Frame:物理层的数据帧概况；

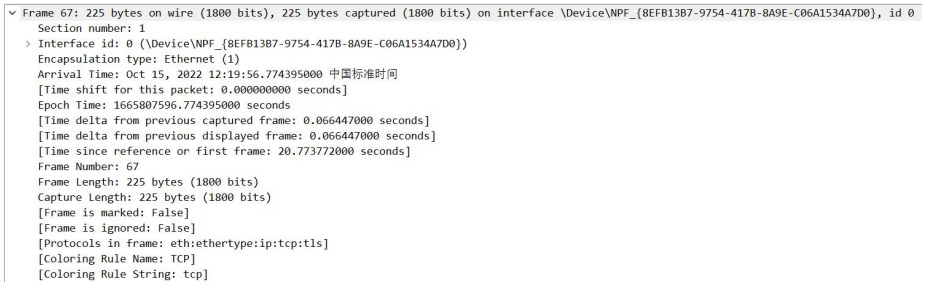
Ethernet II：数据链路层以太网帧头部信息；

Internet Protocol Version 4：网络层IP包头部信息；

Transmission Control Protocol：运输层数据段头部信息，此处是TCP协议；

Transport Layer Security：应用层信息，此处是TLS协议；

物理层数据帧概况：



Interface id：接口 ID

Encapsulation type: Ethernet (1)：封装类型

Arrival Time: 捕获日期和时间

Frame Number：帧序号

Frame Length：帧长度

Capture Length：捕获长度

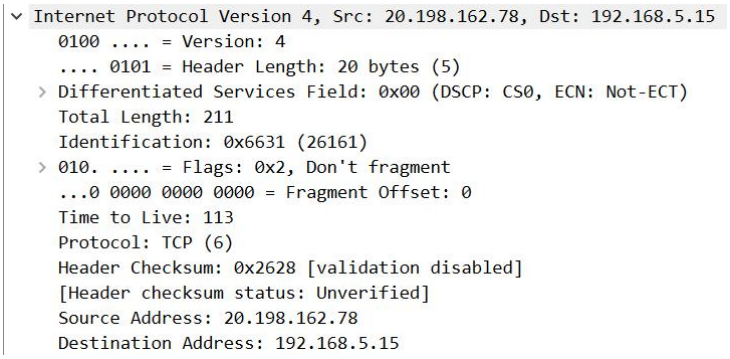
此外还有帧内封装的协议层、着色标记的协议名等信息。

数据链路层以太网帧头部信息：

Destination：目标 MAC 地址

Source：源 MAC 地址

网络层 IP 包头部信息：



Differentiated Services Field：差分服务字段

Identification：标记字段

Header Length：IP 包头部长度

还包括生存期 TTL，标志字段，分的偏移量等信息

运输层数据段头部信息：

```
Transmission Control Protocol, Src Port: 443, Dst Port: 61305, Seq: 1, Ack: 102, Len: 171
    Source Port: 443
    Destination Port: 61305
    [Stream index: 8]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 171]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3300716602
    [Next Sequence Number: 172    (relative sequence number)]
    Acknowledgment Number: 102    (relative ack number)
    Acknowledgment number (raw): 1536318907
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 7990
    [Calculated window size: 7990]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x0a60 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (171 bytes)
```

Source Port：源端口

Destination Port：目标端口

Stream Index：流序号

Sequence Number：序列号

还包括头部长度、TCP 数据段校验、流量控制、确认序列号等信息。

应用层信息：

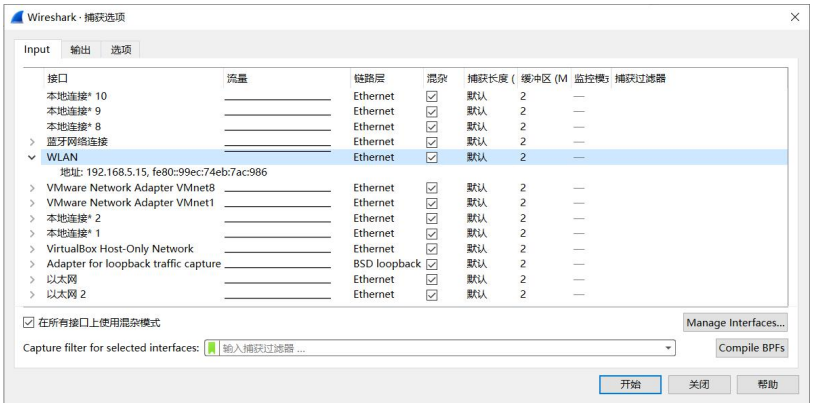
```
Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
```

思考题2：（6分）	得分：

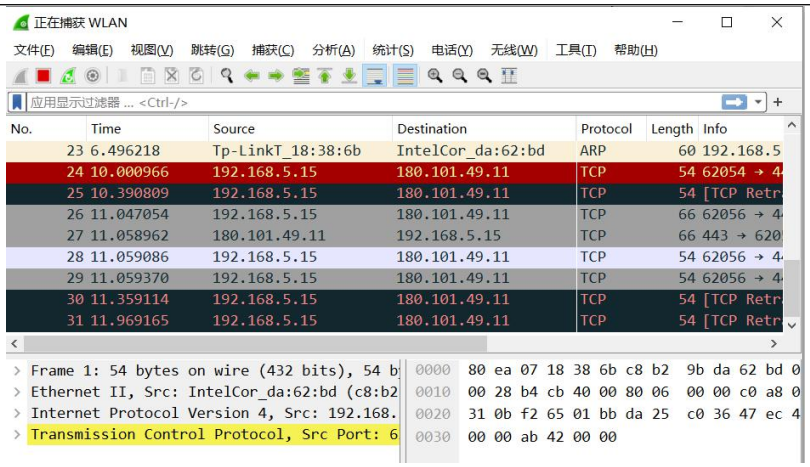
写出实验过程并分析实验结果。

1. 安装WireShark抓包工具；

2. 打开后在“捕获”- “选项”中选择需要监视的网卡。这里我选择WLAN，点击开始后，wireshark启动且处于抓包状态；



选择捕获选项

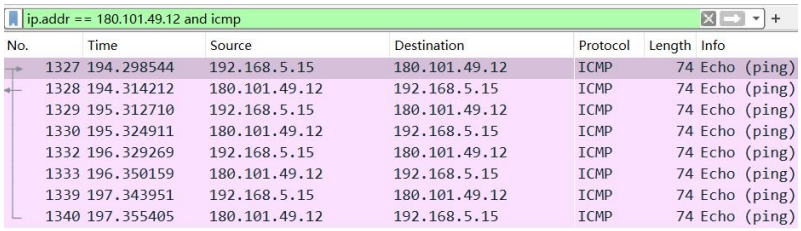


处于抓包状态的wireshark

3. 执行需要抓包的的操作，试一下ping百度，即在cmd中：ping www.baidu.com 可以看到源主机IP为180.101.49.12，就可以在wireshark中过滤出对应的数据包；

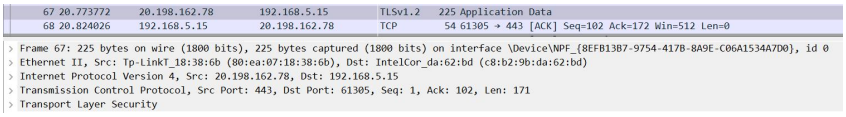
Ping命令连通网络

4. 在wireshark中设置过滤条件，得到所需的数据包；



过滤所需的数据包

5. 数据包详细信息部分



数据包详细信息

Frame:物理层的数据帧概况；

Ethernet II：数据链路层以太网帧头部信息；

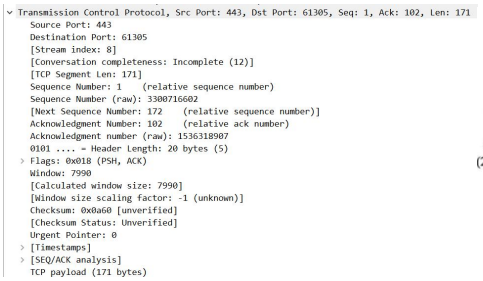
Internet Protocol Version 4：网络层IP包头部信息；

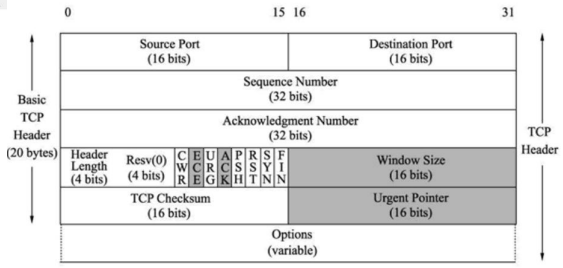
Transmission Control Protocol：运输层数据段头部信息；

Transport Layer Security：应用层

6. TCP包中的具体内容

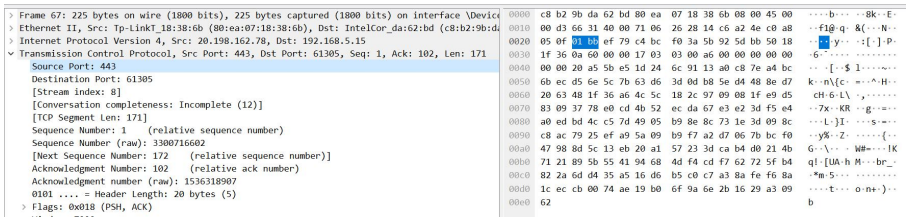
根据TCP的报文格式，可以在所获的TCP包中一一对应；





7. 分组字节流

从分组字节流中，可以找到对应的信息，以上述TCP中Source Port为例，对应了16字节的信息；



指导教师评语：

日期：