**北京邮电大学软件学院**

**2020-2021学年第一学期实验报告**

**课程名称： 计算机网络**

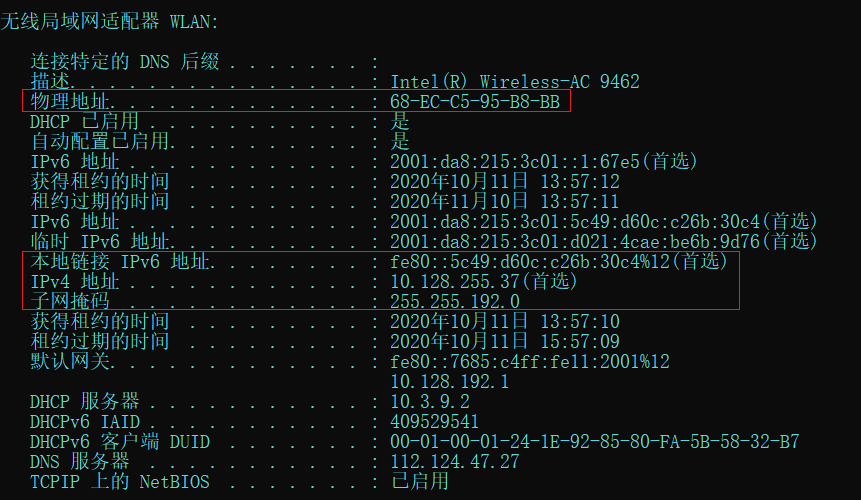
**实验名称： 数据链路层实验**

**指导教师：**\_\_\_\_\_雷友珣\_\_\_\_\_\_\_\_\_

**日 期： 2020年 10 月 15 日**

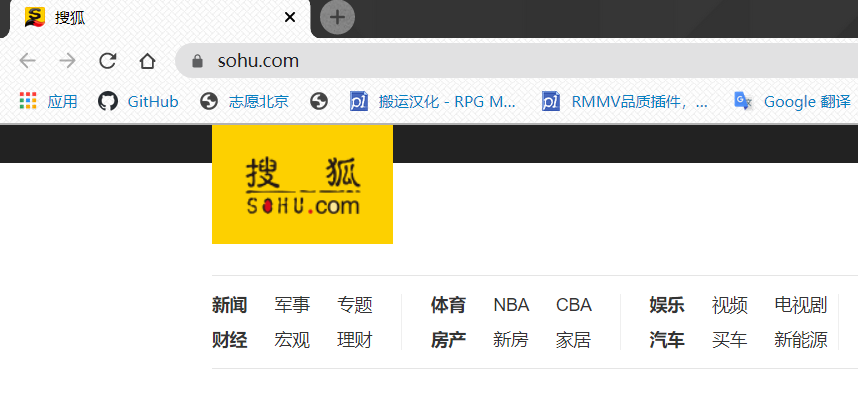
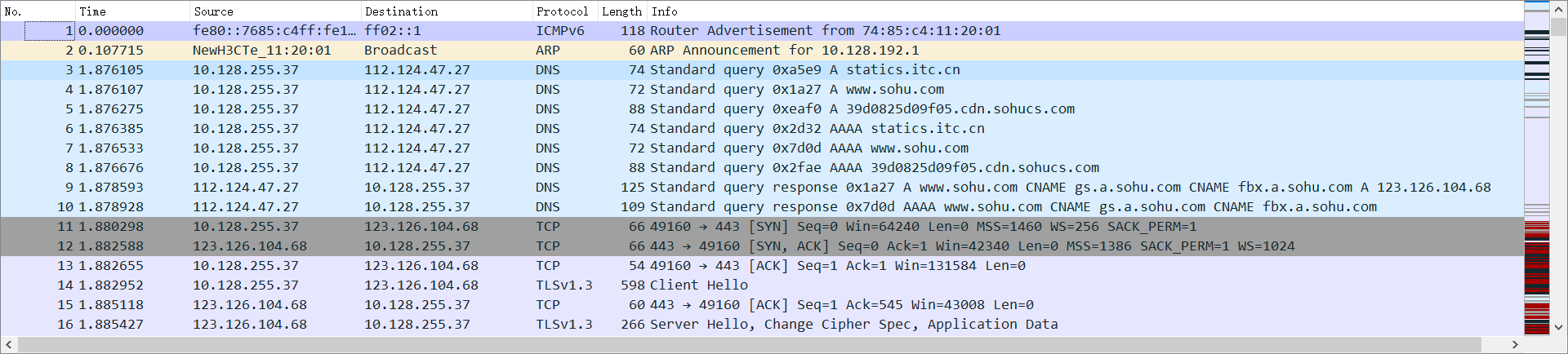
1. **实验目的**

通过本实验使学生理解协议数据单元（PDU）概念、掌握以太网帧结构字段定义和功能。

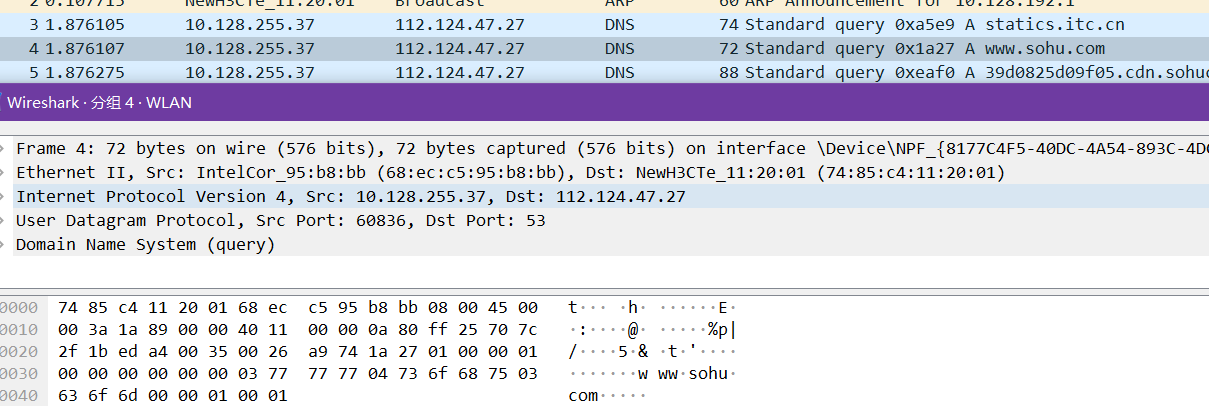
1. **实验内容**
2. 在可以访问互联网的主机上下载并安装网络抓包软件Wireshark。
3. 运行Wireshark软件，启动Wireshark软件的抓包功能抓取本主机访问互联网中某网站过程中发送和接收的数据包。
4. 对所抓取的数据包进行分析，分析所发送和接收的数据包的以太网帧结构中的源MAC地址、目的MAC地址和类型（type）字段的使用方法；理解各字段的含义和功能。
5. 选做部分：分析所抓取的数据包中的DNS（Domain Name System）消息、TCP报文、IP分组、HTTP协议消息的字段组成及作用。
6. **实验环境**
7. Windows系统主机；
8. Wireshark软件，软件下载网址：https://www.wireshark.org/
9. **实验结果**
10. **输入ipconfig/all查看本机MAC地址和IP地址。**

* 本机物理地址为: 68-EC-C5-95-B8-BB
* IP地址为：10.128.255.37
* DNS服务器为：112.124.47.27

1. **对抓取的数据包进行分析。**

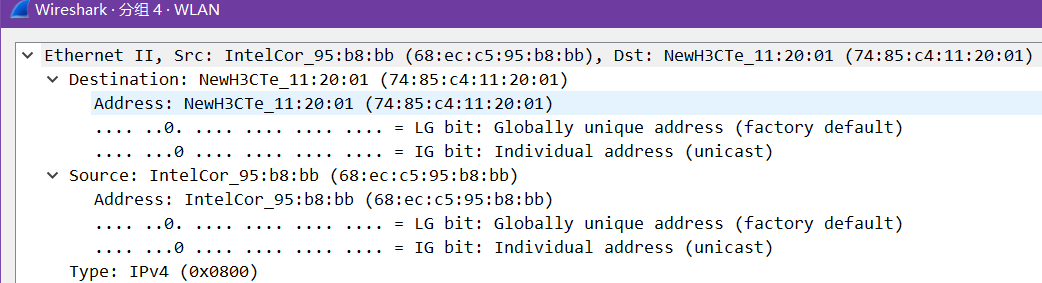
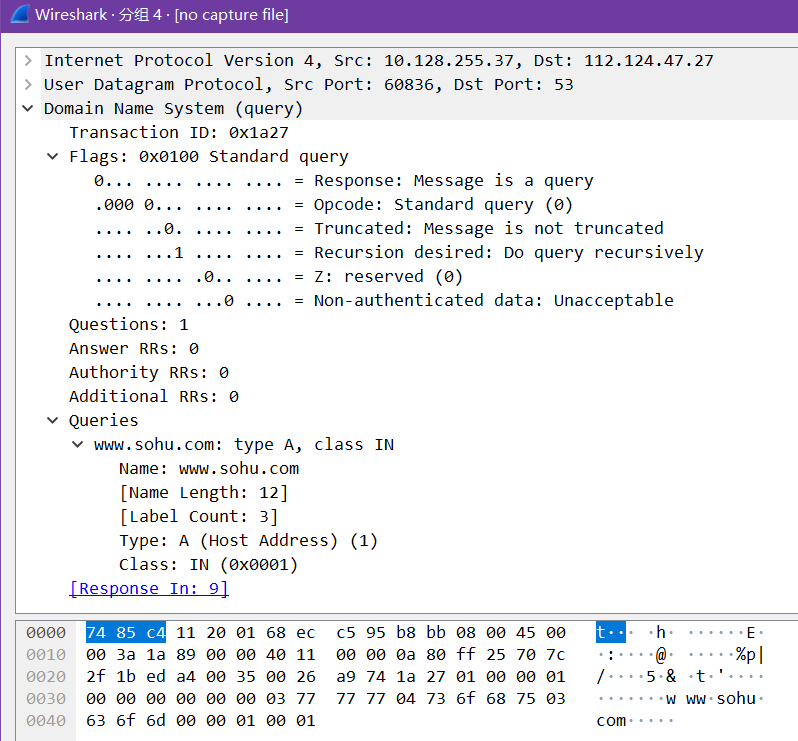
* 打开浏览器，输入[www.sohu.com](http://www.sohu.com)访问搜狐网站。
* 之后使用已打开的WireShark进行抓包分析操作。

从图中可看到从第3帧到10帧协议类型为DNS，源地址和目的地址为本机IP地址和DNS服务器地址，由此可以看出此过程为本机向DNS服务器询问[www.souhu.com](http://www.souhu.com) 的IP地址。

其中第3帧到第8为本地向DNS服务器发送请求，而第9帧到第10帧为DNS相应请求，返回[www.souhu.com](http://www.souhu.com) 的IP地址，

1. **对数据包进行简要分析操作**

以图中第4帧为例，对该数据包进行分析:

1. Frame 4:   物理层的数据帧概况，帧号为4，线路72字节，捕获2字节
2. Ethernet II: 数据链路层以太网帧头部信息，
3. Internet Protocol Version 4（IPV4）: 互联网层IP包头部信息。
4. User Datagram Protocol（UDP）:传输层的数据段头部信息，包含了UDP文字报。
5. Domain Name System（DNS）:应用层的信息。
6. **对Ethernet II数据链路层帧头部进行内容进行分析：** 
   * + 在该部分中共包含Destination、Source、Type三个字段。
     + Destination: (74:85:c4:11:20:01)接收方的MAC地址，该数据包中代表的是DNS服务器的MAC地址。
     + Source: (68:ec:c5:95:b8:bb)发送方的MAC，该数据包中代表的是本机物理地址。
     + Type: IPv4 (0x0800) 使用的IP协议，该数据包网络层使用的是IPV4协议。
7. **选作部分：分析DNS消息。**
   * + 点开第4帧中的Domain Name System（DNS）对其进行分析：
     + Transaction ID字段记录了本次事务的ID，
     + Flags字段，包含以下属性：

Response：响应消息，0代表查询报文。

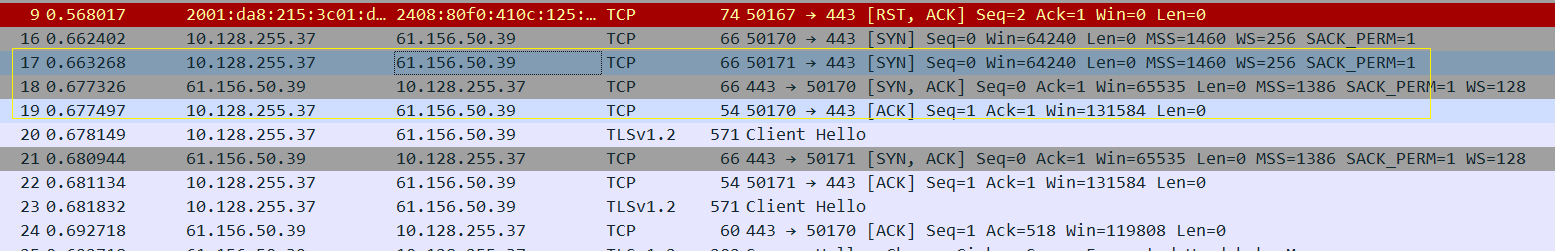
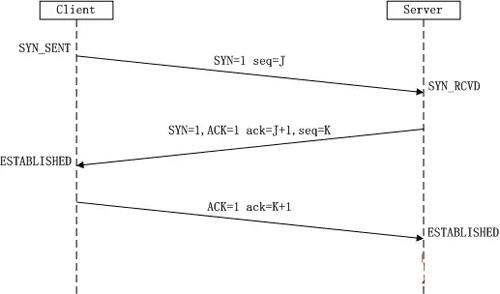
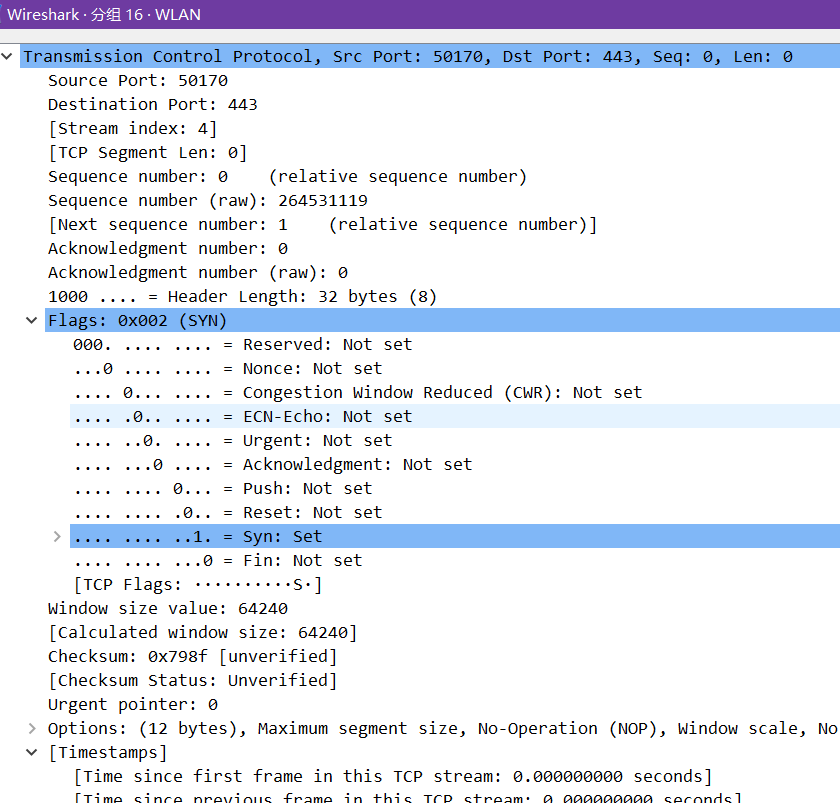
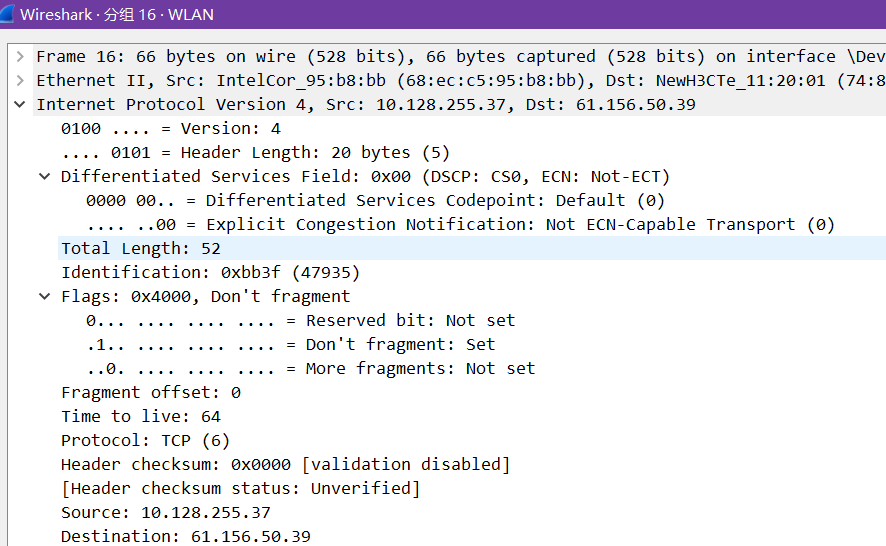
Opcode：通常值为0，标准查询

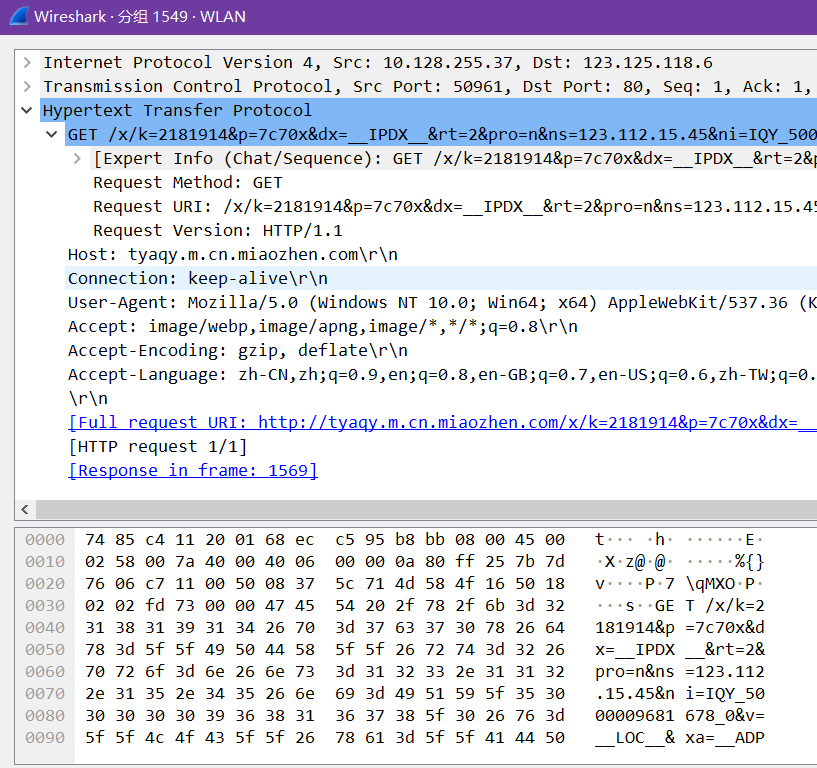
Truncated：表示报文是否可截断，0代表不可截断。

Recursion Desired：表示期望回归。

Z：表示保留值

* + - Question字段：问题计数，由于本次查询的问题只有一个，因此该字段的值为1。
    - Answer RRS字段：表示应答消息计数，可以知道该数据包中没有应答消息。
    - Queries字段：记录了详细的问题，回答9类型为name响应网站名。

1. **选作部分：TCP报文分析。**
   * + 通过浏览器访问[www.huawei.com](http://www.huawei.com) 并在wireshark中进行数据包抓取，过滤出TCP的数据包之后，对TCP数据流进行查看。
     + 查看结果如图所示，黄框所示部分为TCP三次握手建立连接部分：
     + 第一次握手数据包No17：客户端发送一个TCP，标志位为[SYN]表示请求连接，Seq=0初始建立连接值为0，代表客户端请求建立连接。
     + 第二次握手数据包No18：服务器发回确认包, 标志位为[SYN,ACK] 表示同意连接，Seq=0表示当前还没有发送数据，Ack=1表示当前端成功接收的数据位数。
     + 第三次握手数据包No19：客户端发送确认包，标志位为[ACK]表示已经收到记录，Seq=1表示当前已发送数据，Ack=1表示当前端成功接收的数据位数。
     + 至此发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。
     + TCP握手图解：
     + TCP报文分析：
     + Source Port: 发送方端口号，标识报文的返回地址。
     + Destination Port: 接收方端口号，指明接收方计算机上的应用程序接口。
     + Sequence number: 报文的序列号，用来标识TCP源端设备向目的端设备发送的字节流。
     + Acknowledgment number: 确认序列号，标识期望收到的下一个段的第一个字节，并声明此前的所有数据已经正确无误地收到，因此，确认号应该是上次已成功收到的数据字节序列号加1。
     + Header length: 报文头部长度。
     + Flags: 标记字段，记录了报文的性质，比如ACK，SYN，RST，FIN 等。
     + Window size value: 流量控制的窗口大小，通过控制该字段，防止发送方发送消息速度过快，从而淹没接收方。
     + Checknum: 数据段的校验和
     + Options：选项字段是为了适合复杂网络环境和更好地服务于应用层设计的。
     + TimesTamp：时间戳选项用来计算往返时间RTT，发送方在发送报文段时把当前时钟的时间值放入时间戳字段，接收方将该时间戳字段的值复制到确认报文中，当接收方收到确认报文，对比确认报文的时间戳(等于发送方发送报文段的时间戳)和现在的时钟，即可算出RTT。
2. **IP分组字段解析：**
   * + Version: 版本，该包使用的是IPv4协议。
     + Header Length: 头长度，该包中IP字段的总长度为20字节。
     + Differentiated Services Field: 服务类型。
     + Total Length: 数据包总长度。
     + Flags: 标记字段，共R、DF、MF三位。目前只有后两位有效，DF位：为1表示不分片，为0表示分片。MF：为1表示“更多的片”，为0表示这是最后一片。
     + Time to live：IP报文所允许通过的路由器的最大数量。每经过一个路由器，TTL减1，当为0时，路由器将该数据报丢弃。
     + Protocol：指出IP报文携带的数据使用的是那种协议，该包中IP协议的上层协议为TCP协议，协议号为6。
     + Header checksum: 首部校验和，检查IP报头的完整性。
     + Source：10.128.255.37发送方的IP地址，该包中为本机。
     + Destination：61.156.50.39 接收方的IP地址，该包中为HTTP服务器。
3. **HTTP协议消息格式：**
   * + 通过浏览器访问[www.iqiyi.com](http://www.iqiyi.com) 并在wireshark中进行数据包抓取，过滤出HTTP的数据包之后进行分析。



* + - HTTP协议的请求方法有GET、POST、HEAD、PUT、DELETE、OPTIONS、TRACE、CONNECT。这里介绍最常用的GET方法和POST方法。
    - GET:当客户端要从服务器中读取文档时，使用GET方法。GET方法要求服务器将URL定位的资源放在响应报文的数据部分，回送给客户端。使用GET方法时，请求参数和对应的值附加在
    - URL后面，利用一个问号(“?”）代表URL的结尾与请求参数的开始，传递参数长度受限制。例如，/index.jsp?id=100&op=bind。
    - POST:当客户端给服务器提供信息较多时可以使用POST方法。POST方法将请求参数封装在HTTP请求数据中，以名称/值的形式出现，可以传输大量数据，可用来传送文件。

1. **附录**

**调试心得：**通过使用Wireshark软件对网络数据包进行抓取，对日常生活中的一些网络使用有了更清晰的了解，对各种协议字段组成及含义有了更深的了解，对数据链路层的协议数据单元及功能有了更深的认识，另外提前预习了其他层协议的一些基础知识，对计算机网络有了更加深刻的理解。