**《计算机网络》课内实验**

**实 验 指 导 手 册**

**授课教师：**

**实验指导教师：**

**教学对象：软件工程专业**

**开课时间： 第五学期**

**北京邮电大学计算机学院**

**2022年8月**

**实验一：协议过程及数据包格式分析（3学时）**

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、网络层IP分组、传输层协议数据包、应用层协议消息的字段定义和功能；理解应用层、传输层、网络层、数据链路层协议过程。

1. **实验任务**

基于Windows或Linux等操作系统环境，安装网络抓包软件（Wireshark软件），搭建实验环境。使用网络抓包软件（Wireshark软件）抓取访问某Web网站过程中所产生的数据包，分析访问该Web网站过程中所产生的应用层协议消息、传输层协议消息、网络层协议消息、数据链路层协议消息的交互过程；分析其中的以太网帧、网络层IP分组、传输层协议数据包、应用层协议消息的字段定义和作用。

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Web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，分析以太网帧、网络层IP分组、传输层协议数据包、应用层协议消息的字段定义和字段的作用，包括但不限于分析抓取的以太网帧、ARP协议数据包、IP分组、TCP协议数据包、HTTP协议消息、DNS协议消息的字段组成及作用。
5. 分析访问Web网站过程中的协议消息过程。
6. **实验环境**
7. Windows系统主机或Linux系统主机；
8. Wireshark软件，软件下载网址：https://www.wireshark.org/
9. **实验进度安排**

本实验3学时。在实验前，根据所使用的主机操作系统，下载正确的Wireshark软件版本、下载Wireshark软件使用手册，学习Wireshark软件的使用；预习DNS协议、HTTP协议、TCP协议、IP协议、ARP协议、以太网数据链路层协议的功能、协议过程和协议消息格式定义。

1. **实验方法与步骤**
2. 在主机上安装Wireshark软件。在安装过程中勾选上Wireshark软件提示的“Plugins & Extensions”、“Npcap”、“Install USBPcap”等可选安装选项，以及弹出的“Installation Options”弹出窗口中列出的包括“Support raw 802.11 traffic(and monitor mode) for wireless adaptors”在内的所有可选项。
3. 检查主机是否能够正常访问互联网。如果不能，检查出错原因并排除故障。
4. 以管理员身份运行Wireshark软件，选择主机访问互联网所使用的网卡（NIC），开启在这个网卡上的抓包功能。通过点击如图1所示的Wireshark主窗口的“捕获”→“选项”菜单项，弹出图2所示窗口，在图2窗口中，列出了计算机中配置的网卡；然后，点中访问互联网所要使用的网卡，然后点击“开始”按钮，就可以开启对该网卡上发送/接收到的消息的捕获。

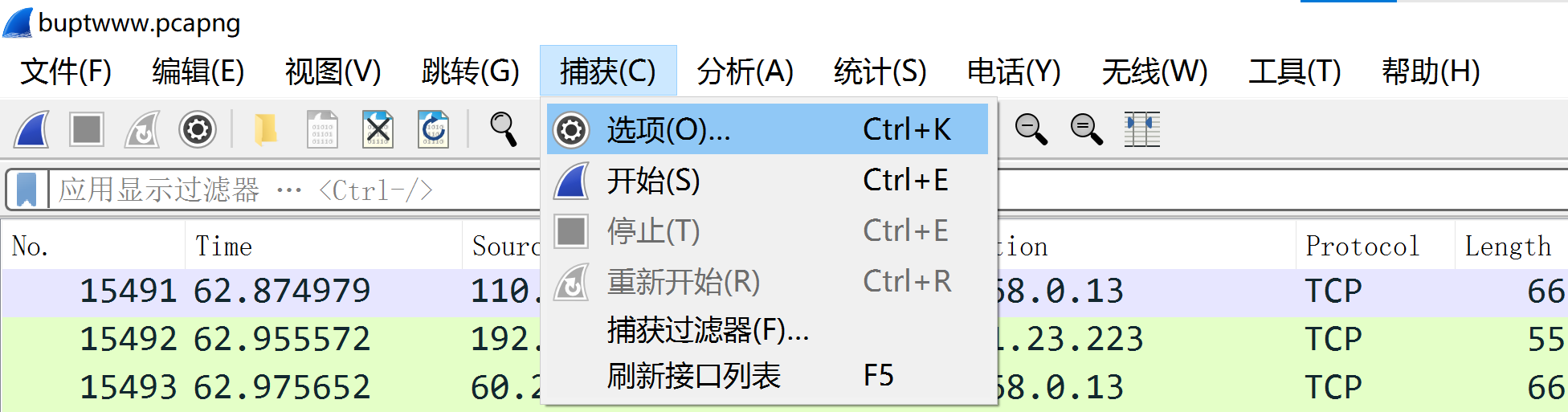


图1

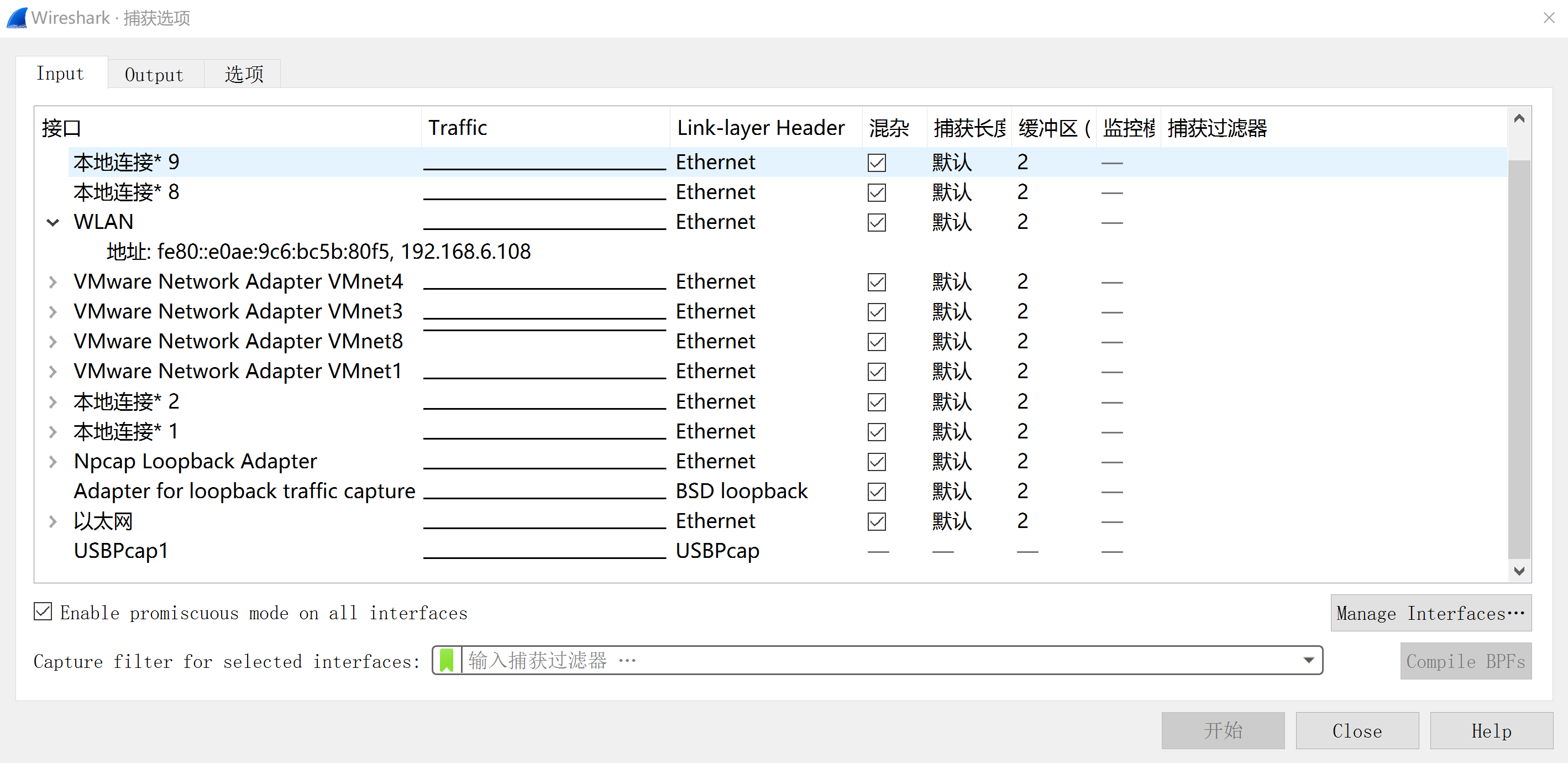


图2

1. 然后，在主机上启动浏览器程序，在浏览器的地址栏输入需要访问的Web网站的网址（URL地址）。正常情况下，应该可以看到在浏览器窗口上呈现网页内容过程的同时，在Wireshark软件主窗口中看到Wireshark抓取的数据包在不断递增。若鼠标双击Wireshark主窗口中与一个数据包对应的记录，会弹出此数据包的解析窗口。

图3展示的是Wireshark软件主窗口展示的抓取的消息。在图4 所示的Wireshark软件主窗口的查询框中，输入“dns.qry.name == 所访问的网站域名”，查看本次网站访问过程中，主机是否发出了用于查询域名的DNS查询请求消息。图4所示的查询框中可以设置多种查询条件，以从所抓取的消息中筛选出想查看的消息。图5展示了查询webvpn.bupt.edu.cn域名的DNS查询请求消息和响应消息。

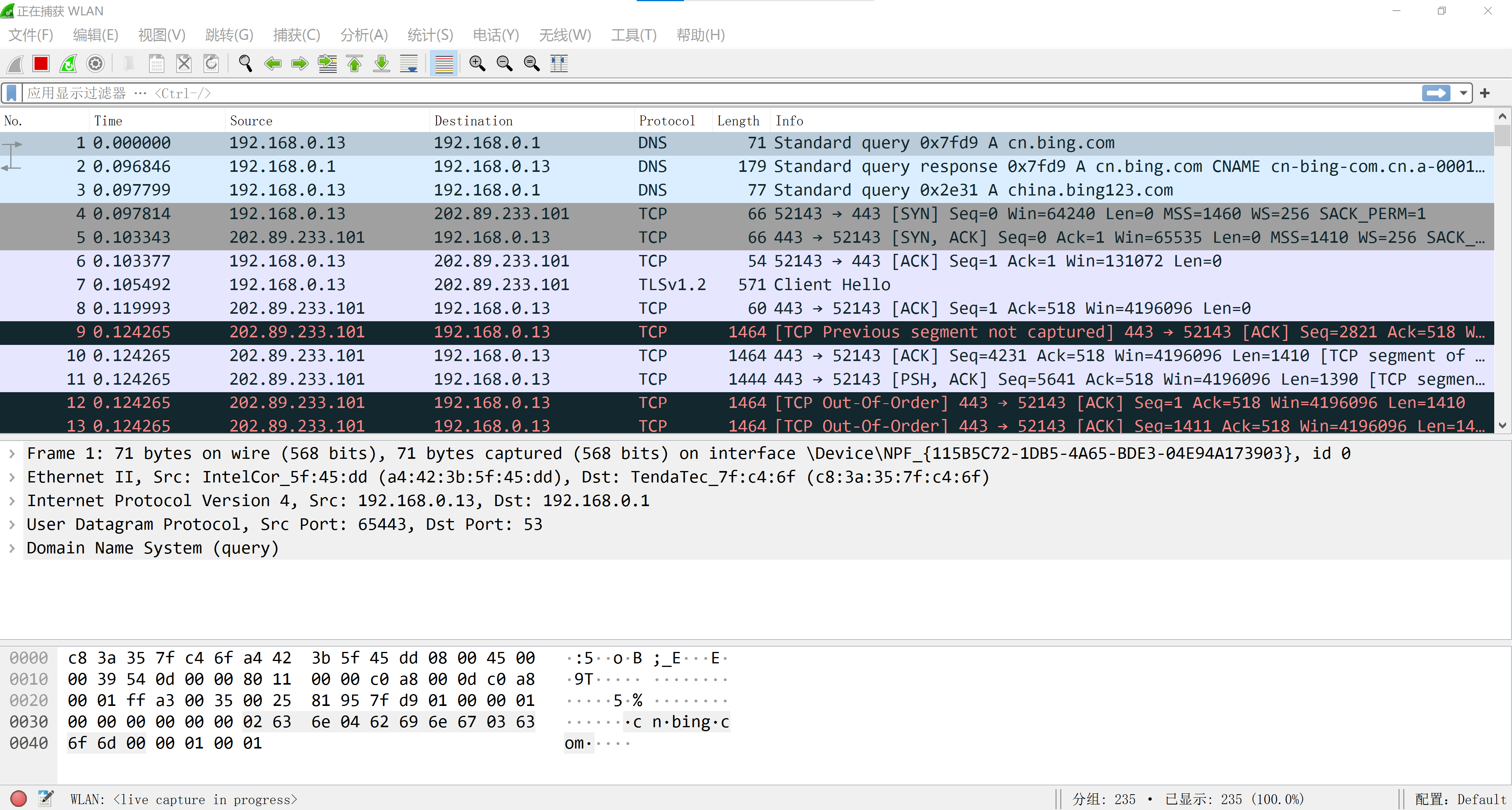


图3

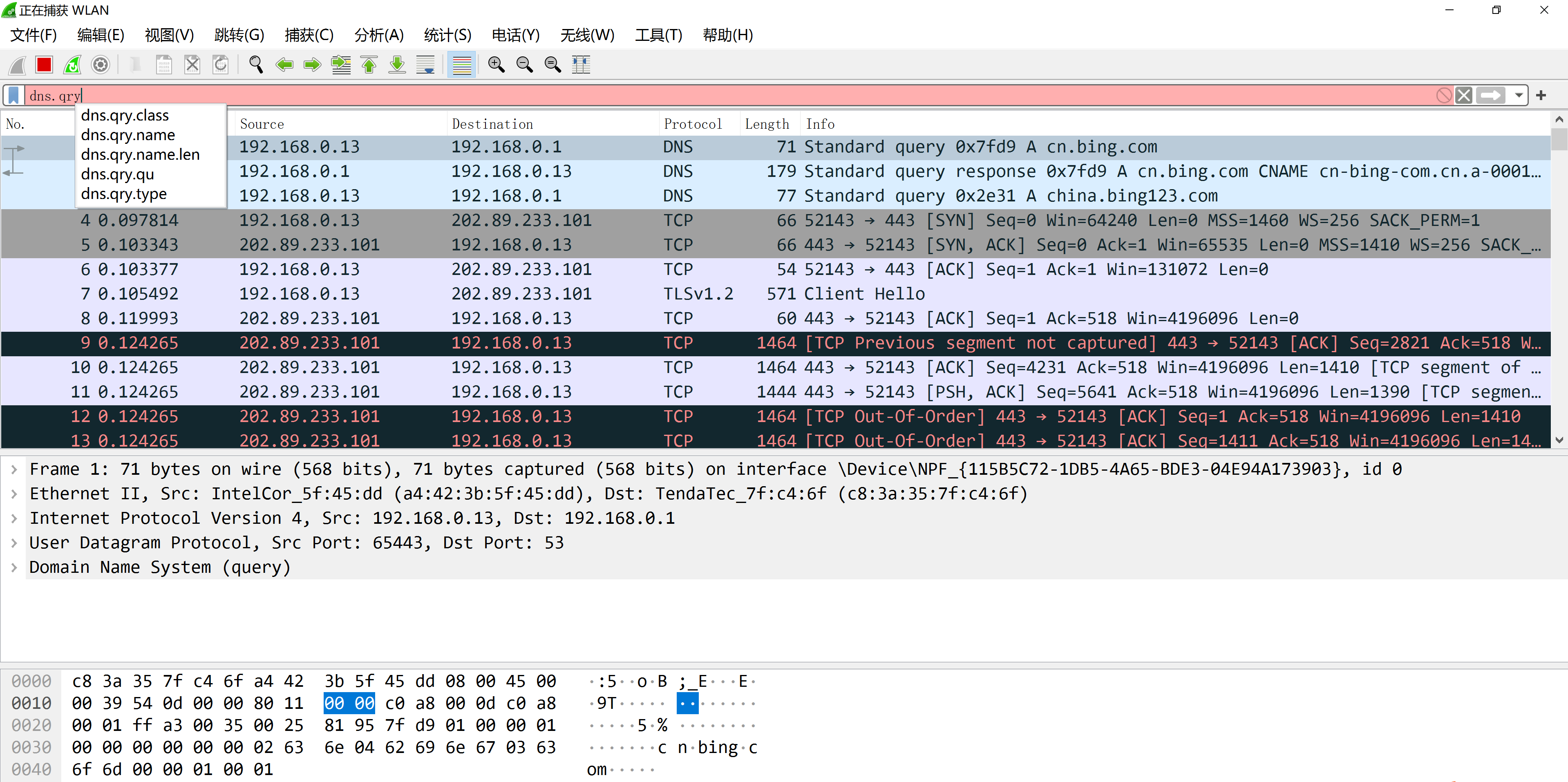


图4.

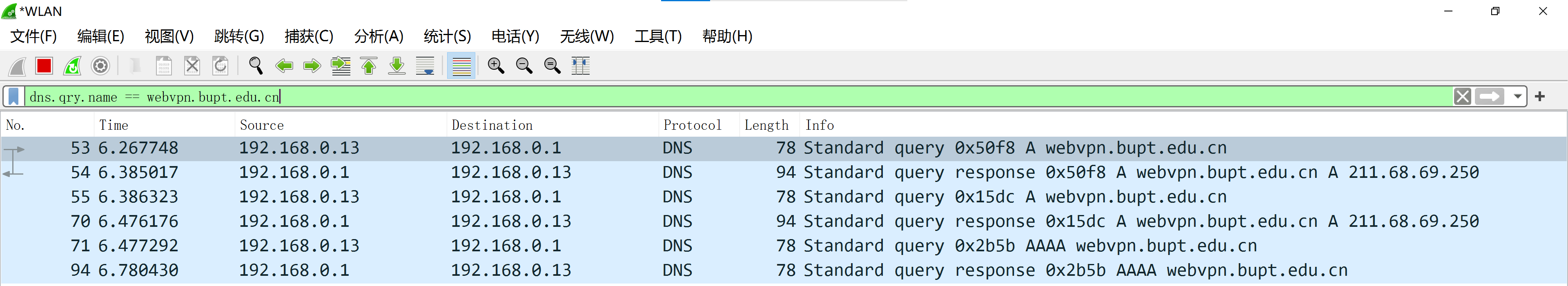


图5

双击图5中的第一条消息（序号为53的消息，该条消息为DNS查询请求消息），弹出图6窗口。图6窗口展示了图5中第一条消息的消息解析结果。双击图5中的第二条消息（序号为54的消息，该条消息为DNS查询响应消息），弹出图7窗口。图7窗口展示了对应于图6中的DNS查询请求消息的DNS查询响应消息，该DNS查询响应消息中携带了域名webvpn.bupt.edu.cn对应的IP地址信息。

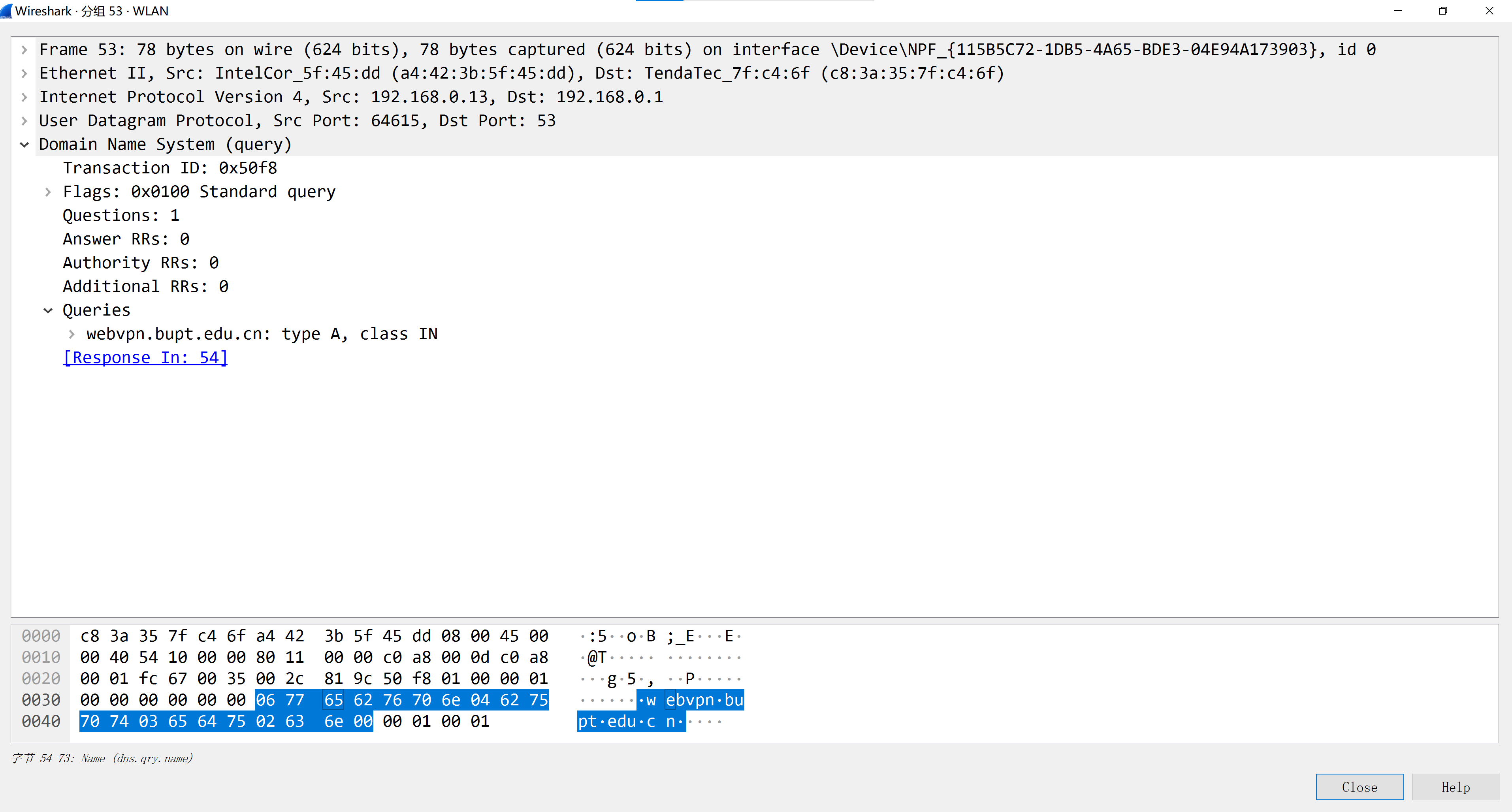


图6

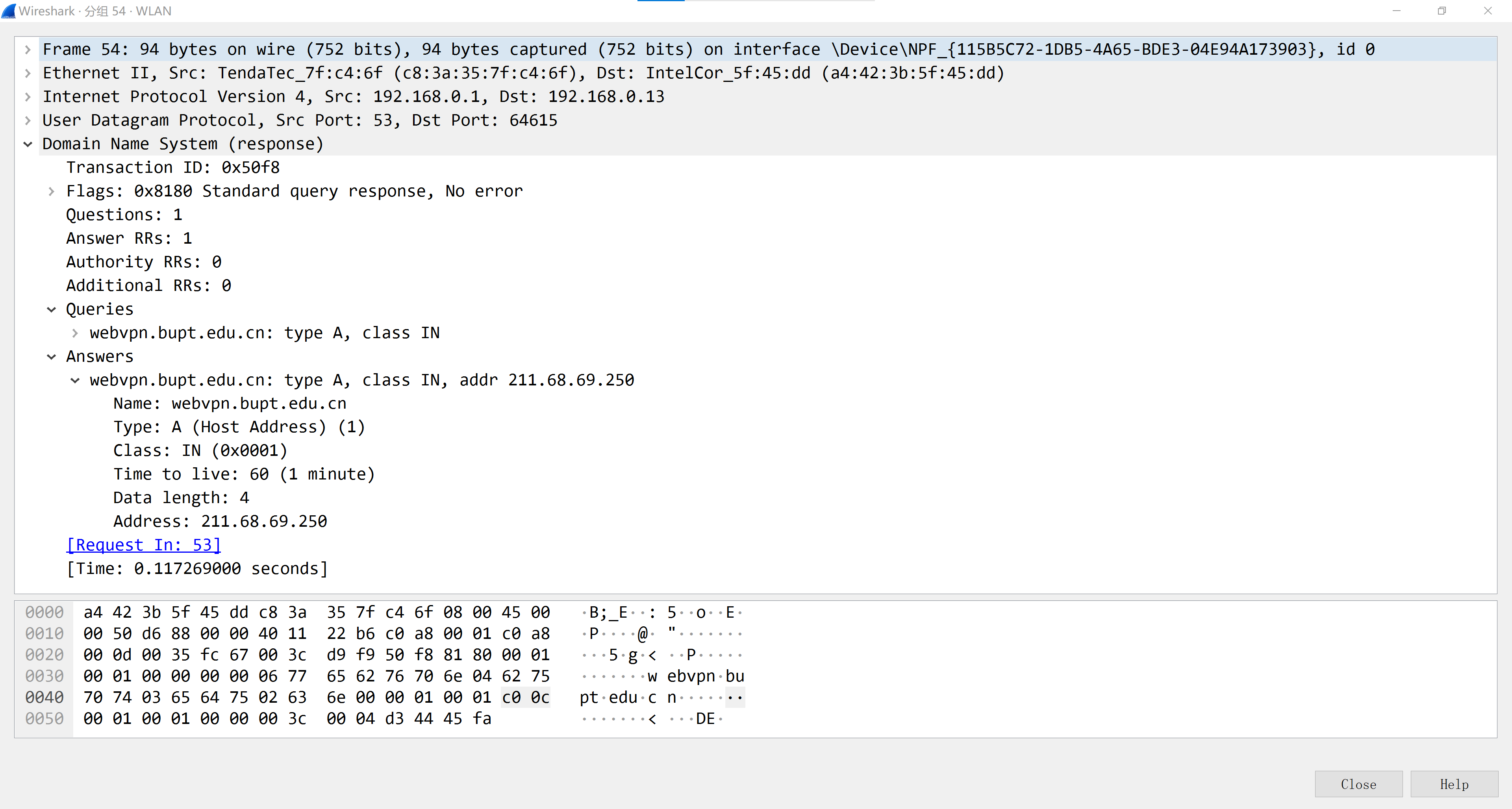


图7

1. 协议消息过程分析：在Wireshark主界面的查询栏中输入“ip.addr == 所访问的网站的IP地址”，可以看到在Wireshark主界面的窗口中显示本主机与该网站交互（发送/接收）的消息。图8展示的是本次访问https://webvpn.bupt.edu.cn过程中，主机与该网站交互的消息。(注：实验中，所访问的网站可以是使用HTTP协议进行访问的网站，不需要是使用HTTPS协议进行访问的网站。)

在Windows系统中，使用*ipconfig*命令查看本机网卡的IP地址和MAC地址；不同的Linux系统版本中，可使用*ifconfig*命令或*ip address*命令查看网卡的IP地址和MAC地址，在Ubuntu 18系统中可使用*ip address*命令。在获得本机网卡的IP地址后，在Wireshark主窗口的查询栏中设置查询条件为“ip.addr == 本机抓包所使用的网卡的IP地址”，查询本机通过该网卡所发送/接收的数据包。

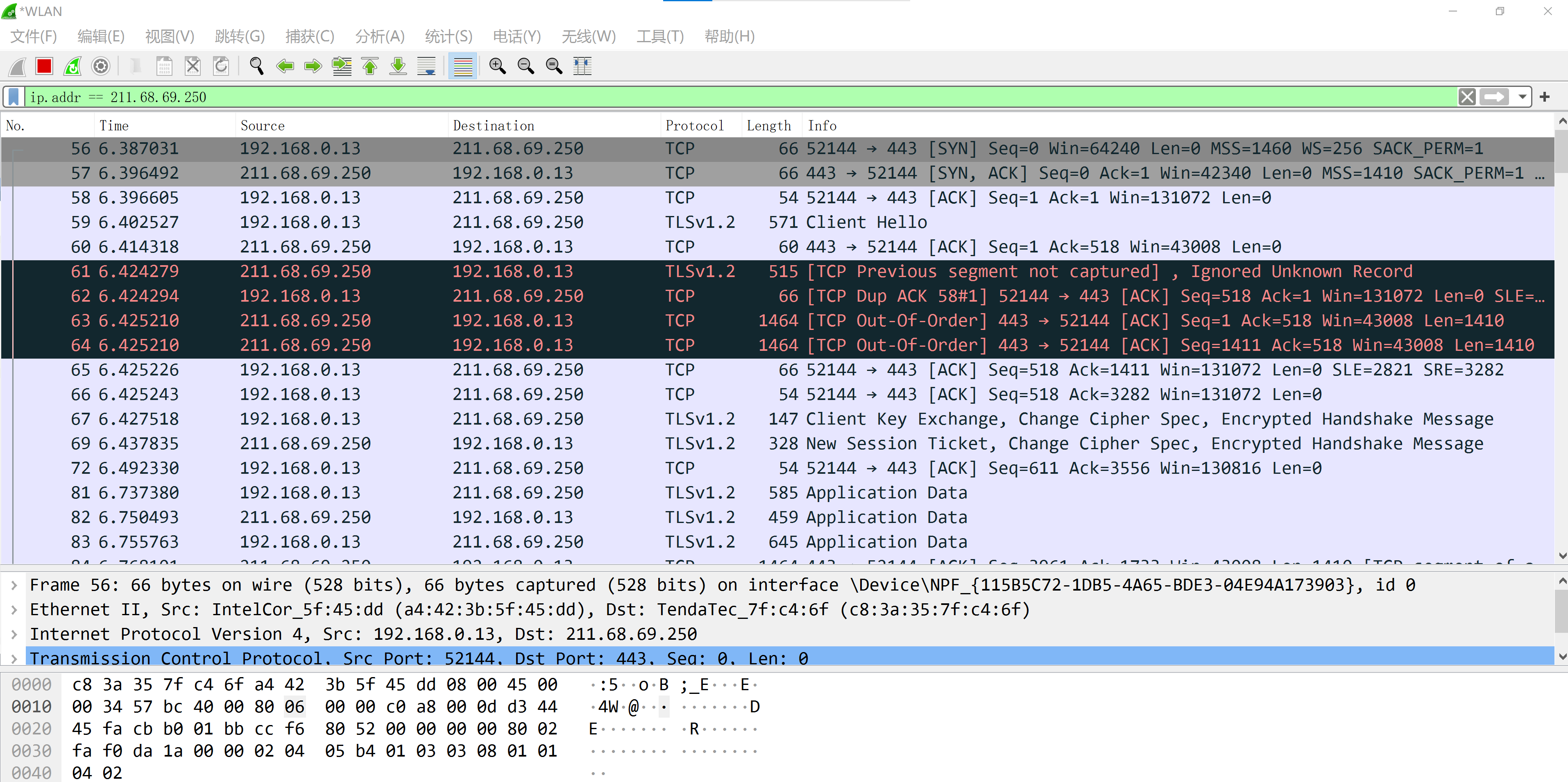


图8

主机访问Web网站的协议消息交互的基本过程如下：在主机的缓存中没有该网站的DNS域名对应的IP地址信息时，主机会发出DNS查询请求消息，以获得网站域名对应的IP地址，如果在主机的缓存中有该网站的DNS域名对应的IP地址信息，主机不会发出DNS查询请求消息；在主机获得网站的IP地址后，主机与Web网站建立TCP连接，TCP连接的建立过程采用三次握手机制，在建立TCP连接的过程中，主机与所访问的Web网站之间交互三条TCP协议消息；在TCP连接建立后，主机会在这条TCP连接上发送用于访问该Web网站网页内容的HTTP请求消息，Web网站接收到该HTTP请求消息后，会发出包含有该网页内容的HTTP响应消息，在该HTTP响应消息长度大于一个TCP报文能够携带的消息的长度时，该HTTP响应消息会通过多条TCP协议消息发送给主机。主机的浏览器在接收到响应消息后，解析该网页内容，包括该网页中携带的超链接（Hyperlink），这些超链接有些指示了需要进一步获取的资源（如图片、音频、视频）的网址，对这些资源，浏览器会分别向这些超链接地址发出获取资源的请求消息。

在互联网使用的TCP/IP协议体系结构中，用于标识主机与Web网站间的一条TCP连接所使用的信息是：主机端的网卡IP地址、主机端的TCP端口号、Web网站端的IP地址、Web网站端的TCP端口号。

图8中序号为56、57、58的三条消息是访问webvpn.bupt.edu.cn网站时，建立TCP连接时主机与网站交互的三条TCP协议消息。分别鼠标双击图8中的这三条消息，Wireshark软件弹出图9、10、11所示三个窗口，这三个窗口展示了Wireshark软件对这三条消息的解析结果。图9、10、11窗口展示的内容有：IP分组头（IP Header）字段的解析、TCP报文的报文头（TCP Header）字段的解析、以及数据链路层消息（以太网帧）头字段的解析。

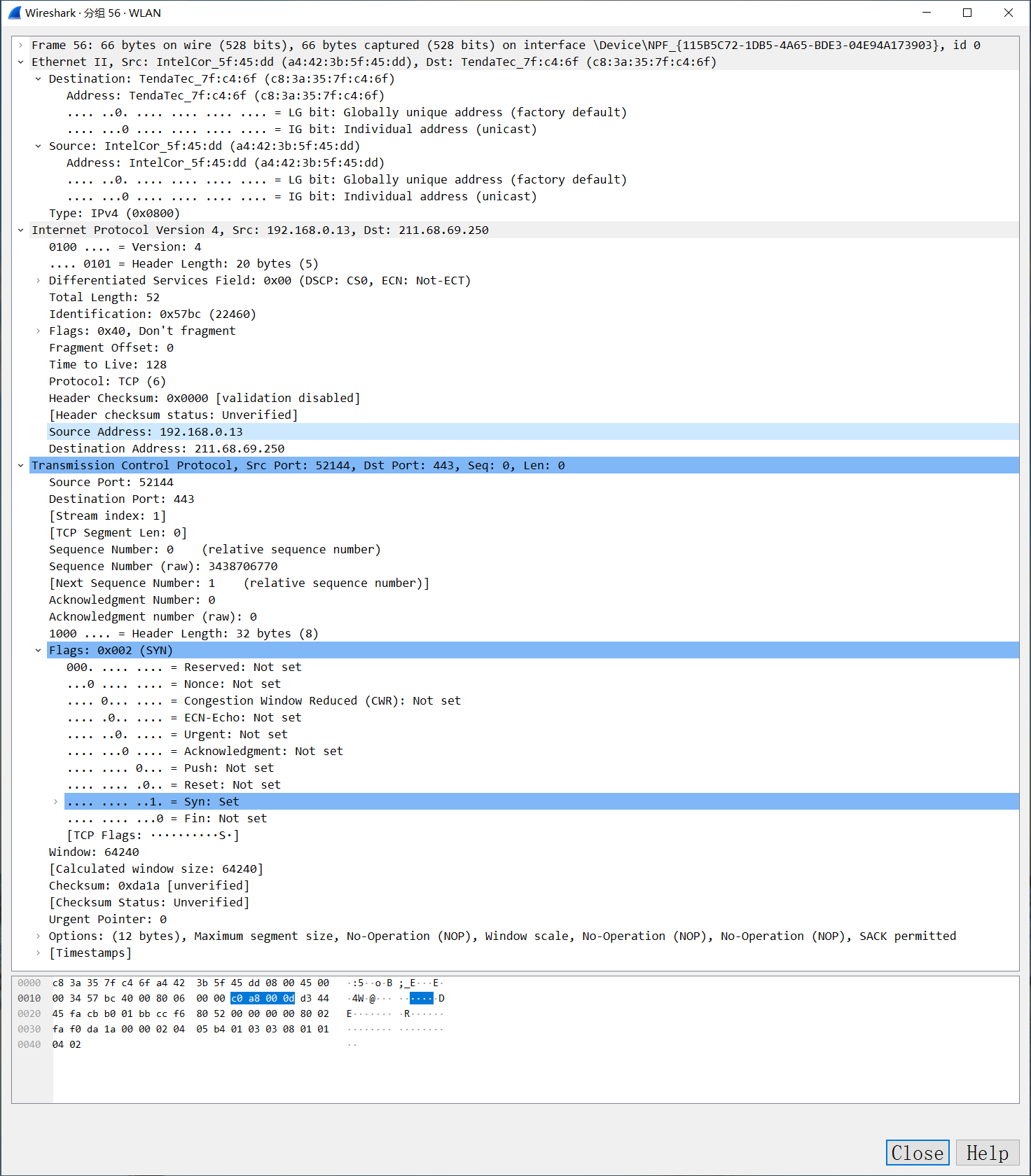


图9

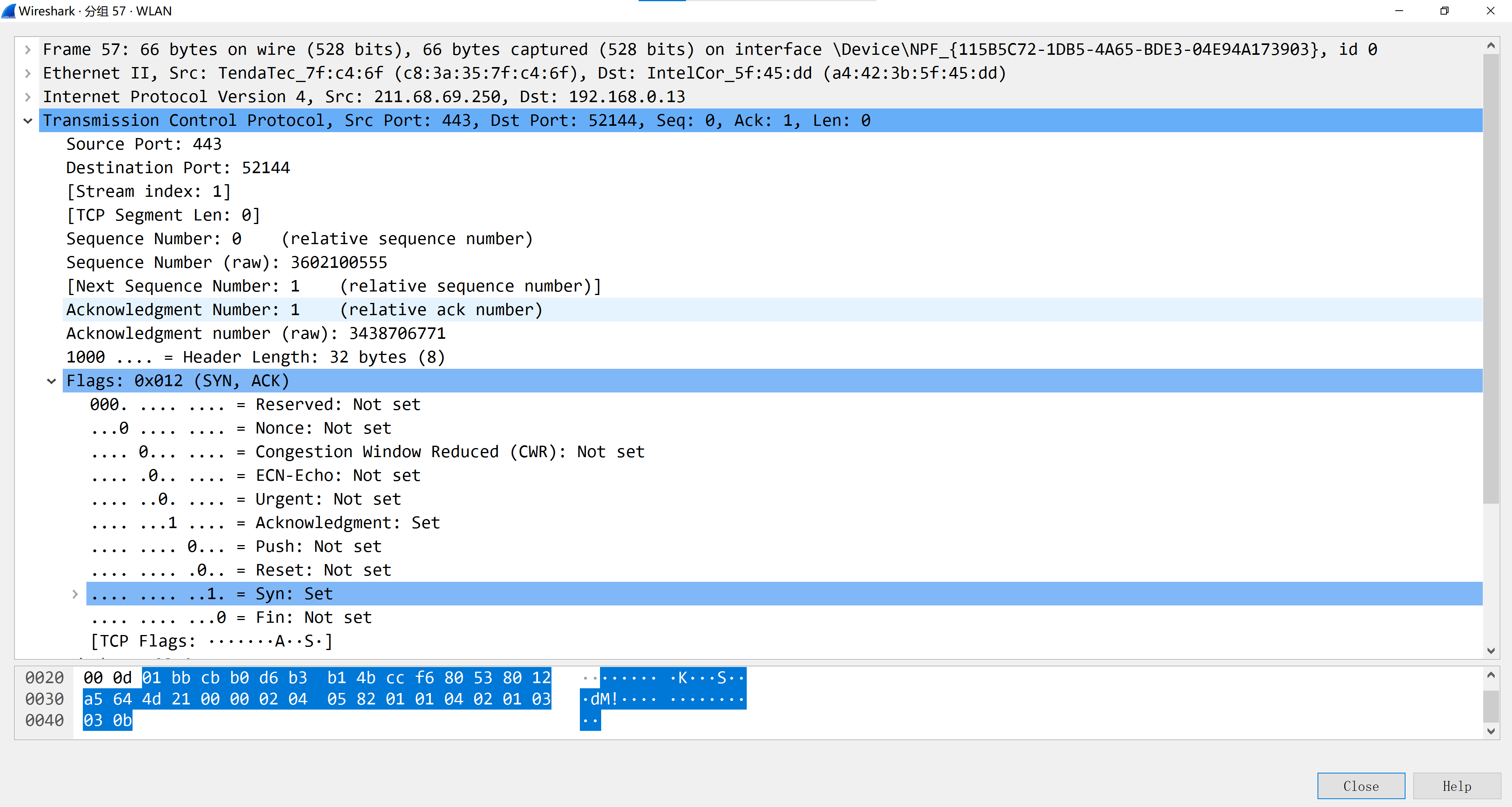


图10

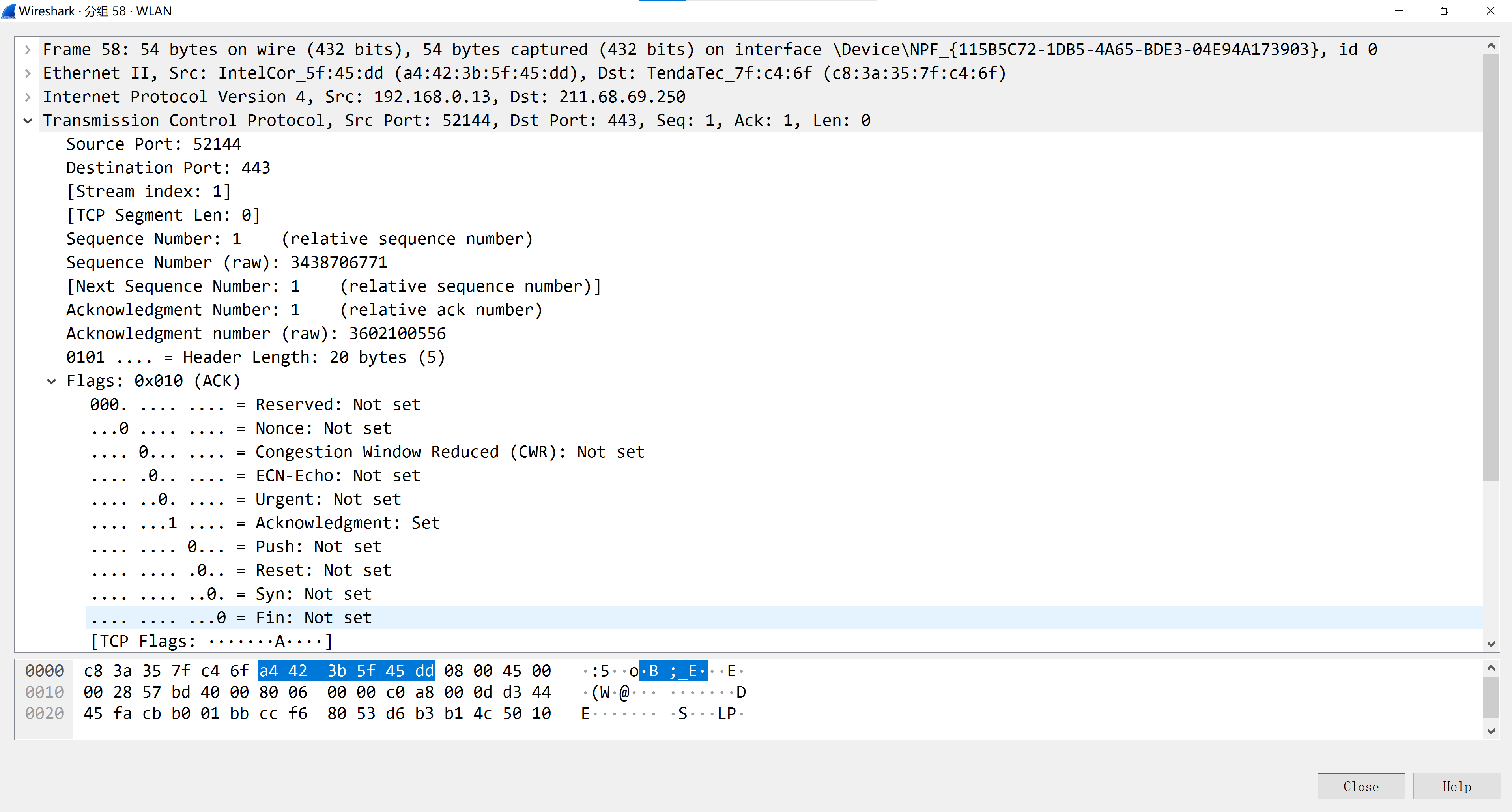


图11

通过分析主机与Web网站交互的消息，分析在本Web网站访问过程中，HTTP协议消息收发过程、TCP连接建立过程、IP消息收发过程、以太网帧的收发。注：主机发出的以太网帧中的目的MAC地址不是所访问的Web网站的IP地址所对应的网卡的MAC地址；主机所发出的以太网帧中的目的MAC地址是主机所在子网中的某一路由器的网卡的MAC地址，主机访问该Web网站时发送的消息通过该路由器转发。

分析所抓取的数据包是本主机发送的数据包，还是本机接收的数据包。分析访问该Web网站过程中发生的DNS协议过程、HTTP协议过程、TCP协议过程、IP分组收发、以太网帧的收发过程；并分析以下数据包的字段格式定义及字段的作用：以太网帧、IP分组、TCP协议消息；DNS协议消息。

1. 查看在上述抓包过程中是否抓取到了ARP协议消息，分析所抓取的ARP协议消息的字段组成和作用。如果没有抓取到ARP消息，停止Wireshark抓包过程，将所抓取的数据包存入一个新的文件中，以备后用。然后，使用*arp –a*命令查看本主机的arp缓存（arp cache）中的信息，在管理员权限（或超级用户权限）下使用*arp -d*命令清空本主机的arp缓存，然后再做一次上述的抓包过程，查看是否能抓取到ARP协议消息。对Windows或Linux系统中的*arp*命令的使用请查阅相关手册和资料。
2. 停止Wireshark抓包过程，退出Wireshark软件前将所抓取的数据包存入一个新的文件中，以备后用。
3. **实验管理规则及实验验收**

实验完成后填写并提交实验报告。实验报告需记录实验过程、所抓取的数据包界面截图，分析所抓取的数据包。对所抓取的数据包，选择能够体现协议过程的数据包，对其中的以太网帧结构、ARP协议数据包、IP分组、TCP数据报、DNS协议消息字段的定义和作用进行说明，并基于所抓取的数据包阐述协议过程。

实验报告需要对实验过程描述清晰、规范、准确。