# 信息通信网络及应用实验报告

**实验名称： WireShark网络数据包捕获和分析**

**姓名：**

**班级：**

**学号：**

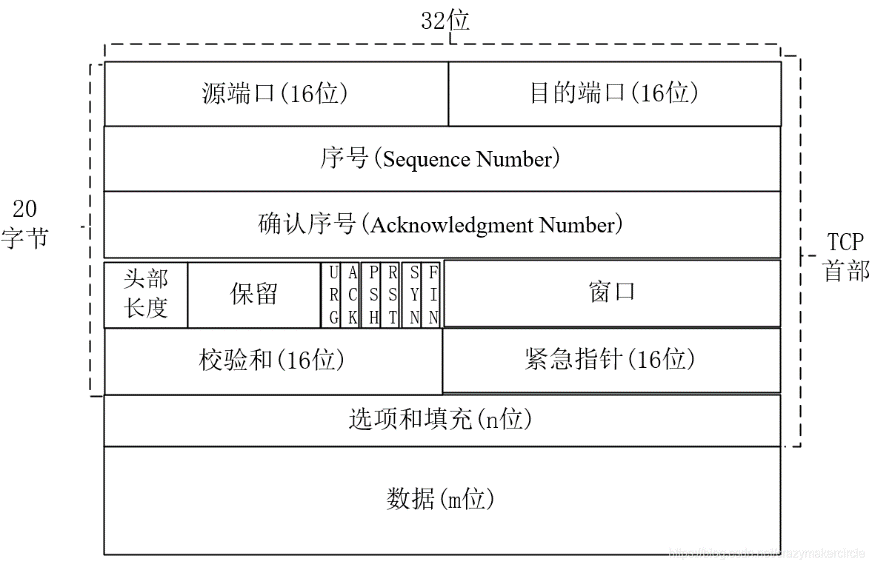
**日期： 2024年6月13日**

**评阅意见：**

**分数： 签名：**

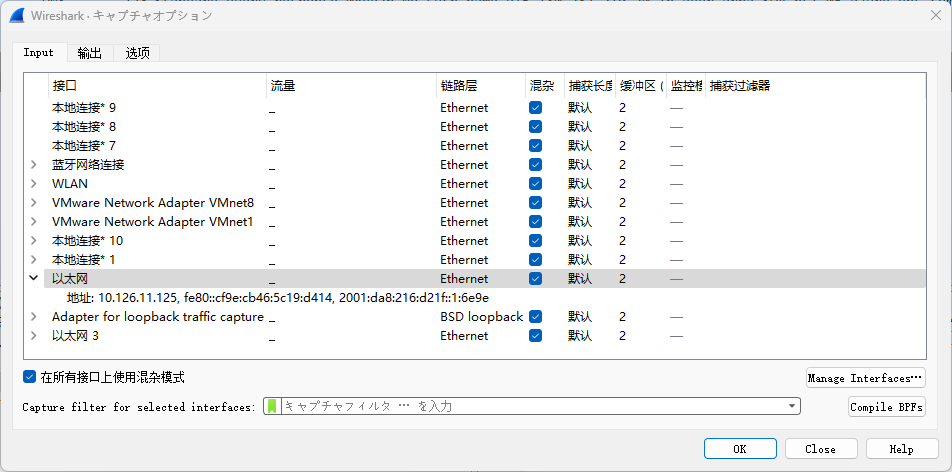
**日期：**

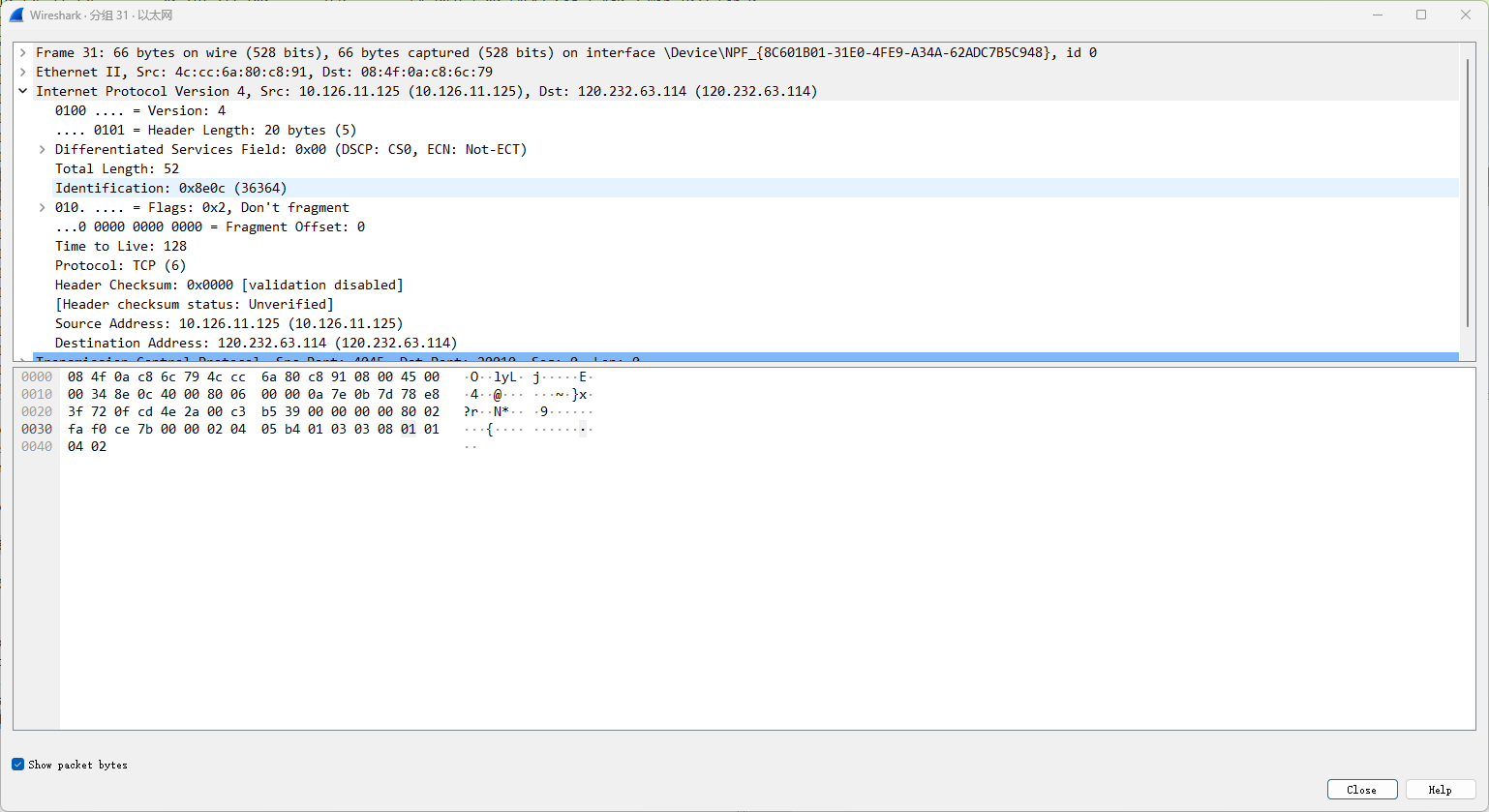
1. 实验目的与任务
2. 学习并熟练运用网络分析软件Wireshark，包括其设置和使用技巧。
3. 利用Wireshark进行网络数据包的捕获，并对捕获到的数据包结构进行深入分析。
4. 理解并掌握TCP（传输控制协议）模型，通过Wireshark观察并理解TCP的三次握手过程及其标准流程。
5. 掌握ARP（地址解析协议）的工作原理，通过Wireshark分析ARP请求和响应的交互过程。
6. 实验基本原理



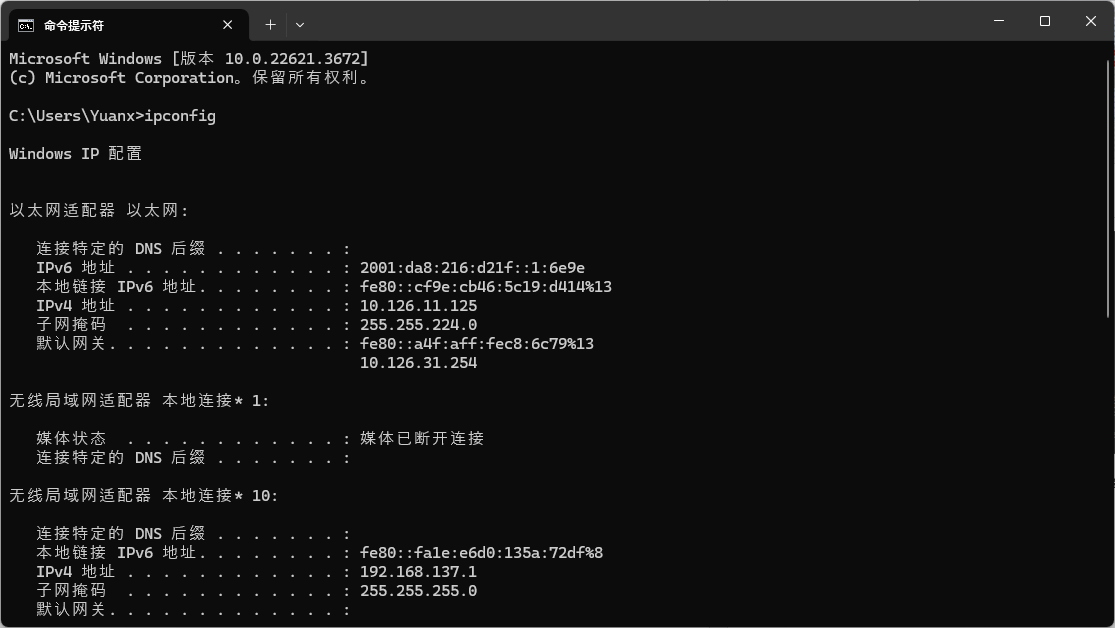
TCP协议模型

1. 实验步骤
2. 使用Wireshark进行抓包（使用有线网连接）

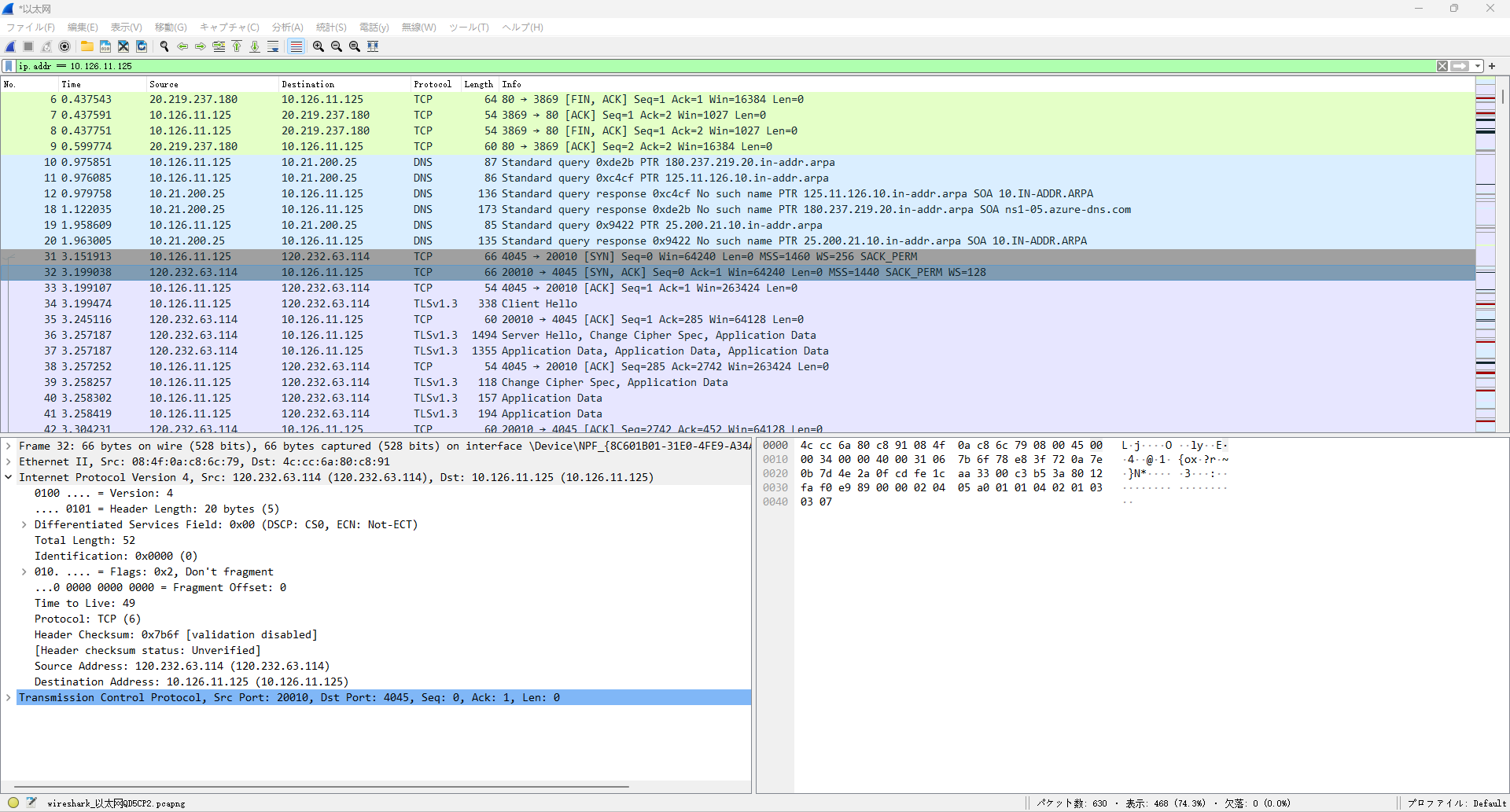




1. IP筛选



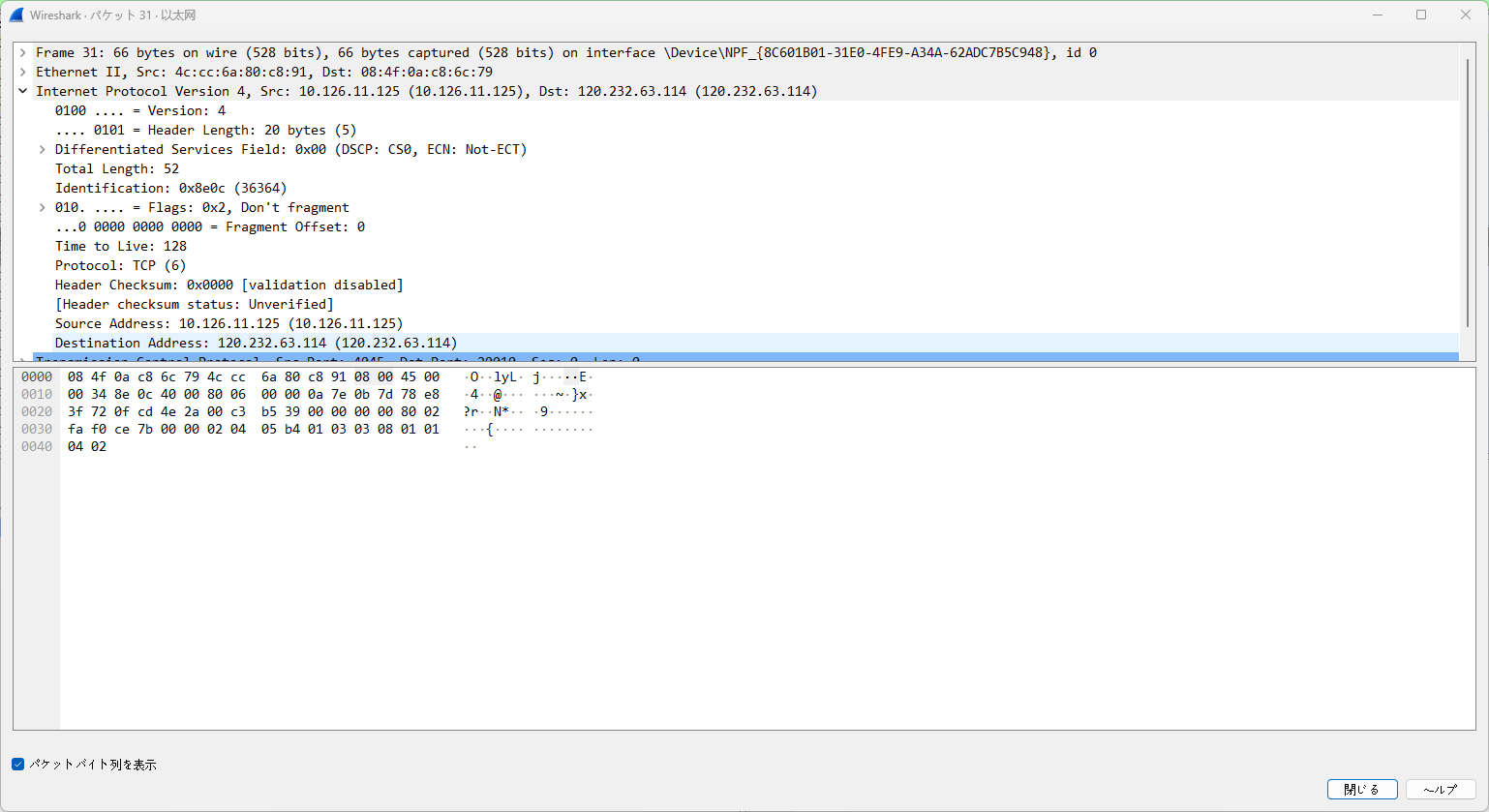
可以看到IPv4地址为10.126.11.125，并以此IP地址作为筛查



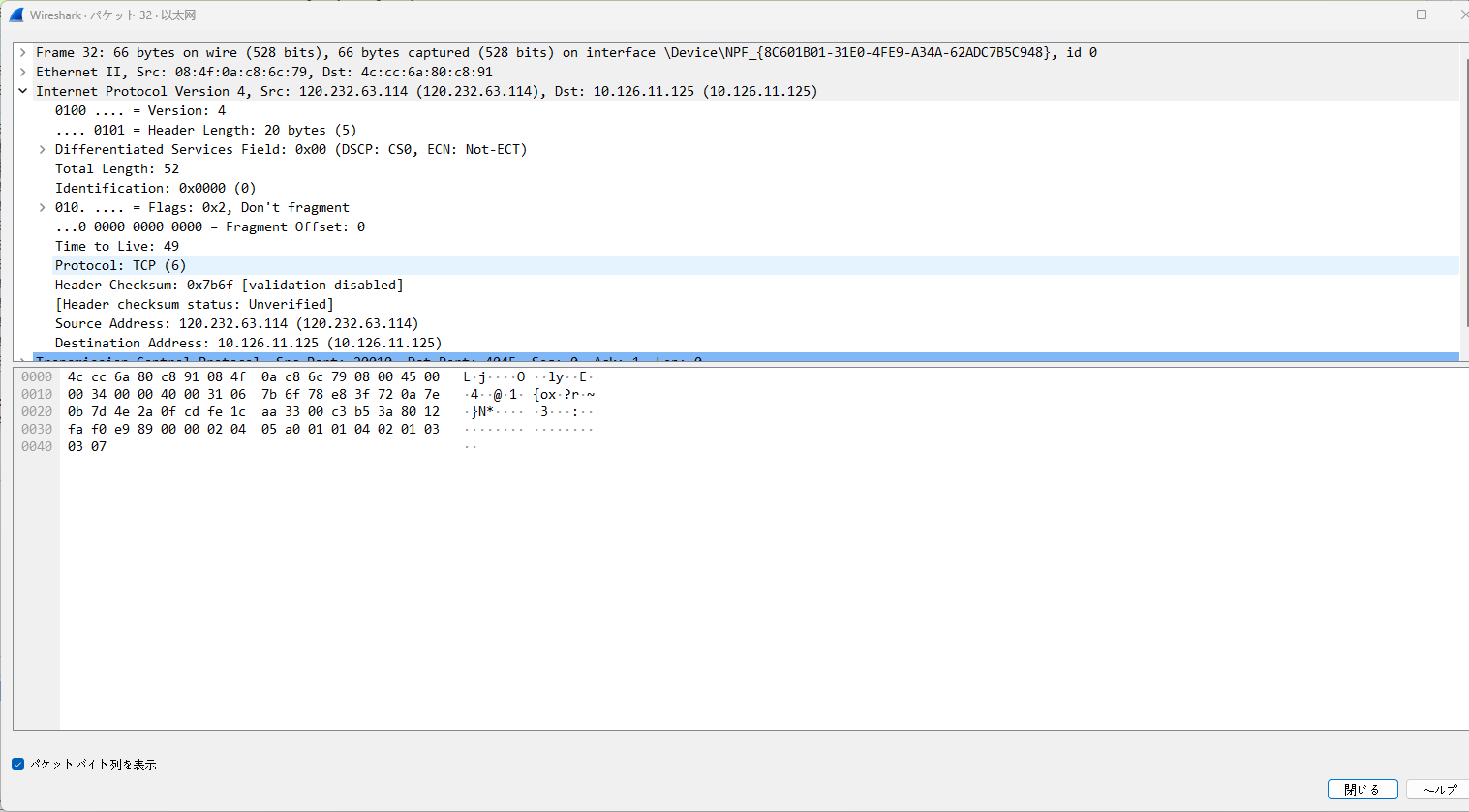
1. 分析IP协议的两次握手

第一次握手：

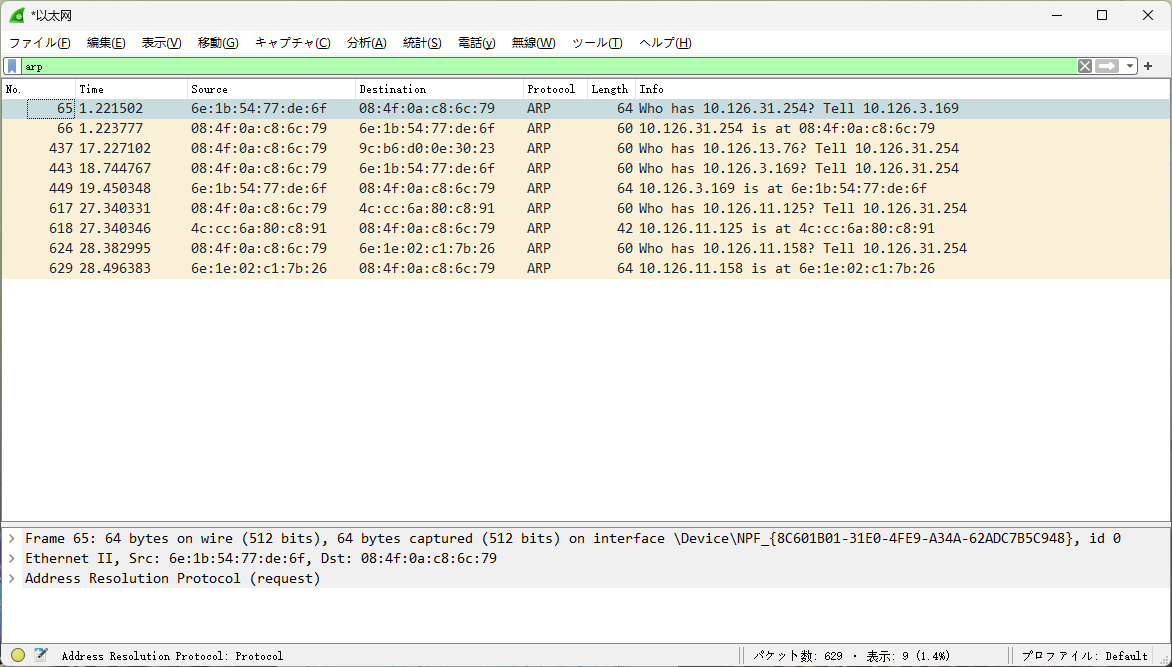
由10.126.11.125向120.232.63.114发送建立连接请求，标志位为[SYN]，随机产生序列号，SeqNum=0。



第二次握手：由120.232.63.114向10.126.11.125发送应答，标志位为[SYN][ACK]，AckNum=SeqNum+1=1。



1. 分析ARP请求和ARP回应



在进行网址访问抓包的过程中，仅捕获到了ARP请求报文，而没有观察到ARP响应报文。图片中所显示的ARP请求和ARP响应是在抓包过程中暂时断开WiFi连接并重新连接后所产生的。

1. 实验结论

**第一次握手**：Client进入SYN\_SENT状态，发送一个SYN帧来主动打开传输通道。该帧的SYN标志位被设置为1，同时会带上Client分配好的SN序列号。该SN是根据时间产生的一个随机值，通常每隔4ms加1。除此之外，SYN帧还会带一个MSS（最大报文段长度）可选项的值，表示客户端发送的最大数据块长度。

**第二次握手**：Server在收到SYN帧之后，进入SYN\_RCVD状态，同时返回SYN+ACK帧给Client。主要目的是通知Client，Server已收到SYN消息，需要进行确认。Server发出的SYN+ACK帧的ACK标志位被设置为1，其确认序号AN（Acknowledgment Number）值被设置为Client的SN+1；SYN+ACK帧的SYN标志位被设置为1，SN值为Server生成的SN序列号；SYN+ACK帧的MSS表示的是Server的最大数据块长度。

**第三次握手**：Client在收到Server的SYN+ACK确认帧后，状态从SYN\_SENT变为ESTABLISHED，表示客户端方向的连接通道已成功建立，Client可以发送数据给Server。然后，Client发送ACK帧给Server，该ACK帧的ACK标志位被设置为1，其确认序号AN值被设置为Server的SN序列号+1。还有一种情况，Client可能将ACK帧和第一帧要发送的数据合并一起发送给Server。

Server在收到Client的ACK帧后，状态从SYN\_RCVD变为ESTABLISHED，至此，服务器方向的通道连接建立成功，Server可以发送数据给Client，TCP的全双工连接建立完成。

ARP 请求包

Sender MAC 地址: 08:4f:0a:c8:6c:79

Sender IP 地址: 10.126.31.254

Target MAC 地址: 00:00:00:00:00:00 (表示未知)

Target IP 地址: 10.126.13.76

ARP 回复包

Sender MAC 地址: 9c:b6:d0:0e:30:23

Sender IP 地址: 10.126.13.76

Target MAC 地址: 08:4f:0a:c8:6c:79

Target IP 地址: 10.126.31.254

解释：

在校园网络中，新华三设备（如交换机或路由器）会发送ARP请求广播包，询问某个IP地址（如10.126.13.76）对应的MAC地址。当主机收到该广播包后，如果其IP地址匹配，则会发送ARP回复包，告知其MAC地址。

从图像中可以看到一系列ARP请求包，示例如下：

08:4f:0a:c8:6c:79 向 ff:ff:ff:ff:ff

发送ARP请求，询问10.126.13.76的MAC地址。

08:4f:0a:c8:6c:79 不断发送类似的请求，分别询问不同IP地址的MAC地址。

总的来说，这些ARP请求主要用于网络设备发现其他设备的MAC地址，以便进行通信。