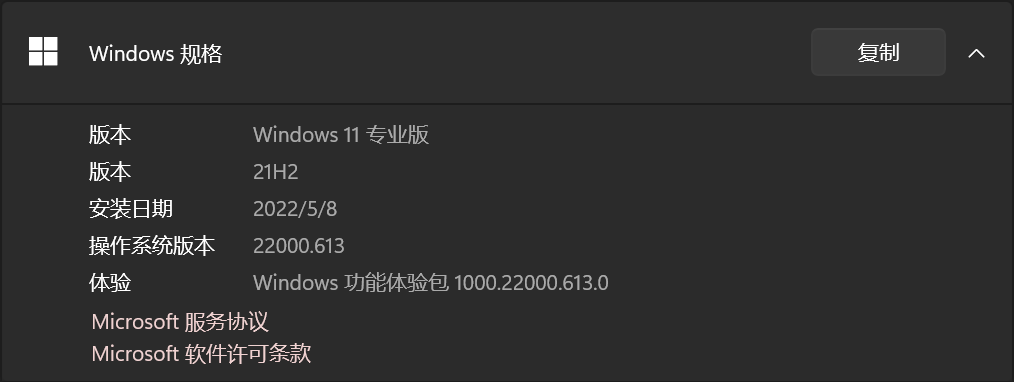
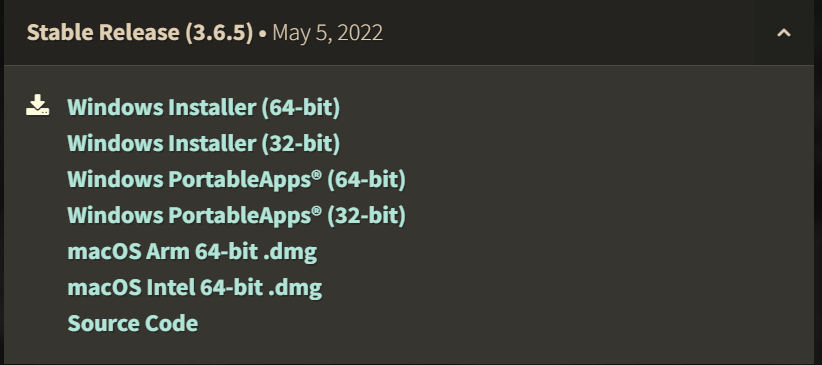
1. 实验目的

-熟悉使用sinffer类软件

-分析网络的层次结构

1. 实验环境

Windows11

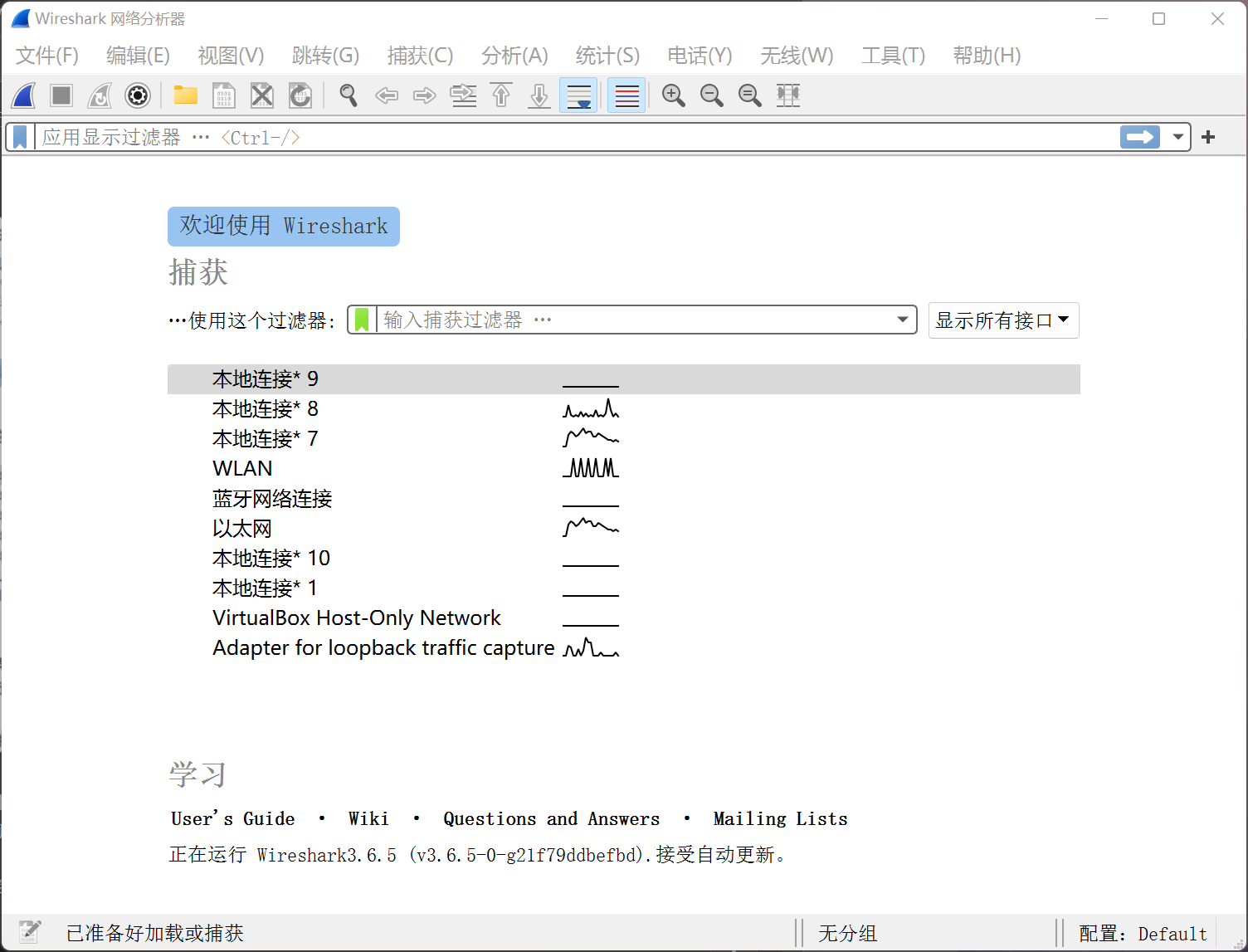
Wireshark

1. 实验截图

实施抓包

安装好 Wireshark 以后，就可以运行它来捕获数据包了。方法如下：

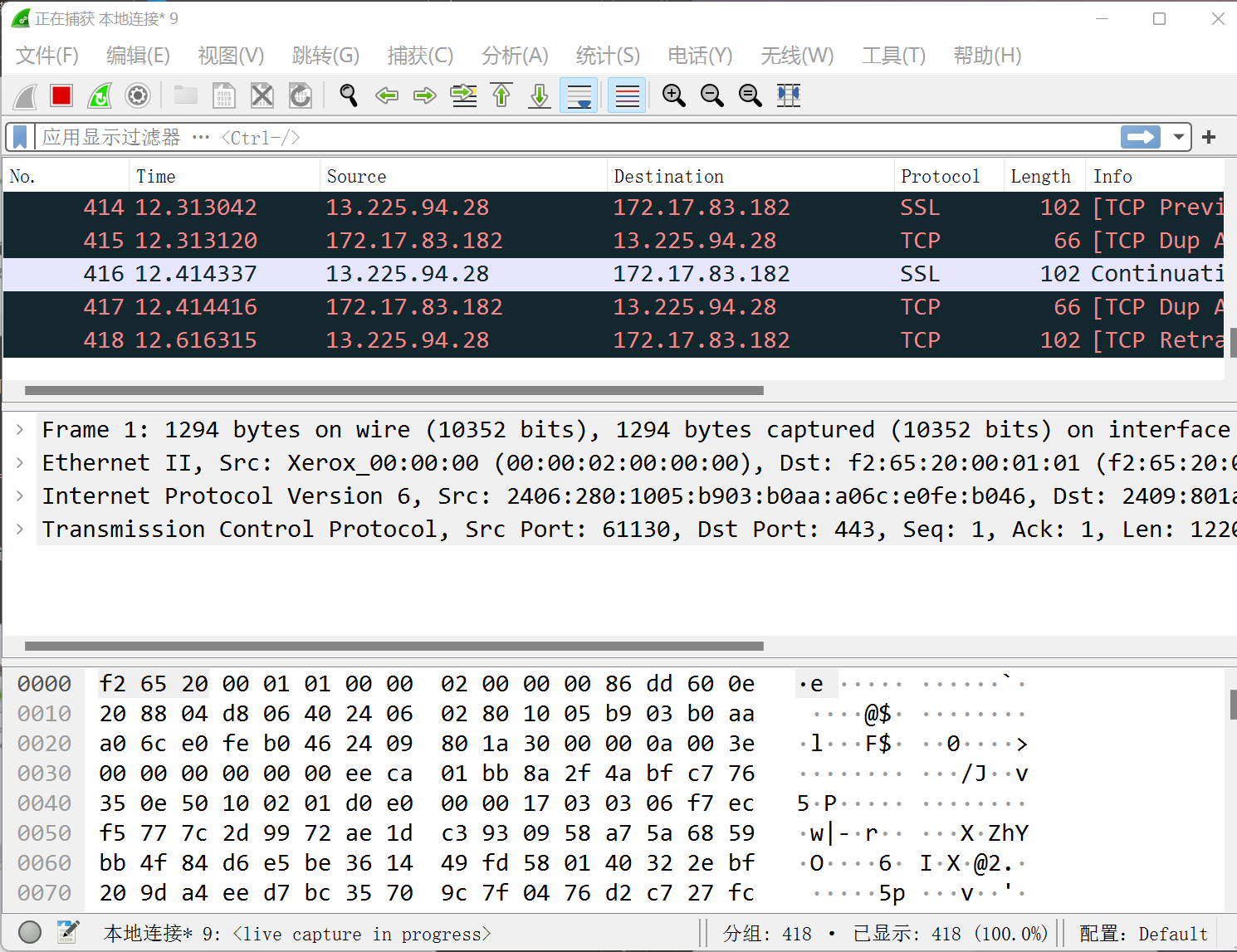
1) 在 Windows 的“开始”菜单中，单击 Wireshark 菜单，启动 Wireshark，如图所示。



该图为 Wireshark 的主界面，界面中显示了当前可使用的接口。要想捕获数据包，必须选择一个接口，表示捕获该接口上的数据包。

在上图中，选择捕获“本地连接”接口上的数据包。选择“本地连接”选项，然后单击左上角的“开始捕获分组”按钮，将进行捕获网络数据，如下如所示。

图中没有任何信息，表示没有捕获到任何数据包。这是因为目前“本地连接”上没有任何数据。只有在本地计算机上进行一些操作后才会产生一些数据，如浏览网站。

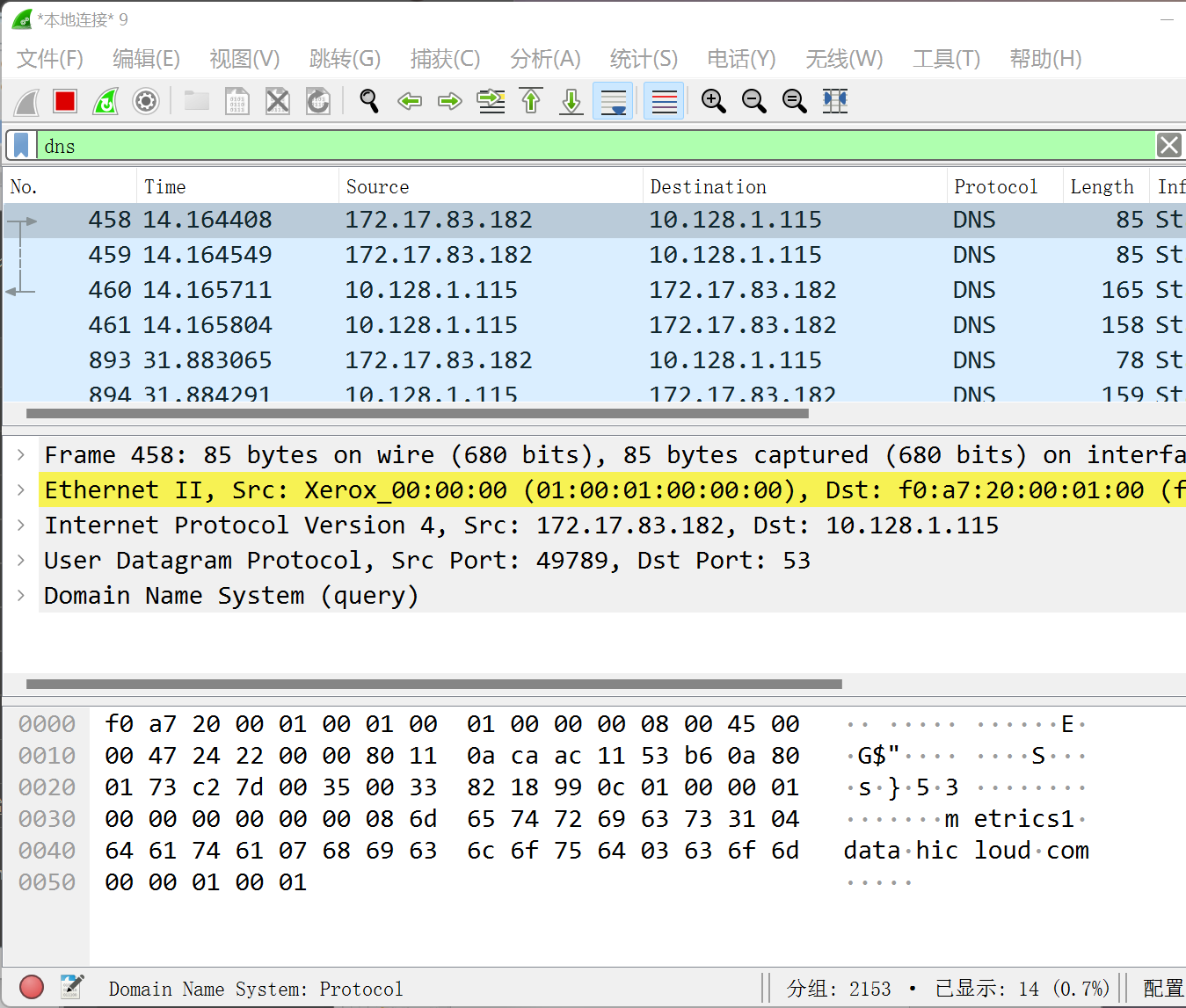


使用显示过滤器

默认情况下，Wireshark 会捕获指定接口上的所有数据，并全部显示，这样会导致在分析这些数据包时，很难找到想要分析的那部分数据包。这时可以借助显示过滤器快速查找数据包。

显示过滤器是基于协议、应用程序、字段名或特有值的过滤器，可以帮助用户在众多的数据包中快速地查找数据包，可以大大减少查找数据包时所需的时间。

使用显示过滤器，需要在 Wireshark 的数据包界面中输入显示过滤器并执行，如图所示。



例如，要从捕获到的所有数据包中，过滤出 DNS 协议的数据包，这里使用 dns 显示过滤器，过滤结果如图所示。图中显示的所有数据包的协议都是 DNS 协议。

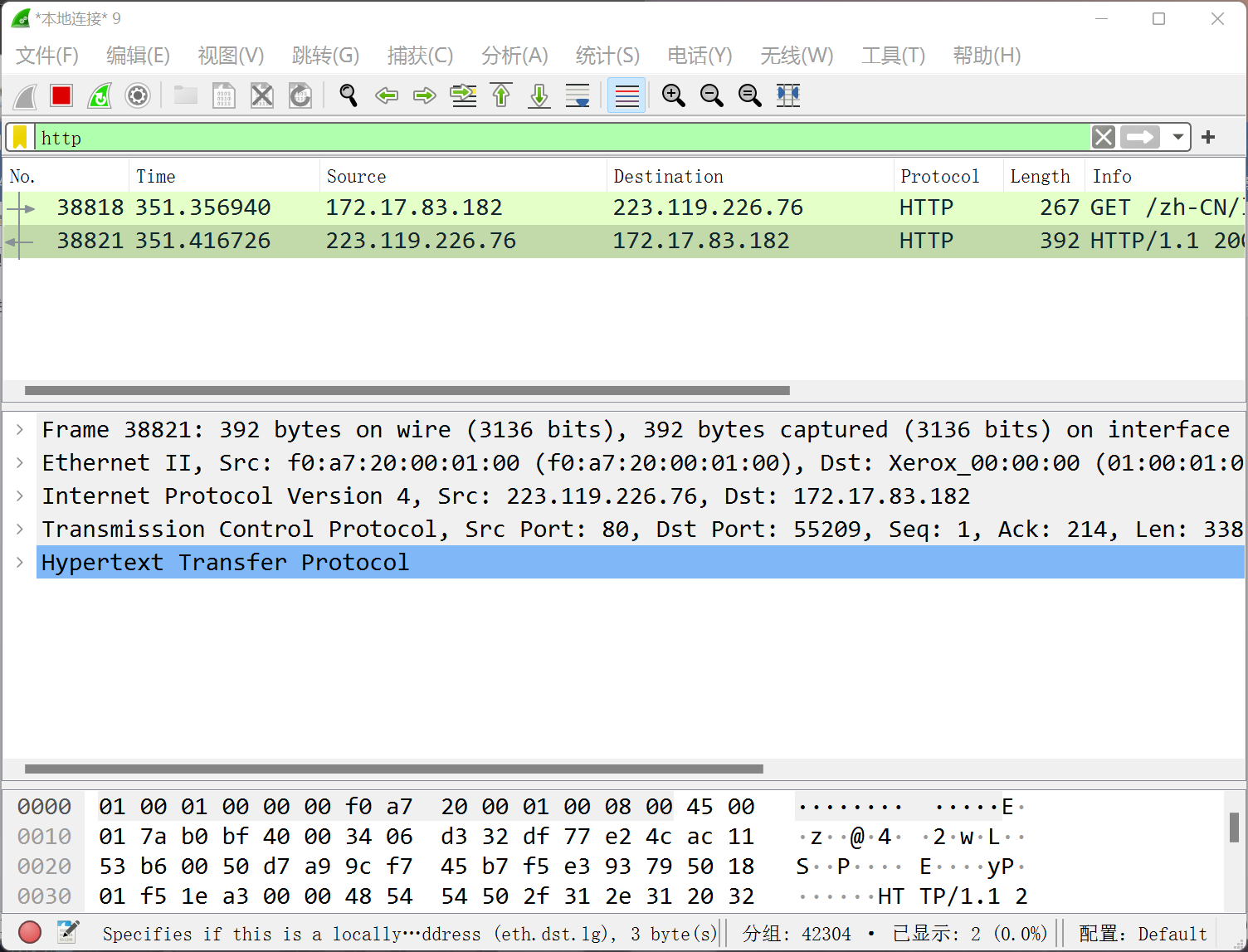
例如，要从捕获到的所有数据包中，过滤出 DNS 协议的数据包，这里使用 dns 显示过滤器，过滤结果如图所示。图中显示的所有数据包的协议都是 DNS 协议。

上图中所显示的信息从上到下分布在 3 个面板中，每个面板包含的信息含义如下：

Packet List 面板：上面部分，显示 Wireshark 捕获到的所有数据包，这些数据包从 1 进行顺序编号。

Packet Details 面板：中间部分，显示一个数据包的详细内容信息，并且以层次结构进行显示。这些层次结构默认是折叠起来的，用户可以展开查看详细的内容信息。

Packet Bytes 面板：下面部分，显示一个数据包未经处理的原始样子，数据是以十六进制和 ASCII 格式进行显示。



2) 以 HTTP 协议数据包为例，了解该数据包的层次结构。在 Packet List 面板中找到一个 HTTP 协议数据包，如图所示。

其中，编号 21 的数据包是一个 HTTP 协议数据包。此时在 Packet Details 面板上显示的信息就是该数据包的层次结构信息。

这里显示了 5 个层次，每个层次的含义如下：

Frame：该数据包物理层的数据帧概况。

Ethernet II：数据链路层以太网帧头部信息。

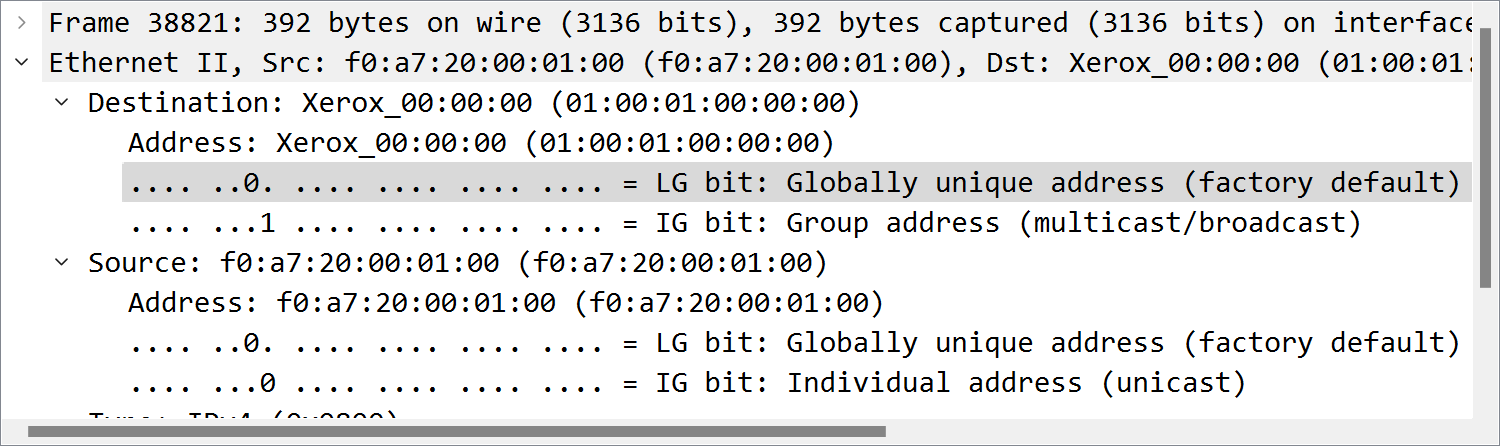
Internet Protocol Version 4：网际层 IP 包头部信息。

Transmission Control Protocol：传输层的数据段头部信息。

Hypertext Transfer Protocol：应用层的信息，此处是 HTTP 协议。

由此可见，Wireshark 对 HTTP 协议数据包进行解析，显示了 HTTP 协议的层次结构。

3) 用户对数据包分析就是为了查看包的信息，展开每一层，可以查看对应的信息。例如，查看数据链路层信息，展开 Ethernet II 层，显示信息如下：

显示的信息包括了该数据包的发送者和接收者的 MAC 地址（物理地址）。

可以以类似的方法分析其他数据包的层次结构。

1. 实验心得

关于抓包我们平时使用的最多的可能就是Chrome浏览器自带的Network面板了（浏览器上F12就会弹出来）。另外还有一大部分人使用Fiddler，Fiddler也是一款非常优秀的抓包工具。但是这两者只能对于HTTP和HTTPS进行抓包分析。wireshark是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。Wireshark不仅可以对我们常见的HTTP、HTTPS、TCP等协议进行抓包分析，还能对工业上的BACnet、ModBus、S7Communication和其他PLC协议进行报文抓包分析。