**实验3： 抓包**

**一、实验目的**

通过实验，了解和掌握报⽂捕获⼯具 Wireshark 的使⽤⽅法和基本特点，使 ⽤ Wireshark 捕获⽹络报⽂，并分析各种⽹络协议的报⽂格式和⼯作过程。

**二、实验内容**

安装Wireshark，并会基本的使用；

使⽤ Wireshark 捕获⽹络报⽂，以DNS为例分析其报⽂格式和⼯作过程。三、实验原理、方法和手段

**3.1 什么是DNS**

DNS是⼀种⽤于internet上提供IP地址和域名相互映射的分布式服务系统。可以通过IP地址获取相应的域名，也可以通过域名获取IP， 这样可以不⽤记住难记的IP。

我们实际⽹络中的DNS服务是由⽹络运营商提供的。⼤多数地区都有相应的域名服务器。114.114.114.114是⼀个公共的DNS服务器，任何地⽅都可以通过这个服务器获取DNS服务。

域名是通过.来区分不同级的，其中最后⼀级为顶级域名如：com，edu，org等等。域名的分配是通过授权机构来完成的。 cmd中可以通过nslookup查询本地dns服务器IP，linux中⼀般应⽤host可以进⾏域名的解析。

DNS是⼀个应⽤层协议，基于TCP/IP传输，⼀般的DNS报⽂传输层是UDP报⽂。下⾯是DNS报⽂的格式：

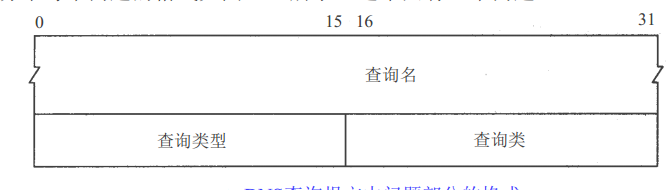


DNS报⽂由12字节长的⾸部和4个长度可变的字段组成。

标识字段：由客户程序设置并由服务器返回结果。客户程序通过它来确定响应与查询是否匹配。（可以视为报⽂ID） 标志字段：定义各种标志位。

问题数、资源记录数、授权资源记录数和额外资源记录数记录下⾯4个字段对应的数⽬。

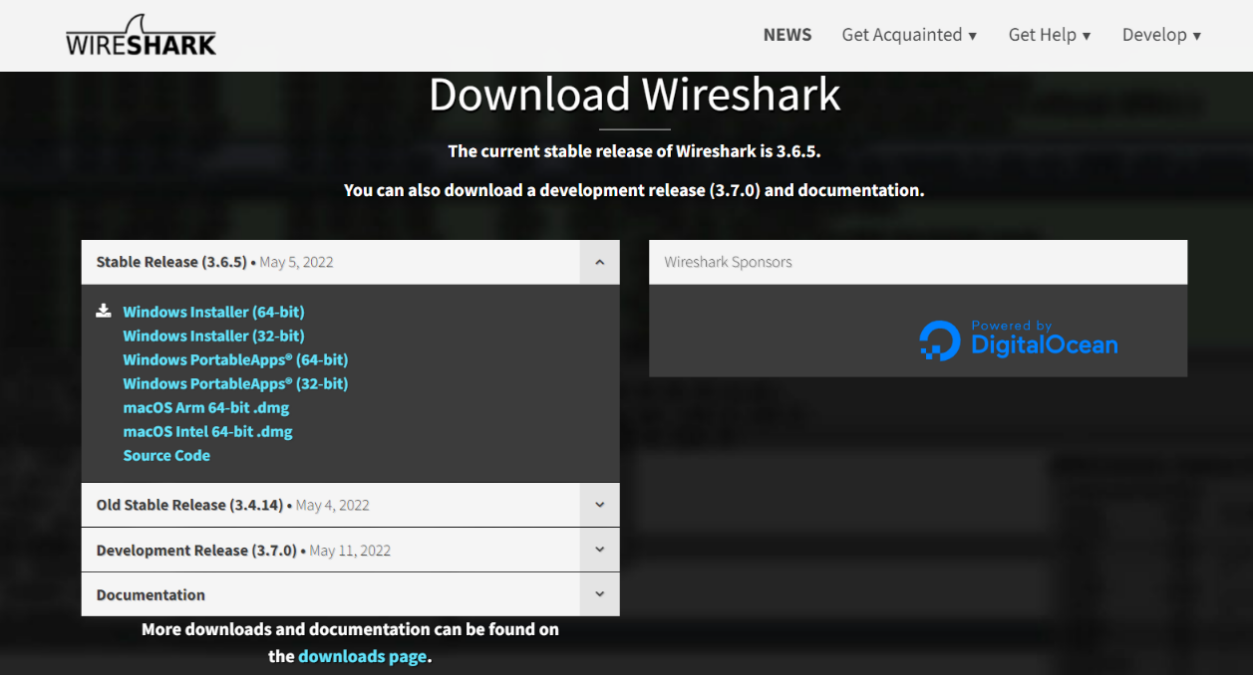
DNS查询报⽂中的问题部分



查询名是要查找的名字（域名），它是⼀个或多个标识符的序列。每个标识符以⾸字节的计数值来说明随后标识符的字节长度，每个名字以 最后字节为0结束，长度为0的标识符是根标识符。实际的存储结构由下图所⽰：

**3.2 Wireshark安装**

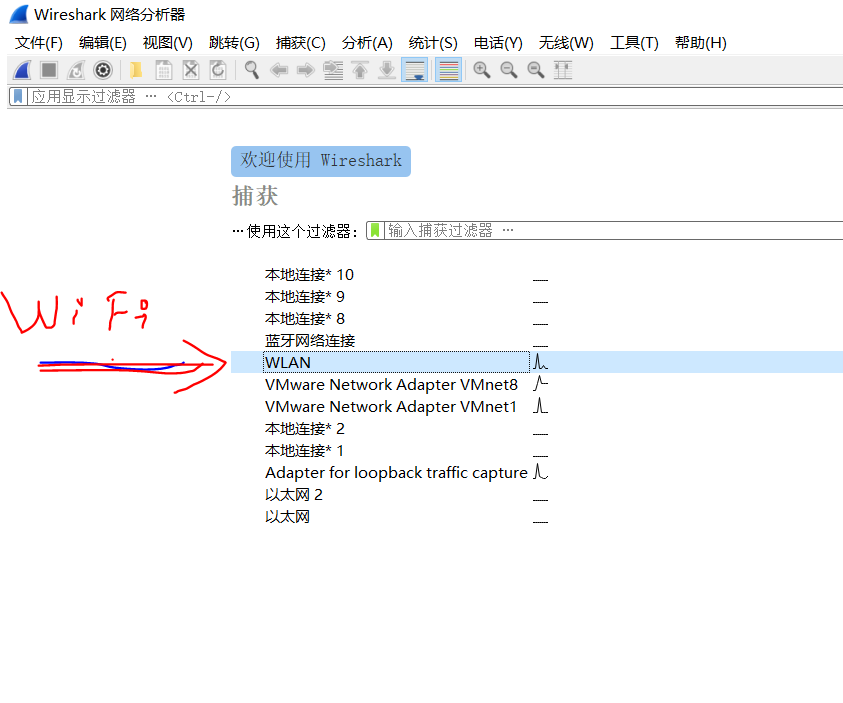
官方网站是<https://www.wireshark.org/>，免费开源。请选对你的操作系统，下载适合的版本并安装。



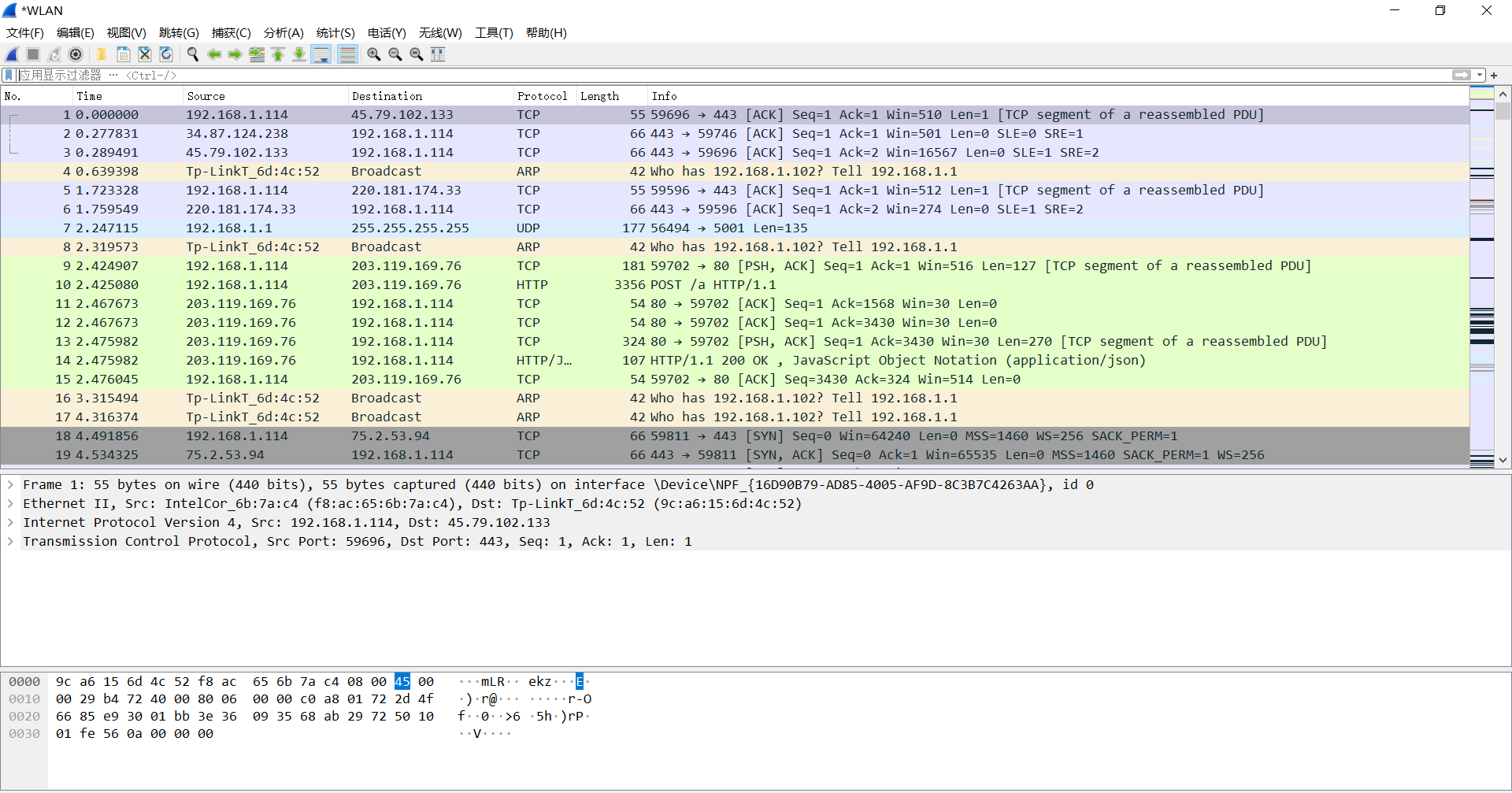
**3.3 使用Wireshark获取DNS数据**

（1）打开Wireshark

打开软件，并选择你的网卡（正在上网那块网卡，wifi还是其它网卡得看你实际情况）。以我为例，我这会儿用无线上网，所以如下图选择WLAN。



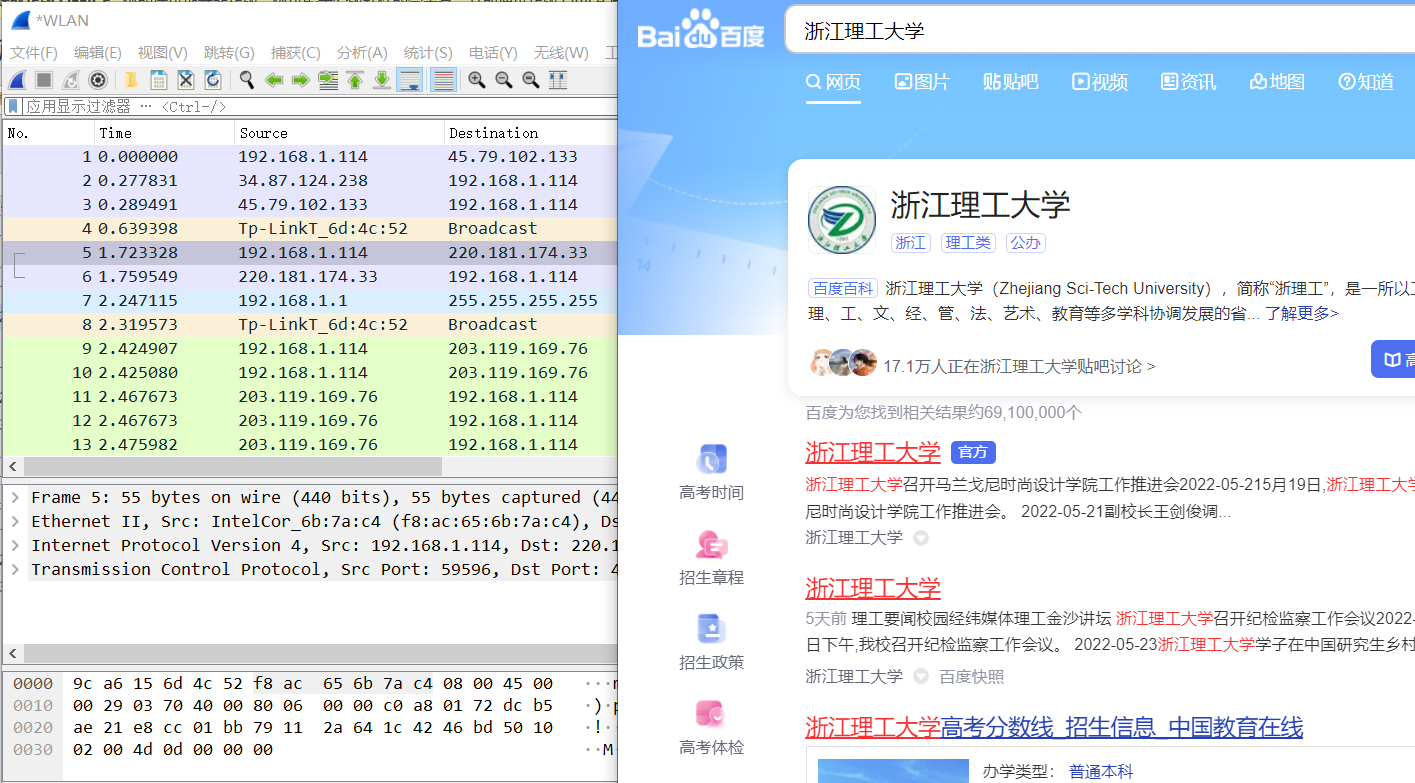
选择网卡后，可以看到软件在源源不断的监听网卡，抓取数据包：



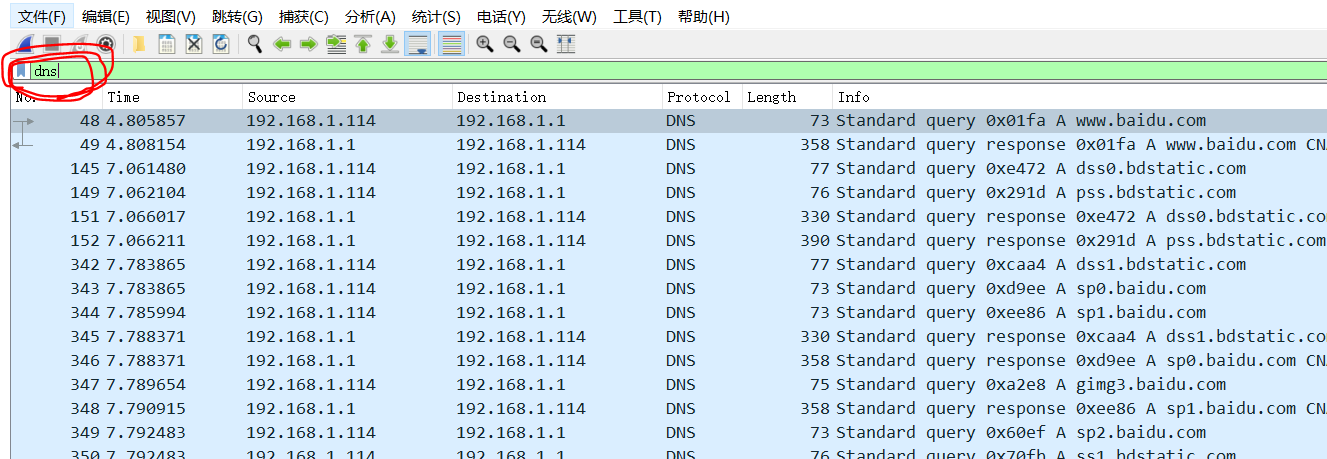
其中，左上角“鲨鱼鳍”表示开始抓包，“█”表示暂停抓包，请配合使用。

（2）抓取dns数据

确认现在处在抓包状态。打开浏览器，在浏览器里随便用baidu搜点什么，如下图。



然后Wireshark里，点击“█”暂停抓包，并搜索“dns”。这时候罗列的信令就是刚才baidu搜索过程中的dns请求。



Wen

**四、实验内容**

**4.1 安装Wireshark，并抓包**

**4.2 浏览器里几个浙理工校内的页面**

**4.3 抓包dns，并列出包的内容**

**五、实验组织运行要求**

单人实验，单独完成。

**六、实验条件**

（1）计算机（win、linux、osx不限）

（2）Wireshark，官网下载。

**七、实验结果**

**7.1 截图你的搜索网站，并标注下DNS协议的字段内容，获得90%的分数**

|  |
| --- |
| 图片1 |

**7.2 扩展题**

|  |
| --- |
|  |