**【实验名称】：**DNS实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-12-18

**【实验目的】**

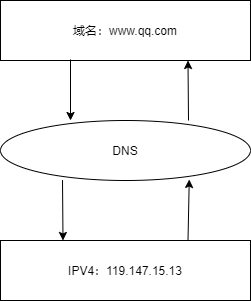
了解DNS的原理，学会通过软件工具抓取DNS包并进行解读与分析，在了解抓取DNS包的方法的同时，掌握分析DNS包内容的方法。

**【实验原理】**

1.DNS的概述

为什么需要DNS解析域名为IP地址？网络通讯大部分是基于TCP/IP的，而TCP/IP是基于IP地址的，所以计算机在网络上进行通讯时只能识别如“202.96.134.133”之类的IP地址，而不能认识域名。我们无法记住10个以上IP地址的网站，所以我们访问网站时，更多的是在浏览器地址栏中输入域名，就能看到所需要的页面，这是因为有一个叫“DNS服务器”的计算机自动把我们的域名“翻译”成了相应的IP地址，然后调出IP地址所对应的网页。

具体什么是DNS？DNS( Domain Name System)是“域名系统”的英文缩写，是一种组织成域层次结构的计算机和网络服务命名系统，它用于TCP/IP网络，它所提供的服务是用来将主机名和域名转换为IP地址的工作。DNS就是这样的一位“翻译官”，它的基本工作原理可用下图来表示：



2.DNS的过程

DNS是应用层协议，事实上他是为其他应用层协议工作的，包括不限于HTTP和SMTP以及FTP，用于将用户提供的主机名解析为ip地址。具体过程如下：

①用户主机上运行着DNS的客户端，就是我们的PC机或者手机客户端运行着DNS客户端。

②浏览器将接收到的url中抽取出域名字段，就是访问的主机名，比如http://www.baidu.com/, 并将这个主机名传送给DNS应用的客户端。

③DNS客户机端向DNS服务器端发送一份查询报文，报文中包含着要访问的主机名字段（中间包括一些列缓存查询以及分布式DNS集群的工作）。

④该DNS客户机最终会收到一份回答报文，其中包含有该主机名对应的IP地址。

⑤一旦该浏览器收到来自DNS的IP地址，就可以向该IP地址定位的HTTP服务器发起TCP连接。

3.DNS服务的体系架构

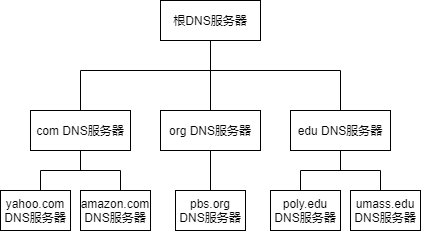
DNS domain name system 主要作用就是将主机域名转换为ip地址。假设运行在用户主机上的某些应用程序（如Web浏览器或者邮件阅读器）需要将主机名转换为IP地址。这些应用程序将调用DNS的客户机端，并指明需要被转换的主机名。（在很多基于UNIX的机器上，应用程序为了执行这种转换需要调用函数

gethostbyname()）。用户主机的DNS客户端接收到后，向网络中发送一个DNS查询报文。所有DNS请求和回答报文使用的UDP数据报经过端口53发送。

经过若干ms到若干s的延时后，用户主机上的DNS客户端接收到一个提供所希望映射的DNS回答报文。这个查询结果则被传递到调用DNS的应用程序。因此，从用户主机上调用应用程序的角度看，DNS是一个提供简单、直接的转换服务的黑盒子。但事实上，实现这个服务的黑盒子非常复杂，它由分布于全球的大量DNS服务器以及定义了DNS服务器与查询主机通信方式的应用层协议组成。

4.DNS分布式集群工作方式

DNS的一种简单的设计模式就是在因特网上只使用一个DNS服务器，该服务器包含所有的映射，在这种集中式的设计中，客户机直接将所有查询请求发往单一的DNS服务器，同时该DNS服务器直接对所有查询客户机做出响应，尽管这种设计方式非常诱人，但他不适用当前的互联网，因为当今的因特网有着数量巨大并且在持续增长的主机，这种集中式设计会有单点故障（故障一个，全球着急）。



5.DNS域名称

域名系统作为一个层次结构和分布式数据库，包含各种类型的数据，包括主机名和域名。DNS数据库中的名称形成一个分层树状结构称为域命名空间。域名包含单个标签分隔点，例如：im.qq.com完全限定的域名 (FQDN) 唯一地标识在 DNS 分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。

DNS域名称空间的组织方式：按其功能命名空间中用来描述 DNS 域名称的五个类别的介绍详见下表中，以及与每个名称类型的示例。

|  |  |  |
| --- | --- | --- |
| 名称类型 | 说明 | 示例 |
| 根域 | DNS域名中使用时，规定由尾部句点(.)来指定名称位于根或更高级别的域层次结构 | 单个句点(.)或句点用于末尾的名称。 |
| 顶级域 | 用来指示某个国家/地区或组织使用的名称的类型名称 | .com |
| 第二层域 | 个人或组织在Internet上使用的注册名称 | qq.com |
| 子域 | 已注册的二级域名派生的域名，通俗的讲就是网站名 | www.qq.com |
| 主机名 | 通常情况下，DNS域名的最左侧的标签 | h1.www.qq.com |

互联网域名系统由名称注册机构负责维护分配由组织和国家/地区的顶级域在Internet上进行管理。这些域名有很多缩写，两个字母和三个字母的国家/地区使用的缩写使用下表所示。一些常见的DNS域名称如下表：

|  |  |
| --- | --- |
| DNS域名称 | 组织类型 |
| com | 商业公司 |
| edu | 教育机构 |
| net | 网络公司 |
| gov | 非军事政府机构 |
| Mil | 军事政府机构 |
| xx | 国家/地区代码(cn表中国) |
| …. | …. |

6.DNS域名解析顺序

1）浏览器缓存：当用户通过浏览器访问某域名时，浏览器首先会在自己的缓存中查找是否有该域名对应的IP地址（若曾经访问过该域名且没有清空缓存便存在）；

2）系统缓存：当浏览器缓存中无域名对应IP则会自动检查用户计算机系统Hosts文件DNS缓存是否有该域名对应IP；

3）路由器缓存：当浏览器及系统缓存中均无域名对应IP则进入路由器缓存中检查，以上三步均为客服端的DNS缓存；

4）ISP（互联网服务提供商）DNS缓存：当在用户客服端查找不到域名对应IP地址，则将进入ISP DNS缓存中进行查询。比如你用的是电信的网络，则会进入电信的DNS缓存服务器中进行查找；

5）根域名服务器：当以上均未完成，则进入根服务器进行查询。全球仅有13台根域名服务器，1个主根域名服务器，其余12为辅根域名服务器。根域名收到请求后会查看区域文件记录，若无则将其管辖范围内顶级域名（如.com）服务器IP告诉本地DNS服务器；

6）顶级域名服务器：顶级域名服务器收到请求后查看区域文件记录，若无则将其管辖范围内主域名服务器的IP地址告诉本地DNS服务器；

7）主域名服务器：主域名服务器接受到请求后查询自己的缓存，如果没有则进入下一级域名服务器进行查找，并重复该步骤直至找到正确纪录；

8）保存结果至缓存：本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时将该结果反馈给客户端，客户端通过这个IP地址与web服务器建立链接。

**【实验设备】**

HUAWEI MateBook X Pro（安装有Cisco Packet Tracer与Wireshark抓包分析工具）

【**实验步骤**】

1.设置WEB服务器和简单的DNS服务器；

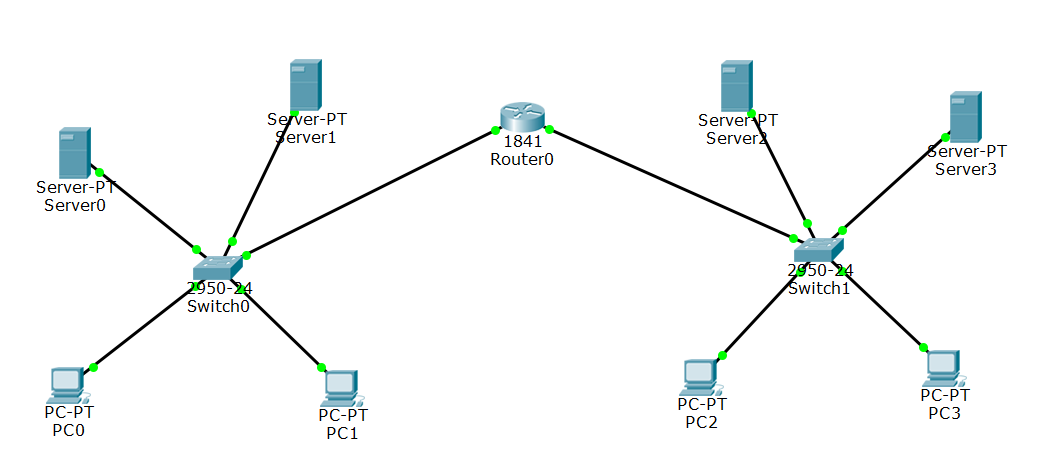
2.打开PC2浏览器，输入配置Web服务器的Web地址，如www.tongji.edu.cn,产生数据报文。

3.打开Wireshark，选择抓取WLAN的数据包，并设置“dns”过滤器；

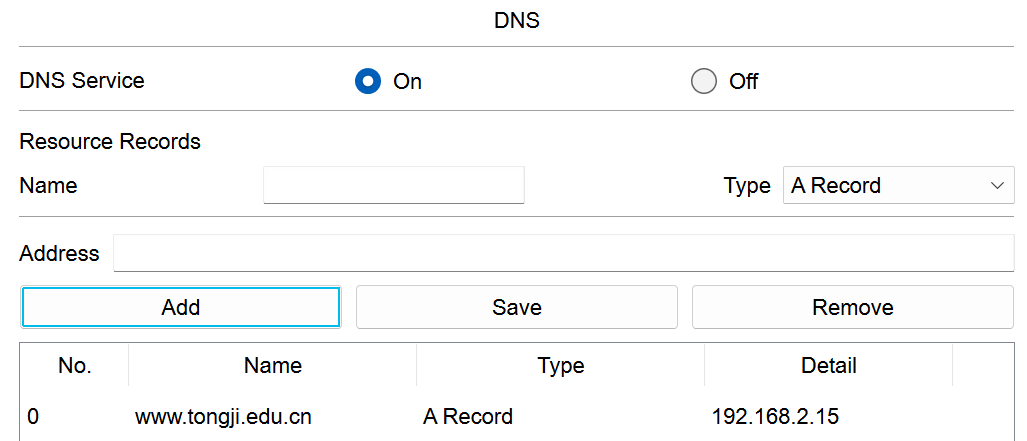
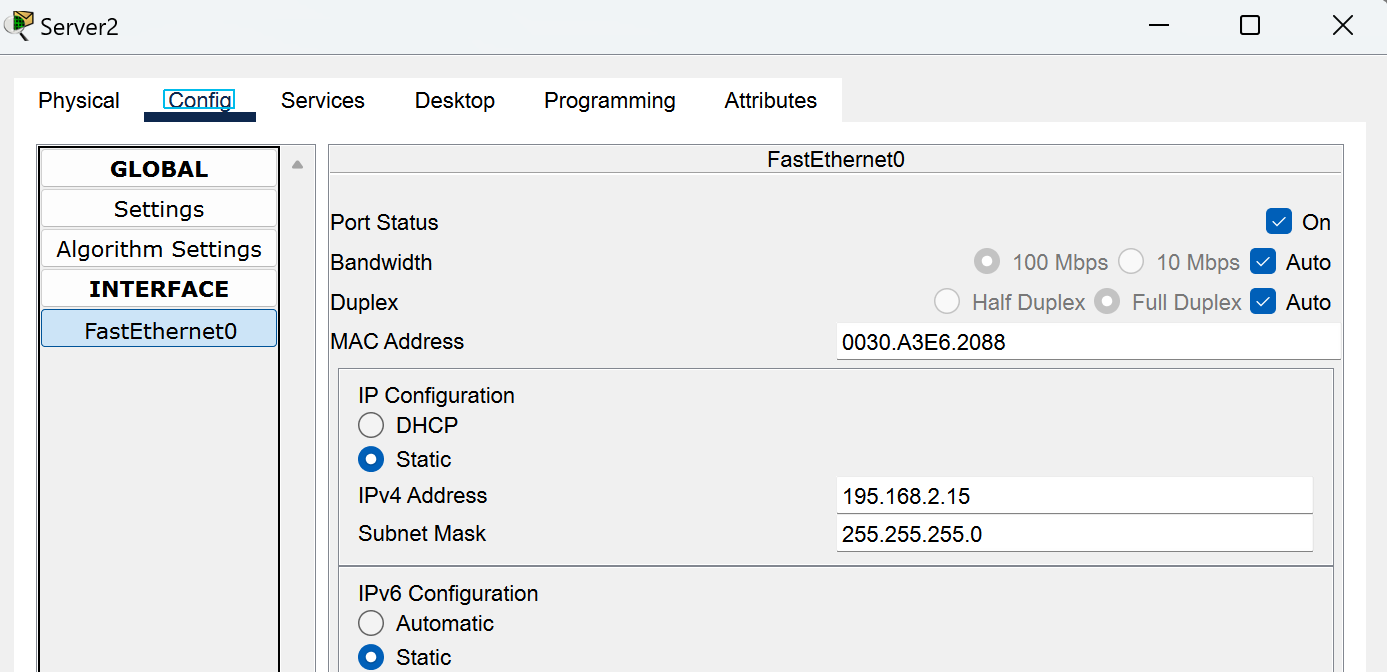
4.分析抓取到的DNS报文。

**【实验现象】**

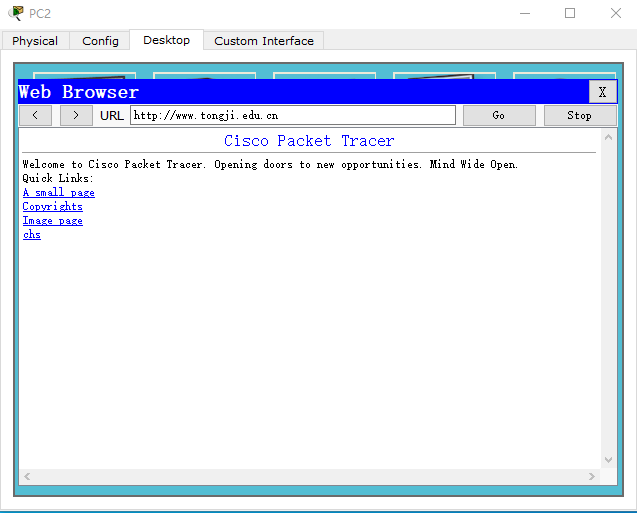
1.设置WEB服务器和简单的DNS服务器。

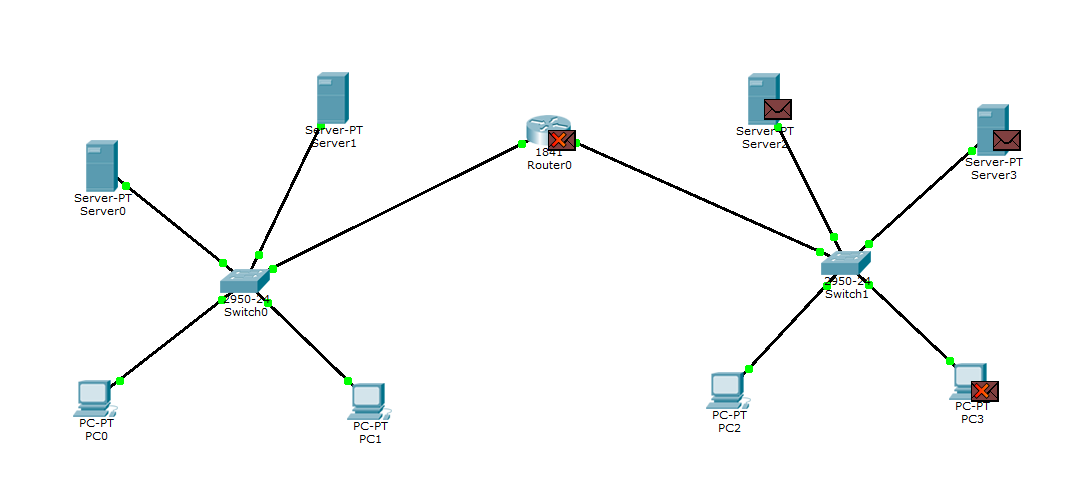


2.将Server2设置为WEB服务器，并在Server3上设置DNS：

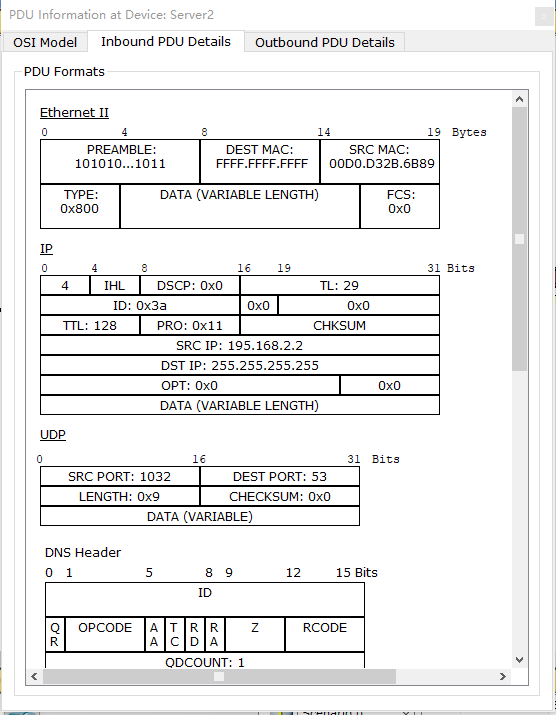
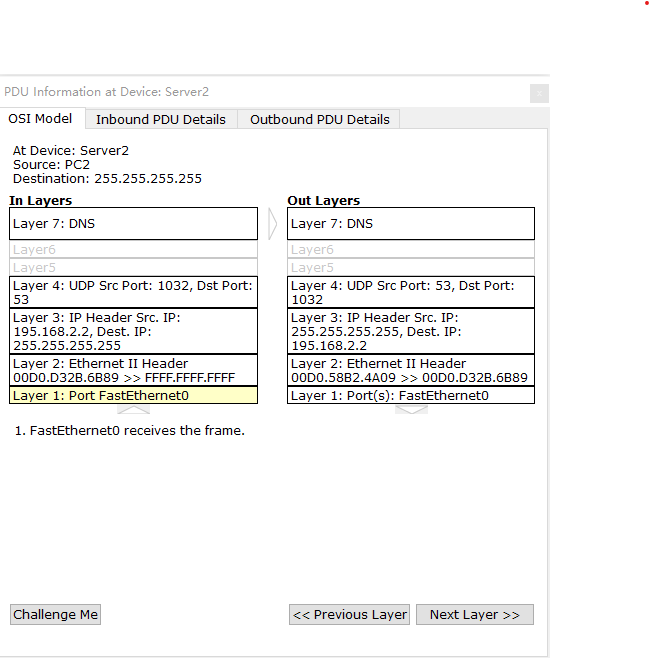


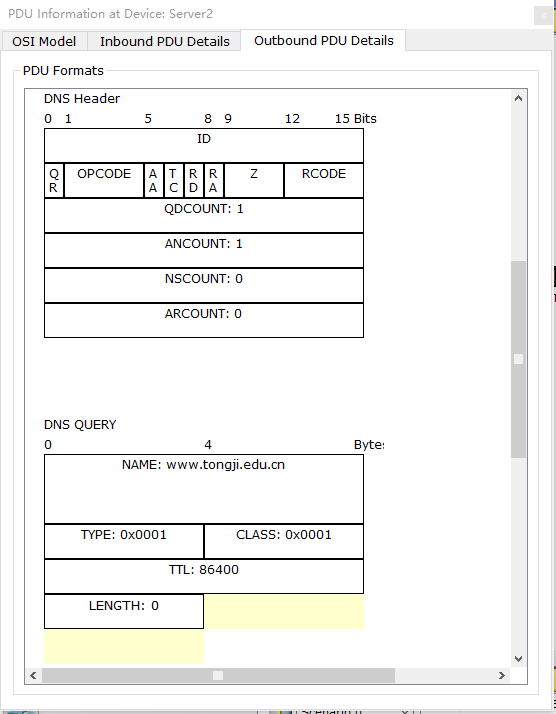
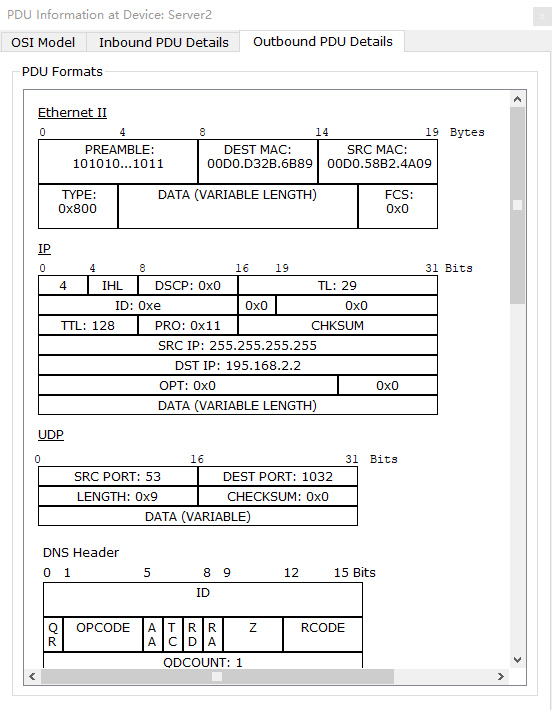
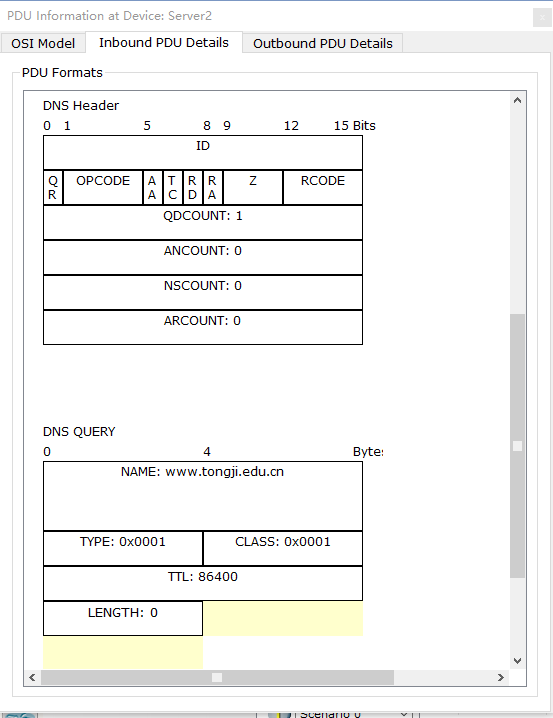
3.打开PC2浏览器，输入配置Web服务器的Web地址www.tongji.edu.cn，产生数据报文：



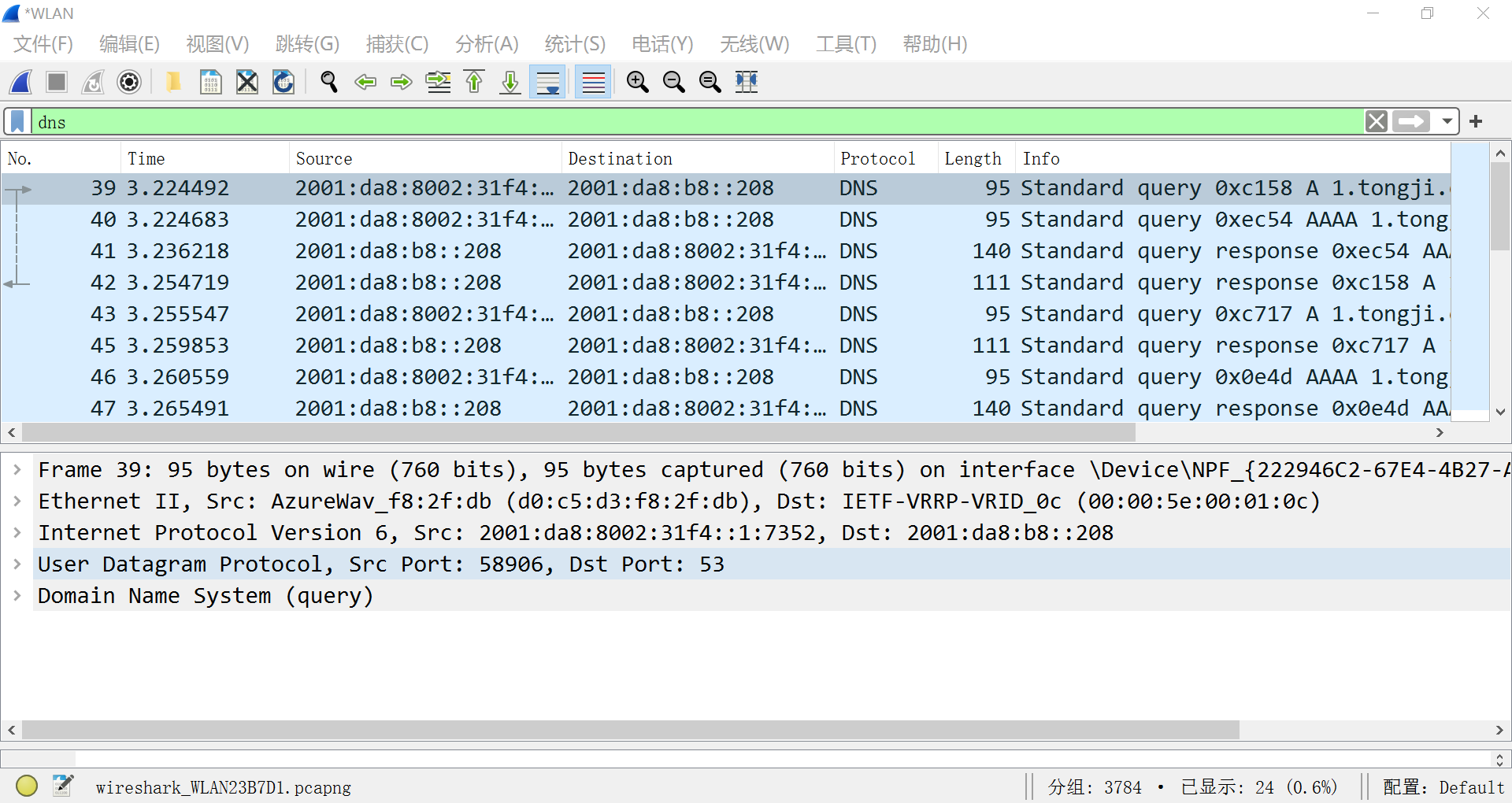


查看DNS数据包内容：





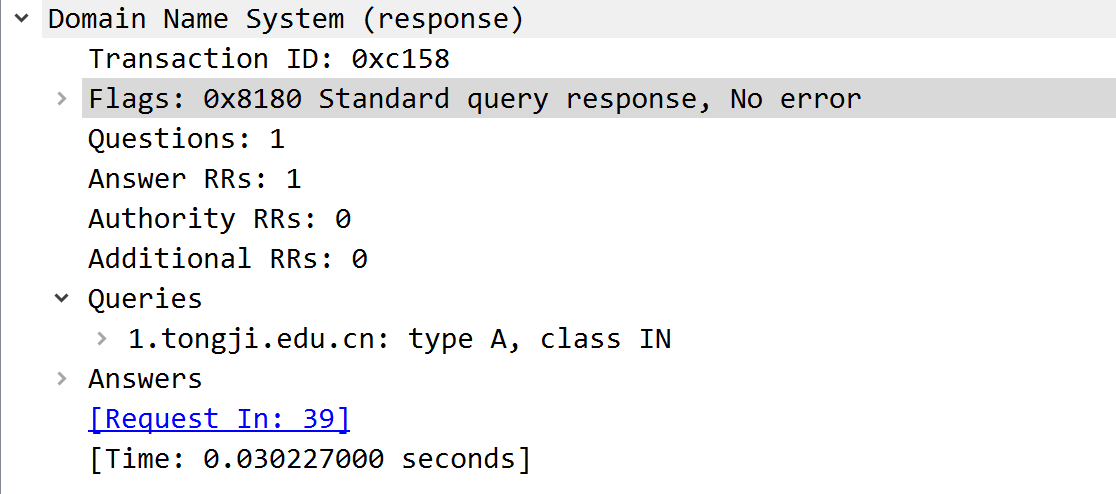
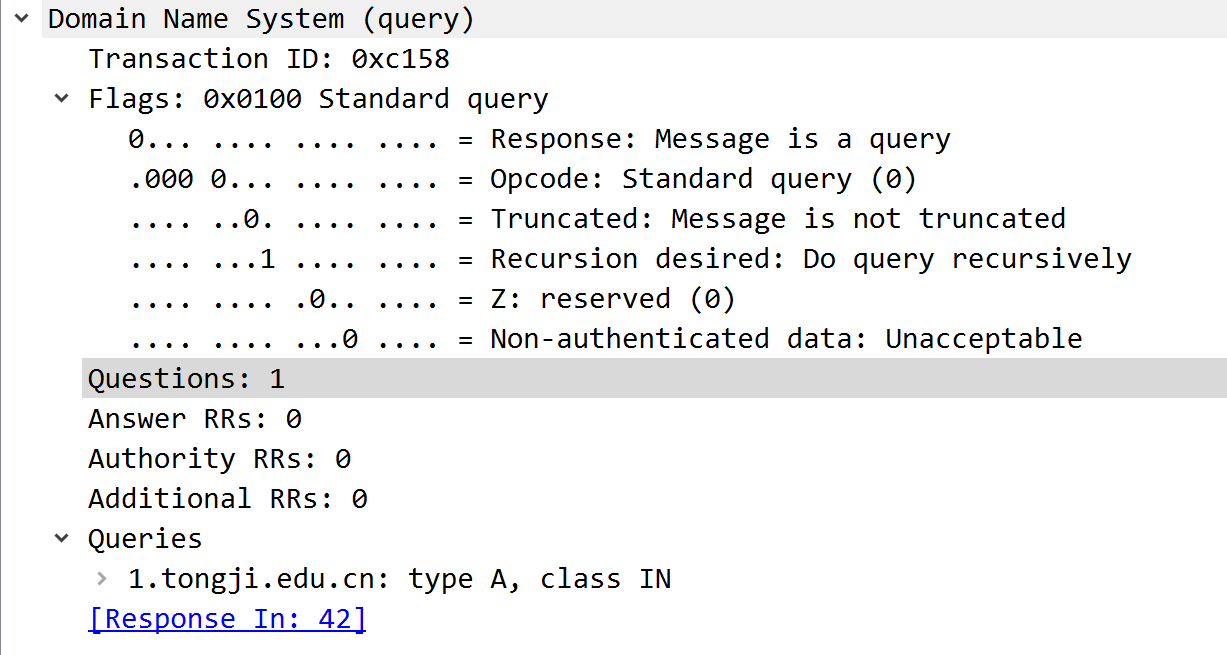
4.打开Wireshark，选择抓取WLAN的数据包，并设置“dns”过滤器：



2.分析抓取到的DNS报文：

从图，39帧是请求帧，42帧是与之对应的回应帧，且DNS数据包有五层内容。

其中第一行为帧序号和到达时间等内容；第二行为源MAC地址和目的MAC地址等内容，并记录了此处采用IPV6协议；第三行为源IP地址和目的IP地址等内容（为IPV6的IP地址）。第四行为UDP协议部分，有源端口号、目的端口号、UDP首部和数据长度、校验和等内容。前四行与UDP数据报前四行相同。第五行为DNS数据内容。请求帧该部分可以看到请求计数、请求主机域名等内容；回应帧该部分可以看到问题计数、回应计数等内容。



**【分析讨论】**

在此次DNS实验中，我通过Wireshark抓包分析DNS请求和响应的数据包，了解DNS的数据包格式和传输过程，进一步深入理解DNS的工作原理。这能帮助我熟悉DNS的基本架构、DNS服务器的分类、工作方式以及DNS缓存等基础知识。这些知识和技能对于域名管理、网络运维等领域非常重要，也有利于我们更深入地理解计算机网络的运作。