华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程　　**年级：**2020 级　　**上机实践成绩：**

指导教师：张召　　**姓名：**张熙翔　　**学号：**10205501427

上机实践名称：DNS 报文分析　　**上机实践日期：**2022/5/3

一、实验目的

了解系统命令 nslookup 的用法

学习 DNS 协议并掌握 DNS 的工作原理

二、实验任务

nslookup 命令的简单使用

使用 Wireshark 分析 DNS 协议

三、使用环境

nslookup

Wireshark

四、实验过程

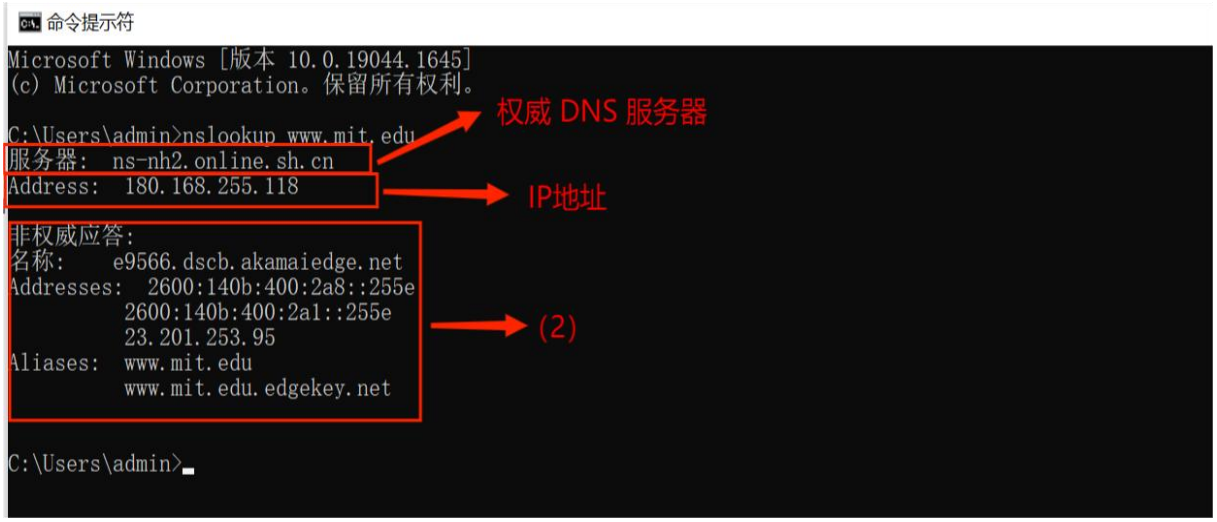
task1：运行 nslookup 来确定一个国外大学（www.mit.edu）的 IP 地址以及其权威 DNS 服务器，请在实验报告中附上操作截图并详细分析返回信息内容。

windows 平台下打开 cmd 命令行输入指令：nslookup www.mit.edu

此命令的响应提供两条信息：

（1）提供响应的 DNS 服务器的名称和 IP 地址；

（2）响应本身，即 www.mit.edu 的主机名和 IP 地址。虽然响应来自 mit 的本地 DNS 服务器，但本地 DNS 服务器很可能会迭代地联系其他几个 DNS 服务器来获得结果。



task2：运行 nslookup，使用 task1 中一个已获得的 DNS 服务器，来查询 google 服务器(www.google.com)的 IP 地址(可直接查询)，请在实验报告中附上操作截图并详细分析返回信息内容。

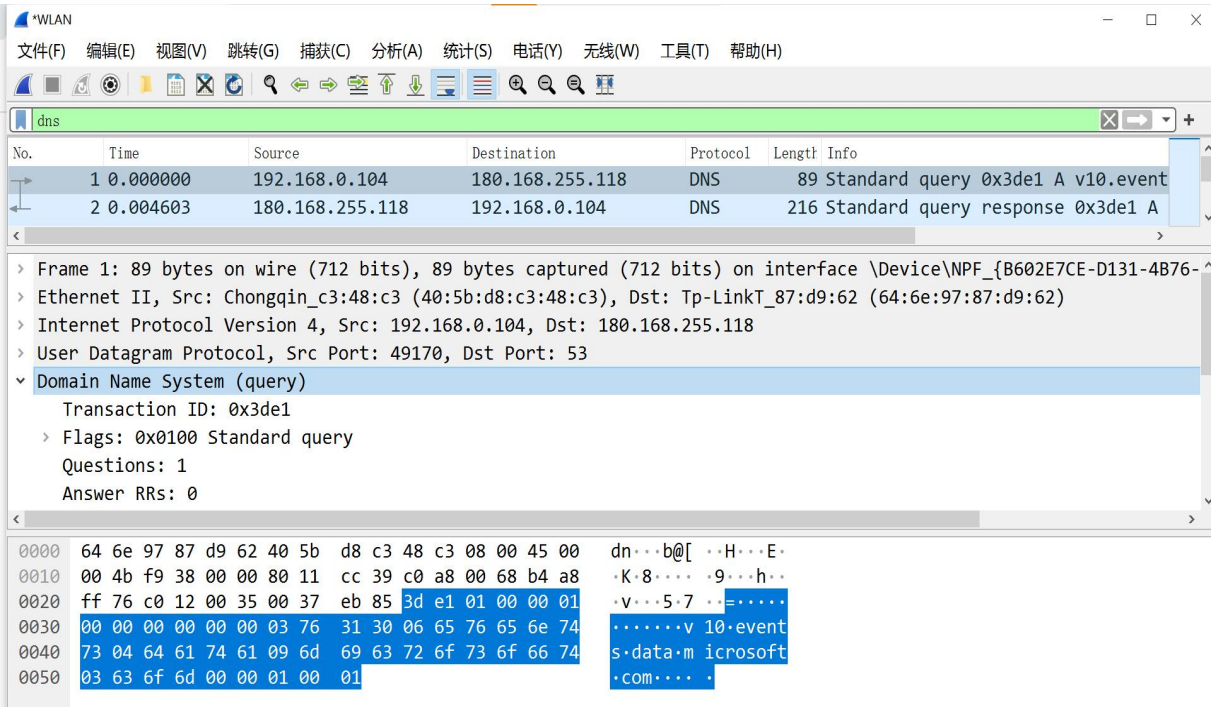
使用 DNS 服务器：ns-nh2.online.sh.cn

输入指令：nslookup www.google.com ns-nh2.online.sh.cn

task3：根据 Wireshark 抓取的报文信息（例下图所示示例），分别分析 DNS 查询报文和响应报文的组成结构，参考上面的报文格式指出报文的每个部分（如头部区域等），请将实验结果附在实验报告中。

刷新 DNS 解析缓存

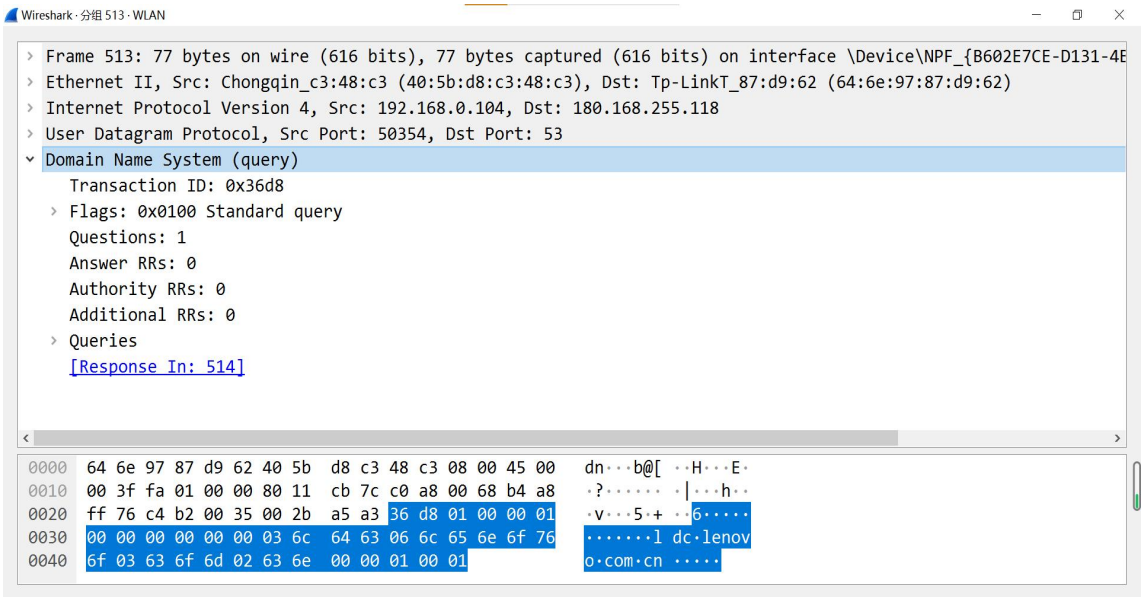
Wireshark 中过滤器输入 dns，获取查询报文和响应报文：



DNS 查询报文和响应报文有相同的格式：

注：
查询报文仅仅包含查询部分。响应报文包含查询部分、响应部分，也可能包含其他两部分。

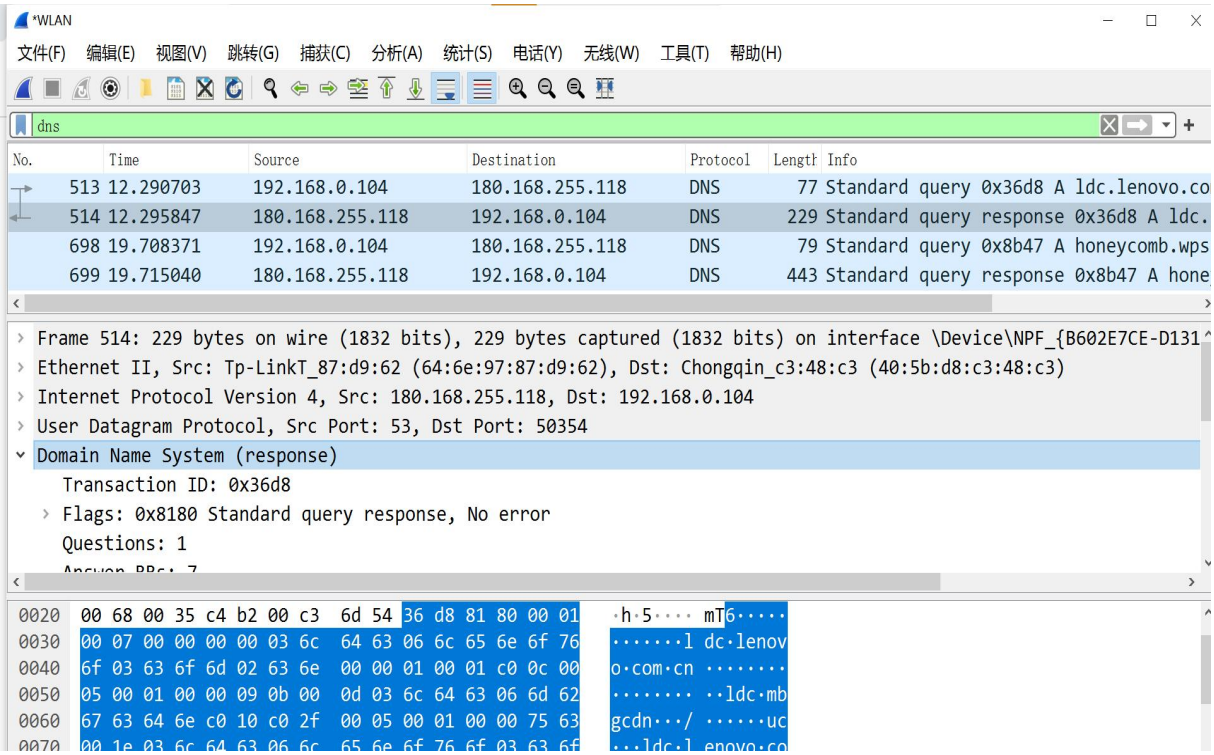
查询报文：



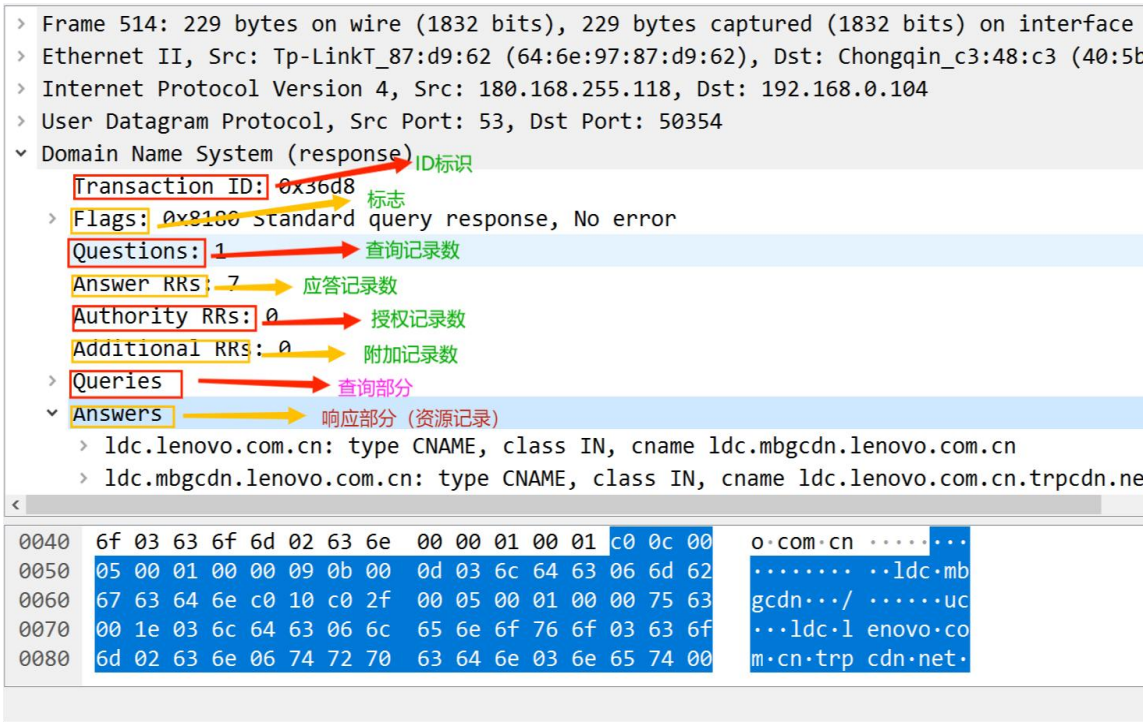
其中各部分如下表所示：

头部	Transaction ID（事务 ID），DNS 报文的 ID 标识，对于请求报文和其对应的应答报文，该字段的值是相同的 ID 课题区。通过这个分 DNS 应答报文是对哪个请求进行相应的。
头部	Flags（标志）
头部	Questions(问题计数)
头部	Answer RRs(回答资源记录数)
头部	Authority RRs(权威名称能服务器计数)
头部	Additional RRs(附加资源记录数)
问题部分	Queries（查询问题区域）

响应报文：

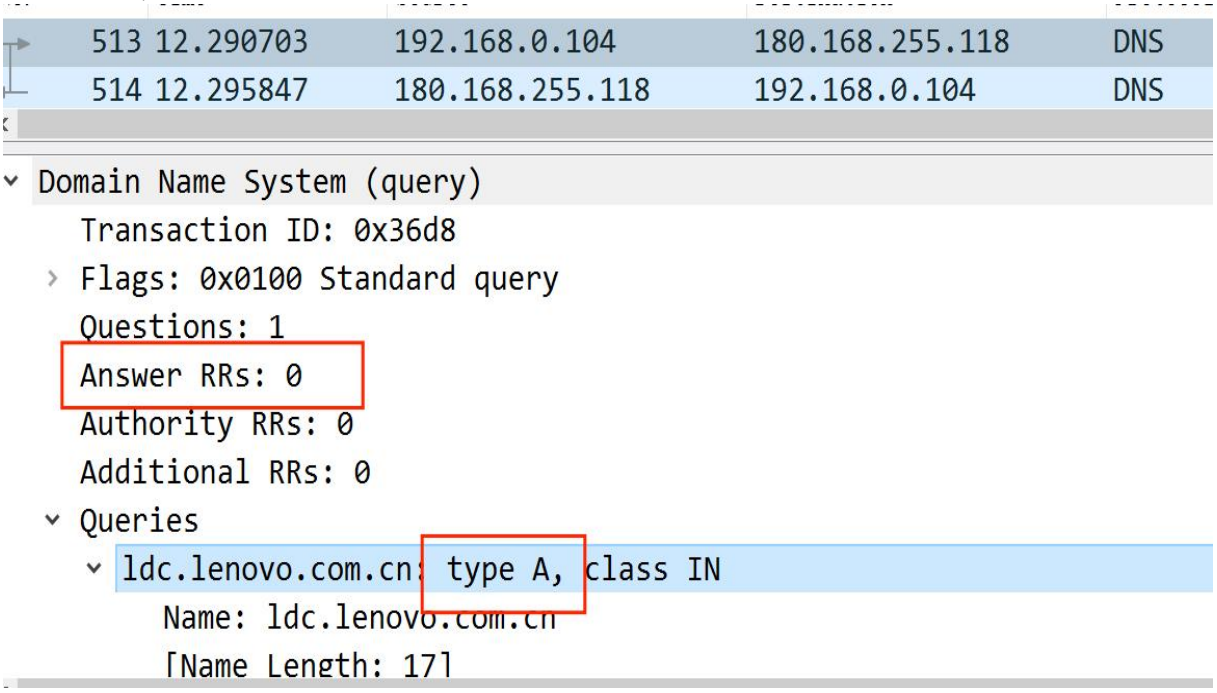


DNS 响应报文的头部、查询问题区域结构基本和响应报文一致。并且一些查询主机的名字、查询类型等信息也需要保持一致。但是比起查询报文，响应报文多了一个资源记录部分。

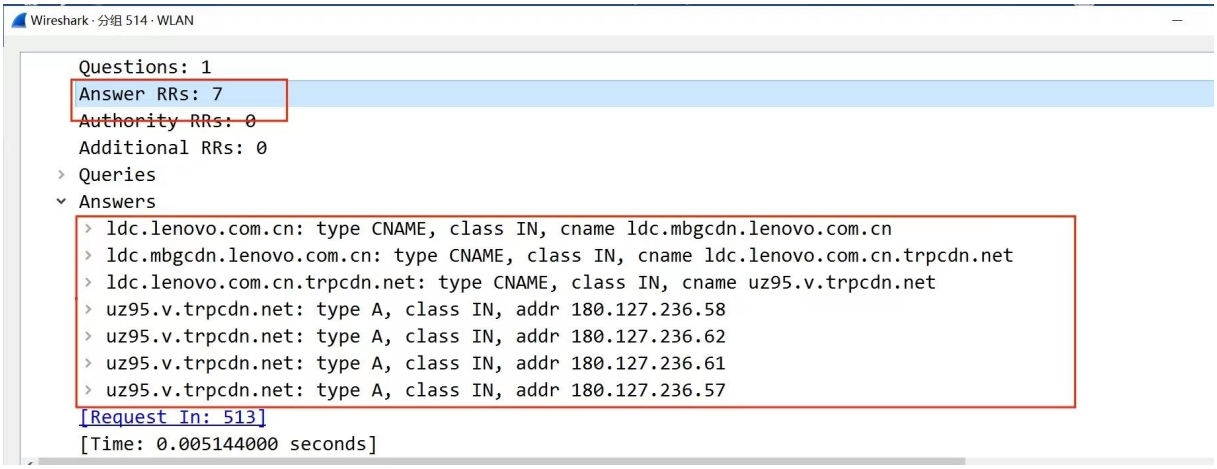


task4：基于 task3 中得到的查询和响应报文进行分析，试问这里的查询是什么“Type”的，查询消息是否包含任何“answers"？试问这里的响应消息提供了多少个“answers”，这些“answers”具体包含什么？请将实验结果附在实验报告中。

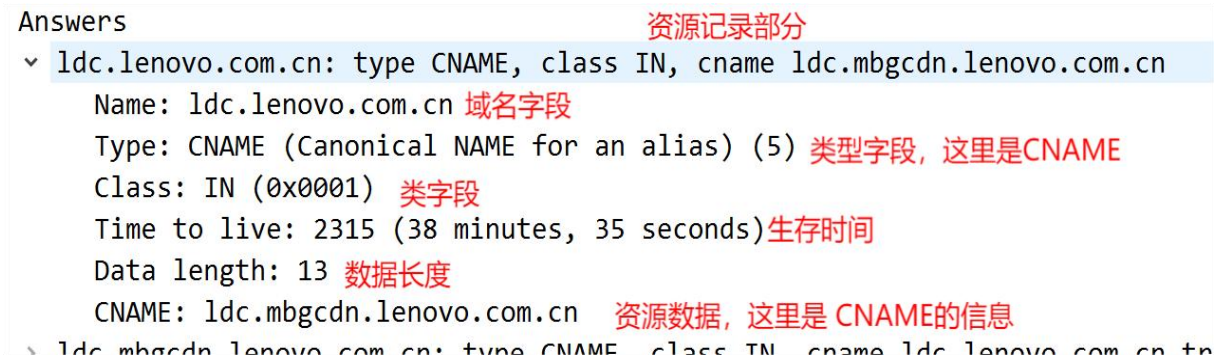
查询 Type，查询消息不包含任何“answer”：



响应消息提供了 7 个“answers”：



“answers”具体包含：



五、总结

通过本次实验，学习了系统命令 nslookup 的简单使用，理解了 DNS 协议并掌握 DNS 的工作原理，能够实验使用 Wireshark 分析 DNS 协议。