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：** 21 级	**上机实践成绩：**
指导教师： 张召	**姓名：** 杨茜雅	**学号：** 10215501435
上机实践名称： Lab10		**上机实践日期：** 2023.5.12
上机实践编号： 10	**组号：**	**上机实践时间：** 5.12

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

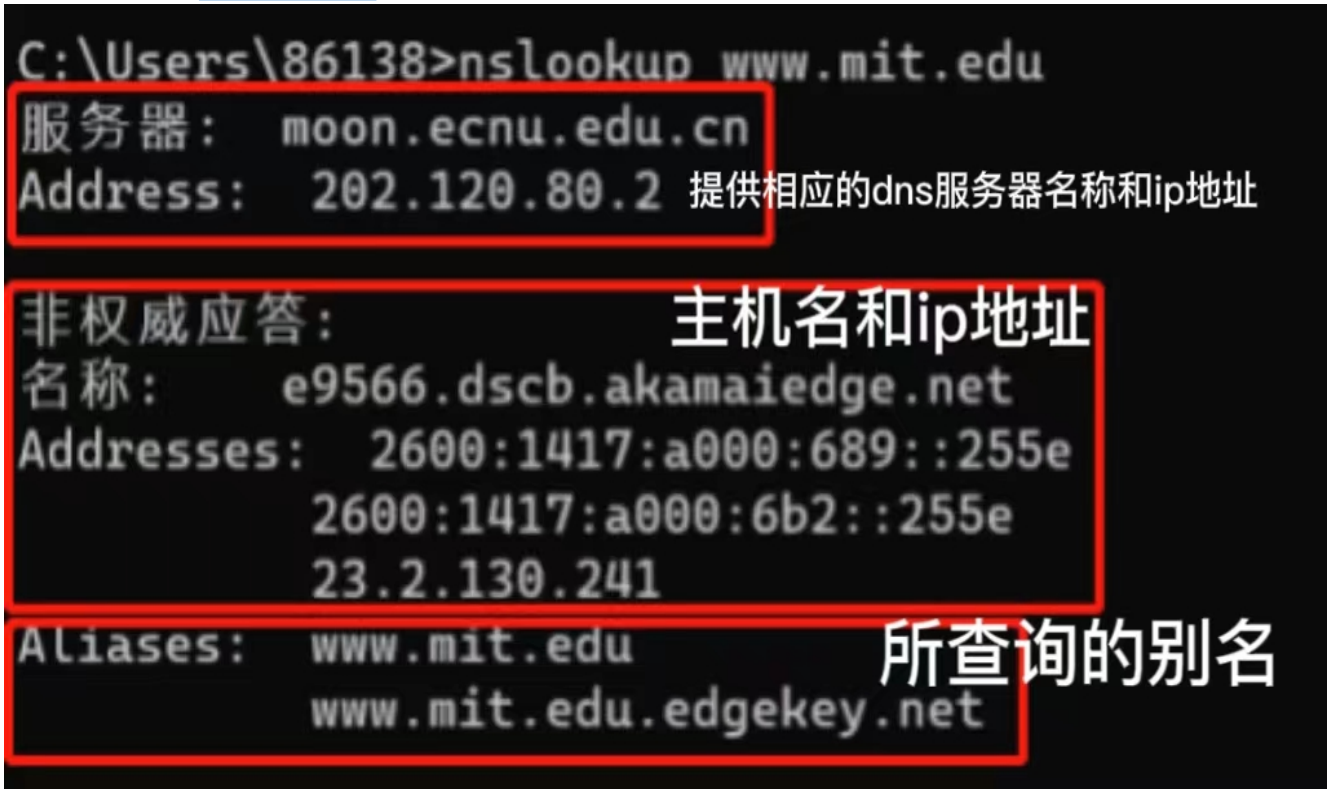
- nslookup
- Wireshark

四、 实验过程

Task 1：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。

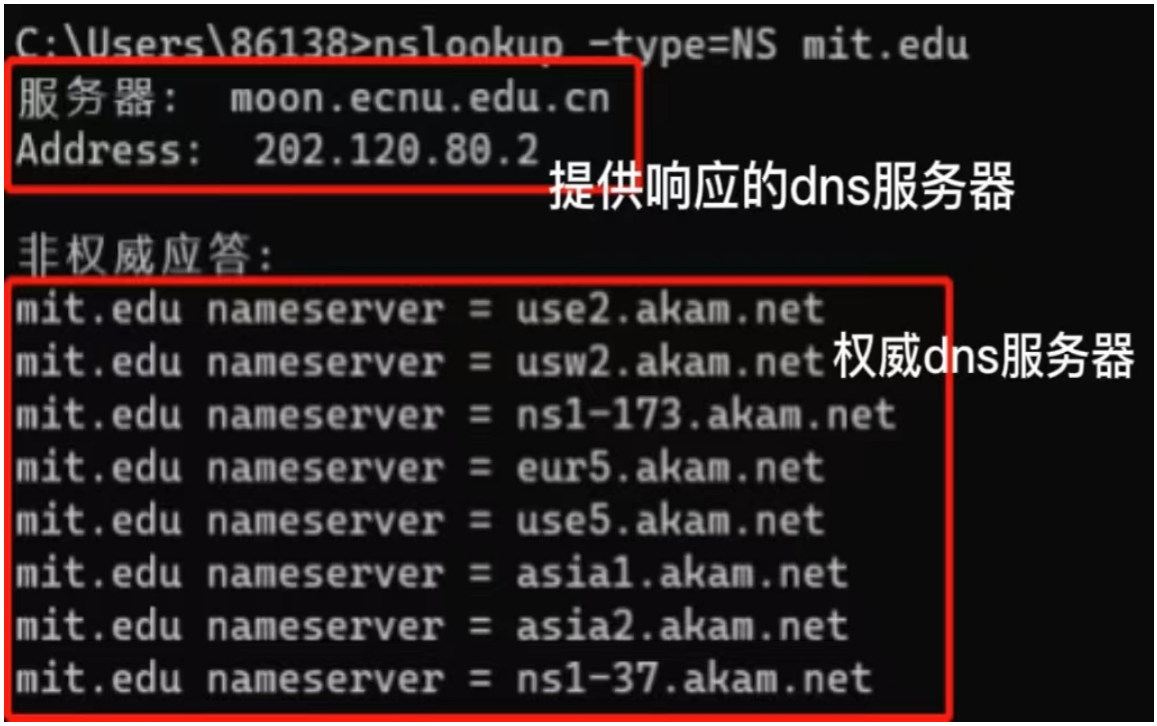
尝试三个不同 nslookup 命令的结果：

1、nslookup www.mit.edu



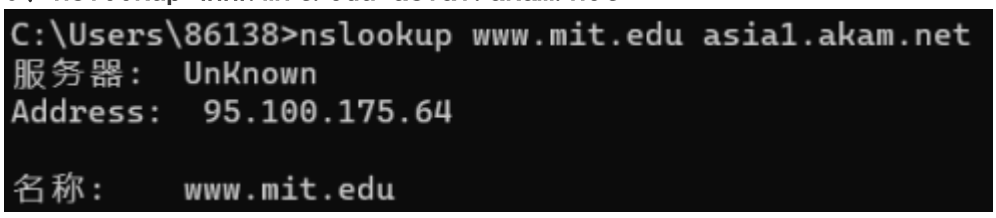
这个命令是说，请告诉我主机 www.mit.edu. 的 IP 地址。如上图所示，此命令的响应提供两条信息：（1）提供响应的 DNS 服务器的名称和 IP 地址；（2）响应本身，即 www.mit.edu.的主机名和 IP 地址。虽然响应来自mit的本地 DNS 服务器，但本地 DNS 服务器很可能会迭代地联系其他几个 DNS 服务器来获得结果。

2、nslookup -type=NS mit.edu ：查询权威 DNS



在这个例子中，我添加了选项 -type=NS 和一级域名 mit.edu。这将使得 nslookup 将NS（域名服务器记录，Name Server）记录发送到默认的本地 DNS 服务器。换句话说，“请给我发送 mit.edu 的权威 DNS 的主机名”（当不使用 -type 选项时，nslookup 使用默认值，即查询 A 类记录。）上图中，首先显示了提供响应的 DNS 服务器（这是默认本地 DNS 服务器）以及八个 mit 域名服务器。这些服务器中的每一个确实都是校园主机的权威 DNS 服务器。然而，nslookup 也表明该响应是非权威的，这意味着这个响应来自某个服务器的缓存，而不是来自权威mit DNS 服务器。

3、nslookup www.mit.edu asia1.akam.net



在这个例子中，我们希望将查询请求发送到 DNS 服务器 asia1.akam.net ，而不是默认的本地DNS 服务器 。因此，查询和响应事务直接发生在我们的主机和 asia1.akam.net 之间。在这个例子中，DNS 服务器 asia1.akam.net提供主机 www.mit.edu. 的 IP 地址信息。

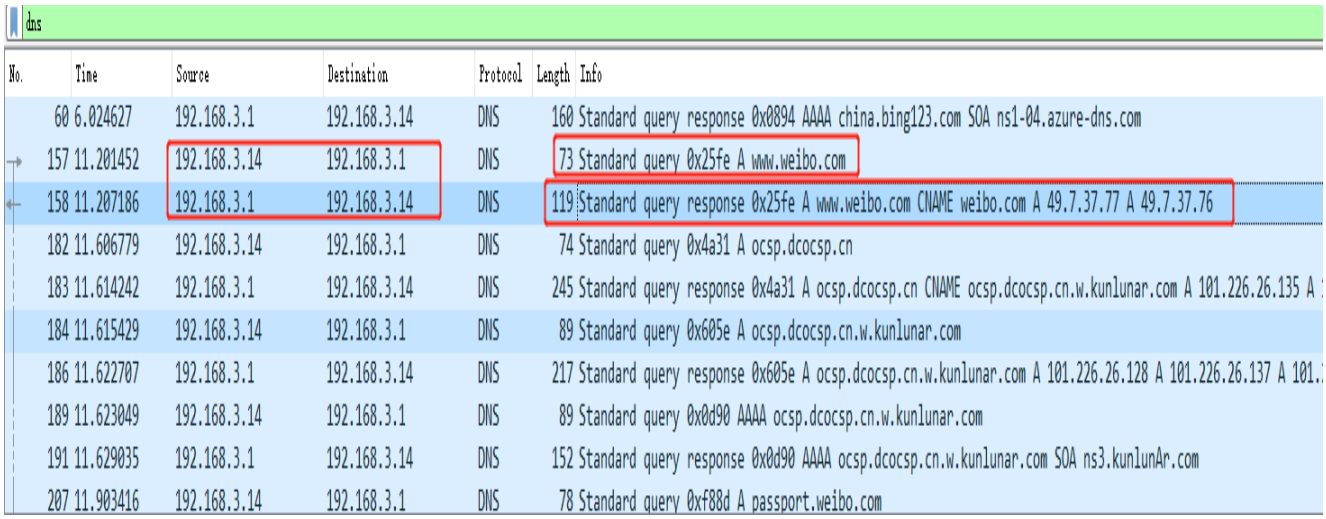
Task 2：运行 nslookup ，使用task1中一个已获得的 DNS 服务器，来查询google服务器(www.google.com)的 IP 地址(可直接查询)，请在实验报告中附上操作截图并详细分析返回信息内容。

使用DNS 服务器：moon.ecnu.edu.cn
输入指令：nslookup www.google.com moon.ecnu.edu.cn

Task 3：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。

先刷新 DNS 解析缓存

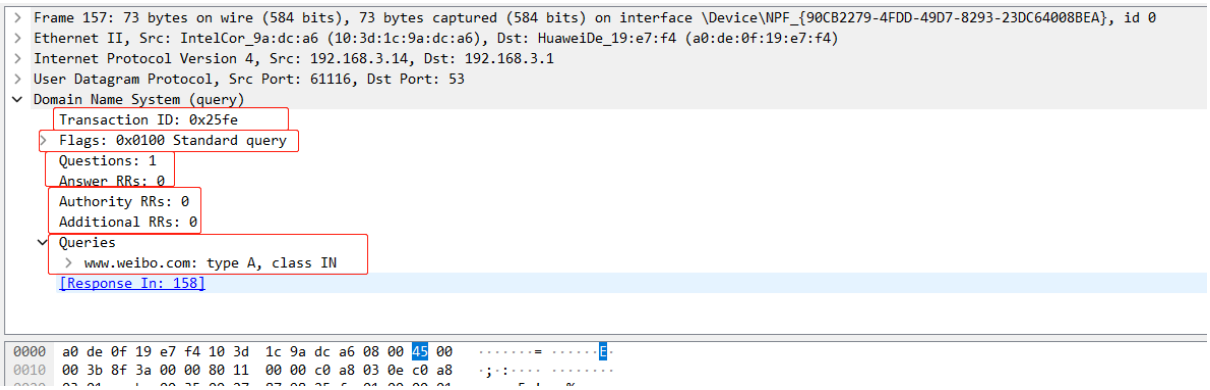
在浏览器中查询 www.weibo.com，在 Wireshark 中过滤器输入 dns，获取查询报文和响应报文：



DNS 只有两种报文：查询报文、响应报文，两者有着相同格式，如下：

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：



头部：

Transaction 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,这里是0x25fe。

Flags:标志（query 查询，query response 响应）,此处为 0x0100 Standard query

Questions:问题计数，此处为 1

Answer RRS:回答资源记录数，此处为 0

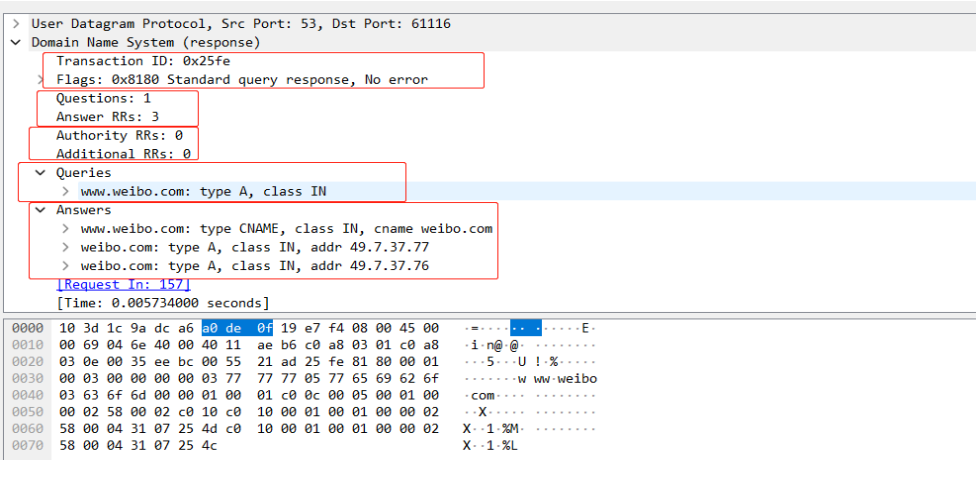
Authority RRS:权威名称能服务器计数，此处为 0

Additional RRs:附加资源记录数，此处为 0

因查询报文仅包含查询部分，所以**查询部分**：

Queries: 查询问题区域，此处为 www.weibo. com: type A, class IN

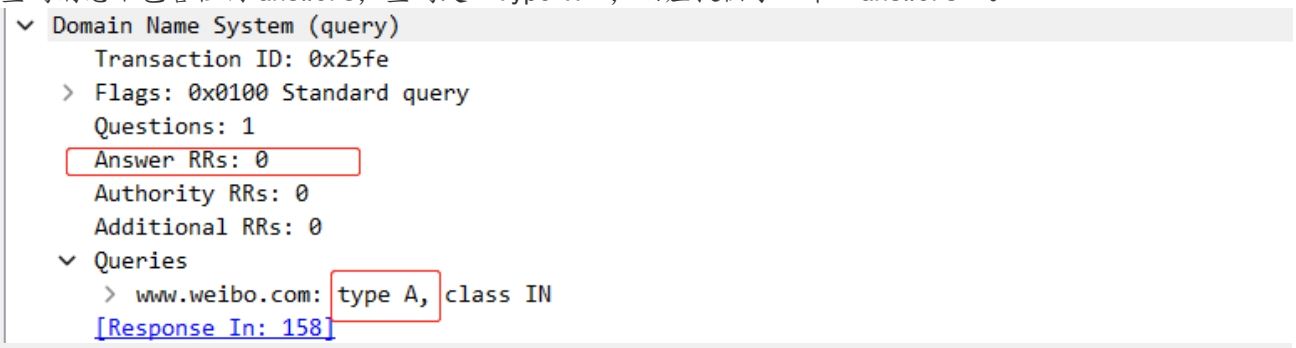
响应报文：

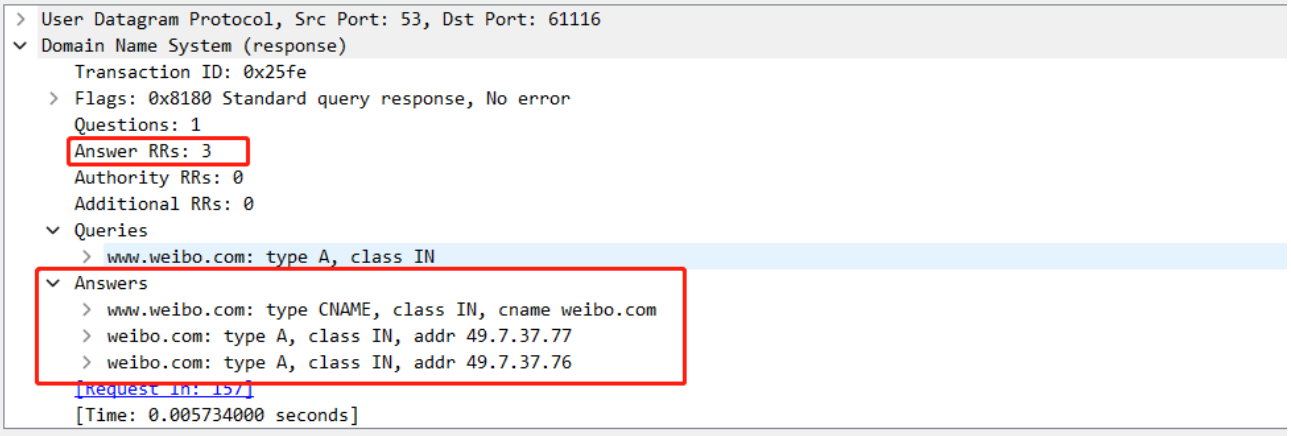


DNS 响应报文的头部、查询问题区域结构基本和响应报文一致。并且一些查询主机的名字、查询类型等信息也需要保持一致。比如上图的Transaction ID、Flags、Questions、Authority RRS、Additional RRs、Queries，但是此处Answer RRS（应答记录数）的数量变为三个，并且比起查询报文，响应报文多了一个Answers(资源记录部分)。

Task 4: 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。

查询消息不包含任何 answers，查询是‘Type A’，响应提供了三个‘answers’。





五、总结

通过本次实验，我学习了系统命令nslookup 的简单使用，学会了三个不同nslookup命令的不同结果。理解了DNS 协议并掌握DNS的工作原理，能够实验使用Wireshark 抓取查询和响应报文并分析字段。