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：**2021	**上机实践成绩：**
指导教师：张召	**姓名：**温兆和	**学号：**10205501432
上机实践名称： DNS 报文分析		**上机实践日期：**2022.04.29
上机实践编号：10	**组号：**001-432	**上机实践时间：**13：00

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

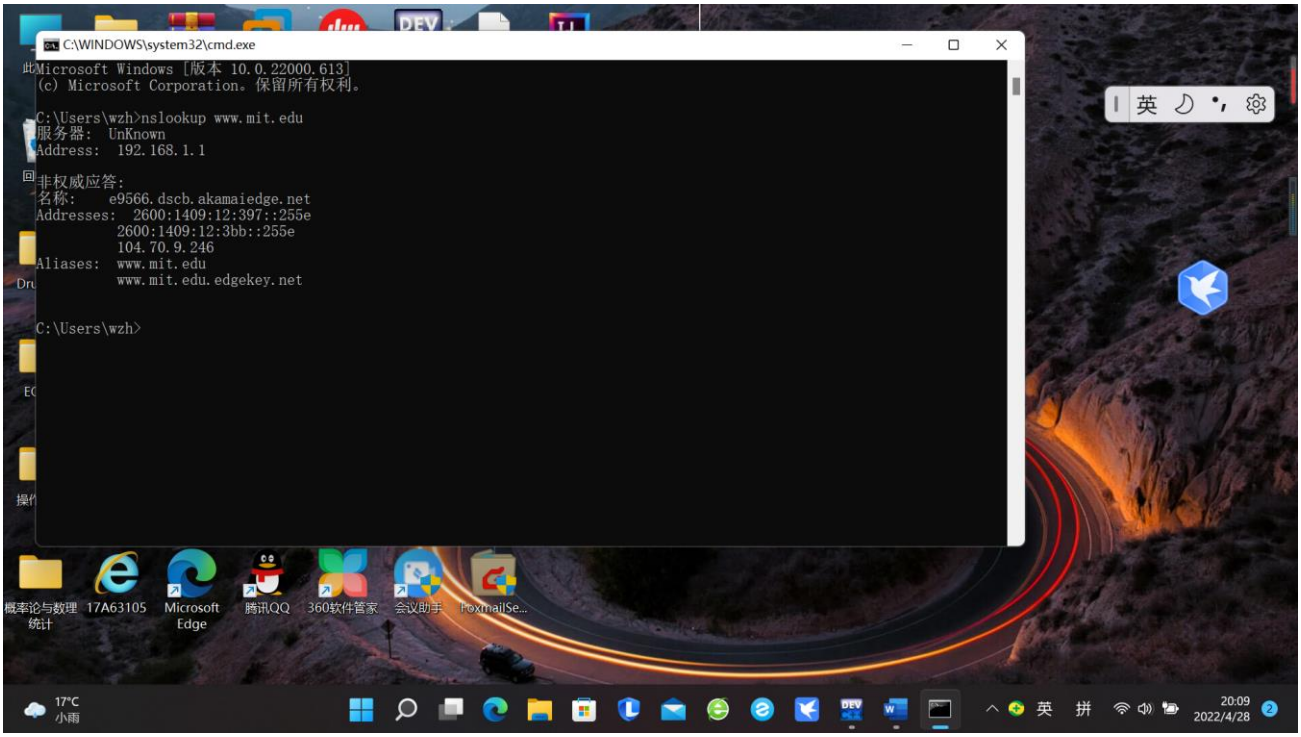
Wireshark

四、 实验过程

Task1. 运行 nslookup 来确定一个国外大学的 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并详细分析返回信息内容。

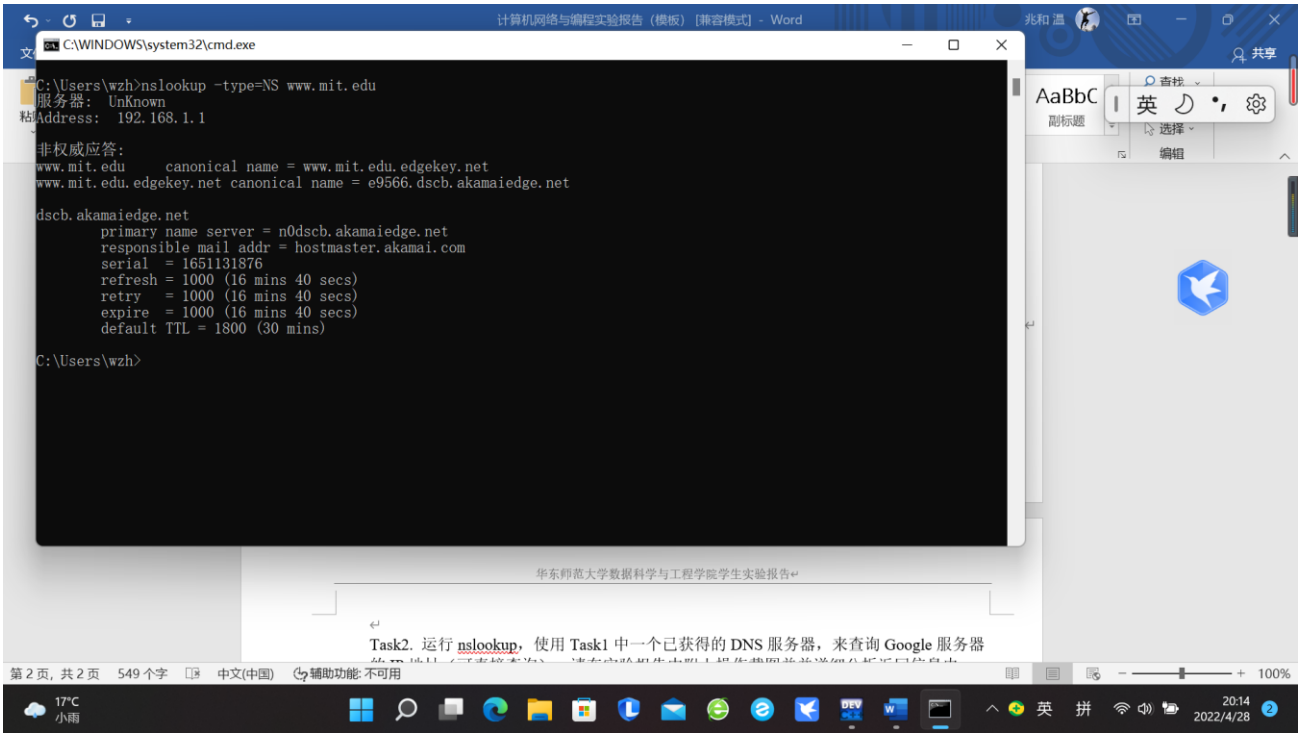
目标：www.mit.edu

IP 地址：



包含信息：提供响应的 DNS 服务器的 IP 地址（本地 DNS 服务器）；目标的主机名和 IP 地址。

权威 DNS 服务器：

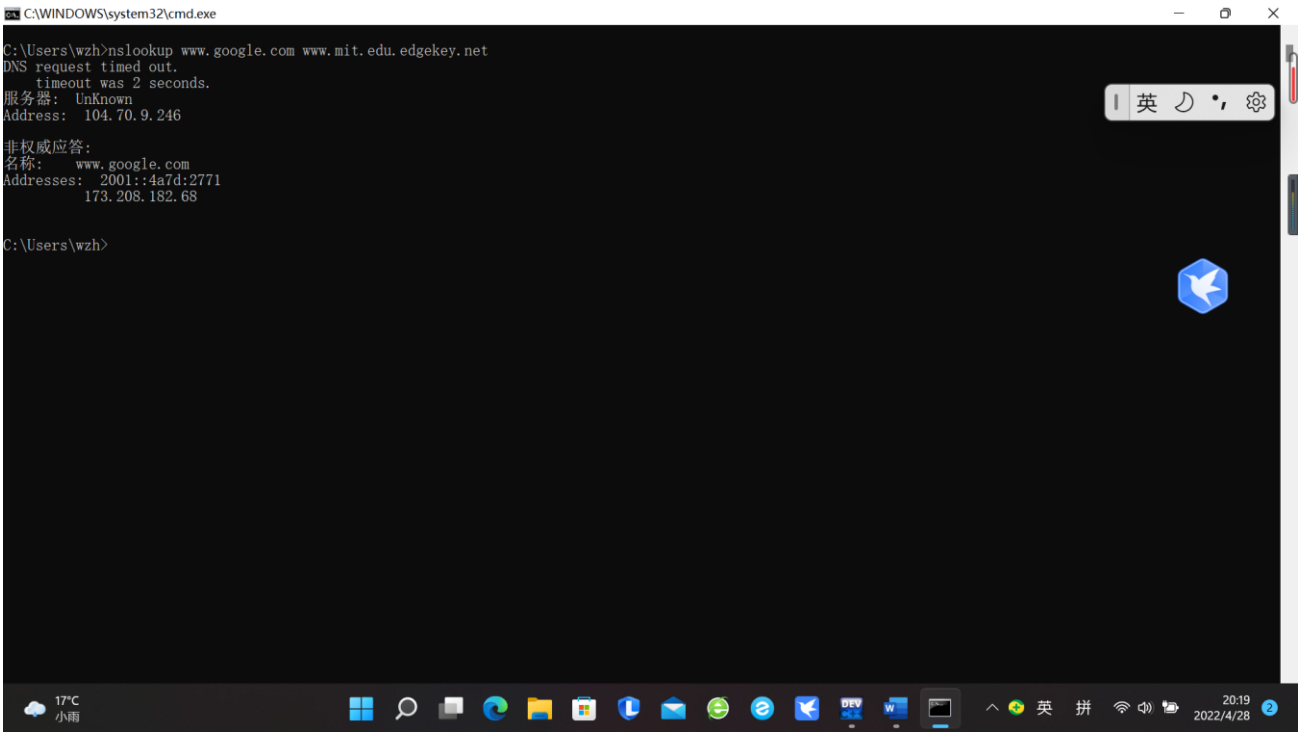


包含信息：提供响应的 DNS 服务器的 IP 地址（本地 DNS 服务器）；目标的两个权威 DNS 服务器。

Task2. 运行 nslookup，使用 Task1 中一个已获得的 DNS 服务器，来查询 Google 服务器的 IP 地址（可直接查询），请在实验报告中附上操作截图并并详细分析返回信息内容。

目标：www.google.com

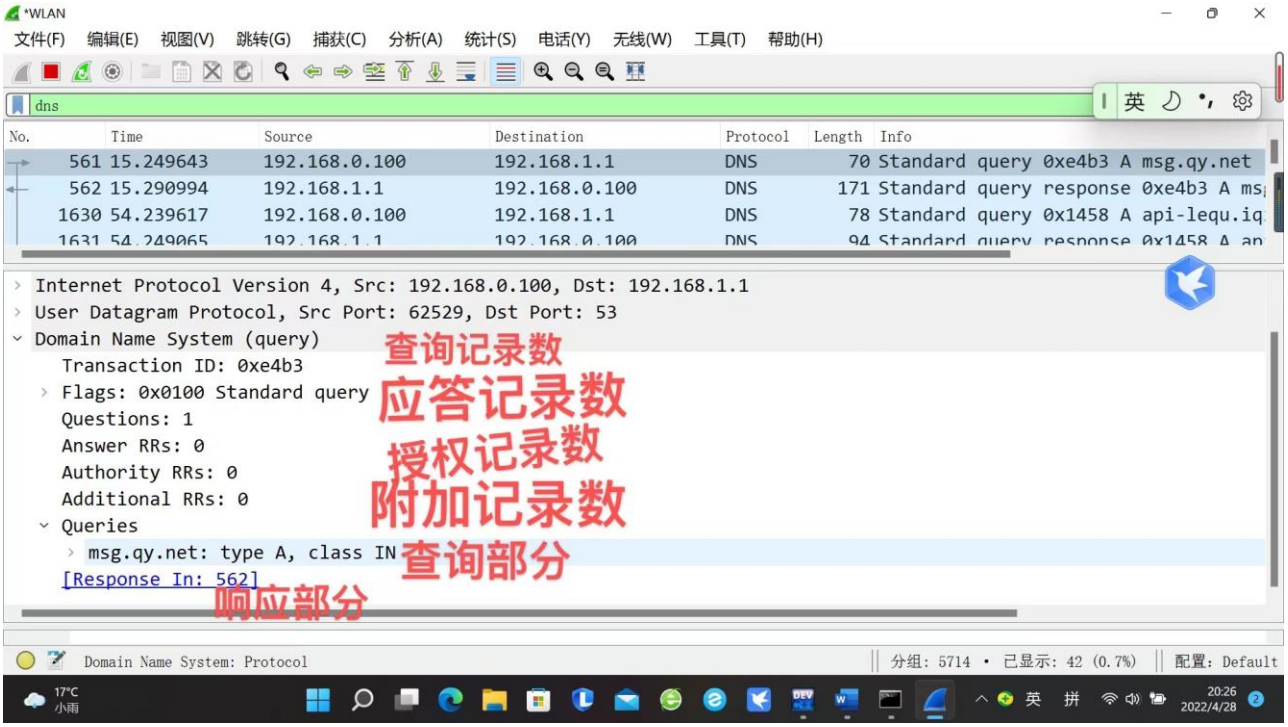
IP 地址：



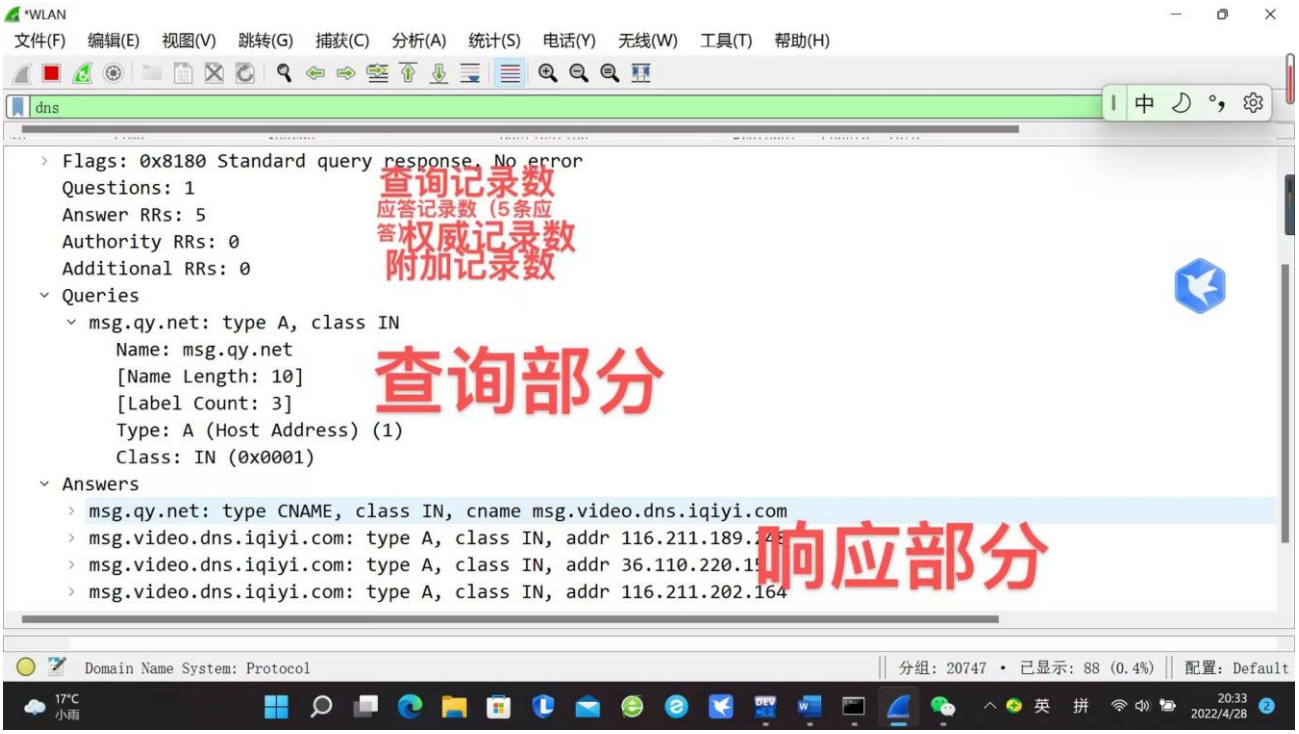
包含信息：提供响应的 DNS 服务器的 IP 地址（MIT 的 DNS 服务器）；目标的主机名和 IP 地址。

Task3. 根据 Wireshark 抓取的报文信息，分别分析 DNS 查询报文和响应报文的组成结构并指出报文的每个部分，请将实验结果附在实验报告中。

查询报文：

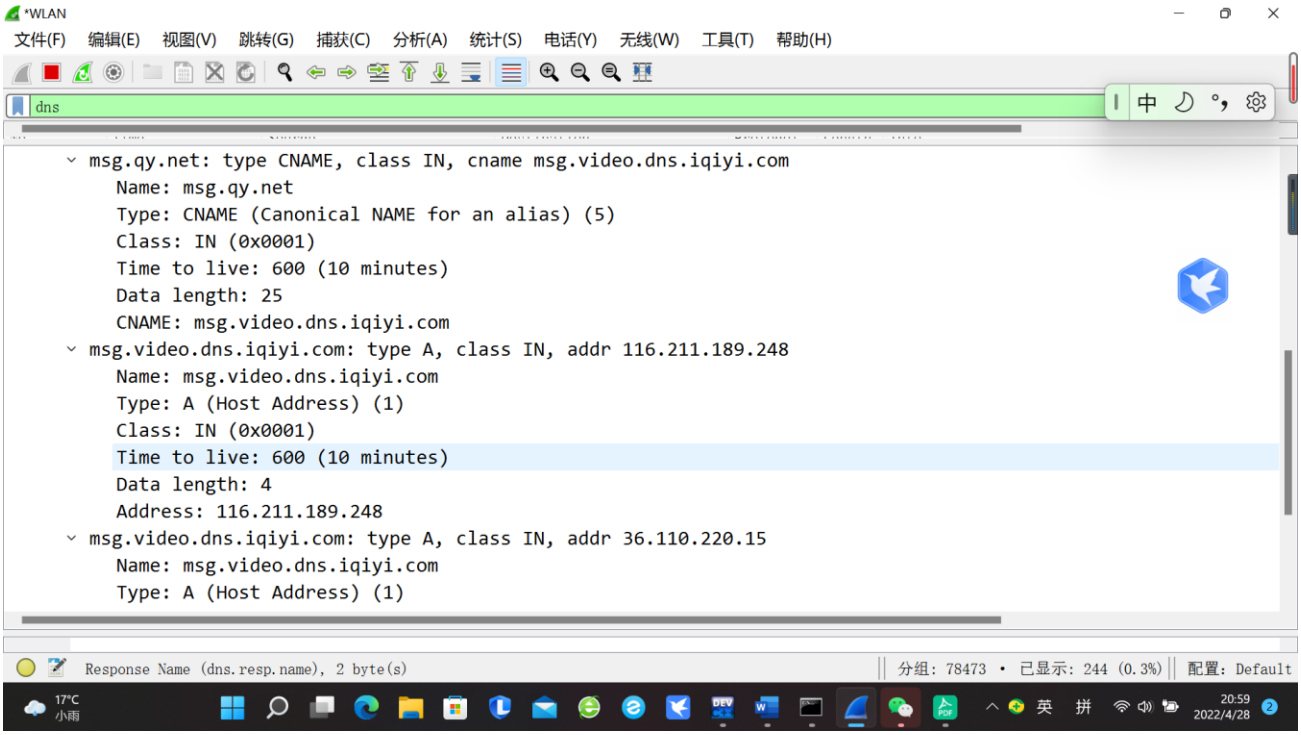


响应报文：



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。

响应部分具体内容：



查询是类型 A 的；

查询报文中相应部分为空；

响应消息中包含了 5 条回复，主要包含：别名为 msg.qiyi.net 的主机的规范主机名、msg.video.dns.iqiyi.com 的 IP 地址、字节长度（Data length）和缓存时间（Time to live）。

五、总结

在本周的实验中，我们掌握了 nslookup 命令的基本使用并对 DNS 协议进行了分析，巩固了课内知识，并为今后的学习打下了基础。