# 

# 桂 林 电 子 科 技 大 学

## 计算机网络 实 验 报 告

|  |
| --- |
| 评语：  指导教师签名：  成绩： |

实验名称 实验七 域名解析与DNS协议分析

计算机与信息安全学院 学院

计算机科学与技术 专 业

**姓名 吴河山**

**学号 2000500927**

实 验 日 期2022年 12 月 5 日

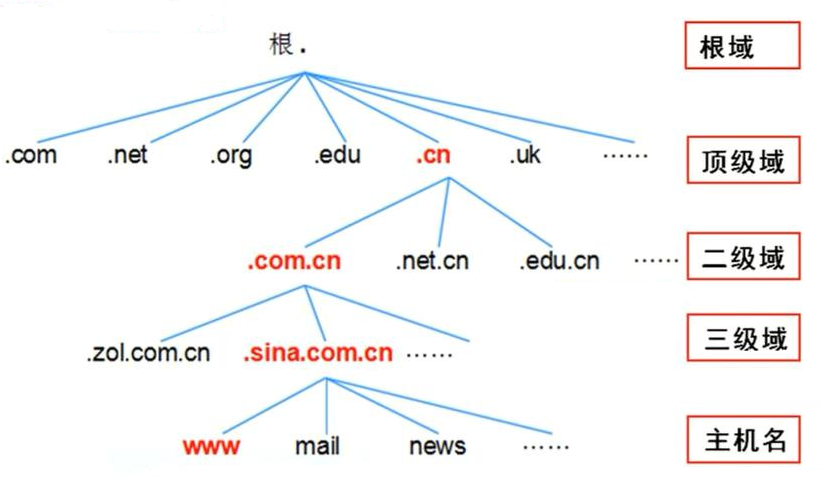
**一．实验目的**

1. 加深理解DNS系统的工作机制
2. 熟悉与掌握域名解析工具nslookup用法
3. 了解域名解析过程
4. 熟悉与掌握域名解析工具dig用法
5. 初步了解DNS报文结构

**二．实验环境**

1. 头歌基于Linux的虚拟机桌面系统
2. 网络报文分析工具wireshark
3. 浏览器firefox
4. **相关原理或知识点**
5. **INTERNET域名空间结构**

为了保证域名的唯一性，域名系统采用层次结构，整体呈树状，主机域名由主机名加其所在网络域名组成，例如www.sina.com.cn就是一个主机域名，属于三级域名，这台主机提供WEB服务。



1. **域名服务器**

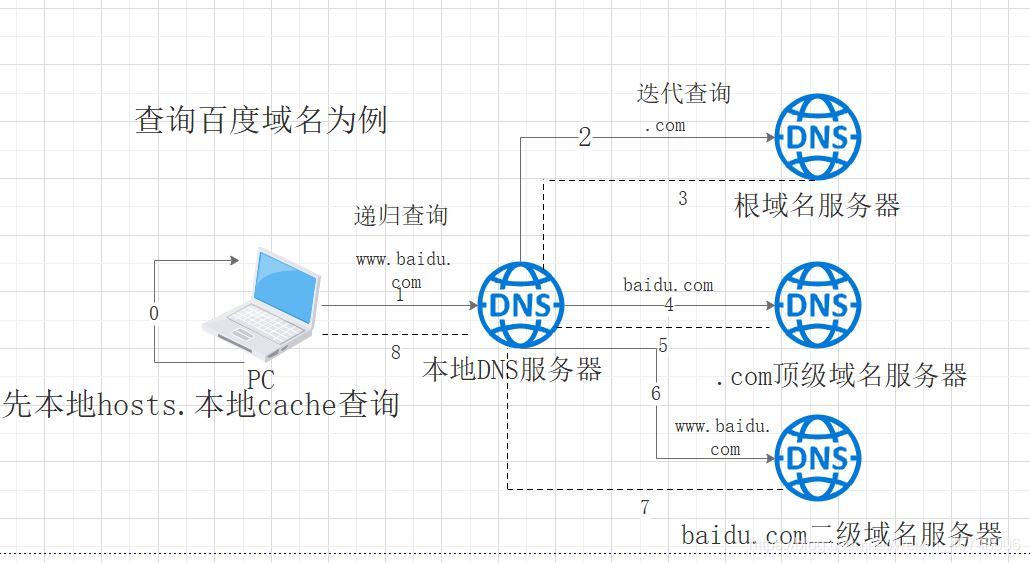
域名不是IP协议通信时直接使用的地址，因此应用软件使用域名通信时，会自动在后台借助于域名服务器，去解析域名。

**3、域名解析工具**nslookup

域名解析主要是将主机名（例如www.example.com）转换为计算机友好的 IP 地址（例如192.168.1.1） 。

nslookup 是一种网络管理命令行工具，可用于查询 DNS 域名和 IP 地址。无论是 linux 或者是 window 下都有这个工具，用好它对平常的域名解析情况，或者对域名服务器的维护都有帮助。 语法： nslookup [ -Option … ] [ Host ] [ -NameServer ] nslookup 命令以两种方式查询域名服务器： 交互模式: 当没有给出操作参数时进入，操作对象和操作方式可以通过相应交互命令来告诉。 命令模式: 在一个命令行中将操作对象和操作方式告知命令，nslookup 将执行结果返回。

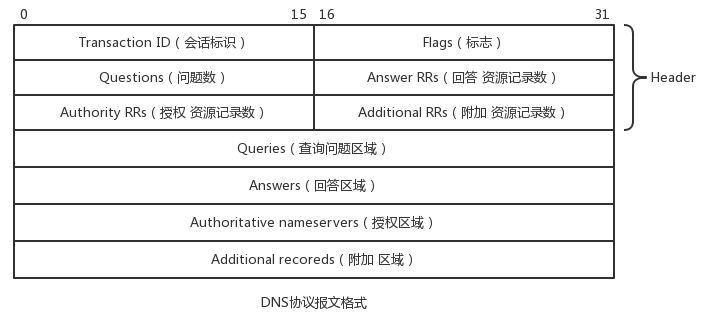
**4、域名解析过程**



**5、DNS报文结构**

DNS报文分请求、响应两种类型。

1. **DNS查询响应的一般格式**



**（2）DNS查询报文中的问题部分**



查询名：即要请求的域名，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。如下图报文06表示了teredo长度，04表示ipv6的长度，以此类推，最后以00结束。计数字节的值必须是 0 ~ 63的数，对于每一级域名长度的限制是63个字符，域名总长度则不能超过253个字符。

**（3）DNS响应报文中的资源记录部分**

DNS报文中最后的三个字段，回答字段、授权字段和附加信息字段，均采用一种称为资源记录RR( Resource Record）的相同格式。



1. **实验内容**

**第1关 域名解析与NSLOOKUP应用**

1、双击打开桌面上的工作区文件夹workspace，再双击实训文件夹myshixun，打开文件message6-1.txt。

2、使用 cat 命令查看本机默认的 DNS 服务器，属于本地域名服务器操作：cat /etc/resolv.conf将查到的ip地址写到文件message6-1.txt第一行末尾，末尾添加1个空格。

3、查询网站www.educoder.net的IP 将查到的ip地址写到文件message6-1.txt第一行末尾，末尾添加1个空格。

4、查询域名为educoder.net区域的DNS 服务器IP将查到的ip地址写到文件message6-1.txt第一行末尾。

5、查询域名为qq.com区域的邮件服务器IP(不止一个)将查到的ip地址按从小到大顺序写到文件message6-1.txt第二行末尾，相邻两个IP地址之间加1个空格分隔，并保存该文件。

**第2关 域名解析过程与报文分析**

1、双击打开桌面上的工作区文件夹workspace，再双击实训文件夹myshixun， 打开文件message6-2.txt。

2、打开终端工具在平台桌面空白处，按鼠标右键，选“在此打开终端”

3、查询INTERNET根域DNS服务器**，**执行命令：dig观察得到的数据， 将根域DNS服务器的个数、以及它们所在网络区域的域名（以点结束）依次写到文件message6-1.txt第一行末尾，答案之间要加1个空格分隔。

4、以迭代查询方式解析www.baidu.com域执行命令：dig [www.baidu.com](http://www.baidu.com) +trace

5、查询网络区域guet.edu.cn内有哪些域名服务器，并指出哪个是主DNS服务器。

执行命令：dig guet.edu.cn ns

执行命令：dig guet.edu.cn soa

6、查询网络区域guet.edu.cn内有哪些邮件服务器，执行命令：dig guet.edu.cn mx

7、跟踪nslookup www.baidu.com，分析DNS报文

（1）打开 Wireshark ，并在过滤器中输入 DNS 。筛选出 DNS 协议报文，并开始捕获报文。

（2）打开终端，输入命令并执行nslookup www.baidu.com，在 Wireshark 中停止捕获报文， 查看报文列表，可以看到成对的DNS 查询-响应报文。

（3）展开最后一对中的查询报文，分析协议字段中各字段的值，将 Queries Name 的值写入文件第2行的末尾，然后再写入一个空格。

（4）展开最后一对中的响应报文，分析协议字段中各字段的值，将 Answers Cname 的值写入文件第2行的末尾，然后再写入一个空格。

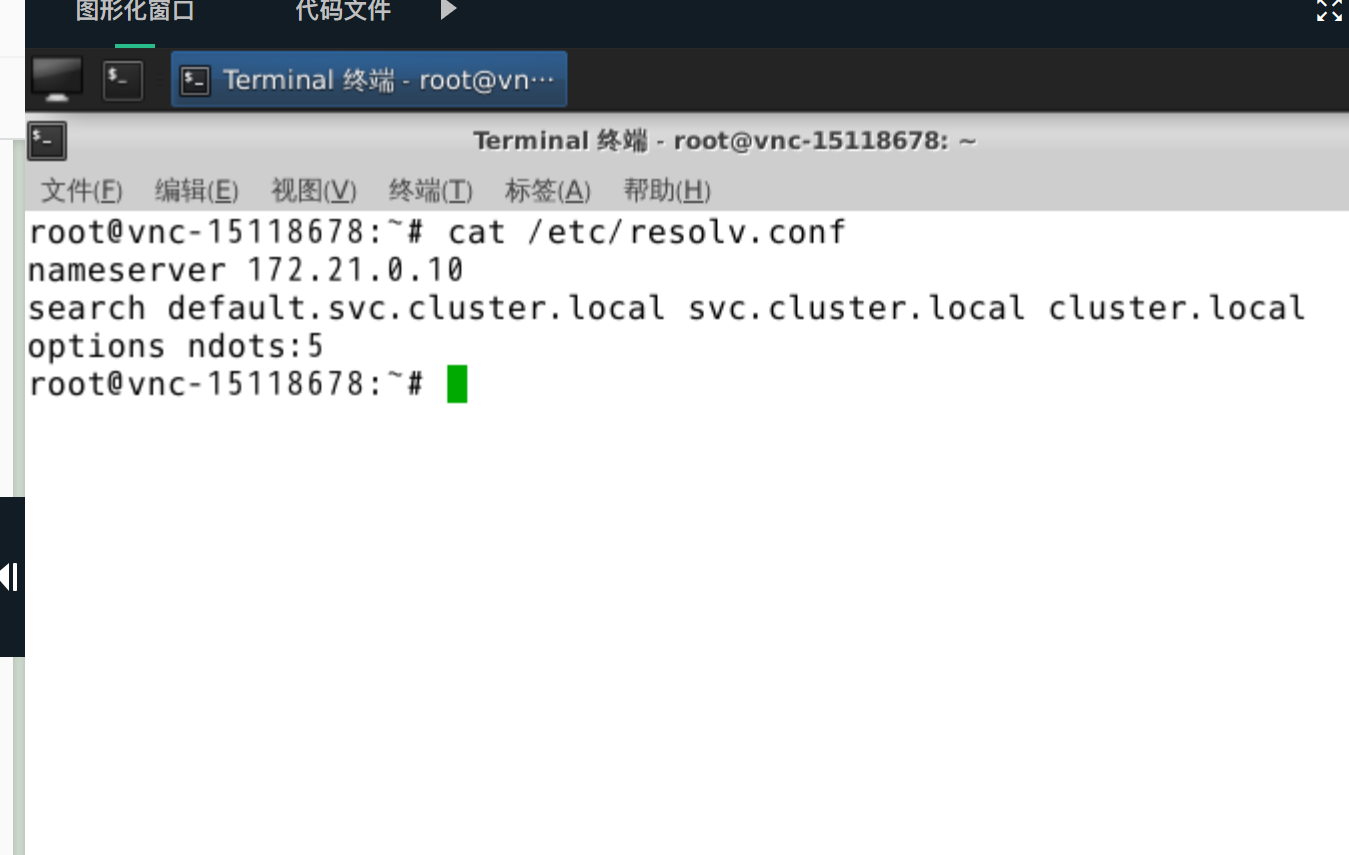
（5）展开最后一对中的响应报文，将 Answers 中的那个最小IP 值写入文件第2行的末尾。

（6）保存文件message6-2.txt。

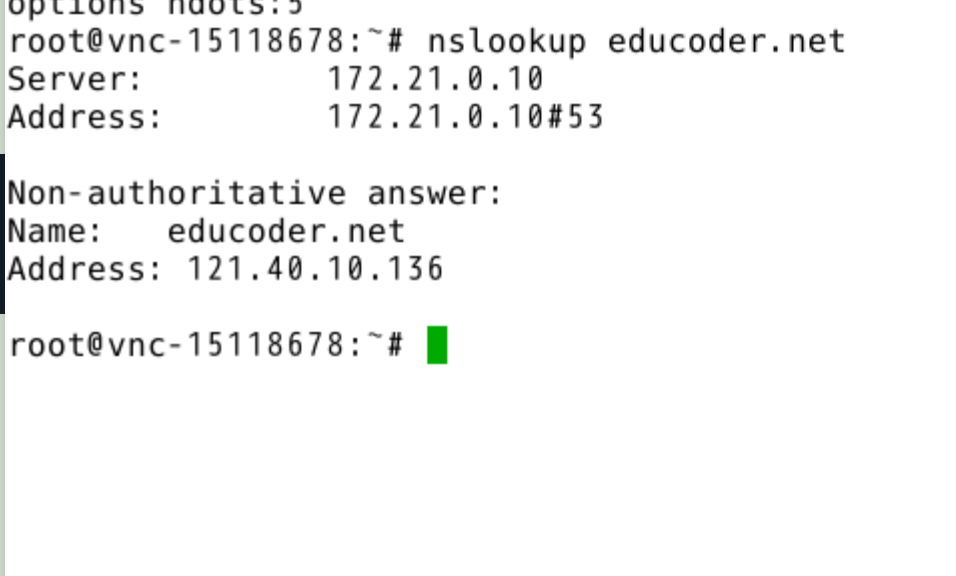
1. **实验结果及其分析**

**第1关 域名解析与NSLOOKUP应用**

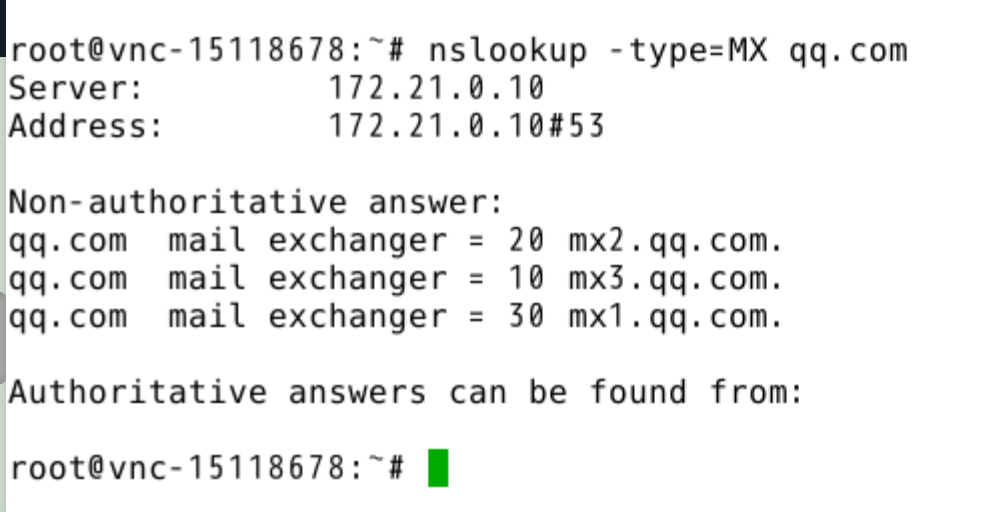
1. **如下图所示执行cat /etc/resolv.conf 查询到本机的DNS服务器地址为172.21.0.10；**



1. **从图中可以看出:** www.educoder.net **的ip地址为121.40.10.136；**



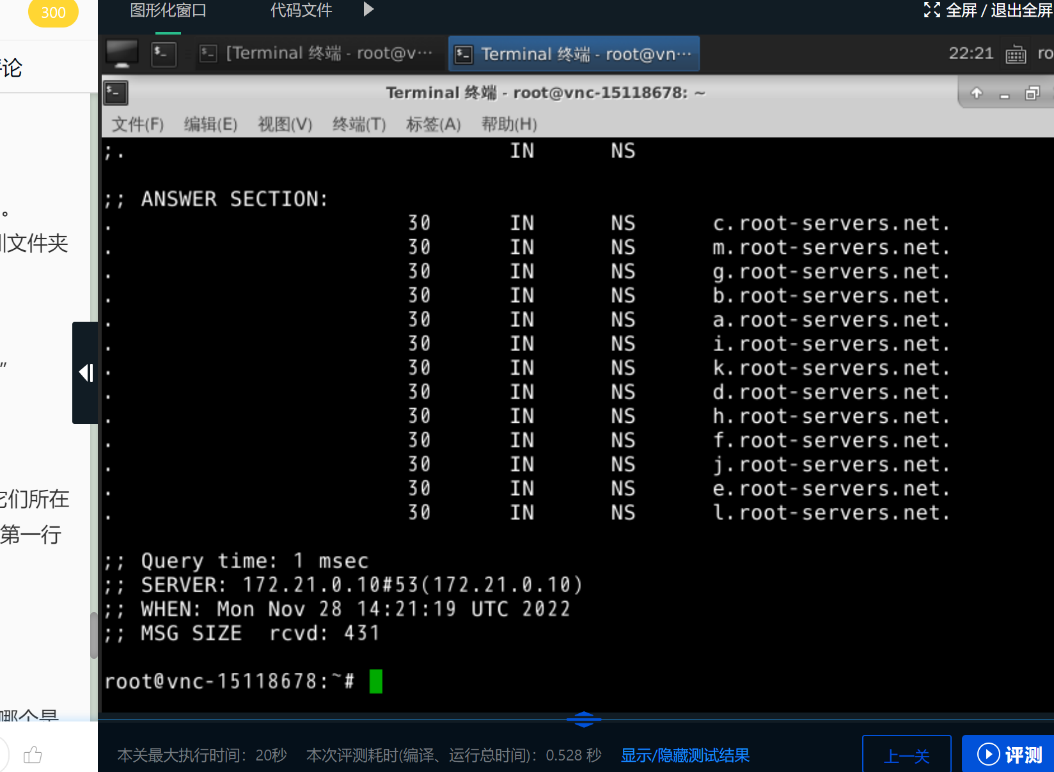
1. **从上图中可以看出:** www.educoder.net **的ip DNS服务器地址为172.21.0.10；**



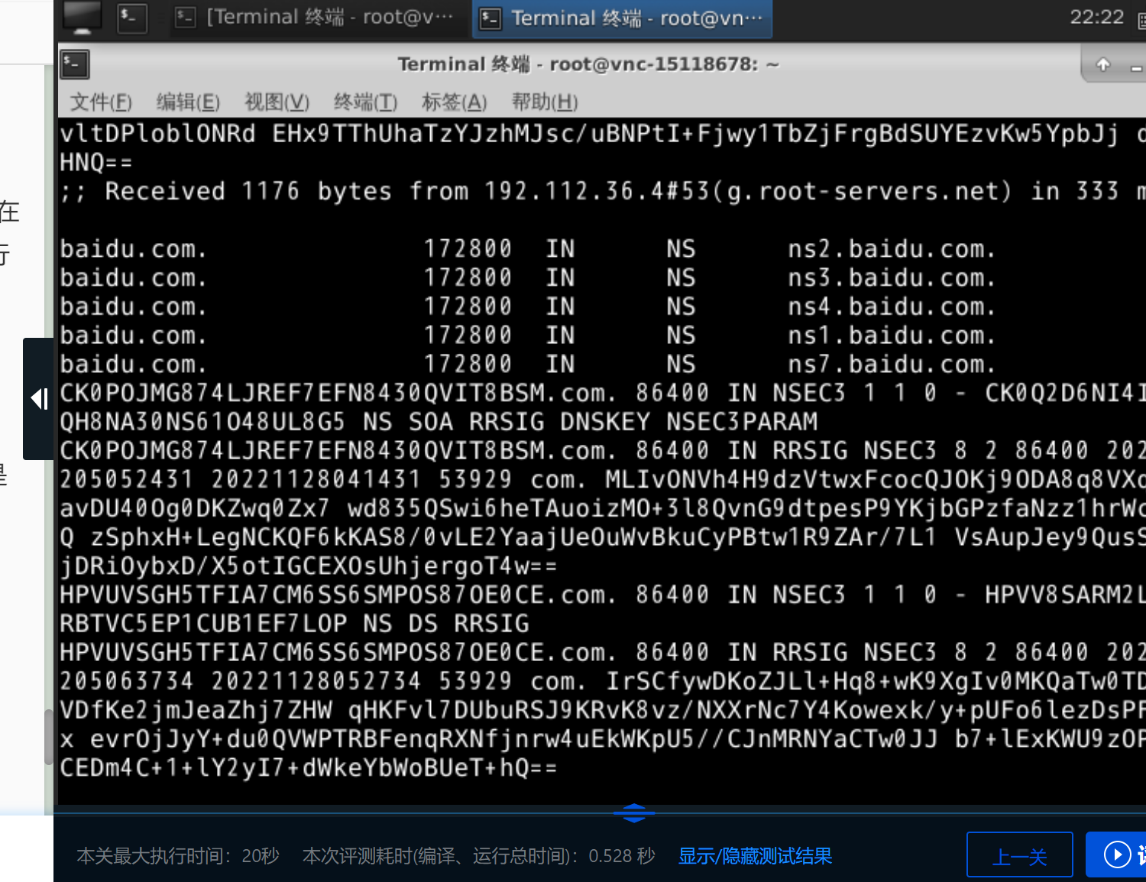
1. **qq.com区域的邮件服务器IP为**58.251.110.111 113.96.208.206 113.96.210.17 157.255.173.201

**第2关 域名解析过程与报文分析**

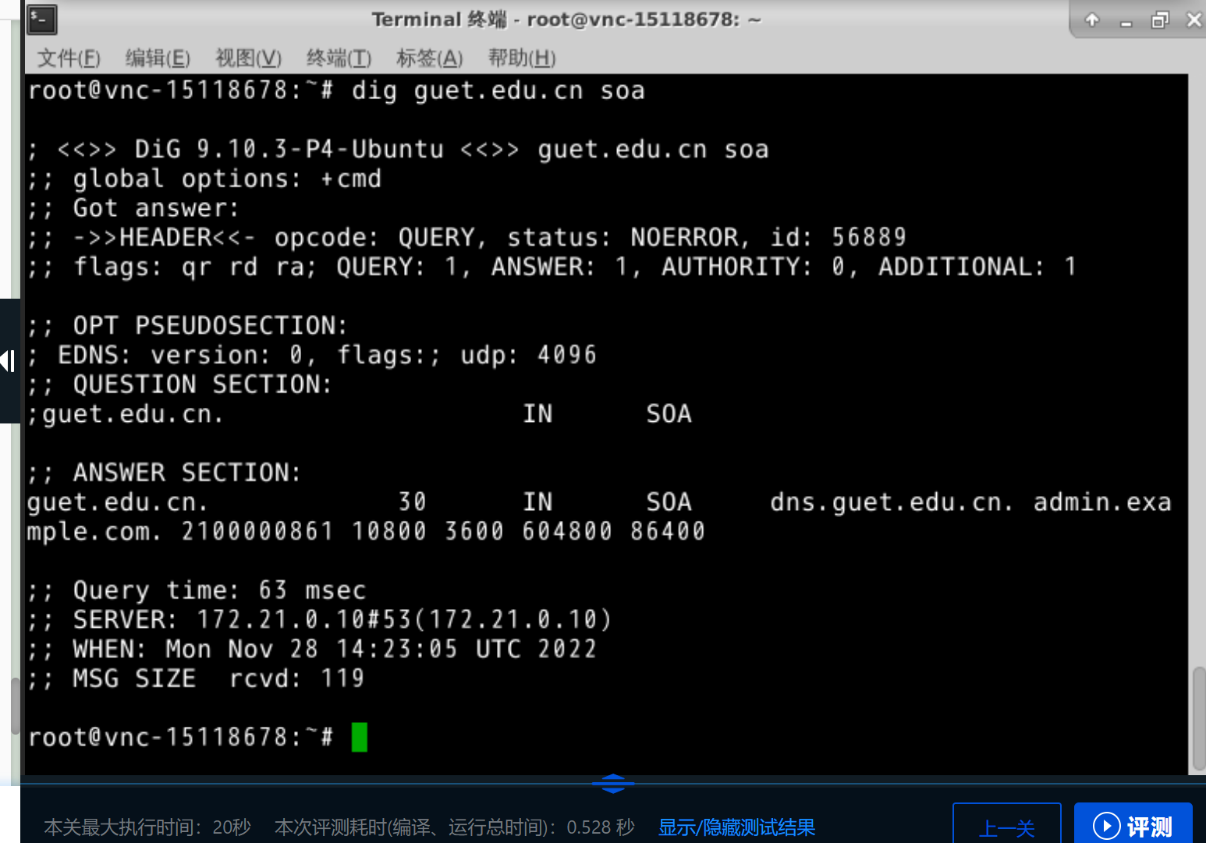
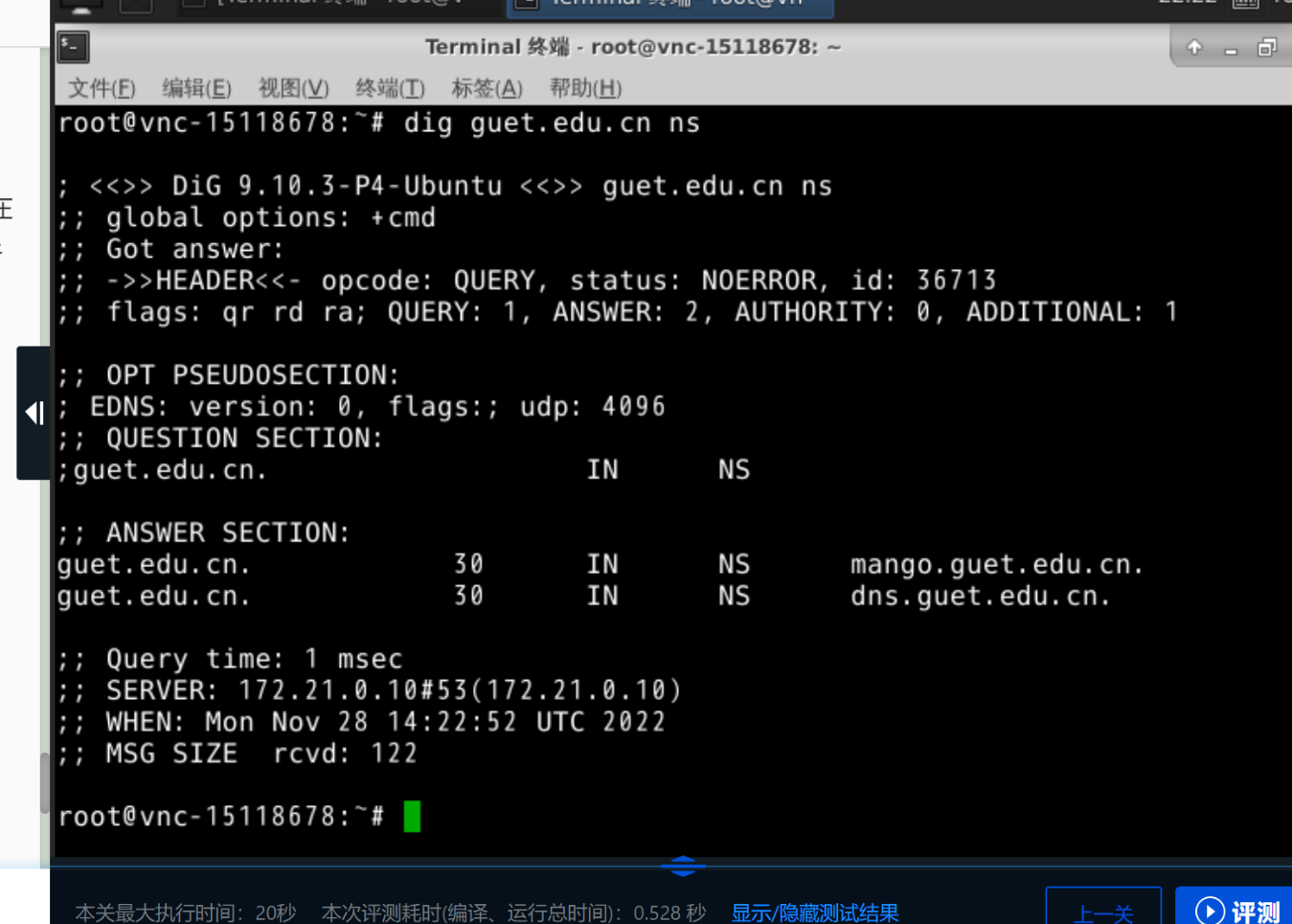
1. **查询INTERNET根域DNS服务器，执行命令：dig 如上图所示， 根域DNS服务器的个数有13个、以及它们所在网络区域的域名为：root-servers.net**



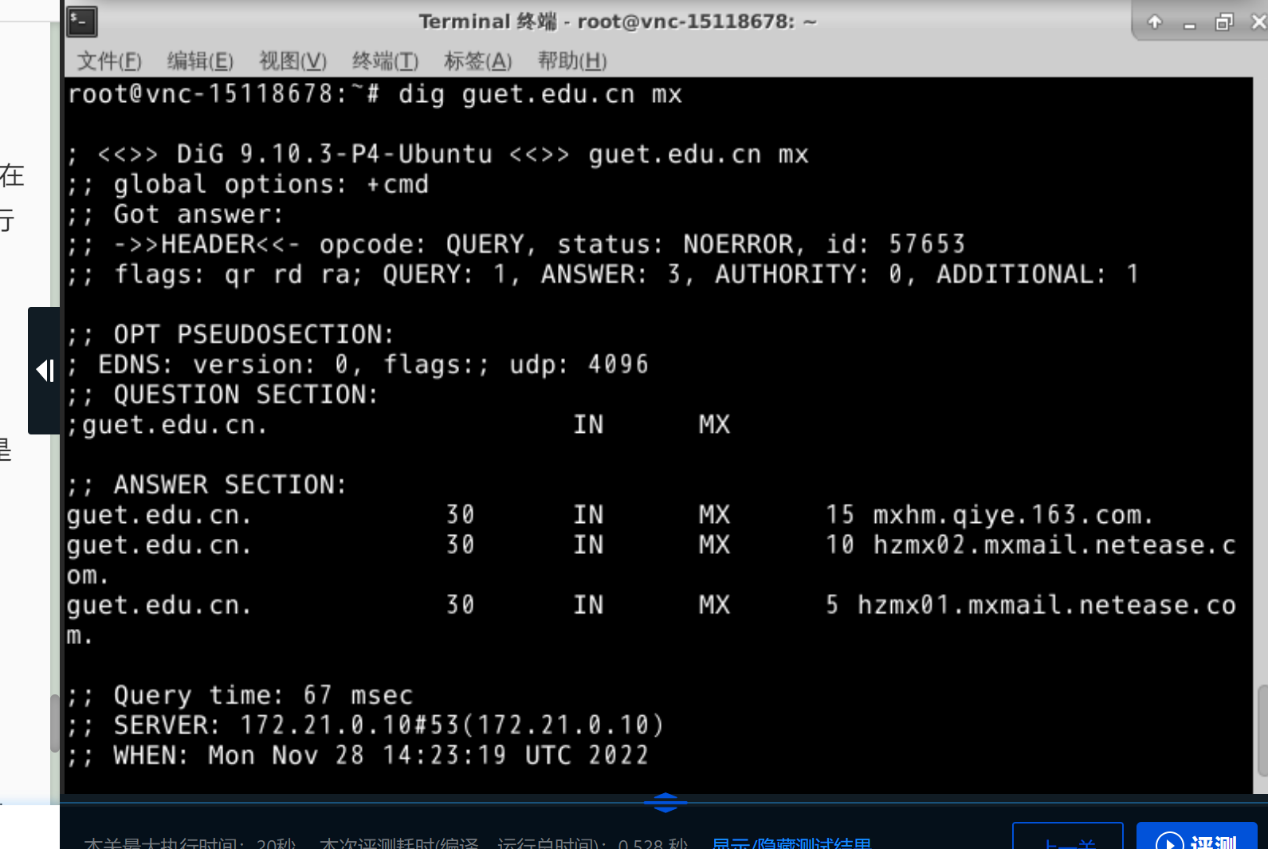
1. 执行命令：dig [www.baidu.com](http://www.baidu.com) +trace 如下图所示



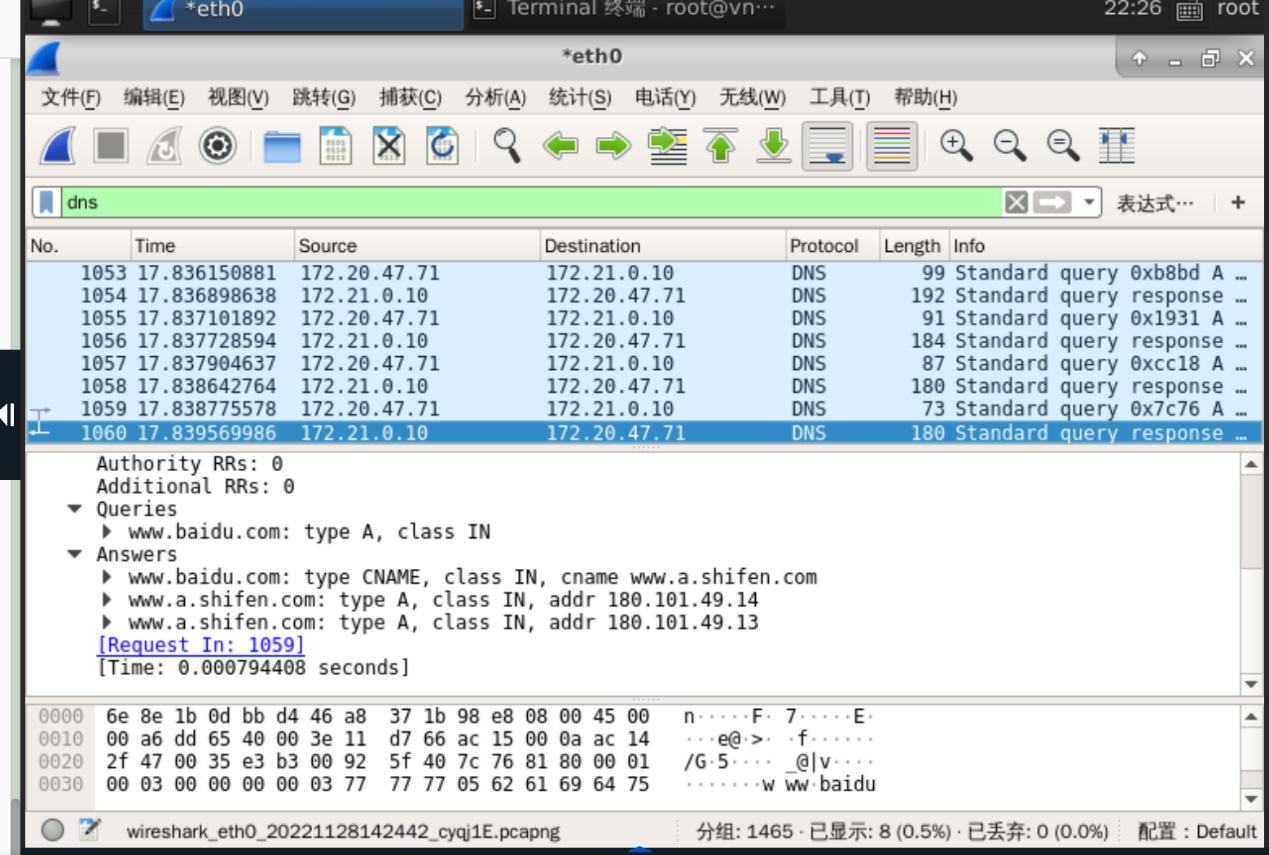
1. **执行命令：dig guet.edu.cn ns dig guet.edu.cn soa，如下图所示SOA表明主DNS服务器为：dns.guet.edu.cn**



1. **执行命令：dig guet.edu.cn mx ,可以分析有邮件服务器3个：**



1. **执行nslookup www.baidu.com，在 Wireshark 中停止捕获报文， 查看报文列表，可以看到成对的DNS 查询-响应报文。**



**其中**Queries Name为[www.baidu.com](http://www.baidu.com)；Answers有一个CNAME域名重定向，与返回的两个ip：180.101.49.14与180.101.49.13

1. **实验总结**

本次实验学习了域名解析与DNS协议分析，掌握了掌握域名解析工具nslookup用法，在第一关的时候，由于DNS所带解析参数过多需要逐个了解，理论课未涉及到详细内容但实验上花费了时间学习。第二关主要是了解了域名解析过程，过程也极为复杂，但学习了解析工具dig用法和DNS报文结构加深了我对DNS解析的了解。