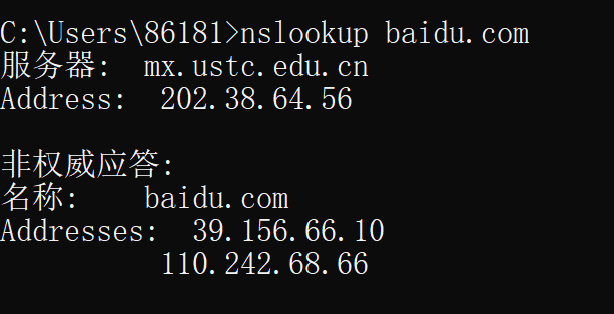
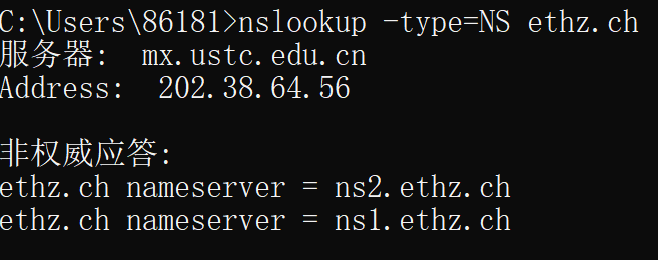
**DNS实验**

**陈鸿绪 PB21000224 10.3**

1. 运行nslookup获取任意一个亚洲Web服务器的IP地址。该服务器的IP地址是什么？



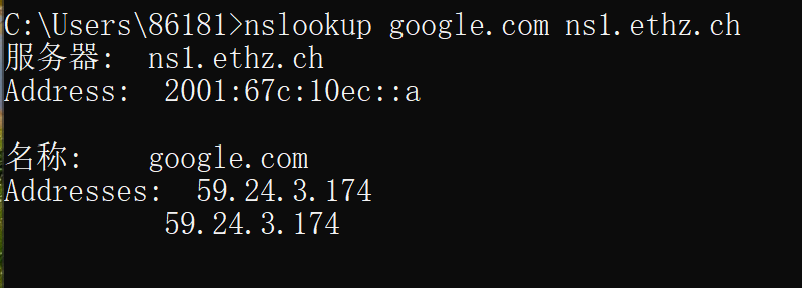
1. 运行nslookup以确定欧洲一所大学的权威DNS服务器。



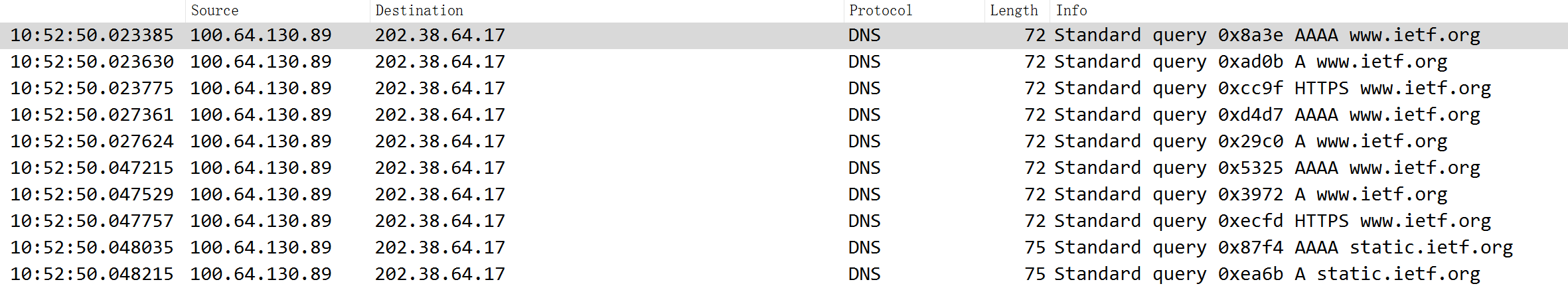
这里我们选取的欧洲大学是苏黎世联邦理工。

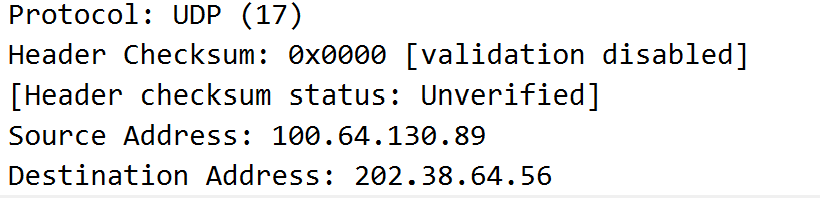
1. 运行nslookup，以便查询在问题2中获得的其中一个DNS服务器，以获取Yahoo！邮件的邮件服务器。它的IP地址是什么？

由于在2中我们获得的权威DNS服务器无法解析Yahoo，这里选取google.com:



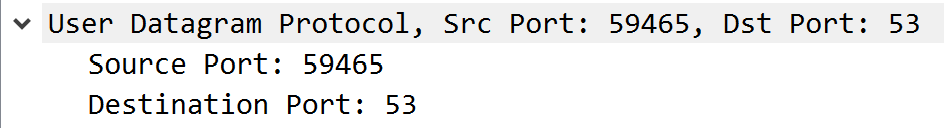
1. 找到DNS查询和响应消息。它们是通过UDP还是TCP发送的？

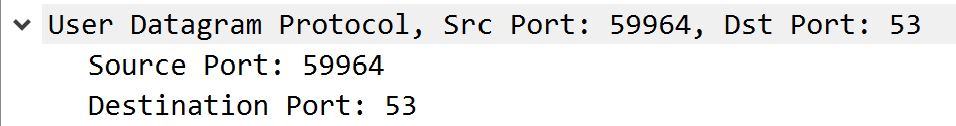


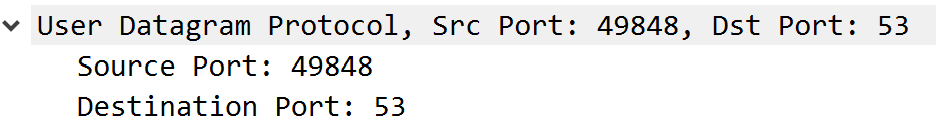


均经过UDP发送的。

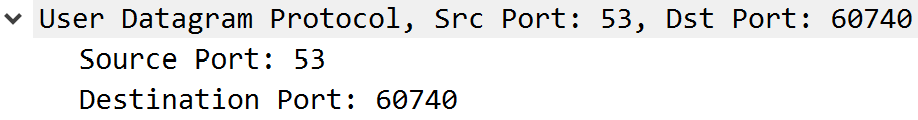
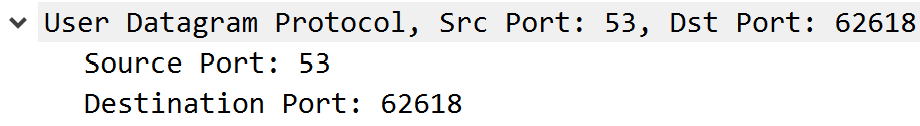
1. DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？







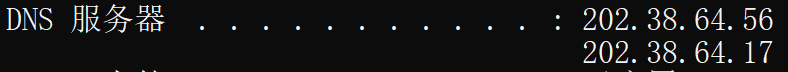
以上是一部分DNS的查询消息的端口展示，目标端口均为53。



以上是一部分DNS的相应消息的端口展示，相应端口均为53。

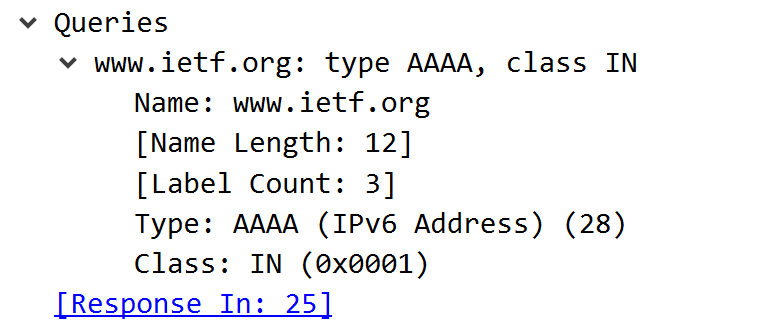
1. DNS查询消息发送到哪个IP地址？使用ipconfig确定本地DNS服务器的IP地址。这两个IP地址相同吗？

使用ipconfig -all指令：



在题四中可以发现DNS查询消息发送到了202.38.64.17，所以与上图中下方的IP地址相同。

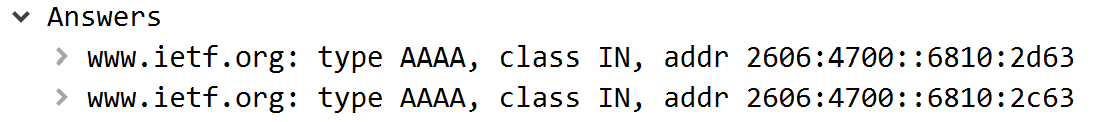
1. 检查DNS查询消息。它是什么“类型”的DNS查询？查询消息是否包含任何“answers”？



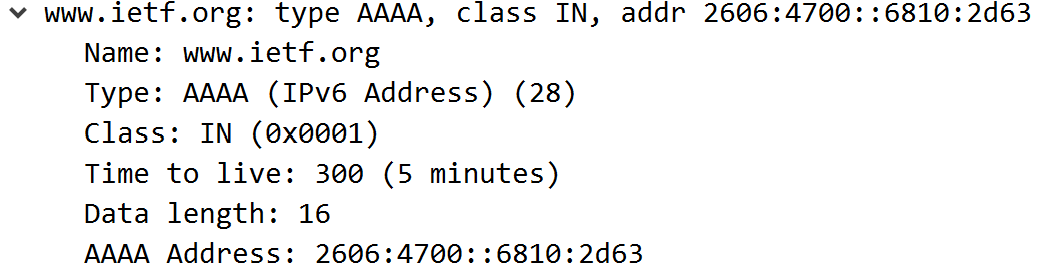
Type=AAAA 查询消息不包含任何形式的“answers”。

1. 检查DNS响应消息。提供了多少个“answers”？每个answers包含什么内容？

提供了两个答案：



其中一个答案包含了如下内容：



1. 考虑您的主机发送的后续TCP SYN数据包。SYN数据包的目标IP地址是否与DNS响应消息中提供的任何IP地址相对应？

后续SYN数据包的目标IP地址一定在DNS响应消息中提供的IP中。只不过由于IPv4与IPv6的原因不能直观显示出来。

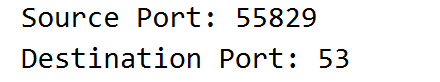
1. 此网页包含图像。在检索每个图像之前，您的主机会发出新的DNS查询吗？

不会，浏览器会缓存之前解析过域名的IP地址，IP地址一般不会变动。

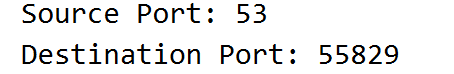
以下是使用nslookup [www.mit.edu](http://www.mit.edu)命令的实验：

1. DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

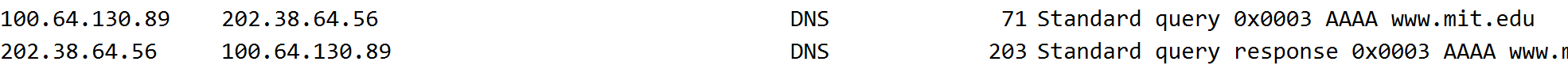
下面是DNS查询，目标端口为53



下面是DNS响应，源端口为53

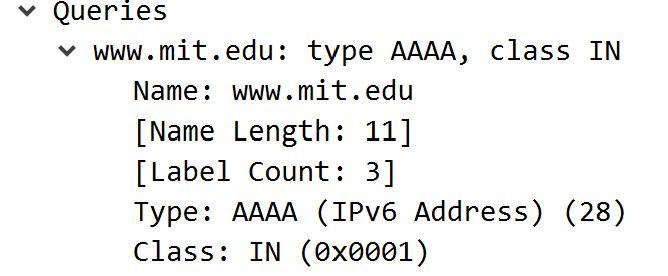


1. DNS查询消息发送到哪个IP地址？这是您默认本地DNS服务器的IP地址吗？



发送到了202.38.64.56地址。是本地DNS服务器IP地址。

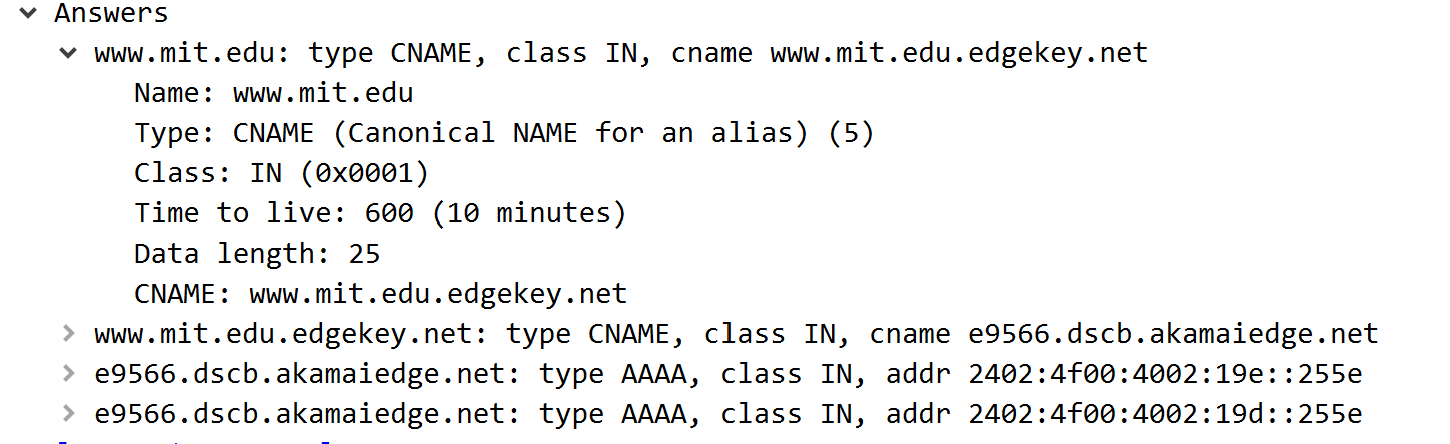
1. 检查DNS查询消息。它是什么“类型”的DNS查询？查询消息是否包含任何“Answers”？



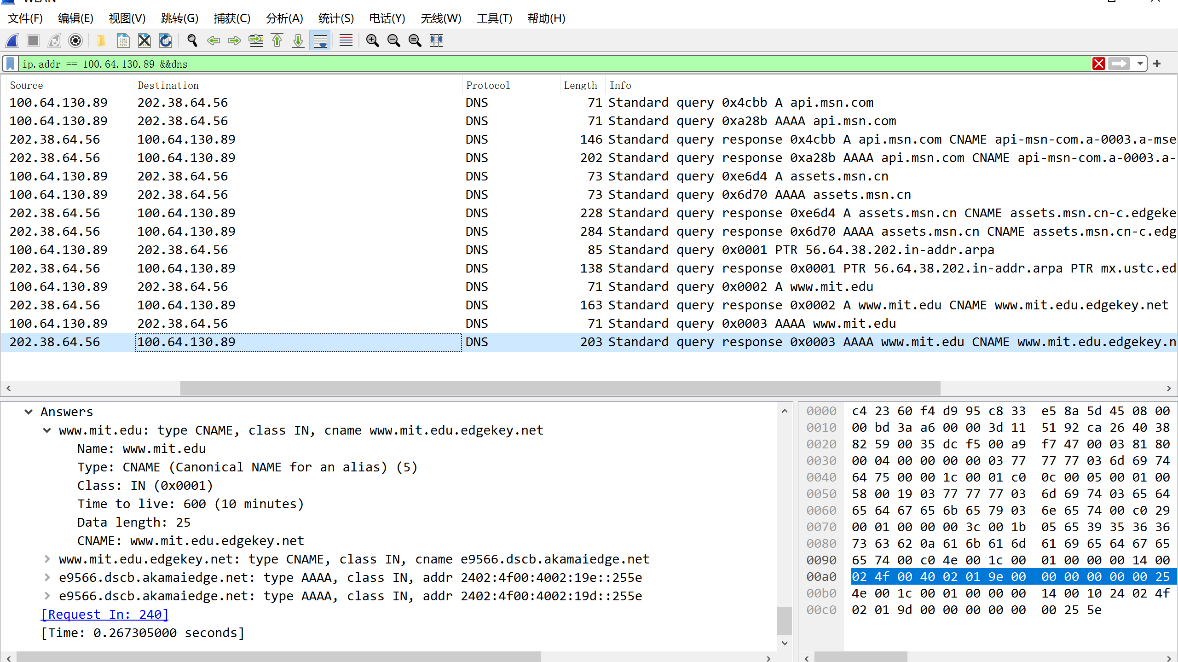
Type: AAAA 不包含任何Answers 。

1. 检查DNS响应消息。提供了多少个“Answers”？Answer包含什么内容？

提供了四个，其中一个Answer中的具体内容如下展示。



1. 提供一张屏幕截图

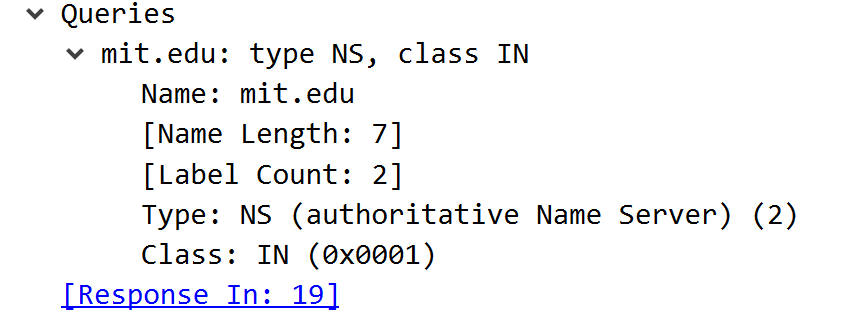


以下是使用nslookup –type=NS mit.edu命令的实验：

1. DNS查询消息发送到哪个IP地址？这是您默认本地DNS服务器的IP地址吗？

发送到了202.38.64.56地址。是本地DNS服务器IP地址。

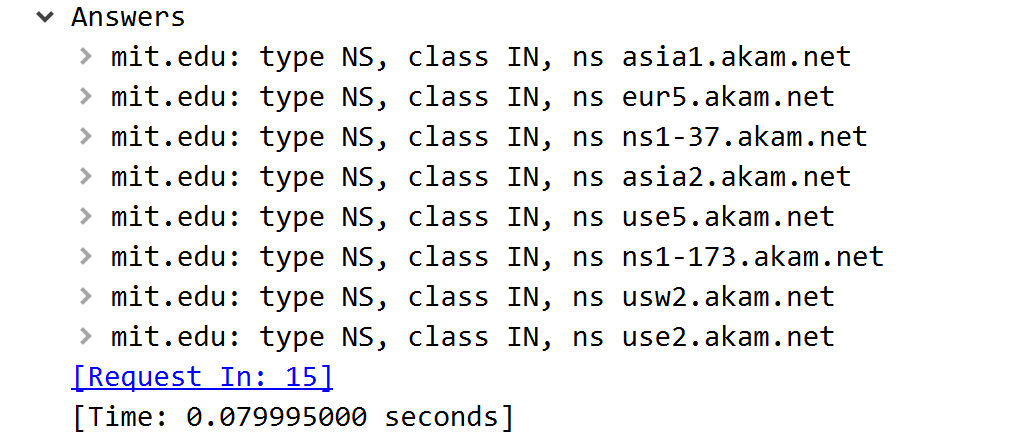
1. 检查DNS查询消息。它是什么“类型”的DNS查询？查询消息是否包含任何“Answers”？



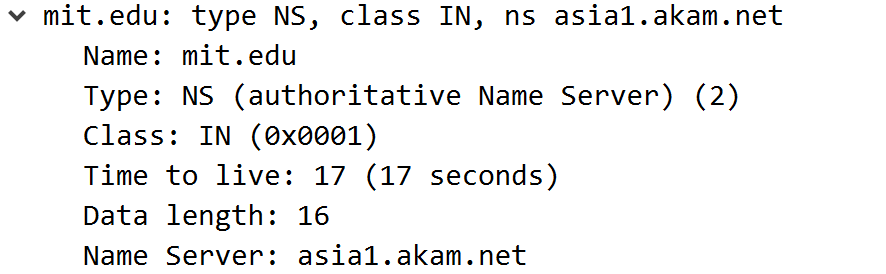
Type:NS 不包含任何Answers

1. 检查DNS响应消息。响应消息提供了哪些MIT名称服务器？该响应消息是否还提供了MIT名称服务器的IP地址？

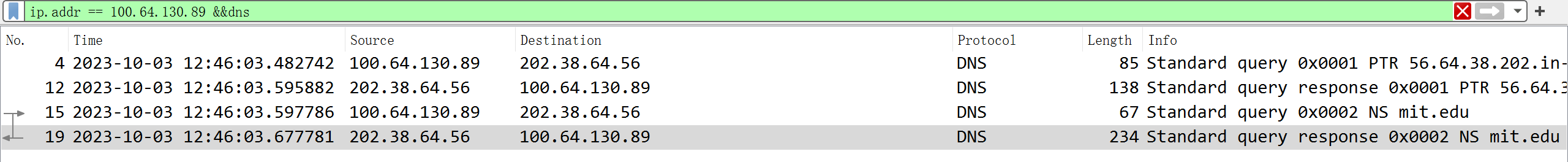
以下是提供的一些MIT服务器：



展开其中一个发现并没有提供IP地址：



1. 提供一张屏幕截图。

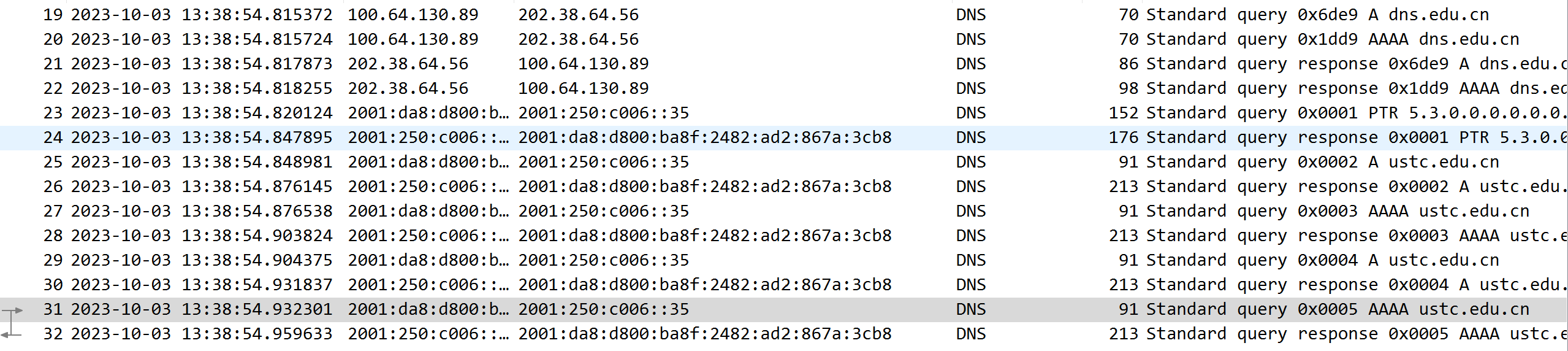


以下是使用nslookup ustc.edu.cn dns.edu.cn的命令实验

1. DNS查询消息发送到哪个IP地址？这是您默认本地DNS服务器的IP地址吗？如果不是，该IP地址对应的是什么？

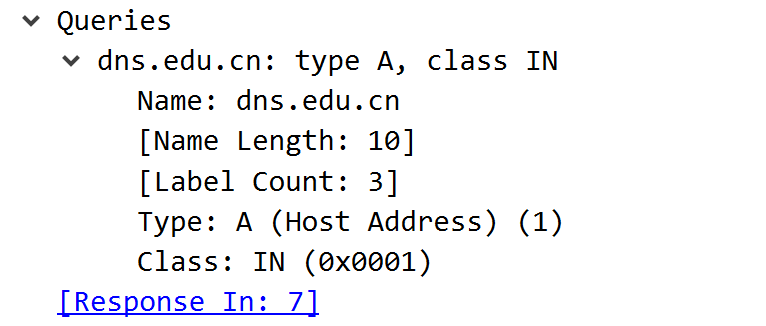
其中有一些发送到了202.38.64.56地址。是本地DNS服务器IP地址。

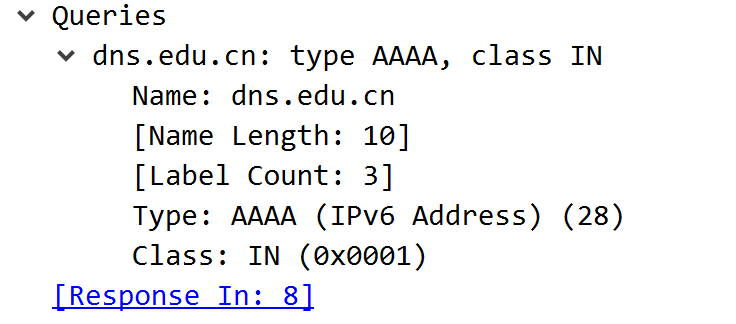
但是有些并不是上述IP地址，该IPv6地址对应的应该为dns.edu.cn。

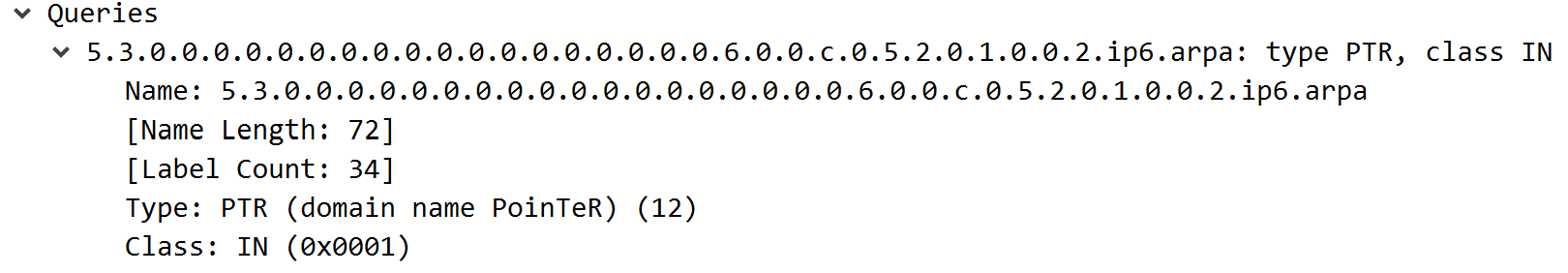


1. 检查DNS查询消息。它是什么“类型”的DNS查询？查询消息是否包含任何“Answers”？

这是选取的三个代表性DNS查询，一个type为 A，一个type为AAAA，还有一个为PTR，均不包含任何Answers。

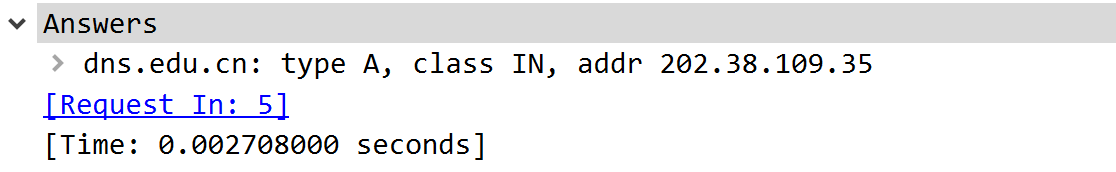


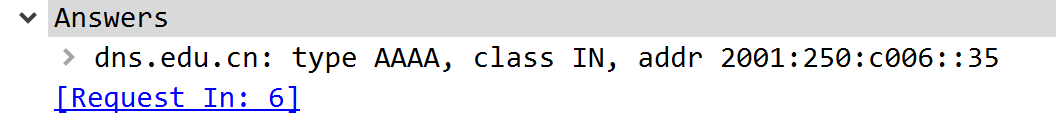


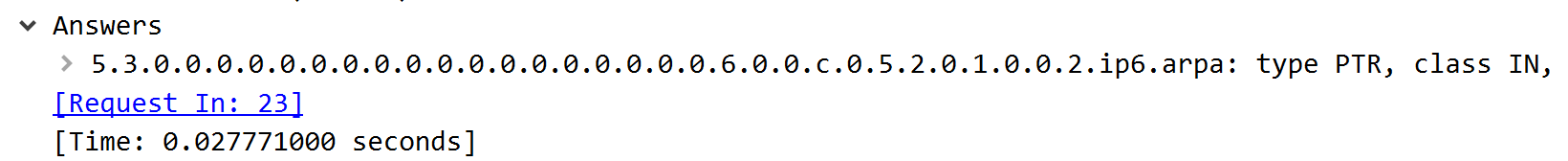


1. 检查DNS响应消息。提供了多少个“Answers”？每个Answer包含什么内容？

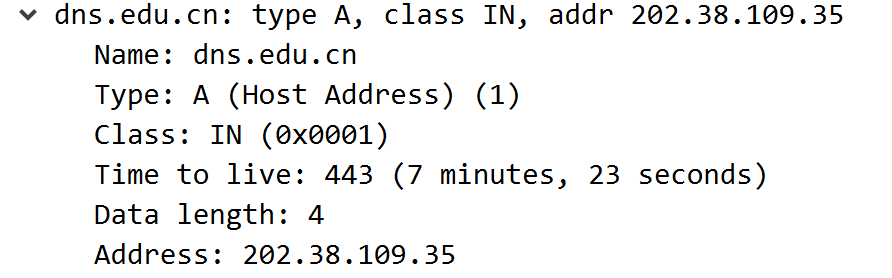
有的DNS响应有1个answer。



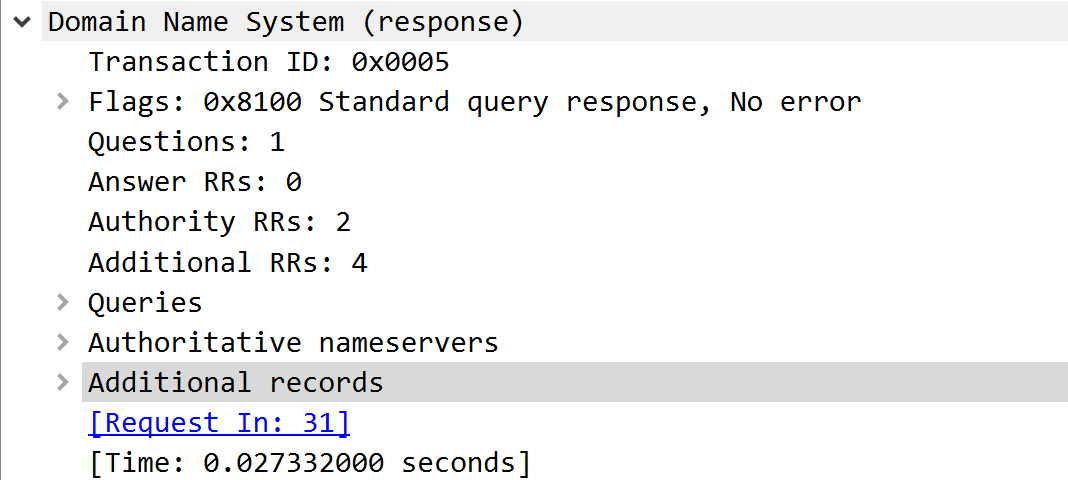




三个均每个提供一个答案，答案包含类似以下内容：



但是有的DNS响应报文中就并没有Answers，如下图所示：



并没有发现Answers的存在。

1. 提供一张屏幕截图。

