第一章作业

（1）

PROP =

TRANSP =

Latency=TRANSP+PROP=

（2）

PROP =

TRANSP =

Latency=TRANSP+PROP=

（3）

统计多路复用的核心思想是不需要将带宽提升至每一个数据流的峰值之和那么多，因为在真实的网络中流的峰值的出现具有突发性，是不平稳的，每个流的峰值可能出现在不同的时间，所以说可以将带宽设置在多个流的峰值之和以下以实现统计多路复用增益。

但是，如果网络中的数据流突然大规模出现，或者网络中多个流在一个时间段内都同时出现峰值，这就会导致统计多路复用后的带宽大小无法满足其共同传输的要求，可能会出现丢弃报文分组的情况出现。

所以说引入统计多路复用后，因为网络中流量的突发性以及不平稳，当数据量大规模同时出现时也会出现端到端延迟情况的出现，主要原因是数据在传输过程中可能被丢弃。

第二章作业

第一题：

查询域名的IP地址时出现了DNS服务器为Unknown的情况，查询了一下网上的资料是说没有配置域名的反向解析，我尝试了一下不太会，而且我觉得他返回的Address也不太对于是采用了一个新的办法。



于是我换了一个方法：将域名服务器切换到谷歌的开放dns服务器上，输入命令"server 8.8.8.8"，再做域名的解析就可以得到我们需要的答案了

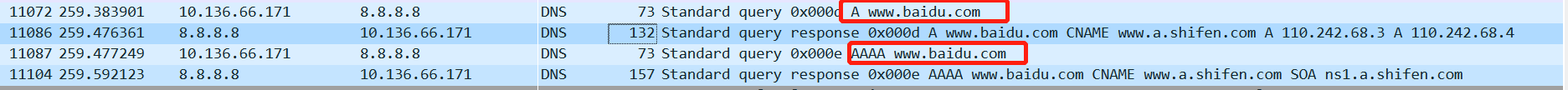


第一部分是本机使用的DNS服务器的信息，客户端先到主DNS Server进行连接查询

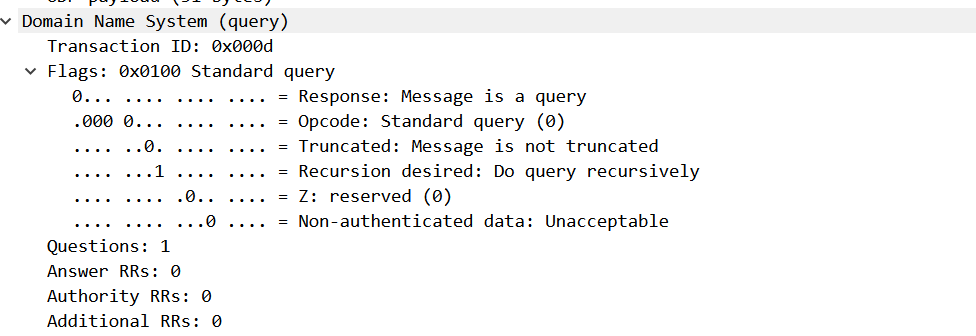
第二部分内容给我们返回了“非权威应答”。非权威应答的意思是假设某个DNS服务器没有域名www.baidu.com的信息，当有客户端通过它请求百度的ip地址时会通过反复解析或者递归解析的方式从欧诺个实际存储域名-ip对应关系的DNS服务器中获取baidu的域名信息，获得后再反馈给客户端，同时，该域名服务器也会将记录信息放在缓存中，如果再其失效前再有客户端访问就可以直接返回给客户端。

第三部分内容我们可以首先看到了一个www.a.shifen.com，这说明一个网站很多时候都不止有一个域名，可能会拥有很多备用域名。上网查找了一下资料：www.a.shifen.com[是百度原来的域名,百度原来就叫十分网,因为点击量每点一下赚10分钱,现在作废了。然后可以看到nslookup返回了两个ip地址，也就是一个域名可能会对应多个ip地址，但是在用户对某一域名发起访问时只会对应到一个ip地址，但是在不同时间不同地点访问同一个域名可能会反馈回不同的ip地址。服务器会根据路由器中跳数最小的IP地址作为用户一次访问时的IP地址，这样做不仅可以保证提升访问效率，也可以通过多个](http://www.a.shifen.com是百度原来的域名,百度原来就叫十分网,因为点击量每点一下赚10分钱,现在作废了。然后可以看到nslookup返回了两个ip地址，也就是一个域名可能会对应多个ip地址，但是在用户对某一域名发起访问时只会对应到一个ip地址，但是在不同时间不同地点访问同一个域名可能会反馈回不同的ip地址。服务器会根据路由器中跳数最小的IP地址作为用户一次访问时的IP地址，这样做不仅可以保证提升访问效率，也可以将几个)ip地址映射提升系统的鲁棒性。最后一个Aliases顾名思义，就是别名的意思，是目标域名的别名。

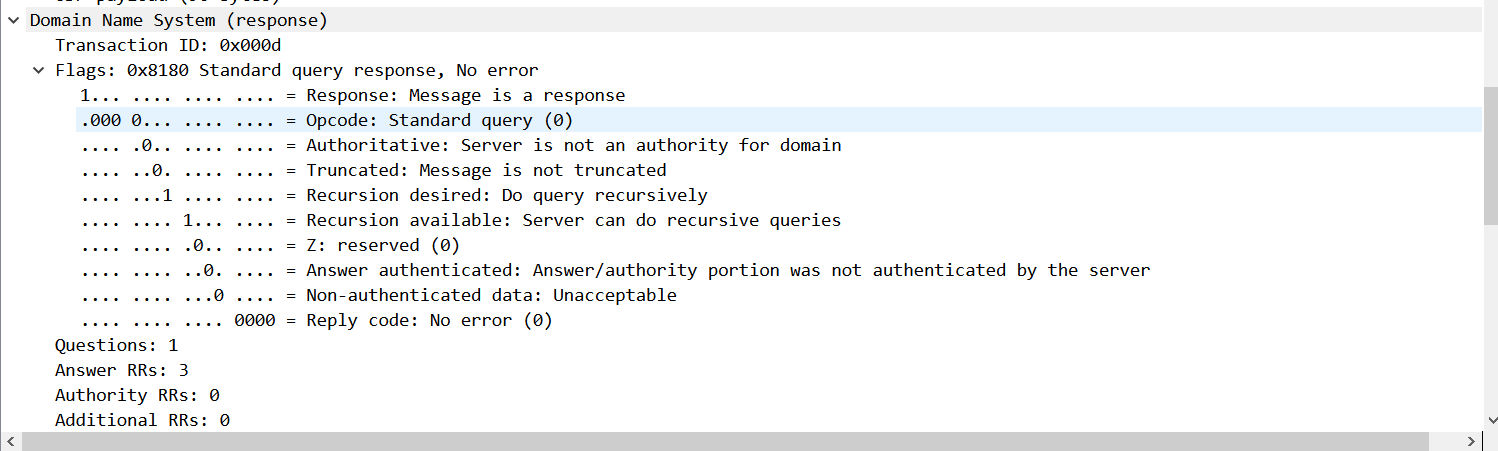
然后我们来使用wireshark来捕获本次的查询结果，可以看到主机向google DNS提交了两次域名解析的请求，第一次是A [www.baidu.com，第二次是AAAA](http://www.baidu.com，第二次是AAAA) www.baidu.com,两次的区别在于A是解析IPV4地址，第二次是请求解析IPV6地址



DNS的请求包头部：TransactionId是事务的ID，Flags是报文中的标志字段，Response字段为0是因为这个包是一个请求包，OPCOODE为零代表着标准查询，Truncated是TC字符安，Recursion是RD字段，reserved保留位为0，Questions问题计数为1，其余的回答资源记录数、权威名称服务器计数以及附加资源记录数均为0



DNS的响应包头部：事务ID与发出时的事务ID相对应，报文中的标志字段为返回，并且没有错误，QR字段为1表示一个响应包，AA字段、TC字段、为0，RD和RA字段均为1，并对一个问题返回了3个回答。

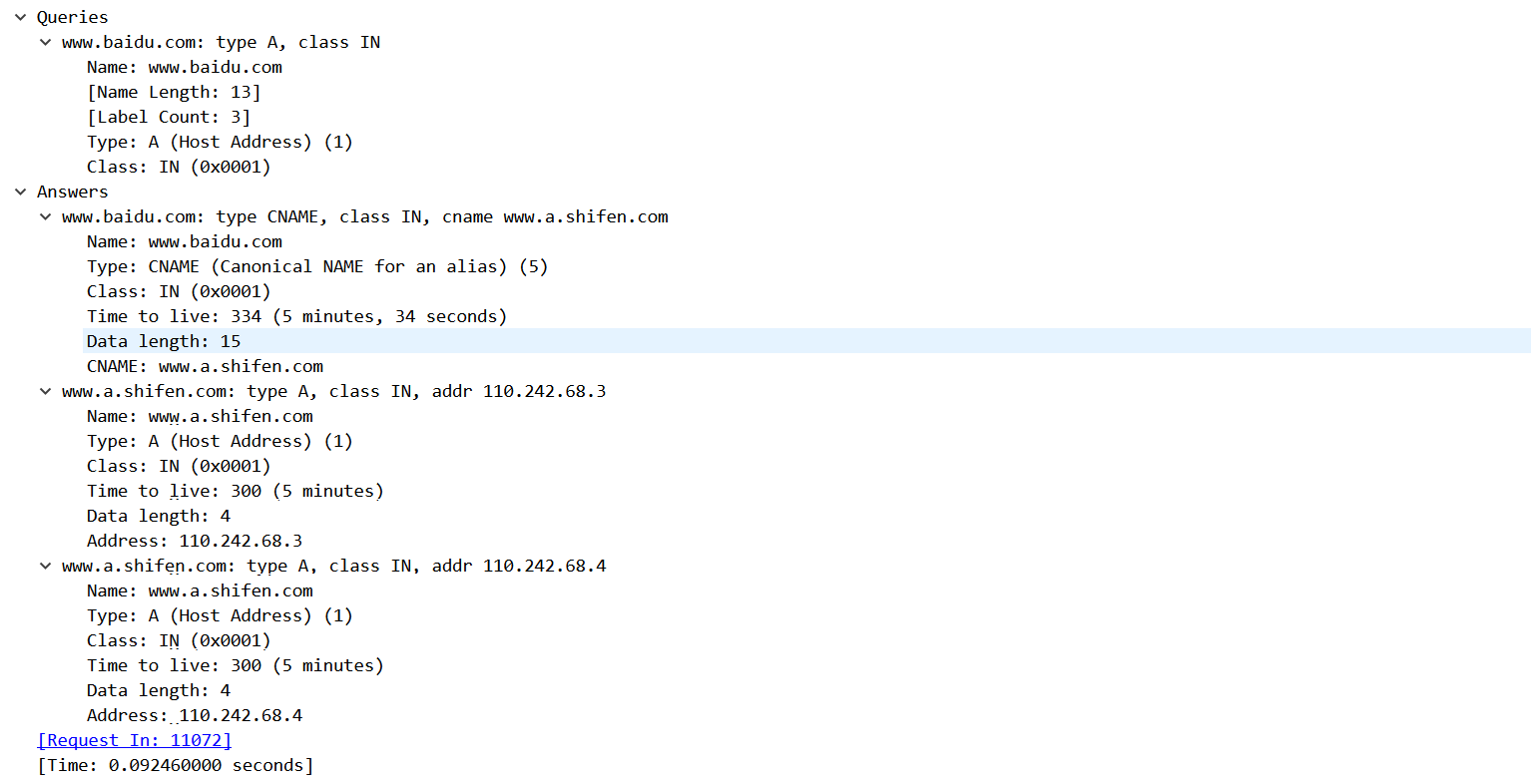


然后我们以IPV4的地址解析为例分析google DNS返回的内容：

首先，第一条回答的别名为CNAME，表示这一个键值对返回的是域名的别名，也就是我们在命令行窗口处看到的名称www.a.shifen.com

接下来两条得到的类型都为A，也就是解析了32位的IPV4地址，分别解析出来了这个域名所对应的两个ip地址。

其他的一些参数例如Time To Live代表了有效时间，Data Length代表了数据的长度，Class In表示在新特网上搜索

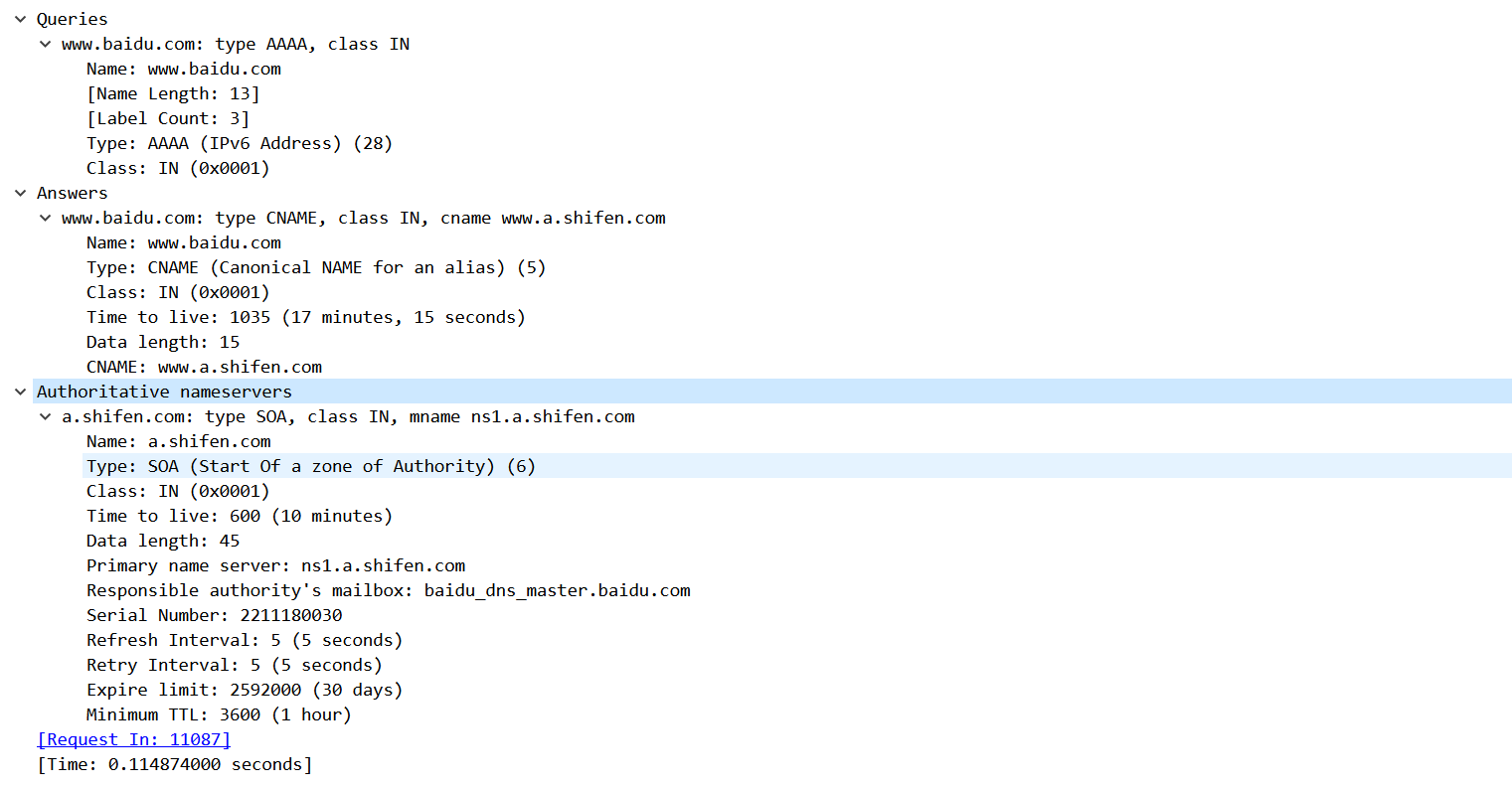


而在对IPV6的解析中看到了更加丰富的内容：在回答中出现了Authoritative nameservers，我在网上也找到了关于授权服务器的定义，与理论课上学习的基本一致：DNS名称服务器保存着域名空间中部分区域的数据。如果[DNS服务器](https://baike.baidu.com/item/DNS%E6%9C%8D%E5%8A%A1%E5%99%A8/8079460" \t "https://baike.baidu.com/item/%E5%90%8D%E7%A7%B0%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)负责管辖一个或多个区域时，称此DNS服务器为这些区域的授权服务器（Authoritative NameServer）。名称服务器 （Name Server）资源记录用于标记被指定为区域权威服务器的DNS 服务器。通过在 NS 资源记录中列出服务器，其他服务器就认为它是该区域的权威服务器。

SOA代表着区域数据库的开始，描述负责区域的域名服务器、版本信息以及从属域名服务器备份时的一些参数。

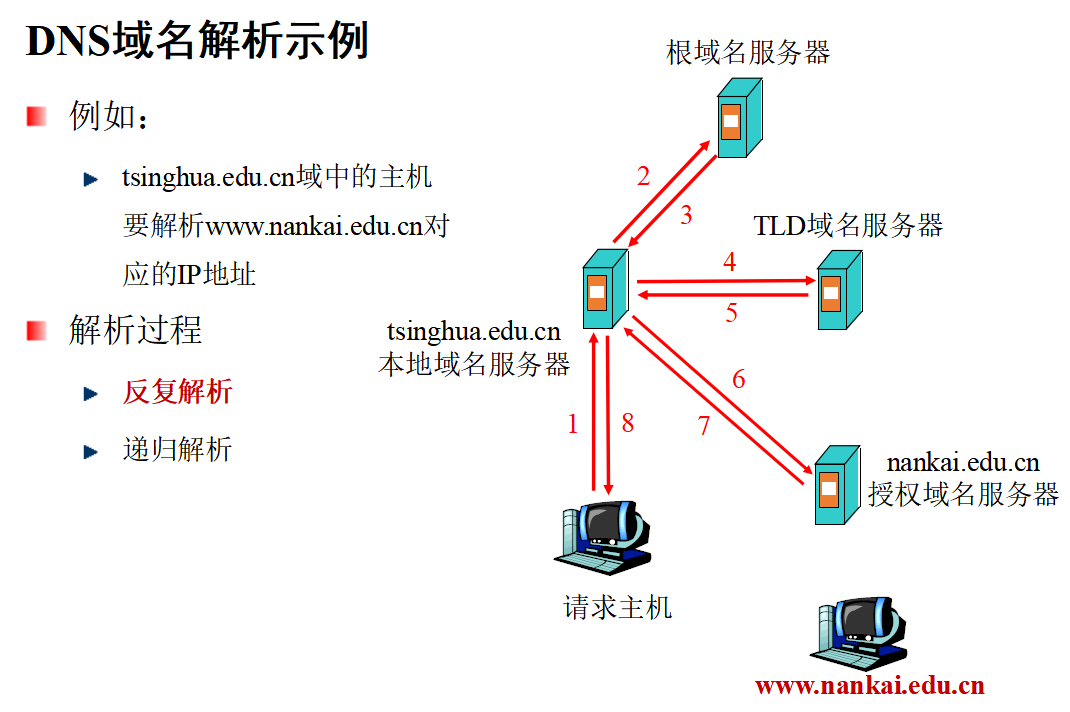
主要名称服务器：主要名称服务器（PrimaryNameServer），它保存着区域中的相关设置数据，当区域中的数据更改，如添加主机时，这些更改就被保存到主要名称服务器中。

Responsible authority’s mailbox表示负责人（管理员）的邮箱等一些其他的信息，因为涉及到授权服务器，所以信息也比非授权的服务器要丰富些。



第二题：

1. 以反复解析为例分析域名解析的基本过程



以ppt上的图为例说明DNS的解析过程。

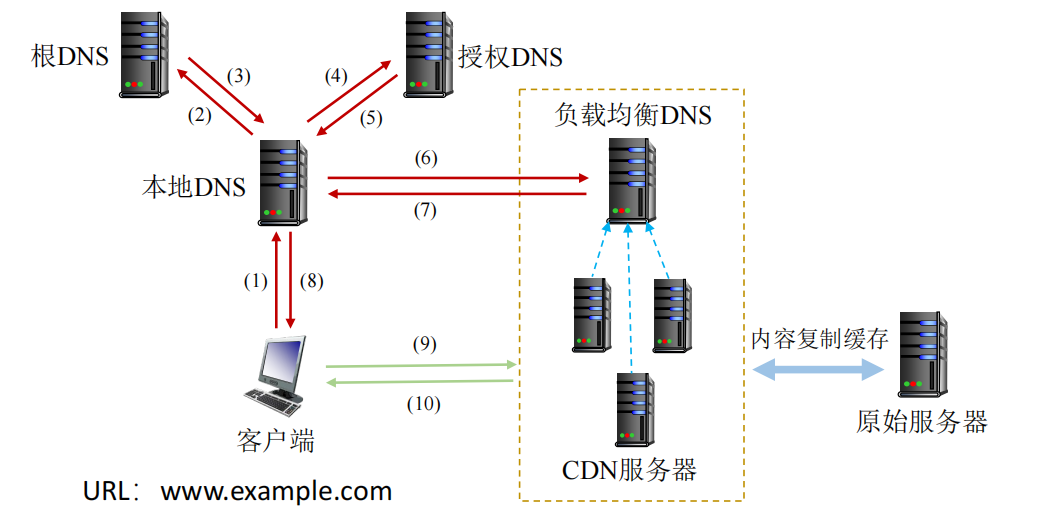
首先，请求主机向本地域名服务器发起请求，本地域名服务器查看是否有该域名到IP地址的映射，如果有且未过期直接返回，如果没有就发给根域名服务器。

根局域名服务器是最高层级的域名服务器，根服务器知道所有顶级域名服务器的域名和ip地址，根域名服务器会向本地域名服务器发送负责该域名解析的TLD域名服务器地址。如果根域名服务器存在域名到ip的映射且未过期则直接返回ip地址。

顶级域名服务器负责管理管理在该顶级域名服务器注册的所有二级域名，当收到本地域名服务器的请求时给出相应的回答，这个回答可能是一个授权域名服务器的地址，也可以因为有未过期的缓存而直接返回正确的域名对应的ip地址。

授权域名服务器是对于名字与地址映射，保留其初始数据来源的服务器，用来保存所有其所管辖的主机域名到ip地址的映射，授权域名服务器会将解析的结果返回给本地域名服务器，再由本地域名服务器传递给请求主机

（二）给出内容分发网络（CDN）中DNS重定向的基本方法，说明原始资源记录应该如何修改，并描述重定向过程



在内容分发网络中，客户端的解析请求将首先被发送至本地DNS，如果本地DNS无法根据缓存完成域名解析，本地DNS会将请求发送至根DNS，并由DNS返回一个授权DNS的IP地址，并由该IP地址给出负载均衡DNS的IP地址。

负载均衡DNS负责决策CDN服务器选择，负载均衡DNS需要收集CDN服务器的位置和负载情况，如果找不到被请求的对象，需要从原始服务器获取。负载均衡DNS会根据下属各个CDN服务器服务器的工作状况以及传输效率等因素综合考量，返回给本地DNS一个最合适的CDN服务器的IP地址，本地服务器会将该IP地址返回给客户端。

客户端将通过该IP地址定位到一个CDN服务器并根据该CDN服务器与原始服务器的交互进行域名解析或者根据缓存进行域名解析，最后返回的值完成对域名的解析。

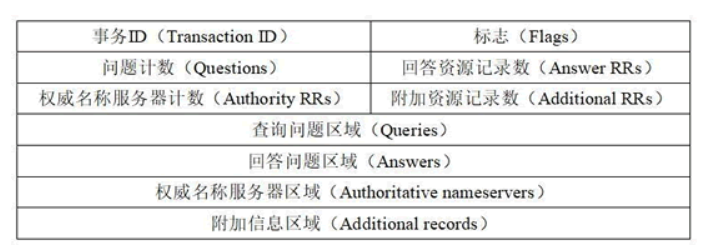
第三题：

在DNS域名系统中，域名解析时使用UDP协议提供的传输层服务（DNS服务器使用UDP的53端口），而UDP提供的是不可靠的传输层服务，请你解释DNS协议应如何保证可靠机制。

DNS协议的可靠机制可以由应用层来保障。具体保障的手段可以参考TCP所使用的校验和验证（差错重传）以及超时重传。例如在应用层进行校验和的计算并且根据发送的域名解析请求进行计时，如果超时则再次重复进行域名解析请求。

除此之外还要充分利用DNS数据包的特殊结构来帮助我们完成检测，比如说：在之前的wireshark抓包中，我们可以看到两处被标明了No error，分别在Flags位置以及Reply Code的位置，我们可以根据数据包头部的标志位以及ReplyCode来判断数据是否可能存在破损，例如，一个请求数据报的OPCode应该是1，根据这样的检测也可以检测出数据报是否可能存在传输时的差错。

并且，仔细观察其头部：



DNS数据报的头部记录了问题的计数、回答资源记录数等等，可能通过这些信息于世界查询问题区域的数量进行比较来判断是否可能存在差错或者丢包的发生。

最后，因为UDP不是面向连接的通信方式，所以在发送消息之前不需要进行连接确认，所以说如果DNS服务器损坏，将会造成大量域名无法解析的情况发生，于是DNS体系也在不同区域范围内部署多台冗余服务器来避免单点丢失，弥补UDP的劣势。