**DNS的工作原理及递归和迭代解析过程**

[](https://www.zhihu.com/people/bai-ge-46-41)

[**百哥**](https://www.zhihu.com/people/bai-ge-46-41)

网络工程师/云计算工程师/创业者

​关注他

24 人赞同了该文章

**什么是DNS？**

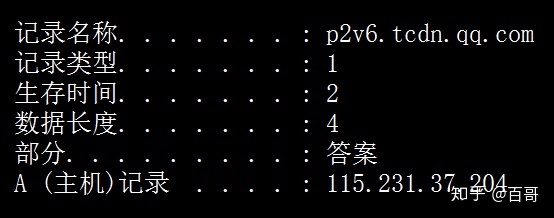
DNS（Domain Name System）域名系统，简单点来说，就是当我们在浏览器输入一个网址，需要有一台DNS服务器帮我们解析成IP地址，我们才能打开这个网站。

**dns解析的过程是这样的**

**第一步：输入域名后，电脑首先看自己有没有对应域名的缓存，有缓存就直接用缓存里的ip访问。**

在windows的命令行下可以看到现有的dns缓存

C:\Users\hubaixin>ipconfig /displaydns

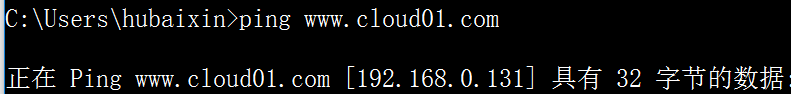
其中1条缓存

**第二步，如果缓存中没有，则去查询hosts文件，hosts文件在这里**

c:\windows\system32\drivers\etc\hosts

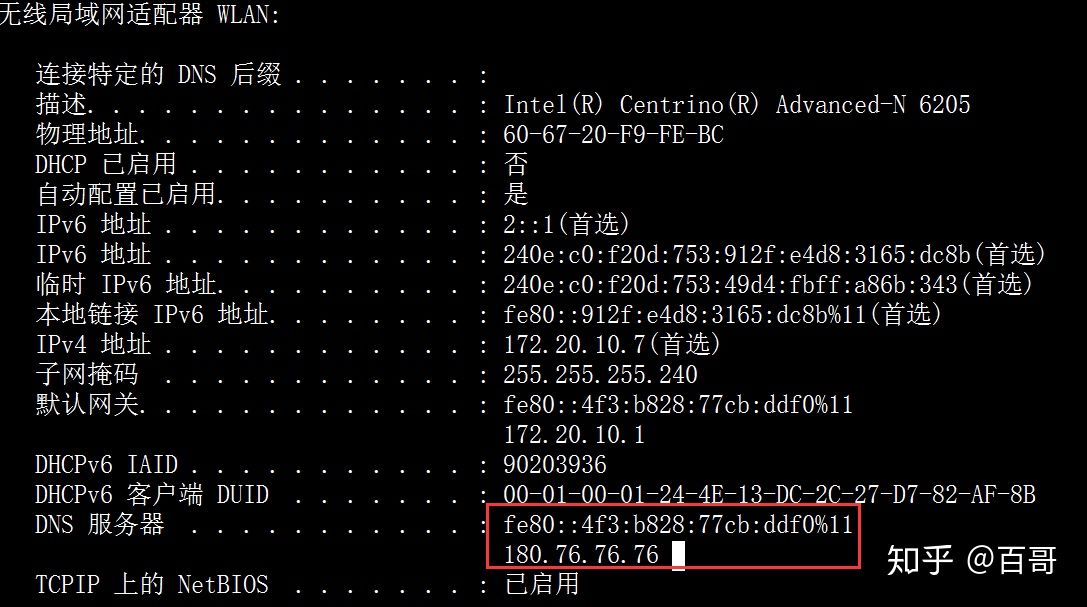


如图，现在这台电脑的hosts文件里有两个记录，那么这两个域名可以直接从hosts文件里读取



**第三步，如果hosts文件里也没找到想解析的域名，则将域名发往自己配置的dns服务器，也叫本地dns服务器**

在windows命令行ipconfig/all可以看到自己的本地dns服务器，如图



**第四步，如果本地dns服务器有相应域名的记录，则返回记录。**

电脑的dns服务器一般是各大运营商如电信联通提供的，或者像180.76.76.76，223.5.5.5，4个114等知名dns服务商提供的，本身缓存了大量的常见域名的ip，所以常见的网站，都是有记录的。不需要找根服务器。

**第五步，如果电脑自己的服务器没有记录，会去找根服务器。根服务器全球只要13台，回去找其中之一。**

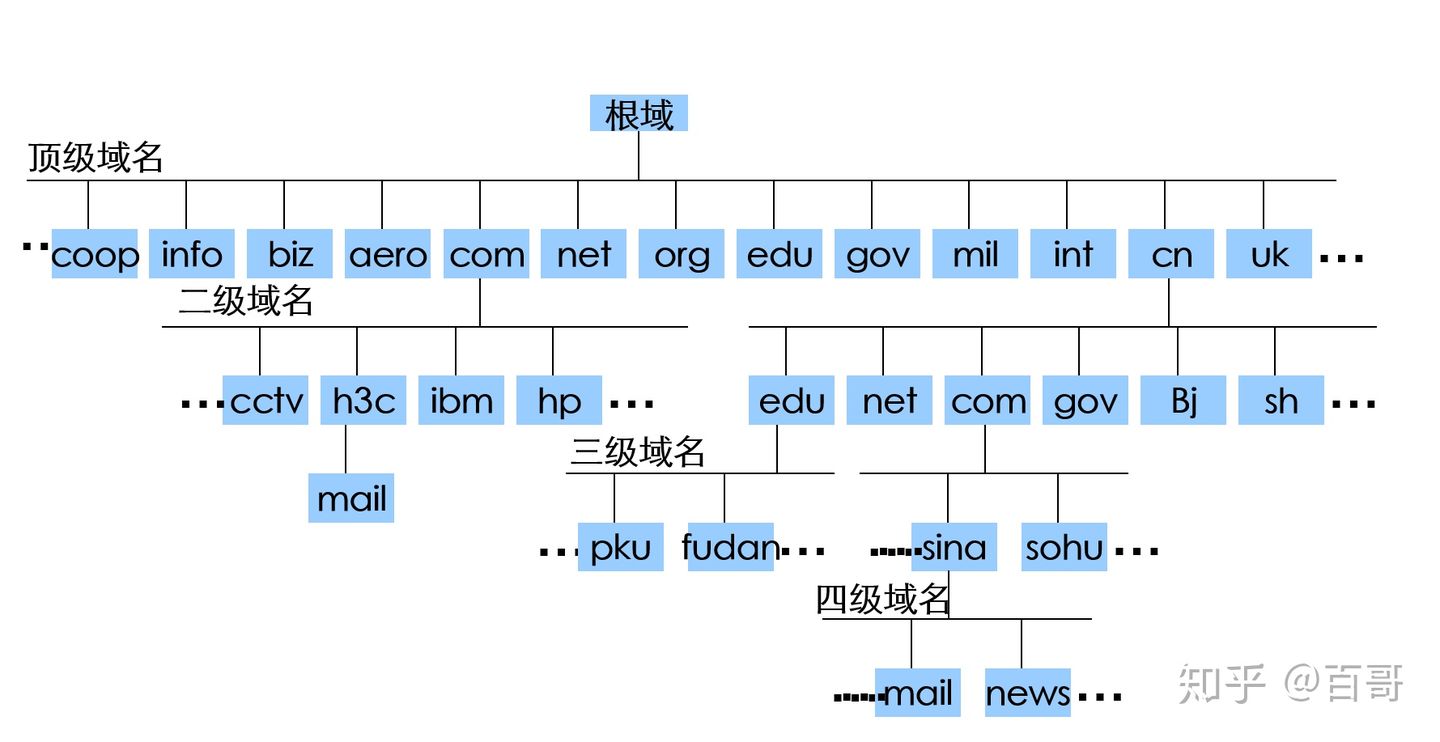
**找了根服务器后，根服务器会根据请求的域名，返回对应的“顶级域名服务器”，如：**

如果请求的域名是[http://xxx.com](https://link.zhihu.com/?target=http%3A//xxx.com" \t "_blank)，则返回负责com域的服务器

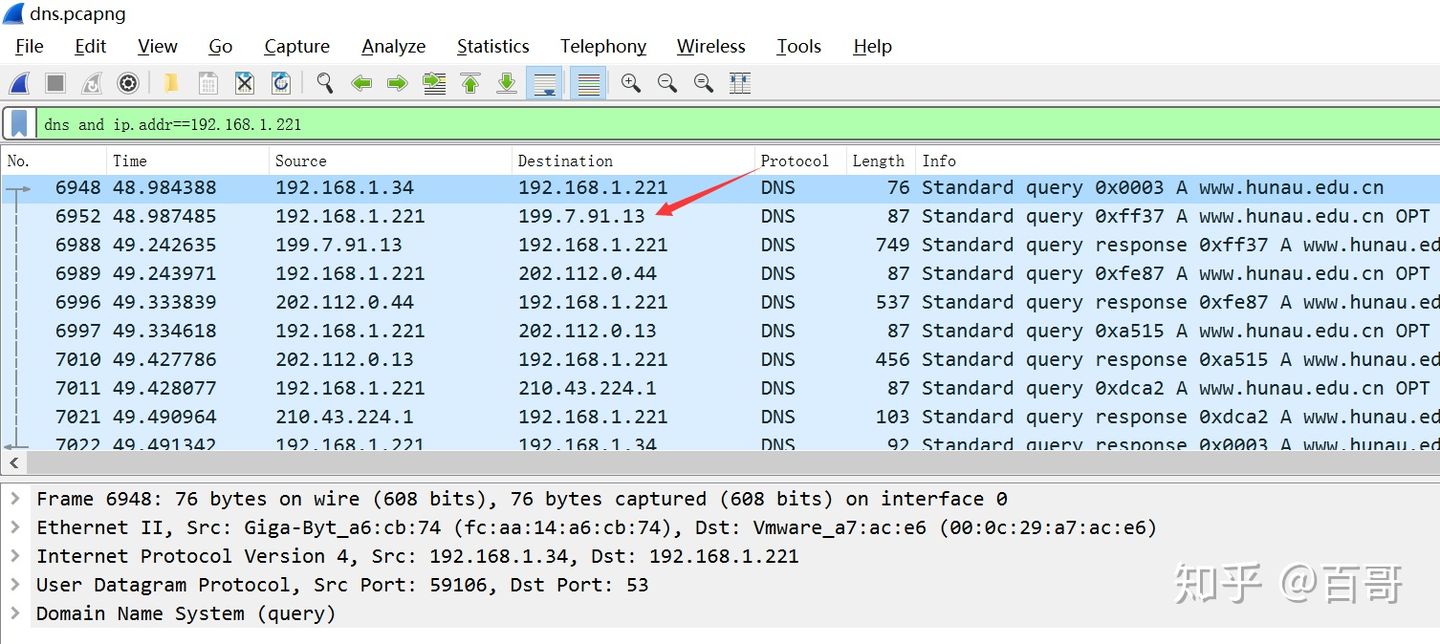
如果是[http://xxx.cn](https://link.zhihu.com/?target=http%3A//xxx.cn)，则发给负责cn域的服务器

如果是[http://xxx.ca](https://link.zhihu.com/?target=http%3A//xxx.ca)，则发给负责ca域的服务器

常见的顶级域有

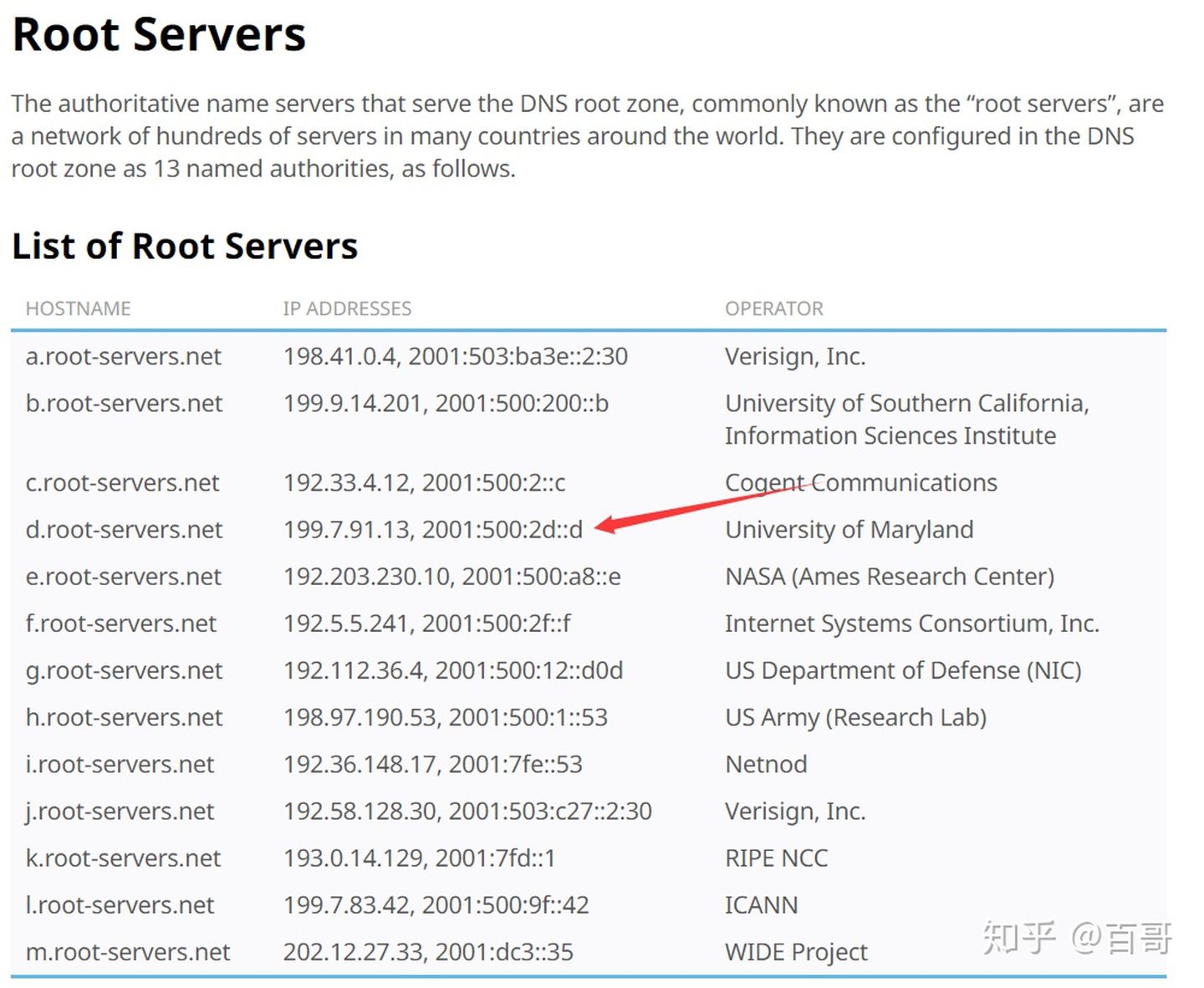


抓包分析



客户端是192.168.1.34，本地dns服务器是192.168.1.221，当客户端向服务器请求[http://www.hunau.edu.cn](https://link.zhihu.com/?target=http%3A//www.hunau.edu.cn" \t "_blank)

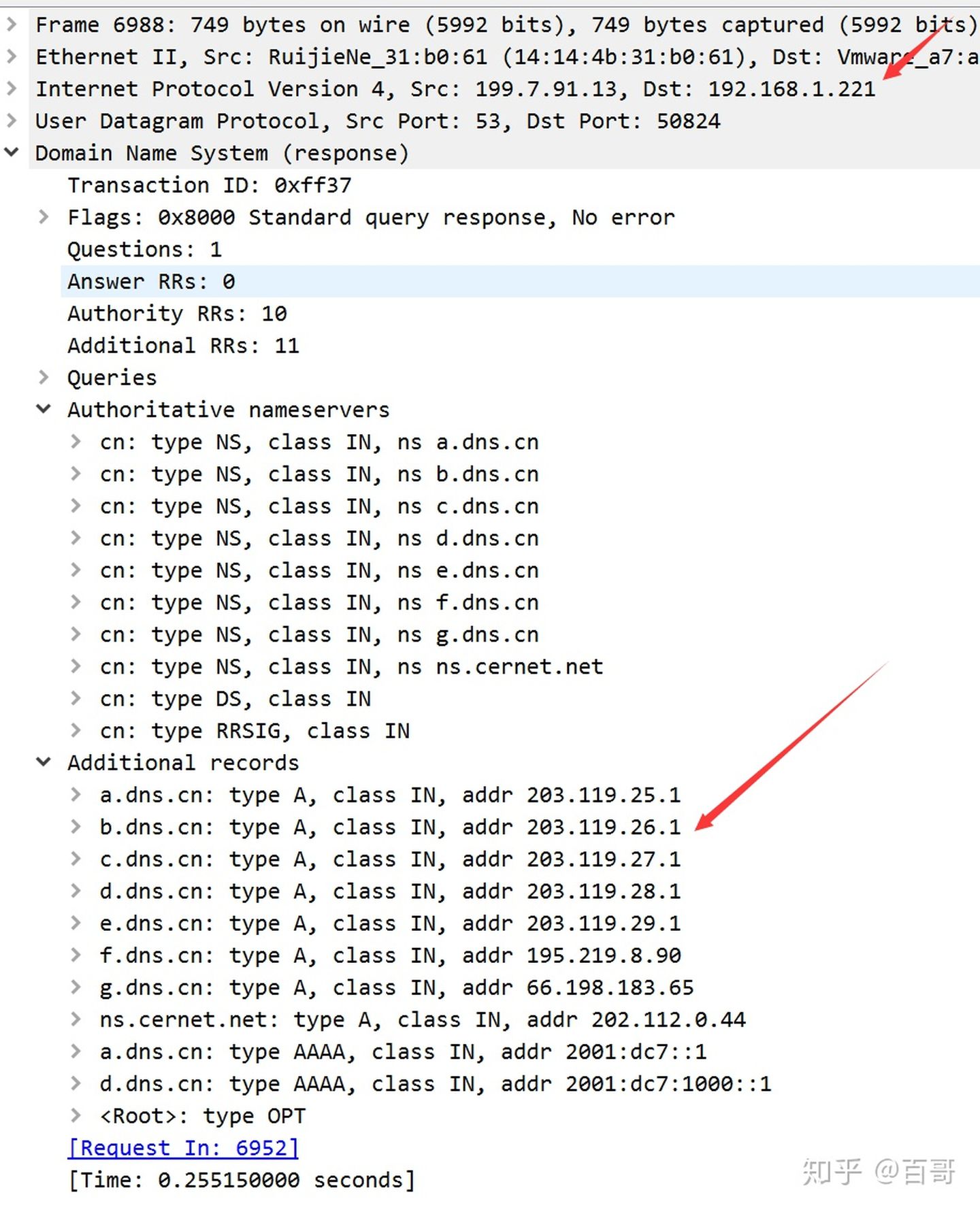
本地服务器向根服务器199.7.91.13转发,这是其中一台根服务器

在iana上可看到所有的根服务器地址和管理者

**第六步，顶级域服务器收到请求，会返回二级域服务器的地址。**

比如一个网址是[http://www.xxx.edu.cn](https://link.zhihu.com/?target=http%3A//www.xxx.edu.cn" \t "_blank)，则顶级域名服务器再转发给负责.[http://edu.cn](https://link.zhihu.com/?target=http%3A//edu.cn)域的二级服务器

抓包分析



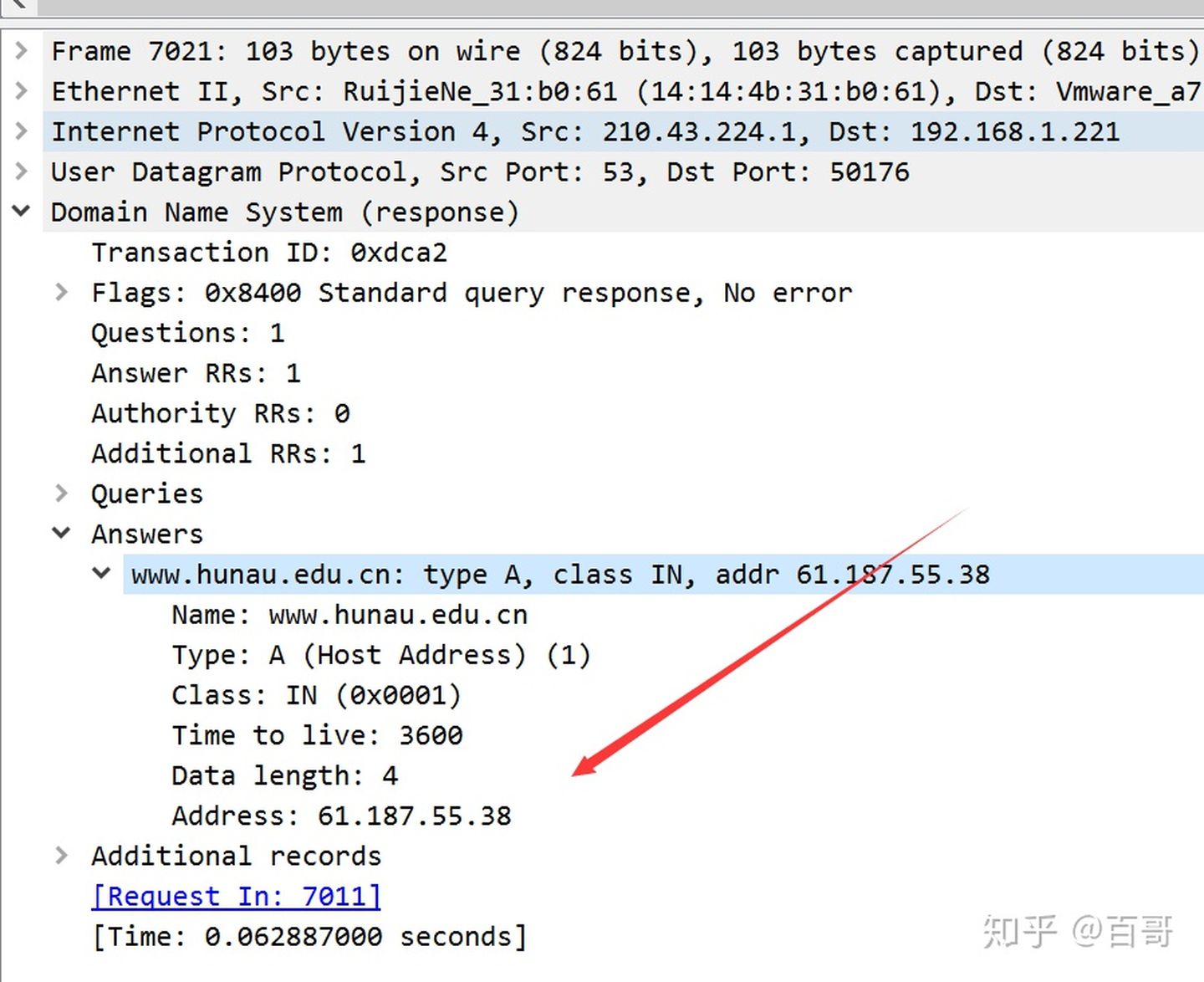
这是由根服务器返回的结果，负责cn域的服务器有这么多，接下来将选择其中一台

然后负责cn的服务器，返回负责[http://edu.cn](https://link.zhihu.com/?target=http%3A//edu.cn" \t "_blank)的

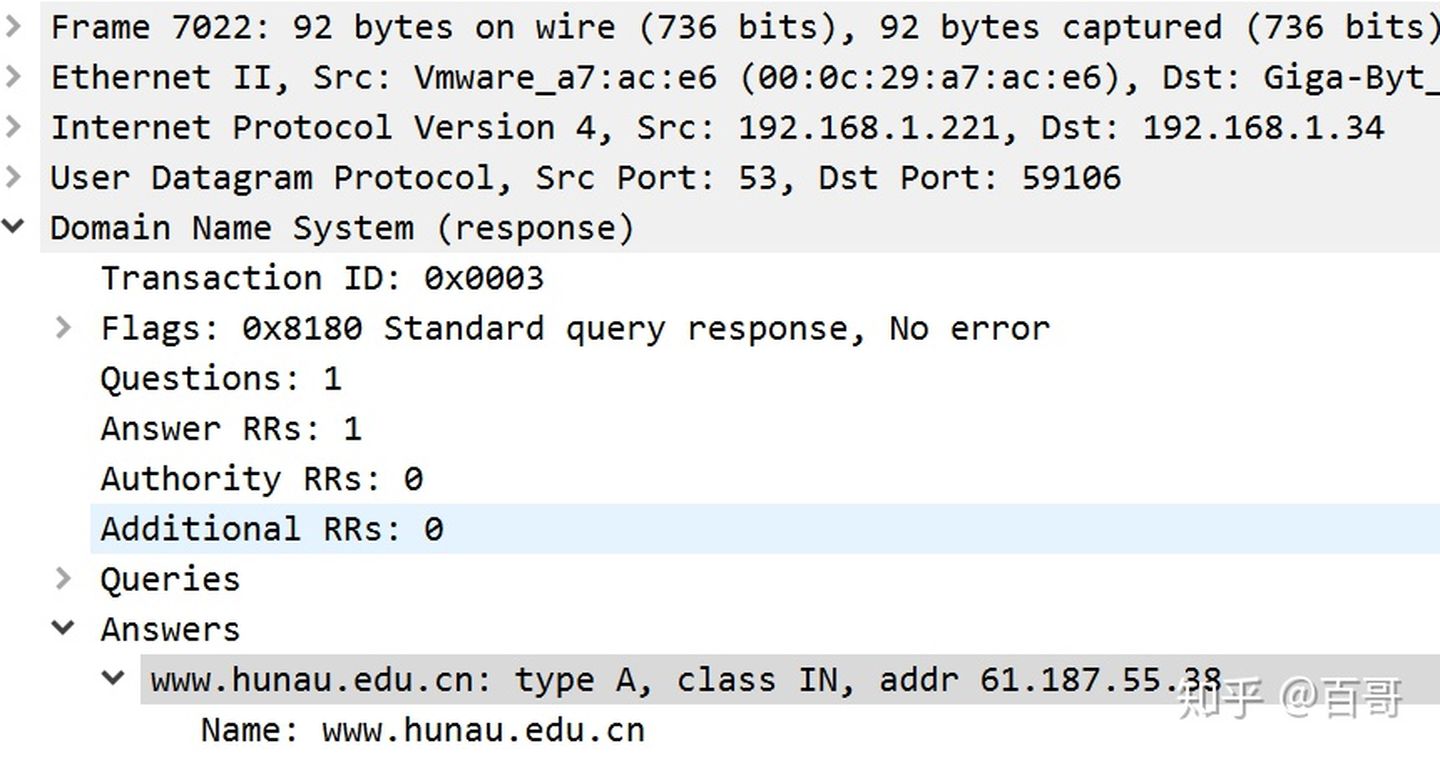
。。。

**第七步，以此类推，最终会发到负责锁查询域名的，最精确的那台dns，可以得到查询结果。**

抓包分析，这是[http://www.hunau.edu.cn](https://link.zhihu.com/?target=http%3A//www.hunau.edu.cn)的解析结果



**最后一步，本地dns服务器，把最终的解析结果，返回给客户端，对客户端来讲，只是一去一回的事，客户端并不知道本地dns服务器经过了千山万水。**



**迭代解析：本地服务器，一步步，经过多个步骤得到域名结果的过程**

**递归解析：客户端和本地服务器之间，一去一回得到域名结果的过程**