**实验四、应用层协议分析实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. 实验目的

分析应用层协议（如FTP，HTTP）的工作过程，理解应用层与传输层及下层协议的关系。

1. 实验内容

（1）每组同学利用现有实验室网络及云服务器搭建内网、外网环境；

（2）用Wireshark截获HTTP报文，分析报文结构及浏览器和服务器的交互过程；分析HTTP协议的缓存机制。分析应用层协议跟TCP/DNS等协议的交互关系。

（3）用Wireshark截获FTP的报文，分析FTP协议的连接；分析被动模式，普通模式的区别；分析NAT对FTP的影响。使用netcat工具模拟FTP的客户端。

**注：HTTP和FTP两个协议二选一。**

1. 实验环境与分组

每2名同学一组，以现有校园网络环境及云服务器搭建内网、外网网络。

1. 实验组网

以各组现有网络实际情况为准，标注内网、公网地址。



1. 实验过程及结果分析

【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

**1、HTTP协议分析**

（一）清空缓存后的ARP，DNS和HTTP协议分析

步骤1：在计算机终端上运行Wireshark截获所有的报文。

步骤2：清空ARP，DNS和HTTP浏览器的缓存：

浏览器缓存的清除以Chrome浏览器为例，地址栏中输入chrome://settings/，找到高级选项中的“隐私设置和安全性”，清除浏览数据。

执行“ipconfig /flushdns”清除本地DNS缓存。

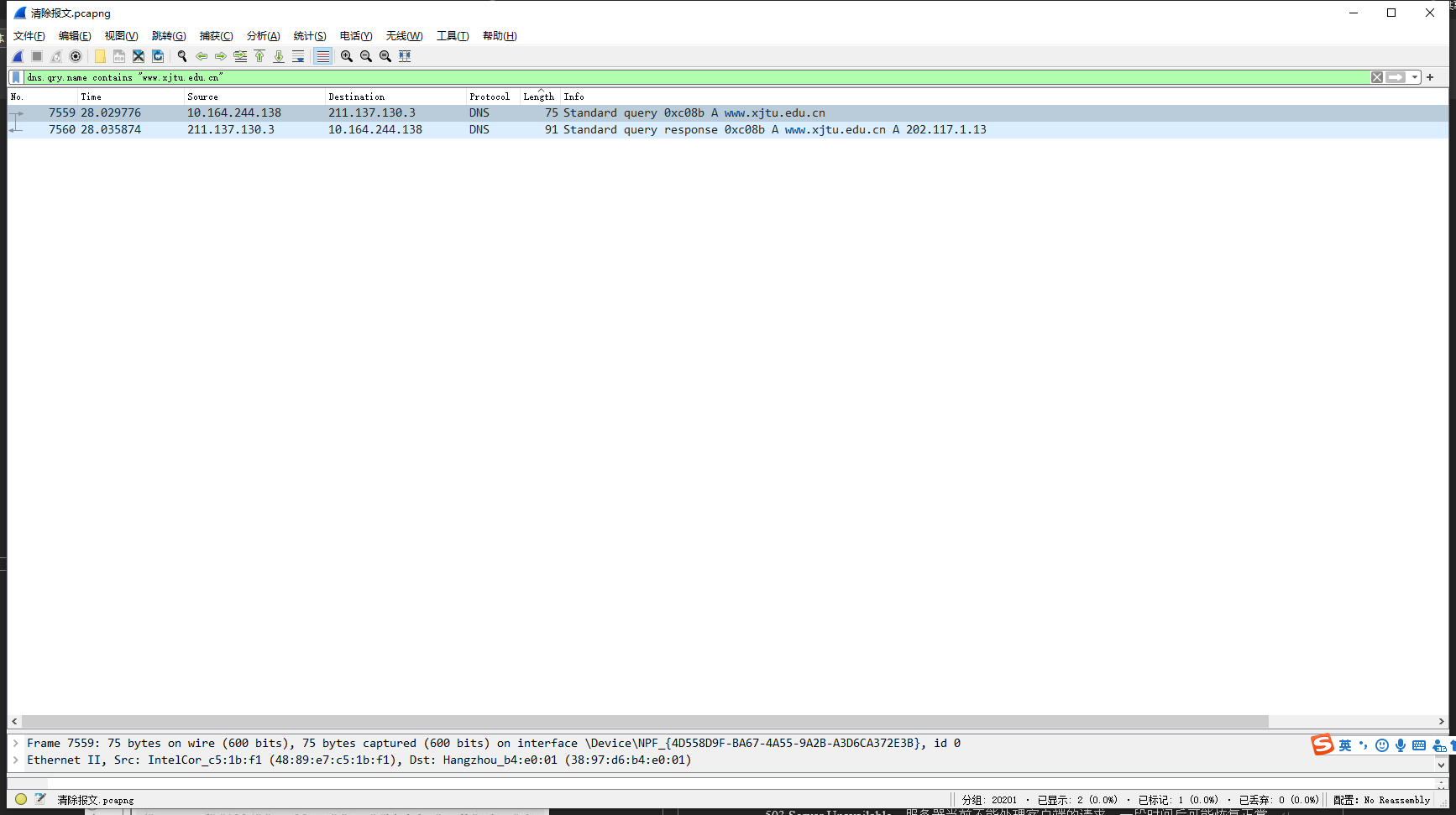
执行“arp –d”命令清空arp缓存。

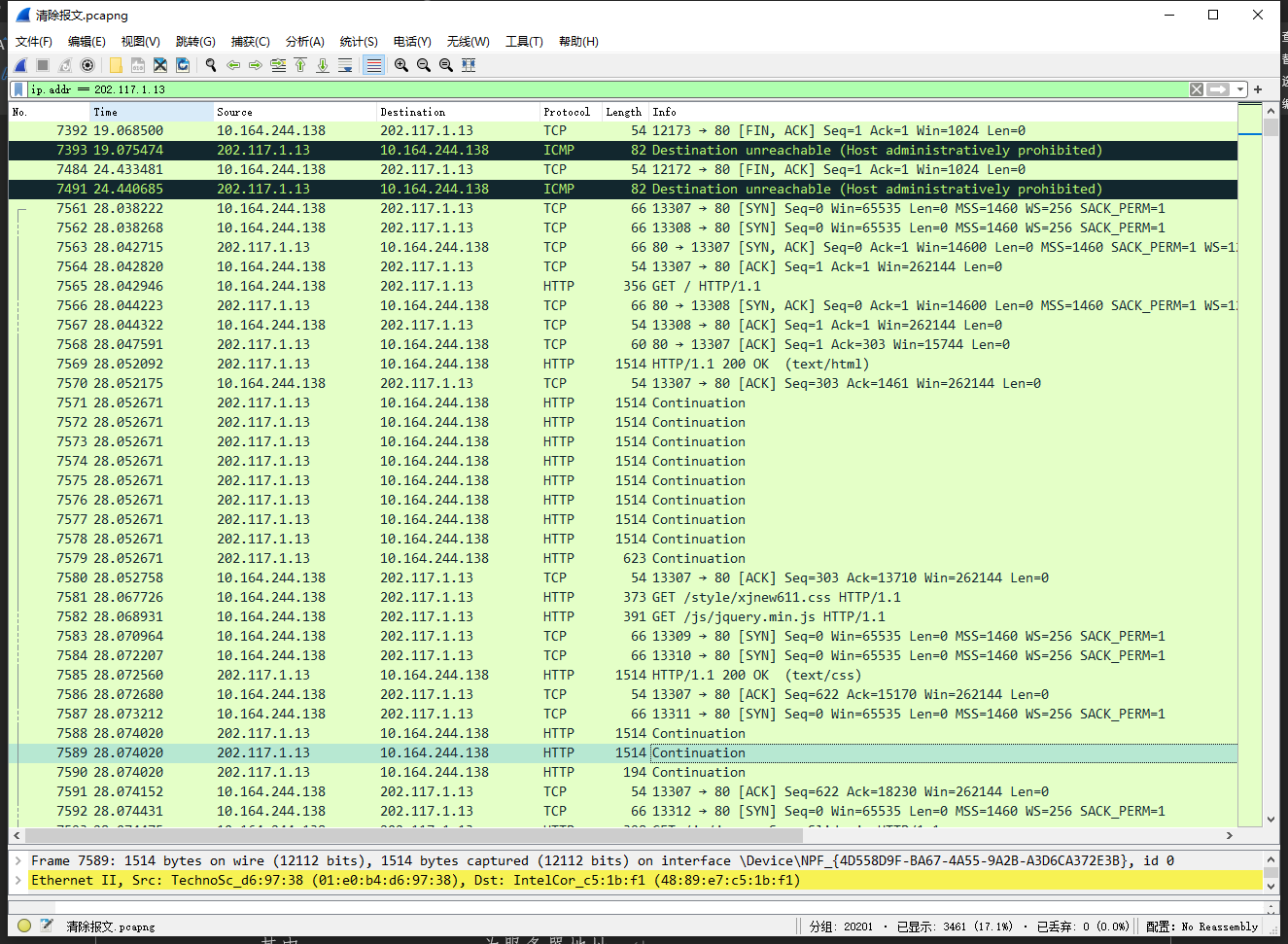
步骤3：在浏览器中访问3个网址，比如[www.xjtu.edu.cn](http://www.xjtu.edu.cn), [www.github.com](http://www.github.com), [www.unb.br](http://www.unb.br)；

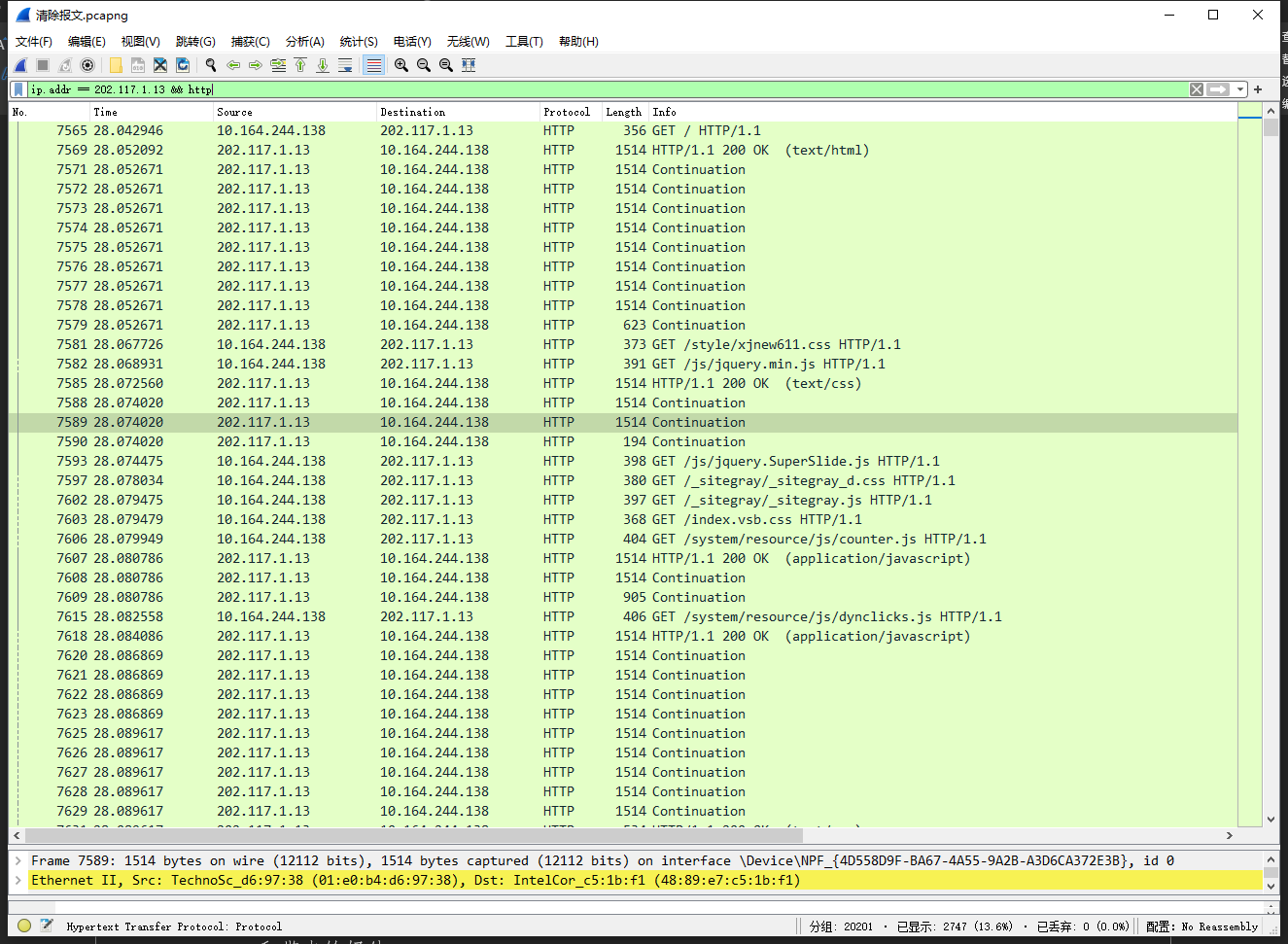
步骤4：执行完之后，Wireshark停止报文截获，分析截获的报文。

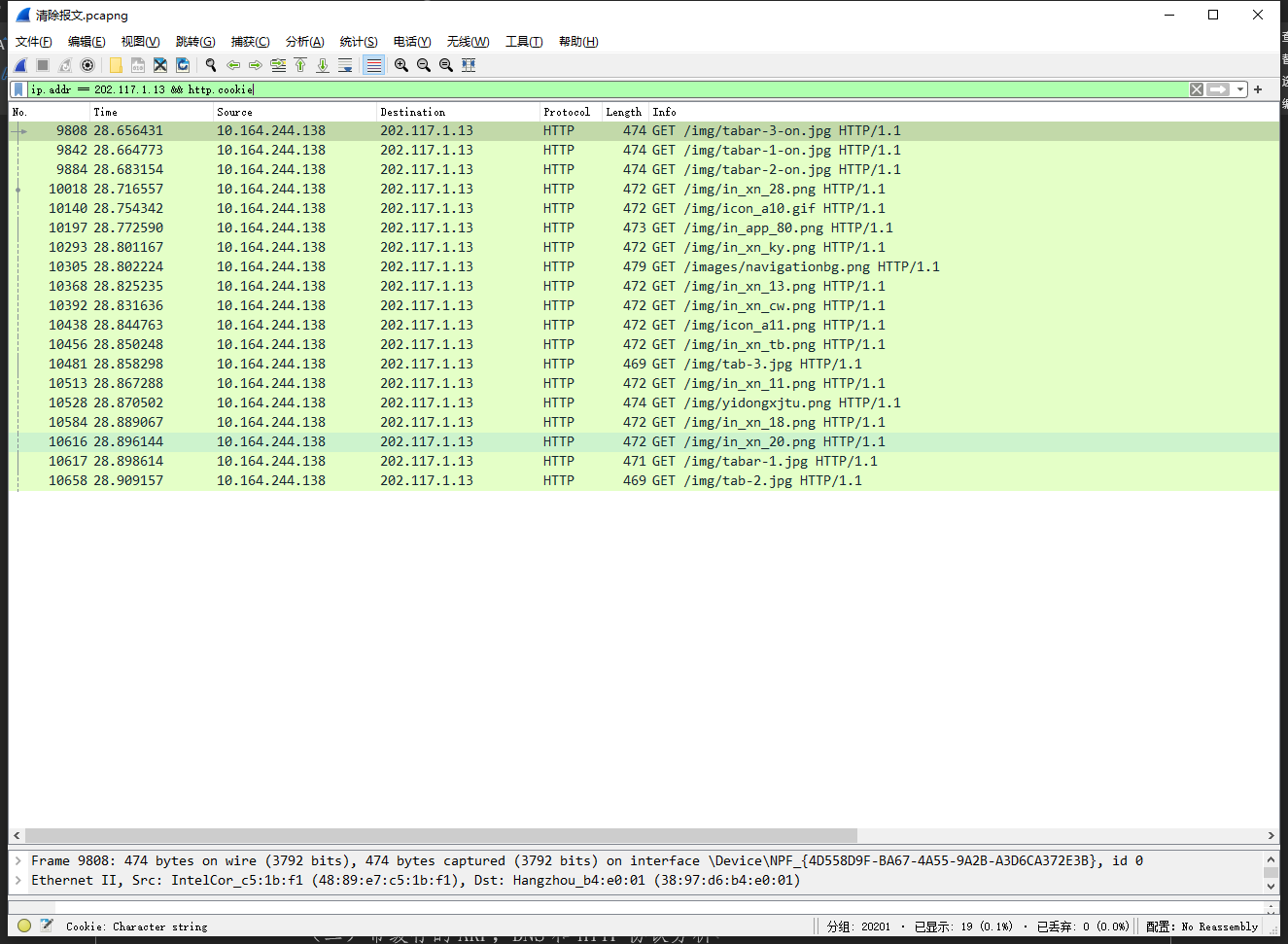
观察几个协议的配合使用，注意访问的延迟情况。特别分析HTTP的请求和应答。注意一个网址的访问中，用了几个连接，取了几个对象（HTML，CSS，JS，图片等），有几次DNS解析，有没有Cookie等。

访问各网页时，产生了不同数量的DNS解析，取了HTML, CSS, JS等对象。4399.com中未保存cookie。

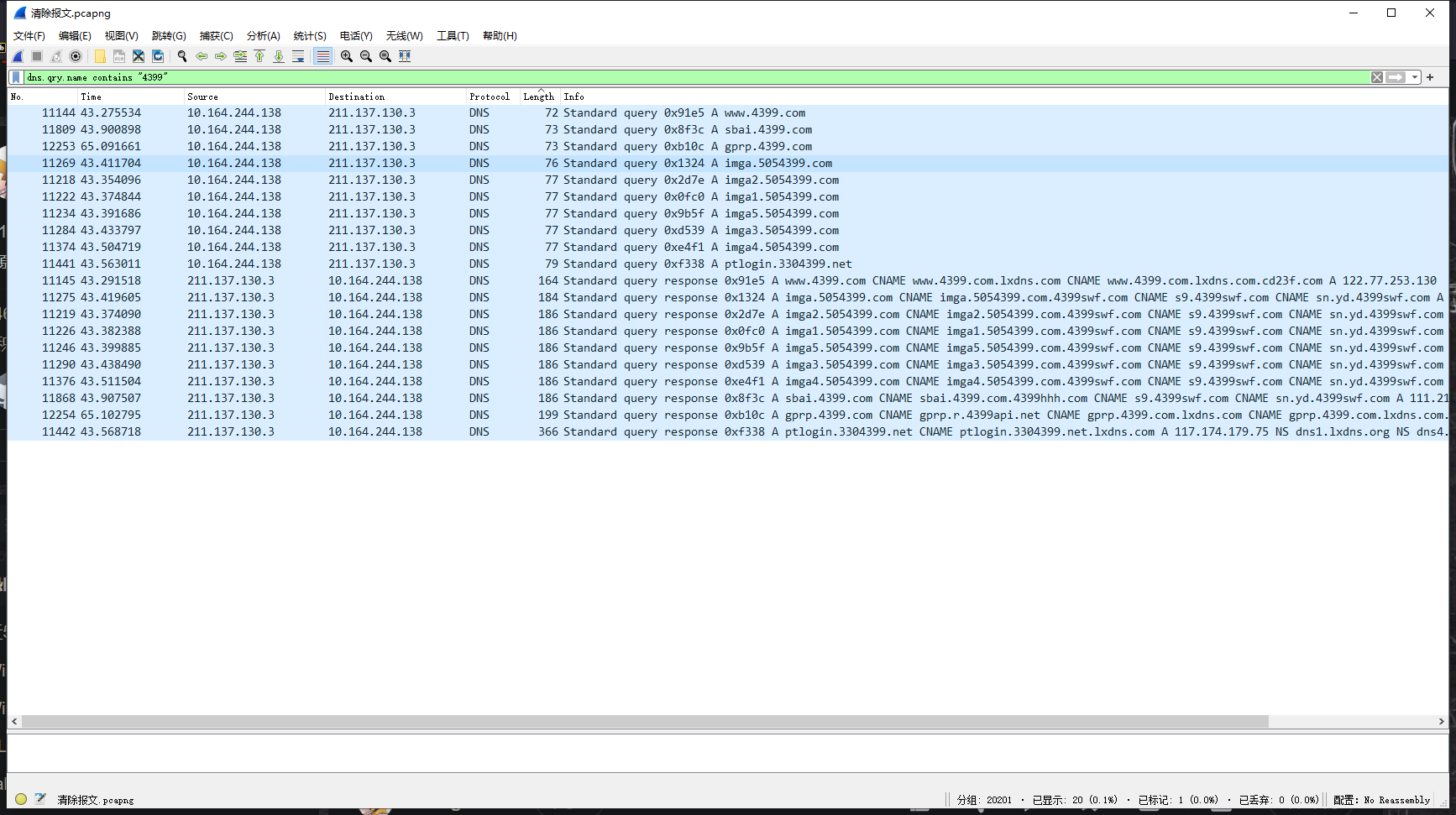


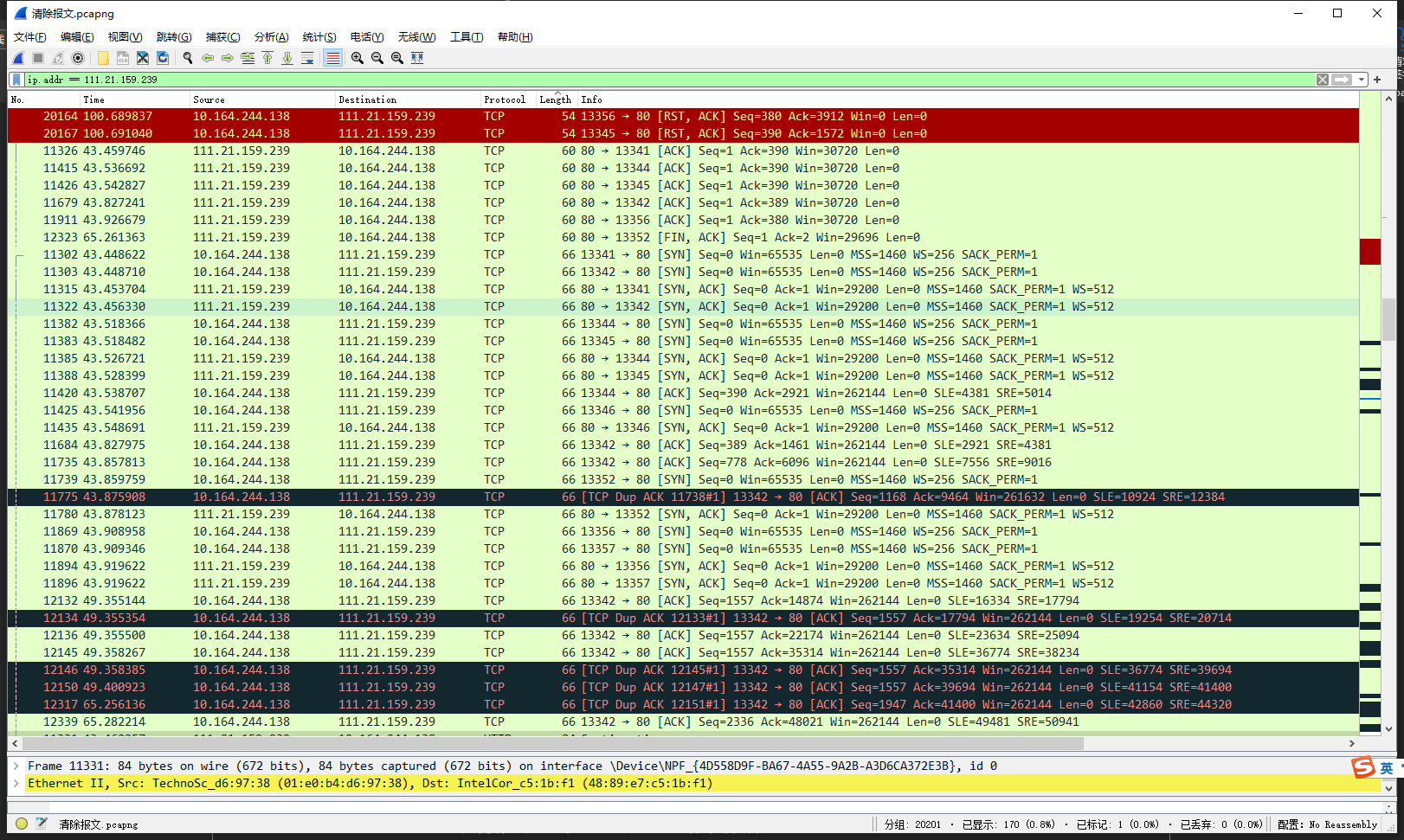


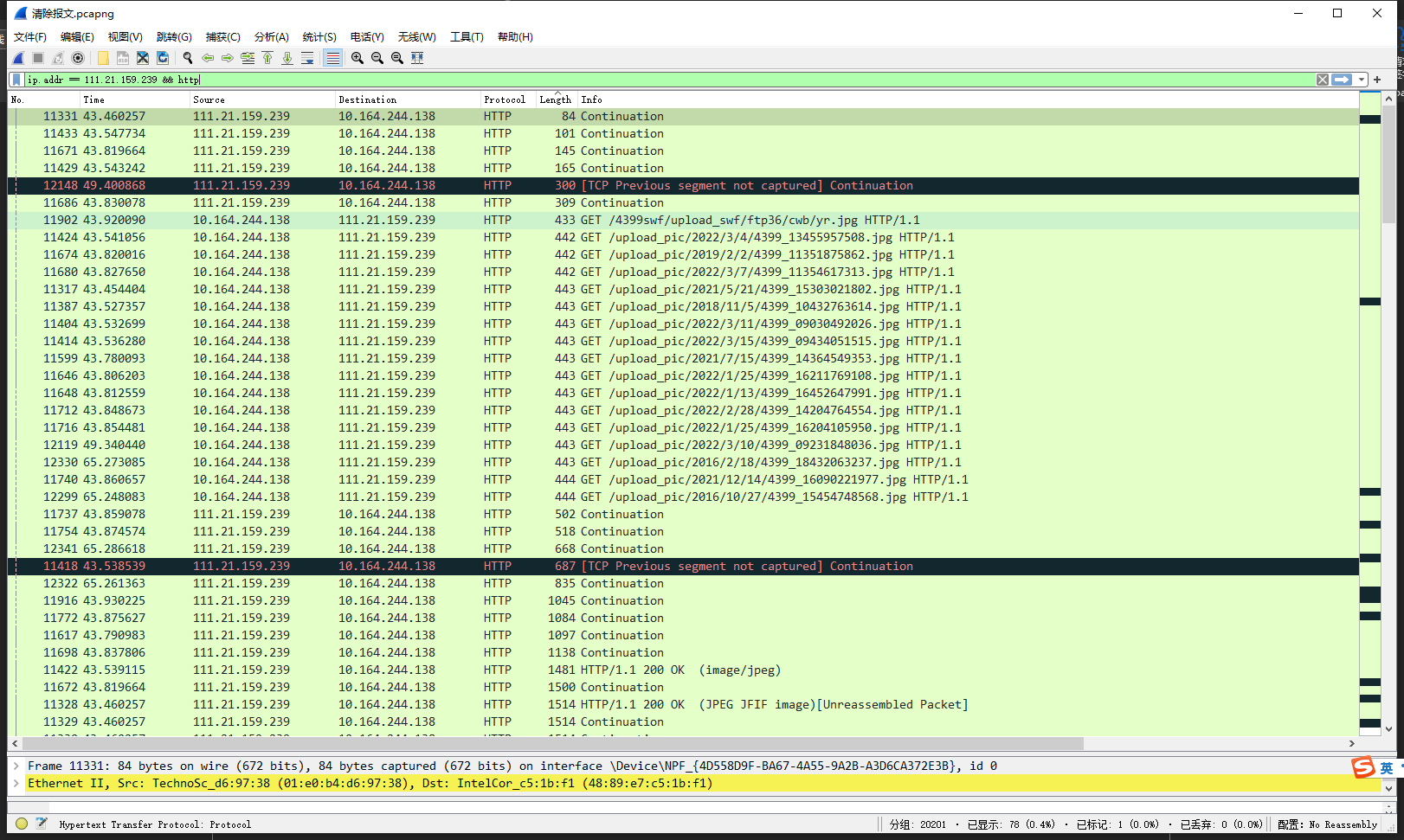


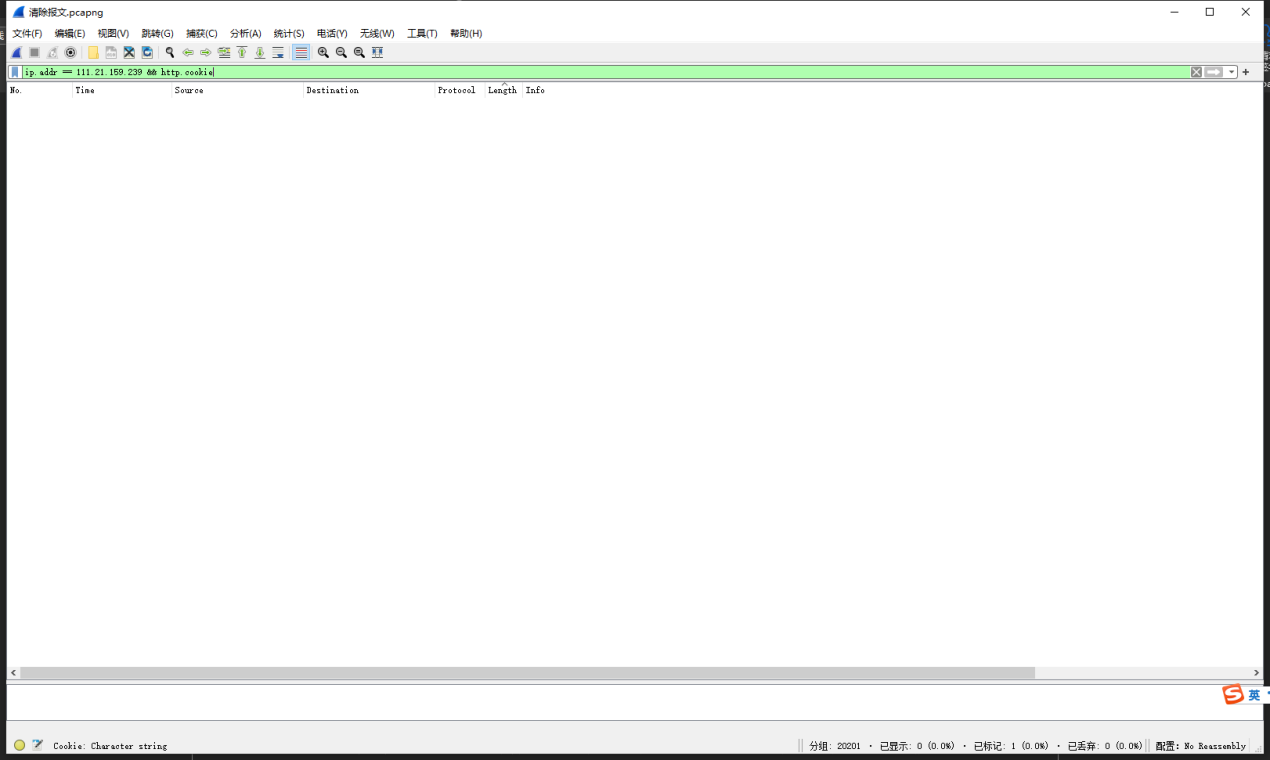


[www.4399.com](http://www.4399.com)

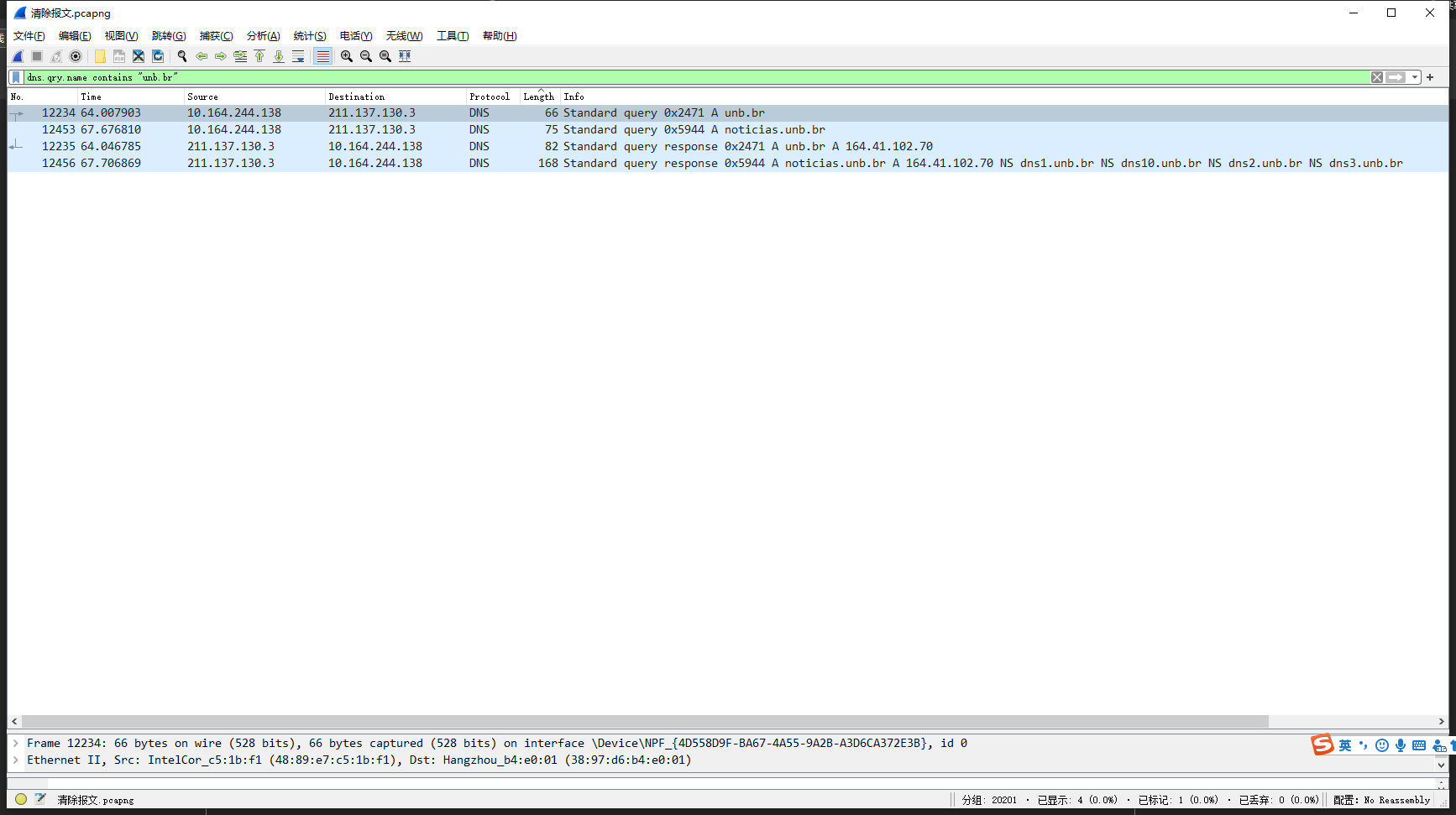


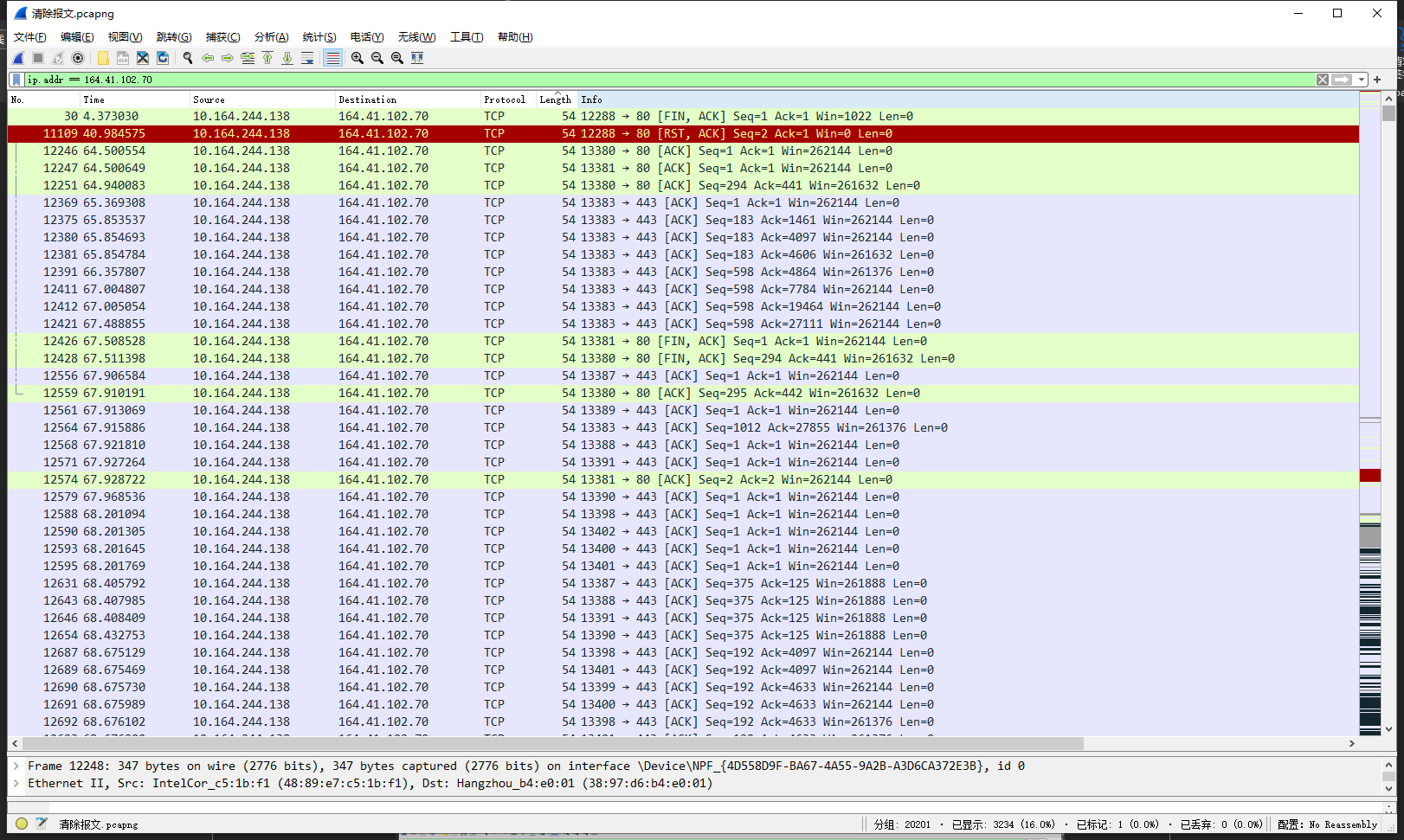


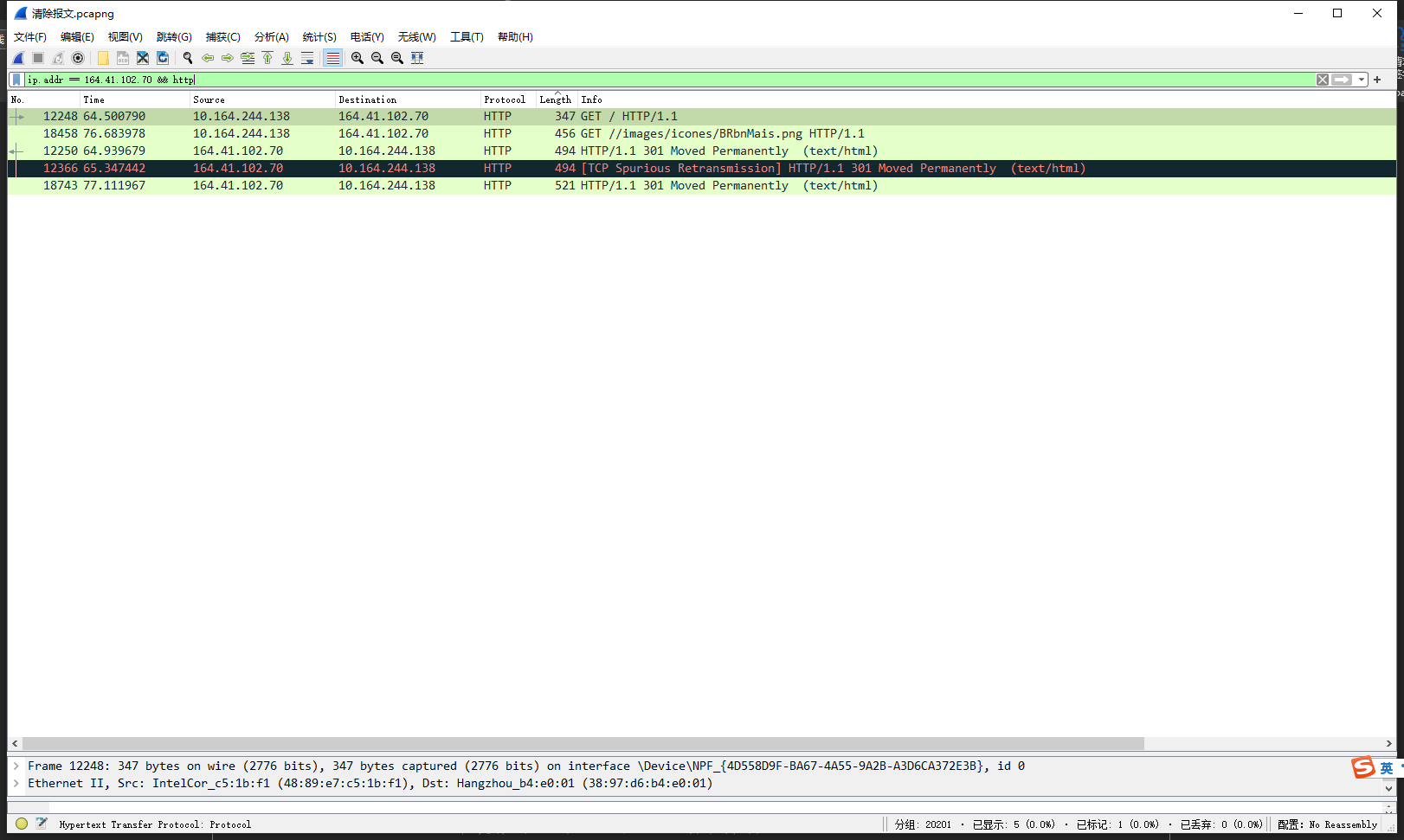


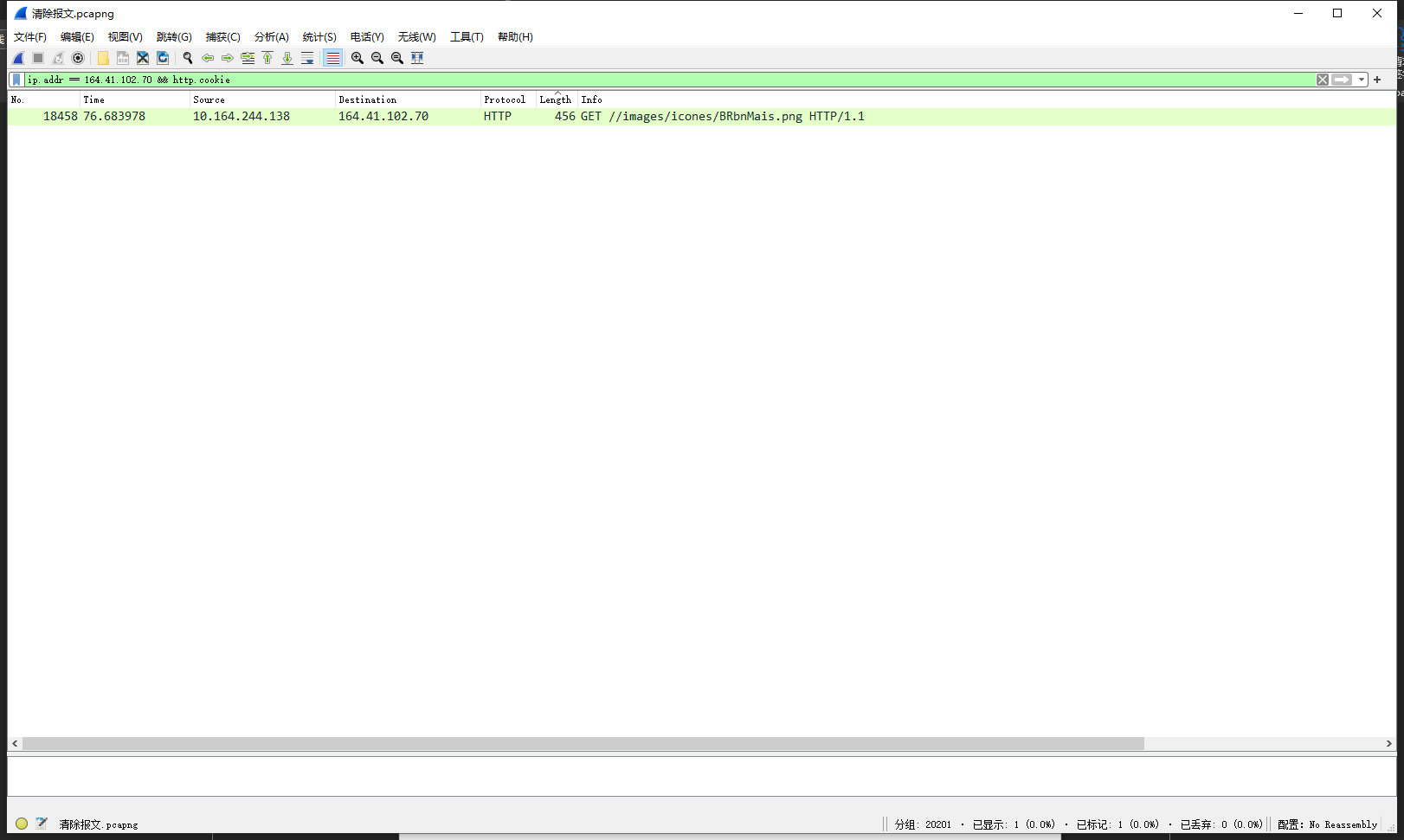


[unb.br](http://www.unb.br)









（二）带缓存的ARP，DNS和HTTP协议分析

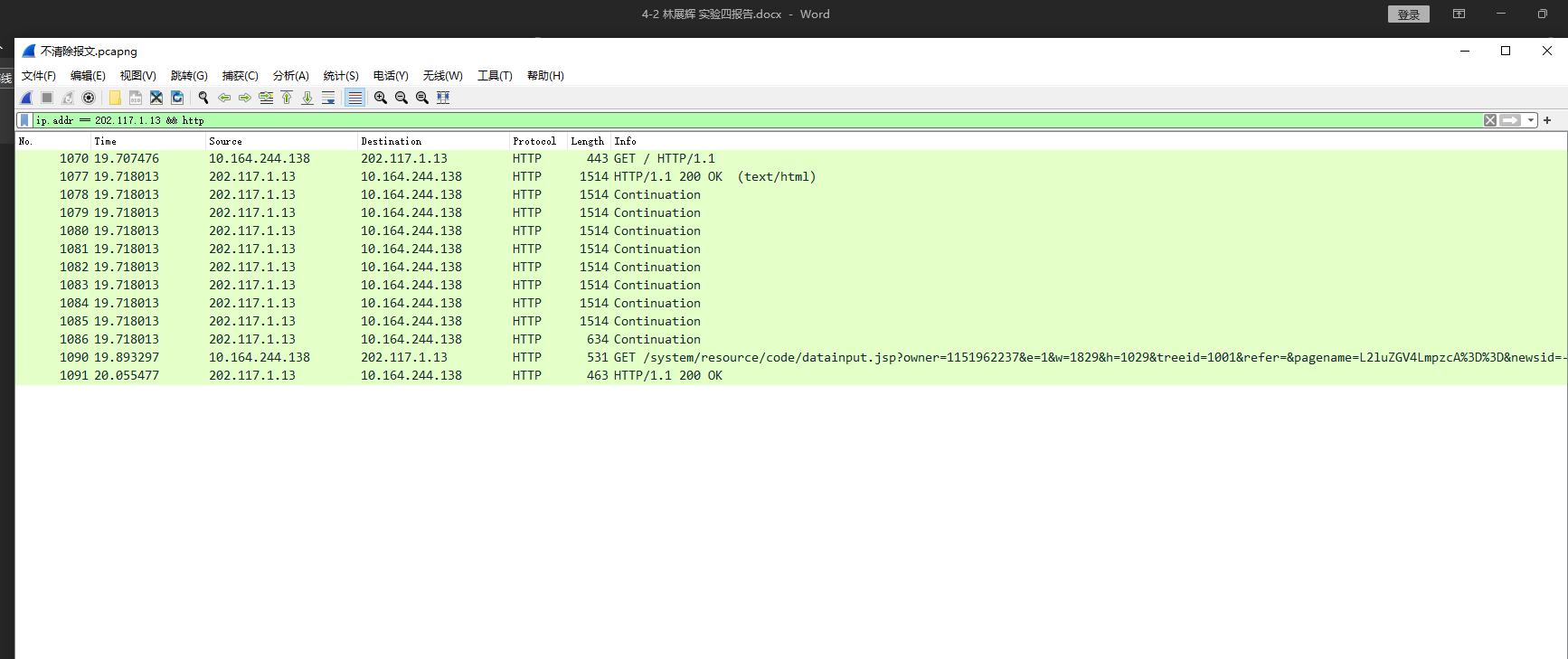
照着1.7.1中的步骤1-4再次执行一遍，但不执行步骤2。观察缓存的使用和带来的好处。

[www.xjtu.edu.cn](http://www.xjtu.edu.cn)

无dns解析

http请求对象大幅减少

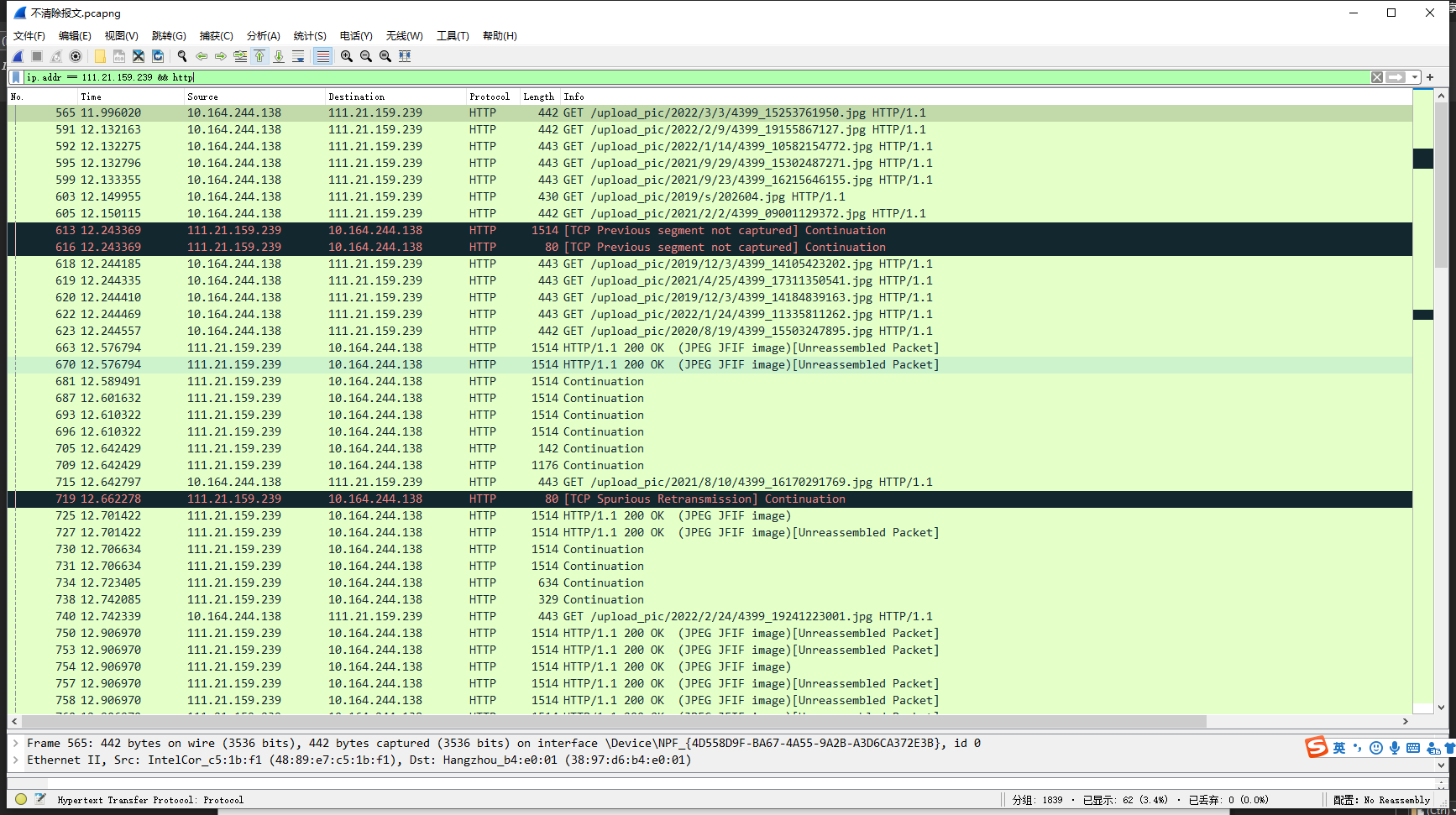




4399.com

未保存cookie

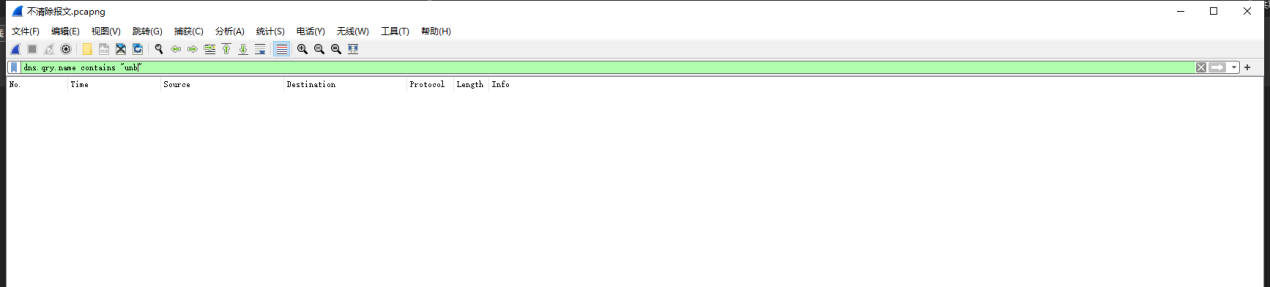
请求的对象仍然很多

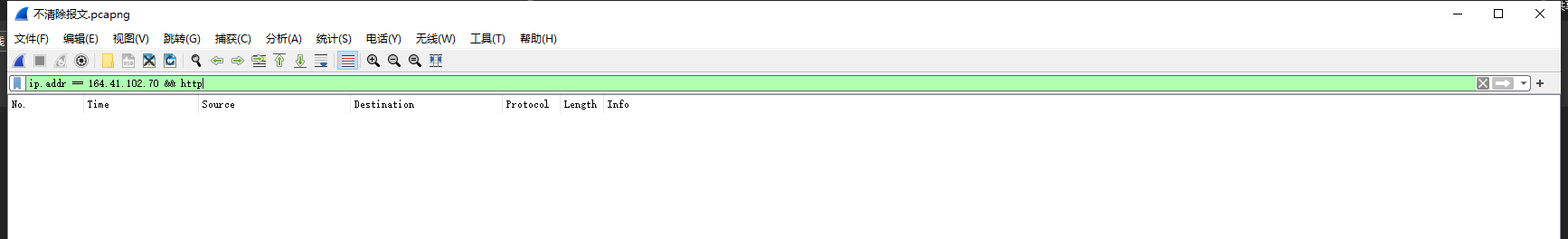


[www.unb.edu.bz](http://www.unb.edu.bz)

保存了cookie

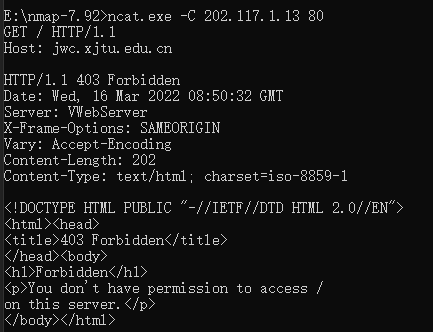
无dns解析





（三）使用ncat工具访问HTTP服务

参考1.7.1中的步骤1-4和分析结果，在命令窗口执行ncat -C xxx.xxx.xxx.xxx 80，ncat连接上HTTP服务器后，根据协议输入合适的请求。其中xxx.xxx.xxx.xxx 为服务器地址。



**2、FTP协议分析**

（一）FTP协议的分析

步骤1：在远程的云服务器上开启ftp服务，并在云服务器控制台把21端口开放。在云服务器上运行报文截获工具（如Linux的tcpdump，Windows的Wireshark）截获FTP报文。

步骤2：在计算机终端上运行Wireshark截获报文，使用IE浏览器来访问该FTP服务器。比如在地址栏输入 <ftp://xxx.xxx.xxx.xxx/> 其中xxx.xxx.xxx.xxx 是该云服务器的IP地址。

步骤3：进入FTP服务器中的某个目录中，下载一个文件。结束后，停止报文截获。

分析该FTP的过程。注意对照服务器和客户端的一起分析，注意NAT的影响。观察是否使用了被动模式，如果是主动模式并且工具允许，使用被动模式再做一次下载，并分析。

如果FTP不能正常工作，请仔细抓包并分析原因。NAT穿越问题可能是原因之一。

（二）使用ncat工具来访问FTP服务

步骤1：提前把用到的FTP命令准备好（写在notepad++中）。

步骤2：在云服务器上运行报文截获工具准备截获FTP报文。在命令窗口执行ncat –C xxx.xxx.xxx.xxx 21，ncat连接上FTP服务器后，根据协议输入合适的命令。其中xxx.xxx.xxx.xxx 为云服务器地址。

步骤3：解析完毕后停止报文截获。把过程整理记录到报告中。

在ncat模拟FTP客户端的过程中，请查看服务器的文件列表，并下载一个不大的文本文件。过程中，必要时用netstat命令观察双方的（新开）端口监听情况。

1. 互动讨论主题

1、HTTP协议的缓存，DNS的缓存；缓存对网络访问速度的影响。

HTTP中具有缓存功能的是浏览器缓存，以及缓存代理服务器。HTTP缓存的是指:当Web请求抵达缓存时， 如果本地有“已缓存的”副本，就可以从本地存储设备而不是从原始服务器中提取这个文档。

DNS 域名系统给应用访问带来了额外的时延，另外由于 DNS 域名解析采用不可靠的 UDP 协议通讯，受内外部网络环境的影响较大，特别是在有丢包的情况下，导致的时延可能达到数秒。因此DNS 解析采用了缓存机制。在客户第一次访问之后，递归服务器和客户端都会缓存到该域名的解析记录，并设置相应的缓存生存时间（TTL），在TTL有效期内，客户再次对同域名发起访问时，直接通过客户端本地和本地 DNS 服务器高速缓存解析，不再需要经过迭代查询过程。

缓存的好处有：减少了冗余的数据传输；减少了服务器的负担， 大大提高了网站的性能；加快了客户端加载网页的速度

2、NAT对FTP传输的影响，比较HTTP与FTP的特点；

ALG（Application Level Gateway），即应用程序级网关技术：传统的NAT技术只对IP层和传输层头部进行转换处理，但是一些应用层协议，在协议数据报文中包含了地址信息。为了使得这些应用也能透明地完成NAT转换，NAT使用一种称作ALG的技术，它能对这些应用程序在通信时所包含的地址信息也进行相应的NAT转换。例如：对于FTP协议的PORT/PASV命令、DNS协议的 "A" 和 "PTR" queries命令和部分ICMP消息类型等都需要相应的ALG来支持。

FTP是文件传输协议，HTTP是超文本传输协议，都基于TCP协议，都在客户、服务器模型的应用层协议之上。HTTP用于访问Internet上的不同网站，将网页内容从Web服务器传输到客户端的Web浏览器，被称为单向系统。FTP用于在FTP服务器和FTP客户端之间上传和下载文件，可以将文件从一个主机传输到另一个主机，被称为双向系统。HTTP仅建立一个链接：数据连接。FTP建立两个链接：数据连接和控制连接。HTTP使用TCP的80端口，而FTP使用TCP的20和21端口。HTTP不需要身份验证；而FTP使用密码进行身份验证。