**实验2:HTTP、DNS协议分析**

# 1实验目的

捕获HTTP/DNS数据包，理解Application Layer典型协议的工作过程。

# 2基础实验环境和准备工作（后续也要用）

(1)对windows机器：安装Vmware.或virtualbox,并在启用Linux操作系统（不限），或者

使用WSL:windows subsytem for linux,或者如果你有自己的云服务器（腾讯、百度等），也以在云服务器上完成实验。

注1：保证host os（Windows）--guest os（Ubuntu）的连通性，vmware的网络连接模式？请search.(NAT/host-only/bridge)

注2:Vmware或virtualbox耗资源；替代方式之一是使用vagrant或docker.(什么是vagrant?Vagrant如何使用？请search.)

****

**虚拟机没网看看下面方框里的对勾是不是没有勾选**

**连不上主机看看上面圆角部分是不是没有设置好**

(2)在guest os中：

方式一：如果有，使用你之前web开发课程中搭建的网站。

方式二：现做一个网页，网页内容中要包含你个人的基本信息(必须信息包括：姓名、学号)，网页的组成对象中要包含一个简单的表单(form);之后使用httpd或tomcat或nginx发布。具体如何在linux下使用httpd或者nginx或者tomcat等等发布网页，请自行search。

例如对httpd而言：

guest os:

- systemctl status httpd

- service start sshd

- service start httpd

把你的html放到"/var/www/html"目录中

(3)在host os上，运行wireshark做(host os——guest os之间的)各协议HTTP/DNS

报文交互的捕获(packet capture),通过观察协议报文，进一步掌握协议。

④学习使用wireshark,约1小时，请自行google/bing/baidu。

# 3实验内容

**!!!每次做【各】协议分析实验之前：**

**(1)清除掉浏览器上的所有cache;**

**(2)清空arp缓存（命令行模式下，先使用arp -a查看atp缓存；再使用命令“arp -d缓存中的IP”）；**

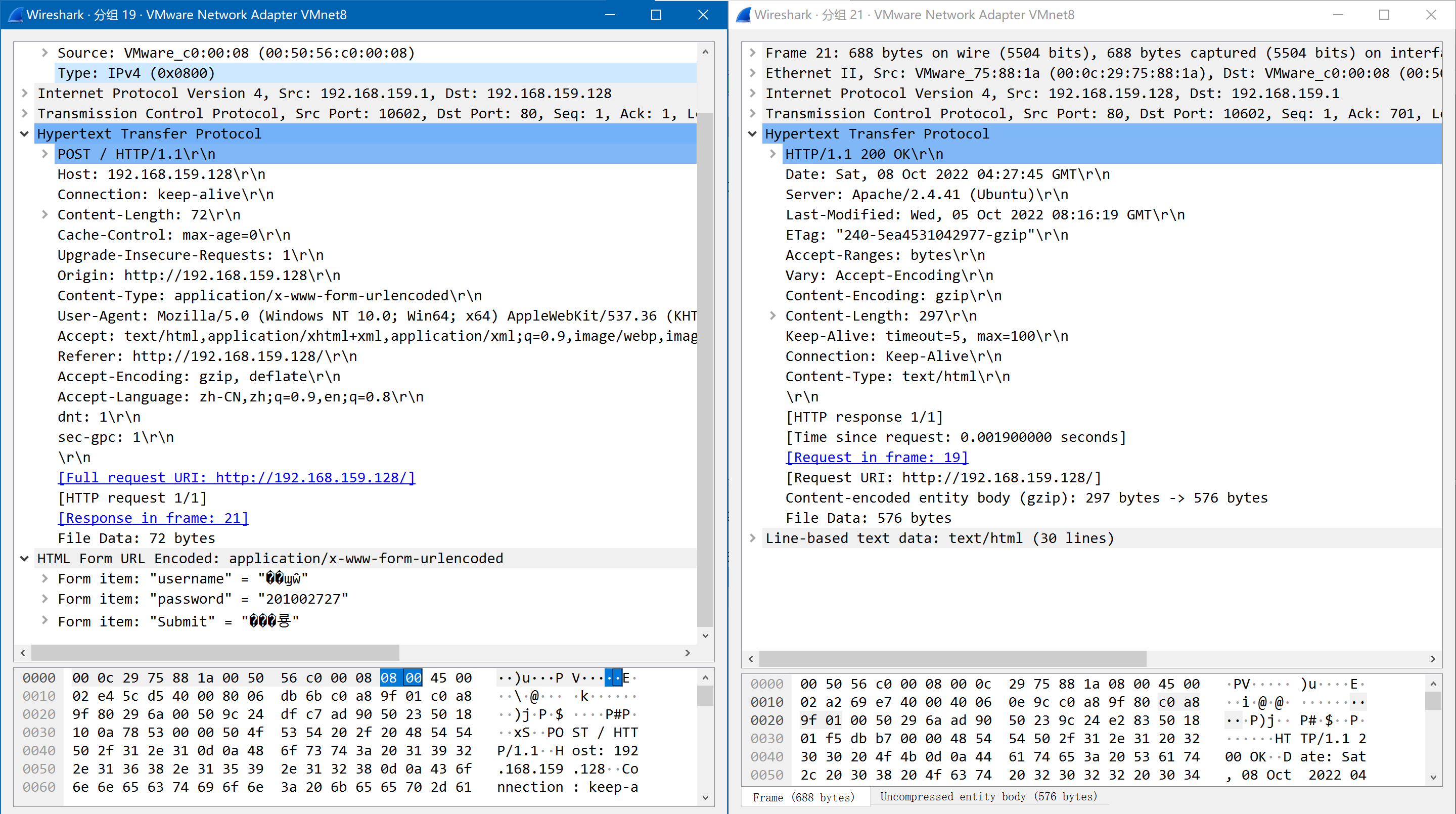
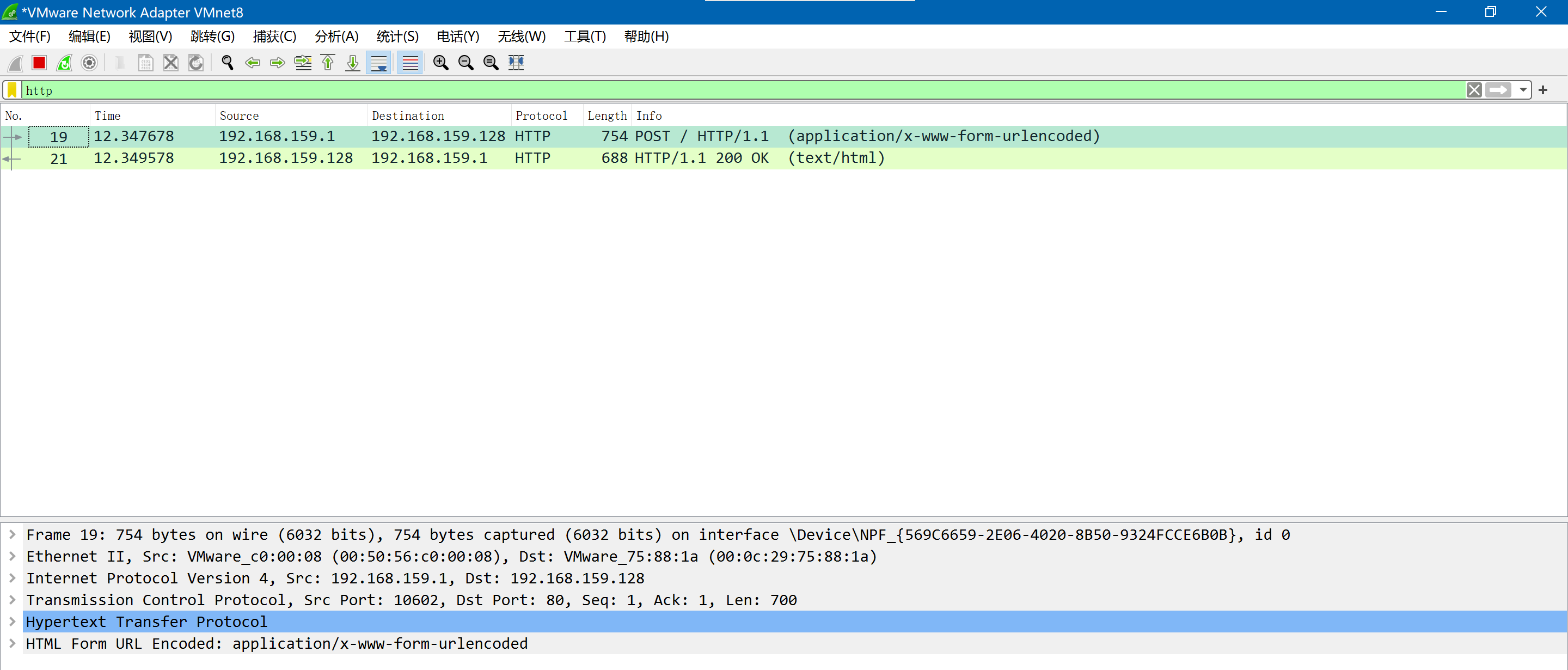
**(3)清空dns缓存(ipconfig/flushdns)。且，请查看“实验一”熟悉Linux、windows下常用的网络命令.!!!**

(1)在host OS.上访问guest OS中的website。

## 使用wireshark捕获HTTP数据包，

查看HTTP message,request/response报文交互过程，并【结合截图】回答如下问题：

打开登陆网页后打开wireshark，设置过滤器输入http后点击开始抓包，输入姓名学号点击提交后在wireshark控制台查看http的request和response报文。



http报文结构，第一行是请求方法（get），请求URL（register.html）和HTTP协议及版本（HTTP/1.1)，后面key-value形式的参数是报文头，再后面是请求体。

a.浏览器和server支持的HTTP分别是哪个版本？

都是HTTP/1.1

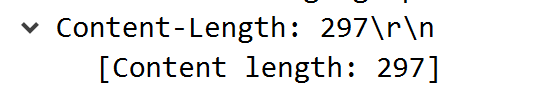
 

b.获取的html在浏览器上的最新更新时间是？

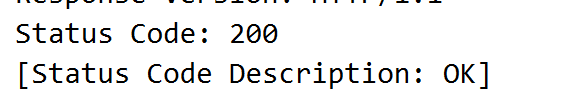


c.从server获取了多少字节的数据到浏览器？

297字节



d.从server返回到浏览器的状态码是什么？



e.从request报文中，可以看出浏览器内核是？

是chrome

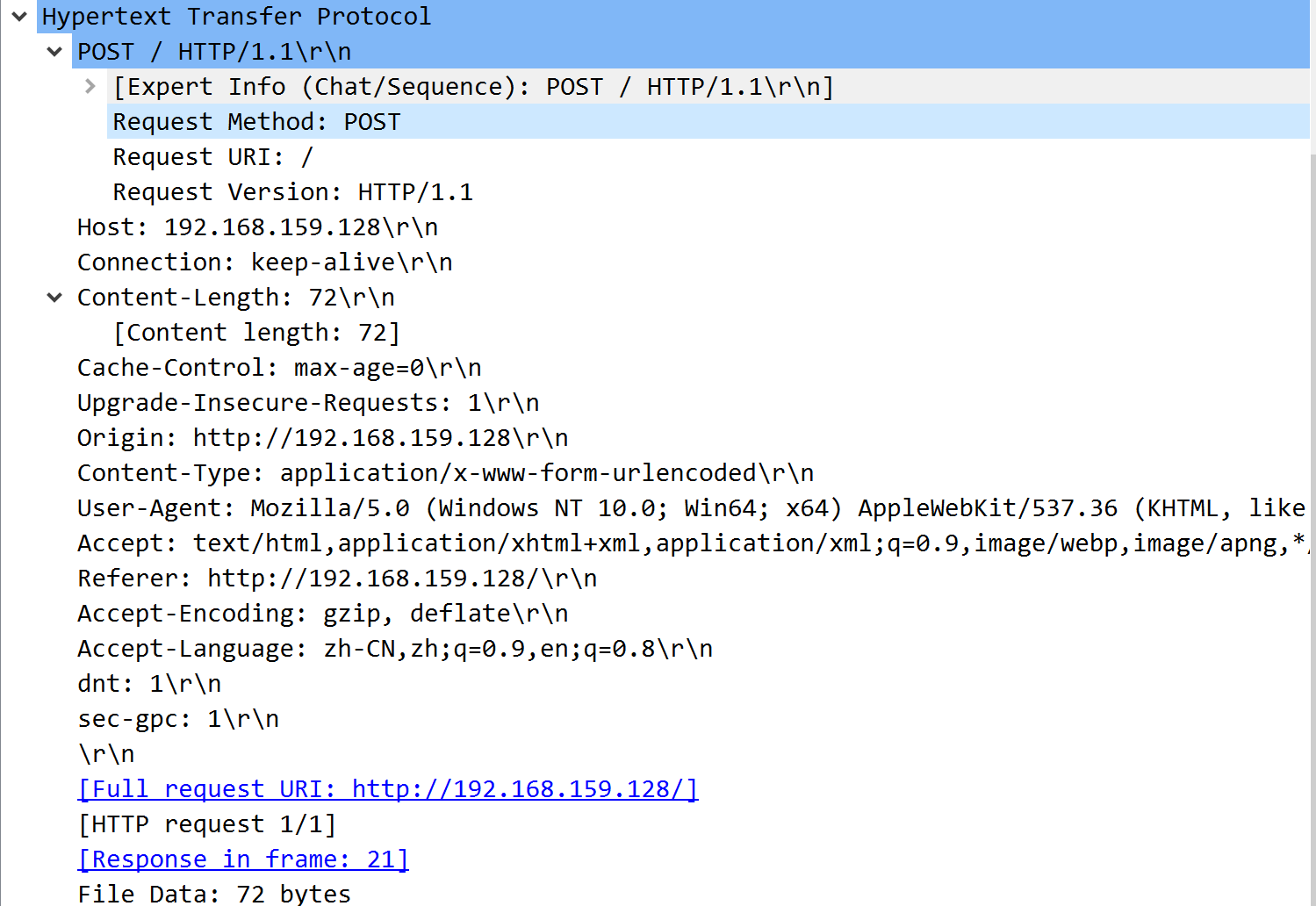


f.通过表单提交数据给server,HTTP request报文中的method是什么？

POST



g.其他你解读出的信息？

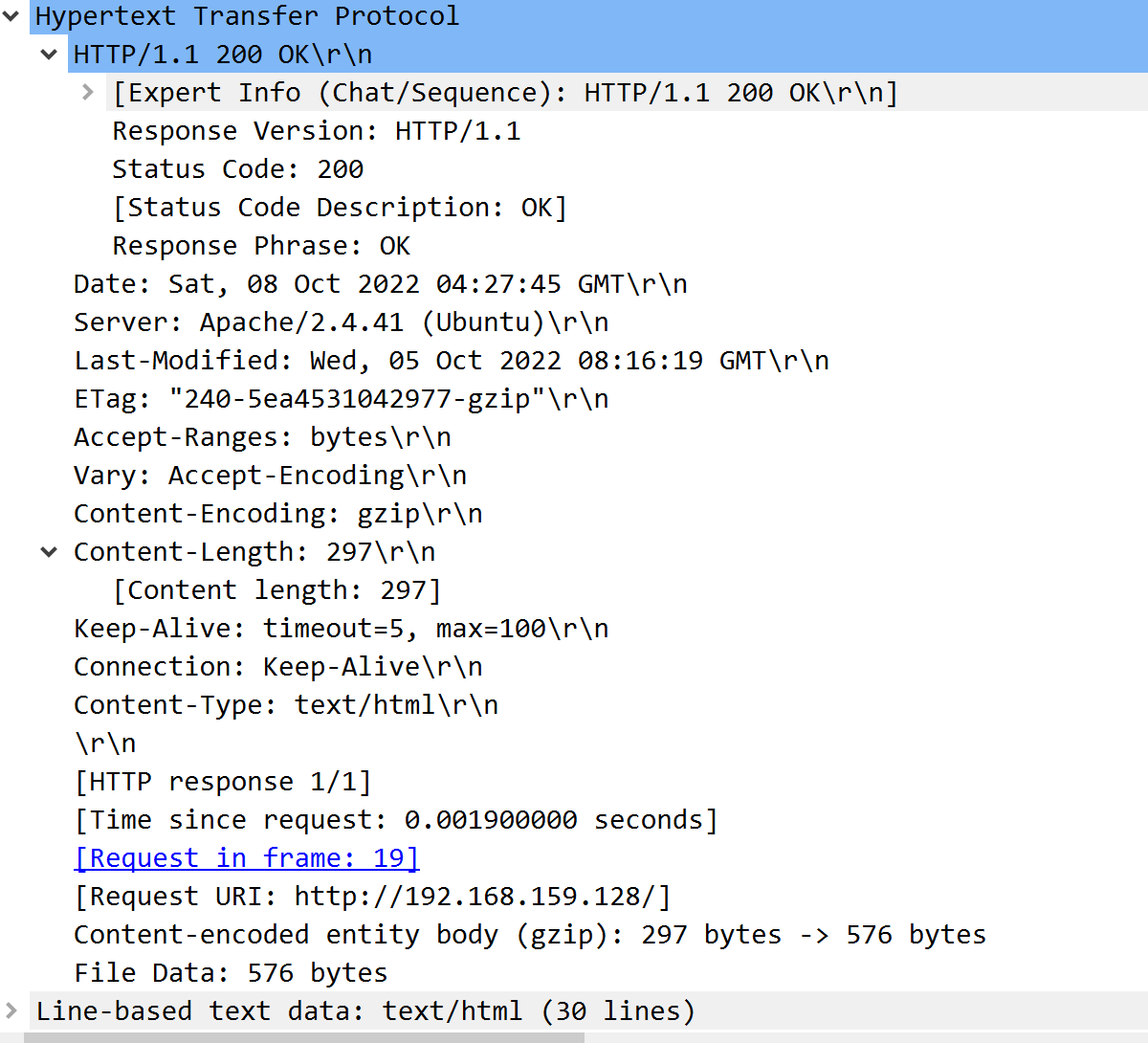


客户机IP是192.168.159.128。

浏览器接受text,xml, xhtml等类型的信息，编码类型是gzip，deflate

接受中文、英文的字符

连接方式为1.1的长连接（keep-alive）



服务器是Apache,来自Ubuntu主机，接受的是字节，内容在服务器上最后一次修改的时间是2022年10月8日，报文长度297字节，回复的内容类型是html语言，超时失效时间是5分钟，经过0.0019s将回复发送到主机。

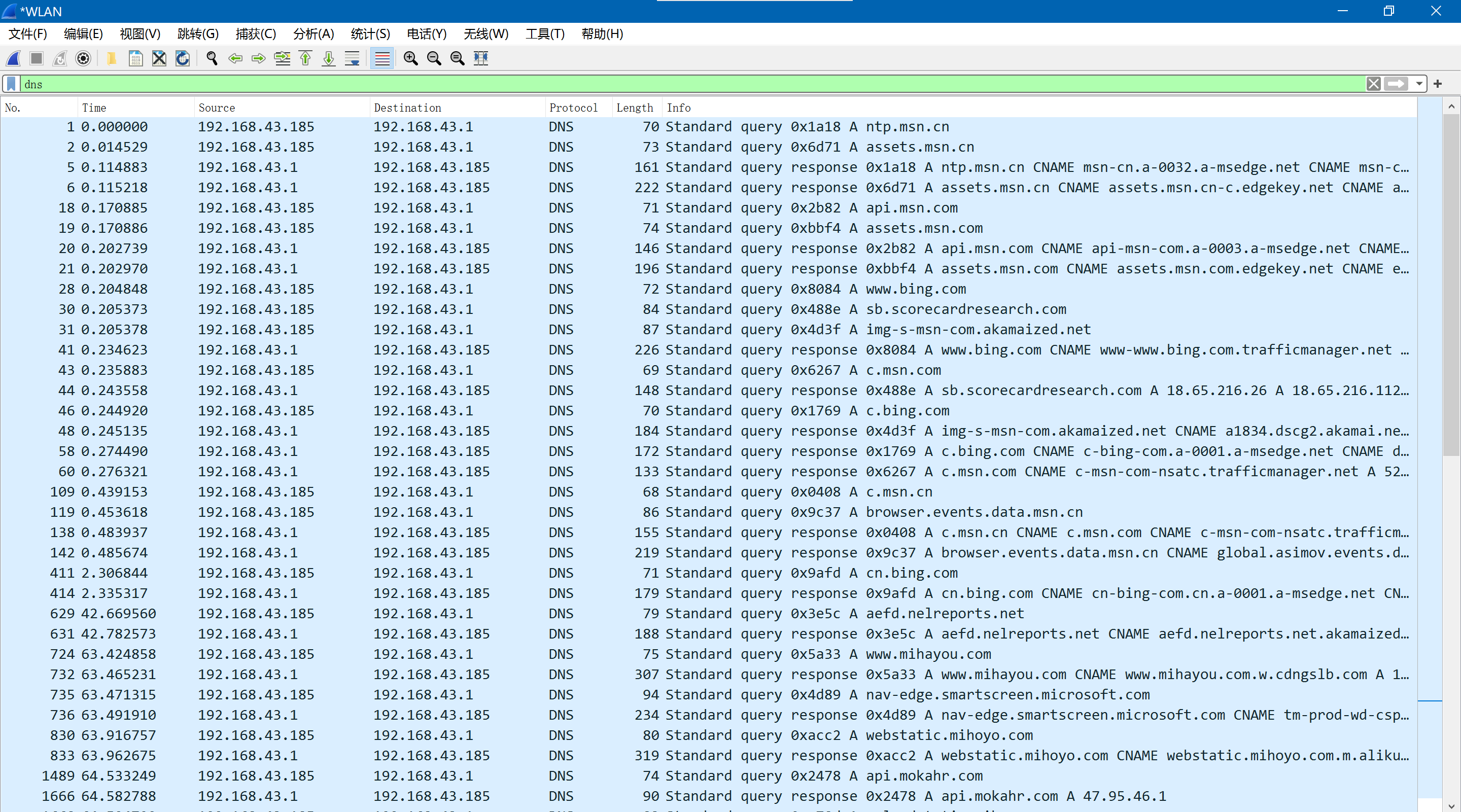
（2）在host OS上，启动wireshark捕获host os访问外网(如[www.bjfu.edu.cn](http://www.bjfu.edu.cn))时的DNS报文，并就DNS Query和Response报文做分析。

## 捕获DNS报文：

方式一：

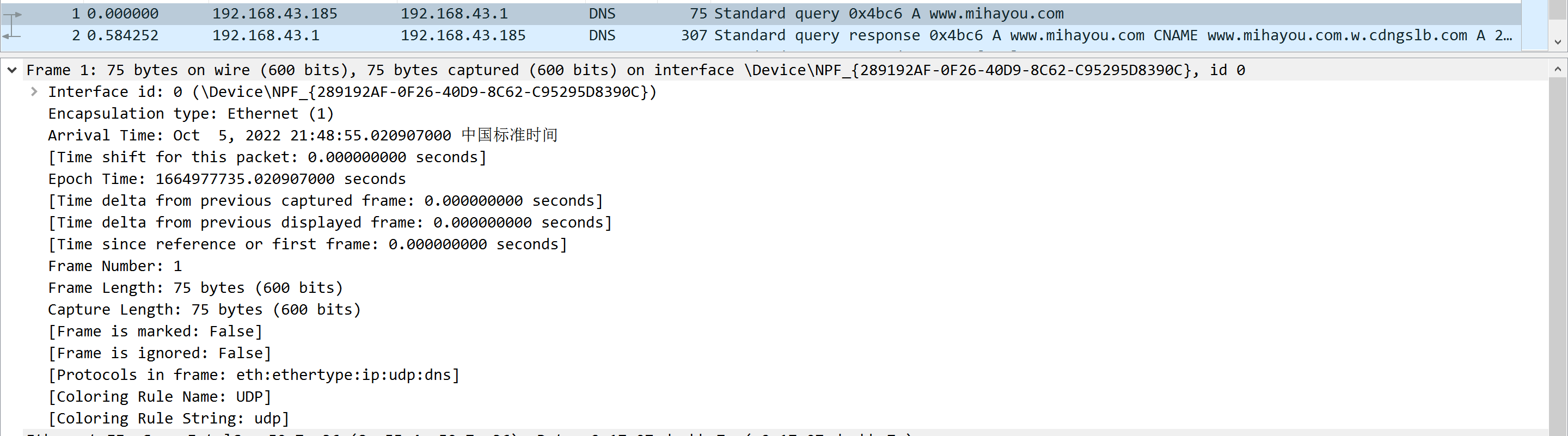
启动wireshark开始捕获，浏览器访问网站如www.mit.edu来触发，停止捕获，**操作之前使用ipconfig/flushdns清空dns缓存；**

方式二：使用dig命令：启动wireshark,命令行下执行dig命令，停止捕获。并【结合截图】回答以下问题：



1. DNS使用传输层的TCP还是UDP?

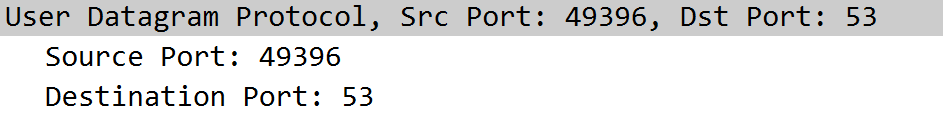
是udp



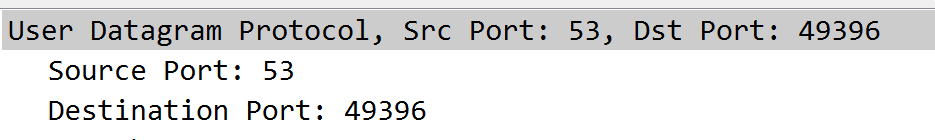
1. DNS query报文的目标端口号是？DNS response(reply)报文的源端口是？

query：

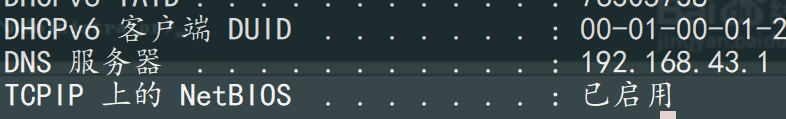
目标端口53，源端口49396



reply：目标端口：53，源端口：49396

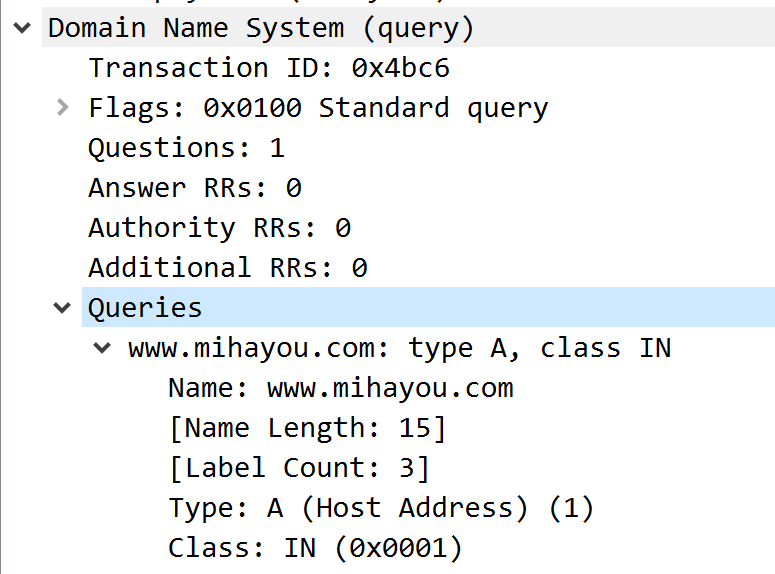


c.你的(local DNS server、authoritative DNS server)地址是什么？



1. 在DNS query报文中，该query报文的Type字段的值是什么？代表什么？

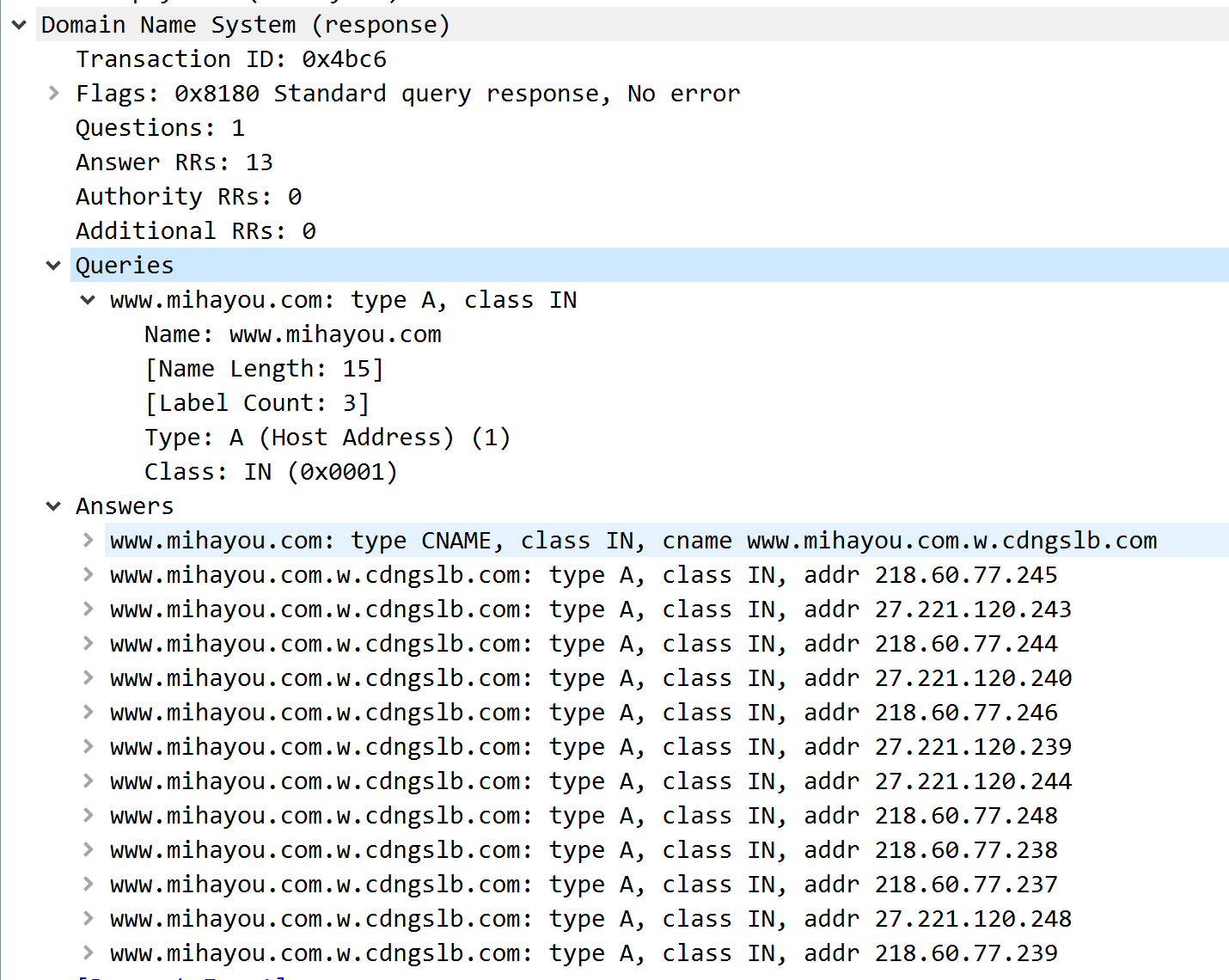
A记录，指定域名对应的IP地址。



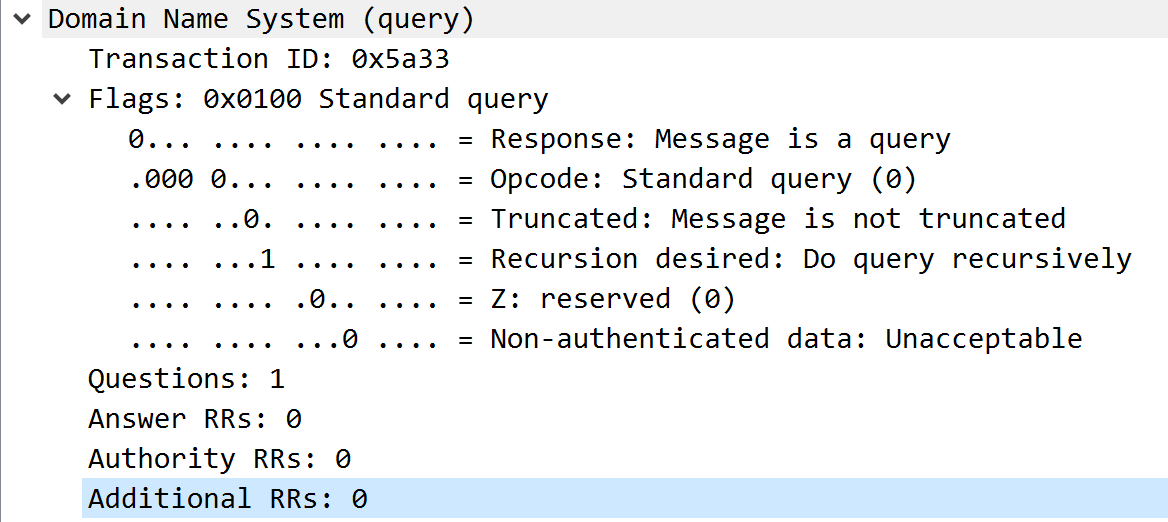
e.一次DNS解析，你捕获了几个DNS query报文？几个DNS reply报文？

30个query报文，23个reply报文

f.与query中的question对应的reply报文中的Answer是什么？



g.其他，你解读出的信息？



第一个是Transaction ID为标识字段,2字节,用于辨别DNS应答报文是哪个请求报文的响应，如图是0x5a33的响应

第二个是Flags标志字段,2字节,每一位的含义不同。

QR: 查询/响应,1为响应,0为查询，图上是0，在Response中也给了描述是query提示了。

Opcode: 查询或响应类型,这里0表示标准。

TC: 截断,1表示超过512字节并已被截断,0表示没有发生截断，没有截断

RD: 是否希望得到递归回答，如图，希望得到递归回答。

zero: 全0保留字段

DNS 请求报文中基础结构部分中包含的字段以及对应的值。在请求中 Questions 的值不可能为 0；Answer RRs，Authority RRs，Additional RRs 的值都为 0，因为在请求中还没有响应的查询结果信息。这些信息在响应包中会有相应的值。

 DNS 请求类型为 A，那么得到的响应信息也应该为 A 类型。

# 4 实验要求

(1)wireshark截图，并对报文结构、和交互过程进行文字分析说明。

(2)实验报告组成：截图、文字(分析、说明)