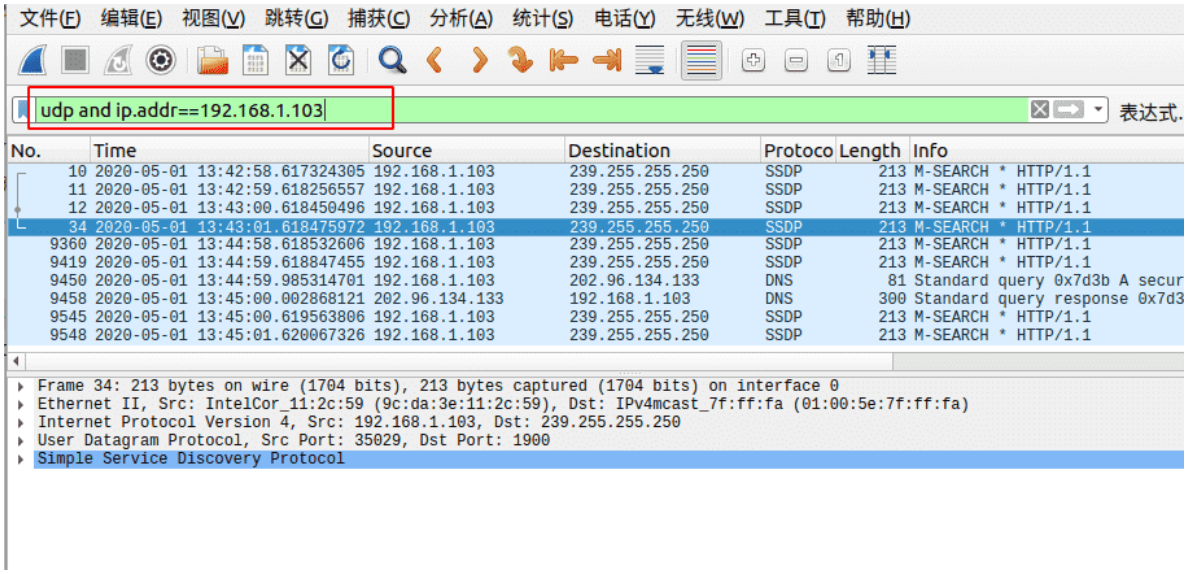
实验目的

了解UDP报文格式

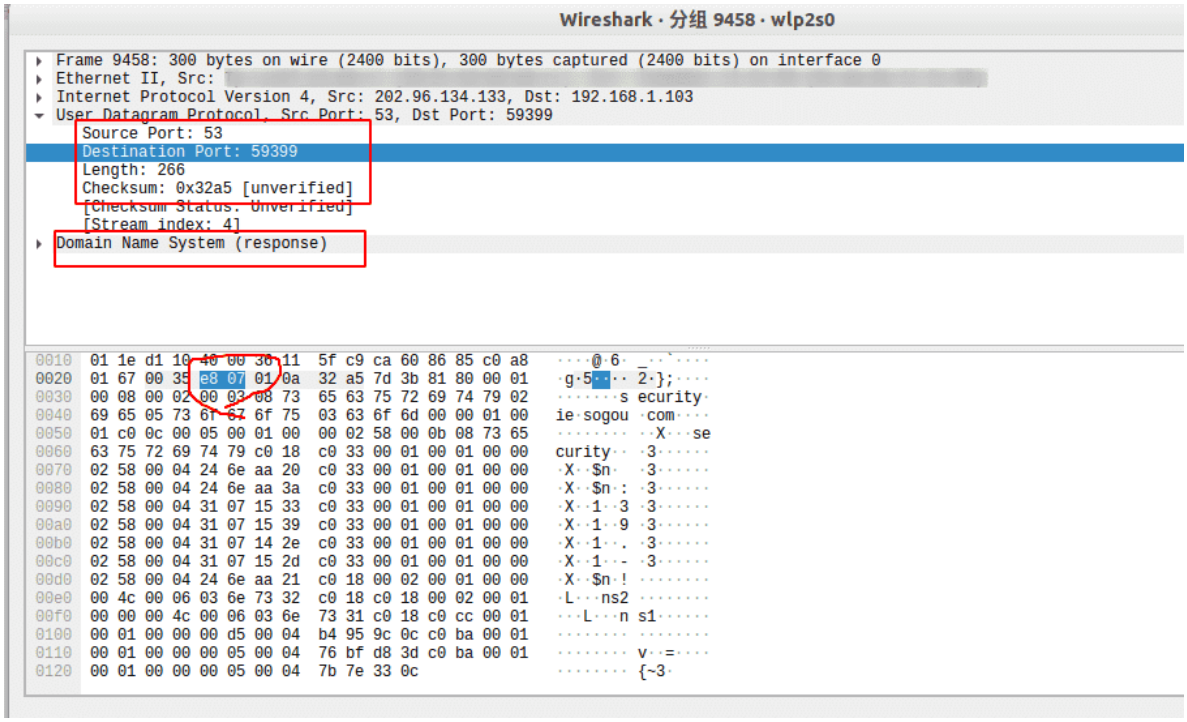
实验内容

`ifconfig` 找到自己的地址是 `192.168.1.103`，然后打开Wireshark开始嗅探，随便浏览器点点什么然后隔一小段时间停止抓包。在过滤表中输入条件 `udp and ip.addr==192.168.1.103`。



回答问题

1.从跟踪中选择一个UDP数据包，从此数据包中,确定UDP标头中有多少字段，并为这些字段命名。

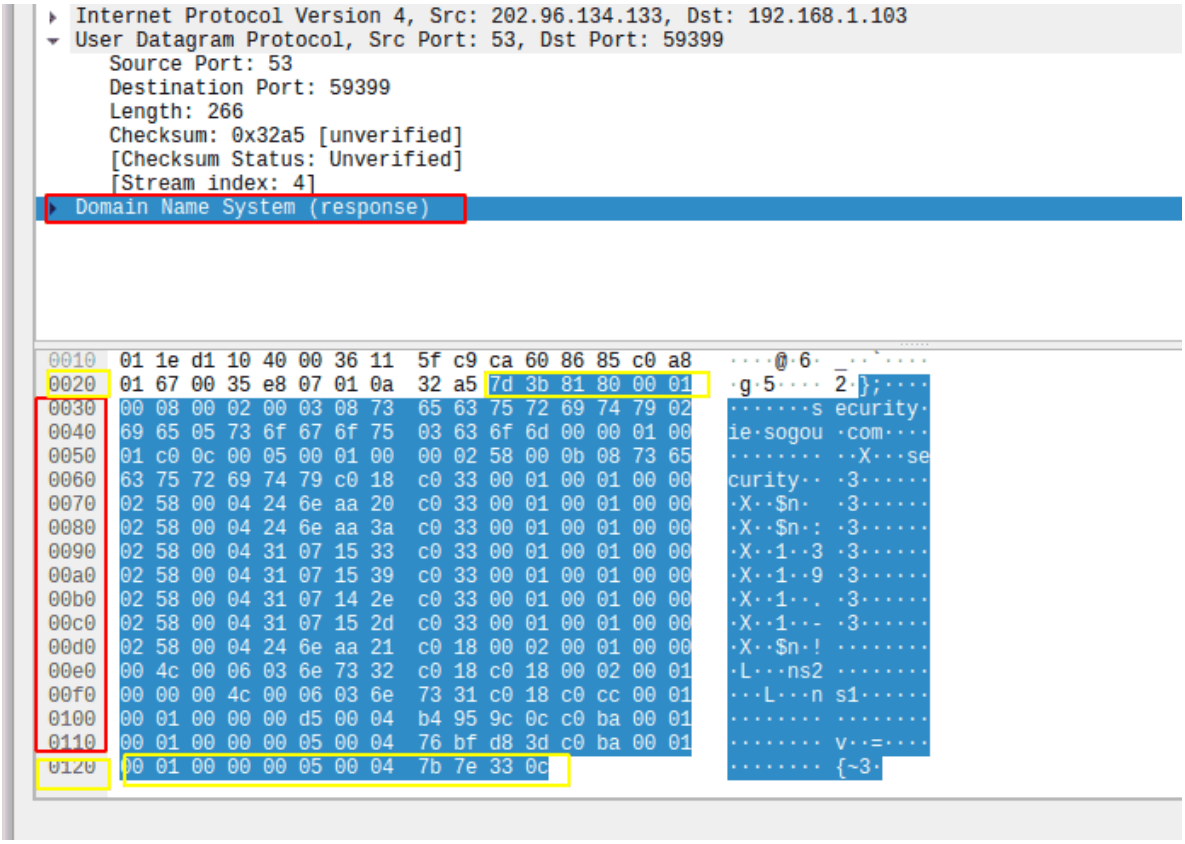


这是我随便选择的一个报文，可以看到UDP标头中有源端口src port，目的端口号dst port，长度length，校验和checksum。都是占2个字节。（图中圈出来的是目的端口号十六进制的表示形式，刚好是两个字节）

2.通过查询Wireshark的数据包内容字段中显示的信息,确定每个UDP报头字段的长度(以字节为单位)。

从上个回答就可以知道头字段的长度2*4=8个字节。

3.长度字段中的值是指的是什么?使用捕获的UDP数据包验证您的声明。



UDP中的length值为266个字节，刚好DNS的消息内容长度为258个byte，所以加上UDP的头部消息就是266个byte。
DNS：（0110-0030）= 16*14 16*14+12+6=258byte

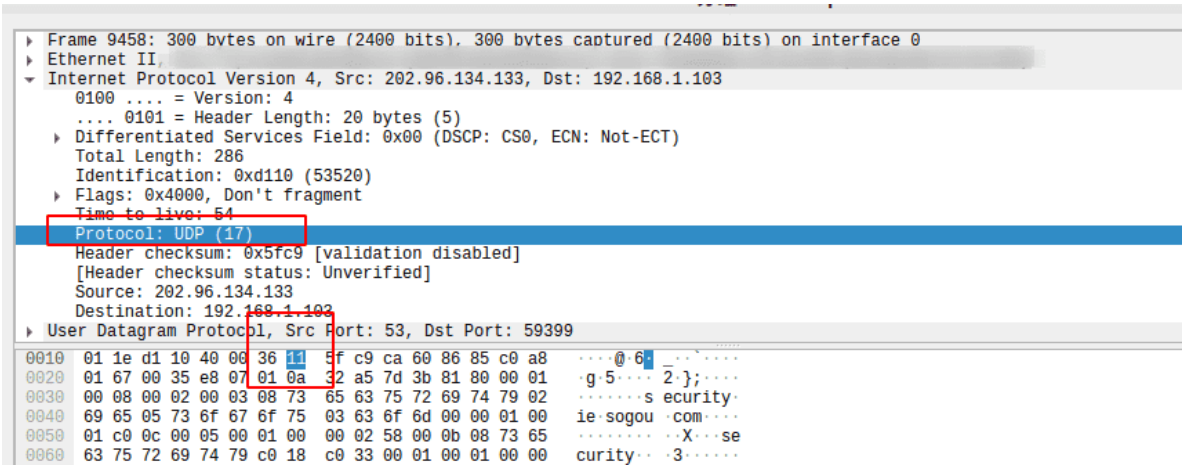
4.UDP有效负载中可包含的最大字节数是多少?

UDP头部的length是2个byte，所以可以包含的最大字节数是（2^16-1=65535）-8=65527byte。（UDP头部的length是以byte为单位的）

5.最大可能的源端口号是多少?

其实跟上道题同样的道理，最大的端口号是65535。

6.UDP的协议号是什么？以十六进制和十进制表示法给出答案。



在IP数据报里面显示UDP协议号是17，在下面的十六进制表示是0x11。

参考资料

> TCP支持的应用协议主要有：Telnet、FTP、SMTP等；
>
> UDP支持的应用层协议主要有：NFS（网络文件系统）、SNMP（简单网络管理协议）、DNS（主域名称系统）、TFTP（通用文件传输协议）等。