**计算机网络2022**

作业5

1. 以下各图是利用抓包工具Wireshark捕获主机192.168.1.102访问WEB站点www.sohu.com的部分数据包，请回答下列问题：

(1) DNS有哪两种解析方法？当前的DNS服务器地址是什么？ （2分）

递归 迭代

202.101.172.35

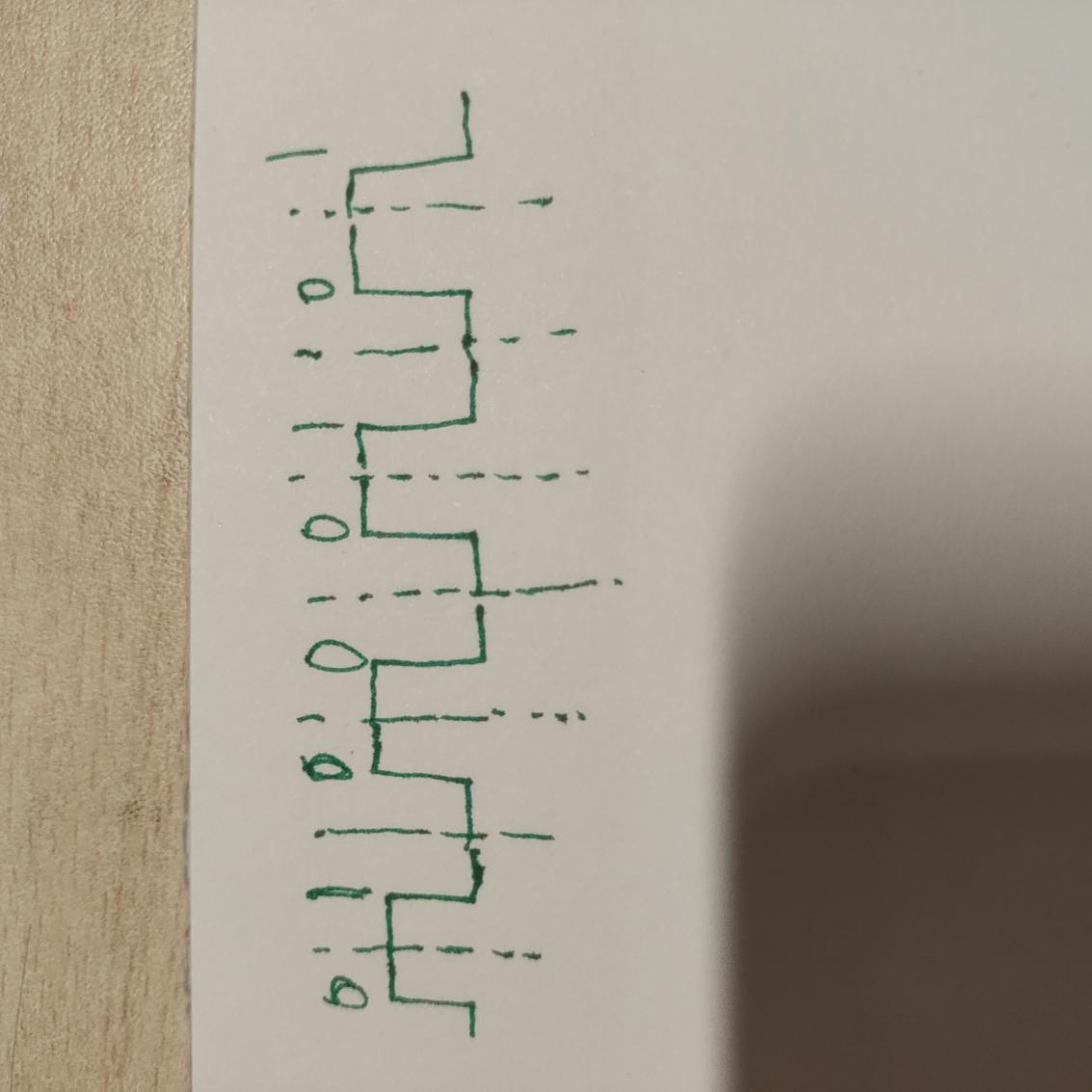
1. 访问www.sohu.com的主机地址192.168.1.102是一个什么类型的IP地址？重定向后，源主机从哪台主机获取Web页面数据? （2分）

C类 114.80.130.92

1. 网络层的协议类型和长度字段值为45H，请画出该数值对应的曼彻斯特编码波形图。（2分）

45H

01000101



(4) 编号375的数据包中的win=64240表示什么？在传输层流量控制中有何作用？（2分）

TCP接收缓存大小 控制流速

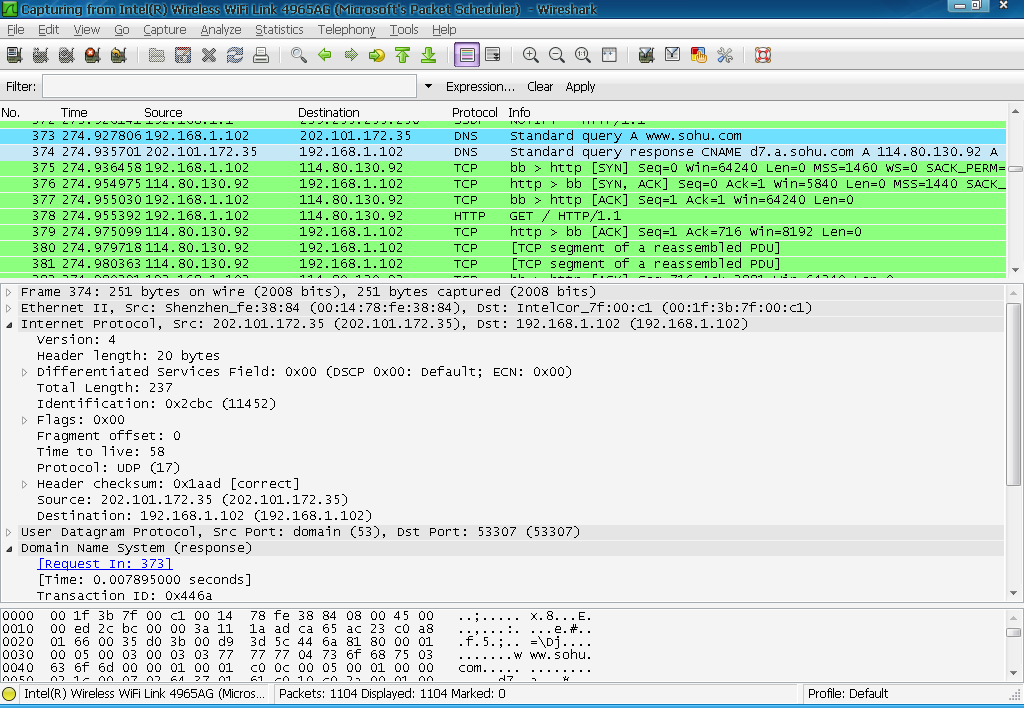
(5) 请从图中找出所有用于建立http连接的握手数据包，并指出其传输层协议名称。（2分）

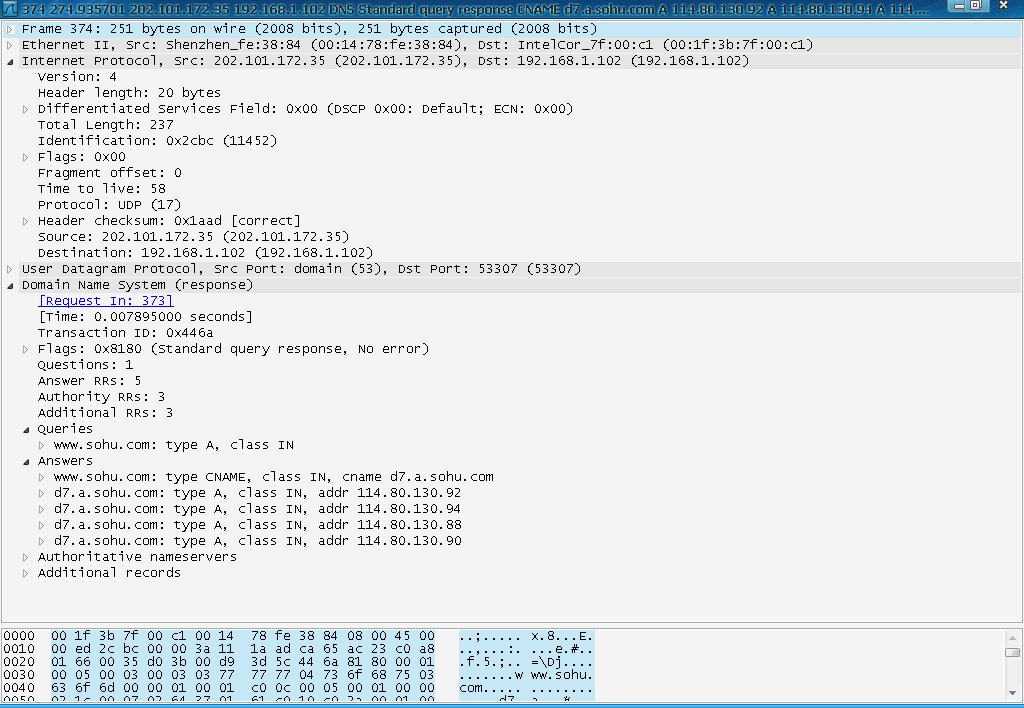
375 376 377

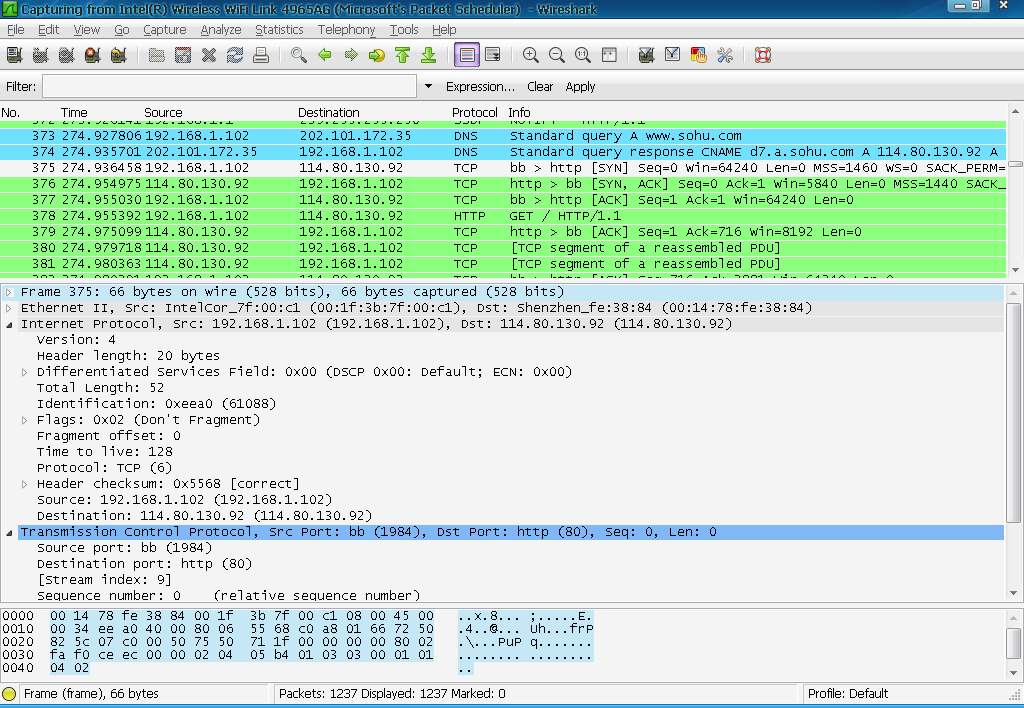
TCP

(6) 源主机和WEB站点间连接的源端口和目的端口分别是多少？（2分）

1984 80







2. 请阅读以下材料并回答相关问题：

（a）据新浪科技报道，著名中文搜索引擎百度于2010年1月12日上午遭受黑客攻击，其域名DNS服务器和主域名[www.baidu.com](http://www.baidu.com)被劫持，导致输入域名后首页无法正常访问，部分能打开的首页自动跳转到带有伊朗国旗和“Iranian Cyber Army”字样的页面，直到12日下午5点，各地百度域名才陆续恢复正常访问。

（b）Windows中的命令nslookup可以获取域名对应的IP地址，下图1是在命令窗口输入“nslookup www.baidu.com”后返回的结果：

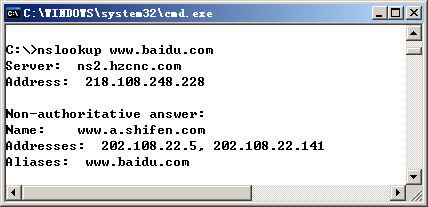
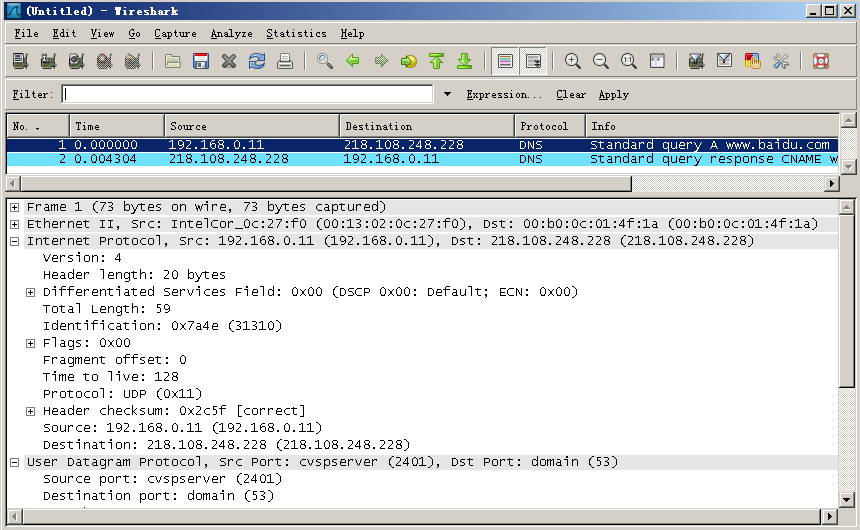


图1 命令返回结果

（c）利用抓包工具Wireshark对刚才nslookup命令产生的数据包进行捕获，可以抓到DNS查询相关的两个数据包，详细信息如下图2所示：

图2 Wireshark抓包结果

请结合以上材料，回答下列问题：

1. 什么是DNS？DNS服务器的域名解析算法有哪两种？（3分）

域名服务，提供域名和IP地址之间的解析功能。

递归 迭代

1. 从以上图示可以知道，主机访问的DNS服务器IP地址是多少？访问过程中依赖的传输层协议是什么协议？（2分）

218.108.248.228

UDP协议

1. 从捕获的数据包可以得知，源主机用来连接DNS服务器的源端口是多少？该DNS查询的IP数据包的数据部分的长度是多少字节？（3分）

2401

59

1. 结合DNS服务器域名解析原理，你认为这次百度受到攻击导致首页无法正常访问的原因是什么？（2分）

攻击者劫持域名，使原域名转向了另外的服务器。

（5）请解释基于WWW的搜索引擎的基本工作原理。（2分）

将查询到的信息储存在数据库中，搜索引擎可以在这数据库中提供所需信息。