浙大城市学院实验报告

- 课程名称：计算机网络实验
- 实验项目名称：实验十二 Wireshark抓包软件高级
- 学生姓名：徐彬涵
- 专业班级：软件工程2003
- 学号：32001272
- 实验成绩：
- 指导老师：霍梅梅
- 日期：2022/05/12

一. 实验目的和要求

1. 进一步学习掌握Wireshark过滤规则的设置
2. 使用Wireshark捕获Ethernet帧，并对高层协议数据包进行分析

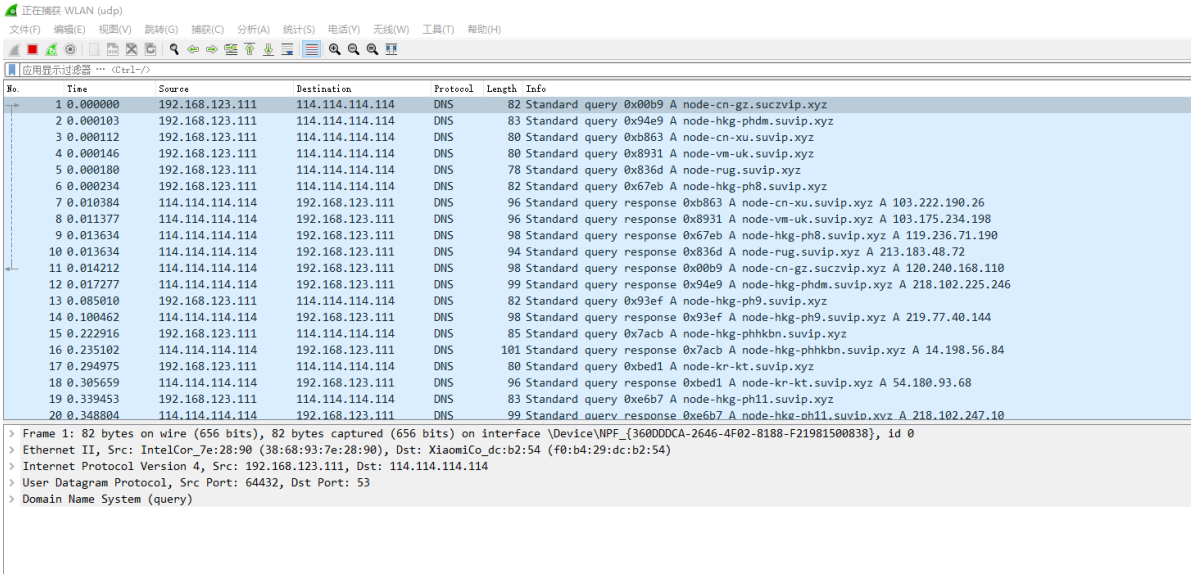
二. 实验内容、原理及实验结果与分析

在**Wireshark**中创建并设置以下过滤规则

1.1 捕获局域网上的所有**UDP**数据包

【过滤规则】

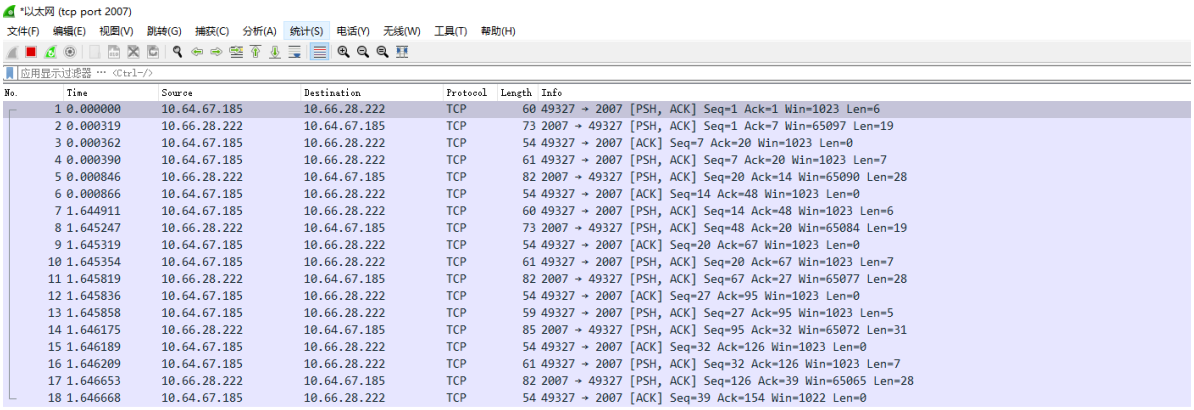
```
udp
```



1.2 捕获本地主机收到和发出的所有FTP数据包

【过滤规则】

```
1 tcp port 21 || tcp port 20
2 tcp port 2007
```



1.3 捕获本地主机和某一主机之间的远程桌面控制数据包（TCP端口3389）

【过滤规则】

```
1 tcp port 3389
```

1.4 捕获本地主机和www.zucc.edu.cn之间的通信

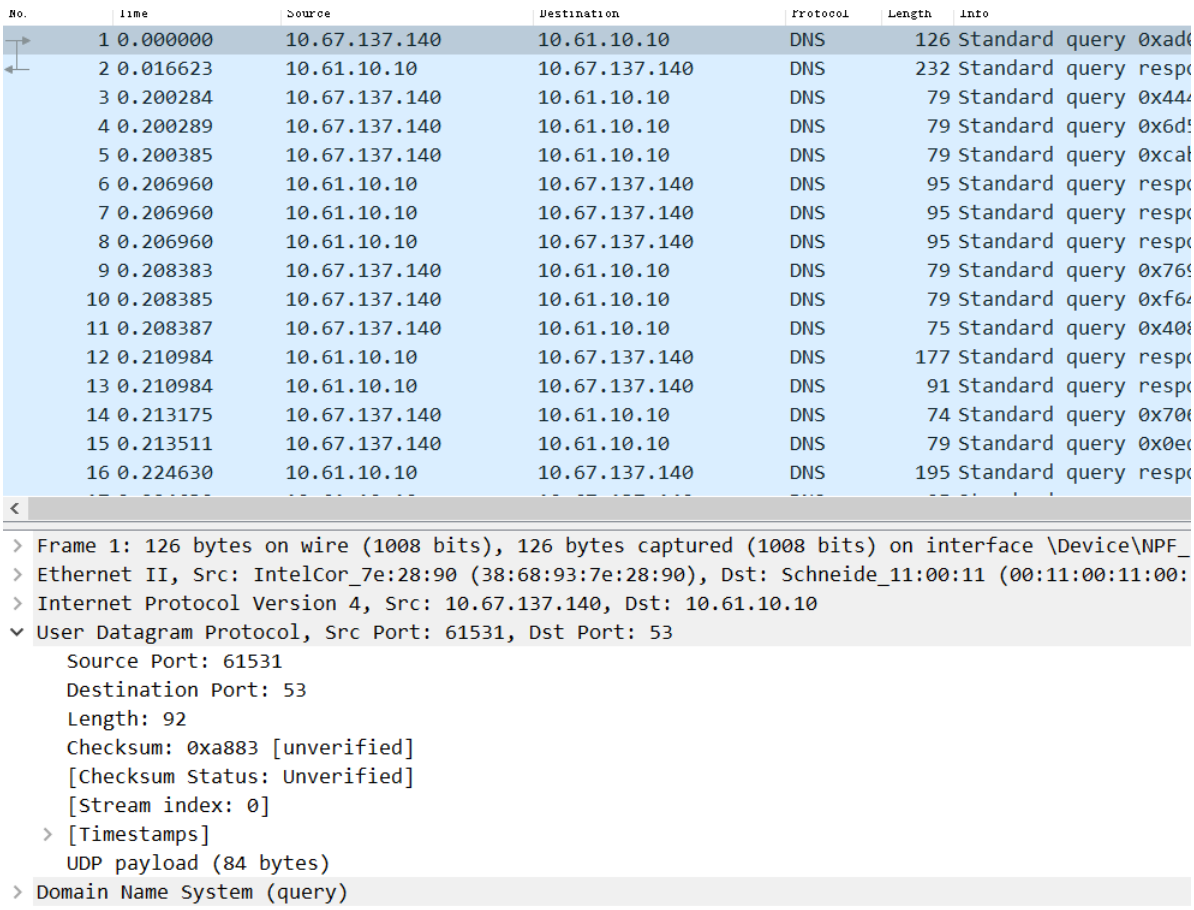
【过滤规则】

```
1 host www.baidu.com
```

捕获并解析TCP/IP协议的高层协议数据包

2.1 捕获解析本机发出或接收的**UDP**数据包，并对照**UDP**报头格式进行解释（如发送**QQ**信息构造**UDP**数据包）

【实验结果与分析】



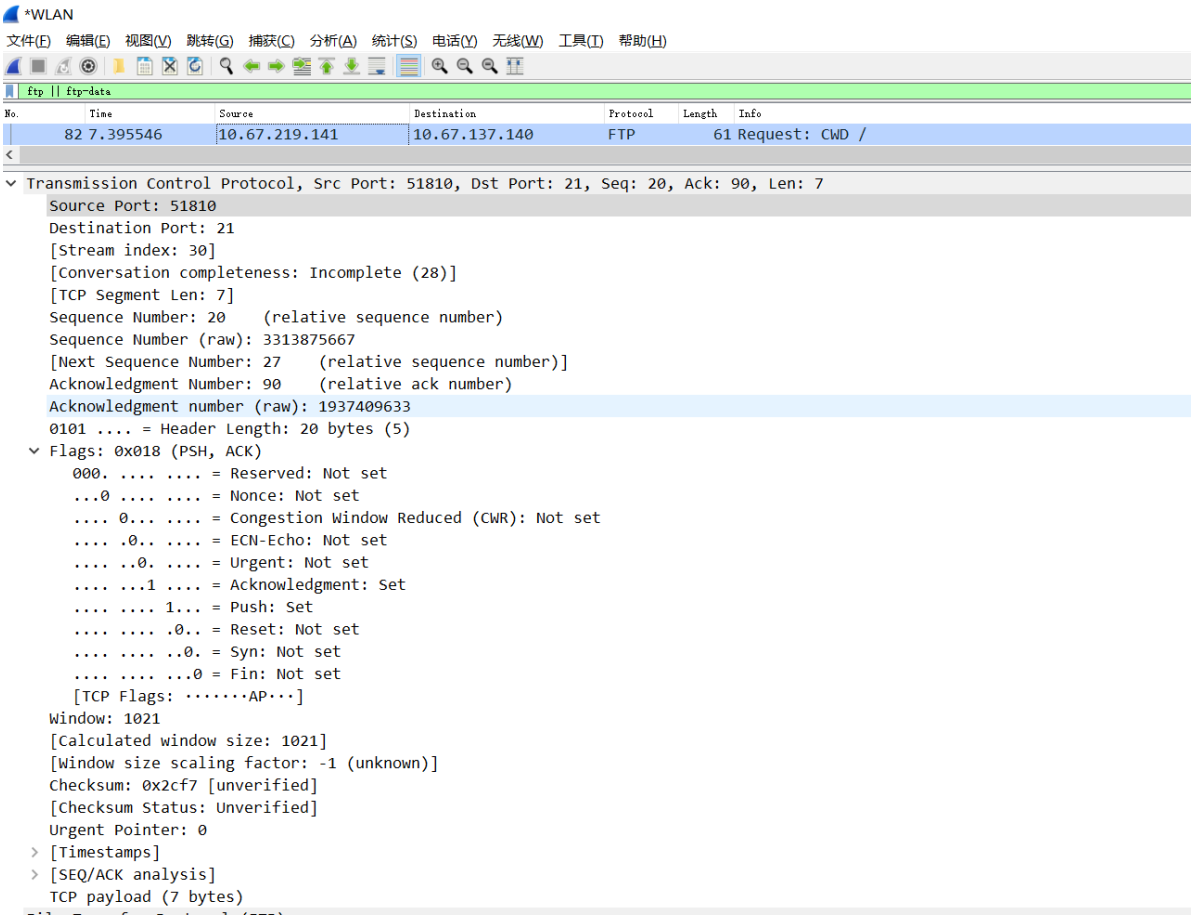
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.67.137.140	10.61.10.10	DNS	126	Standard query 0xad
2	0.016623	10.61.10.10	10.67.137.140	DNS	232	Standard query resp
3	0.200284	10.67.137.140	10.61.10.10	DNS	79	Standard query 0x44
4	0.200289	10.67.137.140	10.61.10.10	DNS	79	Standard query 0x6d
5	0.200385	10.67.137.140	10.61.10.10	DNS	79	Standard query 0xca
6	0.206960	10.61.10.10	10.67.137.140	DNS	95	Standard query resp
7	0.206960	10.61.10.10	10.67.137.140	DNS	95	Standard query resp
8	0.206960	10.61.10.10	10.67.137.140	DNS	95	Standard query resp
9	0.208383	10.67.137.140	10.61.10.10	DNS	79	Standard query 0x76
10	0.208385	10.67.137.140	10.61.10.10	DNS	79	Standard query 0xf6
11	0.208387	10.67.137.140	10.61.10.10	DNS	75	Standard query 0x40
12	0.210984	10.61.10.10	10.67.137.140	DNS	177	Standard query resp
13	0.210984	10.61.10.10	10.67.137.140	DNS	91	Standard query resp
14	0.213175	10.67.137.140	10.61.10.10	DNS	74	Standard query 0x70
15	0.213511	10.67.137.140	10.61.10.10	DNS	79	Standard query 0x0e
16	0.224630	10.61.10.10	10.67.137.140	DNS	195	Standard query resp

```
> Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_7e:28:90 (38:68:93:7e:28:90), Dst: Schneide_11:00:11 (00:11:00:11:00:
> Internet Protocol Version 4, Src: 10.67.137.140, Dst: 10.61.10.10
v User Datagram Protocol, Src Port: 61531, Dst Port: 53
    Source Port: 61531
    Destination Port: 53
    Length: 92
    Checksum: 0xa883 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (84 bytes)
> Domain Name System (query)
```

长度	2字节	2字节	2字节	2字节	长度可变
字段	Source Port(源端口)	Destination Port(目标端口)	Length(长度)	Checksum(校检值)	Data(数据)
值	61531	53	92	0xa883	

2.2 捕获解析本地主机发出及收到的**FTP**数据包，并对照**TCP**报头格式进行解释，同时分析**FTP**发出的命令和响应（如 ftp://10.66.28.222：**2007**构造**FTP**数据包）

【实验结果与分析】



长度	**16**位	**16**位
字段	Source Port(源端口)	Destination Port(目标端口)
值	51810	21

长度	**32**位	**32**位
字段	Sequence Number(数据序号)	Acknowledgment Number(确认序号)
值	20	90

长度	**4**位	**6**位
字段	Header Length(首部长度)	Reversed(保留)
值	20	0

Flags(标志)

长度	**1**位	**1**位	**1**位	**1**位	**1**位	**1**位
字段	URG(紧急指针	ACK(确认序号	PSH(接收方应该尽快将这个报文	RST(重建连	SYN(同步序号发起连	FIN(发端完成发送任

	标志)	有效)	段交结应用层)	接)	接)	务)
长度	1位	1位	1位	1位	1位	1位
值	0	1	1	0	0	0

长度	16位	16位	16位
字段	Window size(窗口大小)	Checksum(校检和)	紧急指针
值	1021	0x2cf7	0

ftp || ftp-data

o.	Time	Source	Destination	Protocol	Length	Info
73	7.360741	10.67.219.141	10.67.137.140	FTP	60	Request: noop
74	7.361174	10.67.137.140	10.67.219.141	FTP	84	Response: 200 noop command successful.
76	7.372231	10.67.219.141	10.67.137.140	FTP	61	Request: CWD /
77	7.372810	10.67.137.140	10.67.219.141	FTP	83	Response: 250 CWD command successful.
79	7.383846	10.67.219.141	10.67.137.140	FTP	60	Request: noop
80	7.384139	10.67.137.140	10.67.219.141	FTP	84	Response: 200 noop command successful.
82	7.395546	10.67.219.141	10.67.137.140	FTP	61	Request: CWD /
83	7.396075	10.67.137.140	10.67.219.141	FTP	83	Response: 250 CWD command successful.
85	7.405835	10.67.219.141	10.67.137.140	FTP	59	Request: PWD
86	7.406094	10.67.137.140	10.67.219.141	FTP	85	Response: 257 "/" is current directory.
88	7.416789	10.67.219.141	10.67.137.140	FTP	61	Request: CWD /
89	7.417420	10.67.137.140	10.67.219.141	FTP	83	Response: 250 CWD command successful.
91	7.425709	10.67.219.141	10.67.137.140	FTP	62	Request: TYPE I
92	7.426055	10.67.137.140	10.67.219.141	FTP	74	Response: 200 Type set to I.
94	7.436093	10.67.219.141	10.67.137.140	FTP	60	Request: PASV
95	7.436935	10.67.137.140	10.67.219.141	FTP	106	Response: 227 Entering Passive Mode (10,67,137,140,204,239).
100	7.457960	10.67.219.141	10.67.137.140	FTP	69	Request: SIZE test.txt
101	7.458724	10.67.137.140	10.67.219.141	FTP	61	Response: 213 4
103	7.468885	10.67.219.141	10.67.137.140	FTP	69	Request: RETR test.txt
104	7.469507	10.67.137.140	10.67.219.141	FTP	108	Response: 125 Data connection already open; Transfer starting.
106	7.506172	10.67.137.140	10.67.219.141	FTP-DA…	58	FTP Data: 4 bytes (PASV) (SIZE test.txt)
109	7.592158	10.67.137.140	10.67.219.141	FTP	78	Response: 226 Transfer complete.

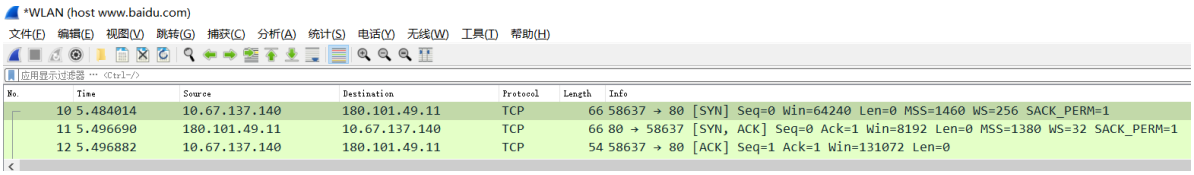
110： 重新启动标记应答。	332： 登录时需要帐户信息
120： 在n分钟内准备好	350： 下一步命令
125： 连接打开准备传送	421： 不能提供服务，关闭控制连接
150： 打开数据连接	425： 不能打开数据连接
200： 命令成功	426： 关闭连接，中止传输
202： 命令失败	450： 请求的文件操作未执行
211： 系统状态	451： 中止请求的操作：有本地错误
212： 目录状态	452： 未执行请求的操作：系统存储空间不足
213： 文件状态	500： 格式错误，命令不可识别
214： 帮助信息	501： 参数语法错误
215： 名字系统类型	502： 命令未实现
220： 新用户服务准备好了	503： 命令顺序错误
221： 服务关闭控制连接，可以退出登录	504： 此参数下的命令功能未实现
225： 数据连接打开，无传输正在进行	530： 未登录
226： 关闭数据连接，请求的文件操作成功	532： 存储文件需要帐户信息
227： 进入被动模式	550： 未执行请求的操作
230： 用户登录	551： 请求操作中止：页类型未知
250： 请求的文件操作完成	552： 请求的文件操作中止，存储分配溢出
257： 创建"PATHNAME"	553： 未执行请求的操作：文件名称检测通
331： 用户名正确，需要口令	

这里我进行了从ftp下载文件到本地的操作，客户端向服务端发送请求test.txt文件的操作，服务端回应125表示连接打开准备传送，传送完成后服务端发送226表示关闭数据连接，请求的文件操作成功

我这里使用的是匿名登录，但如果是用户登录的话用户名和密码都会直接以明文方式显示在ftp数据包中，所以ftp是不安全的协议

2.3 捕获解析本机和一特定**WWW**服务器之间的通信（如www.baidu.com），找出其中三次握手的数据包，并进行解释，同时分析**HTTP**的命令和响应

【实验结果与分析】



客户端：10.67.137.140

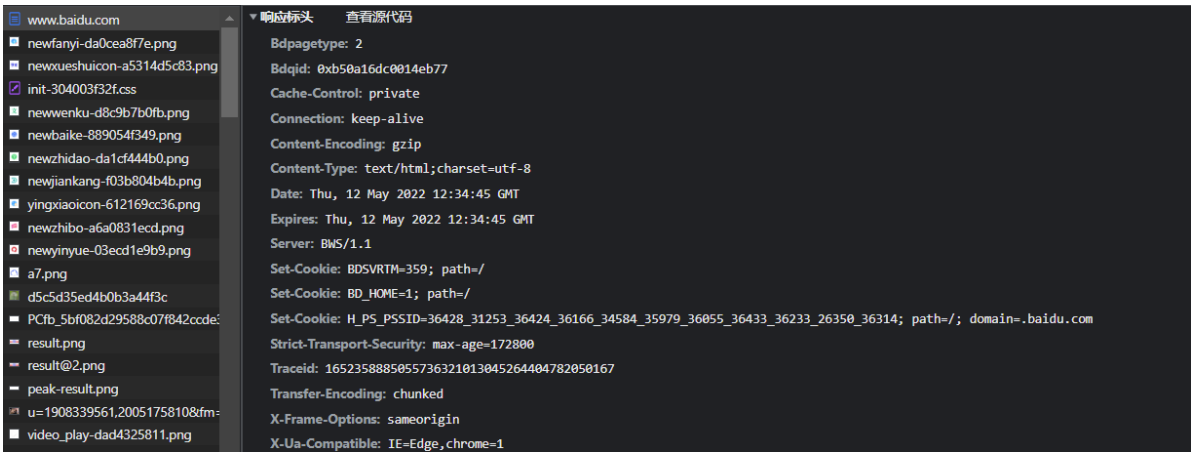
服务端：180.101.49.11

1. 客户端向服务端发送建立连接请求，标志位SYN为1
2. 服务端接收到客户端的请求后，向客户端同样发送确认建立连接报文，标志位SYN为1,ACK为第一个数据包的SEQ+1
3. 客户端接收到服务端的回应后，向服务端发送确认报文ACK为第二个数据包的SEQ+1

- HTTP命令（主要）
  - GET
  - POST

- 响应标头
  - Bdpagetype 页面类型
  - Bdqid
  - Cache-Control 通用消息头字段，被用于在http请求和响应中，通过指定指令来实现缓存机制
  - Connection 决定当前的事务完成后，是否会关闭网络连接
  - Content-Encoding 列出了对当前实体消息（消息荷载）应用的任何编码类型，以及编码的顺序
  - Content-Type 实体头部用于指示资源的MIME类型
  - Date 当前的GMT时间
  - Expires 响应头包含日期/时间，即在此时候之后，响应过期
  - Server 服务器名字
  - Set-Cookie 设置和页面关联的Cookie
  - Strict-Transport-Security 是一个安全功能，它告诉浏览器只能通过HTTPS访问当前资源，而不是HTTP

- Traceid 全链路日志追踪
- Transfer-Encoding 指明了将 entity 安全传递给用户所采用的编码形式。
- X-Frame-Options 用来给浏览器指示允许一个页面可否在frame、iframe、embed或者object中展现的标记。站点可以通过确保网站没有被嵌入到别人的站点里面，从而避免点击劫持 攻击
- X-Ua-Compatible 可以指定网页的兼容性模式设置



三. 讨论、心得

记录实验感受、上机过程中遇到的困难及解决办法、遗留的问题、意见和建议等。