

# 利用Wireshark观察网络报文

曹旭磊

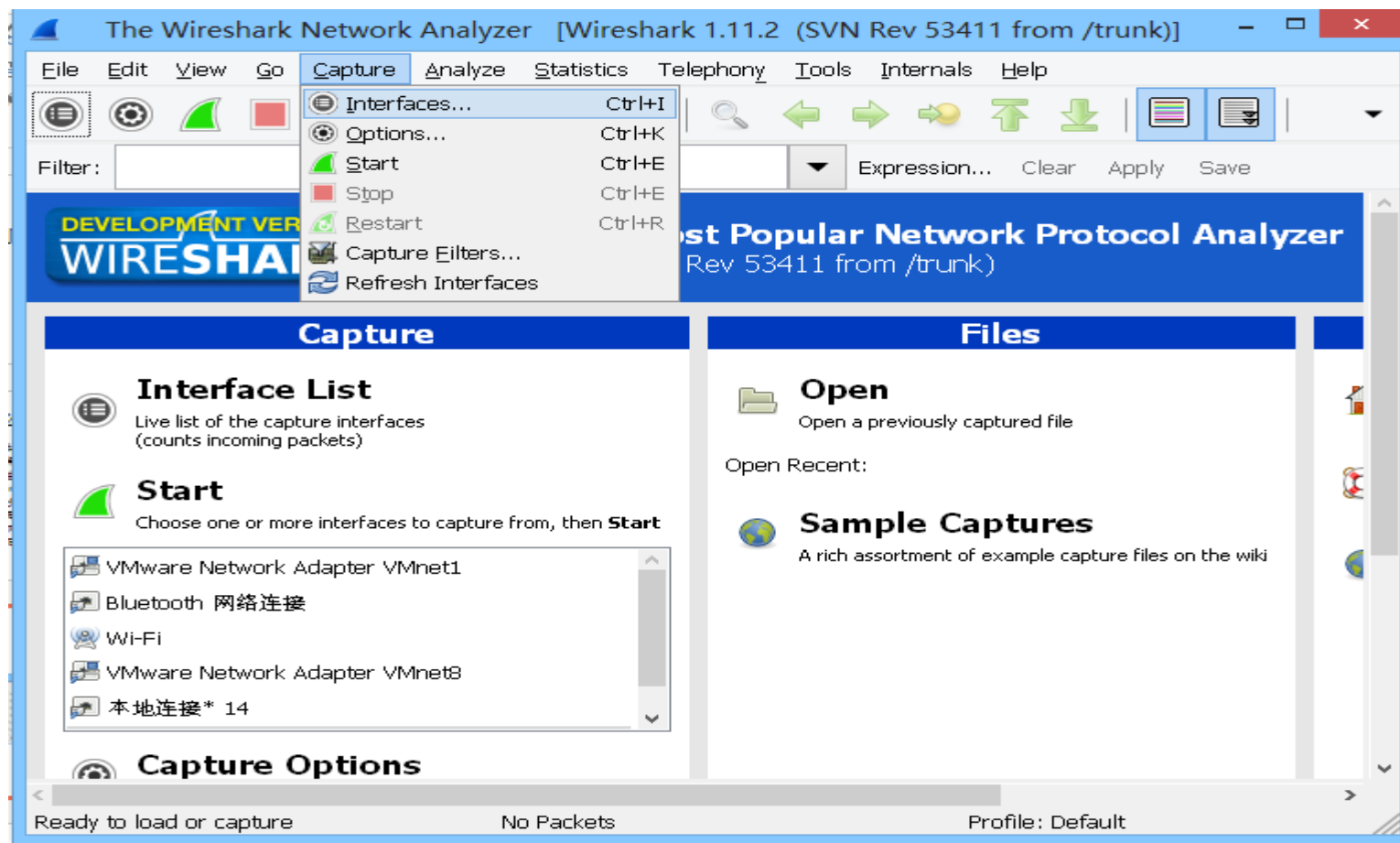
2013.11.24

# 什么是Wireshark

- 网络协议分析器是对通用协议的数据包进行解码并以人可读的格式显示网络流量内容的软件或设备。
- **Wireshark**（前称Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。
- 抓取报文+协议分析

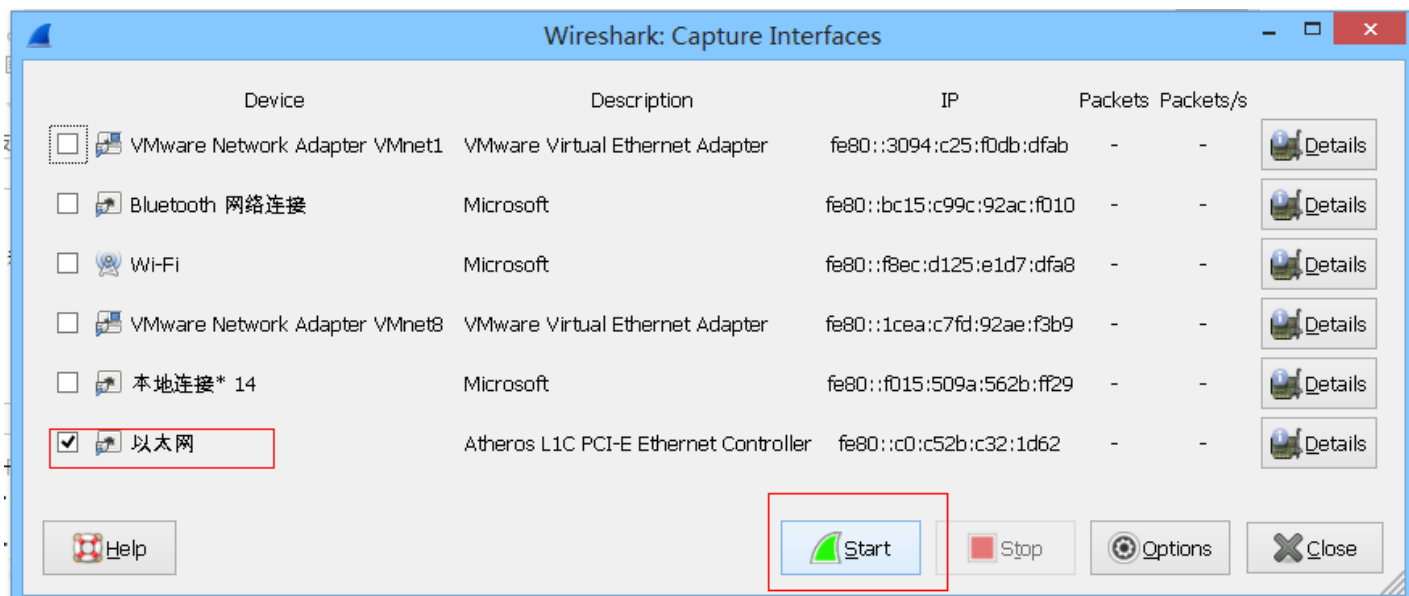
# 利用Wireshark观察网络报文

1、打开wireshark      可在ftp: 222.195.68.83下载软件



# 利用Wireshark观察网络报文

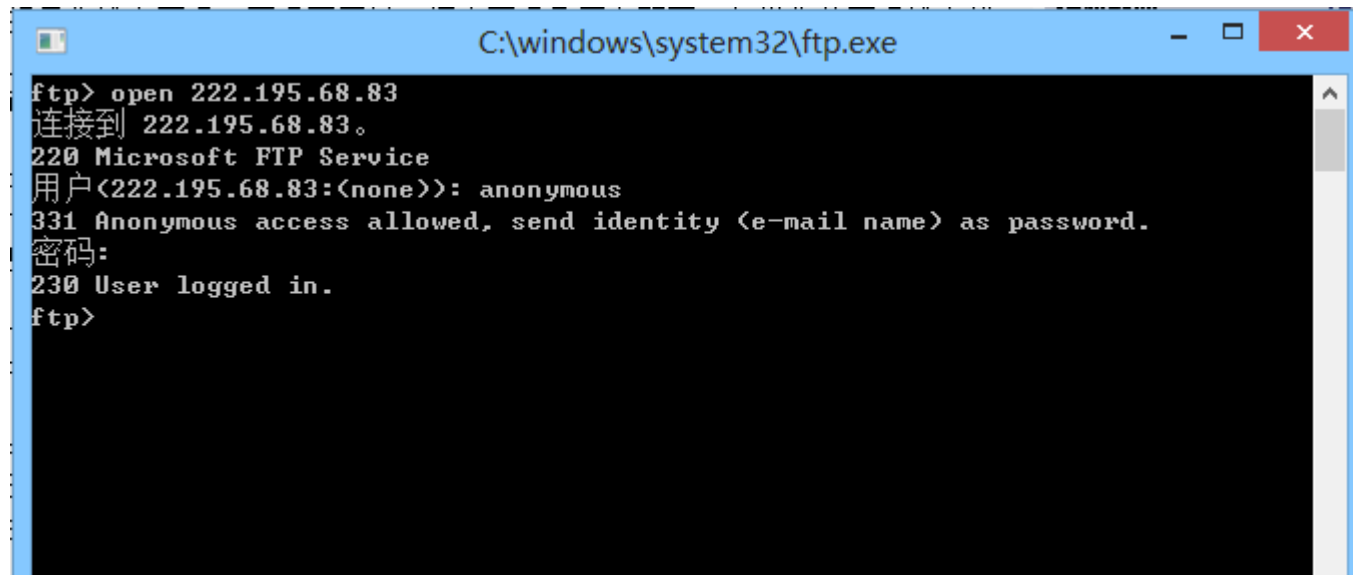
- 2、设置抓取数据包的接口： Capture->Interfaces
- 根据实际情况勾选相应接口



- 1.观察TCP三次握手过程

通过抓取FTP登陆过程数据包，深入了解TCP三次握手过程。

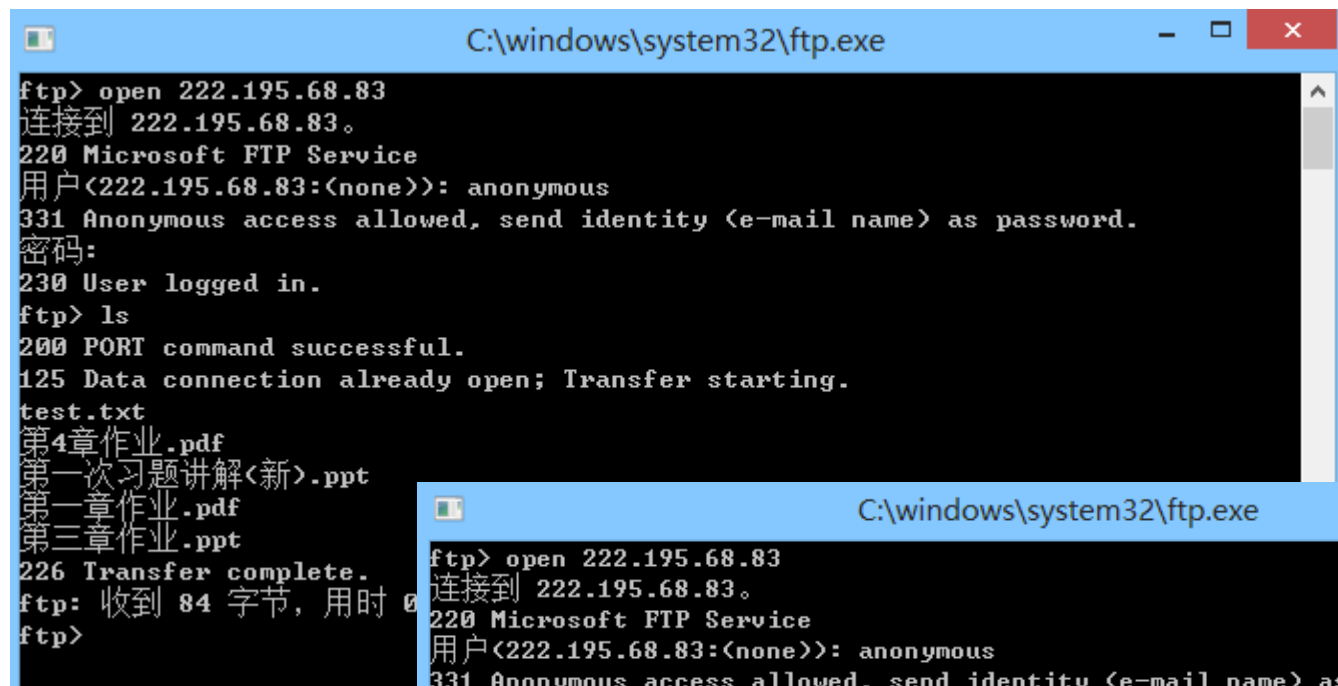
a.按键“WIN+R”输入FTP，调出终端。输入open +FTP地址，可以使用实验室FTP试验。



```
ftp> open 222.195.68.83
连接到 222.195.68.83。
220 Microsoft FTP Service
用户(222.195.68.83:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
密码:
230 User logged in.
ftp>
```

b.输入用户名anonymous，密码： any string

c.列出FTP服务器目录: `ls`



```
C:\windows\system32\ftp.exe
ftp> open 222.195.68.83
连接到 222.195.68.83。
220 Microsoft FTP Service
用户(222.195.68.83:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
密码:
230 User logged in.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
test.txt
第4章作业.pdf
第一次习题讲解<新>.ppt
第一章作业.pdf
第三章作业.ppt
226 Transfer complete.
ftp: 收到 84 字节, 用时 0.00秒 42.00千字节/秒。
ftp>
```

d.切换到本地目录

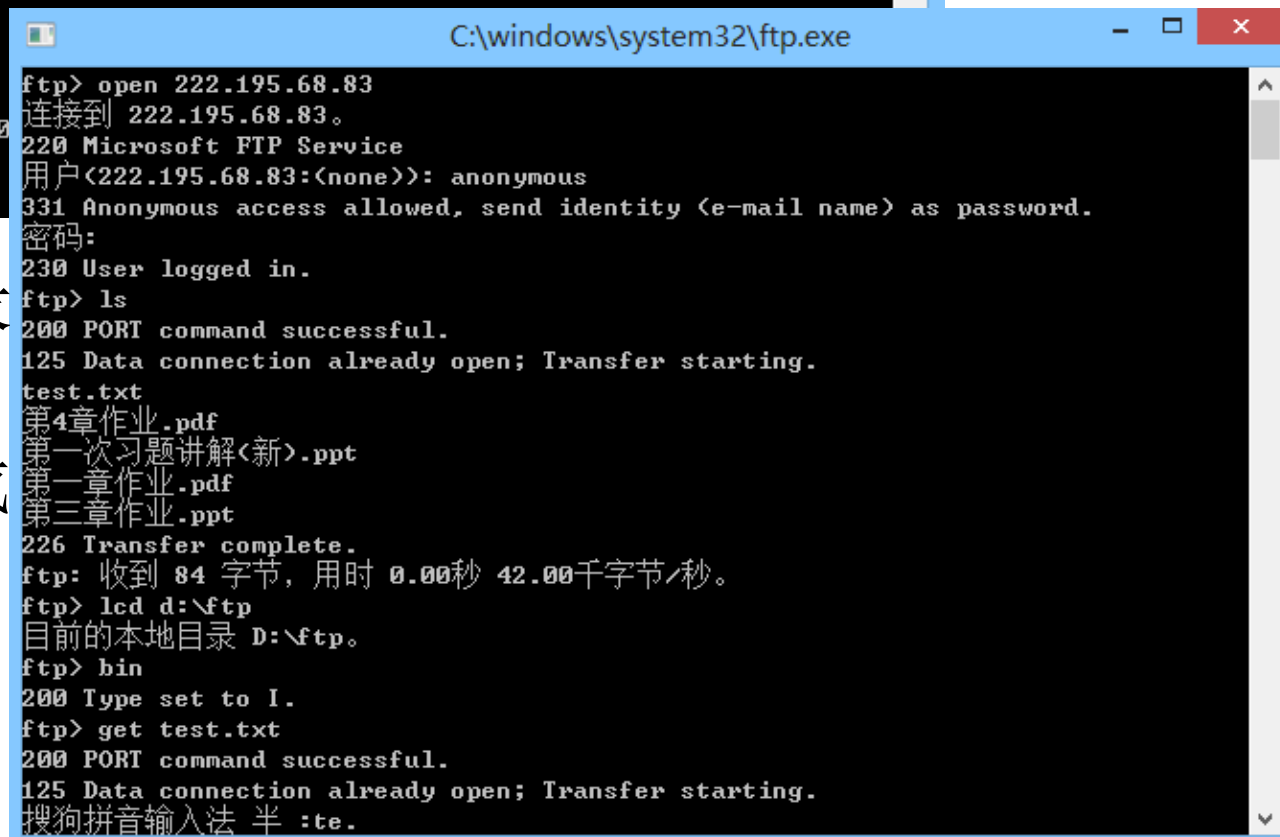
`lcd d:\ftp`

e.使用二进制下载

`bin`

f.下载文件

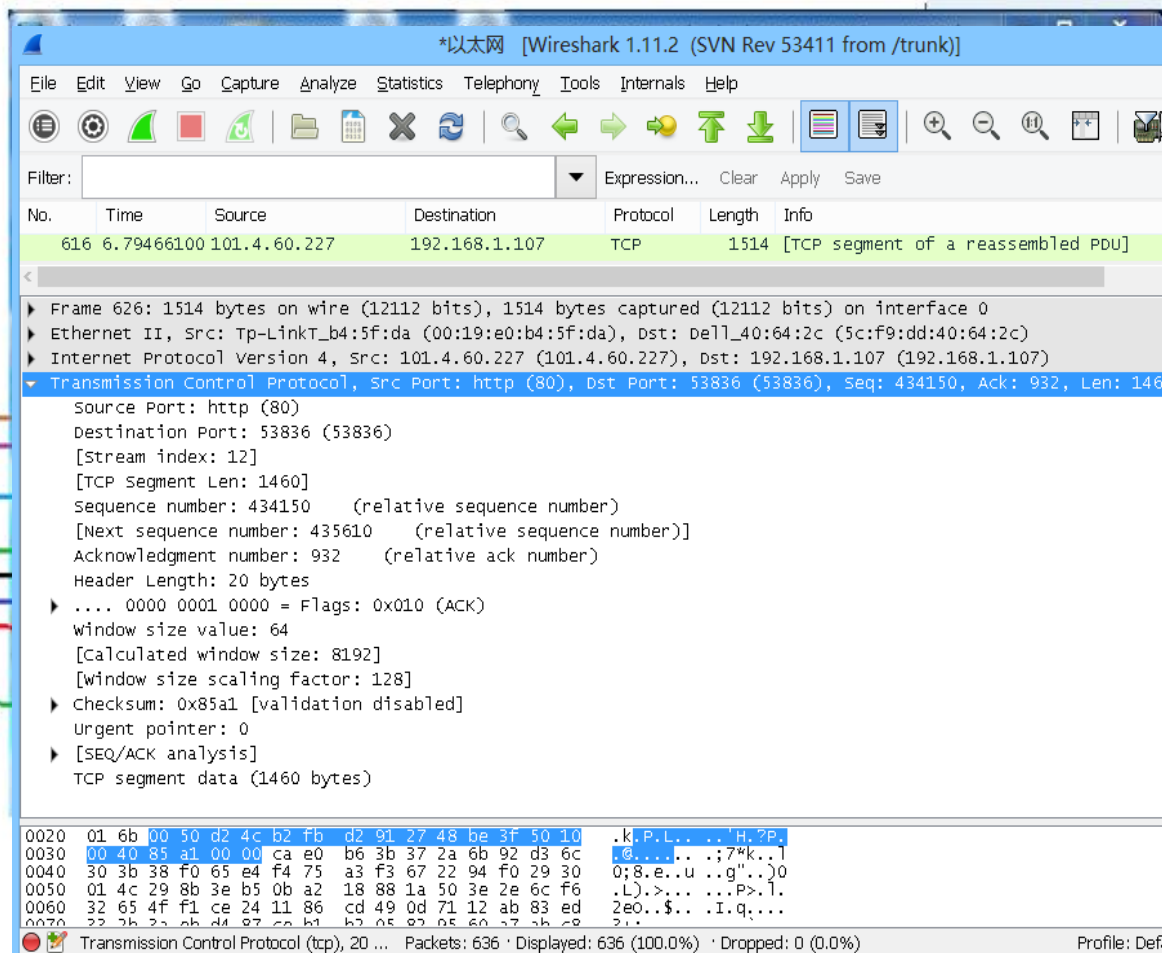
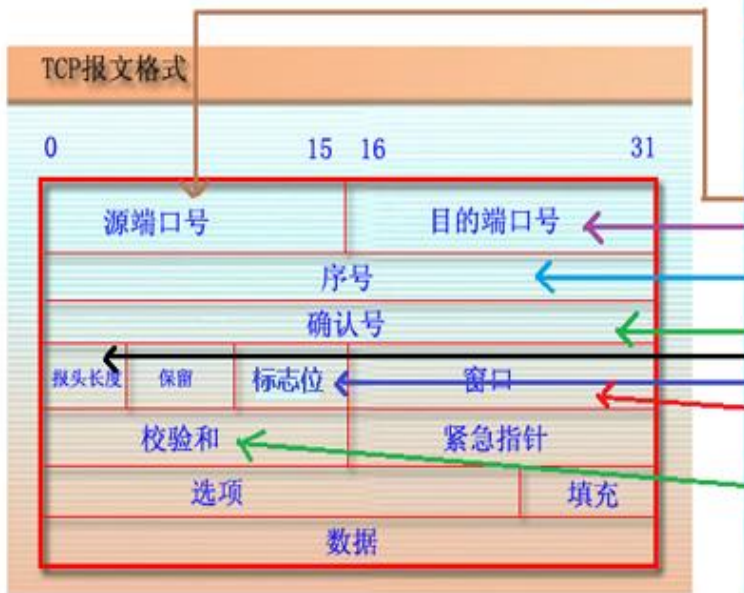
`get test.txt`



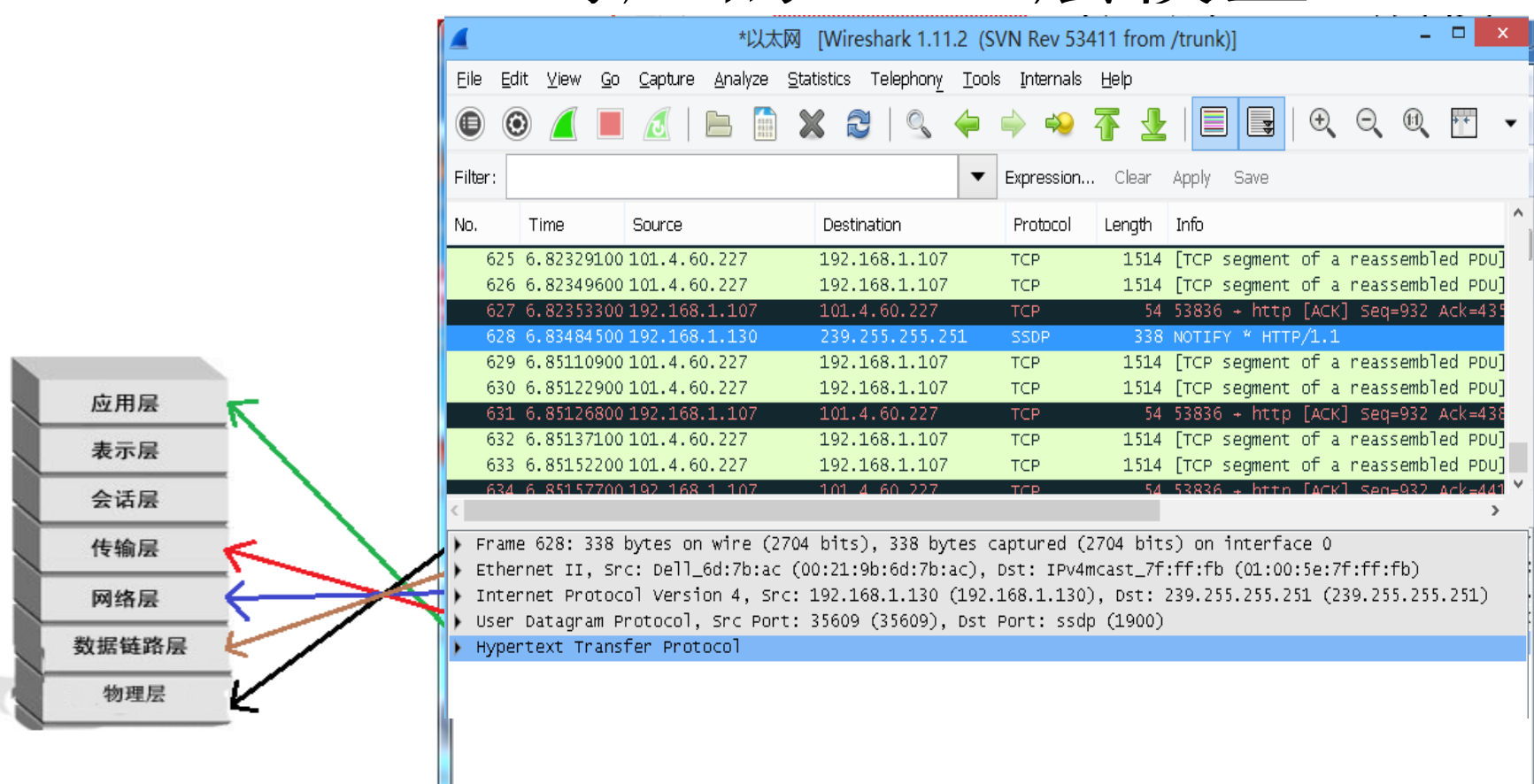
```
C:\windows\system32\ftp.exe
ftp> open 222.195.68.83
连接到 222.195.68.83。
220 Microsoft FTP Service
用户(222.195.68.83:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
密码:
230 User logged in.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
test.txt
第4章作业.pdf
第一次习题讲解<新>.ppt
第一章作业.pdf
第三章作业.ppt
226 Transfer complete.
ftp: 收到 84 字节, 用时 0.00秒 42.00千字节/秒。
ftp> lcd d:\ftp
目前的本地目录 D:\ftp。
ftp> bin
200 Type set to I.
ftp> get test.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
搜狗拼音输入法 半 :te.
```

# 利用Wireshark观察网络报文

## 3.TCP报文格式分析



# Wireshark 对应的OSI七层模型



Frame: 物理层的数据帧概况

Ethernet II: 数据链路层以太网帧头部信息

Internet Protocol Version 4: 互联网层IP包头部信息

Transmission Control Protocol: 传输层T的数据段头部信息，此处是TCP

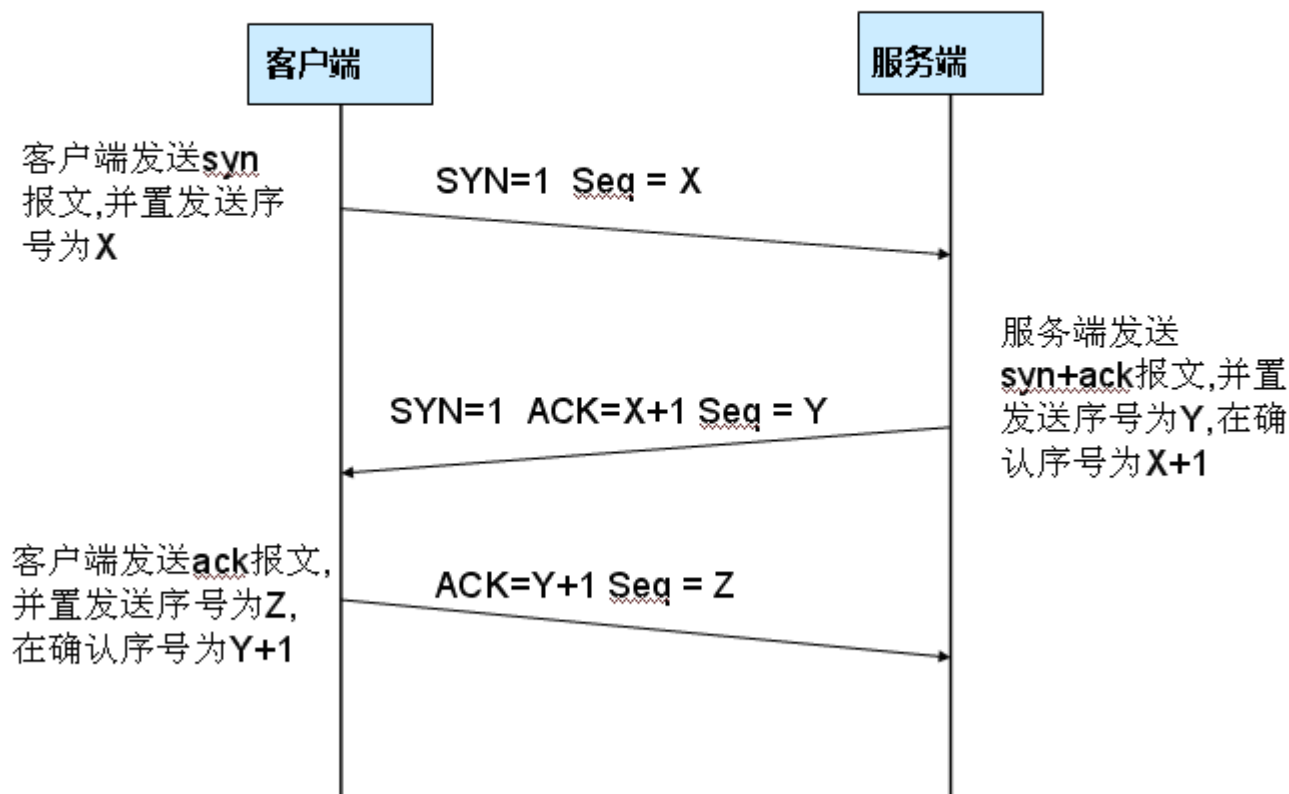
Hypertext Transfer Protocol: 应用层的信息，此处是HTTP协议



# 利用Wireshark观察网络报文

三次握手过程为

## TCP 三次握手



# 利用Wireshark观察网络报文

## 第一次握手

Atheros L1C PCI-E Ethernet Controller - Wireshark

文件(F) 编辑(E) 视图(V) 定位(G) 抓包(C) 分析(A) 统计(S) 电信(Y) 工具(T) 帮助(H)

过滤: `ip.src == 222.195.68.83||ip.dst==222.195.68.83` 表达式... 清除 应用

No.	Time	Source	Destination	Protocol	Info
150	19.370362	192.168.1.107	222.195.68.83	TCP	11583 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 SACK_PE
151	19.372462	222.195.68.83	192.168.1.107	TCP	ftp > 11583 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 W
152	19.372553	192.168.1.107	222.195.68.83	TCP	11583 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
153	19.388059	222.195.68.83	192.168.1.107	FTP	Response: 220 Microsoft FTP Service
154	19.440563	192.168.1.107	222.195.68.83	TCP	11583 > ftp [ACK] Seq=1 Ack=28 Win=8165 Len=0
180	22.682097	192.168.1.107	222.195.68.83	FTP	Request: USER xianliangshude
186	22.702173	222.195.68.83	192.168.1.107	FTP	Response: 331 Password required
199	22.745761	192.168.1.107	222.195.68.83	TCP	11583 > ftp [ACK] Seq=22 Ack=51 Win=8142 Len=0
242	27.778350	192.168.1.107	222.195.68.83	FTP	Request: PASS Nhpcc409
243	27.838475	222.195.68.83	192.168.1.107	TCP	ftp > 11583 [ACK] Seq=51 Ack=37 Win=65536 Len=0
244	27.923673	222.195.68.83	192.168.1.107	FTP	Response: 230 User logged in.
245	27.974237	192.168.1.107	222.195.68.83	TCP	11583 > ftp [ACK] Seq=37 Ack=72 Win=8121 Len=0

Frame 150: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: 5c:f9:dd:40:64:2c (5c:f9:dd:40:64:2c), Dst: Tp-LinkT\_b4:5f:da (00:19:e0:b4:5f:da)

Internet Protocol, Src: 192.168.1.107 (192.168.1.107), Dst: 222.195.68.83 (222.195.68.83)

Transmission Control Protocol, Src Port: 11583 (11583), Dst Port: ftp (21), Seq: 0, Len: 0

源 端口号:11583(11583)  
目的端口号:ftp(21)  
[Stream index: 33]  
Sequence number: 0 (relative sequence number)  
Header length: 32 bytes  
Flags: 0x02 (SYN)  
Window size: 8192  
Checksum: 0xe550 [validation disabled]  
Options: (12 bytes)  
Maximum segment size: 1460 bytes  
NOP  
Window scale: 0 (multiply by 1)

## 第二次握手

- ⊕ Frame 151: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
- ⊕ Ethernet II, Src: Tp-LinkT\_b4:5f:da (00:19:e0:b4:5f:da), Dst: 5c:f9:dd:40:64:2c (5c:f9:dd:40:64:2c)
- ⊕ Internet Protocol, Src: 222.195.68.83 (222.195.68.83), Dst: 192.168.1.107 (192.168.1.107)
- ⊖ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 11583 (11583), Seq: 0, Ack: 1, Len: 0
  - 源 端口号:ftp(21)
  - 目的端口号:11583(11583)
  - [Stream index: 33]
  - Sequence number: 0 (relative sequence number)
  - Acknowledgement number: 1 (relative ack number)
  - Header length: 32 bytes
  - ⊕ Flags: 0x12 (SYN, ACK)
  - Window size: 8192
  - ⊕ Checksum: 0x0c25 [validation disabled]
  - ⊖ Options: (12 bytes)

## 第三次握手

- ⊕ Frame 152: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
- ⊕ Ethernet II, Src: 5c:f9:dd:40:64:2c (5c:f9:dd:40:64:2c), Dst: Tp-LinkT\_b4:5f:da (00:19:e0:b4:5f:da)
- ⊕ Internet Protocol, Src: 192.168.1.107 (192.168.1.107), Dst: 222.195.68.83 (222.195.68.83)
- ⊖ Transmission Control Protocol, Src Port: 11583 (11583), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0
  - 源 端口号:11583(11583)
  - 目的端口号:ftp(21)
  - [Stream index: 33]
  - Sequence number: 1 (relative sequence number)
  - Acknowledgement number: 1 (relative ack number)
  - Header length: 20 bytes
  - ⊕ Flags: 0x10 (ACK)
  - Window size: 8192
  - ⊕ Checksum: 0xe544 [validation disabled]
  - ⊕ [SEQ/ACK analysis]

936	42.551342	222.195.68.83	192.168.1.107	UDP	Source port: 42551	Destination port: 54061
938	42.780780	192.168.1.107	222.195.68.83	FTP	Request: USER anonymous	
939	42.781614	222.195.68.83	192.168.1.107	FTP	Response: 331 Anonymous access allowed, send identi	
941	42.828604	192.168.1.107	222.195.68.83	TCP	192.168.1.107 → 222.195.68.83 [ACK] Seq=17 Ack=100 Win=8093 Len=0	
946	43.621275	192.168.1.107	222.195.68.83	FTP	Request: PASS 1	
947	43.622280	222.195.68.83	192.168.1.107	FTP	Response: 230 User logged in.	

- 可以看到FTP协议其用户名和密码以及传输的数据都是明文传输。

502 35.145617 222.195.68.83 192.168.1.107 FTP Response: 230 User logged in.

C:\windows\system32\ftp.exe

```

2013/11/25 16:00 <DIR>
0 个文件
3 个目录 53,069,197,312
ftp> bin
200 Type set to I.
ftp> get test.txt
200 PORT command successful.
125 Data connection already open; Tran
226 Transfer complete.
ftp: 收到 13 字节, 用时 0.04秒 0.30千字节
ftp> open 222.195.68.83
已经连接到了 222.195.68.83, 请首先使用
ftp> ls
远程主机关闭连接。
ftp> open 222.195.68.83
用户(222.195.68.83:(none)): anonymous
密码:
ftp> ls
test.txt
第4章作业.pdf
第一次习题讲解<新>.ppt
第一章作业.pdf
第三章作业.ppt
ftp>
搜狗拼音输入法 半:

```

点睛文本编码查询 (http://llf.126.com)

**Text:** test.txt 第4章作业

**ASCII:** 746573742E74787420203F343F3F3F

**Default:** 746573742E7478742020B5DA34D5C2D7F7D2B5

**Unicode:** 74006500730074002E00740078007400200020002C7B3400E07A5C4F1A4E

**BigEndUni:** 0074006500730074002E007400780074002000207B2C00347AE04F5C4E1A

**UTF-8:** 746573742E7478742020E7ACAC34E7ABA0E4BD9CE4B89A

**UTF-7:** 746573742E74787420202B6579772D342B65754250584534612D

**GBK:** 746573742E7478742020B5DA34D5C2D7F7D2B5

**BIG5:** 746573742E7478742020B2C434B3B9A7403F

```

0000 5c f9 dd 40 64 2c 00 19 e0 b4 5f da 08 00 45 00 \..@d.. .._...E.
0010 00 79 3d 58 40 00 7f 06 d8 fc de c3 44 53 c0 a8 .y=X@... ..DS..
0020 01 6b 00 14 c3 0b 1b a1 86 06 20 bd d8 0d 50 18 .k.....P.
0030 01 00 fe b6 00 00 74 65 73 74 2e 74 78 74 0d 0a .....te st.txt..
0040 b5 da 34 d5 c2 d7 f7 d2 b5 2e 70 64 66 0d 0a b5 ..4.... .pdf...
0050 da d2 bb b4 ce cf b0 cc e2 bd b2 bd e2 28 d0 c2 ..... (.
0060 29 2e 70 70 74 0d 0a b5 da d2 bb d5 c2 d7 f7 d2 ).ppt...
0070 b5 2e 70 64 66 0d 0a b5 da c8 fd d5 c2 d7 f7 d2 ..pdf.....
0080 b5 2e 70 70 74 0d 0a .....ppt..

```

- 实验要求
- 1、捕获观察并分析以太帧结构。
- 2、观察并分析ARP协议的报文。
- 3、捕捉UDP报文并验证其校验和。
- 4\*、捕捉TCP报文的连接释放--四次握手（注意 TCP Segment Len、Windows size value、Checksum等）。
- 5\*、捕捉除TCP、UDP之外的4种IP层以上的网络协议（例如HTTP、ICMP、SSDP、QICQ等），并尝试分析。