

广州大学学生实验报告

开课学院及实验室：计算机科学与工程实验室 518

2019 年 11 月 13 日

学院	计算机科学与 教育软件学院	年级/专 业/班	软件 171	姓名	谢金宏	学号	1706300001
实验课 程名称	计算机网络实验					成绩	
实验项 目名称	使用网络协议分析器捕捉和分析协议数据包					指导 老师	唐琳

一、实验目的

- 1、熟悉一种网络协议分析器（Wireshark 或 Ethereal，后者为前者的前身）的使用。
- 2、验证各种协议数据包的格式。
- 3、学会捕捉并分析各种数据包。

二、实验环境

- 1、安装有 TCP/IP 协议的 Windows 计算机。
- 2、安装有 Wireshark 或 Ethereal 网络协议

三、实验内容

- 1、安装网络协议分析器。
- 2、捕捉数据包，验证数据帧、IP 数据报、TCP 数据段的报文格式。
- 3、捕捉并分析 ARP 报文。
- 4、捕捉 ping 过程中的 ICMP 报文，分析结果各参数的意义。
- 5、捕捉 tracert 过程中的 ICMP 报文，分析跟踪的路由器 IP 是哪个接口的。
- 6、捕捉并分析 TCP 三次握手建立连接的过程。
- 7、捕捉整个 FTP 工作过程的协议包。对协议包进行分析说明。
 - a. 地址解析 ARP 协议执行过程
 - b. FTP 控制连接建立过程
 - c. FTP 用户登录身份验证过程
 - d. FTP 数据连接建立过程
 - e. FTP 数据传输过程
 - f. FTP 连接释放过程（包括数据连接和控制连接）
- 8、捕捉及研究 WWW 应用的协议报文，回答以下问题：
 - a. 当访问某个网页时，从应用层到网络层，用到了哪些协议？
 - b. 对于用户请求的百度主页（www.baidu.com），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是 RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？
 - c. 两个存放在同一个服务器中的截然不同的 Web 页（例如，<http://www.gzhu.edu.cn/index.jsp>和

<http://www.gzhu.edu.cn/cn/research/index.jsp> 可以在同一个持久的连接上发送吗？

- d. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？
- e. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif 图像和两个远地.gif 图像，那么需要建立几次 TCP 连接和有几个 UDP 过程？

四、实验步骤、记录和结果

实验中 FTP 服务端的 IP 地址为 202.192.34.70，FTP 客户端的 IP 地址为 202.192.34.36。捕捉 FTP 工作过程的协议包：

1、地址解析 ARP 协议执行过程

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Elitegro_f5:ee:5d	Broadcast	ARP	42	Who has 202.192.34.36? Tell 202.192.34.70
2	0.000217	Elitegro_f3:ee:0c	Elitegro_f5:ee:5d	ARP	60	202.192.34.36 is at c0:3f:d5:f3:ee:0c

图中可见 202.192.34.70 正在询问 FTP 服务器的 202.192.34.36 的 MAC 地址。

2、FTP 控制连接建立过程

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	202.192.34.70	202.192.34.36	TCP	66	62263 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000231	202.192.34.36	202.192.34.70	TCP	66	21 → 62263 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.000269	202.192.34.70	202.192.34.36	TCP	54	62263 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.000709	202.192.34.36	202.192.34.70	FTP	197	Response: 220-FileZilla Server 0.9.60 beta

上图中可见 TCP 三次握手过程，以及控制连接建立过程。

3、FTP 用户登录身份验证过程

5	0.001709	202.192.34.70	202.192.34.36	FTP	64	Request: AUTH TLS
6	0.001944	202.192.34.36	202.192.34.70	FTP	99	Response: 502 Explicit TLS authentication not allowed
7	0.002113	202.192.34.70	202.192.34.36	FTP	64	Request: AUTH SSL
8	0.002441	202.192.34.36	202.192.34.70	FTP	99	Response: 502 Explicit TLS authentication not allowed
9	0.005700	202.192.34.70	202.192.34.36	FTP	65	Request: USER root
10	0.006024	202.192.34.36	202.192.34.70	FTP	86	Response: 331 Password required for root
11	0.006089	202.192.34.70	202.192.34.36	FTP	68	Request: PASS rootpwd
12	0.006607	202.192.34.36	202.192.34.70	FTP	69	Response: 230 Logged on
13	0.007462	202.192.34.70	202.192.34.36	FTP	59	Request: PWD
14	0.007686	202.192.34.36	202.192.34.70	FTP	85	Response: 257 "/" is current directory.

上图为 TCP 三次握手过程和 FTP 用户登录身份验证过程。

4、FTP 数据连接建立过程

No.	Time	Source	Destination	Protocol	Length	Info
65	19.059019	202.192.34.70	202.192.34.36	FTP	62	Request: TYPE I
66	19.059350	202.192.34.36	202.192.34.70	FTP	73	Response: 200 Type set to I
67	19.059440	202.192.34.70	202.192.34.36	FTP	60	Request: PASV
68	19.059924	202.192.34.36	202.192.34.70	FTP	104	Response: 227 Entering Passive Mode (202,192,34,36,247,52)
69	19.060140	202.192.34.70	202.192.34.36	FTP	90	Request: RETR FileZilla_Server-0_9_60_2.exe
70	19.060346	202.192.34.70	202.192.34.36	TCP	66	62268 → 63284 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
71	19.060726	202.192.34.36	202.192.34.70	TCP	66	63284 → 62268 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	19.060769	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
73	19.061309	202.192.34.36	202.192.34.70	FTP	154	Response: 150 Opening data channel for file download from server o...

上图为 FTP 进入二进制被动模式并建立数据连接的过程。

5、FTP 数据传输过程

No.	Time	Source	Destination	Protocol	Length	Info
70	19.060346	202.192.34.70	202.192.34.36	TCP	66	62268 → 63284 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PER...
71	19.060726	202.192.34.36	202.192.34.70	TCP	66	63284 → 62268 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=25...
72	19.060769	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
74	19.061550	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
75	19.061552	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
76	19.061598	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=2921 Win=4194304 Len=0
77	19.061795	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
78	19.062006	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)

.....

No.	Time	Source	Destination	Protocol	Length	Info
1695	19.087865	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1696	19.087866	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1697	19.087866	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1698	19.087867	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1699	19.087869	202.192.34.36	202.192.34.70	FTP-DATA	702	FTP Data: 648 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1700	19.087869	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1701	19.087870	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1702	19.087871	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1703	19.087872	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1704	19.087873	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1705	19.087874	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1706	19.087875	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1707	19.087875	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1708	19.087876	202.192.34.36	202.192.34.70	FTP-DATA	1366	FTP Data: 1312 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
1709	19.087877	202.192.34.36	202.192.34.70	TCP	60	63284 → 62268 [FIN, ACK] Seq=2241217 Ack=1 Win=65536 Len=0
1712	19.087965	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1713	19.088138	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [FIN, ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1714	19.088385	202.192.34.36	202.192.34.70	TCP	60	63284 → 62268 [ACK] Seq=2241218 Ack=2 Win=65536 Len=0

上图为从服务器上下载某个大文件时的 FTP 过程。

6、FTP 连接释放过程（包括数据连接和控制连接）

下图为数据连接释放过程：

1709	19.087877	202.192.34.36	202.192.34.70	TCP	60	63284 → 62268 [FIN, ACK] Seq=2241217 Ack=1 Win=65536 Len=0
1712	19.087965	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1713	19.088138	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [FIN, ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1714	19.088385	202.192.34.36	202.192.34.70	TCP	60	63284 → 62268 [ACK] Seq=2241218 Ack=2 Win=65536 Len=0

下图为控制连接释放过程：

1717	29.012583	202.192.34.70	202.192.34.36	TCP	54	62263 → 21 [FIN, ACK] Seq=97 Ack=678 Win=64768 Len=0
1718	29.012872	202.192.34.36	202.192.34.70	TCP	60	21 → 62263 [ACK] Seq=678 Ack=98 Win=65536 Len=0
1719	29.013087	202.192.34.36	202.192.34.70	TCP	60	21 → 62263 [FIN, ACK] Seq=678 Ack=98 Win=65536 Len=0
1720	29.013116	202.192.34.70	202.192.34.36	TCP	54	62263 → 21 [ACK] Seq=98 Ack=679 Win=64768 Len=0

五、实验分析

1、捕捉整个 FTP 工作过程的协议包，并分析 FTP 协议。

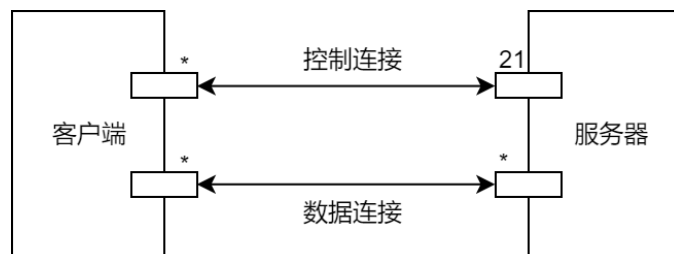


图 1 工作在被动模式下的 FTP

FTP 协议的工作过程大致可划分为地址解析 ARP 过程（不总是需要进行）、控制连接建立过程、控制指令传输过程、用户身份认证过程、数据链接建立过程、数

据传输过程和数据连接释放过程以及控制连接释放过程。逐过程分析如下（不考虑异常过程）：

a. 地址解析 ARP 协议执行过程

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Elitegro_f5:ee:5d	Broadcast	ARP	42	Who has 202.192.34.36? Tell 202.192.34.70
2	0.000217	Elitegro_f3:ee:0c	Elitegro_f5:ee:5d	ARP	60	202.192.34.36 is at c0:3f:d5:f3:ee:0c

图示为 FTP 客户端 202.192.34.36 使用 ARP 查询同一网段下的 FTP 服务器 202.192.34.36 的 MAC 地址。在捕获的第 1 分组中，ARP 查询报文被封装在 IP 数据包中，在同网段中进行广播。在捕获的第 2 分组中，服务器端 202.192.34.36 将自己的 MAC 地址以 IP 单播的方式告知客户端。这样，客户端获知了服务器端的 MAC 地址，（服务器端也可通过 ARP 获知客户端的地址，）两者可以通过 IP 数据报进行网络层通信了。

b. FTP 控制连接建立过程

FTP 控制连接建立在运输层协议 TCP 之上。要建立控制连接，首先要建立 TCP 连接。在完成 a 过程后，服务器和客户端已经能进行网络层通信里，接下来需要进行 TCP 三次握手，建立 TCP 连接。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	202.192.34.70	202.192.34.36	TCP	66	62263 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000231	202.192.34.36	202.192.34.70	TCP	66	21 → 62263 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 S
3	0.000269	202.192.34.70	202.192.34.36	TCP	54	62263 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0

图示为 TCP 三次握手过程。在捕获的第 1 分组中，客户端向服务器发送自己随机挑选的报文段序号 0，并置 SYN 比特，表示请求建立 TCP 连接。在第 2 分组中，服务器向客户端回应自己挑选的序号 0，并置 SYN 比特，将 ACK 设为 1，表示已经确认了客户端发送的序号为 0 的报文段。在第 3 分组中，客户端向服务器发送序号为 1 的报文段，置 ACK 为 1，表示确认收到服务器端序号为 0 的报文段。这时，TCP 连接已经建立了。

4	0.000709	202.192.34.36	202.192.34.70	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
---	----------	---------------	---------------	-----	-----	--

如图所示，TCP 连接建立后，服务器向客户端发送 FTP 报文，报告服务器使用的软件版本号。（这是欢迎消息。）FTP 连接建立。

c. FTP 用户登录身份验证过程

5	0.001709	202.192.34.70	202.192.34.36	FTP	64	Request: AUTH TLS
6	0.001944	202.192.34.36	202.192.34.70	FTP	99	Response: 502 Explicit TLS authentication not allowed
7	0.002113	202.192.34.70	202.192.34.36	FTP	64	Request: AUTH SSL
8	0.002441	202.192.34.36	202.192.34.70	FTP	99	Response: 502 Explicit TLS authentication not allowed
9	0.005700	202.192.34.70	202.192.34.36	FTP	65	Request: USER root
10	0.006024	202.192.34.36	202.192.34.70	FTP	86	Response: 331 Password required for root
11	0.006089	202.192.34.70	202.192.34.36	FTP	68	Request: PASS rootpwd
12	0.006607	202.192.34.36	202.192.34.70	FTP	69	Response: 230 Logged on

FTP 连接建立后，用户当前处于匿名身份，需要进行用户名和密码验证以切换身份。如图所示，客户端先后使用 Auth TLS 和 Auth SSL 指令请求服务器

加密 FTP 连接，但都被服务器拒绝。（实验时禁用了 TLS 和 SSL 设置，因为这样会使得网络协议分析器难以解密 FTP 报文。）于是客户端继续使用明文连接，先后使用 USER 和 PASS 指令，向服务器发送用户名和密码。服务器验证密码通过后接受了用户的登录请求。

d. FTP 数据连接建立过程

65	19.059019	202.192.34.70	202.192.34.36	FTP	62 Request: TYPE I
66	19.059350	202.192.34.36	202.192.34.70	FTP	73 Response: 200 Type set to I
67	19.059440	202.192.34.70	202.192.34.36	FTP	60 Request: PASV
68	19.059924	202.192.34.36	202.192.34.70	FTP	104 Response: 227 Entering Passive Mode (202,192,34,36,247,52)
69	19.060140	202.192.34.70	202.192.34.36	FTP	90 Request: RETR FileZilla_Server-0_9_60_2.exe
70	19.060346	202.192.34.70	202.192.34.36	TCP	66 62268 → 63284 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PER...
71	19.060726	202.192.34.36	202.192.34.70	TCP	66 63284 → 62268 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=25...
72	19.060769	202.192.34.70	202.192.34.36	TCP	54 62268 → 63284 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
73	19.061309	202.192.34.36	202.192.34.70	FTP	154 Response: 150 Opening data channel for file download from server o...

实验时，FTP 工作在被动模式。如图所示，客户端先使用 TypeI 指令，将数据连接设置为二进制传输模式，接着使用 PASV 指令，指示服务器进入被动状态。最后使用 RETR 指令，表示从服务器中下载某文件。PASV 响应报文中，服务器向客户端说明自己在 63284 端口（ $63284=247*256+52$ ）接收下一个 FTP 数据连接。于是客户端与服务器在服务器的 63284 端口进行 TCP 三次握手，TCP 连接建立，FTP 数据连接即相应地建立。

注意此时客户端并非与服务器端的 20 端口建立数据连接，而是进入 FTP 被动模式，与服务器端的动态端口进行连接。这里的被动是指服务器进入被动状态，等待客户端连接自己的动态端口，而不是通过 20 端口主动连接客户端的动态端口。

e. FTP 数据传输过程

No.	Time	Source	Destination	Protocol	Length	Info
154	19.064712	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
155	19.064713	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
156	19.064714	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
157	19.064715	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
158	19.064715	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
159	19.064716	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
160	19.064717	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
161	19.064718	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
162	19.064799	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=115341 Win=4194304 Len=0
163	19.065012	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
164	19.065013	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
165	19.065014	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
166	19.065015	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
167	19.065016	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
168	19.065017	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
169	19.065018	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
170	19.065019	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
171	19.065020	202.192.34.36	202.192.34.70	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR FileZilla_Server-0_9_60_2.exe)
172	19.065093	202.192.34.70	202.192.34.36	TCP	54	62268 → 63284 [ACK] Seq=1 Ack=128481 Win=4194304 Len=0

如图所示，FTP 数据传输过程中，FTP 数据连接中，低层次的 TCP 需要发送携带 ACK 字段的确认报文段，确认客户端已经正确地服务器端接收到了数据。

f. FTP 连接释放过程（包括数据连接和控制连接）

1709	19.087877	202.192.34.36	202.192.34.70	TCP	60 63284 → 62268 [FIN, ACK] Seq=2241217 Ack=1 Win=65536 Len=0
1710	19.087917				125 <Ignored>
1711	19.087944				54 <Ignored>
1712	19.087965	202.192.34.70	202.192.34.36	TCP	54 62268 → 63284 [ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1713	19.088138	202.192.34.70	202.192.34.36	TCP	54 62268 → 63284 [FIN, ACK] Seq=1 Ack=2241218 Win=4194304 Len=0
1714	19.088385	202.192.34.36	202.192.34.70	TCP	60 63284 → 62268 [ACK] Seq=2241218 Ack=2 Win=65536 Len=0

如图所示，在数据传输完毕后，数据连接进行关闭连接的四次挥手。服务器主动关闭连接，先是服务器发送 FIN，客户端确认；然后是客户端发送 FIN，服务器确认。

1717	29.012583	202.192.34.70	202.192.34.36	TCP	54 62263 → 21 [FIN, ACK] Seq=97 Ack=678 Win=64768 Len=0
1718	29.012872	202.192.34.36	202.192.34.70	TCP	60 21 → 62263 [ACK] Seq=678 Ack=98 Win=65536 Len=0
1719	29.013087	202.192.34.36	202.192.34.70	TCP	60 21 → 62263 [FIN, ACK] Seq=678 Ack=98 Win=65536 Len=0
1720	29.013116	202.192.34.70	202.192.34.36	TCP	54 62263 → 21 [ACK] Seq=98 Ack=679 Win=64768 Len=0

如图所示，客户端主动向服务器传送指示关闭 FTP 连接的 QUIT 指令后，控制连接的 TCP 进行关闭连接的四次挥手。客户端主动关闭连接，客户端向服务器发送 FIN，服务器确认；然后服务器向客户端 FIN，客户端确认。报文段顺序恰好与数据连接相反。

2、捕捉及研究 WWW 应用的协议报文，回答以下问题：

- a. 当访问某个网页时，从应用层到网络层，用到了哪些协议？

应用层：域名解析协议 DNS、超文本传输协议 HTTP/HTTPS。

运输层：用户数据报协议 UDP、传输控制协议 TCP。

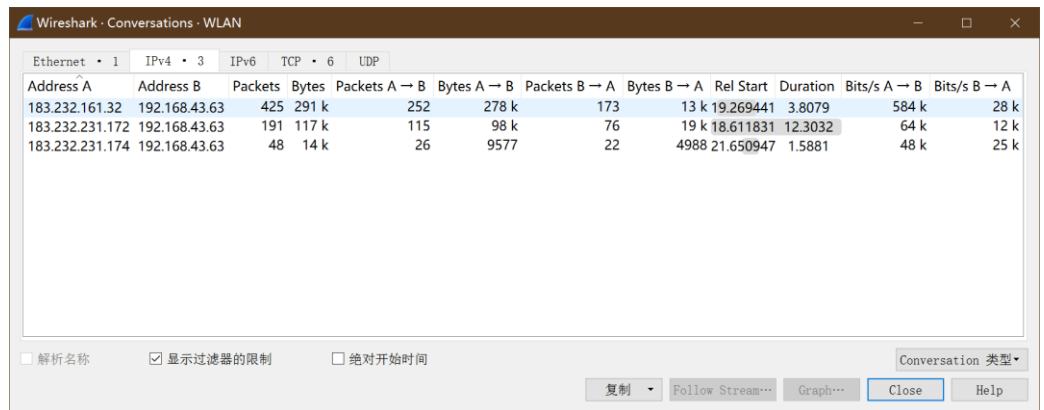
网络层：网际协议 IP、地址解析协议 ARP、网际控制报文协议 ICMP。

- b. 对于用户请求的百度主页（www.baidu.com），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是 RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？

如图是一次实验的实验数据记录：

Status	Method	Domain	File	Cause	Type	Transferred	Size	ms
200	GET	sp1.baidu.com	v.gif?logactid=1234567890&showTab=10000&opType=showpv&mod...	img	gif	289 B	0 B	157 ms
200	GET	ss1.bdstatic.com	soutu.css	stylesheet	css	2.59 KB	13.29...	19 ms
200	GET	www.baidu.com	sugrec?prod=pc_his&from=pc_web&json=1&sid=30085_1422_21127...	xhr	plain	776 B	658 B	34 ms
200	GET	ss1.bdstatic.com	mt_show.1.8.js	script	js	6.61 KB	17.98...	30 ms
200	GET	ss1.bdstatic.com	camera_new_5606e8f.png	img	png	1.01 KB	647 B	15 ms
200	GET	www.baidu.com	favicon.ico	img	x-icon	1.25 KB	16.56...	25 ms
200	GET	www.baidu.com	chromelib_1_1.js?_=1573730418218	xhr	js	7.32 KB	17.08...	32 ms
200	GET	ss0.bdstatic.com	min_notice_8a6de3fd.js	script	js	5.32 KB	15.34...	37 ms
200	GET	ss0.bdstatic.com	super_load_45128b95.js	script	js	13.95 KB	38.53...	33 ms
200	GET	ss0.bdstatic.com	min_tips_e4616384.js	script	js	2.07 KB	4.20 KB	33 ms
200	GET	ss0.bdstatic.com	activity_start_52498d2c.js	script	js	1.33 KB	1.76 KB	32 ms
200	GET	ss0.bdstatic.com	ubase_5a7b0933.js	script	js	15.36 KB	41.77...	23 ms
200	GET	ss0.bdstatic.com	nsguide_a8cbc2e7.css	stylesheet	css	1.22 KB	2.87 KB	16 ms
200	GET	ss0.bdstatic.com	super_ext_5031d813.css	stylesheet	css	3.17 KB	10.12...	16 ms
200	GET	www.baidu.com	tipspluslist?indexType=manht&req_seqid=0xf332a721000c25a&asyn...	xhr	html	384 B	73 B	41 ms
200	GET	ss0.bdstatic.com	mt_min_2247e202.css	stylesheet	css	2.51 KB	8.20 KB	11 ms
200	GET	sp3.baidu.com	ps_fp.html?pid=superman&fp=undefined&sim=undefined&wf=undefin...	img	html	410 B	114 B	132 ms
200	GET	ss0.bdstatic.com	ubase_9376fdcf.css	stylesheet	css	2.47 KB	7.79 KB	12 ms
200	GET	www.baidu.com	personalcontent?num=8&indexType=manht&req_seqid=0xf332a7210...	xhr	html	353 B	27 B	161 ms

36 requests 986 KB / 341.84 KB transferred Finish: 5.15 s DOMContentLoaded: 2.78 s load: 3.62 s



Wireshark - Conversations - WLAN

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
183.232.161.32	192.168.43.63	425	291 k	252	278 k	173	13 k	19.269441	3.8079	584 k	28 k
183.232.231.172	192.168.43.63	191	117 k	115	98 k	76	19 k	18.611831	12.3032	64 k	12 k
183.232.231.174	192.168.43.63	48	14 k	26	9577	22	4988	21.650947	1.5881	48 k	25 k

☐ 解析名称
 ☒ 显示过滤器的限制
 ☐ 绝对开始时间

Conversation 类型: 复制 Follow Stream... Graph... Close Help

在图示的一次实验中，客户端收到了来自 `www.baidu.com` (183.232.231.172)，`ss0.bdstatic.com` (183.232.161.32)，`ss1.bdstatic.com` (183.232.161.32)，`sp1.baidu.com` (183.232.231.174)，`sp3.baidu.com` (183.232.231.174) 的共计 664 个 TCP 报文段，共收到来自各个域名的 36 个 HTTP 报文。

报文段 RTT 与请求主页到浏览器上出先完整页面的时间，在理论上与传输报文段的数量有关，约等于 RTT 乘以传输报文的数量。

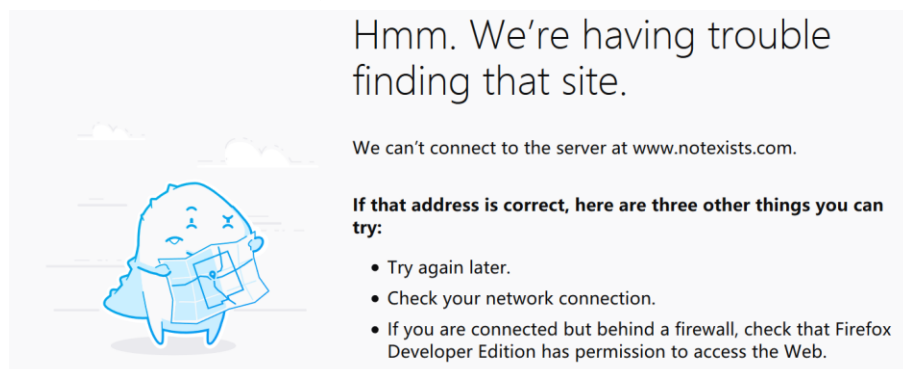
在图示的一次实验中，加载并显示完整页面的时间是 5.15 秒。

- c. 两个存放在同一个服务器中的截然不同的 Web 页（例如，`http://www.gzhu.edu.cn/index.jsp` 和 `http://www.gzhu.edu.cn/cn/research/index.jsp` 可以在同一个持久的连接上发送吗？

一般可以在同一个持久连接上发送，具体取决于 HTTP 服务器的设置。对于 HTTP/1.0 用户端可以使用“Connection: Keep-Alive”首部请求持久连接。对于 HTTP/1.1，持久连接是默认开启的。

- d. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？

浏览器报告“无法找到服务器”。



- e. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif 图像和两个远地.gif 图像，那么需要建立几次 TCP 连接和有几个 UDP 过程？

DNS 查询，取决于远地文档和图像的域名数量，可能产生 1~3 个 UDP 过程，与域名的数量相当。

本地连接不需要建立 TCP 连接或 UDP 连接。文本和两个图像，视乎于是否在同一个域名以及网页服务器的相关设定，可能在 1~3 个 TCP 连接中传输。

六、实验建议

请更新 2015 网络实验指导书中的 Ethereal 软件为 Wireshark。在 2006 年，Ethereal 因商标问题重命名为 Wireshark。名为 Ethereal 的软件不再维护，已经很难用于现代硬件。相比于 Ethereal，Wireshark 提供的功能更加丰富。