《计算机网络》实验指导

# 实验六: UDP 与 TCP 协议分析

# 一、实验目的

- 1、理解 UDP 和 TCP 协议的基本原理;
- 2、理解 UDP 和 TCP 报文格式和各字段含义;
- 3、理解 TCP 协议的通信过程和状态变迁机制。

#### 二、实验学时

2 学时

#### 三、实验类型

综合性

### 四、实验需求

1、硬件

每人配备计算机1台。

2、软件

Windows 7 以上操作系统,安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持,能够访问校园网。

4、工具

无。

## 五、实验理论

1、UDP协议基本原理及其报文结构;

2、TCP协议基本原理及其报文结构。

# 六、实验任务

- 1、完成 UDP 和 TCP 数据报文的采集;
- 2、完成 UDP 和 TCP 数据报文结构的分析;
- 3、完成 TCP 通信过程的报文分析。

## 七、实验内容及步骤

### 1、UDP 数据包分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件"<u>udp</u>",选择【Start】, 开始进行 报文采集, 如图 6-1 所示。

en: udp	ny Itols Internas Help	
WIRESHARK The World's Most Version 1.10.5 (SWN Rev Capture	Popular Network Protocol Analyzer 54262 from /trunk-1.10) Files	Online
Interface List     Use if the capture interfaces     (coder incoming packet)     Start     Cooce are or more interfaces to capture from, then Start     /: 130EUR	Open         Open a previously captured file           Open Recent:         Image: Capture Size on the web           And assochment of example capture files on the web         And assochment of example capture files on the web	Website       Valt Be project website       Image: Standard Constraints       Image: Standard Constraints </td
Capture Options     Sart s capture with dataled captors     Capture Help     Mow to Capture     Day by days in a socientif capture setue     Sector Information for capturing on:     Butter MUAN		

②在 Wireshark 的抓包窗体中,查看已获取的 UDP 数据报文,如图 6-2 所示。

Captaining nom 4-states (Vineshark 2.2.6 (V	zzzo-o-gszdacoa)j		
<u>File Edit View Go Capture Analyze St</u>	atistics Telephony <u>T</u> ools <u>I</u> nternals	Help	
• • <b>* * * * * * *</b>	2, 🗇 🌳 🖓 7 👱 🔲 🖬 🗌	ର୍ ପ୍ 🔍 🖾   🎬 🖾 🍢 🎉 📜	
Filter: udp	<ul> <li>Express</li> </ul>	ion Clear Apply Save	
lo Time Source	Destination Protors	ength Info	
10142 159, 105995 192, 168, 1, 103	234,123,12,1 UDP	266 20141 + 20141 Len=224	
10143 159, 122570 192, 168, 1, 108	101.24.54.88 UDP	1450 10101 - 12375 Len=1408	
10146 159.333485 101.24.54.88	192.168.1.108 UDP	72 12375 - 10101 Len=30	
10147 159.333834 192.168.1.108	101.24.54.88 UDP	1450 10101 → 12375 Len=1408	
10148 159. 333933 192. 168. 1. 108	101.24.54.88 UDP	1450 10101 → 12375 Len=1408	
10149 159.334019 192.168.1.108	101.24.54.88 UDP	1450 10101 → 12375 Len=1408	
10150 159.334159 192.168.1.108	101.24.54.88 UDP	72 10101 → 12375 Len=30	
10167 161.106224 192.168.1.103	234.123.12.1 UDP	266 20141 → 20141 Len=224	
10177 162.101227 192.168.1.108	140.207.62.150 UDP	121 4009 → 8000 Len=79	
10180 162.268259 140.207.62.150	192.168.1.108 UDP	89 8000 → 4009 Len=47	
10189 163.103498 192.168.1.103	234.123.12.1 UDP	266 20141 → 20141 Len=224	
10204 165.102328 192.168.1.103	234.123.12.1 UDP	266 20141 - 20141 Len=224	
10205 165.299155 192.168.1.1	192.168.1.255 UDP	157 1024 → 5001 Len=115	
10222 167.094140 192.168.1.103	234.123.12.1 UDP	266 20141 → 20141 Len=224	
<pre>internet Protocol Version 4, 57 User Datagram Protocol, Src Por NetBIOS Name Service 0000 1111111 11111111 11111111 0008 00000110 1110011 11111000 010 00000000 01100010 01110011 0018 01110011 1110111 0101100 0220 01100010 11111111 00000000</pre>	c: 1/2.17.101.2, Dst: 172.17 t: 137, Dst Port: 137 11111111 1111111 1111111 0 01000100 00001000 00000000 0 00010001 01000000 00000000 0001001 01000000 00000001 0 0001001 00000000 010001001 0	100.255 100000 0001101	
0030 00000000 00000000 00000000	00000000 00000000 00000000 00000000 0000	D100000 01000101 E	
) 💅 本地连接: <live capture="" in="" progress=""> File:</live>	Packets: 10775 · Displayed: 1730 (	16.1%)	Profile: Default
	<u>क</u>	1000 粉根根本	

(2) 数据报文分析

Г

从获取的 UDP 数据报文中任意选择其中一条数据报文,对该数据报文进行详细分析,并填 写表 6-1。

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第 位		
2	Destination Port		第 位		
3	Length		第 位		
4	Checksum		第 位		

表 6-1 UDP 协议报文分析

3

	抓取数据包的详细内容:
5	

# 2、TCP 数据包分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件"<u>tcp</u>",选择【Start】, 开始进行报文采 集, 如图 6-3 所示。

Edit View Go Capture Analyze S	itatistics Telephony	ools Jnternals Heb Cols Jnternals Heb Cols Cols Cols Cols Cols Cols Cols Cols		
● Capture Options ② Capture Options ③ Capture Interfaces (courts incoming packets) ③ Start ⑦ Attilize ③ Capture Options Start capture with detailed options	2.2.6 (v2.2.6 0.332d	acca)  Files  Popen a previously captured file Open Recent:  Sample Captures A rich assortment of example capture files on the wiki	€ V V © L T	Online Vebsite Bit the project's website Joser's Guide Deser's Guide He User's Guide (online version) Security York with Wreshark as securely as possible
How to Capture     Step by step to a successful capture setup     Network Media     Ready to load or capture	No Packets			Profile: Default

②在 Wireshark 的抓包窗体中,查看已获取的 TCP 数据报文,如图 6-4 所示。

	apture Analyze Statist	ics Telephony Tools	Internals Hel	p
		~ ~ <del>~</del> ~ ~ ~ ~ []		
Filter: tcp			Expression	Clear Apply Save
o. Time S	ource	Destination	Protocol I	ength Info
233 0.014133 1	.52.100.1.1	152.100.1.100	11115	234 mile/1.1 302 moved remportering
294 6.814291 1	.92.168.1.1	192.168.1.108	TCP	66 80 - 32525 [FIN, ACK] Seq=169 Ack=257 Win=16384 Len=0 TSval=32689415 T
295 6.814349 1	.92.168.1.108	192.168.1.1	TCP	66 32525 - 80 [ACK] Seq=257 ACK=170 Win=66440 Len=0 TSVa1=22675245 TSecr=
296 6.814457 1	.92.168.1.108	192.168.1.1	TCP	66 32525 - 80 [FIN, ACK] Seq=257 Ack=170 Win=66440 Len=0 TSval=22675245 T
297 6.814572 1	.92.168.1.1	192.168.1.108	TCP	66 80 + 32525 [ACK] Seq=170 Ack=258 Win=16383 Len=0 TSval=32689415 TSecr-
298 6.8382/2 1	.92.168.1.108	101.226.161.154	TCP	74 32526 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 TSVal=
301 6.888811 1	.01.226.161.154	192.168.1.108	TCP	66 80 - 32526 [SYN, ACK] SEQ=0 ACK=1 W1n=14600 Len=0 MSS=1452 SACK_PERM=
302 6.888929 1	.92.168.1.108	101.226.161.154	TCP	54 32526 - 80 [ACK] Seg=1 ACK=1 W1n=66792 Len=0
303 6.889109 1	.92.168.1.108	101.226.161.154	HTTP	517 POST /wcheckquery HTTP/1.1 (application/x-www-form-urlencoded)
307 6.939599 1	.01.226.161.154	192.168.1.108	TCP	60 80 + 32526 [ACK] Seq=1 Ack=464 Win=15744 Len=0
308 6.941421 1	.01.226.161.154	192.168.1.108	HTTP	362 HTTP/1.1 200 OK (application/octet-stream)
309 6.941421 1	.01.226.161.154	192.168.1.108	TCP	60 80 → 32526 [FIN, ACK] seq=309 Ack=464 Win=15744 Len=0
310 6.941529 1	.92.168.1.108	101.226.161.154	TCP	54 32526 → 80 [ACK] seq=464 Ack=310 Win=66484 Len=0
311 6.941623 1	.92.168.1.108	101.226.161.154	TCP	54 32526 - 80 [FIN, ACK] Seq=464 Ack=310 Win=66484 Len=0
Internet Protoco	l version 4, Src: trol Protocol, Src	192.168.1.108, Ds Port: 32518, Dst	t: 192.168. Port: 80,	11 Seq: 0, Len: 0
Transmission Con				
Transmission Con				
Transmission Con				
000 00110000 111:	1100 01101000 111	10100 01110101 10	101001 0010	20000 00011010 0.h.u
000 00110000 1111 008 0000110 1110	1100 01101000 111 00101 11111000 010	10100 01110101 10 00100 00001000 00	101001 0010 000000 0100	00000 00011010 0.h.u 00101 00000000D.E.
Transmission Con 000 00110000 111: 008 0000010 111 010 0000000 001:	1100 01101000 111 0101 11111000 010 1100 01110011 100	10100 01110101 10: 00100 00001000 00 01001 01000000 00	101001 0010 000000 0100 000000 0100	00000 00011010 0.h.u 00101 0000000
000 00110000 111: 008 0000110 111: 008 0000010 111: 010 0000000 0001 010 0000000 0001	1100 01101000 111 00101 11111000 010 11100 0110011 100 00000 11000000 101	10100 01110101 10: 00100 00001000 00 01001 01000000 00 01000 00000001 01:	101001 0010 000000 0100 000000 0100 101100 1100	00000 00011010 0.h.u 00101 00000000D.E. 00000 00000110
Transmission Con           0000         001100000         1111           008         0000010         1111           010         00000000         0011           013         00000000         0001           014         0000000         0001           015         0000000         0001           020         00000001         0000           028         10100001         1111	11100 01101000 111 00101 11111000 010 (1100 01110011 100 0000 0100000 101 0000 01000000 0000	10100 01110101 10 00100 00001000 00 01001 01000000 00 01000 00000001 01 00110 00000000	101001 0010 000000 0100 000000 0100 101100 1100 010000 0010	00000 00011010 0.h.u 00101 0000000 D.E. 00000 0000101 S.8.8. 0000 10101101
Transmission Con           000         00110000         111           008         00000110         111           010         0000000         001           010         0000000         001           020         0000000         001           020         0000001         101           020         0000001         101           023         0010000         000	11100 01101000 111 0101 11111000 010 1100 01110011 100 0000 11000000 101 0000 0000000 000 00000 00000001 111	10100 01110101 10 00100 00001000 00 01001 01000000 00 01000 0000000 01 00110 0000000 00 0110 0000000 00 0110 0000000 00	101001 0010 000000 0100 101100 1100 010000 0010 000000 1010 000000 0000	00000 00011010 0.h.u 00101 00000000b.E. 00000 10010000 1. 00000 10000010
Transmission Con           0000         00110000         111           008         00000110         111           018         0000000         001           108         0000000         000           000         0001000         000           00000001         000         000           000         0010000         000           00100000         001         111	1100 01101000 111 10101 11111000 010 11100 0111001 100 0000 1100000 101 0000 0000000 000 0000 0000000 100 0000 0000001 000	10100 01110101 10 00100 00001000 00 01001 01000000 00 01000 0000000 01 00100 0000000 00 00000 0000000 00 01100 00000000	101001 0010 000000 0100 101100 1100 000000 0010 000000 1010 000000 0000 000000 0000	00000 00011010 0.h.u 00101 0000000 b. E. 00000 0000110 s. e. 00000 1001110 P 00000 100000100 00010 00000100
000 00110000 111: 008 0000110 111 00 000000 001 010 0000000 000 020 000000 000 020 00000000	1100 01101000 111 1000 111000 010 1100 011011 100 10000 11000000 100 10000 01000000 000 10000 0000000 100 1000 00000001 000 1000 0000000000	10100 01110101 10 00100 00001000 00 01001 01000000 00 0000 00000000	101001 0010 000000 0100 101100 1100 000000 0101 000000 0010 000000 0000 000010 0000 ved: 23492 (75	00000 00011010 0. h.u 00101 0000000 D. E. 00000 1001000 1. 00000 1001000 1. 00000 10000010
Transmission Con           000         00110000         111           000         0000010         111           010         0000000         001           020         0000000         001           020         0000000         001           020         0000000         101           030         0010000         000           020         0010000         101           020         0010000         101           020         File: "C:\Users\LX	11100 01101000 111 00101 11111000 010 11100 0110011 100 0000 0100000 010 0000 01000000 000 0000 010000011 111 0000000000	10100 01110101 10 00100 00001000 00 01001 01000000 01 01000 00000001 01 00000 00000000	101001 0010 000000 0100 01000 0100 010000 0101 000000 0000 000000 0000 000010 0000 yed: 23492 (75	00000 00011010 0.h.u 0101 00000005.8. 00000 01010100
Transmission Con           000         00110000         111           008         0000110         111           010         0000000         001           020         0000000         000           020         0000000         000           038         000000         001           038         0000000         101           038         0000000         101           036         File: "C:(Users'LUX)	1100 01101000 111 00101 11111000 010 1100 0111000 0000 10100000 100 10000 00000000 000 00000 00000001 011 10100 00000001 000 \$ppData\Loca\Temp\	10100 01110101 10: 00100 00001000 000 01000 0000000 001 00110 00000000	101001 0010 000000 0100 101100 1100 000000 0010 000000 0010 000000 0000 000010 0000 yed: 23492 (75	00000         00011010         0. h. u           00101         00000100         b. E.           00000         1001000         1.           00000         1011010         P.           00000         0000010         1.           00000         0000010         P.           00000         0000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           00100         00000010         1.           <

(2) 数据报文分析

从获取的 TCP 数据报文中任意选择其中一条数据报文,对该数据报文进行详细分析,并填 写表 6-2。

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第 位		
2	Destination Port		第 位		
3	Sequence Number		第 位		
4	Acknowledgement Number		第 位		
5	Header Length		第 位		
6	Reserved		第 位		
7	Flags		第 位		
8	Window Size		第 位		
9	Checksum		第 位		
10	Urgent Pointer		第 位		
	抓取数据包的详细内	容:			
11					

表 6-2 TCP 协议报文分析

## 3、TCP 通信过程数据包分析

(1) TCP 建立连接报文分析

①获取建立连接报文。

a、打开 Wireshark, 在【Filter】选项中输入报文过滤条件 "<u>tcp and ip.addr==192.168.1.103(本</u> <u>地主机 IP 地址</u>), 选择【Start】, 开始进行报文采集;

b、通过浏览器访问学校官网(http://www.hactcm.edu.cn),网站访问后,点击左上角红色按钮停止报文采集,如图 6-5 所示。

0	A 1			- <u>-</u>	GN   (			<b>7</b> 1			0.0	P7 (	58 F	a 💼	201	978						
•		<b>198</b> (\$55)			19		~ ~	T A		* 4	44				an	<u>es</u>						
Filter	tcp and	d ip.add	r==192	.168.1.1	.03				▼ Exp	pression.	Clear	Apply	Save	,								
No.	Time	-	Coure		_	Des	tination		Pre	stocol	Longt		nfo	_				-				_
	36 8.0	92886	192.	168.1	103	211	69. 32	2.50	TC	P		74 0	51881	→ 80	[SYN]	Seq=	0 Wir	n=8192	Len=0	) MSS=1	460 \	ws=4 s
	37 8.0	93201	211.	69.32.	. 50	192	.168.1	.103	TC	P		74 8	30 ÷ 1	61879	[SYN	ACK]	Seq=	0 Ack	=1 Wir	1=14480	Len	=0 MSS
	39 8.0	93448	192.	168.1.	.103	211	. 69. 32	. 50	тс	P		66 6	51879	→ 80	[ACK	Seq	1 Ack	=1 Wi	n=1669	52 Len=	0 TS	val=49
	40 8.0	33868	211.	69.32.	50	192	.168.1	103	тс	P		74 8	50 - 1	51880	LSYN	ACK	Seq-	O ACK	-1 WIT	1=14480	Len	=0 MSS
	41 8.0	33809	107	169.32.	107	192	. 108.1	. 103	TO	P		74 8	50 - 1	01881	LSYN,	ALK.	Seq=	O ACK	-1 WIT	1=14480	Len	=0 MSS
	42 0.0	1166	192.	168 1	103	211	69.32	50	TC	P		66 6	51880	- 80	EACK	Seq	1 Ack	-1 Wi	n=1665	7 1 00-	0 TE	val_49
	44 8.0	4272	192	168.1	103	211	69.32	50	TC	P		66.6	51881	+ 80	FACK	Seg		=1 wi	n=6666	18 Len=	0 15	val=49
	45 8.0	94608	192.	168.1	.103	211	. 69. 32	. 50	тс	P		74 6	51884	+ 80	[SYN	Seg-	0 wir	=8192	Len=0	) MSS=1	460 1	WS=4 S
	46 8.0	97451	211.	69.32	. 50	192	.168.1	.103	тс	P		74 8	30 -	61882	[SYN.	ACK	Seq=	O Ack	=1 Wir	=14480	Len	=0 MSS
	47 8.0	97685	192.	168.1	.103	211	. 69. 32	. 50	тс	P		66 6	51882	+ 80	[ACK	Seq=	1 Ack	=1 wi	n=1665	2 Len=	0 TS	va1=49
	48 8.1	00103	211.	69.32	. 50	192	2.168.1	.103	тс	P		74 8	80 - 1	61883	[SYN	ACK]	Seq=	O Ack	=1 Wir	1=14480	Len	=0 MSS
	49 8.1	00105	211.	69.32	. 50	192	2.168.1	.103	TC	P		74 8	80 + 1	61884	[SYN,	ACK]	Seq=	O Ack	=1 Wir	1=14480	Len	=0 MSS
	50 8.1	00453	192.	168.1	.103	211	. 69. 32	. 50	TC	P		66 6	51883	+ 80	[ACK]	Seq=	1 Ack	:=1 wi	n=6660	08 Len=	0 TS	val=49
	51 8.1	00592	192.	168.1.	.103	211	. 69. 32	. 50	TC	P		66 6	51884	+ 80	[ACK]	Seq-	1 Ack	(=1 Wi	n=6660	08 Len=	O TSI	va1=49
4			100		103		CO 35		~~				-+ 005		- Fanad		A					
⊕ Et ⊕ Ir ⊕ Tr	ame 36 hernet iternet ansmis	II, S Proto	ontrol	teonT ersion Prot	e_0592 e_95:4 4, sr ocol,	d:ca (i c: 192. Src Por	28:e3:4 168.1. T: 618	103, 0 881, D	4d:ca), Dst: 21 St Port	DST: 1.69.3 : 80,	Tp-Lin 2.50 Seq: 0	kT_2c	: 0	4 (bc	:46:9	):2c::	80:44)	)				
0000	10111	100 0	100011	0 100	11001	0010110	0 0011	0000	0100010	0 0010	1000 1	10001	11	F.,00	D(.							
0008	01000	0000 0	0111110	0 011	00011	0110101	0 0000	00000	0000000	0 0100	0101 0	000000	10		. E.							
0018	00100	0001 1	100110	0 110	00000	1010100	00 0000	00001	0110011	1 1101	0011 0	100010	01		g.E							
10000	00100	0000 0	011001	.0 111	10001	1011100	0000	00000	0101000	0 1011	1100 0	111011	LO	2	P.V							
0020		Ucorchi	IVI AppD	ata\l or	al Temp	Pac	kets: 133	· Disnla	ved: 109	(82.6%)	· Dropp	o) 0 the	0%) .	Ignored	d: 3 (2	(%)			Pr	ofile: Def	ault	
0020	File: "C						and the second sec					and a set of the set o		A	and the second second					manual Model		

②建立连接报文分析。

对抓取到的 TCP 报文进行分析,找到建立连接的三次握手机制所对应的报文,进行详细内容分析,并根据数据报文内容填写表 6-3。

皮旦	今四夕夜	第一次	第二次	第三次	字四事示的信息
5	于权石林	字段值	字段值	字段值	于权农小时旧志
1	Source Port				
2	Destination Port				
3	Sequence Number				
4	Acknowledgement Number				
5	Header Length				
6	Reserved				
7	Flags				
8	Window Size				
9	Checksum				
10	Urgent Pointer				
	抓取数据包的详细内	容:			
11					

表 6-3 TCP 建立连接报文分析

(2) TCP 释放连接报文分析

①获取释放连接报文。关闭浏览器后,由于长时间未进行连接,将进行释放该 TCP 连接操作,可通过 Wireshark 网络分析工具,获取释放 TCP 连接的数据报文如图 6-6 所示。

File	Edit View Go	Capture Analyze	Statistics Telephony Tools	ls Internals Help								
0	⊙ <b>∡ ≡</b> <u>∅</u>	E 🗋 🗶 🛃	् 🗢 🕸 🖓 🐺 👱		0, 🖭   👪	¥ 🐔	%   <b>(</b>	2				
Filter	r: tcp and ip.add	dr==192.168.1.103		Expression Cle	ear Apply Sav	re						
No.	Time	Source	Destination	Protocol Len	ath Info							1
	23 4.387534	211, 69, 32, 50	172.17.101.2	TCP	66 80 -	37609	FIN.	ACK1 S	eg=1 A	ck=1 Win-	114 Le	en=0 TSva
	24 4.387691	172.17.101.2	211.69.32.50	TCP	66 37609	9 → 80	[ACK]	Seg=1	Ack=2	Win=16652	Len=0	) TSval=2
	25 4.587559	211.69.32.50	172.17.101.2	TCP	66 80 →	37606	[FIN,	ACK] S	eq=1 A	ck=1 win=	114 Le	en=0 TSva
	26 4.587709	172.17.101.2	211.69.32.50	TCP	66 37606	5 - 80	[ACK]	Seg=1	Ack=2	win=16652	Len=0	TSval=2
	28 4.980006	211.69.32.50	1/2.1/.101.2	TCP	66 80 -	37608	LFIN,	ACK S	eq=1 A	kck=1 Win=	114 Le	en=0 TSva
	29 4.980213	172.17.101.2	211.69.32.50	TCP	66 37608	8 - 80	[ACK]	Seq=1	Ack=2	win=16652	2 Len=0	) TSval=2
	20 4 000222	211, 69, 32, 50	172.17.101.2	TCP	66 80 →	37605	[FIN,	ACK] S	eq=1 A	kck=1 Win=	114 Le	en=0 TSva
	50 4.900525											
	31 4.988491	172.17.101.2	211.69.32.50	TCP	66 37605	5 - 80	[ACK]	Seq=1	Ack=2	Win=16652	2 Len=0	) TSval=2
< ⊞ Fr ⊞ Et ⊠ Tn	ame 23: 66 k	172.17.101.2 bytes on wire (5 frc: Digitalc_1a brcol Version 4	211.69.32.50 "" 28 bits), 66 bytes ca :76:22 (00:03:0f:1a:7 Spc: 211 69 32 50 ps	TCP aptured (528 bits 76:22), Dst: Comp st: 172 17 101 2	66 3760 ) on interfa alIn_e5:f8:4	5 → 80 ace 0 44 (20:	[ACK] 1a:06	Seq=1 .	Ack=2 44)	Win=16652	2 Len=C	) TSVal=2
<ul> <li>✓</li> <li>✓</li> <li>✓</li> <li>Fr</li> <li>✓</li> <li>Tr</li> </ul>	ame 23: 66 k thernet II, s ternet Proto	172.17.101.2 bytes on wire (5 src: Digitalc_1a scol Version 4, control Protocol	211.69.32.50 m 28 bits), 66 bytes ca :76:22 (00:03:0f:1a:7 Src: 211.69.32.50, Ds , Src Port: 80, Dst F	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq:	66 3760 ) on interfa alIn_e5:f8:4 1, Ack: 1,	5 - 80 ace 0 44 (20: Len: (	[ACK] 1a:06	Seq=1 .	Ack=2 44)	win=16652	2 Len=0	) TSVal=2
< ♥ Fr ♥ Et ♥ In ♥ Tr	ame 23: 66 b chernet II, s ternet Proto	172.17.101.2 pytes on wire (5 src: Digitalc_la ocol Version 4, control Protocol	211.69.32.50 m 28 bits), 66 bytes ca 76:22 (00:03:0f:1a:7 Src: 211.69.32.50, 05 , Src Port: 80, Dst F	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq:	66 3760 ) on interfa alIn_e5:f8:4 1, Ack: 1,	5 → 80 ace 0 44 (20: Len: (	[ACK] 1a:06	seq=1 /	Ack=2 44)	win=16652	2 Len=0	) TSVal=2
< ♥ Fr ♥ Et ♥ In ♥ Tr	ame 23: 66 b chernet II, s nternet Proto	172.17.101.2 pytes on wire (5 src: Digitalc_la ocol Version 4, control Protocol	211.69.32.50 "" 28 bits), 66 bytes ca :76:22 (00:03:0f:1a:7) Src: 211.69.32.50, DS , Src Port: 80, DSt F	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq:	66 37609 ) on interfa alIn_e5:f8:4 1, Ack: 1,	5 → 80 ace 0 44 (20: Len: (	[ACK] 1a:06	seq=1 /	Ack=2	win=16652	2 Len=0	) TSval=2
< ⊞ Fr ⊞ Et ∎ In ⊕ Tr	ane 23: 66 b chernet II, 5 cansmission (	172.17.101.2 systes on wire (5 src: Digitalc_la scol Version 4, control Protocol	211.69.32.50 m 28 bits), 66 bytes cc :76:22 (00:03:0f:1a: 5rc: 211.69.32.50, 05 , Src Port: 80, Dst F	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq:	66 3760: ) on interfi alIn_e5:f8:4 1, Ack: 1,	5 → 80 ace 0 44 (20: Len: (	[ACK]	seq=1 ;	44)	win=16652	2 Len=0	) TSval=2
<	ame 23: 66 b thernet II, 2 ternet Proto ansmission C	172.17.101.2 pytes on wire (5 src: Digitalc_la scol Version 4, control Protocol 00011010 0000011	211.69.32.50 m 28 bits), 66 bytes cc :76:22 (00:03:0f:1a: :76:22 (00:32:06) 00 , Src Port: 80, Dst F 0 11100101 11111000 0	TCP aptured (528 bits 76:22), pst: Comp st: 172.17.101.2 Port: 37609, Seq:	66 3760: ) on interf; alIn_e5:f8:4 1, Ack: 1, 00000011	ace 0 44 (20: Len: (	[ACK] 1a:06	seg=1 ,	44)	win=16652	2 Len=0	) TSva]=2
<ul> <li>✓ Fr</li> <li>♥ Et</li> <li>♥ In</li> <li>♥ Tr</li> </ul>	314.988491 ame 23: 66 b thernet II, s hternet Proto ansmission ( 0 00100000 0 0 00100000 0 0 0010111 (	172.17.101.2 hytes on wire (5 src: DigitalCla col Version 4, control Protocol 00011010 00000011 00011010 0010011	211.69.32.50 "" 28 bits), 66 bytes cz :76:22 (00:03:0f:1a:7 5rc: 211.69.32.50, bs , Src Port: 80, Dst F 0 11100101 11111000 C 0 00100101 00001000 C	TCP aptured (528 bits 76:22), pst: Comp st: 172.17.101.2 port: 37609, Seq: 01000100 00000000	66 3760: ) on interfa alIn_e5:f8:4 1, Ack: 1, 000000011 00000000	ace 0 44 (20: Len: C	[ACK] 1a:06	:e5:f8:	44)	win=16652	2 Len=0	) TSva]=2
<ul> <li>✓ </li> <li></li></ul>	314.988491 ame 23: 66 b thernet II, s thernet Proto ansmission ( 0 001000000 ( 0 00000111 ( 0 00000000 ( 0 0000000 ( 0 0000000 ( 0 0000000 ( 0 000000 ( 0 0000000 ( 0 000000 ( 0 0000000 ( 0 000000 ( 0 00000 ( 0 000000 ( 0 000000 ( 0 0000000 ( 0 00000 ( 0 000000 ( 0 000000 ( 0 00000 ( 0 0000 ( 0 0000 ( 0 000000 ( 0 0000 ( 0 000000 ( 0 0000 ( 0 00000 ( 0 0000 ( 0 0000 ( 0 0000 ( 0 0000 ( 0 0	172.17.101.2 pytes on wire (5 src: Digitalc_la col version 4, control Protocol 00011010 00000111 00011010 0111011 00011010 0111011	211.69.32.50 m 28 bits), 66 bytes cc 76:22 (00:03:0f:1a: 5rc: 211.69.32.50, 05 , Src Port: 80, Dst F 0 11100101 11111000 C 0 0010000 010000 C 0 00100000 0100000 C	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq: 01000100 00000000 00000000 010011010	66 3760: ) on interfa alrn_e5:f8:4 1, Ack: 1, 000000011 000000010 00000000	ace 0 44 (20: Len: (	[ACK] 1a:06	:e5:f8:	44)	win=16652	2 Len=0	) TSva]=2
<ul> <li>Fr</li> <li>Et</li> <li>In</li> <li>Tr</li> <li>0000</li> <li>0008</li> <li>0010</li> <li>0020</li> </ul>	31 4.988491 31 4.988491 31 4.988491 ame 23: 66 L chernet II, S tternet Prote ansmission ( 0 00100000 c 0 0000000 c 0 0000000 c 0 0010111 ( 0 001011 ( 0 0010000 ( 0 00100000 ( 0 00100000 ( 0 00100000 ( 0 00100000 ( 0 0000000 ( 0 00000000 ( 0 0000000000	172.17.101.2 ytes on wire (5 rrc: Digital_la col version 4,	211.69.32.50 "" 28 bits), 66 bytes cz 76:22 (00:03:0f:1a: 5rc: 211.69.32.50, bs , Src Port: 80, Dst F 0 11100101 11111000 C 0 0010001 00001000 C 0 0010000 01000000 C 0 0010000 01000000 C	TCP aptured (528 bits 76:22), Dst: Comp st: 172.17.101.2 Port: 37609, Seq: 01000100 00000000 00000000 0100101 00000000	66 3760: ) on interfa alln_e5:f8: 1, Ack: 1, 00000001 0000000 0000010 00000010 00000010	ace 0 44 (20: Len: 0 E 	[ACK] 1a:06	seq=1 ;	44)	win=16652	2 Len=0	) TSva]=2
<ul> <li>Fr</li> <li>Et</li> <li>In</li> <li>Tr</li> <li>00000</li> <li>0008</li> <li>0010</li> <li>0020</li> <li>0020</li> </ul>	and 1.988491 and 23: 66 b thernet II. 5 tternet Prote ansmission ( 0 00100000 c 0 0000000 c 0 0000111 c 0 00100111 c	172,17,101.2 wytes on wire (5 cr: Digital_la col version 4, control Protocol 0001010 0000011 0001010 011011 0001010 101000 0001010 0000001 0000001 101000	211.69.32.50 m 28 bits), 66 bytes cc :76:22 (00:03:0f:1a: 5rc: 211.69.32.50, 00 , Src Port: 80, Dst F 01100101 11111000 CC 00100010 00001000 00100010 00001000 00100010 0010000 00100000 100100010 011000101 11001000C	TCP aptured (528 bits 76:22), bst: Comp 51:172.17.101.2 Port: 37609, Seq: 01000100 00000000 00000000 01000110 0000000 01000101 0001001 0101010 11010100 1010100	66 3760: ) on interf; alIn_e5:f8:4 1, Ack: 1, 000000011 00000001 00010001 10111100 0000001	ace 0 44 (20: Len: ( 	[ACK] 1a:06	:e5:f8:	44)	win=16652	2 Len=0	) TSVa1=2

#### ②释放连接报文分析。

对抓取到的 TCP 报文进行分析,找到释放连接所对应的数据报文,进行详细内容分析,并 根据数据报文内容填写表 6-4。

	1	÷				
皮旦	今四夕称	第一次	第二次	第三次	第四次	字码丰二的信息
ליל	于权石称	字段值	字段值	字段值	字段值	于权农小时信息
1	Source Port					
2	Destination Port					
3	Sequence Number					
4	Acknowledgement Number					
5	Header Length					
6	Reserved					
7	Flags					
8	Window Size					
9	Checksum					
10	Urgent Pointer					
	抓取数据包的详细内	容:				
11						

#### 表 6-4 释放连接报文分析

## (3) 对比分析

根据 TCP 建立连接和释放连接的报文结构,比较两个过程数据报结构的 6 个关键差别,并填写 表 6-5。

皮旦	字段名称	请求	连接报文	释	放连接报文
ኯኇ	于权石协	字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6					
	对比描述详细内容:				
7					
,					

# 表 6-5 TCP 通信过程报文对比分析

## 八、实验分析

## 1、UDP 报文和 TCP 报文结构有何区别?

- (1) UDP 报文和 TCP 报文结构上有什么不同?
- (2) UDP 协议和 TCP 协议的不同之处是什么?

#### 2、如何找到欲分析的数据报文?

- (1) 网络抓包时如何找到指定协议的数据报文?
- (2) 网络抓包时如何找到指定来源和目的地址的数据报文?
- (3) 网络抓包时如何找到指定套接字的数据报文?
- (4) 如何从众多的 TCP 数据报文中找到建立连接和释放连接的数据报文?

## 3、聊天工具使用的传输协议

- (1) 使用 TCP 传输协议的聊天工具有哪些,使用 UDP 传输协议的聊天工具有哪些?
- (2) QQ 软件发送消息和发送文件使用的传输协议是否一样? 分别是什么?
- (3) 软件开发者在开发软件时如何选取软件使用的传输协议?