## 第三届上海市大学生网络安全大赛 流量分析 traffic WriteUp

● 于 2020-08-27 01:19:44 发布 ● 540 🛠 收藏 1 mutou990 分类专栏: <u>CTF</u> 文章标签: <u>安全</u> 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/mutou990/article/details/108248461

版权

CTF 专栏收录该内容

17 篇文章 1 订阅 订阅专栏 参考1: https://www.cnblogs.com/sn1per/p/11835479.html 参考2: https://blog.csdn.net/JaySRJ7/article/details/102215248

题目链接: https://pan.baidu.com/s/1Utfg8W-NS4Afl0xG-HgSbA 提取码: 9wgs

解题思路:

打开流量包后,按照协议进行分类,发现了存在以下几种协议类型:

ARP / DNS / FTP / FTP-DATA / ICMP / ICMPv6 / IGMPv3 / LLMNR / NBNS / SSDP / SSL / TCP / TLSv1.2 / UDP

				「「「「「「」」であるので、「「」」であるので、「「」」であるので、「「」」であるので、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、		石石	待刀		4 <u>†</u> 7		
traffic.pcapng											X
文件(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H)								
											1
↓ 应用显示过滤器 … 《Ctrl-	/>										+
fo. Time	Source	Destination	Protocol Length	Info							<u> </u>
8571 78.359918	bc:20:10:ca:48:8c	IntelCor_97:33:df	ARP Protocol 2	Who has 192.168.43.1	159? Tell 192.1	.68.43.1					
8572 78.359974	IntelCor_97:33:df	bc:20:10:ca:48:8c	ARP 42	192.168.43.159 is at	t 68:07:15:97:3	3:df					
8924 102.510611	bc:20:10:ca:48:8c	IntelCor_97:33:df	ARP 42	Who has 192.168.43.1	159? Tell 192.1	.68.43.1					
8925 102.510667	IntelCor_97:33:df	bc:20:10:ca:48:8c	ARP 42	192.168.43.159 is at	t 68:07:15:97:3	3:df					
9253 130.371912	bc:20:10:ca:48:8c	IntelCor_97:33:df	ARP 42	Who has 192.168.43.1	159? Tell 192.1	.68.43.1					
9256 130.371936	IntelCor_97:33:df	bc:20:10:ca:48:8c	ARP 42	192.168.43.159 is at	t 68:07:15:97:3	3:df					
17943 154.842916	bc:20:10:ca:48:8c	IntelCor_97:33:df	ARP 42	Who has 192.168.43.1	159? Tell 192.1	.68.43.1					
17944 154.842965	IntelCor_97:33:df	bc:20:10:ca:48:8c	ARP 42	192.168.43.159 is at	t 68:07:15:97:3	3:df					
315 2.384300	240e:e8:f306:db7f:	c… 240e:5a::6666	DNS 93	Standard query 0x9f	f A gt1.baidu.	com					
316 2.384390	240e:e8:f306:db7f:	c 240e:5a::6666	DNS 93	Standard query 0x63	e7 A gt2.baidu.	com					
317 2.384619	240e:e8:f306:db7f:	c 240e:5a::6666	DNS 93	Standard query 0xb1	1 AAAA gt2.bai	.du.com					
318 2.384743	240e:e8:f306:db7f:	c 240e:5a::6666	DNS 93	Standard query 0xc70	19 AAAA gt1.bai	.du.com					
319 2.414875	240e:e8:f306:db7f:	c 240e:5b::6666	DNS 93	Standard query 0x63	e7 A gt2.baidu.	com					
320 2.415862	240e:e8:f306:db7f:	c 240e:5b::6666	DNS 93	Standard guery 0xc70	d9 AAAA gt1.bai	.du.com					
321 2.415944	240e:e8:f306:db7f:	c 240e:5b::6666	DNS 93	Standard query 0x9fo	cf A gt1.baidu.	com					
322 2.416023	240e:e8:f306:db7f:	c 240e:5b::6666	DNS 93	Standard query 0xb1	1 AAAA gt2.bai	.du.com					Ŧ
Ename 1: 42 bytes	on wine (226 bits) A	2 bytes centured (226	hits) on intenfe	200 0							_
Frame 1: 42 Dytes	Un wire (556 Dits), 4	2 Dytes Captured (356	bits) on interna	ace 0	0-)						
V Ethernet II, Src:	Vension 4 Ensy 102 1	69 42 150 Date 144 76	DC:20:10:Ca:40:	OC (DC:20:10:Ca:40:	6C)						
Internet Protocol	version 4, Src: 192.1	Det Dept: 25003	. 39.04								
v user batagram Prot	.0001, SPC POPU: 40527	, DSC POPC: 25905									
0000 bc 20 10 ca 4	8 8c 68 07 15 97 33 (	df 08 00 45 00H	.h3E.								
0010 00 1c 0c ee 4	0 00 03 11 b2 fb c0 a	a8 2b 9f 90 4c@	+L								
0020 3b 54 b4 f7 6	5 2f 00 08 2d cf	;Te	/								
🔵 🍸 traffic					分组: 17953 ・ 已駅	显示: 17953 (1	.00.0%)	<ul> <li>加载时间:</li> </ul>	0:0.749	配置文件: Defa	wift]0,
	10 m 1	Wireshark · 协议分级统计 · traff	c								~
》 统计(S) 电话(Y) 无线(V	V) 工具(T) 帮助(H)	14 M					11.44			a latin	
d 捕获文件属性	Ctrl+Alt+Shift+C	17/12		按分组白分比 分组	按字节白分比	字节	比特/秒	End Packets	End Bytes	End Bits/s	
- 已解析的地址	-1	4 Frame		100.0 1795	3 100.0	16633916	843 k	0	0	0	
(=	E-	4 Ethernet	1	100.0 1795	3 1.5	251342	12 k	0	0	U	
对话		Internet Protocol Ver	sion o	1.2 213	0.0	8520	432	1	0	0	
C: 端点	3:	Link-local Mult	ticast Name Resolution	0.0 2	0.0	44	2	2	44	2	

分组长度	15.	Domain Name System	1.0	175	0.1	21194	1074	175	21194	1074
1/0 图表(1)	7	Transmission Control Protocol	0.0	3	0.0	96	4	3	96	4
	1.	Internet Control Message Protocol v6	0.2	32	0.0	1012	51	32	1012	51
10035 NO. 2010 101 101 101 101 101 101 101 101 10	7.	<ul> <li>Internet Protocol Version 4</li> </ul>	98.7	17726	2.1	354540	17 k	0	0	0
DHCP (BOOTP) Statistics		User Datagram Protocol	0.7	133	0.0	1064	53	116	928	47
ONC-RPC Programs	7	Simple Service Discovery Protocol	0.1	12	0.0	2096	106	12	2096	106
29West		NetBIOS Name Service	0.0	3	0.0	150	7	3	150	7
ANCD	20	Link-local Multicast Name Resolution	0.0	2	0.0	44	2	2	44	2
ANCE	26	Transmission Control Protocol	98.0	17585	96.1	15991818	811 k	15468	13840202	701 k
BACnet	-96	Secure Sockets Layer	11.9	2136	94.0	15642468	793 k	1920	15135530	767 k
Collectd	36	<ul> <li>Hypertext Transfer Protocol</li> </ul>	0.4	64	41.5	6903889	350 k	32	43778	2220
DNS	36	Media Type	0.1	11	41.2	6849528	347 k	11	6850035	347 k
流量图	36	Line-based text data	0.0	3	0.0	73	3	3	73	3
HART-IP	)6	JavaScript Object Notation	0.0	2	0.0	768	38	2	768	38
HDEEEDS	<u>)</u> 6	Compuserve GIF	0.1	16	0.0	680	34	16	680	34
	a	Malformed Packet	0.0	4	0.0	0	0	4	0	0
HIIP	1:2.	FTP Data	0.2	28	0.2	29435	1492	28	29435	1492
HTTP2		File Transfer Protocol (FTP)	0.4	80	0.0	2069	104	80	2069	104
Sametime		Data	0.1	21	0.0	2819	142	21	2819	142
TCP 流图形		Internet Group Management Protocol	0.0	5	0.0	80	4	5	80	4
UDP 多播流		Internet Control Message Protocol	0.0	3	0.0	52	2	3	52	2
		Address Resolution Protocol	0.1	14	0.0	392	19	14	392	19
IPv4 Statistics	# # # # # # # #	- 55								
IPv6 Statistics	7.257.122	· · ·								
,	- (III							Close	夏	制 🔻 н

(这里可以在过滤输入框里输入FTP回车后,再对筛选过的包进行分析查看,也可以ctrl+F 查找【字符串】关键字ctrl+F 查找关键字flag或者flag的【十六进制】666c6167进行快速查找,下面直接用查找flag关键字方法)



<b>_</b> t	raffic.pcapng						- 🗆 🗙					
文作	文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电活(V) 工具(T) 帮助(H)											
	ք 🔳 🖉 💿 🕌 陆 🗙 🖻 🔍 👄 😤 🖗 🖳 🗐 Q. Q. Q. X.											
	应用显示过滤器 ⋯ 《Ctr	-1-/>					应用此过滤器					
	分组字节流 ▼	宽窄 🔻 🔳 🛛	≤分大小写 字符串 ▼	flag		查找 查找 一	取消					
No.	Time	Source	Destination	Protocol	Length Info		<b>^</b>					
	7402 17.381176	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6298395 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7403 17.381176	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6299795 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7404 17.381177	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6301195 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7405 17.381177	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6302595 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7406 17.381177	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6303995 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7407 17.381177	180.97.34.136	192.168.43.159	TCP	1454 443 → 58146	46 [ACK] Seq=6305395 Ack=1871 Win=18176 Len=1400 [TCP segment	of a					
	7408 17.381178	180.97.34.136	192.168.43.159	TI Sv1.2	1249 [SSI segmen	ent of a reassembled PDUl						

		2001011011200			TEAS [SSE SeBmette of a reasonated roo]					
7	409 17.381242	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seq=1871 Ack=6294419 Win=5364480 Len=0					
7	410 17.381399	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seg=1871 Ack=6297891 Win=5364480 Len=0					
7	411 17.381482	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seg=1871 Ack=6301363 Win=5364480 Len=0					
7	412 17.381527	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seg=1871 Ack=6304835 Win=5364480 Len=0					
7	413 17.381593	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seq=1871 Ack=6307990 Win=5364480 Len=0					
7	414 17.441227	182.254.217.142	192.168.43.159	FTP	106 Response: 227 Entering Passive Mode (182,254,217,142,47,56).					
7	415 17.441586	192.168.43.159	182.254.217.14	2 FTP	65 Request: RETR flag	-				
<pre>&gt; Frame 7415: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0 &gt; Ethernet II, Src: IntelCor_97:33:df (68:07:15:97:33:df), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c) &gt; Internet Protocol Version 4, Src: 192.168.43.159, Dst: 182.254.217.142      Transmission Control Protocol, Src Port: 58106, Dst Port: 21, Seq: 7, Ack: 53, Len: 11     Source Port: 58106     Destination Port: 21     [Stream index: 34]     [TCP Segment Len: 11]     Sequence number: 7 (relative sequence number)     [Next sequence number: 18 (relative sequence number)]     Acknowledgment number: 53 (relative ack number)     0101 = Header Length: 20 bytes (5) &gt; Flags: 0x018 (PSH, ACK) Window size value: 20950</pre>										
	lindow size value: Calculated window Window size scali hecksum: 0x16fe [ Checksum Status:	: 20950 w size: 20950] ing factor: -1 (unkno unverified] Unverified]	wn)]			-				
0000 0010 0020 0030 0040	bc 20 10 ca 48 8 00 33 66 50 40 6 d9 8e e2 fa 00 1 51 d6 16 fe 00 6 0a	3c 68 07 15 97 33 df 100 40 06 57 a0 c0 a8 15 e8 2e 84 6e 0d e2 100 52 45 54 52 20 66	08 00 45 00 2 2b 9f b6 fe 2 c8 1c 50 18 6 6c 61 67 0d	H.h3E .3FP@.@. W+ nP QRE TR flag	查找出来没有用,继续查找					
07	Request and (ftp.requ	uest.arg). 4 字节			│ 分组: 17953 · 己見示: 17953 (100.0%) · 加載时间::0/0.572 @ 露客文件/ Def	faul ()				

2010       Billion	_					
Image Control         Image Control         Image Control         Image Control           Image Control	文件(F)	编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助	(H)
■ Data 1       ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	🛋 🔳 /	// 💿 🚺 🔚 🗙	🔓 । ९. 🗢 🗢 🕾 🗿 👃	📃 🗐 🔍 🔍 🔍 🎹		
地球状理         (E)         (E)<	<b>」</b> 应用5	显示过滤器 … ⟨Ctrl-/	$\diamond$			□ - 表达式… + 应用此过滤器
Tem         Tem <th>[</th> <th>分组字节流 ▼</th> <th><b>572</b> ▼ □ ⊠4</th> <th>→大小写   字符串   ▼</th> <th>flag</th> <th>古田山の「古田山」</th>	[	分组字节流 ▼	<b>572</b> ▼ □ ⊠4	→大小写   字符串   ▼	flag	古田山の「古田山」
1/2       100.07.34.15       102.168.4.3.159       107       104.4.43 - S1346 [ACC] SequentS (ACC] Sequent of a.         1/2       100.07.34.15       102.168.4.3.159       110.07.34.15	No	Time	Source	Destination	Protogol	
27 17.38177       100.97.34.156       152.186.43.159       110	7/	106 17 381177	180 97 34 136	192 168 /3 159	TCP	$1/51/4/3 \rightarrow 581/6$ [ACK] Seg=6303995 Ack=1871 Win=18176 Len=1/00 [TCP segment of a
748 17.31178       180.97.34.136       152.186.4.3.159       1152.18.4.3.159       1152.18.4.3.159       1152.18.4.3.159       1152.18.4.3.159       1152.18.4.3.159       1152.154.4.3.159       1159.97.34.136       1177       55 531.66 - 443       [ACC] Sequility Active 239459       Nun-5364480       Lem-6         7410 17.33159       132.166.4.3.159       180.97.34.136       1179       55 531.66 - 443       [ACC] Sequility Active 239459       Nun-5364480       Lem-6         7411 17.33159       132.166.4.3.159       180.97.34.136       1179       55 531.66 - 443       [ACC] Sequility Active 330435       Nun-5364480       Lem-6         7413 17.33157       132.166.4.3.159       180.97.34.136       1179       55 531.66 - 443       [ACC] Sequility Active 330435       Nun-5364480       Lem-6         7413 17.33157       132.254.217.142       132.168.4.3.159       182.254.217.142       170       56 531.69 - 120.85       State Active Mode (182.254.217.142,47.159)       182.254.217.142       170       54 531.69 - 120.86       ACKI Sequility State Active Mode (182.254.217.142,47.159)       182.254.217.142       152.168.4.3.159       182.254.217.142       152.168.4.3.159       182.254.217.142       152.168.4.3.159       182.254.217.142       152.168.4.3.159       182.254.217.142       152.168.4.3.159       182.254.217.142       152.168.4.3.159       182.254.217.142	74	107 17 381177	180 97 34 136	192 168 43 159	TCP	$1454 443 \rightarrow 58146$ [ACK] Seq=6305395 Ack=1871 Win=18176 Len=1400 [TCP segment of a
27 approx 17, 331242       192, 168, 43, 159       180, 47, 34, 156       TCP       55 83146 - 443       CKC, 55 cm 437, Ack-630789       Minth and an and an and an and an and an and and	74	108 17.381178	180.97.34.136	192.168.43.159	TLSv1.2	1249 [SSI segment of a reassembled PDU]
111 17.381399       192.168.43.159       180.97.34.156       TCP       54 58146       -443 [ACK] Seq=1371 Ack-6307391 Min-3564480 Len-0         7411 17.381537       192.168.43.159       180.97.34.156       TCP       54 58146       -443 [ACK] Seq=1371 Ack-6307391 Min-3564480 Len-0         7413 17.381537       192.168.43.159       180.97.34.156       TCP       54 58146       -443 [ACK] Seq=1371 Ack-6307399 Min-3564480 Len-0         7413 17.381537       192.168.43.159       180.97.34.156       TCP       54 58146       -443 [ACK] Seq=1371 Ack-6307399 Min-3564480 Len-0         7414 17.44127       162.254.17.142       TCP       56 58149       -443 [ACK] Seq=1671 Ack-6307399 Min-3564480 Len-0         7414 17.441361       192.168.43.159       180.254.217.142       TCP       56 58149       -443 [ACK] Seq=0 Ack-1 Min-556480 Len-0         7414 17.441361       192.168.43.159       180.254.217.142       TCP       FG8 58149       -444.1 Min-5564680 Len-0         7418 17.48129       192.168.43.159       172.168.43.159       182.254.277.142       TCP       FG8 58149       -444.1 Min-5564680 Len-0         719 17.522353       182.254.217.142       TCP       158 Septoner Min-65535 Len-0       MS5-1469 KAK, MSPHelt M.         710 17.52353       182.254.217.142       TCP       158 Septoner Min-65531 Len-0       Min-76191 (Piston)	74	409 17.381242	192,168,43,159	180.97.34.136	TCP	$54 58146 \rightarrow 443 [ACK] Seq=1871 Ack=6294419 Win=5364480 Len=0$
1117.381482       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-1871 Ack-6303133 Hkm-5364480 Lene9         7412 17.381533       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-1871 Ack-6303799 Hkm-5364480 Lene9         7413 17.381533       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-1871 Ack-6308799 Hkm-5364480 Lene9         7413 17.381533       192.168.43.159       182.254.277.142       TDP 106 Response: 227 Intering Passive Mode (182.254.277.142, 47.56).         7415 17.44156       192.168.43.159       182.254.277.142       TCP       66 58149 + 12088 [XML SS535 Lene9 MSS-1460 SACK PERM+1 ML 7418 17.45207 Han2-4520 Lene9 MSS-1460 SACK PERM+1 ML 7418 17.452159       192.168.43.159       182.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5366488 Lene9         7413 17.42047       192.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5366488 Lene9       7419 TT.723233       182.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5366488 Lene9       7419 TT.723233       182.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5366488 Lene9       7419 TT.723233       182.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5364698 Lene9       7419 TT.723233       182.254.277.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Hkm-5364698 Lene9       7419 TT.742748141 T.441913 TT.741914 TT.741914 TT.741914 T	74	410 17.381399	192.168.43.159	180.97.34.136	ТСР	54 58146 → 443 [ACK] Seq=1871 Ack=6297891 Win=5364480 Len=0
7412 17.381527       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-1871 Act+03099 Min-3564480 Lene0         7413 17.38153       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-1871 Act+03099 Min-3564480 Lene0         7413 17.48159       192.168.43.159       180.97.34.136       TCP       54 58146 + 443 [ACK] Seq-0871 Act+03099 Min-3564480 Lene0         7415 17.44154       192.168.43.159       182.254.217.142       FTP       168 Response: 227 Entering Passive Mode (182,254,217,142,47,56).         7415 17.441541       192.168.43.159       182.254.217.142       TCP       65 61208 - 5248 [StH], Ack[ Seq-0871 Act+01075535 Len-0 MSS-1460 MS-128 SALK PEM+1         7418 17.42159       192.168.43.159       182.254.217.142       TCP       65 12088 - 5248 [StH], MacK[ Seq-0871 Act+01075535 Len-0 MSS-1460 MS-128 SALK PEM+1       Min-32200 Len-0 MSS-1460 MS-128 SALK PEM+1         7418 17.42159       192.168.43.159       TCP Aston       61 2088 - 5248 [StH], Ack [ Seq-0871 Act+010756488 Lene0         7419 17.522353       182.254.217.142       TCP Aston       FTP 115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         [TCP Sequence number: 13       (relative sequence number)       Actional Actiona	74	411 17.381482	192,168,43,159	180,97,34,136	TCP	54 58146 → 443 [ACK] Seg=1871 Ack=6301363 Win=5364480 Len=0
13 17.381393       192.166.43.159       180.97.34.136       TCP       54 5814.6       +43.164.54(5)       Seq.1821.Ack-6307390 Min-5364.88 Len-0         7416 17.441227       182.254.17.142       FTP       136 Request: RETK flgg         7416 17.441394       192.166.43.159       182.254.217.142       FTP       65 Request: RETK flgg         7416 17.441394       192.166.43.159       182.254.217.142       TCP       66 50184 > 22080 [SW]. Scq=0 Min=55555 Len=0 MS5-1460 MS-128 SACK PERM=1         7417 17.44247       182.254.217.142       TCP       66 50184 > 22080 [SW]. Scq=0 Akr-3 Sage Min=55555 Len=0 MS5-1460 MS-128 SACK PERM=1 Min-2500 Len=0 MS5-1460 MS-128 MIRE MIN-2500 Len=0 MS5-146	74	412 17.381527	192.168.43.159	180.97.34.136	ТСР	54 58146 → 443 [ACK] Seg=1871 Ack=6304835 Win=5364480 Len=0
7414 17.441227       182.254.217.142       192.168.43.159       FTP       106 Response: 227 Entering Passive Mode (182,254.217.142,7,56).         7415 17.441396       192.168.43.159       182.254.217.142       FTP       65 Request: RETR flg         7415 17.441394       192.168.43.159       182.254.217.142       172       66 5 12088 - 58149 eNin-655355 Lem-d MSn-1460 NS-1460 NS-128 SACK PERM-1 NC         7417 17.482447       182.254.217.142       192.168.43.159       TCP       66 5 12088 - 58149 eNin-55535 Lem-d MSn-1460 NS-1460 NS-128 SACK PERM-1 NC         7418 17.482159       192.168.43.159       TCP       65 12088 - 58149 eNin-55535 Lem-d MSn-1460 NS-1460 NS-128 SACK PERM-1 NC         7418 17.482159       192.168.43.159       TCP       55 Request: RETR flg       55 Request: RETR flg         7419 17.522553       182.254.217.142       192.168.43.159       TCP       55 Request: RETR flg         7419 17.522553       182.254.217.142       192.168.43.159       TCP       55 Request: RETR flg         7419 17.522553       182.254.217.142       192.168.43.159       TCP       55 Request: RETR flg         7419 17.522553       182.254.217.142       192.168.43.159       TCP       51 Seguence number: S1         8010 Seguence number: 13       (relative act number)       Internet Seguence number: S1       FCP       105 Seguence number: S1       FCP </td <td>74</td> <td>413 17.381593</td> <td>192.168.43.159</td> <td>180.97.34.136</td> <td>TCP</td> <td>54 58146 → 443 [ACK] Seg=1871 Ack=6307990 Win=5364480 Len=0</td>	74	413 17.381593	192.168.43.159	180.97.34.136	TCP	54 58146 → 443 [ACK] Seg=1871 Ack=6307990 Win=5364480 Len=0
7 145 17.441586       192.168.43.159       182.254.217.142       FTP       65 Request: RETH flag         7416 17.441586       192.168.43.159       182.254.217.142       192.168.43.159       120.268.159       120.868       182.254.217.142       170       66 12888 + 51288 (MN) Seq=0 Atx-1 Min-25335 Lene 0 MS-1460 MS-1400 SACK_PERM-1 M.         7418 17.482047       182.254.217.142       127.168.43.159       122.254.217.142       170       54 58149 + 12088 (ACK) Seq=0 Atx-1 Min-25365 Lene 0 MS-1460 SACK_PERM-1 M.         7418 17.25235       182.254.217.142       122.168.43.159       FTP       115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         [Mext sequence number)       [Mext sequence number)       [Mext sequence number: 114 (relative sequence number)]       Actional degment number: 129       [Calculated window size: 229]       [Calculated window size: 229]       [Calculated window size: 229]       [Mindow size scaling factor: -1 (unknown)]       Checksum: 8xcle6 [Unverified]       Inceksum: 92.96 01 20 ca 48 8 c 68 00 45 60       h3HE.       Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20 10 ca 48 8 c 68 00 45 60       h3HE.       Incelsum:	74	414 17.441227	182.254.217.142	192.168.43.159	FTP	106 Response: 227 Entering Passive Mode (182,254,217,142,47,56).
2 / 16 17, 441941       192, 168, 43, 159       182, 254, 217, 142       TCP       66 58149 + 12088   5%1] Seq=0 Min-65335 Len-0 MSS-1460 MS-128 SACK PERM-1 Min-25035 Len-0 MSS-1460 SACK PERM-1 Min-25035 Len-0         7418       17, 482159       192, 168, 43, 159       182, 254, 217, 142       TCP       54 58149 + 12088 + 58149 [SWN, AcK] Seeq-0 Ack-1 Min-25036 Len-0       SACK PERM-1 Min-25035 Len-0 MSS-1460 SACK PERM-1 Min-25036 Len-0         7418       17, 482159       192, 168, 43, 159       182, 254, 217, 142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Min-25036 Len-0         719       119, 15, 22353       182, 254, 217, 142       192, 168, 43, 159       FTP       115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         ICP Sequence number:       13       (relative sequence number)       [Mext sequence number:       14       (relative sequence number)         [Mext sequence number:       14       (relative sequence number)       [Mext sequence number:       16       (relative ack number)         [Mindow size value:       229       [Calculated window size:       229       [Calculated window size:       229         [Calculated window size:       229       [Calculated window size:       19       [Seguence Protocol (FP)       *       *         * 150 Opening BINARY mode data connection for flag (7 bytes).       *       *       *       *	74	415 17.441586	192.168.43.159	182.254.217.142	FTP	65 Request: RETR flag
741 17.482047       182.254.217.142       192.168.43.159       TCP       66 12088 + 56149 (SW), ACK] Seq=1 Ack-1 Win-23208 Len-0         7418 17.482159       192.168.43.159       TCP       54 58149 + 12088 [ACK] Seq=1 Ack-1 Win-23208 Len-0         7419 17.52235       182.254.217.142       192.168.43.159       FTP       115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         [TCP Segment Len: 61]       sequence number: 53       (relative sequence number)       [Rext sequence number: 18 (relative sequence number)]         Acknowledgment number: 18 (relative sequence number)       [Rext sequence number: 65]       Flags: 6x018 (SN, ACK)         Window size value: 229       [Calculated window size: 229]       [Calculated window size: 229]       [Calculated window size: 229]         [Interspect cold (FTP)       - 150 Opening BINARY mode data connection for flag (7 bytes). \r\n       Response code: Fla status okay; about to open data connection (150)         Response code: Fla status okay; about to open data connection for flag (7 bytes).      ,, yP,         00000       66 87 15 97 33 df bc 20 10 ca 48 8 c0 80 45 00	74	416 17.441941	192.168.43.159	182.254.217.142	TCP	66 58149 → 12088 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
7418 17.428159       192.166.43.159       182.254.217.142       TCP       54 58149 + 12088 [ACK] Seq-1 Ack-1 Win-5364608 Len-0         7419 17.522353       182.254.217.142       192.168.43.159       FTP       115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         [TCP Segment Len: 61]       Sequence number: 114 (relative sequence number)       [Hext sequence number: 18 (relative ack number)]         Acknowledgemt number: 18 (relative ack number)       [Acknowledgemt number: 18 (relative ack number)]         Acknowledgemt number: 18 (relative ack number)       [Interstepsement Len: 61]         Sequence number: 18 (relative ack number)       [Interstepsement Len: 61]         Mindow size scaling factor: -1 (unknown)       [Checksum: 8xc1c6 [unverified]         [Interstepsement Len: 61]       [Sto2/AK analysis]         TCP payload (61 bytes)       -         * FIBE Transfer Protocol (FIP)       -         * 150 Opening BINARY mode data connection for flag (7 bytes).         * 150 Opening BINARY mode data connection for flag (7 bytes).         @ 68 07 15 97 33 df bc 20 10 ca 48 0x 08 00 45 00      3HE.         @ 000       68 07 15 97 33 df bc 20 10 ca 48 0x 08 00 45 00      3HE.         @ 000       68 07 15 97 33 df bc 20 10 ca 48 0x 08 00 45 00      3HE.         @ 000       68 07 15 97 33 df bc 20 10 ca 48 0x 08 00 45 00	74	417 17.482047	182.254.217.142	192.168.43.159	TCP	66 12088 → 58149 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 W
7419 17.522353       182.254.217.142       192.168.43.159       FTP       115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).         [[CP Segment Len: 61]       Sequence number: 31 (relative sequence number)         [Next sequence number: 114 (relative sequence number)]         Acknowledgment number: 114 (relative sequence number)         [Next sequence number: 209         [Galculated window size: 229]         [Calculated window size: 229]         [Ealculated window size: 229]         [Enducated window size: calculated window size:	74	418 17.482159	192.168.43.159	182.254.217.142	TCP	54 58149 → 12088 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
[TCP Segment Len: 61]         Sequence number: 53       (relative sequence number)         [Next Sequence number: 14       (relative ack number)         [Next Sequence number: 18       (relative ack number)         0101       = Header Length: 20 bytes (5)         Flags: Kox18 (PSH, ACK)       Window size value: 229         [Calculated window size: 229]       [Window size scaling factor: -1 (unknown)]         Checksum: 0xc16 [unverified]       Unverified]         Urgent pointer: 0       >         > 150 [SEQ/ACK analysis]       TCP payload (61 bytes)         TCP payload (61 bytes)       +	74	419 17.522353	182.254.217.142	192.168.43.159	FTP	115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).
[Int Jeguenn Lumber: 5]       (relative sequence number)         [Next sequence number: 114       (relative sequence number)         Acknowledgment number: 120       (relative sequence number)         Acknowledgment number: 120       (relative sequence number)         Acknowledgment number: 120       (relative sequence number)         (Nindow size value: 229       [Calculated window size: 229]         [Calculated window size: 229]       [Calculated window size: 229]         [Indiversified]       (relative sequence number)         Urgent pointer: 0       0         > [SEQ/ACK analysis]       (relative sequence numction for flag (7 bytes).\n\n         Response arg: Opening BINARY mode data connection for flag (7 bytes).       h	[	TCP Segment Lon	• 61]			
Sepence under: 134 (relative sequence number)]         Acknowledgment number: 114 (relative sequence number)]         Itags: 8x018 (PSH, ACK)         Window size value: 229         [Kindow size scaling factor: -1 (unknown)]         Checksum Status: Unverified]         Urgent pointer: 0         • [55Q/ACK analysis]         TCP payload (61 bytes)         • File Transfer Protocol (FIP)         • 150 Opening BINARY mode data connection for flag (7 bytes).         Response code: File status okay; about to open data connection (150)         Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 77 33 df bc 20 10 ca 48 8c 68 a0 45 00       h		equence number:	53 (relative ser	ience number)		
Interf studiet number: 14       (relative ack number)         Acknowledgment number: 18       (relative ack number)         0101 = Header Length: 20 bytes (5)         Flags: 6x018 (PSH, ACK)         Window size value: 229         [Calculated window size value: 219         [Calculated window size value: 229         [Calculated window size value: 220		Next sequence n	umber: 11/ (relati	ive sequence number)]		
<pre>Note: Hower Hander Length: 20 bytes (5) P Flags: 0x018 (PSH, ACK) Window size value: 229 [Calculated window size: 229] [Window size scaling factor: -1 (unknown)] Checksum Status: Unverified] Urgent pointer: 0 P [SEQ/ACK analysis] TCP payload (61 bytes) FILE Transfer Protocol (FTP) File Status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes). \r\n Response arg: Opening BINARY mode data connection for flag (7 bytes). </pre>		cknowledgment n	umber: 18 (relativ	/e ack number)		
<ul> <li>Flags: 0x018 (PSH, ACK)</li> <li>Window size value: 229         <ul> <li>[Calculated window size: 229]</li> <li>[Window size scaling factor: -1 (unknown)]</li> <li>Checksum: 0xc1c6 [unverified]</li> <li>[Checksum Status: Unverified]</li> <li>[Checksum Status: Unverified]</li> <li>Urgent pointer: 0</li> <li>&gt; [SEQ/ACK analysis]</li> <li>TCP payload (61 bytes)</li> </ul> </li> <li>File Transfer Protocol (FTP)         <ul> <li>* IS0 Opening BINARY mode data connection for flag (7 bytes).\r\n</li> <li>Response arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>* M</li></ul></li></ul>	0	101 = Head	er length: 20 bytes (	(5)		
Window size value: 229         [Calculated window size scaling factor: -1 (unknown)]         Checksum: 8xclc6 [unverified]         [Checksum: 8xclc7 [Straft add sto connection for flag (7 bytes). \r\n         Response arg: Opening BINARY mode data connection for flag (7 bytes).         @ 00 for 01 so 21 fa dd ed 2 c8 1 c8 8 c8 479 59 18         *	⊳F	lags: 0x018 (PS	H. ACK)	(-)		
[Calculated window size: 229] [Window size scaling factor: -1 (unknown)] Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis] TCP payload (61 bytes) ■ File Transfer Protocol (FTP) ■ 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response arg: Opening BINARY mode data connection for flag (7 bytes). Response arg: Opening BINARY mode data connection for flag (7 bytes). 0000 66 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00 0010 06 51 7 de 40 00 30 06 b5 e0 b6 fe d 98 ec 0 a8 2 b 9f 00 15 e2 1a 0d e2 c8 1c e8 2e 84 79 50 18 7 4 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 0016 07 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 6d fi 0017 72 06 65 c6 16 67 20 28 37 20 62 79 74 65 73 29 0018 00 e5 1 c6 00 00 31 35 31 20 62 79 74 65 73 29 0019 2e 0d 0a 002 2e 0d 0a 003 2e 0d 0a 004 67 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 6d fi 105 0 r flag (7 bytes) 005 72 62 57 70 42 67 73 29 007 2e 0d 0a 008 00 65 17 (bytes) 55 \$\pm 1 009 008 00 00 00 00 00 00 00 00 00 00 00 00	W	indow size valu	e: 229			
[Window size scaling factor: -1 (unknown)]         Checksum: 0xclc6 [unverified]         [Checksum Status: Unverified]         [Urgent pointer: 0         > [SEQ/ACK analysis]         TCP payload (61 bytes)         * File Transfer Protocol (FTP)         * 150 Opening BINARY mode data connection for flag (7 bytes).\r\n         Response org: Opening BINARY mode data connection for flag (7 bytes).\r\n         Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00       h3HE.         .e6.0.	Г П	Calculated wind	ow size: 2291			
Checksum: Øxclc6 [unverified] [Checksum Status: Unverified] Urgent pointer: 0       ●         9 [SEQ/ACK analysis] TCP payload (61 bytes)       ●         4 File Transfer Protocol (FTP)       ●         • 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response code: File status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes).       ●         0000       68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00 00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8 2b 9f 00 15 e2 fa 0d e2 c d8 1c e8 2e 84 79 50 18 15 0 Openin 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 56 37 20 28 37 20 62 79 74 65 73 29 2e 0d 0a       milit 17953 · CB素: 17953 (100.08) · jmtthill: 0:0.572]       mttty for left before         • **       ************************************	l h	Window size sca	ling factor: -1 (unkr	nown)]		
[Checksum Status: Unverified]         Urgent pointer: 0         > [SEQ/ACK analysis]         TCP payload (61 bytes)         4 File Transfer Protocol (FTP)         * 150 Opening BINARY mode data connection for flag (7 bytes).\r\n         Response code: File status okay; about to open data connection (150)         Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00         0010       00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8	l à	hecksum: 0xc1c6	[unverified]	/1		
Urgent pointer: 0       >         > [SEQ/ACK analysis] TCP payload (61 bytes)         - File Transfer Protocol (FTP)         • 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response code: File status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20       10 ca 48 8c 08 00 45 00 bf 60 15 e2 64 o0 42 c8 1c e8 26 84 79 50 18 	Г <u>г</u> о	Checksum Status	: Unverified]			
<ul> <li>▷ [SEQ/ACK analysis] TCP payload (61 bytes)</li> <li>✓ File Transfer Protocol (FTP)         <ul> <li>▲ 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>■ 68 07 15 97 33 df bc 20 10 ca 48 8 c0 80 04 500 Mestanse arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>■ 68 07 15 97 33 df bc 20 10 ca 48 8 c0 80 04 500 Mestanse arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>■ 6000 00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8 .eeeeeee.</li></ul></li></ul>	Ū	rgent pointer:	0			
TCP payload (61 bytes)         ▲ File Transfer Protocol (FTP)         ▲ 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response code: File status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8 t	▶ [	SEQ/ACK analysi	s]			
<ul> <li>File Transfer Protocol (FTP)         <ul> <li>I50 Opening BINARY mode data connection for flag (7 bytes).\r\n Response code: File status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>68 07 15 97 33 df bc 20 10 ca 48 8 c0 80 04 50 0 00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8 e c0 a8 .e0.0.</li> <li>b 97 00 15 e2 fa 0d e2 c 81 ce 82 e8 47 95 01 8 t15 0 Opening 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e ta conne ction fo r flag (7 bytes) </li> </ul> </li> <li>Mary mode data connection for r flag (7 bytes) </li> </ul>	T T	CP payload (61	bytes)			
<ul> <li>▲ 150 Opening BINARY mode data connection for flag (7 bytes).\r\n Response code: File status okay; about to open data connection (150) Response arg: Opening BINARY mode data connection for flag (7 bytes).</li> <li>● 000 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8 2b 9f 00 15 e2 fa 0d e2 c 81 ce 82 e8 479 50 18 +15 0 Opening 000 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e 72 60 24 24 94 e4 15 25 92 20 6d 6f 64 65 20 6d fi 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 72 20 56 6c 61 67 20 28 37 20 62 79 74 65 73 29 2e 0d 0a</li> <li>● Response arg (ftp. response arg), 55 字节</li> <li>● 38 Response arg (ftp. response arg), 55 字节</li> </ul>	⊿ File	e Transfer Proto	ocol (FTP)			
Response code: File status okay; about to open data connection (150)         Response arg: Opening BINARY mode data connection for flag (7 bytes).         0000       68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00       h3HE.         0010       00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8       h3HE.         2b 9f 00 15 e2 fa 0d e2 c8 1c e8 2e 84 79 50 18       h	⊿ 1	50 Opening BINA	RY mode data connecti	ion for flag (7 bytes)	.\r\n	
Response arg: Opening BINARY mode data connection for flag (7 bytes).       ▼         0000       68 07 15 97 33 df bc 20       10 ca 48 8c 08 00 45 00       h3.      HE.         0010       00 65 17 de 40 00 30 06       b5 e0 b6 fe d9 8e c0 a8       h3.		Response code:	: File status okay; a	bout to open data con	nection (19	50)
0000       68 07 15 97 33 df bc 20       10 ca 48 8c 08 00 45 00       h3      HE.         0010       00 65 17 de 40 00 30 06       b5 e0 b6 fe d9 8e c0 a8       e.e.@.0.		Response arg:	Opening BINARY mode	data connection for f	lag (7 byte	25).
0000       68 07 15 97 33 df bc 20       10 ca 48 8 c 08 00 45 00       h3					- · ·	
000 65 1 / de 40 00 30 06 b5 e0 b6 fe d3 8e c0 a8 0020 2b 9f 00 15 e2 fa 0d e2 c8 1c e8 2e 84 79 50 18 +	0000	68 07 15 97 33	df bc 20 10 ca 48 8	3c 08 00 45 00 h	3H	Ε.
0020       26 9 f 00 15 e2 f a 00 e2 cs 1c e0 2e 64 79 50 18       +	0010	00 65 17 de 40	00 30 06 b5 e0 b6 f	fe d9 8e c0 a8 .e(		open BINARV 也且没有田
0040       67       20       42       49       42       15       59       20       616       64       65       20       46       1       10       0       10       <	0020	20 97 00 15 62	00 31 35 30 20 4F	12 04 / 9 00 18 +	15 0 Open	
0050       74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f       ta conne ction fo         0050       72 20 66 6c 61 67       20 28 37 20 62 79 74 65 73 29       r flag ( 7 bytes)         0070       2e 0d 0a          ● 3       Response arg (ftp.response.arg), 55 字节	0040	67 20 42 49 49	41 52 59 20 6d 6f 6	54 65 20 64 61 Ø BTI	VARY mode	da
0060 72 20 <u>66 6c 61 67</u> 20 28 37 20 62 79 74 65 73 29 r flag (7 bytes) 2e 0d 0a ● 2 Response arg (ftp.response.arg), 55 字节	0050	74 61 20 63 6f	6e 6e 65 63 74 69 6	5f 6e 20 66 6f ta c	onne ction	fo
0070 2e 0d 0a ● ℤ Response arg (ftp.response.arg), 55 字节	0060	72 20 <mark>66 6c 61</mark>	67 20 28 37 20 62 7	79 74 65 73 29 r <mark>f1</mark>	ig (7 byte	s)
<ul> <li>● ※ Response arg (ftp.response.arg), 55 字节</li> <li>分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.572   配置文件: Default</li> </ul>	0070	2e 0d 0a				
● 🝸 Response arg (ftp.response.arg), 55 字节 月前1993 (100.0%) · 加载时间: 0:0.572    配置文件: Default						
	07	Response and (ftm )	response ang) 55 字带			│
		mapping and (rep. r	contourse and the one of the			II JISH. AROO LARVA. AROO (LOUGH) JURAAAAA UK. BERKUIT. BERKUIT

🖌 traffic.pcapng	
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)	
🗹 🔳 🔬 🐵 😼 🔁 🔍 😓 🚍 🗐 Q. Q. Q. X	
■ 应用显示过滤器 ··· Ctrl-/> 表达式···	+ 应用此过滤器

	分组字节流 ▼	苋乍	🎽 🔲 区分大小与	字付串	▼ flag		<b>登</b> 找	取消	
No.	Time	Source	Destin	nation	Protocol	Length Info			*
	8005 18.140869	180.97.34.1	36 192.3	168.43.159	TLSv1.2	1285 HTTP/1.1 200 OK (application/zip)			
	8006 18.140928	192.168.43.	159 180.9	97.34.136	TCP	54 58146 → 443 [ACK] Seq=1871 Ack=6860982 Win=5364480 Len=0			
	8007 18.141049	192.168.43.	159 180.9	97.34.136	TCP	54 58146 → 443 [ACK] Seq=1871 Ack=6864454 Win=5364480 Len=0			
	8008 18.141108	192.168.43.	159 180.9	97.34.136	TCP	54 58146 → 443 [ACK] Seq=1871 Ack=6866637 Win=5364480 Len=0			
	8009 18.173753	220.181.7.1	90 192.:	168.43.159	TLSv1.2	85 Alert (Level: Warning, Description: Close Notify)			
	8010 18.173753	220.181.7.1	90 192.:	168.43.159	TCP	54 443 → 58137 [FIN, ACK] Seq=749 Ack=2801 Win=20352 Len=0			
	8011 18.173894	192.168.43.	159 220.3	181.7.190	TCP	54 58137 → 443 [ACK] Seg=2801 Ack=750 Win=16640 Len=0			
	8012 18.235276	192.168.43.	159 144.	76.59.84	UDP	42 46327 → 25903 Len=0			
	8013 18.824537	192.168.43.	159 182.3	254.217.142	FTP	62 Request: TYPE I			-
	8014 18.824638	192.168.43.	159 144.	76.59.84	UDP	42 46327 → 25903 Len=0			
	8015 18.882232	182.254.217	.142 192.3	168.43.159	FTP	85 Response: 200 Switching to Binary mode.		_	
	8016 18.882494	192.168.43.	159 182.3	254.217.142	FTP	60 Request: PASV			
	8017 18,931501	182,254,217	.142 192.3	168.43.159	FTP	108 Response: 227 Entering Passive Mode (182,254,217,142,120,115).			=
	8018 18,931738	192,168,43.	159 182.	254,217,142	FTP	69 Request: RETR flag.zip			=.
⊵	Frame 8018: 69 by	ytes on wire (55	2 bits), 69 by	tes capture	d (552 bits)	on interface 0			-
⊳	Ethernet II, Src:	: IntelCor_97:33	:df (68:07:15:	97:33:df),	Dst: bc:20:10	:ca:48:8c (bc:20:10:ca:48:8c)			
₽	Internet Protocol	l Version 4, Sro	: 192.168.43.1	59, Dst: 18	2.254.217.142				
4	Transmission Cont	trol Protocol, S	rc Port: 58106	, Dst Port:	21, Seq: 32,	Ack: 223, Len: 15			
	Source Port: 5	8106							
	Destination Po	ort: 21							
	[Stream index:	34]							=
	[TCP Segment L	.en: 15]							
	Sequence numbe	er: 32 (relat:	ive sequence nu	umber)					
	[Next sequence	number: 47	(relative seque	ence number)	)]				
	Acknowledgment	number: 223	(relative ack	number)					
	0101 = He	ader Length: 20	bytes (5)						
	▷ Flags: 0x018 (	PSH, ACK)							
	Window size va	lue: 20950							
	[Calculated wi	ndow size: 2095	9]						
	Window size s	caling factor:	-1 (unknown)]						
	Checksum: 0x2b	9f [unverified]							
	[Checksum Stat	us: Unverified]							
									Ψ.
00	00 bc 20 10 ca	48 8c 68 07 15	97 33 df 08 00	94500 .	H.h3	.E.			
00	10 00 37 66 59	40 00 40 06 57	93 c0 a8 2b 9f	fb6fe .	7fY@.@. W+	·····································			
00	20 d9 8e e2 fa	00 15 e8 2e 84	87 0d e2 c8 c6	5 50 18 .		.P. 反现或恐怕忌 Indg.zip			
00	30 51 d6 2b 9f	00 00 52 45 54	52 20 66 6c 61	<mark>67</mark> 2e Q	.+RE TR fla	🖷 🛛 应该联想到解题方向·解压后 里面有flag(	古		
00	40 7a 69 70 0d	0a		Z.	ip				
						✓ RETR是卜载 store是上传 PASV是FTP被动	莫式		
							-		
	🍸 Request arg (ftp	).request.arg), 8 字节	5			│ 分组: 17953 · 已显示: 17953 (100.0%) · 加载时间::000.	572 配置文(	牛: Defaul	t€90

### 继续查找后,发现压缩包内容,如下图

📕 traffic.pcapng			
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C)	分析(A) 统计(S) 电话(Y) 无线(W)	) 工具(T) 帮助(H	)
📕 🔳 🔬 🛞 🕌 🔚 🔀 🖻   🍳 👄 👄 🤤	2 T 🕹 📃 🗐 Q Q Q 🎹		
▲ 应用显示过滤器 … 《Ctrl-/>			▶ 📑 🗾 🚽 表达式… 🛛 + 应用此过滤器
分组字节流 ▼	▼ □ 区分大小写 字符串 ▼	flag	
No. Time Source	Destination	Protocol	Length Info
8012 18.235276 192.168.43	.159 144.76.59.84	UDP	42 46327 → 25903 Len=0
8013 18.824537 192.168.43	.159 182.254.217.142	FTP	62 Request: TYPE I
8014 18.824638 192.168.43	.159 144.76.59.84	UDP	42 46327 → 25903 Len=0
8015 18.882232 182.254.21	150 192.168.43.159	FIP	85 Response: 200 Switching to Binary mode.
	102.234.217.142 7 142 102 168 43 150		108 Response: 227 Entening Passive Mode (182 254 217 142 120 115)
8018 18.931738 192.168.43	.159 182.254.217.142	FTP	69 Request: RFTR flag.zip
8019 18.932023 192.168.43	.159 182.254.217.142	ТСР	66 58150 → 30835 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK PERM=1
8020 18.963066 182.254.217	7.142 192.168.43.159	ТСР	66 30835 → 58150 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM 💻
8021 18.963204 192.168.43	.159 182.254.217.142	TCP	54 58150 → 30835 [ACK] Seg=1 Ack=1 Win=5364608 Len=0
8022 19.002634 182.254.217	7.142 192.168.43.159	FTP-DATA	271 FTP Data: 217 bytes
8023 19.003254 182.254.217	7.142 192.168.43.159	ТСР	54 30835 → 58150 [FIN, ACK] Seq=218 Ack=1 Win=29312 Len=0
8024 19.003254 182.254.217	7.142 192.168.43.159	FTP	121 Response: 150 Opening BINARY mode data connection for flag.zip (217 byt
8025 19.003355 192.168.43	.159 182.254.217.142	ТСР	54 58150 → 30835 [ACK] Seq=1 Ack=219 Win=4194048 Len=0
<ul> <li>Ethernet II, Src: bc:20:10:ca:44</li> <li>Internet Protocol Version 4, Src</li> <li>Transmission Control Protocol, 5</li> <li>Source Port: 30835</li> </ul>	8:8c (bc:20:10:ca:48:8c), Ds c: 182.254.217.142, Dst: 192 Src Port: 30835, Dst Port: 5	st: IntelCor_97 2.168.43.159 58150, Seq: 1,	7:33:df (68:07:15:97:33:df) Ack: 1, Len: 217
Destination Port: 5055 Destination Port: 58150 [Stream index: 38] [TCP Segment Len: 217] Sequence number: 1 (relati [Next sequence number: 218 Acknowledgment number: 1 ( 0101 = Header Length: 26 > Flags: 0x018 (PSH, ACK) Window size value: 229 [Calculated window size: 2931	ve sequence number) (relative sequence number) relative ack number) bytes (5) 21	继续查找后,发现压缩包具体内容,应该联想到提取 这个压缩包。 注意FTP-DATA	
Window size scaling factor:           Checksum: 0x5442 [unverified]           [Checksum Status: Unverified]           0050         08 00 00 00 66 c 61 67 2e           0060         87 03 eb 29 41 f0 85 c5 4e           0070         42 79 61 d2 0a 38 9f b7 ab           0080         18 c4 c5 5e ae a0 56 ab 71           0090         4b 67 38 56 73 48 33 000	274 78 74 a2 3c ed 3e c cd 4d 63 1a 10 95 6d c d 8b 72 87 7f fc 3b ld 36 fa 34 56 cb 50  00 00 85 00 00 00 50 K	. <u>flag</u> .txt. () )A N.Mcm 1.8r; ^V. q.6.4V.P W.3%P	可以通过应用显示过滤器过滤想要更看的协议或方法 如想查看ftp和ftp-data协议 可以在过滤器栏输入ftp or ftp-data 回车
00a0         4b         01         02         1f         00         14         00         09         00           00b0         03         57         d8         33         00         00         00         25         00	0 08 00 7d b9 51 4b b6 K 0 00 00 08 00 24 00 00 .W.	}.QK. 3%\$	Ē

🥚 🍸 FTP Data (ftp-data), 217 字节

Window size value: 229

0050 08 00 00 00 66 6c 61 67

0080 18 c4 c5 5e ae a0 56 ab 0090 4b 07 08 b6 03 57 d8 33 00a0 4b 01 02 1f 00 14 00 09

42 79 61 d2 0a 38 9f b7

[Calculated window size: 29312]

[Window size scaling factor: 128] Checksum: 0x5442 [unverified] [Checksum Status: Unverified] •

 0050
 08
 00
 00
 66
 6c
 61
 67
 2e
 74
 78
 74
 a2
 3c
 ed
 3e
 3e
 a
 10
 55
 4e
 cd
 4d
 63
 1a
 10
 95
 6d

 00b0
 03 57 d8 33 00 00 00 25
 00 00 00 08 00 24 00 00

 00c0
 00 00 00 00 00 20 00 00
 00 00 00 00 00 c6 6c 61

00d0 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18

ab c0 8b 72 87 7f fc 3b 71 1d 36 fa 34 56 cb 50 00 00 00 25 00 00 00 50

00 08 00 7d b9 51 4b b6

0070

🚺 tra	ffic.pcapng							
文件(	F) 编辑(E) 视图(V	) 跳转(G) 捕获(C) 分析	f(A) 统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H)				
	I 🖉 🛞 🕌 🖿	🗙 💼 । ९. 🗢 🔿 🕾 👔	े 👃 📃 🗐 🔍 ର୍ ର୍ 🎹					
、应	用显示过滤器 … ‹Ctu	-1-/>						➡️ ▼ 表达式… ↓ + 应用此过滤器
	分组字节流 ▼	[寛窄 ▼][	□区分大小写 字符串 ▼	flag				查找 取消
No.	Time	Source	Destination	Protocol Leng	th Info	0		
	8012 18.235276	192.168.43.159	144.76.59.84	UDP	42 463	327 → 25903 Len=0		
	8013 18.824537	192.168.43.159	182.254.217.142	FTP	62 Req	quest: TYPE I		
	8014 18.824638	192.168.43.159	144.76.59.84	UDP	42 463	327 → 25903 Len=0		
	8015 18.882232	182.254.217.14	2 192.168.43.159	FTP	85 Res	sponse: 200 Switc	hing to Binary	mode.
	8016 18.882494	192.168.43.159	182.254.217.142	FTP	60 Req	quest: PASV		
Г	8017 18.931501	182.254.217.14	2 192.168.43.159	FTP 1	108 Res	sponse: 227 Enter	ing Passive Mod	de (182,254,217,142,120,115).
	8018 18.931738	192.168.43.159	182.254.217.142	FTP	69 Req	quest: RETR flag.	zip	
	8019 18.932023	192.168.43.159	182.254.217.142	TCP	66 581	150 → 30835 [SYN]	Seq=0 Win=6553	35 Len=0 MSS=1460 WS=128 SACK_PERM=1
	8020 18.963066	182.254.217.14	2 192.168.43.159	TCP	66 308	835 → 58150 [SYN,	ACK] Seq=0 Ack	k=1 Win=29200 Len=0 MSS=1400 SACK_PERM 🔤
	8021 18.963204	192.168.43.159	182.254.217.142	TCP	54 581	150 → 30835 [ACK]	Seq=1 Ack=1 Wi	in=5364608 Len=0
	8022 19.002634	182.254.217.14	2 192.168.43.159	FTP-DATA 2	271 570	Data: 217 bytes		
	8023 19.003254	182.254.217.14	2 192.168.43.159	TCP	54	标记/取消标记 分组(M	) Ctrl+M	:k=1 Win=29312 Len=0
	8024 19.003254	182.254.217.14	2 192.168.43.159	FTP 1	21	忽略/取消忽略 分组(I)	Ctrl+D	lata connection for flag.zip (217 byt… 📃
	8025 19.003355	192.168.43.159	182.254.217.142	тср	54	设置/取消设置 时间参考	≝ Ctrl+T	Vin=4194048 Len=0
N F.	0022. 271	huter on using (2169	hits) 271 bytes conture	d (2168 hits) on	int	时间平移	Ctrl+Shift+T	
D Et	thernet II. Src	: bc:20:10:ca:48:8c	(bc:20:10:ca:48:8c), Dst	: IntelCor 97:33:	df	分组注释	Ctrl+Alt+C	
⊳ Ir	nternet Protoco	l Version 4, Src: 1	82.254.217.142, Dst: 192.	168.43.159		编辑解析的名称		-
⊿ Tr	ansmission Con	trol Protocol, Src	Port: 30835, Dst Port: 58	150, Seq: 1, Ack:	1,			_
	Source Port: 3	0835				作为过滤器应用	•	
	Destination Po	ort: 58150				准备过滤器	+	
	[Stream index:	38]				对话过滤器	•	
	[TCP Segment L	.en: 217]				对话着色	•	
	Sequence numbe	er: 1 (relative s	sequence number)			SCTP	•	
	[Next sequence	e number: 218 (re	elative sequence number)]			2 追踪流	•	
	Acknowledgment	number: 1 (rela	ative ack number)			x00010		
	0101 = He	ader Length: 20 byt	tes (5)			复制	•	
⊳	Flags: 0x018 (	(PSH, ACK)				机沙若洗雨		SSL 流

协议首选项

解码为(A)...

在新窗口显示分组(W)

۲

HTTP 流

|| 分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0(0.572|| 配置文件/ Defaul(

	f pro n.i. (ci	) 017 全世			(148- 1705) · 고티구· 1705) (100 0W) · · ho起明句(100 0W) · · · ho起明句(100 0W)	卑☆件・┓.ኗ]↓
++(+)			(約14.00) 中洋00 工行040	工具の 邦助(4)		
×1++(				工具(1) 邗助(1		
	L 🙂 順 💷		્રાહ્યવ્યા			
te	p.stream eq 38					
	分组字节流 ▼	□ 区	3分大小写 字符串 🔻	flag	查找 取消	
No.	Time	Source	Destination	Protocol	Length Info	
	8019 18.932023	192.168.43.159	182.254.217.142	TCP	66 58150 → 30835 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1	
	8020 18.963066	182.254.217.142	192.168.43.159	TCP	66 30835 → 58150 [SYN, ALK] Seq=0 ACK=1 Win=29200 Len=0 MSS=1400 SALK_PERM=1 WS=	
_	8021 18.963204	192.168.43.159	182.254.217.142		54 58150 → 30835 [ALK] SEq=1 ACK=1 W1n=5364608 Len=0	
	8022 19.002034	102.254.217.142	192.100.43.159	FTP-DATA	2/1 FTP Data: 21/ bytes	
	8025 19.005254	102.234.217.142	182 254 217 142	TCP	54 58150 - 30835 [ACK] Seq-1 Ack-210 Win-29512 Len-0	
	8026 19 003778	192.108.43.159	182.254.217.142	ТСР	$54 58150 \rightarrow 30835$ [ETN ACK] Seq=1 Ack=219 Win=4194048 Len=0	
L	8028 19.050593	182.254.217.142	192,168,43,159	TCP	54 30835 → 58150 [ACK] Seg=219 Ack=2 Win=29312 Len=0	📸 × 🖸 ×
					· · · · · · · · · · · · · · · · · · ·	
				🧧 Wireshark 🤅	追踪 TCP 流 (tcp.stream eq 38) · traffic	
				РК	}.QKW.3%flag.txt.<.>)AN.McmBya.	
				8r	.;^V.q.6.4V.PKW.3%PK	.flag.txt
	Source Port:	30835		1	这是压缩包内容,可以看到里面	角flag.
	Destination P	ort: 58150			tvt	
	[Stream index	: 38]				
	[TCP Segment	Len: 217]				
	Sequence numb	er: 1 (relative sequ	uence number)			
	[Next sequenc	e number: 218 (rela	tive sequence number)	]		
	Acknowledgmen	t number: 1 (relativ	ve ack number)			
	0101 = H	eader Length: 20 bytes	(5)			
ľ	Hindow size y	(FSH, ACK)				
	[Calculated w	indow size: 293121				
	[Window size	scaling factor: 128]				
	Checksum: 0x5	442 [unverified]				
	[Checksum Sta	tus: Unverified]				
	Urgent pointe	r: 0				
⊳	[SEQ/ACK anal	ysis]				

.W.3...% ....\$.. .....fla g.txt..

0030 00 e5 54 42 00 00 50 4b 03 04 14 00 09 00 08 00

TCP payload (217 bytes) FTP Data (217 bytes data)

0040 0050	7d b9 51 4b b6 03 57 d8 33 00 0 08 00 00 00 66 6c 61 67 2e 74 7	00 00 25 00 00 00 }.QK		
0060 0070	87 03 eb 29 41 f0 85 c5 4e cd 4 42 79 61 d2 0a 38 9f b7 ab c0 8	4d 63 1a 10 95 6d) 8b 72 87 7f fc 3b Bva.	<i>4 高产用 分類、2 服券群 分類、4 turn(z).</i> Entire conversation (217 bytes) ▼	<b></b>
0080 0090	18 c4 c5 5e ae a0 56 ab 71 1d 3 4b 07 08 b6 03 57 d8 33 00 00 0	36 fa 34 56 cb 50^ 00 25 00 00 00 50 K	查找: Charage C	H)
00a0 00b0	4b 01 02 1f 00 14 00 09 00 08 0 03 57 d8 33 00 00 00 25 00 00 0	00 7d b9 51 4b b6 K	渡掉此流 打 Hax 转储 UTF-8 返回 Close Help	
• 2	FTP Data (ftp-data), 217 字节		分组: 17953 ・ 已显示: 8 (0.0% - 原始数据 0:0.356   配括文件: "befault **** incompiles	990

PK	}.QKW.3 r;^V.q.6.4 %.FZG)QX	.%flag.txt.<.>)AN.Mc V.PKW.3%PK G)QXG.PKZi	mBya. }.QKW.3%\$	flag.txt	□linux □在线靶场 保存草稿 & 票
	📕 Wireshark · Save Stre	am Content As			
				<ul> <li>✓ 4) 搜索 桌面</li> </ul>	٩
	组织 ▼ 新建文件共	Ę			₩= <b>▼</b> (2)
	☆ 收藏夹	<b>库</b> 系统文件夹	Administrator 系统文件夹		
	<ul> <li>三 桌面</li> <li>〇 库</li> <li>〇 岡 本</li> </ul>	■ <b>计算机</b> 系统文件夹	网络 系统文件夹		
	■ 图片 ■ 文档	360驱动大师 快速方式 1.08 KB	Firefox 快捷方式 928 字节		
	<ul> <li>┛ 音乐</li> <li>▲ Administrator</li> <li>▲ 计算机</li> </ul>	<ul><li> 勝讯会议 </li><li> 快速方式 </li><li> 1.09 KB </li></ul>	<b>mp3</b> 文件夹		
	🂒 WIN7 (C:) ┌── 软件 (D:) ┌── WIN7 <u>(E:)</u>	新建文件夹文件夹	1.txt           文本文档           206 字节		
4 <i>客片場</i> . Entire 查找:	文件名 <mark>(N): 80</mark> 保存类型(T):	22.zipl 保存为zip压缩包,	名字为了好记,选择	了该流量包num	
	▲ 隐藏文件夹			保存(S)	<b>取消</b> 50++++++++++++++++++++++++++++++++++++

▲ Wireshark · 追踪 TCP 流 (tcp.stream eq 38) · traffic	
504b03041400090008007db9514bb60357d833000000250000 31a10956d427961d20a389fb7abc08b72877ffc3b18c4c55ea 01021f001400090008007db9514bb60357d833000000250000 020000000000001001800d125cd465a47d3012951a6185847d 000000	0008000000666c61672e747874a23ced3e8703eb2941f085c54ecd4d6 ea056ab711d36fa3456cb504b0708b60357d83300000025000000504b 000800240000000000000000000000000000666c61672e7478740a0 3012951a6185847d301504b050600000000000000000000000000000000
	点击返回,继续查找 看还有没有flag关键字的流量包

Entire conversation (217 bytes)	显示和保存数据为 [原始数据 🔻		流 38 🚖
查找:			查找下一个 00)
		jo (	Close Help

	traffic.pcapng				
<u>غ</u>	(件(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H)	
	( 🔳 🥖 🟟 🛄 🛤 🖪	1 6 9 9 9 5 7 1			
					🔲 ໄມນັບ ເອັດແມ່ນ 👘
L	应用显示辺滤器 *** 《 tr.				
	分组字节流 ▼	閲宿   🔤 🖸 🖾 🖄	大小与 字符串 ▼	flag	<u> 査技</u> 取消
No	. Time	Source	Destination	Protocol	Length Info
	8022 19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271 FTP Data: 217 bytes
	8023 19.003254	182.254.217.142	192.168.43.159	ТСР	54 30835 → 58150 [FIN, ACK] Seq=218 Ack=1 Win=29312 Len=0
	8024 19.003254	182.254.217.142	192.168.43.159	FIP	121 Response: 150 Opening BINARY mode data connection for flag.zip (21/ byt
	8025 19.003355	192.168.43.159	182.254.217.142	TCP	54 58150 → 30835 [ACK] Seq=1 ACK=219 Win=4194048 Len=0
	8025 19.005778	192.100.43.159	102.254.217.142	TCP	54 56150 → 50655 [FIN, ACK] Seq=1 ACK=219 Win=4194046 Len=0
	0027 19.045459 9039 10 050505	192.100.45.159	102.204.217.142	TCP	54 56100 $\rightarrow$ 21 [ACK] Seq=47 ACK=290 Win=20955 Len=0
	8020 19.050595	102.234.217.142	192.100.43.139	ETD	78 Response: 226 Inconfer complete
	8030 10 002007	102.234.217.142	192.100.45.159		54 58106 -> 21 [ACK] Sog-47 Ack-314 Win-20055 Lon-0
	8031 19 343730	192.168.43.159	144 76 59 84	LIDP	42 46327 → 25903 Len=0
	8032 19 828813	192.168 //3 159	180 97 33 108	тср	$42 40527 \rightarrow 103$ [RST ACK] Sec=2 Ack=1 Win=0 Len=0
	8033 19 828860	192.168 43 159	144 76 59 84	UDP	$42 \ 46327 \rightarrow 25903 \ \text{Len=0}$
	8034 19 830626	192 168 43 159	180 97 33 108	тср	$5458027 \rightarrow 443$ [RST ACK] Seg=2 Ack=1 Win=0 Len=0
	8035 19.832577	192.168.43.159	180.97.33.108	TCP	$54 58085 \rightarrow 443 [RST, ACK] Seg=2 Ack=1 Win=0 Len=0$
4	<pre>[TCP Segment L Sequence numbe [Next sequence Acknowledgment 0101 = He &gt; Flags: 0x018 ( Window size va [Calculated wi [Window size s Checksum: 0xf6 [Checksum Stat: Urgent pointer &gt; [SEQ/ACK analy TCP payload (6 File Transfer Pro- 4 150 Opening BI Response coo Decement to the second second second Response cool Decement to the second second second second second Response cool Decement to the second second</pre>	en: 67] r: 223 (relative sec number: 290 (relati number: 47 (relati ader Length: 20 bytes ( PSH, ACK) lue: 229 ndow size: 229] caling factor: -1 (unkr dd [unverified] us: Unverified] us: Unverified] : 0 sis] 7 bytes) tocol (FTP) NARY mode data connecti le: File status okay; ad	quence number) ive sequence number)] /e ack number) (5) nown)] ion for flag.zip (217 bout to open data con	bytes).\r\n nection (150)	
	000 60 07 45 07 1	-	00.00.45.00	2 11 5	
0 0 0 0 0 0	000         68         07         15         97           010         00         65         17         62           02         2b         9f         00         17         62           030         00         e5         f6         dd         67         24         24         95           040         67         20         42         49         56         64         64         67         20         42         49         56         64         66         72         20         42         49         56         66         72         20         20         65         63         66         72         20         63         66         72         20         63         66         72         20         64         63         74         65         77         62         79         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74         65         74<	33 df bc 20       10 ca 48 &         40 00 30 06       b5 d6 b6 f         e2 fa 0d e2       c8 c6 e8 2         00 00 31 35       30 20 4f 7         4e 41 52 59 20 6d 6f 6       66 66 5         61 67 2e 7a 69 70 20 2         73 29 2e 0d 0a	ic 08 00 45 00         h           Fe d9 8e c0 a8         .k           le 84 96 50 18         +           70 65 6e 69 6e            if 6e 20 66 6f         g B1           if 6e 20 66 6f         ta c           if 8 32 31 37 20         r           byte	3HE. @.0P. P	只是记录以二进制模式打开 压缩包。这个没用,继续查找
	🔪 n (c)	\ a, +++			



|| 分组: 17953 · 戸泉示: 17953 (100.0%) · 加鐵时间: 0:0.308|| 歐害文件: Default

traffic.pcapng 文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H) 🚄 🔳 🖉 💿 📙 🛅 🕱 💼 I 9. 🗢 🗢 🕾 🗿 💆 🚍 🗨 9. 9. 9. 9. ▶ 应用显示过滤器 … 🔜 🔹 表达式…… 🛛 🕇 应用此过滤器 字符串 ▼ flag 査找 取消 Time Source Destination Protocol Length Info No 182.254.217.142 8136 43.183124 192.168.43.159 FTP 60 Request: PASV 8137 43.224221 182.254.217.142 192.168.43.159 107 Response: 227 Entering Passive Mode (182,254,217,142,31,103). FTP 8138 43.224505 192.168.43.159 182.254.217.142 FTP 69 Request: RETR flag.zip 8139 43.224834 192.168.43.159 182.254.217.142 TCP 66 58153 → 8039 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK\_PERM=1 66 8039 → 58153 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK\_PERM= 8140 43.271926 182.254.217.142 192.168.43.159 TCP 54 58153 → 8039 [ACK] Seq=1 Ack=1 Win=5364608 Len=0 8141 43.272009 192.168.43.159 182.254.217.142 TCP 8142 43.303281 182.254.217.142 192.168.43.159 FTP-DATA 271 FTP Data: 217 bytes 8143 43.303965 182.254.217.142 192.168.43.159 TCP 54 8039 → 58153 [FIN, ACK] Seq=218 Ack=1 Win=29312 Len=0 8144 43.303966 182.254.217.142 192.168.43.159 121 Response: 150 Opening BINARY mode data connection for flag.zip (217 byt... FTP 8145 43 304060 192,168,43,159 182.254.217.142 TCP 54 58153 → 8039 [ACK] Seq=1 Ack=219 Win=4194048 Len=0 8146 43.304374 192.168.43.159 182.254.217.142 TCP 54 58153 → 8039 [FIN, ACK] Seq=1 Ack=219 Win=4194048 Len=0 8147 43, 343806 182.254.217.142 192.168.43.159 TCP 54 8039 → 58153 [ACK] Seq=219 Ack=2 Win=29312 Len=0 8148 43, 344706 182.254.217.142 192.168.43.159 FTP 78 Response: 226 Transfer complete. 8149 43, 344750 192.168.43.159 182.254.217.142 TCP 54 58106 → 21 [ACK] Sea=101 Ack=658 Win=20954 Len=0 8150 44.760513 71 Request: CWD /mvdata/gav 192.168.43.159 182.254.217.142 FTP Frame 8138: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0 Ethernet II, Src: IntelCor\_97:33:df (68:07:15:97:33:df), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c) Internet Protocol Version 4, Src: 192,168,43,159, Dst: 182,254,217,142 Iransmission Control Protocol, Src Port: 58106, Dst Port: 21, Seq: 86, Ack: 567, Len: 15 Source Port: 58106 Destination Port: 21 [Stream index: 34] [TCP Segment Len: 15] Sequence number: 86 (relative sequence number) [Next sequence number: 101 (relative sequence number)] Acknowledgment number: 567 (relative ack number) 0101 .... = Header Length: 20 bytes (5) 又找到一个flag.zip Flags: 0x018 (PSH, ACK) Window size value: 67 既可以像上面那个flag.zip那样,继续查找flag.zip的具体内容,然后提取出来 [Calculated window size: 67] [Window size scaling factor: -1 (unknown)]该压缩包。也可以直接在8138上追踪流,本质是一样的。 Checksum: 0x7ba4 [unverified] [Checksum Status: Unverified] bc 20 10 ca 48 8c 68 07 15 97 33 df 08 00 45 00 . ..H.h. ..3...E. 0010 00 37 66 72 40 00 40 06 57 7a c0 a8 2b 9f b6 fe .7fr@.@. Wz..+. 
 0010
 00 37
 66
 72
 40
 00
 40
 65
 77
 a
 c0
 a
 20
 a
 20
 a
 20
 a
 20
 a
 20
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 a
 ....P. . . . . . . .C{...RE TR flag. 0030 zip.. 0040 7a 69 70 0d 0a

🔴 🍸 Request arg (ftp.request.arg), 8 字节

│ 分组: 17953 · 已显示: 17953 (100.0%) · 加载时间:/0:0:277 │ 配置文件:/Defaul€))

📕 tra	affic.pcapng							_ <b>_</b> ×
文件	(F) 编辑(E) 视图(V	/) 跳转(G) 捕获(C) 分析(	(A) 统计(S) 电话(Y) 无线(\	M) 工具(T) 帮助(H)	)			
		🗙 🖸 🤇 🗢 👄 🕾 👔	4 🗐 🗐 🔍 Q 🍭 🎚					
	用显示过滤器 … 《Ct	r1-/>				<b></b>	▼ 表达式…   +	▶ 应用此过滤器
	分组字节流 ▼	宽窄 ▼ 🔳	区分大小写 字符串 ·	• flag			查找	取消
No.	Time	Source	Destination	Protocol	Length Info			
	8134 43.138928	192.168.43.159	182.254.217.142	FTP	62 Request: TYPE I			
	8135 43.182862	182.254.217.142	192.168.43.159	FTP	85 Response: 200 Switching to Binary	mode.		
	8136 43.183124	192.168.43.159	182.254.217.142	FTP	60 Request: PASV			
	8137 43.224221	182.254.217.142	192.168.43.159	FTP	107 Response: 227 Entering Passive Mo	de (182,254,217,142,	31,103).	
	8138 43.224505	192.168.43.159	182.254.217.142	FTP	69 Request: RETR flag.zip	标记/取消标记 会组(M)	Ctrl+M	
	8139 43.224834	192.168.43.159	182.254.217.142	TCP	66 58153 → 8039 [SYN] Seq=0 Win=65	1000/201日のに 33日(191)	Carl+IVI	=1
	8140 43.271926	182.254.217.142	192.168.43.159	TCP	66 8039 → 58153 [SYN, ACK] Seq=0 A		Cul+D	PERM=
	8141 43.272009	192.168.43.159	182.254.217.142	TCP	54 58153 → 8039 [ACK] Seq=1 Ack=1	以直/耿肩以直 则问参考	Ctri+i	
	8142 43.303281	182.254.217.142	192.168.43.159	FTP-DATA	271 FTP Data: 217 bytes	时间平移	Ctrl+Shift+I	
	8143 43.303965	182.254.217.142	192.168.43.159	ТСР	54 8039 → 58153 [FIN, ACK] Seq=218	分组汪释	Ctrl+Alt+C	
	8144 43.303966	182.254.217.142	192.168.43.159	FTP	121 Response: 150 Opening BINARY mo	编辑解析的名称		.7 byt
	8145 43.304060	192.168.43.159	182.254.217.142	TCP	54 58153 → 8039 [ACK] Seq=1 Ack=21			
	8146 43.304374	192.168.43.159	182.254.217.142	TCP	54 58153 → 8039 [FIN, ACK] Seq=1 A	作为过滤器应用	•	
	8147 43.343806	182.254.217.142	192.168.43.159	TCP	54 8039 → 58153 [ACK] Seq=219 ACK=	准备过滤器	•	-
	0140 45.544700	107.734.717.147	197.100.43.139	FIP	To Response: ZZO Transfer complete	对话过滤器	•	
	thornot II Sno	y IntolCon 97:33:df	(69.07.15.07.22.44) r	(552 DILS) ON	142.9c (bc.20.10.co.42.9c)	对话着色	•	l â
	ternet II, Src	Vension 4 Spc: 19	2 168 /3 159 Det+ 183	) 254 217 142	.40.00 (00.20.10.02.40.00)	SCTP	•	
A T	ransmission Con	trol Protocol Src P	ort: 58106 Dst Port:	21 Sea: 86 Ac	k: 567 len: 15	追踪流	•	TCP 流
	Source Port:	58106	010. 00100, 000 1010.	21, 5cq. 00, A	k. 507, Een. 15	包制	•	UDP 流
	Destination P	ort: 21				200		SSL 流
	[Stream index	: 341				协议首选项	•	HTTP 流
	TCP Segment	Len: 15				解码为(A)	L	
	Sequence numb	er: 86 (relative s	sequence number)			在新窗口显示分组(W)		
	[Next sequence	e number: 101 (rel	lative sequence number	)]				·
	Acknowledgmen	t number: 567 (rel	lative ack number)		<b>1</b>			
	0101 = He	eader Length: 20 byte	es (5)	注意	<u>×</u> 里			
Þ	Flags: 0x018	(PSH, ACK)						
	Window size v	alue: 67						
	[Calculated w	indow size: 67]						
	[Window size :	scaling factor: -1 (u	unknown)]					
	Checksum: 0x7	ba4 [unverified]						

1	[Checksum Status: Unverified]																
0000	bc	20	10	са	48	8c	68	07	15	97	33	df	08	00	45	00	H.h3E.
0010	00	37	66	72	40	00	40	06	57	7a	с0	a8	2b	9f	b6	fe	.7fr@.@. Wz+
0020	d9	8e	e2	fa	00	15	e8	2e	84	bd	0d	e2	са	1e	50	18	P.
0030	00	43	7b	a4	00	00	52	45	54	52	20	66	<mark>6</mark> c	61	67	2e	.C{RE TR flag.
0040	7a	69	70	Ød	0a												zip

🔴 🍸 Stream index (tcp. stream)

|| 分组: 17953 • 已显示: 17953 (100.0%) • 加载时间: 0.0.278 || 配置文件: Default

-

#### 点击流的向上按钮

	traffic.pcapng								
文	件(F) 编辑(E) 视图(V	) 跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H	{)				
	🔲 🖉 💿 🚹 🛅	🞗 🔂   ९ 👄 👄 🕾 🕢	🚛 🗐 0, 0, 0, 💷						
	tcp.stream eq 44						▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	式 + 应用此讨滤器	
	分组字节流 ▼	席寝 →   □ 区4	分大小写 「字符串 ▼	flag				李彬 取消	
No	Tino	Sauraa	Destination	Protocol	Longth Info				
10.	8139 43,224834	192,168,43,159	182.254.217.142	TCP	66 58153 → 8039 [	SYN1 Sea=0 Win=65535	len=0 MSS=1460 WS=128 SAG	CK PFRM=1	
	8140 43.271926	182.254.217.142	192.168.43.159	TCP	66 8039 → 58153 [	SYN, ACK] Seq=0 Ack=	1 Win=29200 Len=0 MSS=1400	0 SACK PERM=1 WS=1	
	8141 43.272009	192.168.43.159	182.254.217.142	TCP	54 58153 → 8039 [	ACK] Seq=1 Ack=1 Wir	=5364608 Len=0	_	
	8142 43.303281	182.254.217.142	192.168.43.159	FTP-DATA	271 FTP Data: 217	bytes			
	8143 43.303965	182.254.217.142	192.168.43.159	TCP	54 8039 → 58153 [	[FIN, ACK] Seq=218 Ad	k=1 Win=29312 Len=0		
	8145 43.304060	192.168.43.159	182.254.217.142	TCP	54 58153 → 8039 [	ACK] Seq=1 Ack=219 W	lin=4194048 Len=0		
	8146 43.304374	192.168.43.159	182.254.217.142	ТСР	54 58153 → 8039 [	FIN, ACK] Seq=1 Ack=	219 Win=4194048 Len=0		
	8147 43.343806	182.254.217.142	192.168.43.159	T 📕 Wires	hark · 追踪 TCP 流 (tcp.stream e	eq 44) · traffic	Re-Distance -		
				PK	D.QKNCJ.	flag.txtA	X>,bDJh9.{.grn0	SG.`.aNb5!.L.	
				6x!.d	IL.QPK	D.QKNCJ.	\$flag.t	txt	
					WG	WGPK	21		
E	Enamo 8142, 271	hytos on wino (2169 bit	-c) 271 bytes contum	ad (2)					
	Ethennet II Snc	· bc·20·10·cə·48·8c (bc		- Tn					
Þ	Internet Protoco	1 Version 4. Src: 182.2	254.217.142. Dst: 192	168.					
	Transmission Con	trol Protocol. Src Port	: 8039. Dst Port: 58	153.					
	Source Port: 8	039		,					
	Destination Po	ort: 58153							
	[Stream index:	44]							
	[TCP Segment L	.en: 217]	_						
	Sequence numbe	er: 1 (relative sequ	ence number)						
	[Next sequence	number: 218 (relat	ive sequence number)						
	Acknowledgment	number: 1 (relativ	e ack number)						
	0101 = He	ader Length: 20 bytes	(5)						
	Flags: 0x018 (	PSH, ACK)							
	Window size va	lue: 229							
	[Calculated wi	.ndow size: 29312]							
	[Window size s	caling factor: 126]							
	Checksum Stat	us: Unverified]							
		-2 20 22 -0 04 24 29 7	04 H4 C- E0 19						
0	020 20 9T 1T 67	00 00 50 Ab 03 0A 1A 1	24 04 03 50 10 + 00 09 00 08 00 &	·)#- PK 4-客户端	分组, 2 服务器 分组, 4 turn(s).				
0	040 44 b9 51 4b	ca 2e 96 4e 43 00 00	00 4a 00 00 00 D.O.	N Entire	conversation (217 bytes)	•	显示和保存数据为 ASCII -		流 44 🌒
0	050 08 00 00 00	66 6c 61 67 2e 74 78	74 1d c1 41 0e	flag ##	/		ASCII		
0	80 20 0c 04	c0 bb 89 7f 58 3e e0	9f b0 2c 62 44	道孩:			EBCDIC	2	宣孩下一个(31)
0	070 4a 68 39 f0	7b 13 67 72 8d 17 6e	43 53 47 e1 60 Jh9.	{.gr			- 悲掉此流 打 Hex 转储 - UTF-8	as… 返回 C1	ose Help
0	080 08 61 df de	bo 4e 62 e9 84 15 9d	35 21 ab 4c 83 .a	.ND.			UTF-16 YAMI	/	.1
0	0a0 4b 01 02 1f		44 b9 51 4b ca K	D OK			原始数据		有序列表
								-	无序列表 💠
	) 🌌 Stream index (to	rp. stream)				分组: 17953 ・ 日	显示: 8 (0.0%) ・ 加載时间: 0:0.3	51   配置文件 Default	dn.net/mutou990

traffic.pcapng										
文件(F) 编辑(E) 视图(V)	) 跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T)	帮助(H)						
🚄 🔳 🖉 💿 📕 🛅 🕽	🗴 🖸 🍳 🗢 🗢 🗟 🗿	🗐 🔍 २, २, 🎟								
📕 tcp. stream eg 55								X 🔿 🔹	表达式 + 应用此过滤器	
分组字节流 ▼	寛窄   ▼   区分	→大小写 字符串 ▼	flag						査技 取消	
No. Time	Source	Destination	Proto	col Length	h Info					
8971 125.362905	5 192.168.43.159	182.254.217.142	TCP	6	6 58163 →	50090 [SYN] S	Seq=0 Win=65535 Le	n=0 MSS=1460 WS=1	28 SACK_PERM=1	
8972 125.390918	3 182.254.217.142	192.168.43.159	TCP	6	6 60090 →	58163 [SYN, A	ACK] Seq=0 Ack=1 W	lin=29200 Len=0 MS	S=1400 SACK_PERM=1 WS=	
8973 125.391018	3 192.168.43.159	182.254.217.142	TCP	5	4 58163 →	50090 [ACK] S	Seq=1 Ack=1 Win=53	64608 Len=0		
8974 125.426542	2 182.254.217.142	192.168.43.159	FTP-	DATA 50	2 FTP Data	: 448 bytes				
8975 125.427021	l 182.254.217.142	192.168.43.159	TCP	5	4 60090 →	58163 [FIN, A	ACK] Seq=449 Ack=1	. Win=29312 Len=0		
8977 125.427131	l 192.168.43.159	182.254.217.142	TCP	5	4 58163 →	50090 [ACK] 9	Seq=1 Ack=450 Win=	4193792 Len=0		
8978 125.427242	2 192.168.43.159	182.254.217.142	TCP	5	4 58163 →	50090 [FIN, A	ACK] Seq=1 Ack=450	Win=4193792 Len=	3	
8980 125.480665	5 182.254.217.142	192.168.43.159	Tq	Wireshark · 這路	宗 TCP 流 (tcp.s	stream eq 55) · tra	affic	a, ani usua a	and Mondally Land	
8981 125.480715	5 192.168.43.159	182.254.217.142	TO							
- 8982 125.501354	182.254.217.142	192.168.43.159	10	drwxrwxr-x	2 500	500	4096 Sep 17 2	3:44 docker		
				-rr	1 33	33	/ Aug 16 1	8:51 +1ag		
				-rwxr-xr-x	1 33	33	217 UCT 18 0	1:10 +1ag.Z1p		
					1 33	33	26727 Oct 18 0	1:11 kov log		
				deuxeuxeux	2.0	0	16384 Oct 27	2016 lost+found		
			-	drwxrwxrwx	30	õ	4096 Nov 29	2016 test		
▷ Frame 8974: 502 H	bytes on wire (4016 bit	s), 502 bytes capture	d (4							
Ethernet II, Src	: bc:20:10:ca:48:8c (bc	::20:10:ca:48:8c), Dst	: In							
Internet Protocol	l Version 4, Src: 182.2	54.217.142, Dst: 192.	168.							
Transmission Cont	trol Protocol, Src Port	: 60090, Dst Port: 58	163,							
Source Port: 6	0090									
Destination Po	ort: 58163									
[Stream index:	55]									
[TCP Segment L	.en: 448]									
Sequence numbe	er: 1 (relative seque	ence number)		\=						
[Next sequence	e number: 449 (relat:	ive sequence number)]		返回。	,继续的	查找后,,	又反现FIP日	求珀씸信思。	<b>没用,继续</b> 宜找	
Acknowledgment	number: 1 (relative	e ack number)								
0101 = He	ader Length: 20 bytes	(5)								
Flags: 0x018 (	PSH, ACK)									
101 - Jan - Jan	1									

( [ [ ]	undow sıze value: 229 Calculated window size: 29312] Window size scaling factor: 128] Thecksum: 0x2ba2 [unverified] ""				
0020 0030 0040 0050 0060 0070 0080	2b         9f         ea         ba         a3         11         59         82         06         f5         60         ab         04         50         18           00         e5         2b         a2         00         06         47         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         77         78         72         72         72         20 </td <td>+3.Y +dr 2 50 00 Sep 17 ckerr 1 33</td> <td>5 <u>第十第</u> 分類。2 <u>第条</u>基 分型。4 turn(y). Entire conversation (448 bytes) 查找:</td> <td>▼ 显示和保存数据为 ASCII ▼ 透掉此流 打印 Save as*** 返回</td> <td>流 55 テ 查找下一个 (M) Close Help</td>	+3.Y +dr 2 50 00 Sep 17 ckerr 1 33	5 <u>第十第</u> 分類。2 <u>第条</u> 基 分型。4 turn(y). Entire conversation (448 bytes) 查找:	▼ 显示和保存数据为 ASCII ▼ 透掉此流 打印 Save as*** 返回	流 55 テ 查找下一个 (M) Close Help
0090 00a0	33 20 20 20 20 20 20 20 20 20 20 20 20 20	3 Aug 16	/ 18:51 fl		csdn.net/mutou990

## 注意这里有一个key.log文件

📕 tra	ffic.pcapng					
文件(	F) 编辑(E) 视图(V)	跳转(G) 捕获(C)	分析(A) 统计(S)	电话(Y) 无线(W)	工具(T) 帮助(H)	
	1 🖉 🛞 🚹 🗖	र 🕞 🤉 👄 🔿 🕾	T & I 🗐	0,0,0,1		
		1-/>				
( Value /	分组字节流 ▼	宽窄	- 🔲 区分大小写	字符串 ▼	flag	
No.	Time	Source	Destir	ation	Protocol	Length Info
	7415 17.441586	192.168.43.1	.59 182.2	254.217.142	FTP	65 Request: RETR flag
	7416 17.441941	192.168.43.1	.59 182.2	254.217.142	TCP	66 58149 → 12088 [Sim] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
	7417 17.482047	182.254.217.	142 192.3	168.43.159	TCP	66 12088 → 58149 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM…
	7418 17.482159	192.168.43.1	.59 182.2	254.217.142	TCP	54 58149 → 12088 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
	7419 17.522353	182.254.217.	142 192.3	168.43.159	FTP	115 Response: 150 Opening BINARY mode data connection for flag (7 bytes).
	7420 17.522353	182.254.217.	142 192.3	168.43.159	FTP-DATA	61 FTP Data: 7 bytes
	7421 17.522353	182.254.217.	142 192.3	168.43.159	TCP	54 12088 → 58149 [FIN, ACK] Seq=8 Ack=1 Win=29312 Len=0
	7422 17.522433	192.168.43.1	.59 182.2	254.217.142	TCP	54 58149 → 12088 [ACK] Seq=1 Ack=9 Win=4194176 Len=0
	7423 17.522795	192.168.43.1	.59 182.2	254.217.142	TCP	54 58149 → 12088 [FIN, ACK] Seq=1 Ack=9 Win=4194176 Len=0
	7424 17.562590	192.168.43.1	.59 182.2	254.217.142	TCP	54 58106 → 21 [ACK] Seq=18 Ack=114 Win=20950 Len=0
	7425 17.570091	182.254.217.	142 192.3	168.43.159	FTP	78 Response: 226 Transfer complete.
	7426 17.570091	182.254.217.	142 192.3	168.43.159	TCP	54 12088 → 58149 [ACK] Seq=9 Ack=2 Win=29312 Len=0
	7427 17.611002	192.168.43.1	.59 182.2	254.217.142	TCP	54 58106 → 21 [ACK] Seq=18 Ack=138 Win=20950 Len=0
	7428 17.643602	180.97.34.13	6 192.3	168.43.159	TCP	1454 443 → 58146 [ACK] Seq=6307990 Ack=1871 Win=18176 Len=1400 [TCP segment …
<u> </u>	7429 17.647076	180.97.34.13	6 <u>192.</u> ′	168.43.159	TCP	1454 443 → 58146 [ACK] Sea=6309390 Ack=1871 Win=18176 Len=1400 [TCP segment
	Sequence numbe	r: 7 (relativ	e sequence num	ıber)		A
	[Next sequence	number: 18 (	relative seque	ence number)]	\r	
	Acknowledgment	number: 53 (	relative ack r	number)	i i	
	0101 = He	ader Length: 20	bytes (5)		Į.	
⊳	Flags: 0x018 (	PSH, ACK)				
	Window size va	lue: 20950			1_	
	[Calculated wi	ndow size: 20950				
	[Window size s	caling factor: -	1 (unknown)]		· · · · · ·	
	Checksum: 0x16	fe [unverified]				
	[Checksum Stat	us: Unverified]				
	Urgent pointer	: 0			~ ~	
⊳	[SEQ/ACK analy	sis]			<b>–</b>	
	TCP payload (1	1 bytes)				
4 F1	Le Transfer Pro	tocol (FIP)				
1	KEIK +lag\r\n					
	Request comm	and: KEIK				
	Request arg:	+lag				
0000	ha 20 10 an	49 9- 69 07 45		45.00	U. L. D. E.	
0000	DC 20 10 Ca	40 00 00 07 15	27 33 07 08 06 20 c0 28 25 04	14500	.п.пэЕ.	
0010	d9 8e e2 fa	40 00 40 00 37 00 15 e8 2e 84	6e 0d e2 c8 1c	- 50 18	-@.@.w+ n P	
0030	51 d6 16 fe	00 00 52 45 54	52 20 66 6c 61	67 Ød 0		
0040	0a					

21										
8022.zip	🕌 8142.zip - 3	60压缩				文件	操作	工具	帮助 🕐 🕻	
21	添加	解压到	一键解压	<b>劉</b> 除	四月日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日					09
	★ ■ Ξ [	🏭 8142.zip	- 解包大小为	1 KB				V	▼ 搜索包内文件	
6142.2lp	名称 ]] (上级目录)					压缩前	压缩后	类型 文件夹	修改	日期
	🗍 flag.txt *		📑 输)	入密码					201	7-10-17 23:10
				为加密的文 flag.txt	2件输入密码:			•		
					码					

# 两个压缩包,都需要解密密码

大小:1 KB 共1 个文件 压缩率 90.5%





解密后从压缩包中提取到了一个flag.txt,打开发现是假的flag,并提示"maybe you should focus on the encrypted packets…",意 思是"也许你应该关注加密的数据包…"

下面提取key.log文件

📕 traf	tic.pcapng				
文件(F	) 编辑(E) 视图(N	/) 跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(	H)
4 =	1 🛛 🔒 🖻	🗙 🖾 🔍 🗢 🔿 🕾 🕢	📃 🗐 🔍 🔍 🔍 💷		
	目見示讨渡器 ··· ⟨Ct	rl-/>			
		- 「「「「」」 □ □ □ □		key log	
No	Time	Samaa		Protocol	
10.	9012 127.43525	1 192.168.43.159	182.254.217.142	FTP	67 Request: CWD /mvdata
	9013 127 48233	3 182.254.217.142	192.168.43.159	FTP	91 Response: 250 Directory successfully changed.
	9014 127 52975	5 192.168.43.159	182,254,217,142	TCP	54 58165 → 21 [ACK] Seg=73 Ack=217 Win=17152 Len=0
	9015 128,18954	9 192,168,43,159	182,254,217,142	FTP	62 Request: TYPE I
	9016 128,24125	0 182.254.217.142	192,168,43,159	FTP	85 Response: 200 Switching to Binary mode.
	9017 128.24152	6 192.168.43.159	182.254.217.142	FTP	60 Request: PASV
	9018 128.29148	7 182.254.217.142	192.168.43.159	FTP	105 Response: 227 Entering Passive Mode (182,254,217,142,72,7).
	9019 128.29197	6 192.168.43.159	182.254.217.142	FTP	68 Request: RETR key.log
	9020 128.29231	7 192.168.43.159	182.254.217.142	ТСР	66 58166 → 18439 [SYN] Seg=0 Win=65535 Len=0 MSS=1460 WS=128 SACK PERM=1
	9021 128.34159	8 182.254.217.142	192.168.43.159	TCP	66 18439 → 58166 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK PERM
	9022 128.34169	0 192.168.43.159	182.254.217.142	ТСР	54 58166 → 18439 [ACK] Seg=1 Ack=1 Win=5364608 Len=0
11	9023 128.39038	2 182.254.217.142	192.168.43.159	ТСР	54 21 → 58165 [ACK] Seq=299 Ack=101 Win=29312 Len=0
	9024 128.39274	3 182.254.217.142	192.168.43.159	FTP-DATA	1454 FTP Data: 1400 bytes
	9025 128.39274	4 182.254.217.142	192.168.43.159	FTP-DATA	1454 FTP Data: 1400 bytes 3
	9026 128.39282	9 192.168.43.159	182.254.217.142	ТСР	54 58166 → 18439 [ACK] Seg=1 Ack=2801 Win=5364608 Len=0
4 En	ame 9019: 68 b	ytes on wire (544 bits)	, 68 bytes captured (	(544 bits) or	n interface 0
⊳	Interface id:	0 (\Device\NPF_{4BFDDB	C3-E964-4672-B0EB-016	775AFA79F})	
	Encapsulation	type: Ethernet (1)			
	Arrival Time:	Oct 18, 2017 01:11:59.	901660000 中国标准时间	]	
	[Time shift f	or this packet: 0.00000	0000 seconds]		
	Epoch Time: 1	508260319.901660000 sec	onds		
	FT 1 1 1	· · · · · · · · · · · · · · · · · · ·	0.000400000	. 1	•
0000	bc 20 10 ca	48 8c 68 07 15 97 33	dt 08 00 45 00	H.h3E	
0010	d9 80 03 25	40 00 40 06 57 55 C0 3	ao 20 9t 06 te .6t.	@.@. WU+	
0020	00 43 ca b8	00 00 52 45 54 52 20	6b 65 79 2e 6c	RE TR key	
0040	6f 67 0d 0a		og		
				•	

х 【Wireshark ⋅ 追踪 TCP 流 (tcp.stream eq 58) · traffic CLIENT RANDOM cbdf25c6b2259a0b380b735427629e94abe5b070634c70bd9efd7ee76c0b9dc0 . 6782ad3aa5938c43831971a06e9a20eac27075d559799769ce5d1a3ea85211c981d8e67f75d6fd11fcf5536f331a968b Ξ CLIENT RANDOM 247f33720065429dc7e017e51f8b904309685ec8688296011cd3c53e5bafa75a 921ffbf7bfe6d8c393000f34eab6dc20486e620bdc90f21b6037c3df5592ef91fffca1dc8215699687a98febd45a4ce0 CLIENT\_RANDOM\_2000cef83c759e5e0c8bbdbd0a05388df25014fc32008610577ccd92d5fa3e3e 4c03f7a409b6e0ab7a0b793485696c02ab7743c1a9fda0039b0f7ac05205cf209d5855261ece18897dbe43a116b73627 CLIENT RANDOM c5dd1755eff2a51b5d4a4990eca2cc201d9b637cd8ad217566f21194e19d6f60 c3a065698b99629875b03d6754597349612e6e7468ef66dcf8f277f9e84396ae55a1b72248019df1608ca3962f617252 CLIENT RANDOM 11ae1440556a6e740fd9a18d0264cd4c49749355dcf7093daad965030a21fcfe 219786b326ccf760cd787de3cc7e1dcd668a1a3d336170334f879b061cec81131fff4850ce5c6ea15d907be8a36638b7 CLIENT RANDOM 02002c43f43bc483152fa26cf255da81aa3048edf763c06e646c02dcd53f90fa 6a9b11b24d224c7c74691bfa8ac0086f8f027d8ec05e2135593425d42df5834aee37aedcfb9c2d476cb8998ce41603fb CLIENT RANDOM 444ba97e9d2ca12ec0c627db8ee5b5a97e1a4c49d3df77221e35c55ca3cc3c28 def07b2e4fc18939843a9409f742f243319705c862fac89a9002ed86d00e39401dedda9f9d7bfaa7e4c741ae3fb8500ffabreardedefbabrCLIENT RANDOM ec6b0fc5b006e3ed50f2c682a2be2cad1fb04e92b29111f126725eefd1520b5b cd3f903e551cb61140b7dd40ef3e8024bbdc3fc1c1e5737bbb2617b4a984b9c545e2468866080974a14791a19ac09671 CLIENT\_RANDOM d4f49620d5e82b92f46041ef81fd7b12fc4423740ba5ee798e754b4f7a200b63 008815f111055f310026ac5e496e9f289ca6ed9c8cd9a3dc7c6fdd7dd54d25a0103c2ca48c4c0e4b54976cb572a8bba2 CLIENT RANDOM f8d0b49ea5df02f0d61a5000eb0cbd529c8aea651e9ecd364c5deecfa3ecb4eb b3d6d37d392432d4903b4fcb3bd7a52d2faf0552fe62e4a739bf19f611903cdd893cb8c34c2f895337c885491044b20f CLIENT RANDOM d219d102e23aec7e8bf0720968c5e18ffec8213ee91142ccff47460952c67557 33df1df41dcdf73f6d9a82ee9e75b8bb329bc52565b4861bf511853af59c670a972a5330627dc06cd8b7c24e3fad12ad CLIENT RANDOM c250e14706090035869fa0f2277538089fbedcb34c2ca4916c0cc14f7d03cd82 c7f36b2bf3902015802e44ea0139de8979a7886413782ff91b3e781d388b539c1e289f7ca9dad97e898d46a8f1d3a09b CLIENT RANDOM bf1e202c132e5ac68fde90dc21731b7ee8d37be63ccdf0379655eb33823fd316 a02c80340de4f380fd149ba49052b045ffa5a3cb43a6ee4958f3248f75459d7a548c38221550c1b456c23e37072d4297 CLIENT RANDOM a61be0b892219f5110d62adf0379bc84cb3f8c670d027bdd02f7eeab0f4d6ab9 a155d79f8d678b2577a74c3de308090beeb501d5b7523d11067c6503fa93e0c275bd8b2916e262c8ac6221bf23fab2f5 CLIENT\_RANDOM 41535597a84fbf6cc785687b0d043e59fc5e3786b5de125584b6134b52fdce64 589bdcc87a8da05d93101598073baf0da466297ebc143db4a8949a2a15ecf3e8e9691aeec1247590520c4e2217f9e93d CLIENT RANDOM 723c07e2d837f4c62e2a1009390631a147d36d06aa9c2d2341989a459b379738 13 寒户端 分组, 21 服务器 分组, 12 turn(s). 流 📴 🚔 Entire conversation (26 kB) • 显示和保存数据为 ASCII -查找: 查找下一个()) Close 滤掉此流 打印 Save as... 返回 Help

加密的数据包?那就应该是TLS协议没跑了,又想到key.log这个文件还没有用,然后使用key.log对TLS协议进行解密。(操作步骤:编辑→首选项→Protocols→TLS,然后在下面导入key.log文件)



【 Wireshark · 导出 · HTTP 对象列表 - 0 分组 主机名 内容类型 大小 文件名 8005 nj02all02.baidupcs.com applicatio application/zip 6849 kB e56e57b2ff4745d273ea711004dedf58?bkt=p3-00001c02a7abfa60bc0578fec2cad9928a548cfid application/json 385 bytes download?sign=XekZm95xrHfLCUvXIEf0PnU6wouCPbG37E2KyOM78ZxwaNYhknA6A%3D%3 9823 pan.baidu.com pan.baidu.com 383 bytes\_download?sign=XekZm95xrHfLCUvXIEf0PnU6wouCPbG37E2KyOM7BZxwaNYhhknA6A%3D%3 773 application/json 848 d.pcs.baidu.com text/plain 51 bytes\_e56e57b2ff4745d273ea711004dedf582fid=4145147309-250528-23739752300500&time=1508 44 bytes analytics?\_lsid=1508260199290&\_lsix=1&clienttype=0&vmode=list&searchForm=false&versic 760 , pan.baidu.com image/jpeg 763 pan.baidu.com image/iped 44 bytes analytics? |sid=1508260199293& |six=1&clienttype=0&ymode=list&searchForm=false&yersic

				10	172.100.45.155					,,
ť	来仔(S)	Ctrl+S		.159	180.97.36.16	n	767	pan.baidu.com	image/jpeg	44 bytes analytics?_lsid=1508260199300&_lsix=1&clienttype=0&vmode=list&searchForm=false&versic
5	弓存为(A)	Ctrl+Shift+S	S	.159	144.76.59.84	nt	768	pan.baidu.com	image/jpeg	44 bytes analytics?_lsid=1508260199300&_lsix=1&clienttype=0&vmode=list&searchForm=false&versic
	行件住在			.159	180.97.36.16	er	794	pan.baidu.com	image/jpeg	44 bytes analytics?_lsid=1508260199701&_lsix=1&clienttype=0&vmode=list&searchForm=false&versic ≡
1	КІТЖН		· .	.159	180.97.36.16	со	9810	pan.baidu.com	mage/iper	44 bytes analytics Isid=150820032000000.Line=18/coentrype=0&vmode/list&searchForm=fale=&versic
Ę	寻出特定分组			.159	180.97.33.108		9816	pan.baidu.com	im/ge/ipe	44 bytes analyzes _isd=150920D328224Cs.jsix=1&elenttype=0&vmode=lict&searchileren_faise&versic
Ę	导出分组解析结果		•	.159	180.97.33.108		9821	pan.baidu.com	jhage/jpe	44 byes analytics _lsid=15002600282298lsix=L&client/ype=0&vmode/list&search/orn=f/lse&versic
Ę	异出分组字节流(B)	Ctrl+H		.159	180.97.33.108		9822	pan.baidu.com	image/jpeg	44 bytes_analytics?_lsid=1508260328229&_lsix=1&clienttype=0&vmode=list&searchForm=false&versic
5	■出 DDI 到文件			.159	180.97.33.108	80	9847	pan.baidu.com	image/jpeg	44 bytes_analytics?_lsid=1508260328557& lsix=1&clienttype=0&vmode=list&searchForm=false&versic
				.159	180,97,33,107	- 00	163	imgstat.baidu.com	n age/git	3 b toientcon.gif?_=1578220192105
	эц ээс <u>хира</u> лл				0.97.33.107	21	294	imgstat.baidu.com	mage gif	3 pute: crientcon.gif? = 1508 26019377
	手山刈滅		<u> </u>	DICOM	2,168,43,159		483	imgstat.baidu.com	age, st	
$\leq$	JED(P)	Ctrl+P		HTTP	4.76.59.84		629	imgstat.baidu.com	image/gif	43 bytes clientcon.git/_=150826019/394
-				IMF	As cantured	7	738	hm.baidu.com		43 5 5 5 5 6 5 6 5 6 5 6 7 6 7 6 7 6 7 6 7
i	2出	Ctrl+Q		SMB	5.97.33.df)	<b>`</b>	790	hm.baidu.com		42 b too _it.gov/cc=Udck=1dcl=24 bit8ds= 9 UV UU UV p=cr om 5t bight broard Download chipme
To	tonnot Protocol V	Voncion A	~	TETP	159 Det: 1		0300	imgstat.baidu.com	trager gir	42 bites diverse all = 150220024
	on Determore Prote	ocol Enc	Por	+. 16227	Det Bont: 2590	, <b>-</b>	0403	imgstat.baidu.com	image/gil	43 bytes clientcon.gli?1308200242001
V US	er Datagram Froti	0001, 5PC	FUI	·t. 40527,	DSC FORC. 2000.	· .	0400	imgstat.baidu.com	image/gif	43 bytes clientcon.gli?1508260230912
							9490	ingstat.baldu.com	image/gii	45 bytes cilencon.gir1508200525002
							-	III		· · ·
0000	bc 20 10 ca 48	8c 68 07	1	5 97 33 df	08 00 45 00					Save Save All Close Help
0010	00 1c 0c ee 40	00 03 11	b	2 fb c0 a8	2b 9f 90 4c					
0020	3b 54 b4 f7 65	2f 00 08	2	d cf		1				hite a dhi ka a shekari a sheka

traffic.pcapng

ŧ⊤开

关闭

打开最近

合并(M)..

从 Hex 转储导入(I)...

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线

🛎 T 🕹 📃 🗏 Q Q Q 🖽

Destination

192.168.43.159

Ctrl+O

Ctrl+W

▼ 49 搜索 ke 🔄 🕞 - 📕 → 计算机 → WIN7 (C:) → 用户 → Administrator.PCOS-2020KMUMGH → 桌面 → key 文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H) ■ 使用 酷狗音乐攝放器 播放 ▼ 全部播放 共享 ▼ 刻录 新建文件夹 H • 🔳 🔞 组织 ▼ 📑 key.zip - 360压缩 名称 # 标题 参与创作的艺术家 唱片集 ☆ 收藏夹 5 PI 4  $\leq$ 🖬 2.mp3 1 アスノヨゾラ哨戒班 ウォルピスカータ... ウォルピスカーター... 解压到 💻 桌面 肩 库 **☆** 🔲 Ξ 📕 key.zip - 解包大小为 Au Adobe Audition - 2.mp3 名称 📗 .. (上级目录) 编辑(E) 视图(V) 效果(T) 收藏(R) 选项(O) 窗口(W) 帮助(H 生成 🖬 2.mp3 🔤 编辑 🖽 多轨 🥝 CD 工作区: 编辑查看(默认) 文件 × 效果 收藏式 主群组 ⇒ lx ≞ å ð 8. 2. mp3 Key i AddaddaaAaddaAAddddaaAAAAAddddaadd



#### 直接把该key提交flag,先试试,发现不对。那就解密压缩包

📕 8022.zip - 3	360压缩				文件	キー 操作	工具	帮助	🕐 🖘		3	- *	1 KB	1 KB	· · · · · · · · · · · · · · · · · · ·	2
添加	解压到 -	键解压	副除	西省包语言						0%		☐ flag.txt - 记事本 文件(f) 编辑(E) 格式(O) 查看(V) 帮助(H)	110	IND		×
↑ ■ Ξ	📕 8022.zip - 1	解包大小为	1 KB				V	▼ 搜索	包内文件	)	۹	flag{4sun0_y0zora_sh0ka1h@n#>>_<<#}				*
名称				J	压缩前	压缩后	类型		修改日期							
🎽 (上级目录)	)						文件夹									
🗍 flag.txt *		■■ 輸入 : ! 〔	<ul> <li>密码</li> <li>为加密的文</li> <li>flag.txt</li> <li>显示密</li> <li>管理密码</li> </ul>	件输入密码: 	****** 确定	Ę	<b>▼</b> 消	8	2017-10	.17 23:11	F	イ 2 単 1 小文仕 圧縮家 137.8% 戸紀洗塚 1 KR (1 小文仕)	https	音 M//bioid	頁1行,第1列 SSeinmn⊖7/nne	toru Sist

成功!

下面是别人有用的一部分思路,可以看看。

按照协议类型对数据包进行读取,发现只有FTP协议是由用的,但是同时注意到TLS协议是进行加密的,其他的协议并没有什么作用。然后使用wireshark的过滤器将FTP和FTP-DATA筛选出来。发现了ftp的用户名和密码,尝试登陆,发现不能登录。

	traffi	c.pcapng	-				_		_	-		×
3	て(件(F)	编辑(E)	视图(V)	跳转(G) 捕获(	C) 分析(A)	统计(S)	电话(Y)	无线(W)	工具(T)	帮助(ŀ	(H)	
		10	1 📠 🔀	। 🖸 । ९ 👄 🖻	) 🕾 🛉 👃		$\oplus$ $\Theta$	Q. 🎹				
	ftp										▼ → 表达式…	+
No	C	Time		Source		Destin	nation		Protôco	1 L	length Info	
	5	502 15.0	72834	182.254.2	217.142	192.	168.43.	159	FTP		74 Response: 220 (vsFTPd 3.0.2)	
	5	503 15.0	73113	192.168.4	13.159	182.	254.217	.142	FTP		64 Request: AUTH TLS	
	5	506 15.1	12865	182.254.2	217.142	192.	168.43.	159	FTP		92 Response: 530 Please login with USER and PASS.	
	5	507 15.1	13082	192.168.4	43.159	182.	254.217	.142	FTP		64 Request: AUTH SSL	
	5	508 15.1	55721	182.254.2	217.142	192.	168.43.	159	FTP		92 Response: 530 Please login with USER and PASS.	
	5	509 15.1	55996	192.168.4	43.159	182.	254.217	.142	FTP		64 Request: USER ftp	
	5	510 15.1	95905	182.254.2	217.142	192.	168.43.	159	FTP		88 Response: 331 Please specify the password.	
	5	511 15.1	96161	192.168.4	13.159	182.	254.217	.142	FTP		69 Request: PASS codingay	
	5	767 15.3	02736	182.254.2	217.142	192.	168.43.	159	FTP		77 Response: 230 Login successful.	
	5	777 15.3	02881	192.168.4	13.159	182.	254.217	.142	FTP		68 Request: OPTS UTF8 ON	
	5	785 15.4	46732	182.254.2	217.142	192.	168.43.	159	FTP		80 Response: 200 Always in UTF8 mode.	
	5	786 15.4	51795	192.168.4	13.159	182.	254.217	.142	FTP		59 Request: PWD	
	5	787 15.5	02976	182.254.2	217.142	192.	168.43.	159	FTP		69 Response: 257 "/mydata"	
	7	370 17.3	70995	192.168.4	13.159	182.	254.217	.142	FTP		60 Request: PASV	
	7	414 17.4	41227	182.254.2	217.142	192.	168.43.	159	FTP		106 Response: 227 Entering Passive Mode (182,254,217,142,47,56).	
	7	415 17.4	41586	192.168.4	13.159	182.	254.217	.142	FTP		65 Request: RETR flag	-
	Fra Eth Int Tra Fil	me 5509 ernet I ernet Pr nsmissio e Trans <sup>.</sup>	: 64 byt [, Src: rotocol on Contr Fer Prot	tes on wire IntelCor_97 Version 4, 9 rol Protocol tocol (FTP)	(512 bits :33:df (6 Src: 192.: , Src Por	), 64 by 8:07:15: 168.43.1 t: 58148	tes cap 97:33:0 59, Dst , Dst F	otured ( if), Dst :: 182.2 Port: 21	512 bits : bc:20: 54.217.1 , Seq: 2	) on 10:c 42 1, A	n interface 0 ca:48:8c (bc:20:10:ca:48:8c) Ack: 97, Len: 10	
9 9 9 9 9 9	)000 )010 )020 )030	bc 20 00 32 d9 8e 51 db	10 ca 4 66 4a 4 e3 24 0 78 4c 0	8 8c 68 07 0 00 40 06 0 15 29 79 0 00 55 53	15 97 33 57 a7 c0 dc b8 20 45 52 20	df 08 00 a8 2b 9 65 22 6 66 74 70	0 45 00 f b6 fe f 50 18 0 0d 0a	 .2fJ \$ Q.xL	H.h3 @.@. W )y US ER	E .+ ⊵"oP ftp.	https://blog.csdn.net/mutou	u990

服务器地址: 182.254.217.142 用户名: ftp 密码: codingay

登录	
<b>ftp://182</b> 您与此网:	.254.217.142 站的连接不是私密连接
用户名	
密码	
	<del>發录</del> https://blog.csdn.net/mutou990

(这里可以在过滤输入框里输入FTP回车后,再对筛选过的包进行分析查看,也可以ctrl+F 查找【字符串】关键字ctrl+F 查找关键字flag或者flag的【十六进制】666c6167进行快速查找,本文用查找flag关键字方法)

然后回到数据包刷新一下就可以看到揭秘之后的数据了。因为TLS加密的是http协议,所以解密之后直接过滤http协议就可以了。 查看后可以大致分析出,是用百度网盘下了一个文件,把这个文件导出。(文件→导出对象→HTTP) 导出的文件是一个压缩包,解压后是一个音频文件,使用Audition打开,查看一下频谱帧率,可以看到 用的是audacity不好用,看不清楚。

使用这个key可以解开刚才那个加了密的压缩文件,解压后拿到一个flag.txt,打开即可获得真正的flag!



5.打开这个文档发现flag竟然是假的。。。好吧,我就知道没有这么简单,但是通过这个提示我们可以知道这个流量包是被加密 过的,综合上面得到的key.log不难知道要得到真正的flag需要对这个流量包进行解密 6.虽然没有得到真正的flag,但我们已经知道了接下来的解题方向了,也不算是一无所获。 7.我们把key.log导出(追踪tcp流导出)9.刷新之后出现解密后的流量包,在其中发现了一个隐藏的压缩包,解压出来是一个 MP3音频,用Audacity打开,中间有一段杂音,用频谱图查看 发现是有隐藏密码的,提交发现不是flag,于是想到另一个压缩包,输入密码得到flag