

# 第三届上海市大学生网络安全大赛 流量分析

原创

principle1 于 2021-12-28 12:26:39 发布 2412 收藏

文章标签: [web安全](#) [安全](#)

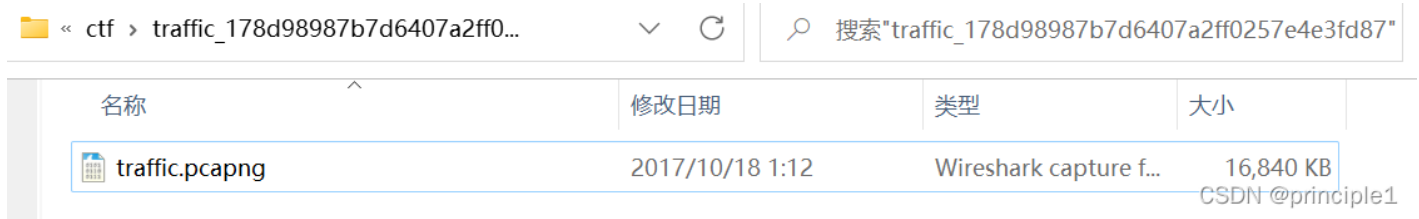
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/principle1/article/details/122186307>

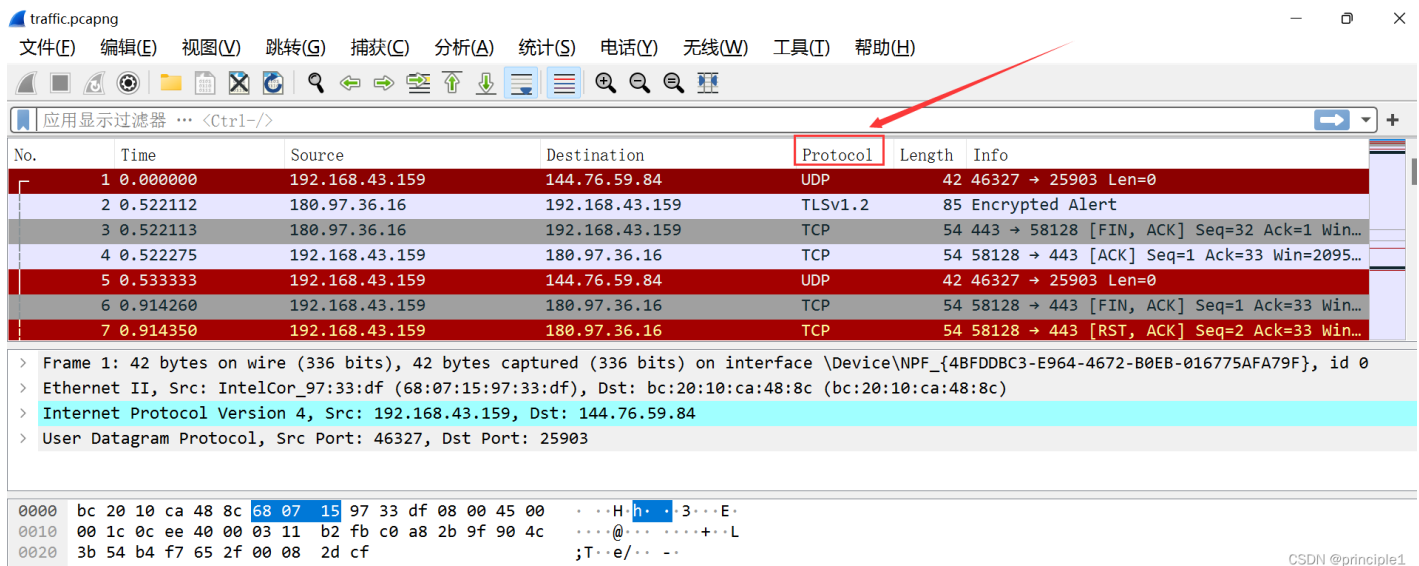
版权

关于这个writeup是写给初学者的, 重点在于如何利用工具。

该题目下载文件打开后是一个抓包文件



使用wireshark打开, wireshark下载地址: [Wireshark - Download \(softonic.com\)](#)



点击Protocol后, 会对协议的名称按字母排序, 可以初略看一下使用了哪些协议

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)

应用显示过滤器 ... <Ctrl- />

No.	Time	Source	Destination	Protocol	Length	Info
9017	128.241526	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
9018	128.291487	182.254.217.142	192.168.43.159	FTP	105	Response: 227 Entering Passive Mode (18...
9019	128.291976	192.168.43.159	182.254.217.142	FTP	68	Request: RETR key.log
9038	128.398154	182.254.217.142	192.168.43.159	FTP	122	Response: 150 Opening BINARY mode data ...
9058	128.498265	182.254.217.142	192.168.43.159	FTP	78	Response: 226 Transfer complete.
7420	17.522353	182.254.217.142	192.168.43.159	FTP-DATA	61	FTP Data: 7 bytes (PASV) (RETR flag)
8022	19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes (PASV) (RETR flag.z...
8110	40.604411	182.254.217.142	192.168.43.159	FTP-DATA	437	FTP Data: 383 bytes (PASV) (LIST)

> Frame 9038: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF\_{4BFDDBC3-E964-4672-B0EB-016775AFA79F}, id 0

> Ethernet II, Src: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c), Dst: IntelCor\_97:33:df (68:07:15:97:33:df)

> Internet Protocol Version 4, Src: 182.254.217.142, Dst: 192.168.43.159

> Transmission Control Protocol, Src Port: 21, Dst Port: 58165, Seq: 299, Ack: 101, Len: 68

> File Transfer Protocol (FTP)

[Current working directory: /mydata]

```

0000  68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00  h...3...H...E
0010  00 6c d7 ac 40 00 30 06 f6 0a b6 fe d9 8e c0 a8  .l..@..
0020  2b 9f 00 15 e3 35 8b 95 78 8b c7 13 e2 22 50 18  +...5..x...P
0030  00 e5 79 bf 00 00 31 35 30 20 4f 70 65 6e 69 6e  .y...15 Openin
0040  67 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 64 61  g BINARY mode da
0050  74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f  ta conne ction fo
0060  72 20 6b 65 79 2e 6c 6f 67 20 28 32 36 37 32 37  r key.lo g (26727
0070  20 62 79 74 65 73 29 2e 0d 0a                   bytes).
  
```

CSDN @principle1

ftp协议用于文件传输，可以点击 右键 -> 追踪流 -> TCP流

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)

应用显示过滤器 ... <Ctrl- />

No.	Time	Source	Destination	Protocol	Length	Info
9017	128.241526	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
9018	128.291487	182.254.217.142	192.168.43.159	FTP	105	Response: 227 Entering Passive Mode (18...
9019	128.291976	192.168.43.159	182.254.217.142	FTP	68	Request: RETR key.log
9038	128.398154	182.254.217.142	192.168.43.159	FTP	122	Response: 150 Opening BINARY mode data ...
9058	128.498265	182.254.217.142	192.168.43.159	FTP	78	Response: 226 Transfer complete.
7420	17.522353	182.254.217.142	192.168.43.159	FTP-DATA	61	FTP Data: 7 bytes (PASV) (RETR flag)
8022	19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes (PASV) (RETR flag.z...
8110	40.604411	182.254.217.142	192.168.43.159	FTP-DATA	437	FTP Data: 383 bytes (PASV) (LIST)

> Frame 9017: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{4BFDDBC3-E964-4672-B0EB-016775AFA79F}, id 0

> Ethernet II, Src: IntelCor\_97:33:df (68:07:15:97:33:df), Dst: IntelCor\_97:33:df (68:07:15:97:33:df)

> Internet Protocol Version 4, Src: 192.168.43.159, Dst: 182.254.217.142

> Transmission Control Protocol, Src Port: 58165, Dst Port: 21, Seq: 299, Len: 60

> File Transfer Protocol (FTP)

[Current working directory: /mydata]

```

0000  bc 20 10 ca 48 8c 68 07 15 97 33 df 08 00 45 00  .f.@...
0010  00 2e 66 97 40 00 40 06 57 5e c0 a8 2b 9f b6 fe  .f.@...
0020  d9 8e e3 35 00 15 c7 13 e2 0e 8b 95 78 58 50 18  .C...F
0030  00 43 f1 b1 00 00 50 41 53 56 0d 0a                   .C...F
  
```

右键菜单:

- 标记/取消标记 分组(M) Ctrl+M
- 忽略/取消忽略 分组(I) Ctrl+D
- 设置/取消设置 时间参考 Ctrl+T
- 时间平移...
- 分组注释
- 编辑解析的名称
- 作为过滤器应用
- 准备作为过滤器
- 对话过滤器
- 对话着色
- SCTP
- 追踪流** Ctrl+Alt+Shift+T
- 复制
- 协议首选项
- Decode As...
- 在新窗口显示分组(W)

追踪流子菜单:

- TCP 流** Ctrl+Alt+Shift+T
- UDP 流 Ctrl+Alt+Shift+U
- DCCP Stream Ctrl+Alt+Shift+E
- TLS 流 Ctrl+Alt+Shift+S
- HTTP 流 Ctrl+Alt+Shift+H
- HTTP/2 Stream

CSDN @principle1

```
220 (vsFTPd 3.0.2)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER ftp
331 Please specify the password.
PASS codingay
230 Login successful.
OPTS UTF8 ON
200 Always in UTF8 mode.
CWD /mydata
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (182,254,217,142,72,7).
RETR key.log
150 Opening BINARY mode data connection for key.log (26727 bytes).
226 Transfer complete.
```

从0开始依次递增



9 客户端 分组, 11 服务器 分组, 18 turn(s).

整个对话 (490 bytes)

Show data as ASCII

流 57

查找:

查找下一个 (N)

清除此流

打印

另存为...

返回

Close

CSDN @principle1

Wireshark · 追踪 TCP 流 (tcp.stream eq 38) · traffic.pcapng

```
PK...    ...}.QK..W.3...%......flag.txt.<.>...)A...N.Mc...mBya.  
8...r...;...^..V.q.6.4V.PK...W.3...%.PK.....    ...}.QK..W.3...  
%...$......    .....flag.txt  
.....%.FZG..)Q..XG..)Q..XG..PK.....Z...i.....
```

zip文件的标识

0 客户端 分组, 1 服务器 分组, 0 turn(s).

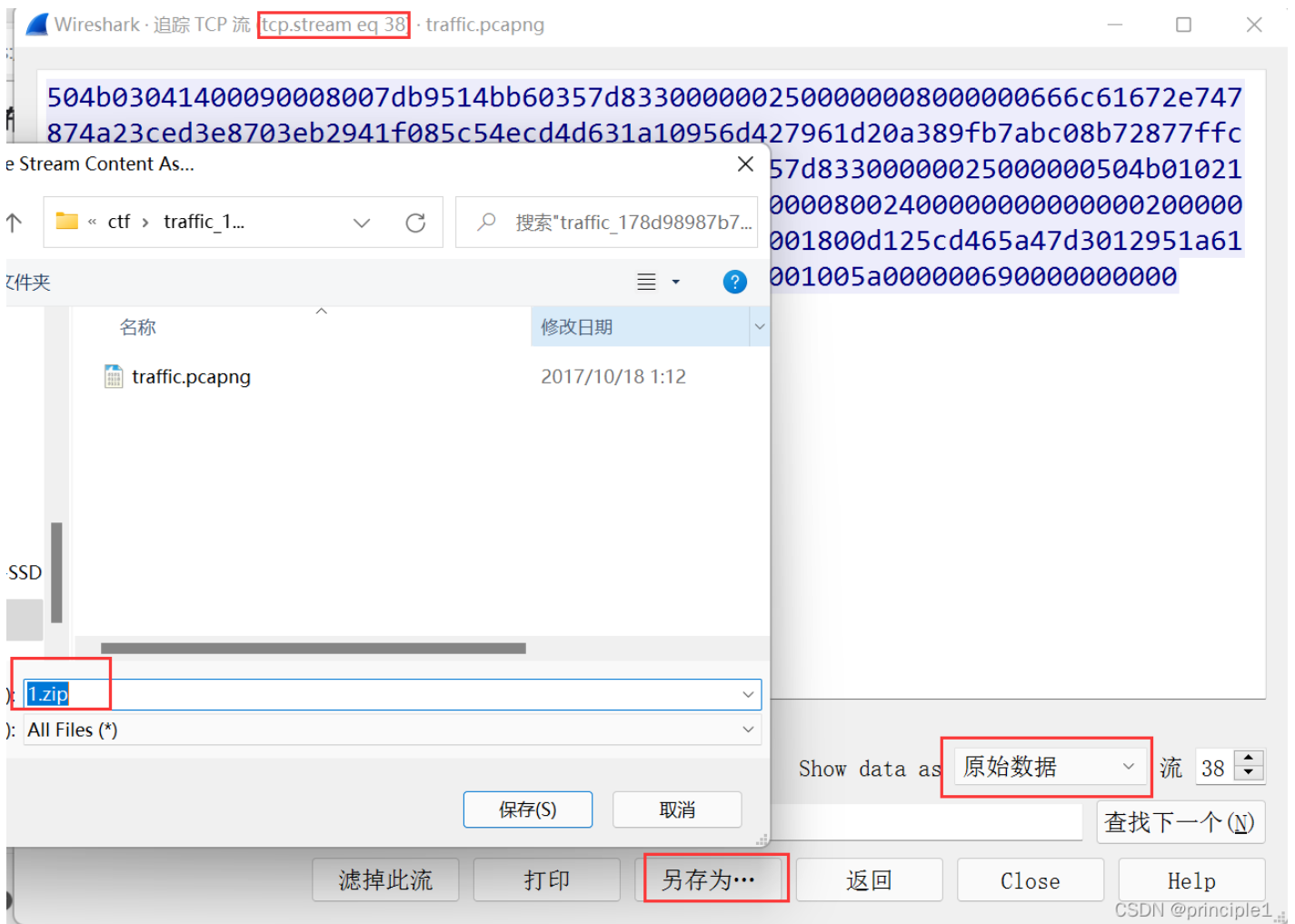
整个对话 (217 bytes) Show data as ASCII 流 38

查找: 查找下一个(N)

滤掉此流 打印 另存为... 返回 Close Help

CSDN @ principle1

把 'Show data as' 的值修改为 '原始数据' 后，保存该zip文件为1.zip



继续往后翻tcp流可以发现还有一个zip文件，按照同样的方式下载下来保存为2.zip



往下翻，可以看到还有一个key.log的文件，该文件能解密出wireshark里面的https的数据流，找到该文件并下载下来

Wireshark · 追踪 TCP 流 (tcp.stream eq 55) · traffic.pcapng

drwxrwxr-x	2	500	500	4096	Sep 17 23:44	docker
-r--r--r--	1	33	33	7	Aug 16 18:51	flag
-rwxr-xr-x	1	33	33	217	Oct 18 01:10	flag.zip
drwx-----	2	107	115	4096	Oct 17 17:38	gay
-rwxr-xr-x	1	33	33	26727	Oct 18 01:11	key.log
drwxrwxrwx	2	0	0	16384	Oct 27 2016	lost+found
drwxrwxrwx	3	0	0	4096	Nov 29 2016	test

0 客户端 分组, 1 服务器 分组, 0 turn(s).

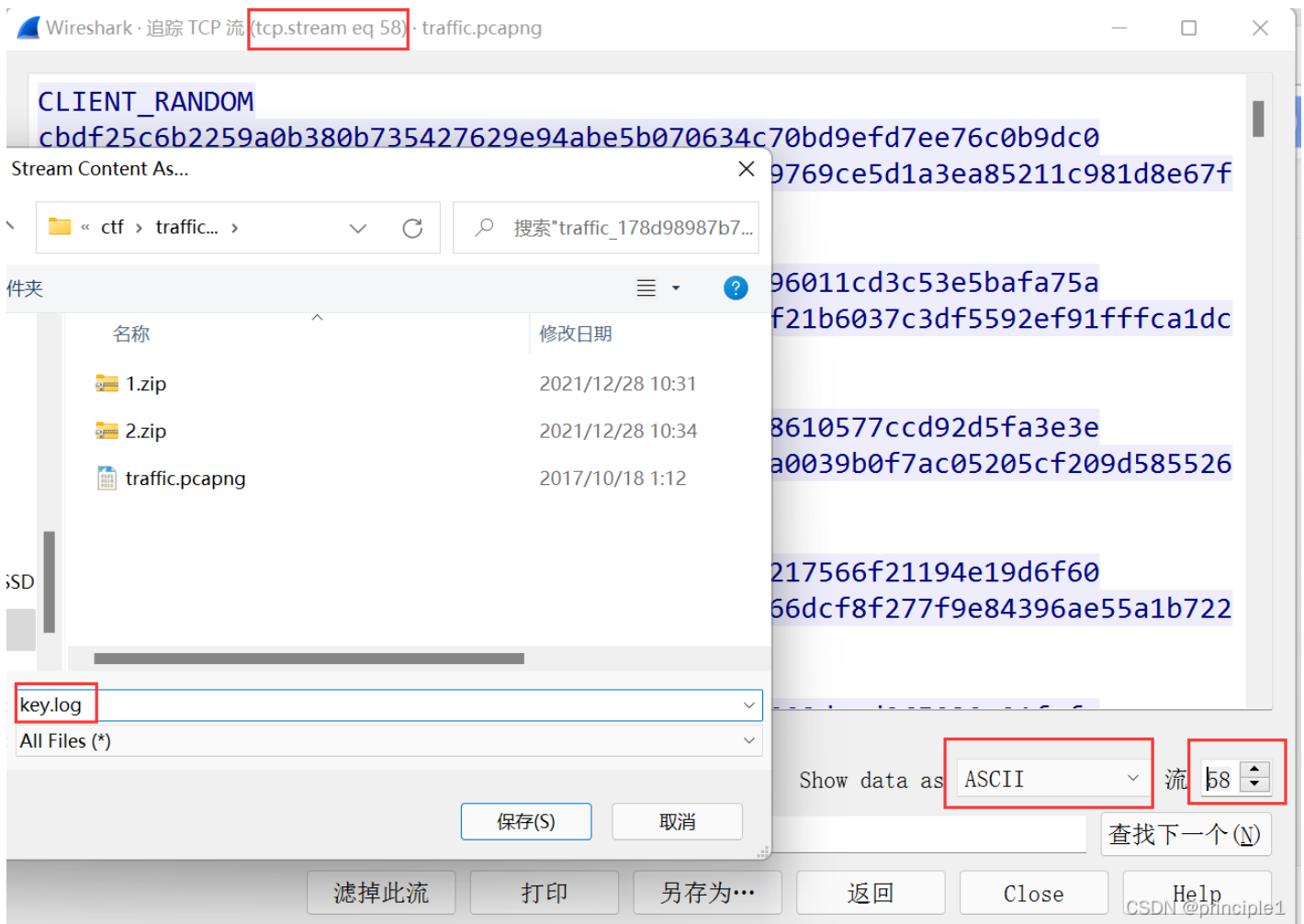
整个对话 (448 bytes) Show data as ASCII 流 55

查找: 查找下一个(N)

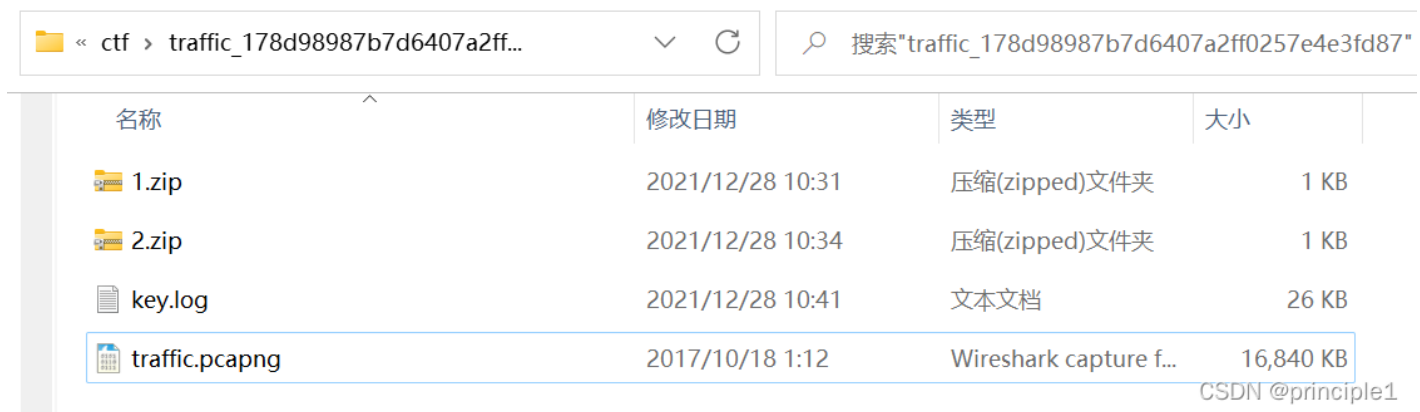
滤掉此流 打印 另存为... 返回 Close Help

GSDN @principle1

找到key.log后直接下载



现在我们下载了两个zip文件和一个key.log文件，解压发现zip文件被加密了



首先考虑是否是zip伪加密，用010editor打开文件，010editorde1的下载链接（[SweetScape Software Inc - Download 010 Editor](#)），破解文件使用的是脚本之家里面的（下载时并没有发现捆绑文件，下载后时一个zip文件，不用解压直接提取破解文件后删除zip文件就行）



010 Editor - D:\ctf\traffic\_178d98987b7d6407a2ff0257e4e3fd87\1.zip

File Edit Search View Format Scripts Templates Debug Tools Window Help

1.zip x 2.zip Inspector

Address	Hex	ASCII
0000h:	50 4B 03 04 14 00 09 00 08 00 7D B9 51 4B B6 03	PK.....}!QK..
0010h:	57 D8 33 00 00 00 25 00 00 00 08 00 00 00 66 6C	W03...%.....f1
0020h:	61 67 2E 74 78 74 A2 3C ED 3E 87 03 EB 29 41 F0	ag.txt<i>#.è)Að
0030h:	85 C5 4E CD 4D 63 1A 10 95 6D 42 79 61 D2 0A 38	...ANIMc...mBya0.8
0040h:	9F B7 AB C0 8B 72 87 7F FC 3B 18 C4 C5 5E AE A0	ÿ·«Ä<r†.ü;.ÄÄ^@
0050h:	56 AB 71 1D 36 FA 34 56 CB 50 4B 07 08 B6 03 57	V«q.6ú4VÉPK..¶.W
0060h:	D8 33 00 00 00 25 00 00 00 50 4B 01 02 1F 00 14	03...%...PK.....
0070h:	00 09 00 08 00 7D B9 51 4B B6 03 57 D8 33 00 00	.....}!QK..W03..
0080h:	00 25 00 00 00 08 00 24 00 00 00 00 00 00 00 20	..%....\$......
0090h:	00 00 00 00 00 00 00 66 6C 61 67 2E 74 78 74 0A	.....flag.txt.
00A0h:	00 20 00 00 00 00 00 01 00 18 00 D1 25 CD 46 5A	.....N%ÍFZ
00B0h:	47 D3 01 29 51 A6 18 58 47 D3 01 29 51 A6 18 58	G0.)Q .XG0.)Q .X
00C0h:	47 D3 01 50 4B 05 06 00 00 00 01 00 01 00 5A	G0.PK.....Z
00D0h:	00 00 00 69 00 00 00 00 00 00 00 00 00 00 00	...i.....

Template Results - ZIP.bt

Name	Value	Start	Size
> struct ZIPFILERECD record	flag.txt	0h	59h
> struct ZIPDATADESCR dataDescr		59h	10h
> struct ZIPDIRENTRY dirEntry	flag.txt	69h	5Ah
> struct ZIPENDLOCATOR endLocator		C3h	16h

Inspector

Type	Value
Binary	01010000
Signed Byte	80
Unsigned Byte	80
Signed Short	19280
Unsigned Short	19280
Signed Int	67324752
Unsigned Int	67324752
Signed Int64	2533360757066576
Unsigned Int64	2533360757066576
Float	1.543356e-36
Double	1.2516465185889...
Half Float	14.625
String	PK□□□
DOSDATE	10/16/2017
DOSTIME	09:26:32
FILETIME	01/11/1609 03:07:...
OLETIME	
time_t	02/19/1972 05:19:...
time64_t	
GUID	{04034B50-0014-...
Opcode (X86-32)	push eax
Opcode (X86-64)	push rax
Opcode (ARM-32)	streq r4, [r3], #-0x...
Opcode (ARM-64)	

Selected: 89 [59h] bytes (Range: 0 [0h] to 88 [58h]) Start: 0 [0h] Sel: 89 [59h] Size: 217 Hex ANSI Q\$DN @pñncp¶¶¶¶

点开

ushort deFlags这个字段与zip伪加密有关，奇数为加密，偶数为没有加密，尝试把9改为0，保存后打开zip文件查看是否已经解密，若出现错误，记得把0改回来之后再保存文件，否则文件破坏后无法解题。

010 Editor - D:\ctf\traffic\_178d98987b7d6407a2ff0257e4e3fd87\1.zip

File Edit Search View Format Scripts Templates Debug Tools Window Help

1.zip x 2.zip Inspector

Address	Hex	ASCII
0000h:	50 4B 03 04 14 00 09 00 08 00 7D B9 51 4B B6 03	PK.....}1QKl.
0010h:	57 D8 33 00 00 00 25 00 00 00 08 00 00 00 66 6C	W03...%.....f1
0020h:	61 67 2E 74 78 74 A2 3C ED 3E 87 03 EB 29 41 F0	ag.txt<<i>#.ë)Að
0030h:	85 C5 4E CD 4D 63 1A 10 95 6D 42 79 61 D2 0A 38	...ANIMc...mBya0.8
0040h:	9F B7 AB C0 8B 72 87 7F FC 3B 18 C4 C5 5E AE A0	Ÿ.«Ä<r#;ü;.AA^@
0050h:	56 AB 71 1D 36 FA 34 56 CB 50 4B 07 08 B6 03 57	V«q.6ú4VÉPK.. .W
0060h:	D8 33 00 00 00 25 00 00 00 50 4B 01 02 1F 00 14	03...%...PK....
0070h:	00 09 00 08 00 7D B9 51 4B B6 03 57 D8 33 00 00	.....}1QKl .W03.
0080h:	00 25 00 00 00 08 00 24 00 00 00 00 00 00 20	..%.....\$.....
0090h:	00 00 00 00 00 00 00 66 6C 61 67 2E 74 78 74 0A	.....flag.txt.
00A0h:	00 20 00 00 00 00 00 01 00 18 00 D1 25 CD 46 5A	.....N%ÍFZ
00B0h:	47 D3 01 29 51 A6 18 58 47 D3 01 29 51 A6 18 58	GÓ.)q .XGÓ.)Q .X
00C0h:	47 D3 01 50 4B 05 06 00 00 00 00 01 00 01 00 5A	GÓ.PK.....Z
00D0h:	00 00 00 69 00 00 00 00 00	...i.....

Inspector

Type	Value
Binary	00001001
Signed Byte	9
Unsigned Byte	9
Signed Short	9
Unsigned Short	9
Signed Int	524297
Unsigned Int	524297
Signed Int64	542732297248073...
Unsigned Int64	542732297248073...
Float	7.346966e-40
Double	6.7907036703883...
Half Float	5.364418e-07
String	
DOSDATE	
DOSTIME	00:00:18
FILETIME	
OLETIME	
time_t	01/07/1970 01:38:...
time64_t	
GUID	{00080009-B97D-...
Opcode (X86-32)	or dword ptr [eax...
Opcode (X86-64)	or dword ptr [rax...
Opcode (ARM-32)	andeq r0, r8, sb
Opcode (ARM-64)	

Template Results - ZIP.bt

Name	Value	Start	Size
struct ZIPDIRENTRY dirEntry	flag.txt	69h	5Ah
char deSignature[4]	PK	69h	4h
ushort deVersionMadeBy	31	6Dh	2h
ushort deVersionToExtract	20	6Fh	2h
ushort deFlags	9	71h	2h
enum COMPTYPE deCompression	COMP_DEFLATE (8)	73h	2h
DOSTIME deFileTime	23:11:58	75h	2h
DOSDATE deFileDate	10/17/2017	77h	2h
uint deCrc	D85703B6h	79h	4h
uint deCompressedSize	51	7Dh	4h

Selected: 2 bytes (Range: 113 [71h] to 114 [72h]) Start: 113 [71h] Sel: 2 [2h] Size: 217 Hex ANSI LQSDN @wringjvt@1

1.zip

traffic\_178d98987b7d6407a2ff0... > 1.zip 搜索"1.zip"

名称	类型	压缩大小	密码保护
flag.txt	文本文档	1 KB	否

压缩(zippped)文件夹错误

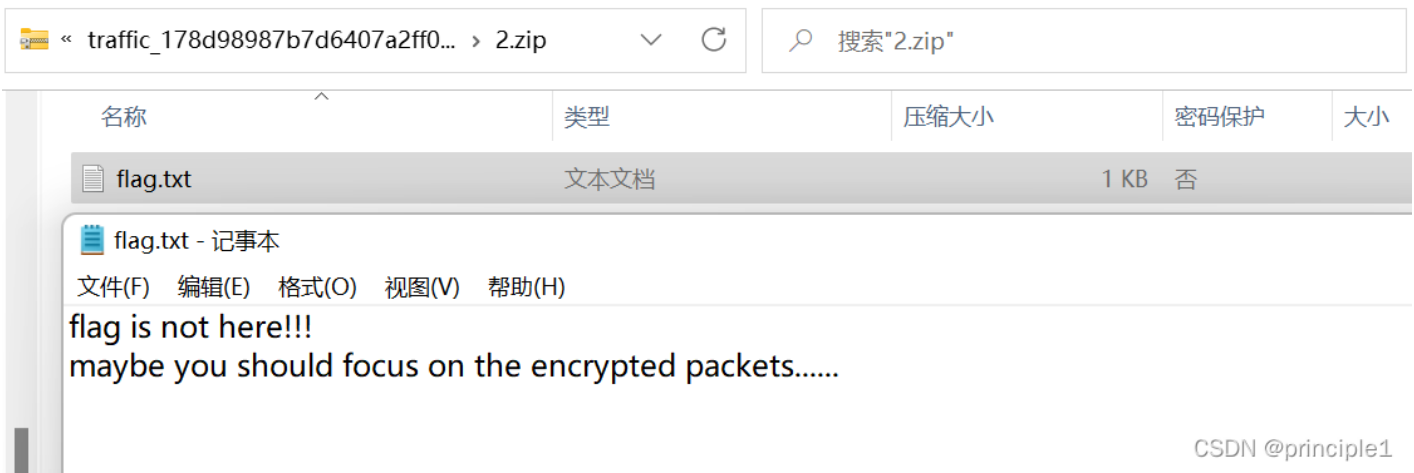
Windows 无法完成提取。  
无法创建目标文件。

确定

CSDN @principle1

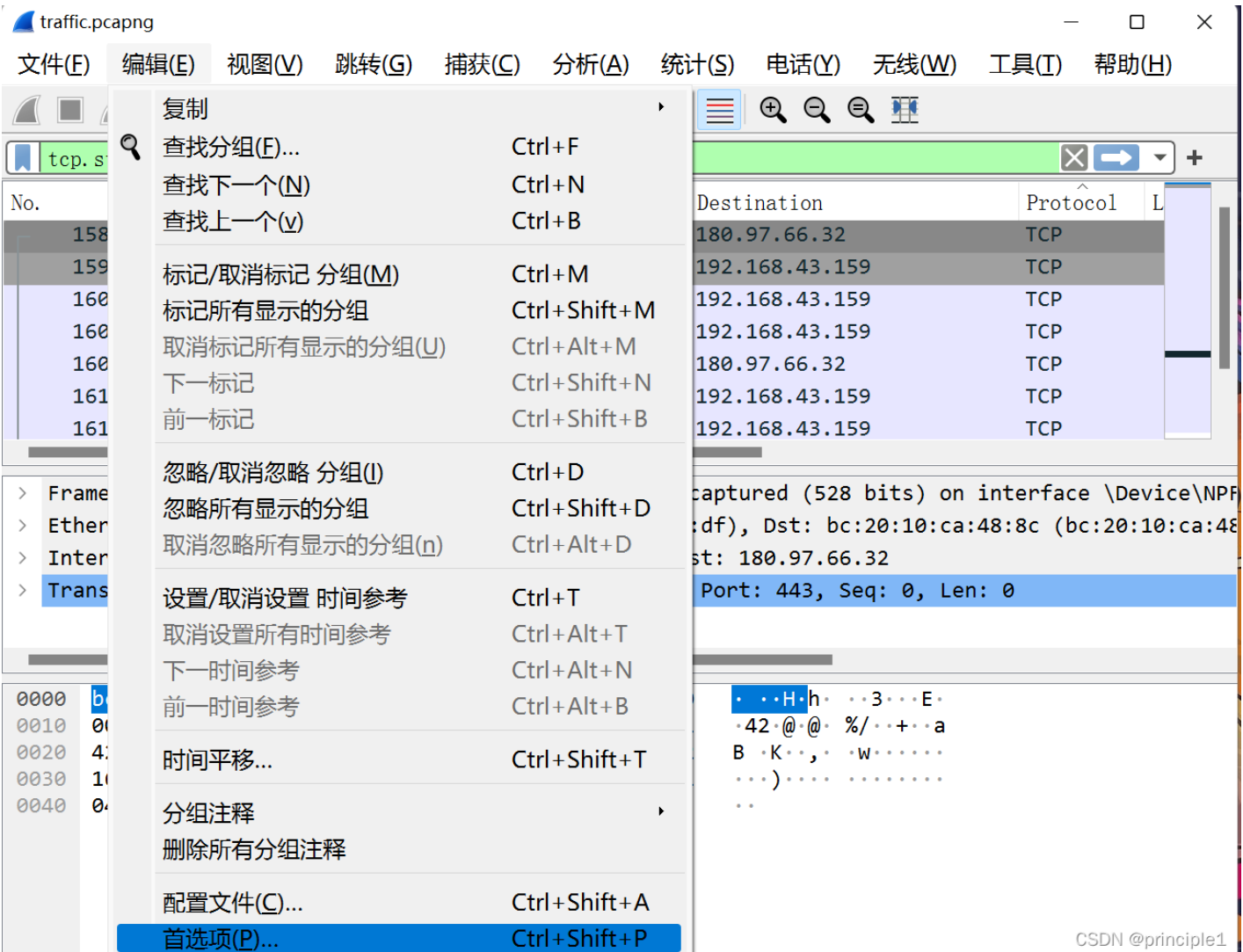
说明1.zip文件不是伪加密，记得把0改成9，还原文件

2.zip

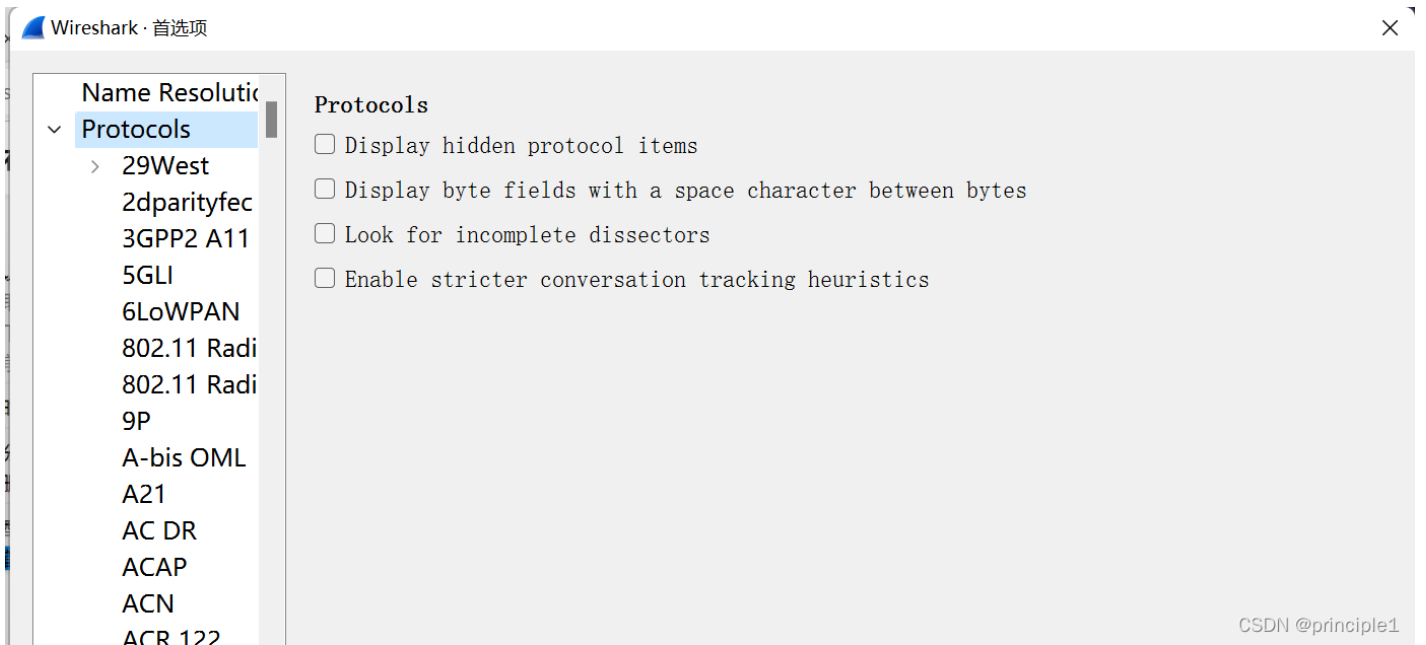


说明 2.zip是伪加密文件，但是该flag.txt中没有flag，然而有提示关注加密包，我们还有一个key.log文件，可以导入wireshark解密https的数据流

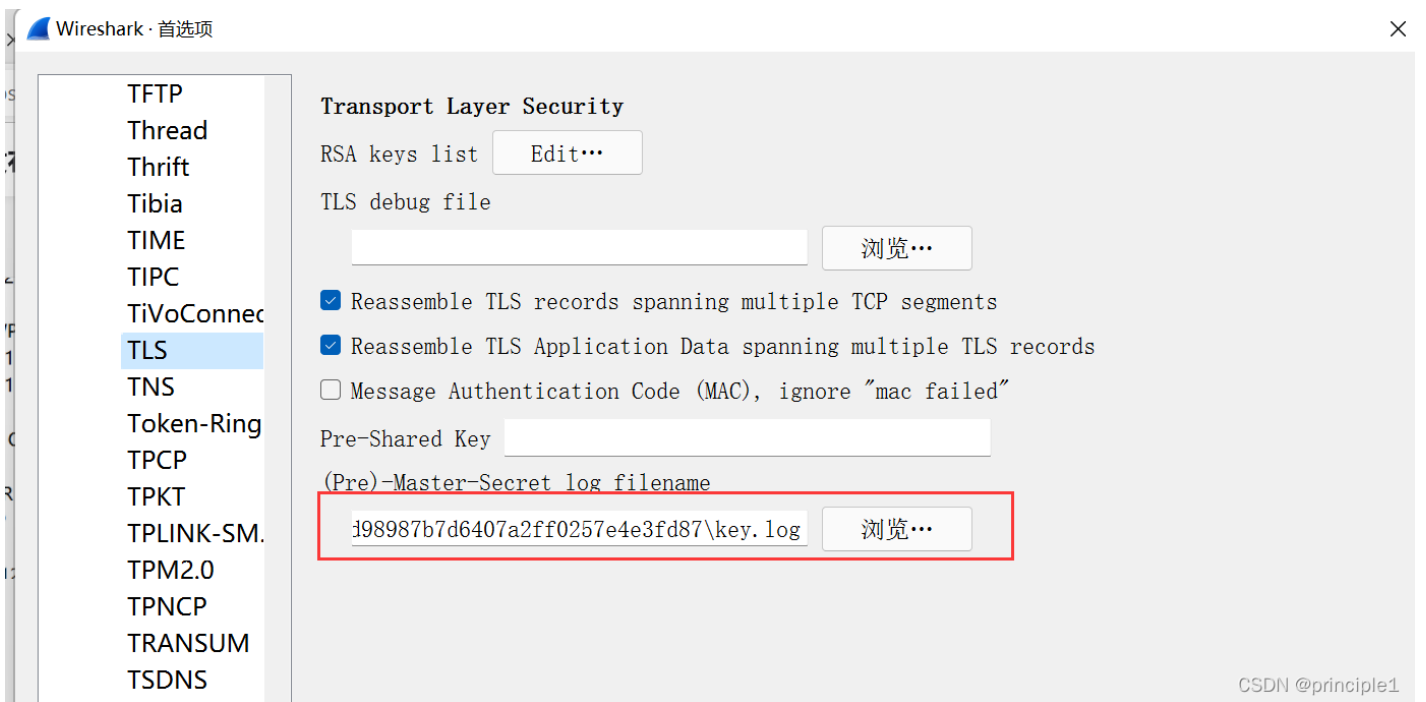
打开wireshark，依次点击 编辑->首选项



点击Protocols，有 SSL 就找 SSL，没有 SSL 就找 TLS



在这里导入下载了的key.log



过滤http，找到一个加密的下载链接，文件名为 music.zip，把该文件保存下来

traffic.pcapng

文件(E) 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(I) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
833	8.321333	180.149.145.242	192.168.43.159	HTTP	282	HTTP/1.1 200 OK (text/html)
843	8.462213	192.168.43.159	220.181.7.165	HTTP	1295	GET /file/e56e57b2ff4745d273ea711004dedf5
848	8.702324	220.181.7.165	192.168.43.159	HTTP	1375	HTTP/1.1 302 Moved Temporarily (text/pla
885	8.915813	192.168.43.159	180.97.34.136	HTTP	1281	GET /file/e56e57b2ff4745d273ea711004dedf5
8005	18.140869	180.97.34.136	192.168.43.159	TLSv1.2	1285	HTTP/1.1 200 OK (application/zip)
8356	50.385888	192.168.43.159	180.97.36.16	HTTP	1261	GET /clientcon.gif?_1508260241787 HTTP/1
8360	50.420583	180.97.36.16	192.168.43.159	HTTP	371	HTTP/1.1 200 OK (GIF89a)
8467	51.082433	192.168.43.159	180.97.36.16	HTTP	1217	GET /clientcon.gif?_1508260242661 HTTP/1

> Transport Layer Security  
> Transport Layer Security  
> [420 Reassembled TLS segments (6849595 bytes): #907(16384), #924(16384), #938(16384), #956(16384), #974(16384), #990(16384), #1005(16384), #  
> Hypertext Transfer Protocol  
> Media Type

```

00000060 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e keep-alive..Con
00000070 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e tent-Dis position
00000080 3a 20 61 74 74 61 63 68 6d 65 6e 74 3b 66 69 6c : attachment;fil
00000090 65 6e 61 6d 65 3d 22 6d 75 73 69 63 2e 7a 69 70 ename="music.zip
000000a0 22 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 ". Content-Lengt
000000b0 68 3a 20 36 38 34 39 30 38 38 0d 0a 43 61 63 68 h: 6849088..Cach
000000c0 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 e-Control: max-a
000000d0 67 65 3d 32 35 39 32 30 30 0d 0a 78 2d 62 73 2d ge=259200..x-bs-
000000e0 63 6c 69 65 6e 74 2d 69 70 3a 20 4e 44 6b 75 4f client-ip: NDKU0
  
```

CSDN @principle1

点击 文件 -> 导出对象 -> HTTP

Wireshark · 导出 · HTTP 对象列表

文本过滤器: | Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
163	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260192995
294	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260193777
359	gt2.baidu.com	image/gif	35 bytes	sp613.gif?t=1508260193005
483	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260194663
629	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260197394
738	hm.baidu.com	image/gif	43 bytes	hm.gif?cc=0&ck=1&cl=24-bit&ds=1920x1080&ep=list_downlo
760	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260199290&_lsix=1&clienttype=0&vmode:
763	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260199293&_lsix=1&clienttype=0&vmode:
767	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260199300&_lsix=1&clienttype=0&vmode:
768	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260199300&_lsix=1&clienttype=0&vmode:
773	pan.baidu.com	application/json	383 bytes	download?sign=XekZm95xrHfLCUvXIEf0PnU6wouCPbG37E2KyC
794	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260199701&_lsix=1&clienttype=0&vmode:
796	hm.baidu.com	image/gif	43 bytes	hm.gif?cc=0&ck=1&cl=24-bit&ds=1920x1080&ep=chromeStra
833	update.pan.baidu.com	text/html	11 bytes	download&ajaxdata=%22success%22
848	d.pcs.baidu.com	text/plain	51 bytes	e56e57b2ff4745d273ea711004dedf58?fid=4145147309-250528
8005	nj02all02.baidupcs.com	application/zip	6849 kB	e56e57b2ff4745d273ea711004dedf58?bkt=p3-00001c02a7abfa
8360	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260241787
8483	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260242661
8866	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260290912
9490	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260323002
9677	imgstat.baidu.com	image/gif	43 bytes	clientcon.gif?_1508260323729
9806	hm.baidu.com	image/gif	43 bytes	hm.gif?cc=0&ck=1&cl=24-bit&ds=1920x1080&ep=list_downlo
9810	pan.baidu.com	image/jpeg	44 bytes	analytics?_lsid=1508260323220&_lsix=1&clienttype=0&vmode:

保存该文件，并命名为 music.zip

CSDN @principle1

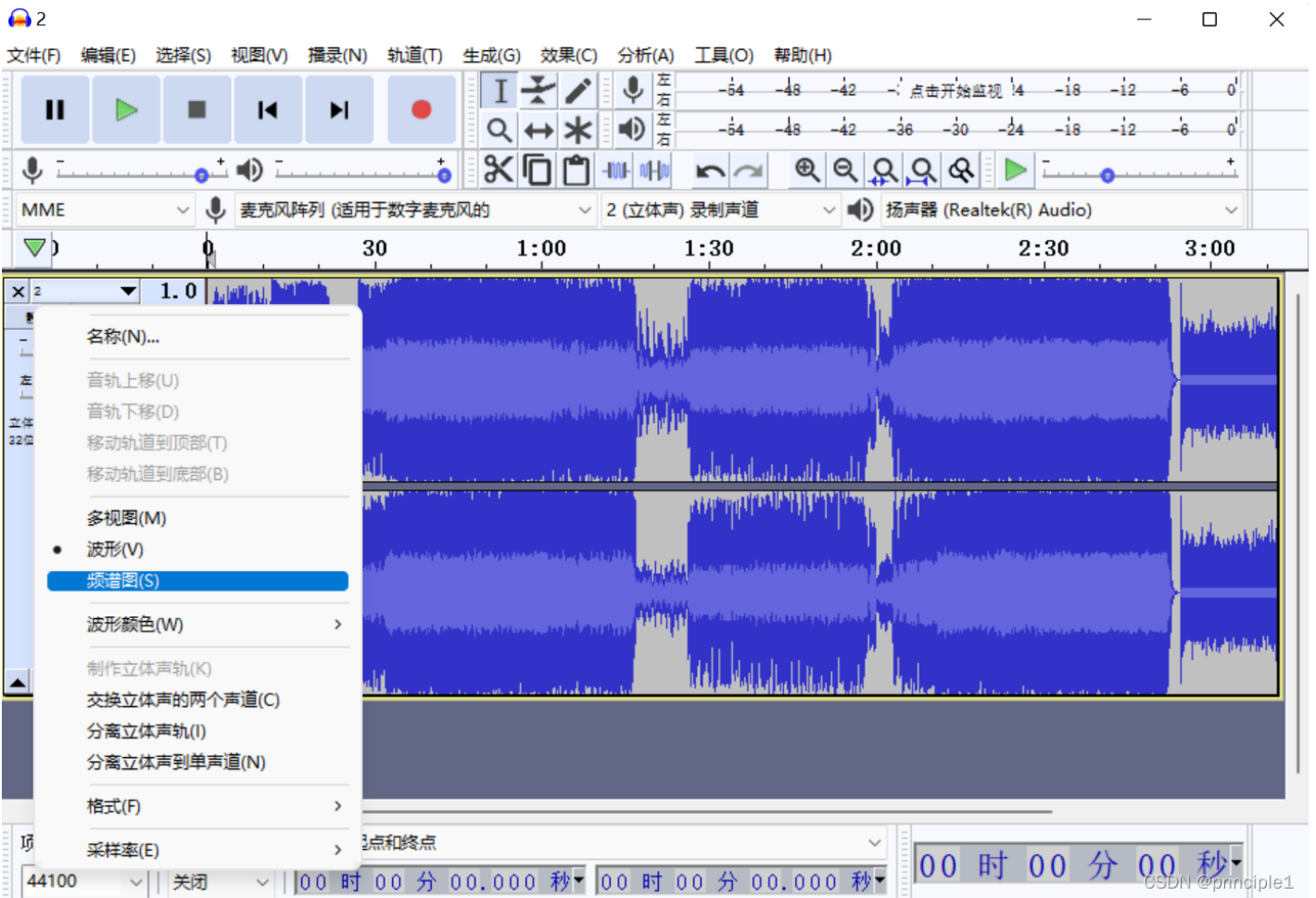
解压后发现是一个音频文件



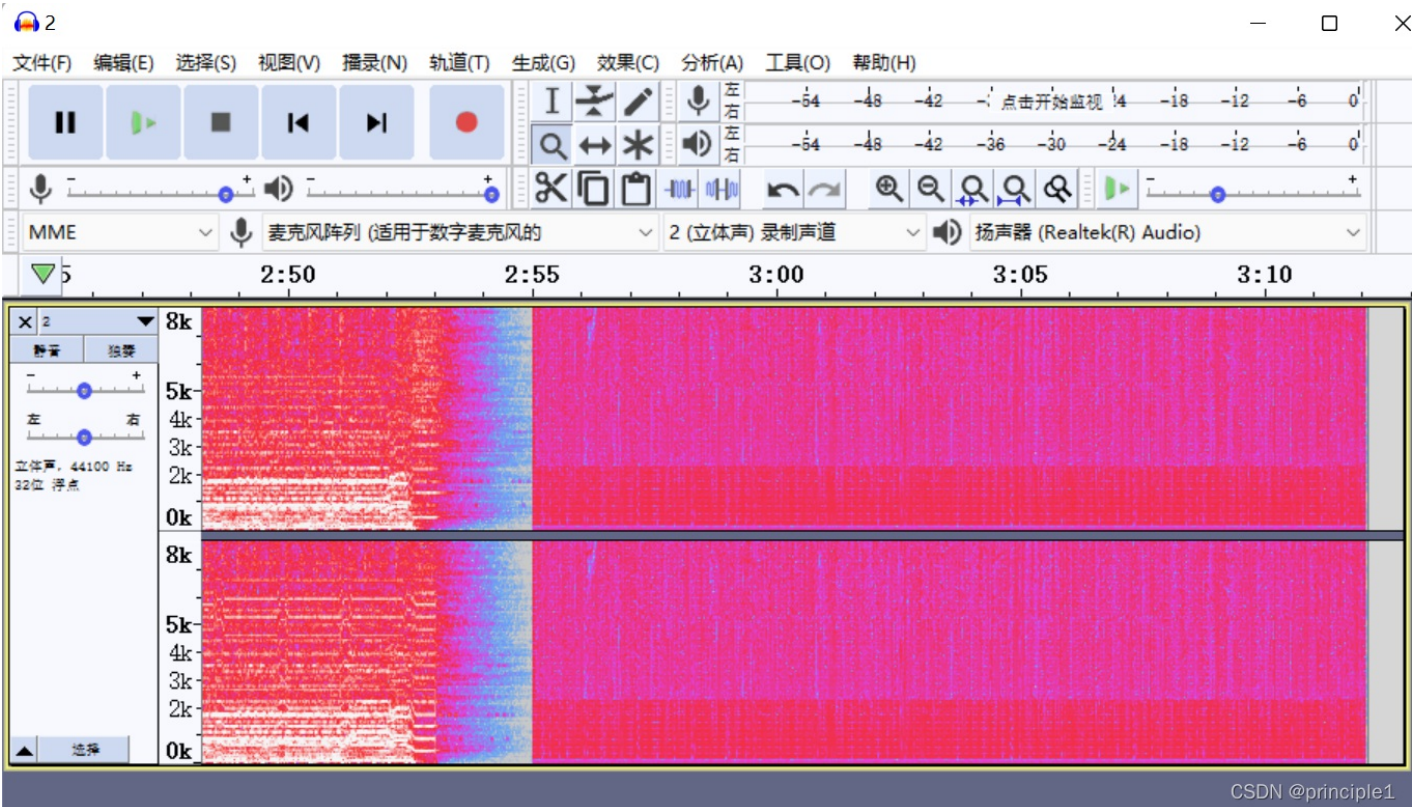
右键属性，发现base64编码，解码是乱码



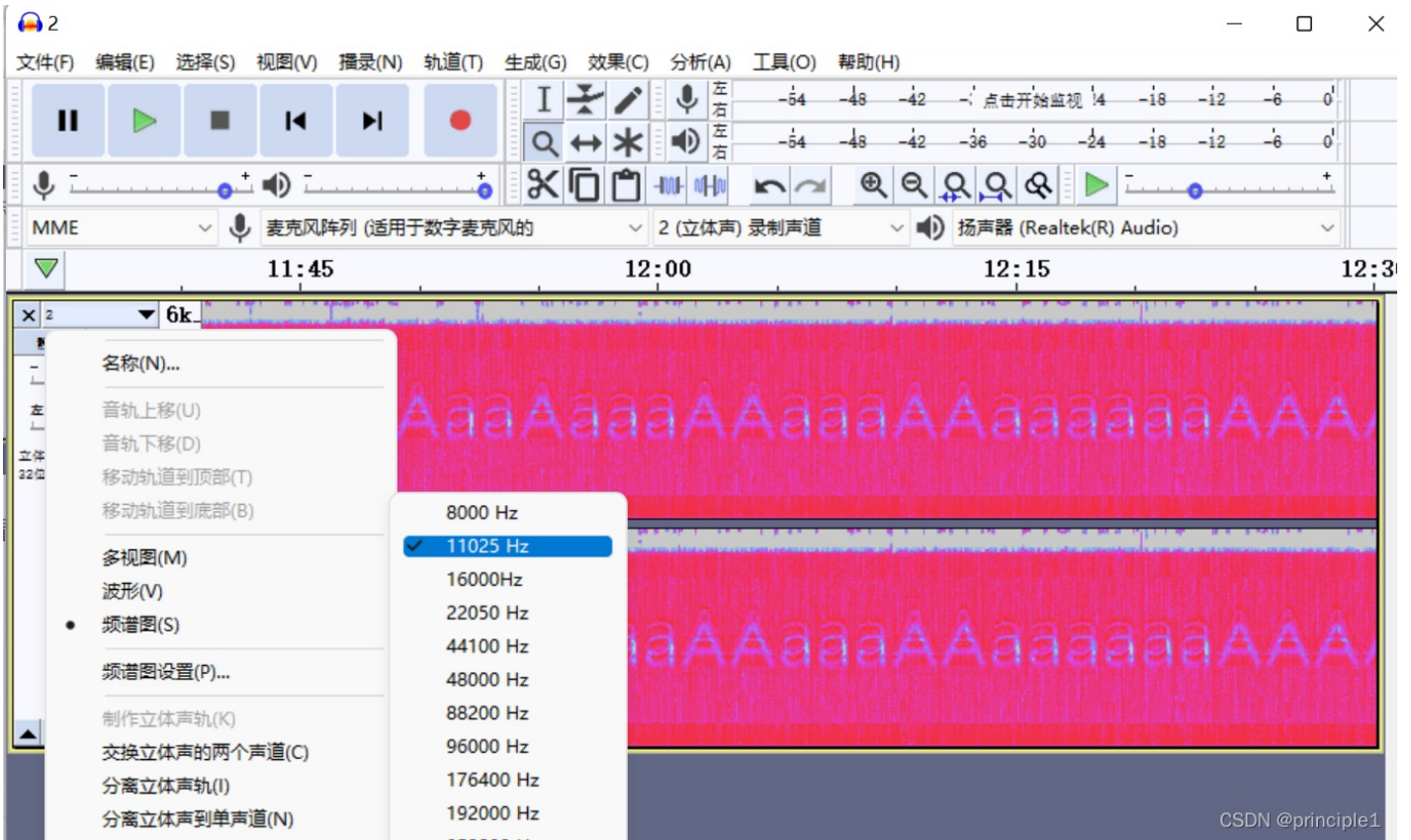
使用 Audacity打开音频，下载地址 ([Download – Audacity](#))，查看频谱图，点击 2 右侧的倒三角，下拉找到频谱图，点击它



听音频发现是后半部分有杂音，可以点击放大镜，左击放大，右击缩小



什么也看不出，可以调节采样率，在找到频谱图的下拉框最下方，从最小的数值开始尝试，发现11025Hz是最清晰的



读取其中内容 (Key: AaaAaaaAAaaaAAaaaaaaAAAAaaaaaa!)

尝试把该密码去解密 1.zip

