高校抗役Writeup-MISC

原创

L.o.W 于 2020-03-10 09:56:36 发布 107 收藏

分类专栏： CTF WriteUp 文章标签： linux 信息安全

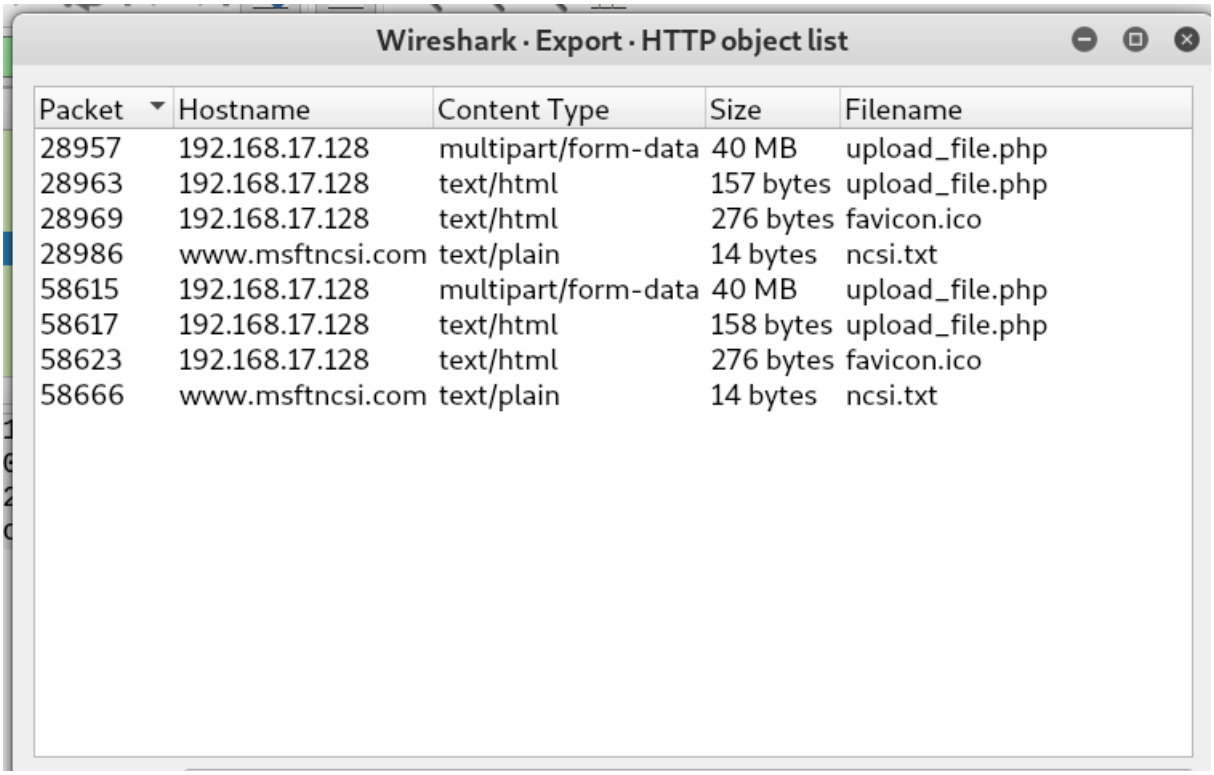
目录

ez_mem&usb

本题考察流量包分析以及内存取证

流量包分析

解压，发现是个流量包，扔进wireshark里，先把HTTP文件倒出来看看



在upload_file.php中发现上传了一个文件

wav | 纯数字.zip | file.None.0xff425090.dat | upload_file.php

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	----------
00000010	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	31	35	34	----------154
00000020	35	35	35	36	32	38	36	37	37	0D	0A	43	6F	6E	74	65	555628677..Conte
00000030	6E	74	2D	44	69	73	70	6F	73	69	74	69	6F	6E	3A	20	nt-Disposition:
00000040	66	6F	72	6D	2D	64	61	74	61	3B	20	6E	61	6D	65	3D	form-data; name=
00000050	22	66	69	6C	65	22	3B	20	66	69	6C	65	6E	61	6D	65	"file"; filename
00000060	3D	22	64	61	74	61	2E	7A	69	70	22	0D	0A	43	6F	6E	="data.zip"..Con
00000070	74	65	6E	74	2D	54	79	70	65	3A	20	61	70	70	6C	69	tent-Type: appli
00000080	63	61	74	69	6F	6E	2F	6F	63	74	65	74	2D	73	74	72	cation/octet-str
00000090	65	61	6D	0D	0A	0D	0A	50	4B	03	04	14	00	00	00	08	eam....PK.....
000000A0	00	07	80	58	50	07	E6	24	20	2D	53	6D	02	00	00	00	..€XP.? -Sm....
000000B0	08	09	00	00	00	64	61	74	61	2E	76	6D	65	6D	EC	5D	.....data.vmem矗
000000C0	0B	5C	53	D7	19	3F	09	08	51	51	52	05	C5	56	5B	5C	.\S?.?..QQR.臬[\
000000D0	69	6B	D7	AE	75	A2	9D	14	ED	40	08	6A	2B	1A	0C	90	ik桩u?..鞫.j+...
000000E0	5A	41	1B	25	18	10	01	E1	5E	83	6D	70	D1	90	CD	34	ZA.%...?^?mp? ?
000000F0	66	73	9B	DB	EC	A6	AB	AD	6E	73	9D	DB	6C	A7	93	4D	fs涳欹猝ns.?1?掮
00000100	AD	51	3B	71	6B	B7	D1	C7	AA	AD	B6	A5	9B	DB	2E	83	璔;qk?亚 顶涳.?
00000110	AE	6C	B5	8A	2D	7A	F7	FF	CE	BD	79	82	16	E7	6F	8F	甽裖-z? 谓y?.?o.
00000120	DF	C6	E5	77	72	CF	E3	7B	9F	73	BE	EF	9C	73	6F	88	咂鋂r?鉶焥掀渟o?
00000130	49	66	5D	94	8E	FE	9E	EE	4A	2A	44	5A	DF	A4	E4	BF	If]?廅炵J*DZ撙淇
00000140	73	89	75	7D	A1	9D	75	15	0F	8B	4C	E6	F7	58	17	FB	s?u}? u..?L?鱔.?
00000150	80	75	8D	1A	CA	FC	F9	DD	AC	2B	1B	69	B4	86	1D	CF	€..庶 ? .i碰.?
00000160	F8	33	EB	5A	80	FC	AE	4F	DC	FF	97	97	DF	43	1E	34	? 隡€甍? 棗逆.4
00000170	FE	FE	27	D6	55	7D	29	44	7F	47	17	EB	7A	77	2D	EB	?U})D.G.?zw-?

除去文件头和文件尾，保存为data.zip

wav | 纯数字.zip | file.None.0xff425090.dat | data.zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	14	00	00	00	08	00	07	80	58	50	07	E6	PK.....€XP.?
00000010	24	20	2D	53	6D	02	00	00	00	08	09	00	00	00	64	61	$ -Sm.....da
00000020	74	61	2E	76	6D	65	6D	EC	5D	0B	5C	53	D7	19	3F	09	ta.vmem?].\S? ?.
00000030	08	51	51	52	05	C5	56	5B	5C	69	6B	D7	AE	75	A2	9D	.QQR.?V[\ik?畊?
00000040	14	ED	40	08	6A	2B	1A	0C	90	5A	41	1B	25	18	10	01	.?@.j+...ZA.%...
00000050	E1	5E	83	6D	70	D1	90	CD	34	66	73	9B	DB	EC	A6	AB	醱僎p?.?4fs?垭八
00000060	AD	6E	73	9D	DB	6C	A7	93	4D	AD	51	3B	71	6B	B7	D1	璶s.踠 M?Q;qk费
00000070	C7	AA	AD	B6	A5	9B	DB	2E	83	AE	6C	B5	8A	2D	7A	F7	仟瑮 ? 儹1?? z?
00000080	FF	CE	BD	79	82	16	E7	6F	8F	DF	C6	E5	77	72	CF	E3	統? 鏾.?棋wr香
00000090	7B	9F	73	BE	EF	9C	73	6F	88	49	66	5D	94	8E	FE	9E	{?s?餃so圛f]攻鵑
000000A0	EE	4A	2A	44	5A	DF	A4	E4	BF	73	89	75	7D	A1	9D	75	頑*DZ?ゃ縮塽}?.u
000000B0	15	0F	8B	4C	E6	F7	58	17	FB	80	75	8D	1A	CA	FC	F9	..婂骥X.龕u..?
000000C0	DD	AC	2B	1B	69	B4	86	1D	CF	F8	33	EB	5A	80	FC	AE	莠+.i?? 哮3?Z€
000000D0	4F	DC	FF	97	97	DF	43	1E	34	FE	FE	27	D6	55	7D	29	O? 槭C.4?? 謁})
000000E0	44	7F	47	17	EB	7A	77	2D	EB	BA	77	24	F3	13	AD	FF	D.G.矲w-牒w$? ?
000000F0	64	7A	FA	FF	FB	FF	42	77	2B	64	5A	76	FB	BF	5F	1F	dz ? Bw+dZv眨

```
00000100  F6 31 57 5F 38 79 43 43  72 4E FA 3B EB FA FD 07  ? W_8yCCrN? 膪?
00000110  A1 B6 E4 91 F7 FF 45 44  DF 6D B8 EB FE BF 50 62  《鏡? ED適鴿  Pb
00000120  03 D7 7F E7 65 D1 67 0F  A5 FB 48 F6 AD 18 C6 FE  .?.?e?g.  H?? 掐
00000130  14 2F CB E3 DF BB ED CD  9B 59 27 63 EF DD C6 D8  ./算呋硗沈'c镙曝
00000140  9B 3F 8B 77 31 2D DA 1D  04 A4 8B D3 E1 53 C3 B2  ? 嫂1-? .?嶝醑貌
00000150  98 46 2B CB 8C FD 34 9E  B1 3C 76 44 43 A5 58 76  椤+?岩4?? vDC?Xv
```

```
026D5240  C4 C7 24 97 6E 3B CF 3B  E9 A5 E7 BC B8 89 3A E9  那$?n;?·楗缠笁:?
026D5250  14 AE 14 AC 7E 52 0F 99  1C 43 2D 6D 43 FD 9D 4B  .?.?~R.?.C-mC?.K
026D5260  D8 0F C4 74 42 3E AA 26  D5 58 4C CF B7 3F 44 54  ??膻B>??詼L???DT
026D5270  6E 31 CB 82 83 9B 94 81  77 99 15 09 64 42 11 CF  n1蔥儹?·w?..dB.?
026D5280  11 C5 A0 B1 22 8A 95 5C  6C 7A 31 A3 00 25 D0 AD  .?杭"?晒1z1?.%协
026D5290  8E 75 76 6A 30 EE 2C BF  0D D4 C1 36 ED 10 F7 3C  嶵vj0?,?.????孓?T
026D52A0  5D 31 08 C8 11 E1 14 84  93 B8 07 3C 48 C2 72 F8  ]1.?.?.?摳.<H?r?
026D52B0  3B C2 1E B2 FE D2 83 73  3E 0E E7 E4 E2 0D CB F2  ;?.?  傮>.玟?%蓑
026D52C0  53 16 87 74 DC 41 97 C3  BA 39 C0 3A 96 45 A8 B7  S.嗋鼟槲????胯ǔT
026D52D0  A9 F4 98 92 B8 4D D8 4E  94 64 CE 4D 50 3D DD 28  ?寰窶豐摝蜂P=??
026D52E0  0A D9 57 1B 59 32 C8 C9  8F A8 32 98 2B 59 B9 0C  .?W.Y2壬.?2?+Y?淒
026D52F0  FC AB E8 7B D9 86 00 D7  31 4D 74 92 B6 E5 01 08  ?鑽賦.?1Mt?跺..
026D5300  84 4F F1 18 D2 15 A3 67  C4 1F CC 96 54 BA 6C 49  凧?霅?孹 ?劃號T?1I
026D5310  B3 8E DA 23 EC 35 1E A9  09 38 36 12 5B D2 C1 9E  硯?.?2.?.86.[?掠
026D5320  16 4E 18 14 EB 4E D9 D5  02 18 5E A0 3F 46 6F BE  .N..隢僬..^??Fo?
026D5330  D6 0D EA 46 A7 80 2D 7C  07 84 95 F0 A3 9F 4A D6  ?汎闆  -|.?鬱  J?
026D5340  D8 81 81 84 2C AF C8 2A  05 4B 55 7B 30 38 2A 74  ?覓.?,???.KU{08*t
026D5350  2F 0A FD 00 50 4B 01 02  3F 00 14 00 00 00 08 00  /.?.PK..?.......
026D5360  07 80 58 50 07 E6 24 20  2D 53 6D 02 00 00 00 08  .€XP.?$ -Sm.....
026D5370  09 00 24 00 00 00 00 00  00 00 20 00 00 00 00 00  ..$.....  .....
026D5380  00 00 64 61 74 61 2E 76  6D 65 6D 0A 00 20 00 00  ..data.vmem.. ..
026D5390  00 00 00 01 00 18 00 78  5E B5 70 E8 EA D5 01 78  .......x^?p?暾.x
026D53A0  5E B5 70 E8 EA D5 01 17  D8 42 70 E8 EA D5 01 50  ^?p?暾..舀p?暾.P
026D53B0  4B 05 06 00 00 00 00 01  00 01 00 5B 00 00 00 54  K..........[...T
026D53C0  53 6D 02 00 00 0D 0A                             Sm.....
```

解压，得到一个data.vmem

内存取证

我们使用kali linux 中的volatility来进行内存取证

1. 首先判断操作系统类型

```
volatility imageinfo -f data.vmem
```

```
root@kali:~/ctf/misc/ez_mem&usb# volatility imageinfo -f data.vmem
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/ctf/misc/ez_mem&usb/data.vmem)
                      PAE type : PAE
                           DTB : 0xb18000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-02-24 07:56:47 UTC+0000
     Image local date and time : 2020-02-24 15:56:47 +0800
```


2. 查看进程

> volatility -f data.vmem --profile=WinXPSP2x86 pslist

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ -----
---------------
0x80ea2660 System                    4      0     52      231 ------      0

0xff57fc28 smss.exe                372      4      3       19 ------      0 2020-02-23 13:17:13 UTC+0000

0xff432020 csrss.exe               464    372     12      317      0      0 2020-02-23 13:17:13 UTC+0000

0xff435020 winlogon.exe            492    372     20      501      0      0 2020-02-23 13:17:13 UTC+0000

0xff445020 services.exe            668    492     16      253      0      0 2020-02-23 13:17:14 UTC+0000

0xff46b020 lsass.exe               680    492     19      309      0      0 2020-02-23 13:17:14 UTC+0000

0xff510bf0 vmacthlp.exe            836    668      1       25      0      0 2020-02-23 13:17:14 UTC+0000

0xff493568 svchost.exe             848    668     14      189      0      0 2020-02-23 13:17:14 UTC+0000
```


3. 提取命令历史记录

> volatility -f data.vmem --profile=WinXPSP2x86 cmdscan

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 464
CommandHistory: 0x556bb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x504
Cmd #0 @ 0x3609ea0: passwd:weak_auth_top100
Cmd #1 @ 0x5576d0: start wireshark
Cmd #13 @ 0x9f009f: ??
Cmd #41 @ 0x9f003f: ?\?????????
```


4. . 通过cmdline查看命令行用到的参数，不过似乎没有什么重要信息

> volatility -f data.vmem --profile=WinXPSP2x86 cmdline

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 cmdline
Volatility Foundation Volatility Framework 2.6
**************************************************************************
System pid:      4
**************************************************************************
smss.exe pid:    372
Command line : \SystemRoot\System32\smss.exe
**************************************************************************
csrss.exe pid:    464
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemTyp
e=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,
2 ProfileControl=Off MaxRequestThreads=16
**************************************************************************
winlogon.exe pid:    492
Command line : winlogon.exe
**************************************************************************
services.exe pid:    668
Command line : C:\WINDOWS\system32\services.exe
**************************************************************************
lsass.exe pid:    680
Command line : C:\WINDOWS\system32\lsass.exe
```


5. 查看文件目录，看看有没有flag文件

> volatility -f data.vmem --profile=WinXPSP2x86 filescan | grep flag

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 filescan | grep flag
Volatility Foundation Volatility Framework 2.6
0x0000000001155f90      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\flag.img
```

6. 导出文件

> volatility -f data.vmem --profile=WinXPSP2x86 dumpfiles -Q 0x1155f90 --dump-dir=./

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 dumpfiles -Q 0x1155f90 --dump-dir=./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x01155f90   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\flag.img
```

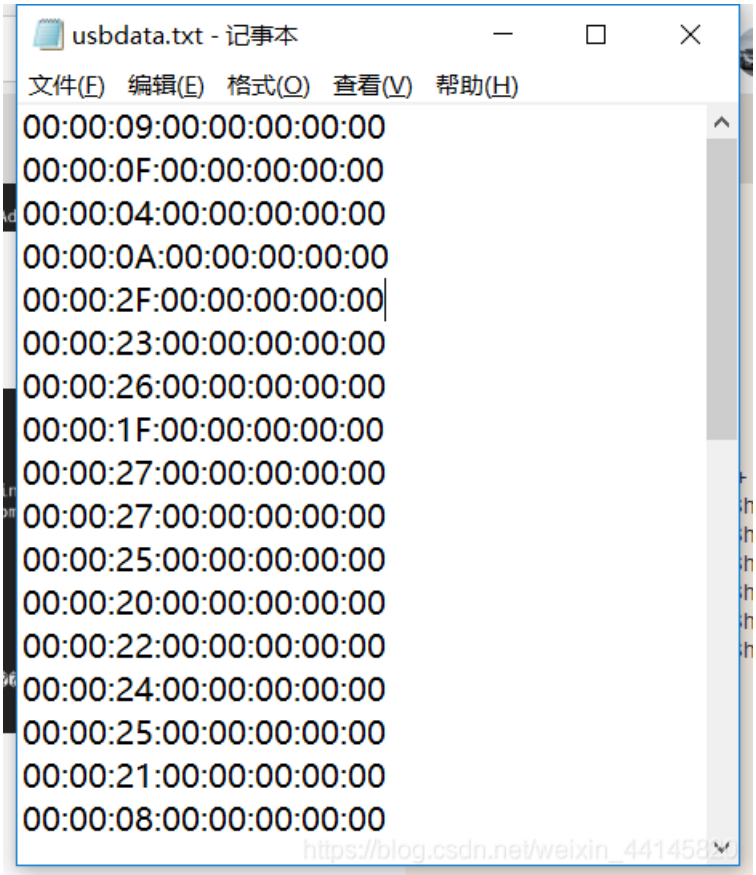
直接用binwalk和foremost提取出文件

```
root@kali:~/ctf/misc/ez_mem&usb# binwalk flag.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
19412         0x4BD4          Copyright string: "Copyright (C) 1994-2013 H. Peter Anvin et al"
62464         0xF400          Zip archive data, encrypted at least v2.0 to extract, compressed size: 111, uncompressed si
ze: 912, name: usbdata.txt
62709         0xF4F5          End of Zip archive, footer length: 22

root@kali:~/ctf/misc/ez_mem&usb# foremost flag.img
Processing: flag.img
|foundat=usbdata.txt
                              G
N&5=
       p
*|
```


提取出一个加密的压缩包，回想起之前查看命令行记录看见的信息，故压缩包密码为 `weak_auth_top100`

```
root@kali:~/ctf/misc/ez_mem&usb# volatility -f data.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 464
CommandHistory: 0x556bb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x504
Cmd #0 @ 0x3609ea0: passwd:weak_auth_top100
Cmd #1 @ 0x5576d0: start wireshark
Cmd #13 @ 0x9f009f: ??
Cmd #41 @ 0x9f003f: ?\?????????
```


解压之后发现如下文件

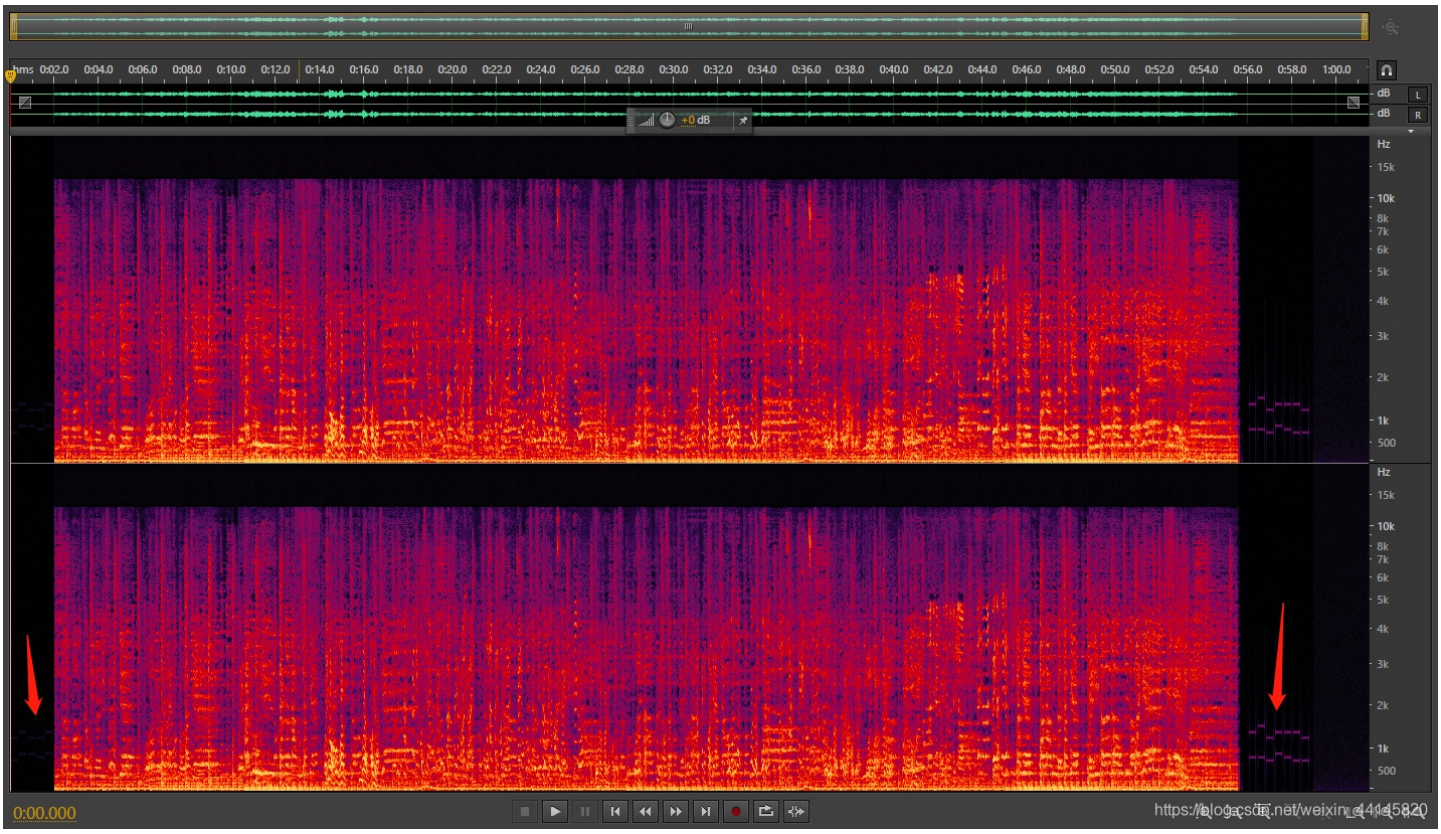


根据文件名usbdata，怀疑是抓到的键盘传输的数据包，使用以下脚本获得flag

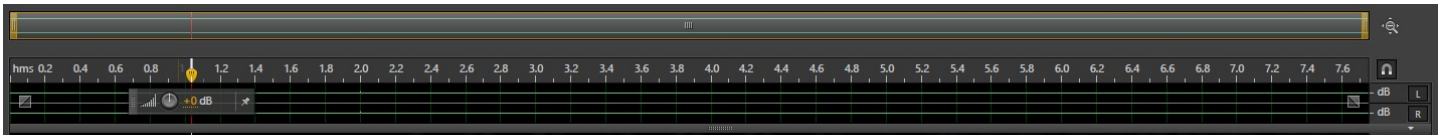
```
hids_codes = {"0x04":"a","0x05":"b","0x06":"c","0x07":"d","0x08":"e","0x09":"f","0x0A":"g","0x0B":"h","0x0C":"i"
,"0x0D":"j","0x0E":"k","0x0F":"l","0x10":"m","0x11":"n","0x12":"o","0x13":"p","0x14":"q","0x15":"r","0x16":"s","
0x17":"t","0x18":"u","0x19":"v","0x1A":"w","0x1B":"x","0x1C":"y","0x1D":"z","0x1E":"1","0x1F":"2","0x20":"3","0x
21":"4","0x22":"5","0x23":"6","0x24":"7","0x25":"8","0x26":"9","0x27":"0","0x36":",","0x33":":","0x28":"\n","0x2
C":" ","0x2D":"_","0x2E":"=","0x2F":"{","0x30":"}"}


flag = ''

file = open('/root/ctf/misc/usbdata.txt','r')
for line in file.readlines():
    conv = '0x' + line.split(':')[2].upper()
    if conv in hids_codes:
        if line[0:2] == '00':
            flag += hids_codes[conv]
        else:
            flag += hids_codes[conv].upper()


print(flag)
```

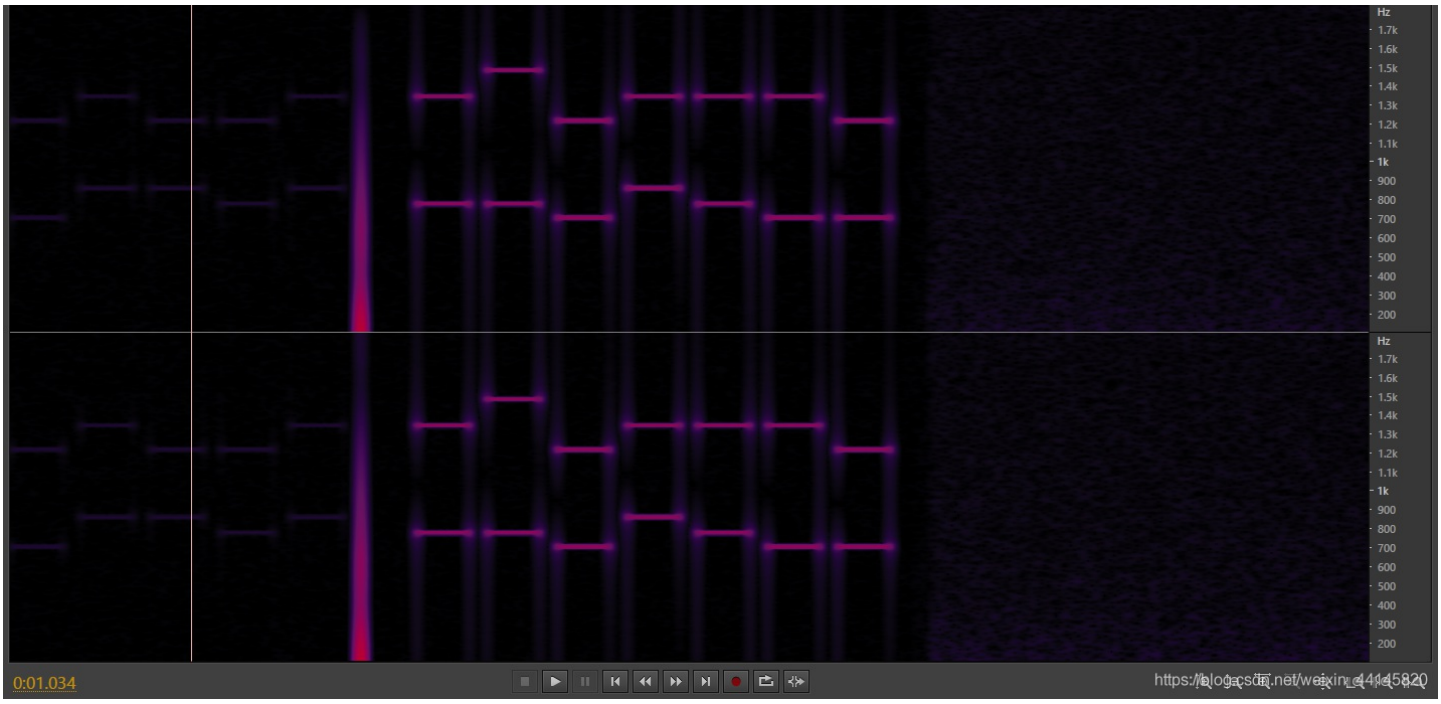
隐藏的信息

使用AU打开WAV文件（这里的压缩包用了伪加密，使用360压缩可以直接解压）
发现了开头和结尾有声音，开头听不出来，结尾可以听出是电话的按键声（DTMF）



把音乐开头和结尾的DTMF信号提取出来

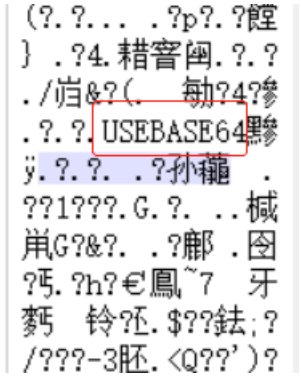


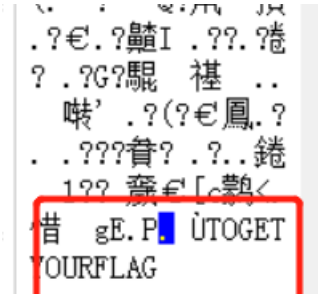


根据下面的表对比得到12个数字：`187485618521`

低群/Hz	高群/Hz			
	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

在二维码中发现提示：





把得到的数字用base64加密得到flag：`MTg3NDg1NjE4NTIx`