

BUUCTF: USB

原创

末初 于 2020-11-11 22:38:16 发布 1356 收藏 6

分类专栏: [CTF_MISC_Writeup](#)

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/mochu7777777/article/details/109632626>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

<https://buuoj.cn/challenges#USB>

Challenge 210 Solves

USB

1

Do your konw usb?? 注意: 得到的 flag 请包上 flag{} 提交

8c90b141-7...

Flag Submit

<https://blog.csdn.net/mochu7777777>

名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期	压缩方法	加密方法	属性	注释
233.rar	1,618,358	1,618,108	RAR 压缩文件	a1a34620	2018/1/5 15:21:25	Deflate		A_	
key.ftm	11,939	90,144	FamiTracker.M...	78531f3f	2018/1/5 15:43:38	Deflate		A_	

使用 010 Editor 打开 key.ftm, 搜索关键词 key, 有很多 key 的关键词, 但在其中发现 zip 数据

233.rar key.ftm x

编辑方式: 十六进制(H) 运行脚本 运行模板

地址	十六进制	ASCII
9C30h	00 00 00 00
9C40h	00 00 00 00
9C50h	00 00 00 00
9C60h	00 00 00 00PK.....
9C70h	7C 25 4C 02 26 D9 AC 7E 11 00 00 86 91 00 00 08	%L.εÜ~...t'....
9C80h	00 00 00 6B 65 79 2E 70 63 61 70 95 DD 0B 94 55	...key.pcap*Y."U
9C90h	53 1C C7 F1 73 EF 6D 9A A6 C7 14 52 84 8C 54 22	S.Çñsĩmš!Ç.R„ET"
9CA0h	25 7A 50 94 92 4A 29 95 24 E9 41 25 F2 28 A5 A7	%zP"/J)*\$éA%ò(¥\$
9CB0h	24 99 5E 0A BD 24 2A 45 A8 44 0C 95 47 24 8F 92	\$™^.%\$*E"D.·G\$.'
9CC0h	22 52 14 85 9E 22 22 93 68 9E 77 AE 7D CF 39 66	"R...ž""hžw@)İ9f
9CD0h	FF AC C5 5A DF DD 3A C3 58 FA AD CF FF BF CF B9	ÿ-ÀZBÝ:ÄXú-İÿçİ¹
9CE0h	8F B9 F7 BF E7 7E B5 6E C5 A2 A8 57 C2 FB E7 4F	.³÷ç~µnÃc'WÂûçO
9CF0h	22 E1 79 79 E6 DF F1 73 3B DE F8 C6 55 25 BD B3	"áyyæßñs;PøEU%²º
9D00h	CD F7 C9 AF D3 BC 9B 9B E4 0C 9F 36 C1 FC 7F F3	Í-É-Ó+>>ã.Ý6Äü.ó
9D10h	27 CD 8B 44 BC 88 F7 60 A4 54 F2 BF A2 E6 08 23	'Í<D4^÷~Tòçæ.#
9D20h	63 3B 69 A4 42 C6 FF 45 22 E6 08 23 DE 0D 4C 89	c;iæBËÿE"æ.#P.L&
9D30h	24 CC F7 89 44 32 F2 CA 6D 4C 91 C2 26 DF CD 14	\$Í÷%D2òÈmL'Â&ßÍ.
9D40h	AF 28 F9 E5 2B 9D 46 32 45 7A 29 FF 00 53 A2 09	-(ùã+.F2Ez)ÿ.Sc.
9D50h	2F 1A F6 12 9D CC 14 89 7C 39 8D 29 52 D8 73 73	/..ö..İ.%. 9.)R0ss
9D60h	9C 95 EB 16 3A 2B 57 2E 61 4A A4 C8 7C 1F 2C F2	æ.e.:+W.aJHÈ .,ð
9D70h	49 AF 40 C5 9E FD BD AF 33 45 CE FE A6 77 9D 95	I_@Äžÿ%³3Eİp w.·
9D80h	07 3E 82 8A 5D B1 C6 9F 41 C5 B6 5F 63 3B 54 6C	.>.,š]±ÈÿAÄq_c;Tl
9D90h	2F C7 BF 63 4A B4 C8 44 02 65 E9 0F CE CA BC 5F	/ÇçcJ'ÈD.eé.ÎÈ%4
9DA0h	99 22 2B D6 EF 4F A6 48 A4 7E 21 53 64 91 F7 C4	™™+ÖİO;Hæ~!Sd'+Ä
9DB0h	52 99 62 2F CB 0D 65 52 99 62 57 6C E2 49 CE 4A	R™b/È.eR™bWlâIİJ
9DC0h	8F D3 A0 62 7B 69 70 B6 B3 D2 B8 3E 53 64 91 4B	.ó b(ipq'ò,>Sd'K
9DD0h	5C 0A 15 1B B9 E5 0A A6 C8 05 B3 39 8B 29 09 73	\...³ã.¡È.²9<).s
9DE0h	24 82 C8 B4 F7 98 92 CC 84 85 B5 FA 18 2A 09 73	\$,È'÷''İ,...µú.*.s
9DF0h	04 91 94 2D 4C 91 C2 36 ED 86 8A 8D B4 3B E2 AC	.''-L'Â6i+š.';ã-
9E00h	FC 18 67 8A B4 9F 95 52 CA 55 19 5F AE 14 52 8A	ü.gš'ÿ·RËU. @.Rš
9E10h	CC 11 46 6A 9F C1 14 89 44 6A 30 45 0A DB DD C0	İ.FjÿÄ.¾Dj0E.ÛÿÄ
9E20h	59 D9 7A 19 53 24 72 D9 95 4C 91 C2 EA B4 77 56	YÜz.S\$ÿÜ·L'Âê'wV
9E30h	BE EE E2 AC BC D8 83 29 12 B9 BF 1F 53 A4 B0 76	%iã-+øf).²ç.Sæ°v
9E40h	77 42 25 79 CB 8F 98 91 0A 43 A1 62 1E C3 C2 C8	wB%ÿË.ø'.C;b.ÄÄÈ
9E50h	DE D1 4C 89 9B BF 1E 46 36 64 32 45 0A 1B 37 95	BñL%>ç.F6d2E..7·

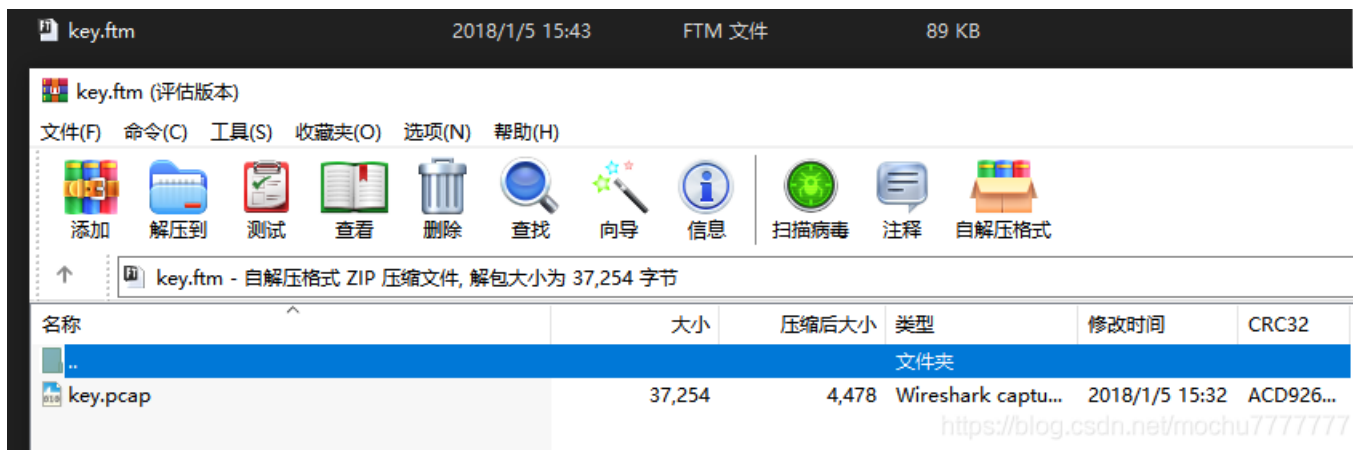
查找结果

地址	值
9975h	key
9987h	key
9C83h	key
AE37h	key
C500h	KEY
D5B0h	KEY
EB6Bh	KEY
FC1Bh	KEY
11EA9h	key
16 12359h	key

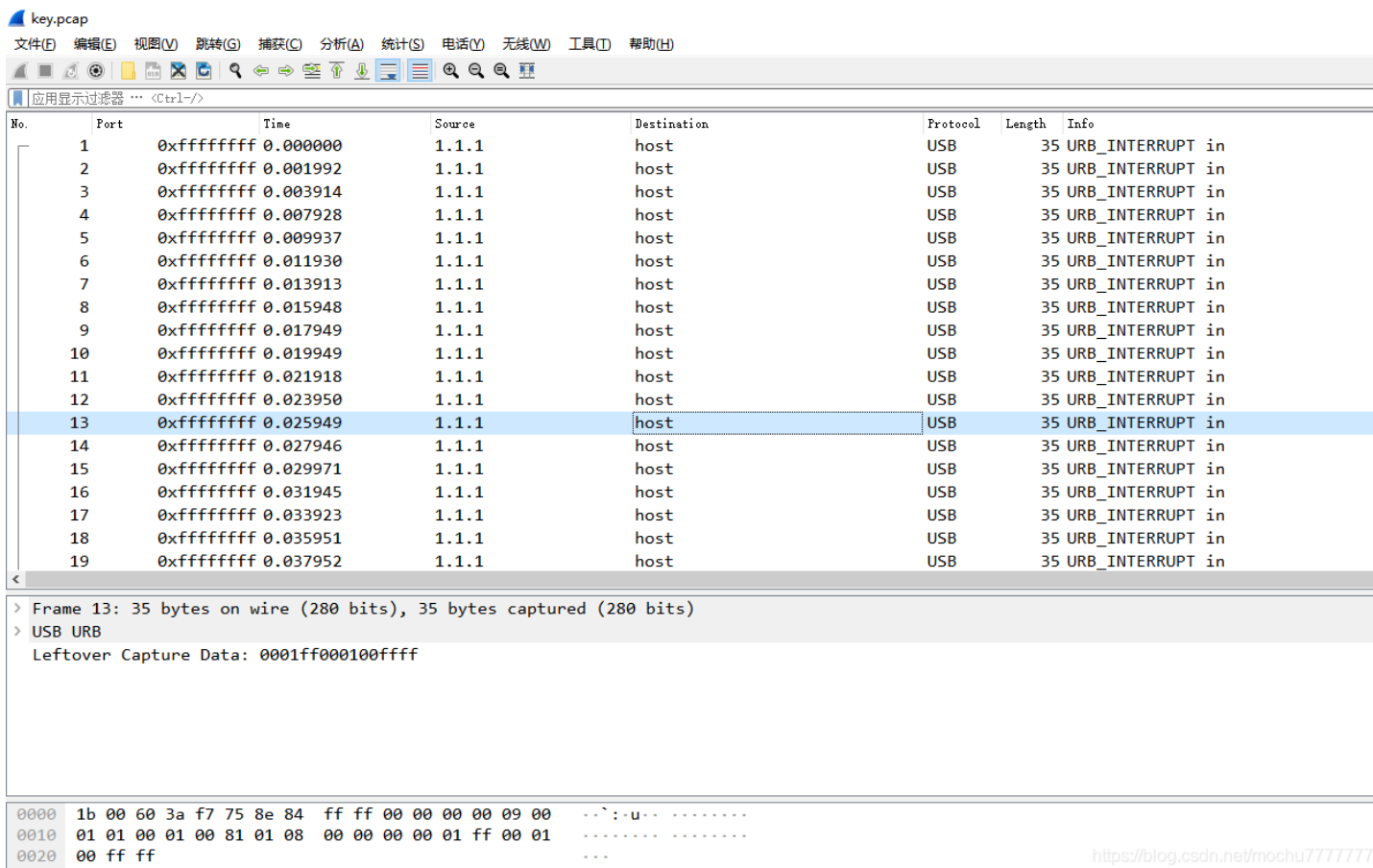
输出 查找结果 多文件中查找 比较 直方图 校验和 进程

https://blog.csdn.net/mechu77777777
开始: 40097 [9C63h] | 选定: 4835 [121Bh]

将 zip 数据另存出来，里面是一个 key.pcap，直接可以解压，或者使用 WinRAR 直接打开 key.ftm，直接可以得到 key.pcap



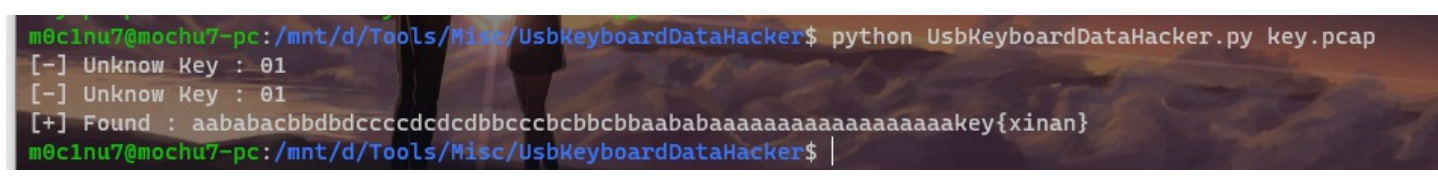
<https://blog.csdn.net/mochu777777>



<https://blog.csdn.net/mochu777777>

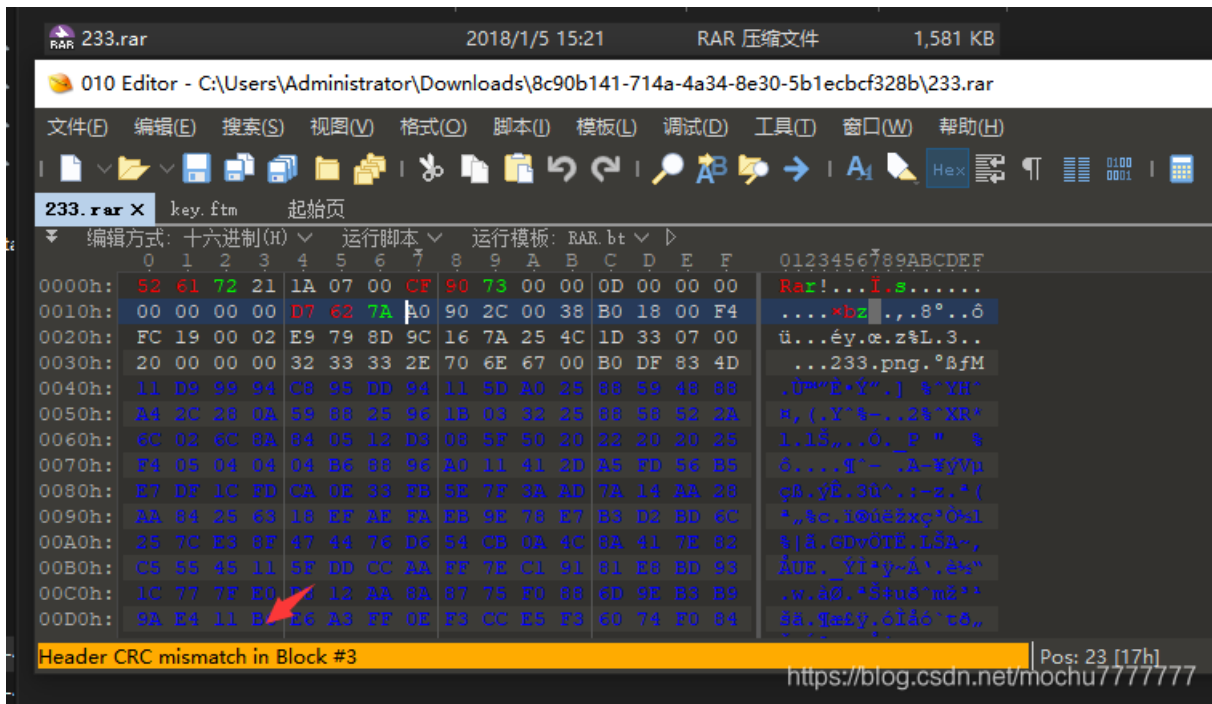
USB数据包，直接使用 `UsbKeyboardDataHacker` 脚本提取内容

<https://github.com/WangYihang/UsbKeyboardDataHacker>



得到内容: `xinan`

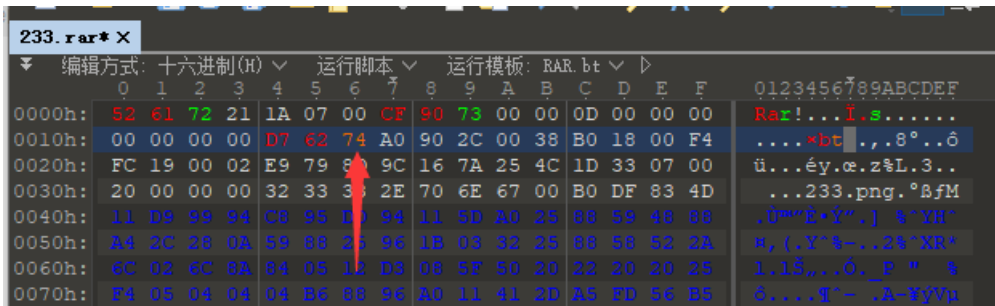
接着使用 `010 Editor` 打开 `233.rar`



CRC报错，报错信息显示是文件的第三个块，RAR结构有四个块：标记块、归档头部块、文件块、结束块

分析RAR文件结构，发现文件块的位置应该是74并不是7A，修改为74后保存

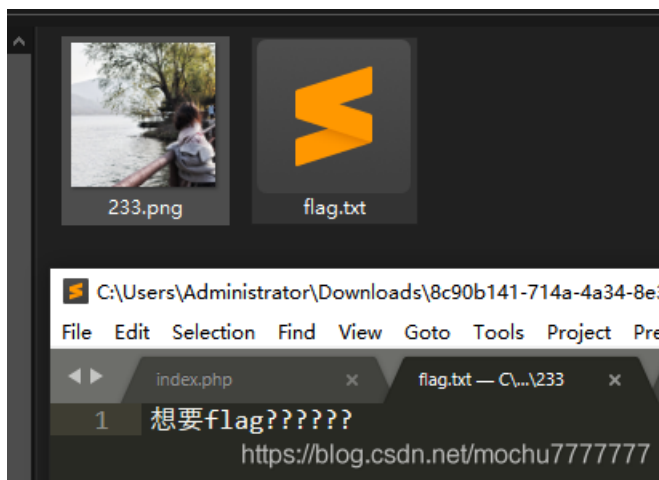
RAR文件结构分析参考：<https://www.freebuf.com/column/199854.html>



即可正常解压

名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
233.png	1,617,976	1,703,156	PNG 文件	9c8d79e9	2018/1/5 15:16:44
flag.txt	16	16	TXT 文件	8ff282b3	2018/1/5 15:19:52

<https://blog.csdn.net/mochu7777777>



Stegsolve 打开 233.png 在 Blue 0 通道发现二维码



<https://blog.csdn.net/mochu7777777>

ci{v3erf_0tygidv2_fc0}

结合上面得到的 xinan，维吉尼亚密码

在线解密: <https://www.qqxiuzi.cn/bianma/weijiniyamima.php>

```
ci {v3erf_0tygidv2_fc0}
```

密钥

```
fa{i3eei_0llgvgn2_sc0}
```

<https://blog.csdn.net/rnochu7777777>

```
fa{i3eei_0llgvgn2_sc0}
```

栅栏密码

栅栏密码在线: <https://www.qqxiuzi.cn/bianma/zhalanmima.php>

```
fa {i3eei_0llgvgn2_sc0}
```

每组字数

```
flag{vig3ne2e_is_c00l}
```

<https://blog.csdn.net/rnochu7777777>

```
flag{vig3ne2e_is_c00l}
```