D^3CTF 2019 ch1pfs wp

拿到一堆文件，先运行一下，要求输入key，进到/test/，里面有文件，但是cat出来一堆乱码。

把CH1P_fs.ko拖到IDA里面看看，可以发现是自己写的一个文件系统，insmod的时候要一个key，key生成f_key，f_key在文件读写的时候进行异或加密。

然后到处看了看（strings rootfs.img、网上找了一下相关的代码、找到个假的getkey），明确给的各个文件的用途：

- CH1P_fs.ko 文件系统的驱动
- image CH1P_fs加密后的文件系统，系统启动后挂载到/test/目录
- waifu.png 明文图片，image里面也有一张
- 其他qemu所需的文件

至此，

明确解题思路：

- 因为是使用顺序的异或加解密，可以通过waifu.png的明密文对找出f_key
- 使用f_key查看其他文件或反推出key

Step1 找出png的明密文对

我patch了rootfs.img中的CH1P_fs.ko，将读取文件时的异或加密nop掉，直接输出raw的文件，使得我们能够定位密文在image中的位置。

png: 0x23bda0-0x732da0

png很大，在image文件中并不是完全连续的，中间还有一些数据，借助hexedit在patch过的文件系统上对比，可以将png密文完全提取出来（但是没有必要

Step2 根据明密文对恢复f_key

拿到明密文对直接异或即能得到f_key

```
with open("ctf/waifu.png", "rb") as f:
    m_data = f.read()

with open("ctf/png_c", "rb") as f:
    c_data = f.read()


for r in range(3):
    f_key = []
```

```
    m = m_data[4096*r:4096*(r+1)]
    c = c_data[4096*r:4096*(r+1)]
    for i in range(4096):
        f_key.append(ord(m[i])^ord(c[i]))
    print f_key
```

```
f_key = [255, 190, 241, 240, 224, 168, 167, 95, 148, 140, 12, 92, 26, 116, 75,
155, 245, 54, 107, 247, 70, 158, 181, 135, 131, 98, 103, 104, 79, 64, 87, 96,
50, 85, 45, 244, 120, 73, 114, 140, 223, 98, 36, 219, 248, 200, 20, 178, 110,
163, 188, 60, 176, 114, 82, 214, 243, 192, 127, 57, 122, 225, 187, 118, 92,
244, 21, 80, 174, 77, 247, 172, 132, 153, 88, 101, 178, 129, 154, 180, 231,
137, 173, 232, 225, 241, 163, 190, 13, 16, 237, 141, 95, 148, 0, 117, 109, 43,
75, 82, 253, 200, 230, 37, 217, 67, 250, 86, 91, 227, 123, 95, 242, 20, 189,
21, 69, 92, 184, 169, 126, 200, 210, 185, 46, 82, 192, 228, 75, 236, 47, 247,
158, 53, 26, 169, 27, 101, 62, 189, 169, 235, 193, 209, 130, 171, 186, 91,
199, 46, 181, 129, 203, 236, 124, 245, 156, 169, 92, 48, 183, 4, 225, 183, 61,
250, 6, 174, 139, 208, 89, 222, 4, 20, 252, 108, 32, 50, 41, 150, 113, 17, 12,
232, 209, 70, 172, 250, 123, 204, 254, 107, 225, 127, 250, 17, 88, 79, 170,
187, 162, 112, 139, 154, 125, 159, 228, 180, 37, 172, 175, 166, 254, 126, 112,
134, 117, 237, 20, 42, 15, 212, 245, 78, 32, 22, 111, 132, 71, 239, 218, 174,
146, 226, 77, 68, 171, 80, 103, 161, 164, 166, 214, 141, 167, 115, 96, 39,
157, 36, 63, 76, 20, 62, 56, 191, 124, 24, 170, 37, 30, 202, 144, 180, 117,
255, 61, 38, 29, 146, 101, 42, 59, 170, 127, 57, 212, 30, 168, 210, 93, 149,
194, 70, 185, 35, 75, 63, 219, 226, 154, 145, 97, 57, 182, 97, 12, 176, 65,
223, 109, 241, 26, 250, 241, 157, 251, 97, 251, 29, 188, 29, 174, 139, 148,
181, 80, 38, 118, 2, 111, 59, 195, 11, 68, 159, 143, 191, 203, 3, 101, 68,
168, 252, 97, 187, 165, 96, 22, 118, 109, 176, 156, 30, 49, 222, 165, 186,
253, 53, 163, 237, 38, 140, 164, 191, 162, 105, 86, 136, 209, 87, 136, 78,
150, 134, 133, 113, 177, 42, 82, 8, 104, 203, 33, 86, 12, 122, 157, 108, 132,
2, 123, 238, 52, 72, 203, 203, 123, 70, 240, 109, 27, 5, 139, 209, 173, 1, 96,
151, 13, 212, 12, 249, 156, 158, 41, 205, 184, 229, 178, 212, 236, 155, 236,
211, 178, 195, 8, 21, 245, 161, 64, 5, 204, 71, 75, 250, 4, 44, 208, 206, 108,
87, 173, 12, 189, 95, 217, 121, 112, 45, 250, 253, 121, 219, 171, 212, 204,
157, 72, 172, 125, 229, 251, 243, 217, 220, 183, 114, 168, 25, 172, 218, 47,
85, 91, 248, 34, 5, 49, 142, 108, 71, 192, 42, 234, 57, 78, 86, 5, 6, 76, 239,
121, 169, 220, 61, 50, 81, 29, 229, 173, 50, 78, 199, 41, 240, 63, 32, 24,
230, 86, 94, 161, 185, 147, 32, 232, 231, 158, 144, 72, 19, 159, 222, 234,
210, 235, 173, 59, 171, 148, 178, 245, 183, 96, 242, 67, 58, 96, 34, 60, 175,
188, 98, 213, 137, 41, 184, 222, 178, 126, 192, 53, 32, 155, 92, 106, 137, 80,
135, 100, 214, 123, 203, 207, 171, 12, 223, 138, 7, 235, 67, 177, 37, 11, 197,
125, 149, 91, 146, 144, 75, 119, 174, 252, 207, 35, 105, 64, 87, 135, 121,
138, 123, 255, 212, 64, 95, 118, 249, 152, 82, 215, 63, 128, 4, 236, 73, 106,
106, 145, 237, 99, 42, 212, 88, 177, 7, 168, 69, 248, 254, 117, 214, 109, 172,
106, 101, 237, 15, 3, 109, 207, 0, 254, 3, 212, 140, 250, 51, 220, 56, 203,
122, 146, 160, 155, 121, 36, 127, 72, 147, 97, 161, 238, 28, 171, 231, 116,
192, 51, 82, 47, 78, 25, 180, 137, 77, 253, 192, 111, 49, 82, 234, 31, 114,
20, 139, 200, 234, 249, 241, 204, 50, 55, 227, 21, 220, 101, 79, 42, 155, 185,
172, 179, 156, 82, 199, 40, 239, 10, 247, 170, 0, 198, 93, 80, 161, 211, 155,
```

252, 1, 175, 37, 214, 202, 234, 190, 122, 99, 2, 110, 138, 21, 105, 193, 125,
102, 34, 212, 63, 162, 73, 103, 120, 10, 212, 167, 34, 198, 77, 231, 7, 90,
173, 210, 54, 108, 4, 15, 43, 89, 149, 123, 212, 73, 101, 239, 109, 228, 85,
130, 224, 204, 41, 10, 236, 172, 69, 159, 9, 190, 191, 184, 148, 108, 242,
108, 141, 135, 23, 40, 1, 142, 105, 55, 85, 68, 215, 183, 118, 86, 184, 236,
160, 41, 192, 65, 154, 84, 83, 30, 93, 224, 193, 157, 200, 239, 32, 229, 154,
226, 158, 223, 42, 248, 1, 39, 77, 161, 136, 119, 238, 223, 21, 78, 209, 197,
221, 119, 206, 133, 5, 104, 234, 6, 88, 212, 17, 207, 109, 131, 139, 115, 216,
70, 29, 245, 152, 165, 80, 115, 164, 26, 50, 75, 88, 241, 219, 198, 191, 170,
64, 2, 135, 253, 13, 217, 254, 170, 140, 252, 216, 7, 162, 4, 122, 196, 65,
60, 62, 148, 207, 156, 114, 37, 167, 121, 147, 168, 215, 123, 228, 134, 147,
116, 200, 195, 173, 250, 234, 111, 136, 204, 187, 188, 148, 31, 135, 32, 79,
57, 202, 183, 220, 1, 41, 3, 137, 126, 173, 219, 118, 118, 101, 172, 123, 110,
105, 78, 151, 116, 131, 77, 213, 159, 97, 159, 211, 141, 244, 159, 195, 54,
249, 49, 231, 196, 52, 73, 67, 218, 142, 236, 206, 135, 128, 50, 84, 116, 90,
96, 141, 27, 208, 138, 243, 214, 66, 82, 112, 240, 237, 183, 41, 186, 235,
236, 236, 45, 237, 221, 17, 226, 21, 209, 20, 252, 229, 231, 166, 194, 158,
50, 38, 85, 168, 83, 41, 247, 70, 153, 176, 177, 134, 214, 248, 176, 23, 252,
234, 39, 85, 209, 86, 170, 36, 236, 67, 213, 179, 50, 243, 88, 239, 248, 200,
128, 73, 64, 201, 139, 239, 125, 46, 201, 8, 160, 146, 103, 37, 63, 191, 100,
108, 95, 228, 116, 163, 255, 10, 25, 122, 64, 93, 137, 149, 166, 231, 125, 61,
38, 130, 125, 172, 22, 153, 10, 166, 64, 218, 204, 202, 51, 66, 239, 0, 46,
233, 66, 45, 93, 142, 150, 125, 164, 187, 117, 175, 126, 96, 181, 183, 146,
88, 147, 85, 94, 132, 130, 180, 37, 253, 170, 206, 101, 211, 180, 153, 190,
95, 178, 49, 16, 115, 83, 239, 207, 31, 119, 206, 139, 151, 110, 211, 205,
243, 61, 44, 5, 50, 4, 228, 39, 109, 41, 106, 112, 147, 21, 188, 105, 197,
101, 117, 51, 203, 219, 111, 22, 192, 145, 255, 168, 176, 3, 52, 170, 206, 82,
209, 69, 211, 8, 120, 219, 116, 26, 151, 10, 217, 123, 93, 28, 241, 113, 44,
32, 112, 37, 212, 16, 97, 31, 255, 30, 5, 207, 55, 9, 110, 23, 63, 156, 133,
130, 72, 157, 14, 223, 127, 123, 175, 190, 104, 185, 176, 108, 213, 230, 162,
199, 70, 55, 11, 248, 92, 29, 61, 56, 49, 96, 51, 47, 213, 111, 254, 3, 112,
158, 169, 102, 75, 55, 148, 26, 174, 195, 80, 241, 130, 16, 143, 180, 110,
100, 74, 60, 151, 58, 40, 72, 177, 13, 234, 141, 119, 110, 25, 127, 253, 93,
129, 202, 169, 60, 112, 101, 100, 8, 246, 185, 164, 5, 41, 95, 92, 10, 222, 5,
93, 110, 63, 175, 117, 41, 111, 179, 7, 121, 196, 142, 168, 70, 43, 75, 162,
155, 247, 187, 72, 193, 226, 3, 43, 162, 39, 241, 199, 68, 136, 5, 148, 196,
16, 200, 209, 142, 77, 255, 20, 144, 245, 26, 43, 186, 145, 54, 53, 174, 68,
212, 105, 250, 240, 213, 255, 60, 2, 55, 133, 39, 187, 200, 160, 119, 134,
240, 37, 180, 66, 22, 193, 66, 79, 63, 123, 109, 157, 101, 133, 11, 219, 59,
196, 79, 217, 36, 185, 91, 232, 96, 67, 148, 77, 74, 165, 220, 152, 106, 113,
139, 91, 114, 231, 119, 113, 231, 42, 174, 146, 41, 131, 150, 97, 44, 232,
235, 128, 207, 10, 120, 0, 122, 58, 126, 75, 117, 51, 3, 239, 118, 218, 131,
70, 105, 76, 200, 24, 247, 53, 204, 135, 25, 105, 200, 230, 68, 162, 98, 233,
157, 195, 154, 131, 97, 213, 66, 60, 2, 49, 109, 56, 5, 243, 201, 37, 224, 23,
236, 80, 169, 166, 185, 198, 239, 31, 229, 141, 36, 201, 220, 209, 246, 182,
37, 155, 78, 74, 239, 113, 53, 177, 54, 64, 60, 70, 89, 114, 148, 17, 207,
140, 52, 254, 35, 199, 34, 20, 82, 107, 206, 1, 113, 154, 255, 76, 89, 173,
225, 217, 43, 218, 65, 129, 83, 32, 115, 2, 246, 203, 6, 49, 255, 42, 166, 96,
242, 133, 32, 133, 138, 142, 202, 35, 137, 24, 244, 196, 59, 24, 3, 193, 167,

138, 186, 18, 101, 223, 120, 108, 114, 150, 123, 13, 51, 75, 30, 33, 95, 153, 221, 47, 57, 119, 29, 28, 85, 8, 3, 5, 228, 254, 96, 238, 150, 44, 75, 114, 253, 244, 131, 59, 95, 90, 48, 53, 212, 26, 18, 226, 90, 150, 112, 98, 40, 5, 100, 43, 190, 212, 3, 206, 126, 212, 206, 85, 87, 155, 253, 171, 235, 164, 234, 158, 37, 184, 44, 61, 122, 112, 182, 112, 44, 103, 30, 78, 248, 153, 171, 174, 41, 50, 103, 120, 181, 121, 83, 120, 226, 10, 148, 11, 104, 220, 132, 41, 96, 154, 56, 75, 144, 117, 108, 205, 63, 96, 234, 79, 222, 45, 215, 201, 184, 166, 231, 68, 115, 186, 118, 192, 184, 212, 96, 189, 15, 211, 35, 44, 135, 125, 87, 173, 89, 58, 254, 111, 200, 141, 212, 123, 117, 152, 201, 106, 108, 240, 234, 46, 39, 60, 49, 124, 141, 59, 78, 19, 236, 132, 75, 33, 115, 20, 166, 94, 179, 239, 158, 44, 22, 78, 187, 137, 59, 76, 172, 105, 129, 145, 81, 41, 148, 4, 15, 192, 34, 48, 0, 135, 137, 68, 199, 52, 137, 101, 211, 194, 215, 129, 81, 148, 61, 168, 172, 171, 229, 94, 218, 59, 89, 159, 238, 59, 194, 160, 110, 39, 149, 229, 77, 150, 55, 59, 178, 72, 226, 239, 252, 44, 45, 206, 79, 17, 20, 135, 189, 14, 225, 91, 125, 231, 244, 130, 154, 194, 14, 18, 109, 103, 206, 160, 97, 83, 208, 140, 224, 153, 134, 163, 205, 131, 36, 100, 5, 214, 220, 189, 191, 201, 13, 211, 176, 254, 37, 27, 168, 252, 46, 242, 54, 57, 86, 127, 175, 178, 101, 192, 193, 247, 138, 21, 151, 11, 52, 114, 128, 188, 21, 191, 20, 218, 167, 96, 196, 90, 127, 104, 147, 83, 115, 142, 158, 252, 166, 142, 40, 203, 58, 85, 179, 16, 239, 97, 195, 191, 167, 168, 124, 78, 30, 109, 7, 17, 222, 58, 111, 49, 23, 89, 56, 141, 40, 176, 90, 115, 248, 84, 158, 188, 225, 220, 29, 173, 203, 242, 214, 61, 49, 102, 184, 185, 98, 36, 243, 57, 178, 210, 85, 138, 106, 253, 7, 15, 54, 51, 79, 85, 137, 164, 4, 246, 12, 46, 49, 14, 9, 88, 217, 119, 230, 227, 200, 146, 27, 212, 123, 121, 142, 108, 209, 94, 127, 75, 115, 182, 146, 57, 101, 233, 127, 31, 84, 75, 134, 163, 56, 91, 68, 131, 1, 106, 110, 177, 14, 229, 214, 49, 199, 230, 241, 192, 19, 169, 170, 227, 153, 40, 95, 63, 8, 144, 89, 198, 240, 194, 138, 94, 88, 195, 75, 103, 240, 21, 243, 22, 174, 68, 189, 170, 249, 191, 245, 164, 78, 112, 13, 42, 126, 127, 31, 232, 9, 241, 142, 115, 13, 105, 93, 123, 204, 204, 61, 176, 249, 151, 110, 242, 74, 63, 235, 147, 42, 111, 94, 133, 146, 179, 207, 186, 9, 145, 69, 59, 89, 158, 74, 231, 208, 161, 112, 88, 130, 255, 51, 254, 13, 251, 8, 12, 160, 99, 233, 187, 159, 218, 116, 50, 33, 246, 117, 78, 186, 88, 116, 36, 62, 34, 60, 132, 35, 184, 142, 216, 253, 227, 121, 59, 31, 39, 239, 187, 235, 254, 49, 160, 53, 16, 92, 66, 221, 220, 131, 35, 155, 142, 123, 56, 14, 248, 72, 242, 108, 199, 88, 43, 80, 179, 22, 251, 89, 43, 76, 161, 151, 70, 243, 149, 173, 2, 26, 45, 211, 227, 197, 239, 29, 125, 254, 46, 119, 144, 71, 126, 179, 118, 164, 52, 37, 226, 96, 41, 139, 144, 223, 124, 38, 63, 140, 250, 229, 181, 1, 64, 90, 186, 29, 173, 39, 190, 215, 228, 45, 10, 143, 242, 59, 252, 94, 129, 117, 93, 234, 94, 127, 84, 96, 109, 61, 96, 52, 214, 169, 199, 52, 46, 18, 126, 28, 136, 134, 104, 20, 194, 97, 58, 65, 72, 137, 24, 156, 86, 195, 62, 236, 20, 246, 99, 33, 239, 87, 9, 116, 94, 114, 53, 44, 112, 80, 87, 200, 140, 189, 154, 164, 47, 26, 162, 198, 50, 165, 0, 218, 170, 201, 156, 88, 50, 235, 31, 95, 46, 81, 48, 206, 56, 73, 93, 154, 193, 84, 151, 231, 190, 113, 0, 42, 107, 42, 125, 103, 8, 12, 107, 253, 136, 142, 104, 226, 19, 238, 144, 60, 16, 114, 168, 132, 197, 188, 114, 28, 118, 242, 37, 121, 12, 50, 49, 237, 150, 254, 244, 108, 190, 101, 215, 20, 89, 88, 74, 209, 25, 100, 184, 223, 3, 213, 165, 6, 149, 175, 12, 187, 25, 67, 127, 136, 220, 144, 66, 52, 176, 76, 155, 252, 137, 139, 176, 51, 197, 39, 38, 44, 178, 219, 97, 246, 226, 226, 40, 241, 189, 199, 254, 22, 154, 214, 191, 154, 98, 16, 1, 235, 82, 203, 44, 146, 200,

252, 6, 1, 56, 252, 203, 224, 74, 21, 168, 107, 167, 209, 163, 95, 194, 195,
40, 209, 225, 94, 27, 159, 162, 211, 187, 33, 72, 75, 226, 225, 202, 120, 99,
87, 224, 165, 211, 248, 252, 176, 191, 232, 182, 33, 221, 43, 226, 219, 48,
162, 119, 172, 243, 236, 59, 227, 116, 81, 239, 174, 199, 131, 180, 159, 128,
151, 42, 205, 56, 104, 122, 90, 111, 194, 134, 168, 103, 153, 117, 191, 241,
39, 217, 109, 124, 32, 42, 240, 54, 246, 5, 37, 46, 43, 146, 216, 162, 119,
199, 8, 46, 222, 246, 85, 57, 14, 117, 255, 64, 107, 53, 55, 92, 141, 165,
215, 89, 38, 181, 70, 95, 10, 250, 227, 108, 221, 174, 106, 118, 206, 29, 190,
15, 86, 94, 53, 4, 203, 90, 5, 74, 159, 12, 121, 201, 196, 166, 8, 106, 151,
33, 137, 178, 225, 148, 14, 8, 58, 206, 175, 20, 167, 57, 148, 7, 102, 202,
167, 36, 203, 31, 209, 28, 14, 243, 93, 4, 65, 210, 255, 19, 70, 205, 12, 71,
31, 224, 126, 152, 142, 154, 250, 134, 248, 22, 26, 186, 123, 197, 205, 66,
185, 110, 212, 61, 204, 248, 219, 26, 171, 65, 28, 94, 106, 86, 82, 214, 98,
72, 186, 128, 108, 116, 119, 155, 188, 70, 177, 176, 228, 156, 31, 73, 66,
254, 190, 160, 35, 22, 131, 131, 146, 1, 139, 80, 91, 114, 172, 21, 54, 218,
208, 52, 141, 112, 157, 223, 35, 94, 199, 22, 86, 178, 63, 131, 163, 135, 60,
238, 107, 175, 87, 221, 116, 73, 218, 122, 91, 134, 119, 202, 186, 31, 133,
225, 101, 198, 197, 98, 55, 125, 155, 107, 128, 27, 41, 57, 151, 158, 176, 30,
245, 2, 245, 35, 102, 231, 16, 61, 124, 109, 232, 226, 136, 133, 99, 195, 253,
216, 34, 197, 229, 27, 248, 66, 130, 7, 13, 243, 34, 43, 145, 46, 138, 109,
82, 124, 114, 28, 36, 68, 179, 236, 199, 67, 227, 10, 48, 214, 149, 82, 249,
163, 10, 181, 126, 145, 140, 22, 158, 201, 20, 101, 175, 122, 165, 211, 171,
129, 135, 186, 26, 60, 179, 68, 9, 173, 50, 73, 137, 180, 211, 111, 146, 250,
227, 217, 181, 208, 200, 205, 24, 133, 148, 142, 40, 88, 127, 1, 244, 201,
245, 91, 226, 80, 248, 161, 83, 213, 242, 147, 50, 19, 203, 186, 85, 98, 75,
49, 251, 163, 158, 153, 162, 26, 21, 104, 76, 17, 40, 111, 59, 168, 232, 0, 8,
46, 241, 225, 72, 213, 88, 154, 65, 186, 203, 105, 193, 154, 115, 107, 179, 0,
9, 204, 162, 144, 166, 209, 139, 144, 216, 120, 99, 205, 188, 225, 17, 220,
176, 43, 113, 29, 66, 188, 97, 239, 4, 93, 107, 242, 220, 189, 159, 61, 171,
76, 9, 13, 229, 80, 129, 23, 134, 73, 179, 88, 126, 204, 186, 234, 176, 11,
42, 19, 50, 56, 162, 166, 208, 76, 200, 49, 195, 230, 249, 49, 99, 76, 106,
188, 39, 250, 240, 169, 178, 71, 42, 3, 106, 74, 243, 132, 171, 186, 250, 226,
158, 167, 198, 115, 149, 212, 64, 97, 159, 171, 236, 254, 50, 250, 80, 208,
182, 105, 69, 80, 215, 206, 13, 120, 1, 10, 151, 8, 111, 253, 183, 248, 76,
155, 161, 117, 124, 38, 144, 121, 29, 229, 146, 15, 62, 172, 18, 166, 220,
106, 122, 98, 134, 246, 243, 126, 253, 95, 46, 151, 157, 163, 78, 118, 122,
162, 119, 208, 130, 215, 130, 148, 152, 224, 85, 82, 170, 149, 212, 109, 76,
190, 106, 186, 134, 124, 82, 68, 160, 244, 15, 49, 243, 71, 118, 206, 31, 99,
153, 24, 217, 73, 113, 10, 164, 0, 172, 7, 29, 74, 83, 207, 153, 139, 180,
244, 242, 117, 247, 223, 206, 181, 36, 167, 47, 22, 75, 217, 33, 79, 145, 124,
113, 237, 125, 84, 50, 187, 84, 245, 87, 63, 204, 74, 94, 46, 143, 90, 213,
15, 109, 252, 209, 13, 133, 234, 123, 97, 87, 91, 236, 250, 140, 61, 40, 7,
45, 91, 17, 58, 165, 148, 69, 164, 25, 155, 121, 54, 82, 121, 156, 93, 182,
119, 2, 120, 162, 39, 103, 241, 170, 71, 147, 98, 118, 140, 21, 102, 149, 128,
253, 19, 214, 67, 180, 204, 205, 193, 156, 133, 16, 202, 171, 113, 148, 245,
241, 57, 199, 114, 243, 68, 104, 68, 14, 6, 125, 79, 152, 200, 81, 217, 176,
169, 42, 42, 158, 182, 147, 97, 13, 12, 86, 34, 144, 116, 135, 132, 209, 209,
254, 172, 39, 23, 193, 242, 160, 193, 192, 243, 166, 243, 203, 180, 116, 139,
56, 142, 168, 183, 12, 151, 139, 228, 114, 129, 156, 112, 22, 1, 182, 84, 150,

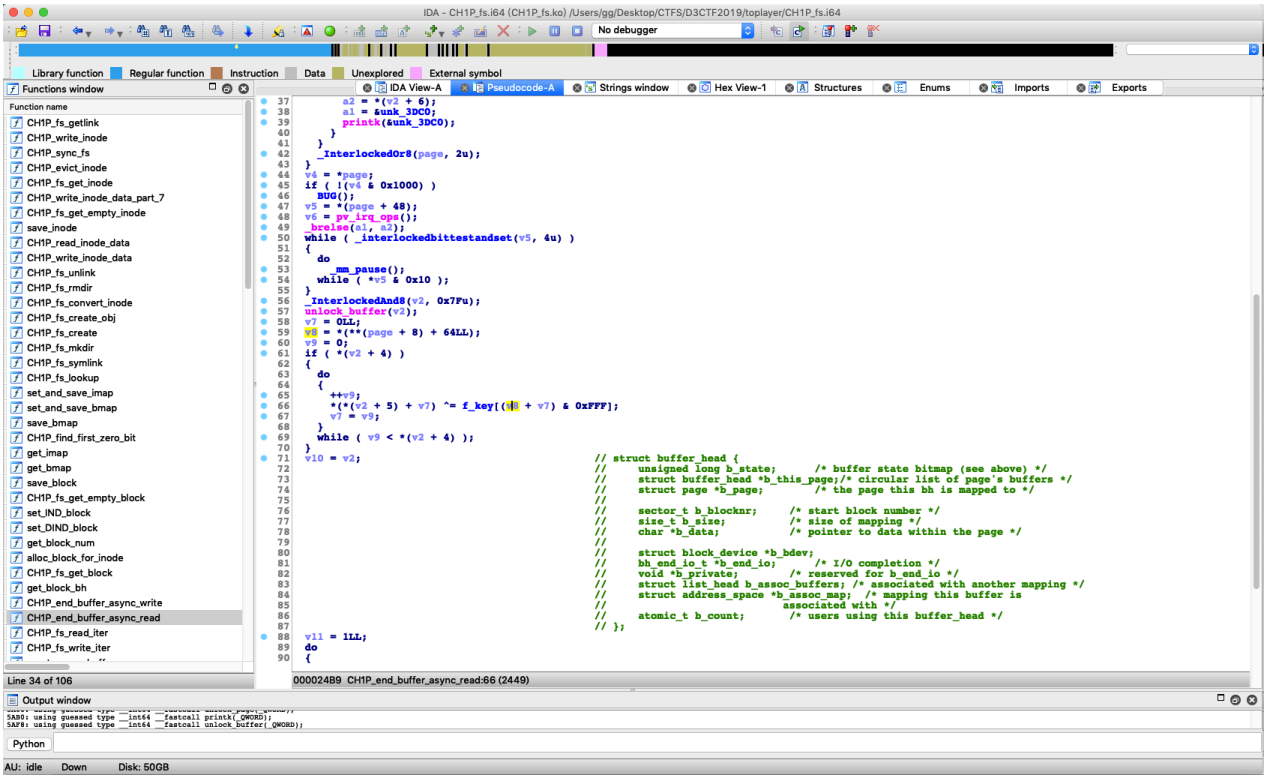
81, 156, 135, 139, 42, 103, 177, 184, 187, 254, 126, 161, 135, 12, 44, 252, 212, 91, 226, 148, 196, 110, 120, 29, 27, 70, 222, 6, 149, 1, 231, 11, 195, 213, 7, 236, 41, 80, 60, 167, 140, 76, 87, 250, 213, 46, 104, 80, 59, 74, 243, 186, 188, 115, 4, 154, 97, 27, 109, 118, 153, 73, 159, 137, 140, 41, 145, 228, 132, 139, 152, 9, 88, 31, 51, 200, 186, 142, 150, 128, 29, 169, 225, 56, 211, 96, 8, 241, 98, 126, 123, 19, 240, 72, 123, 177, 231, 34, 182, 242, 82, 130, 194, 101, 35, 203, 33, 234, 127, 28, 174, 62, 88, 8, 39, 92, 65, 144, 208, 123, 223, 23, 21, 132, 48, 104, 200, 105, 110, 228, 154, 150, 202, 93, 91, 28, 33, 222, 184, 232, 90, 232, 135, 79, 230, 184, 77, 34, 205, 198, 112, 136, 199, 79, 169, 166, 216, 101, 247, 150, 214, 160, 193, 101, 1, 242, 211, 170, 9, 126, 193, 170, 227, 25, 217, 201, 7, 165, 218, 24, 163, 229, 152, 193, 36, 118, 182, 12, 173, 225, 55, 200, 147, 4, 253, 66, 100, 242, 251, 20, 70, 246, 102, 107, 169, 193, 151, 80, 227, 19, 14, 237, 68, 102, 159, 201, 14, 33, 58, 155, 7, 207, 154, 255, 205, 253, 128, 15, 214, 5, 194, 56, 170, 157, 41, 33, 215, 152, 104, 190, 244, 100, 25, 7, 237, 54, 216, 176, 239, 219, 100, 140, 45, 180, 186, 94, 3, 75, 164, 183, 85, 186, 34, 213, 128, 251, 188, 44, 120, 210, 63, 115, 87, 126, 196, 8, 207, 35, 240, 218, 157, 19, 152, 25, 181, 253, 7, 75, 183, 218, 61, 102, 180, 26, 43, 161, 3, 198, 249, 110, 130, 173, 16, 250, 229, 51, 204, 95, 247, 71, 25, 42, 85, 64, 101, 1, 71, 141, 222, 25, 94, 244, 168, 157, 206, 215, 149, 226, 234, 165, 104, 75, 116, 7, 159, 96, 16, 85, 86, 20, 204, 64, 133, 108, 37, 197, 116, 190, 179, 27, 246, 177, 219, 91, 161, 147, 175, 60, 208, 254, 52, 148, 165, 106, 175, 30, 186, 26, 244, 148, 203, 167, 8, 38, 150, 88, 188, 97, 207, 155, 198, 88, 52, 210, 172, 219, 35, 37, 207, 210, 194, 247, 57, 76, 140, 18, 220, 90, 227, 58, 10, 65, 223, 221, 161, 125, 35, 67, 170, 98, 190, 16, 142, 164, 103, 113, 242, 96, 59, 101, 175, 120, 53, 158, 19, 127, 94, 215, 84, 202, 132, 109, 139, 225, 11, 52, 166, 121, 225, 159, 80, 74, 78, 13, 158, 159, 178, 149, 192, 14, 64, 153, 128, 218, 20, 208, 120, 55, 248, 110, 188, 26, 240, 231, 224, 201, 188, 221, 55, 127, 142, 19, 210, 174, 7, 126, 95, 90, 230, 157, 66, 194, 61, 219, 201, 215, 236, 79, 47, 89, 2, 168, 178, 133, 245, 56, 188, 4, 17, 94, 97, 124, 85, 227, 43, 248, 201, 190, 243, 195, 73, 105, 50, 90, 79, 226, 110, 230, 77, 88, 165, 60, 180, 254, 27, 180, 153, 211, 97, 69, 137, 75, 13, 17, 158, 74, 168, 53, 24, 194, 3, 208, 232, 101, 74, 202, 185, 122, 147, 78, 217, 109, 79, 169, 182, 116, 36, 182, 180, 69, 171, 101, 212, 168, 126, 96, 121, 109, 104, 142, 90, 115, 136, 155, 24, 115, 196, 83, 36, 136, 138, 149, 37, 6, 125, 206, 38, 151, 37, 185, 222, 90, 39, 253, 143, 12, 82, 10, 95, 1, 93, 53, 188, 48, 131, 129, 235, 156, 190, 68, 152, 204, 169, 253, 2, 12, 191, 238, 138, 236, 60, 254, 36, 99, 96, 44, 123, 33, 127, 78, 149, 128, 245, 54, 219, 162, 209, 215, 147, 43, 53, 102, 247, 66, 3, 243, 47, 237, 70, 131, 111, 2, 75, 90, 49, 130, 211, 163, 80, 201, 98, 172, 95, 195, 95, 63, 8, 43, 3, 206, 158, 62, 176, 245, 128, 173, 118, 7, 81, 217, 105, 104, 161, 179, 188, 137, 43, 115, 98, 81, 181, 35, 129, 199, 111, 192, 64, 247, 170, 87, 255, 228, 89, 3, 25, 106, 2, 13, 175, 157, 49, 56, 128, 238, 231, 211, 223, 63, 159, 11, 203, 46, 31, 123, 168, 146, 75, 204, 49, 77, 60, 89, 77, 123, 244, 240, 66, 71, 43, 219, 221, 28, 89, 210, 142, 220, 158, 123, 132, 252, 102, 142, 170, 136, 97, 138, 218, 9, 250, 230, 59, 133, 26, 150, 68, 150, 116, 80, 125, 243, 252, 136, 136, 20, 76, 128, 219, 154, 203, 217, 110, 5, 218, 150, 144, 93, 185, 242, 62, 154, 156, 220, 211, 215, 29, 142, 22, 232, 244, 9, 79, 213, 194, 241, 230, 171, 82, 25, 51, 137, 108, 239, 134, 10, 96, 241, 98, 162, 80, 68, 102, 194, 168, 167, 229, 183, 38, 85,

```
214, 123, 111, 101, 140, 24, 55, 121, 54, 184, 28, 16, 140, 0, 227, 254, 50,
221, 229, 110, 108, 57, 185, 241, 209, 83, 3, 12, 86, 158, 55, 98, 205, 86,
237, 230, 225, 114, 169, 130, 98, 157, 36, 96, 132, 117, 105, 82, 115, 243,
234, 107, 44, 53, 12, 238, 72, 178, 189, 32, 184, 21, 54, 184, 177, 80, 30,
48, 141, 88, 170, 150, 68, 233, 217, 204, 85, 147, 237, 119, 65, 126, 136,
131, 67, 179, 157, 127]
```

我只处理了前3*4096字节，发现key是一样的

Step3 解密其他数据

观察加解密的代码。如下图所示，还有个v8不知道，不过爆破4096次肯定能过出来




```
def find_m(flag_c):
    for _ in range(4096):

        flag_m = ""

        for i in range(len(flag_c)):
            flag_m += chr(int(flag_c[i], 16) ^ f_key[(i+_) % 4096])

        import string
        f = True
        for c in flag_m:
            if c not in string.printable:
                f = False
        if f:
```

```
            print flag_m
            return flag_m

hint_c = "97 8F C7 C3 00 F6 F9 78 03 6E 1B 29 FE 96 59 05 83 2F F0 C0 E2
89".split(" ")
# find_m(hint_c)
# good_but_tobecontinue

# find_m(flag_cc)
# not find

key_c = "95 C3 BF EB EF 6E E4 EA 7F 7D 10".split(" ")
find_m(key_c)
# d3_CH1pfs!
```

flag还拿不到，其他数据都能够解密了，有个key文件，解密得到key: `d3_CH1pfs!`，用key进入文件系统。

还有下一关：

```
/test # cat make_flag.sh
#!/bin/sh
gcc ../enc.c -o ./enc --static
./enc ../flag > flag
```

flag用enc加密过，但是并没有enc文件的影子，可能被删掉了，想到文件系统的删除并不是真·擦除，可能从image中恢复。

根据观察，image中只有两个大文件：png和busybox，统计了一下非零字节的个数，验证以上的想法

```
with open("ctf/image", "rb") as f:
    image_data = f.read()

print len(image_data)
count = 0
for c in image_data:
    if ord(c) != 0:
        count += 1
print hex(count)
```

对比发现文件系统里还有一个大文件，又因为enc是静态链接的，绝壁就是它了

如何提取：

- 修改record（不太熟悉linux文件系统，没有尝试

- 手动dump出raw的enc

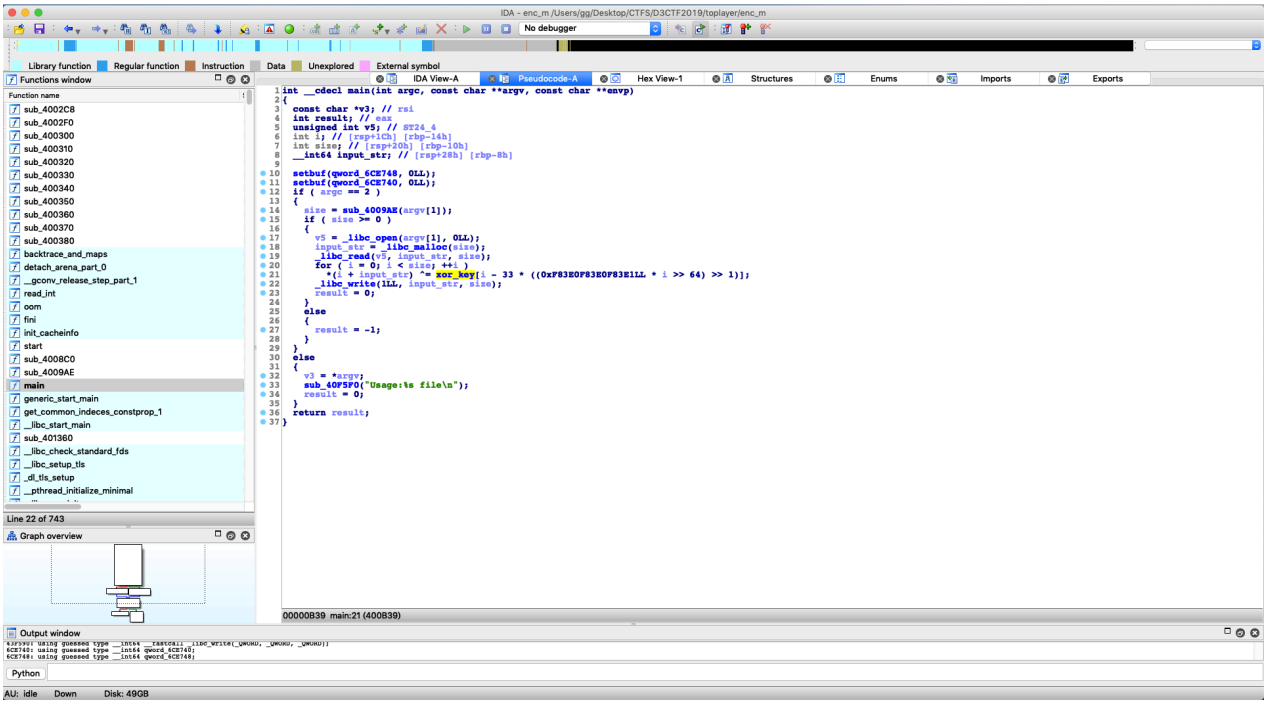
我用了下面这种比较笨的方法

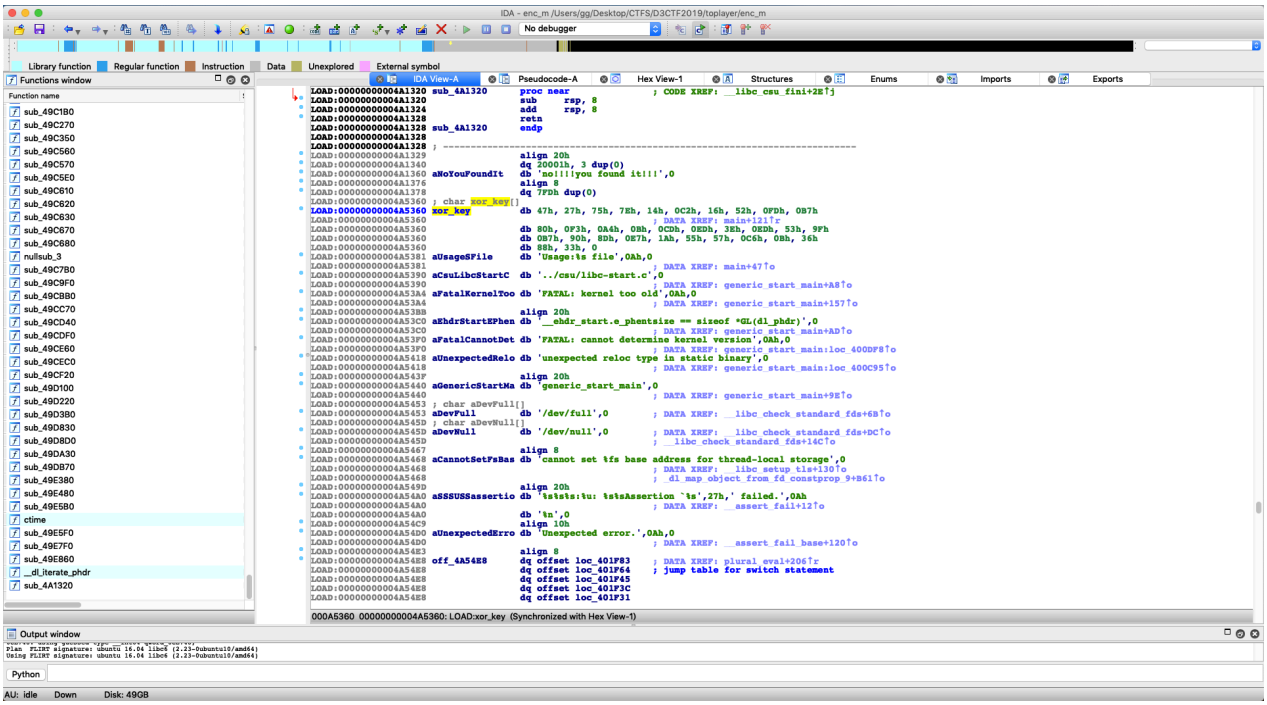
先拿f_key和ELF的开头四个字节定位到ELF的起始位置，手动从010editor中提取出来，中间夹杂着一些无用的数据。边用f_key恢复，拖到IDA里面查看，如果夹杂着没用的数据，汇编代码从那个位置开始很容易就能看出异常，微调即可。

```
def re_enc_binary():
    with open("ctf/enc_c", "rb") as f:
        enc_a_data = list(f.read())

    key_begin = 4

    res = []

    for i in range(len(enc_a_data)):
        # res.append(ord(enc_a_data[i]) ^ f_key[(key_begin+i) % 4096])
        enc_a_data[i] = chr(ord(enc_a_data[i]) ^ f_key[(key_begin+i) % 4096])

    # print res

    with open("ctf/enc_m", "wb") as f:
        f.write("".join(enc_a_data))
```

恢复出enc文件，拖到IDA中查看：

恢复符号表，可以发现逻辑十分简单：





又是异或而已，写出解密脚本：

```
xor_key = [
    0x47, 0x27, 0x75, 0x7E, 0x14, 0xC2, 0x16, 0x52, 0xFD, 0xB7,
    0x80, 0xF3, 0xA4, 0x0B, 0xCD, 0xED, 0x3E, 0xED, 0x53, 0x9F,
    0xB7, 0x90, 0x8D, 0xE7, 0x1A, 0x55, 0x57, 0xC6, 0x0B, 0x36,
    0x88, 0x33, 0
]


def find_flag():
    flag_c = "8B B3 49 9E FE B5 0E 27 D6 85 74 73 CD 14 52 C2 CE 33 8B 6A B3
84 BA 99 29 5D 54 9B 30 6D 19 25 20 50 C5 DE 61".split(
        " ")
    for _ in range(4096):

        flag_m = ""

        for i in range(len(flag_c)):
            flag_m += chr(int(flag_c[i], 16) ^ f_key[(i+_) % 4096] ^ xor_key[i
% 33])

        import string
        f = True
        for c in flag_m:
            if c not in string.printable:
                f = False
        if f:
            print flag_m
            return flag_m
# d3ctf{Do_you_think_vfs_1s_convenient}
```