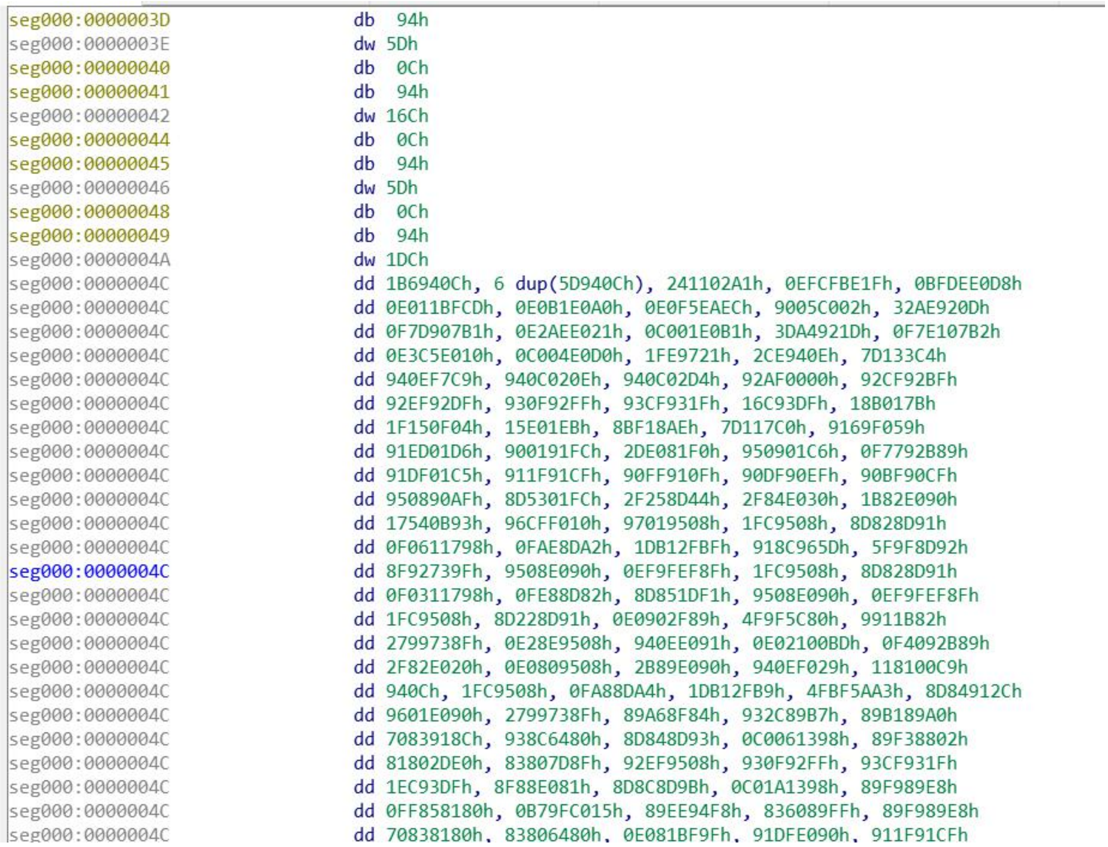
因为这周事比较多，所以菜鸡只水一题

1. pwn 白给题，直接 nc cat flag
2. Iot 题

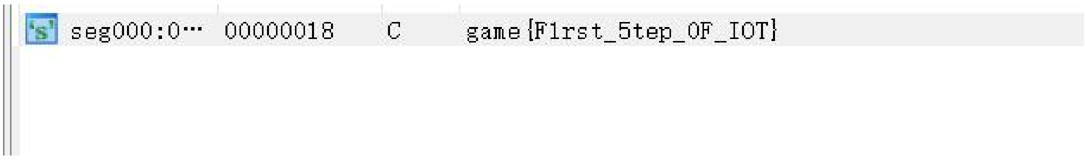
奇妙的固件

看到 hex 文件，先拖到 ida 看一下



```
seg000:0000003D                 db  94h
seg000:0000003E                 dw 5Dh
seg000:00000040                 db  0Ch
seg000:00000041                 db  94h
seg000:00000042                 dw 16Ch
seg000:00000044                 db  0Ch
seg000:00000045                 db  94h
seg000:00000046                 dw 5Dh
seg000:00000048                 db  0Ch
seg000:00000049                 db  94h
seg000:0000004A                 dw 1DCh
seg000:0000004C                 dd 1B6940Ch, 6 dup(5D940Ch), 241102A1h, 0EFCFBE1Fh, 0BFDEE0D8h
seg000:0000004C                 dd 0E011BFCDh, 0E0B1E0A0h, 0E0F5EAECh, 9005C002h, 32AE920Dh
seg000:0000004C                 dd 0F7D907B1h, 0E2AEE021h, 0C001E0B1h, 3DA4921Dh, 0F7E107B2h
seg000:0000004C                 dd 0E3C5E010h, 0C004E0D0h, 1FE9721h, 2CE940Eh, 7D133C4h
seg000:0000004C                 dd 940EF7C9h, 940C020Eh, 940C02D4h, 92AF0000h, 92CF92BFh
seg000:0000004C                 dd 92EF92DFh, 930F92FFh, 93CF931Fh, 16C93DFh, 18B017Bh
seg000:0000004C                 dd 1F150F04h, 15E01EBh, 8BF18AEh, 7D117C0h, 9169F059h
seg000:0000004C                 dd 91ED01D6h, 900191FCh, 2DE081F0h, 950901C6h, 0F7792B89h
seg000:0000004C                 dd 91DF01C5h, 911F91CFh, 90FF910Fh, 90DF90EFh, 90BF90CFh
seg000:0000004C                 dd 950890AFh, 8D5301FCh, 2F258D44h, 2F84E030h, 1B82E090h
seg000:0000004C                 dd 17540B93h, 96CFF010h, 97019508h, 1FC9508h, 8D828D91h
seg000:0000004C                 dd 0F0611798h, 0FAE8DA2h, 1DB12FBFh, 918C965Dh, 5F9F8D92h
seg000:0000004C                 dd 8F92739Fh, 9508E090h, 0EF9FEF8Fh, 1FC9508h, 8D828D91h
seg000:0000004C                 dd 0F0311798h, 0FE88D82h, 8D851DF1h, 9508E090h, 0EF9FEF8Fh
seg000:0000004C                 dd 1FC9508h, 8D228D91h, 0E0902F89h, 4F9F5C80h, 9911B82h
seg000:0000004C                 dd 2799738Fh, 0E28E9508h, 940EE091h, 0E02100BDh, 0F4092B89h
seg000:0000004C                 dd 2F82E020h, 0E0809508h, 2B89E090h, 940EF029h, 118100C9h
seg000:0000004C                 dd 940Ch, 1FC9508h, 0FA88DA4h, 1DB12FB9h, 4FBF5AA3h, 8D84912Ch
seg000:0000004C                 dd 9601E090h, 2799738Fh, 89A68F84h, 932C89B7h, 89B189A0h
seg000:0000004C                 dd 7083918Ch, 938C6480h, 8D848D93h, 0C0061398h, 89F38802h
seg000:0000004C                 dd 81802DE0h, 83807D8Fh, 92EF9508h, 930F92FFh, 93CF931Fh
seg000:0000004C                 dd 1EC93DFh, 8F88E081h, 8D8C8D9Bh, 0C01A1398h, 89F989E8h
seg000:0000004C                 dd 0FF858180h, 0B79FC015h, 89EE94F8h, 836089FFh, 89F989E8h
seg000:0000004C                 dd 70838180h, 83806480h, 0E081BF9Fh, 91DFE090h, 911F91CFh
```

啥都看不出来，再 shift+f12 查看字符串，直接就有了 flag



```
seg000:0…   00000018    C    game{F1rst_5tep_OF_IOT}
```

少了个 h