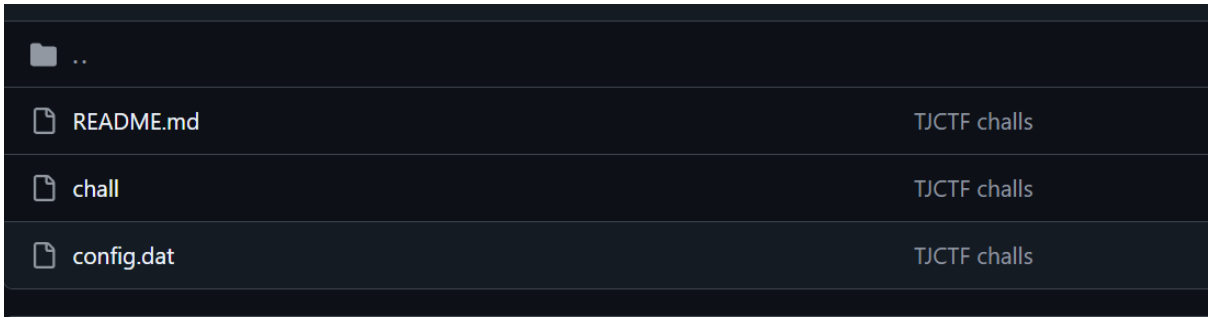


실행파일과 dat파일이 주어진다.

```
28
29  stream = fopen("config.dat", "rb");
30  if ( stream )
31  {
32    fseek(stream, 0LL, 2);
33    size = ftell(stream);
34    fseek(stream, 0LL, 0);
35    ptr = malloc(size);
36    fread(ptr, 1uLL, size, stream);
37    fclose(stream);
38    v24 = *ptr;
39    if ( v24 == 0xDEADC0DE )
40    {
41      v23 = *(ptr + 1);
42      *(ptr + 1) = 0;
43      v22 = sub_120D(ptr, size);                // 0x888a87a0
44      if ( v23 == v22 )
45      {
46        *(ptr + 1) = v23;
47        v21 = ptr + 8;
48        if ( *(ptr + 8) == 0x10 )
```

IDA로 디컴파일하면 config.dat에서 데이터를 읽어들인다.

```
gef> !xxd config.dat
00000000: dec0 adde a087 8a88 1004 1e46 3280 2007  ...........F2. .
00000010: 0803 1747 5a54 2630 046b 3379 21         ...GZT&0.k3y!
gef>
```

dat 파일에 어떤 정보가 저장되어있는지 확인한다.

```
67          v28 = 0;
68          if ( dest + v15 == 0x64 )
69          {
70            v4 = v28++;
71            *(&v10 + v4) = 114;
72          }
73          if ( v16 * dest == 0x5DC )
74          {
75            v5 = v28++;
76            *(&v10 + v5) = 0x33;
77          }
78          if ( v17 - v15 == 0x3A )
79          {
80            v6 = v28++;
81            *(&v10 + v6) = 0x76;
82          }
83          if ( 4 * dest == 0x78 )
84          {
85            v7 = v28++;
86            *(&v10 + v7) = 0x33;
87          }
88          if ( (v16 - 50) <= 1u )
89          {
90            v8 = v28++;
91            *(&v10 + v8) = 0x72;
92          }
93          if ( v15 > 0x3Cu )
94          {
95            v9 = v28++;
96            *(&v10 + v9) = 0x73;
97          }
98          if ( v28 == 7 )
99          {
100           v28 = 8;
```

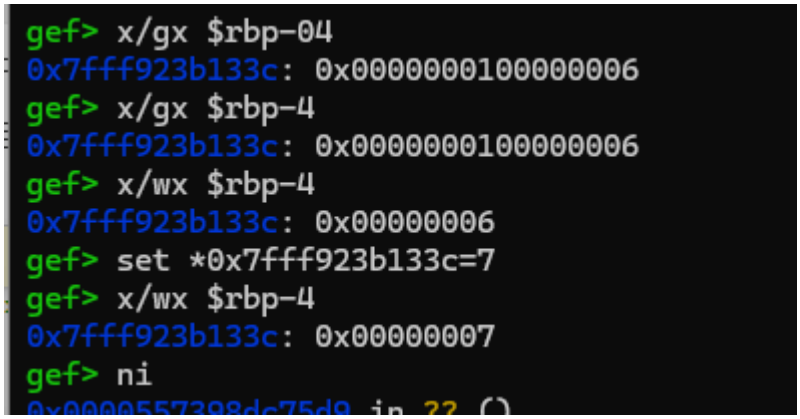
해당 프로그램은 dat파일에 있는 값들을 읽어와 특정 값과 맞는지 비교하는 key값 역할을 한다.

조건문을 만족시키면 v28값을 1씩 플러스한다.

```
97          }
98          if ( v28 == 7 )
99          {
100           v28 = 8;
101           HIBYTE(v10) = 101;
102           sub_1273(v13, 9uLL, v12, 4uLL);
103           printf("Flag: tjctf{%s%s}\n", v13, &v10);
104           free(ptr);
105           return 0LL;
106         }
107         else
```

최종적으로 v28값이 7이되면 FLAG를 반환해준다.

그런데 조건문은 총 6개로 v28을 7로 만족시킬 수 없다. 그래서 디버깅을 통해 강제로 변경해준다.



v28 변수의 주소를 찾고, 7로 세팅해준다.