```python
import angr

p = angr.Project('signal.exe')   #指定angr跑的程序
state = p.factory.blank_state(addr=0x401774)    #新建一个SimState的对象，得到一个初始化到二进
simgr = p.factory.simgr(state)   #创建simulation manager，angr的主要入口

simgr.explore(find=0x004017A5 ,avoid=0x004016E6)  #争取跑到输出成功的地址，避免跑到输出wrong的
if simgr.found:
    flag = simgr.found[0].posix.dumps(0)    #得到flag
    key = simgr.found[0].posix.dumps(1)
    print(flag)
    print(key)
```

angr一把梭

合理分析哪里开始哪里结束即可，不需要运行程序所有部分

```
emory at 0x7ffeff50 with 68 unconstrained bytes referenced from 0x101897f0
t.dll (0x101897f0))
b'757515121f3d478\x00\x08\x02\x08\x08\x02\x08\x00\x0e\x18\x08\x00\x00\x00\
02\x0e\x00\x00\x0c\x02\x00\x02\x00\x0e\x02*\x1a\x08\x02\x00\x02\x8a\x08\x0
1'
```