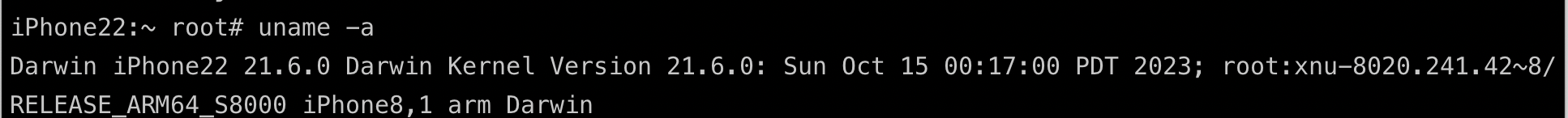
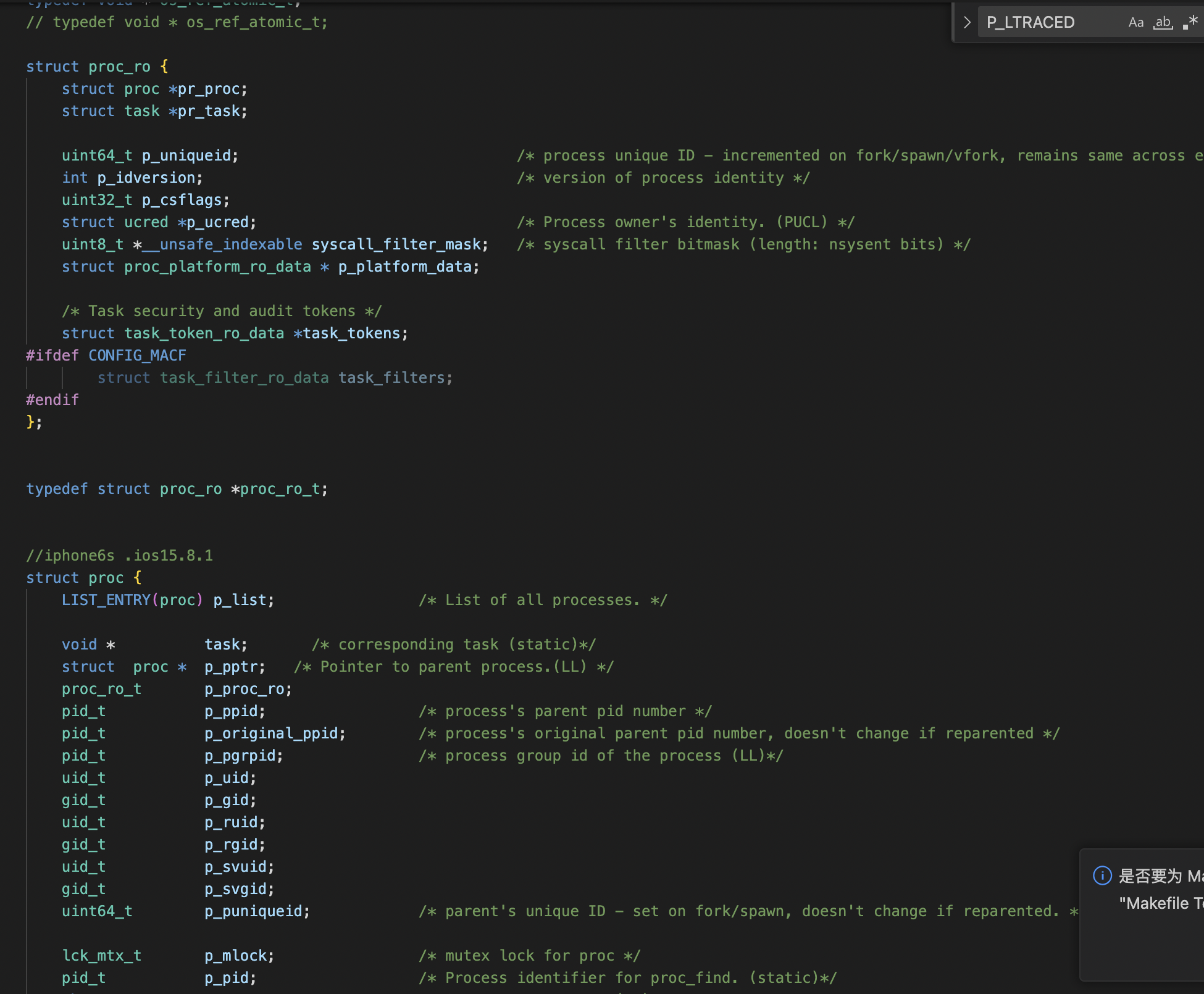
Dopamine越狱iOS15.8.1，IPhone6s；

1，查看unma -a 获取xnu版本，



2，下载源码xnu-8020.241.42，获取 proc 结构



3，通过计算p\_proc\_ro的地址，获取p\_uniqueid来判断对应的p\_list;

// 计算p\_proc\_ro的地址

uint64\_t p\_proc\_ro\_addr = proc2 + offsetof(struct proc, p\_proc\_ro);

// 读取p\_proc\_ro的值

uint64\_t proc\_ro\_addr = kread64(p\_proc\_ro\_addr);

// 计算p\_uniqueid的地址

uint64\_t p\_uniqueid\_addr = proc\_ro\_addr + offsetof(struct proc\_ro, p\_uniqueid);

// 读取p\_uniqueid的值

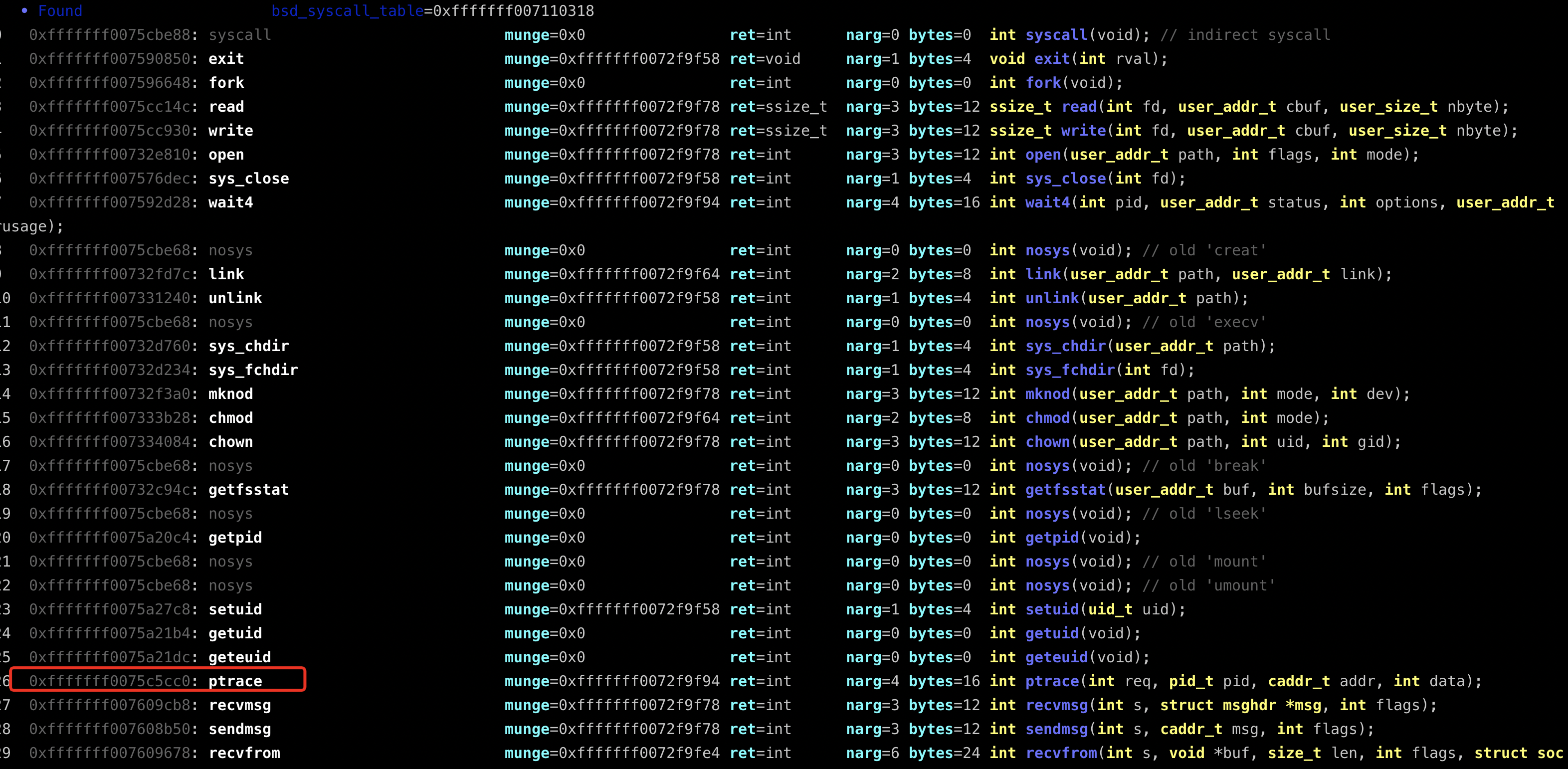
uint64\_t p\_uniqueid\_value = kread64(p\_uniqueid\_addr);

// 打印进程地址和p\_uniqueid值

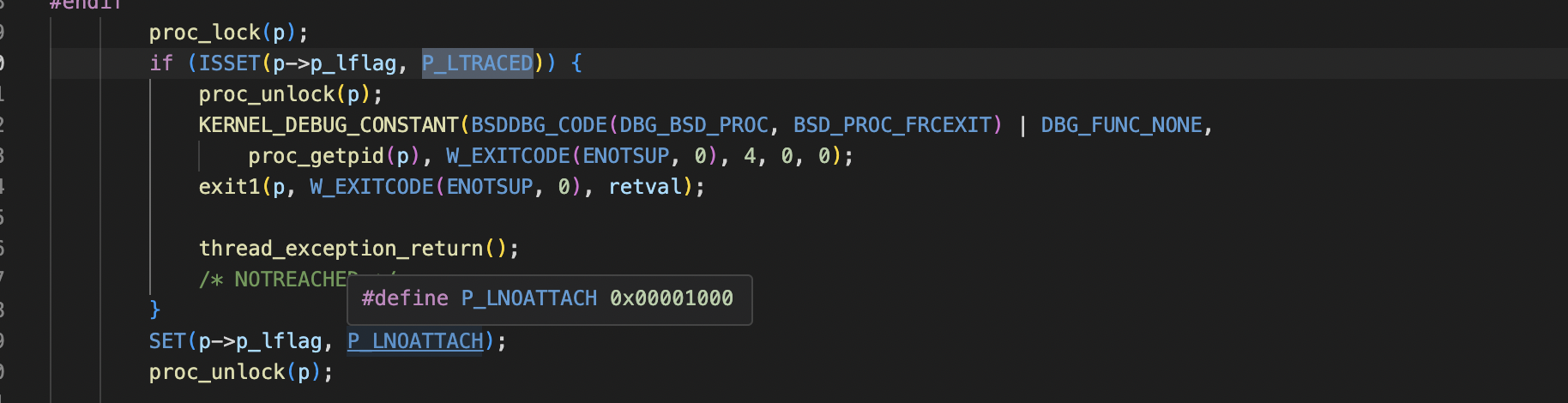
// printf("[i] Process at 0x%llx has unique ID: %llu\n", proc2, p\_uniqueid\_value);

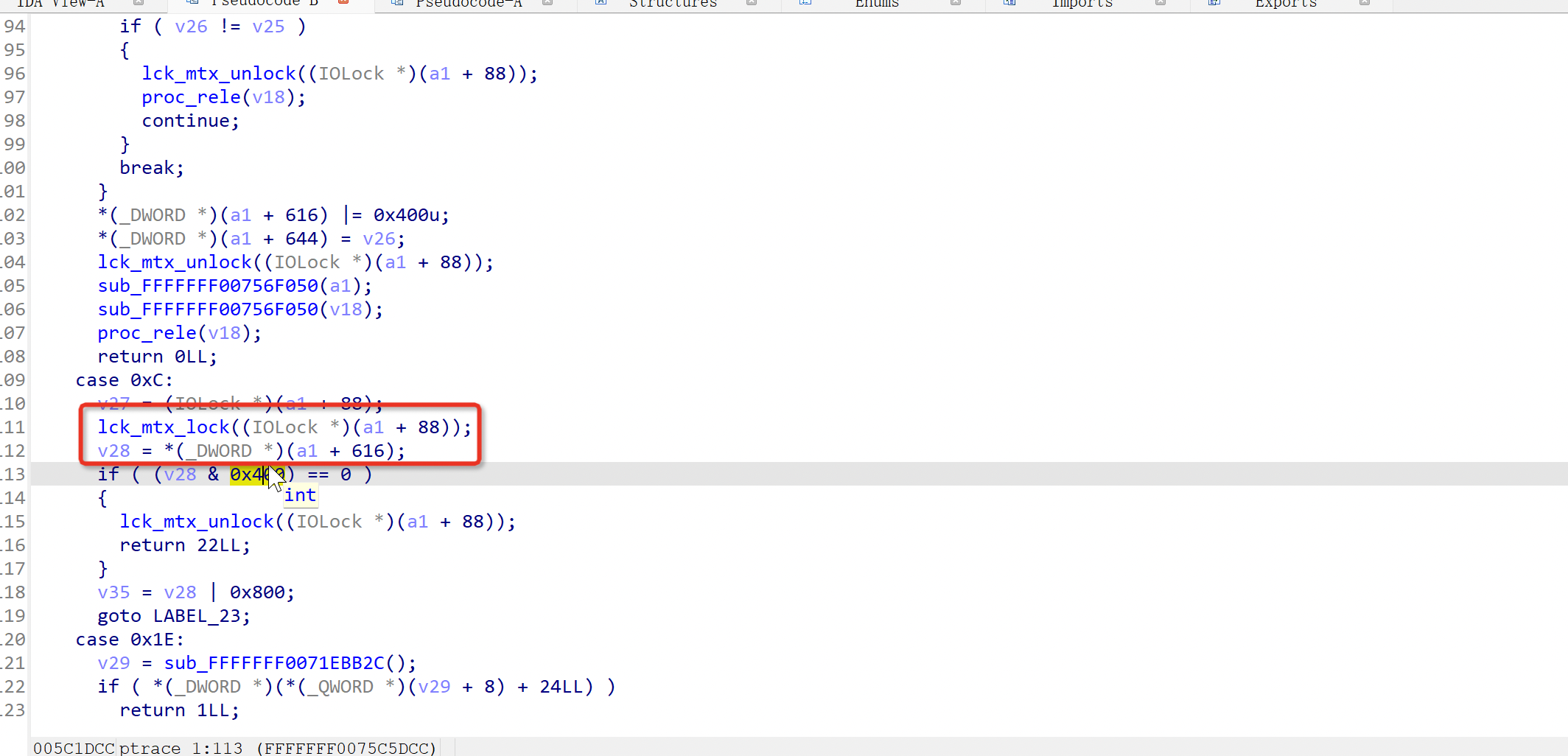
4,获取到pid对应pro地址来获取p\_lflag，

因为通过proc 结构异常，通过kernelcache.release.iPhone8,1解析获取ptrace 地址来判断p\_lflag偏移



对照源码可以知道p\_lflag偏移是0x268





5，最后就通过lflagoffset获取了lflag数据

