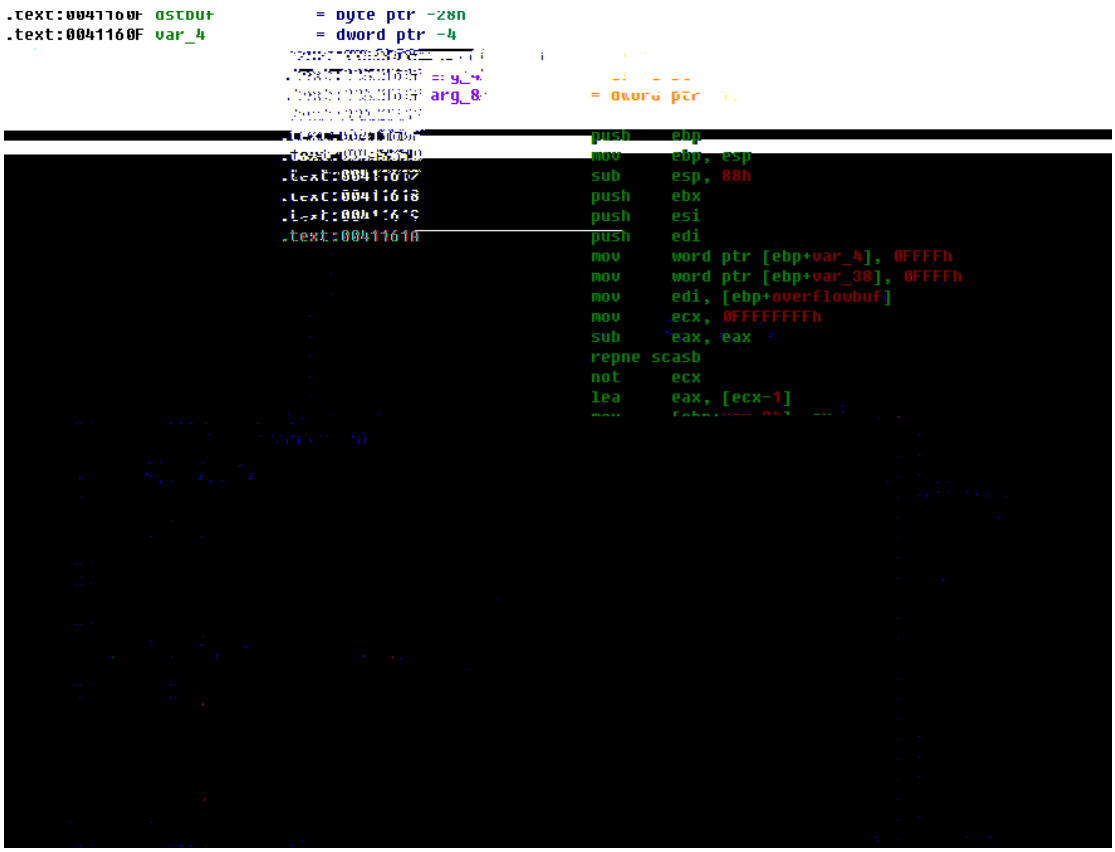
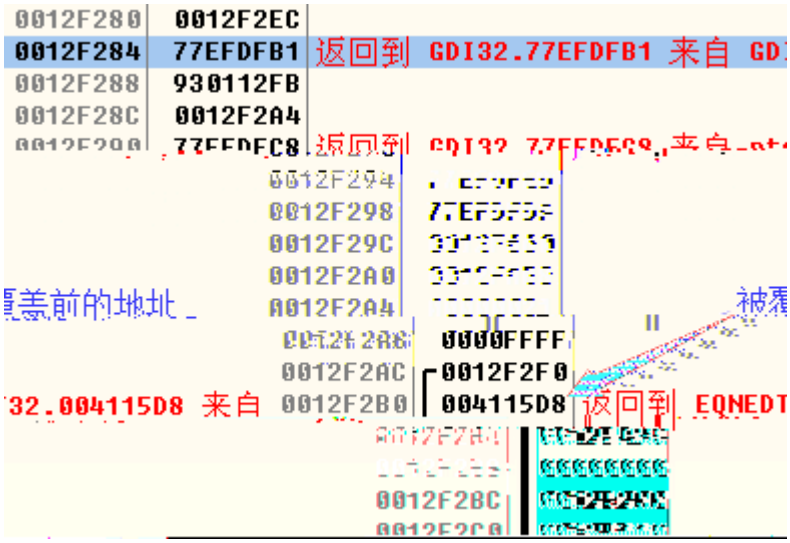
```
struct EQNOLEFILEHDR {
    WORD   cbHdr;
    DWORD  version;
```


.text:0041160F overflowbuf = byte ptr -28h
.text:0041160F var_4 = dword ptr -4
arg_8 = dword ptr
push ebp
mov ebp, esp
sub esp, 88h
push ebx
push esi
push edi
mov word ptr [ebp+var_4], 0FFFFh
mov word ptr [ebp+var_38], 0FFFFh
mov edi, [ebp+overflowbuf]
mov ecx, 0FFFFFFFFh
sub eax, eax
repne scasb
not ecx
lea eax, [ecx-1]


0012F280 0012F2EC
0012F284 77EFDFB1 返回到 GDI32.77EFDFB1 来自 GD
0012F288 930112FB
0012F28C 0012F2A4
0012F294
0012F298
0012F29C
0012F2A0
0012F2A4
0012F2A8 0000FFFF
0012F2AC 0012F2F0
0012F2B0 004115D8 返回到 EQNEDT
0012F2BC
盖前的地址
被覆
32.00411508 来自

ÿ C ÿ' C „

```
RD /d 0x400
```