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

```
.text:0041160F var_4          = dword ptr -4
.text:00411618                push    ebp
.text:00411619                mov     ebp, esp
.text:0041161A                sub     esp, 88h
.text:0041161D                push    ebx
.text:0041161E                push    esi
.text:0041161F                push    edi
.text:00411620                mov     word ptr [ebp+var_4], 0FFFFh
.text:00411626                mov     word ptr [ebp+var_38], 0FFFFh
.text:0041162C                mov     edi, [ebp+overflowbuf]
.text:00411632                mov     ecx, 0FFFFFFFFh
.text:00411637                sub     eax, eax
.text:00411639                repne scasb
.text:0041163B                not     ecx
.text:0041163D                lea     eax, [ecx-1]
```

```
0012F280  0012F2EC
0012F284  77EFDFB1  返回到 GDI32.77EFDFB1 来自 GD
0012F288  930112FB
0012F28C  0012F2A4
0012F290  77EFDFC8  返回到 GDI32.77EFDFC8 来自
0012F294
0012F298  77EF5F5F
0012F29C
0012F2A0
0012F2A4
0012F2A8  0000FFFF
0012F2AC  0012F2F0
0012F2B0  004115D8  返回到 EQNEDT
0012F2B4
0012F2B8
0012F2BC
0012F2C0
```

覆盖前的地址

被覆

32.004115D8 来自

```
RD /d 0x400
```