

本章开始 LyShark 将介绍如何在内核中实现 InlineHook 挂钩这门技术，内核挂钩的第一步需要实现一个动态计算汇编指令长度的功能，该功能可以使用 LDE64 这个反汇编引擎，该引擎小巧简单可以直接在驱动中使用，LDE引擎是 BeaEngine 引擎的一部分，后来让 Beatrix 打包成了一个 ShellCode 代码，并可以通过 typedef 动态指针的方式直接调用功能，本章内容作为后期 Hook 挂钩的铺垫部分，独立出来也是因为代码太多太占空间一篇文章写下来或很长影响阅读。

- LDE反汇编引擎源代码: <https://github.com/BeaEngine/lde64>

首先定义一个 lyshark_lde64.h 头文件，并写入如下 ShellCode 代码片段，当然这不是最新的，如果你需要最新的可以自己下载源代码编译后提取出来替换即可，不过该引擎很多年没有更新了替换的意义也不大毕竟功能就那么几行而已。

```
// 署名权
// right to sign one's name on a piece of work
// thanks to Av0id , cyberbob and lena151 for their remarks and advices
// PowerBy: BeaEngine | Beatrix | LyShark
// Email: me@lyshark.com

// 反汇编引擎
unsigned char szShellCode[12800] =
{
    0x55, 0x48, 0x83, 0xEC, 0x2B, 0x48, 0x89, 0xE5, 0x51, 0x52, 0x56, 0xE8, 0x00, 0x21,
    0x00, 0x00,
    0xEF, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xE7, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xDF, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xD7, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xE5, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x06, 0x22, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xED, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xE5, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xAF, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xA7, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x9F, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x97, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xA5, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xC6, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0xAD, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xBF, 0x2A, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x6F, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x67, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x5F, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x57, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x65, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x86, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x6D, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x65, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x2F, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x27, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
    0x1F, 0x21, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x17, 0x21, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00,
```

	0x25	0x21	0x00	0x00	0x00	0x00	0x00	0x00	0x46	0x21	0x00	0x00	0x00	0x00
0x00	0x00													
	0x2D	0x21	0x00	0x00	0x00	0x00	0x00	0x00	0x25	0x21	0x00	0x00	0x00	0x00
0x00	0x00													
	0xEF	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0xE7	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0xDF	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0xD7	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0xE5	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x06	0x21	0x00	0x00	0x00	0x00
0x00	0x00													
	0x98	0x21	0x00	0x00	0x00	0x00	0x00	0x00	0xE5	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0xAF	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0xA7	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x9F	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x97	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0xA5	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0xC6	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x58	0x21	0x00	0x00	0x00	0x00	0x00	0x00	0xA5	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x6F	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x67	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x5F	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x57	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x65	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x86	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x18	0x21	0x00	0x00	0x00	0x00	0x00	0x00	0x65	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x2F	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x27	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x1F	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x17	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x25	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x46	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0xD8	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x25	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x97	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x8F	0x20	0x00	0x00	0x00	0x00
0x00	0x00													
	0x87	0x20	0x00	0x00	0x00	0x00	0x00	0x00	0x7F	0x20	0x00	0x00	0x00	0x00
0x00	0x00													

	0x80,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x78,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x70,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x68,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x60,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x58,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x50,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x48,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x40,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x38,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x30,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x28,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x20,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x18,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x10,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x08,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x00,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF8,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x16,	0x20,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD7,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0xA8,	0x1F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA0,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0xDF,	0x26,	0x00,	0x00,	0x00,	0x00,	0x00,	0x0A,	0x27,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0xFD,	0x20,	0x00,	0x00,	0x00,	0x00,	0x00,	0x98,	0x20,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0xB5,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x06,	0x1F,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0xA0,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x98,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x90,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x88,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x85,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x7D,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x75,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x6D,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x65,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x5D,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x55,	0x1E,	0x00,	0x00,	0x00,	0x00,	0x00,	0x4D,	0x1E,	0x00,	0x00,	0x00,	0x00,	
0x00,	0x00,													
	0x45,	0x1E,	0x00,	0x00,										

[illegible]

0x80, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x78, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x70, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x68, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x60, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x58, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x50, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x48, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x5E, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x56, 0x1C, 0x00, 0x00, 0x00, 0x00	0x00, 0x00,
0x3F, 0x1D, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xE8, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x06, 0x1D, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xFE, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x2E, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xB4, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xDA, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xB8, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xFF, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xA8, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xA0, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x9D, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xAD, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x88, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x6F, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x67, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x5F, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x57, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x68, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x60, 0x1C, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x50, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x48, 0x1B, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xF2, 0x24, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x22, 0x25, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xB5, 0x25, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x11, 0x26, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x8A, 0x26, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xD6, 0x26, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x3A, 0x27, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x8B, 0x27, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0x05, 0x1B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xFD, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xF5, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xED, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xE5, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xDD, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xD5, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xCD, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xEE, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xE6, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,
0xB8, 0x1C, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xAD, 0x1A, 0x00, 0x00, 0x00, 0x00,	0x00, 0x00,

[illegible]

	0x38,	0x1A,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x30,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x28,	0x1A,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x20,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x4D,	0x1B,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x45,	0x1B,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x3D,	0x1B,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x35,	0x1B,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xAF,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA7,	0x18,	0x00,	0x00,	0x00,	0x00
0x00,	0x00,													
	0x9F,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x97,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x8F,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x87,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x7F,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x77,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x80,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x78,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x70,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x68,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x60,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x58,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xBD,	0x1A,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xB5,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xA0,	0x21,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA5,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xB9,	0x21,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x95,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x8D,	0x1A,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x85,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x7D,	0x1A,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x75,	0x1A,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xEF,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE7,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xDF,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD7,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xCF,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xC7,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xBF,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xB7,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													

	0x4F,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x47,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x3F,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x37,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x2F,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x27,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x1F,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x17,	0x17,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x0F,	0x17,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x07,	0x17,	0x00,	0x00,	0x00,	0x00
0x00,	0x00,													
	0xFF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xEF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xDF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xCF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xC7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xBF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xB7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xAF,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA7,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x9F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x97,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0xAB,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA3,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x7F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x77,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x6F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x7D,	0x1B,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x01,	0x1C,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x85,	0x1C,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x4F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x47,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x3F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x48,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x2F,	0x16,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x27,	0x16,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													
	0x9D,	0x18,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x95,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,													

[illegible]

	0x0F,	0x14,	0x00,	0x00,	0x00,	0x00,	0x00,	0x07,	0x14,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xFF,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF7,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xEF,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE7,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xDF,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD7,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xCF,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xC7,	0x13,	0x00,	0x00,	0x00,	0x00
0x00,	0x00,												
	0xBF,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x6F,	0x18,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xC0,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xB8,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xB0,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA8,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xA0,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x98,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x90,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x88,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x6F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x67,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x5F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x57,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x4F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x47,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xE7,	0x14,	0x00,	0x00,	0x00,	0x00,	0x00,	0x37,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x2F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x27,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x1F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x17,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x0F,	0x13,	0x00,	0x00,	0x00,	0x00,	0x00,	0x07,	0x13,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xFF,	0x12,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF7,	0x12,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xEF,	0x12,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE7,	0x12,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xDF,	0x12,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD7,	0x12,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0xCF,	0x12,	0x00,	0x00,	0x00,	0x00,	0x00,	0xC7,	0x12,	0x00,	0x00,	0x00,	0x00,
0x00,	0x00,												
	0x67,	0x14,	0x00,</										

[illegible]

[illegible]

	0xAD	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0xA5	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x9D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x95	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x8D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x85	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x7D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x75	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x6D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x65	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x5D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x55	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x4D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x45	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x3D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x35	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x2D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x25	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x1D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x15	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x0D	0x11	0x00	0x00	0x00	0x00	0x00	0x00	0x05	0x11	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xFD	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xF5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xED	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xE5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xDD	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xD5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xCD	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xC5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xBD	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xB5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0xAD	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0xA5	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x9D	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0x95	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x8D	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0x85	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													
	0x7D	0x10	0x00	0x00	0x00	0x00	0x00	0x00	0x75	0x10	0x00	0x00	0x00	0x00
0x00,	0x00,													

	0x0D,	0x10,	0x00,	0x00,	0x00,	0x00,	0x00,	0x00,	0x05,	0x10,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xFD,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF5,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xED,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE5,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xDD,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD5,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xCD,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xC5,	0x0F,	0x00,	0x00,	0x00,	0x00
	0x00,	0x00,												
		0xBD,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xB5,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xAD,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0xA5,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x9D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x95,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x8D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x85,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x7D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x75,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x6D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x65,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x5D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x55,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x4D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x45,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x3D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x35,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x2D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x25,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x1D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x15,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0x0D,	0x0F,	0x00,	0x00,	0x00,	0x00,	0x00,	0x05,	0x0F,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xFD,	0x0E,	0x00,	0x00,	0x00,	0x00,	0x00,	0xF5,	0x0E,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xED,	0x0E,	0x00,	0x00,	0x00,	0x00,	0x00,	0xE5,	0x0E,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xDD,	0x0E,	0x00,	0x00,	0x00,	0x00,	0x00,	0xD5,	0x0E,	0x00,	0x00,	0x00,	0x00,
	0x00,	0x00,												
		0xCD,	0x0E,	0x00,	0x00,	0x00,	0							

[illegible]

	0xCD	0x0C	0x00	0x00	0x00	0x00	0x00	0x00	0xC5	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xBD	0x0C	0x00	0x00	0x00	0x00	0x00	0xB5	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xAD	0x0C	0x00	0x00	0x00	0x00	0x00	0xA5	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x9D	0x0C	0x00	0x00	0x00	0x00	0x00	0x95	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x8D	0x0C	0x00	0x00	0x00	0x00	0x00	0x85	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x7D	0x0C	0x00	0x00	0x00	0x00	0x00	0x75	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x6D	0x0C	0x00	0x00	0x00	0x00	0x00	0x65	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x5D	0x0C	0x00	0x00	0x00	0x00	0x00	0x55	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x4D	0x0C	0x00	0x00	0x00	0x00	0x00	0x45	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x3D	0x0C	0x00	0x00	0x00	0x00	0x00	0x35	0x0C	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xCB	0x09	0x00	0x00	0x00	0x00	0x00	0xC3	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xBB	0x09	0x00	0x00	0x00	0x00	0x00	0xB3	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xAB	0x09	0x00	0x00	0x00	0x00	0x00	0xA3	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x9B	0x09	0x00	0x00	0x00	0x00	0x00	0x77	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xED	0x0B	0x00	0x00	0x00	0x00	0x00	0xE5	0x0B	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xDD	0x0B	0x00	0x00	0x00	0x00	0x00	0xD5	0x0B	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x6B	0x09	0x00	0x00	0x00	0x00	0x00	0x63	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x5B	0x09	0x00	0x00	0x00	0x00	0x00	0x53	0x09	0x00	0x00	0x00	0x00
	0x00	0x00												
		0xAD	0x0B	0x00	0x00	0x00	0x00	0x00	0xA5	0x0B	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x9D	0x0B	0x00	0x00	0x00	0x00	0x00	0x95	0x0B	0x00	0x00	0x00	0x00
	0x00	0x00												
		0x8D	0x0B	0x00	0x00	0x00								

[illegible]

[illegible]

[illegible]

[illegible]

0xAD, 0x04, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xA5, 0x04, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x9D, 0x04, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x95, 0x04, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x8D, 0x04, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x85, 0x04, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x7D, 0x04, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x75, 0x04, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xAC, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xA4, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x9C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x94, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x8D, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xAF, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xB3, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x74, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x6C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x64, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x5C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x54, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x4D, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x44, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x3C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x34, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x2C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x24, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x1C, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x14, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x0D, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x04, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xFC, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xF4, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xEC, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xE4, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xDC, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xD4, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xCC, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xC4, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0xBC, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xB4, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00,
0x5E, 0x51, 0x8F, 0x45, 0x23, 0x89, 0x55, 0x1E, 0xC6, 0x45, 0x22, 0x00, 0xC7, 0x45,
0x02, 0x20,
0x00, 0x00, 0x00, 0xC7, 0x45, 0x06, 0x20, 0x00, 0x00, 0x00, 0x83, 0x7D, 0x1E, 0x40,
0x75, 0x07,
0xC7, 0x45, 0x06, 0x40, 0x00, 0x00, 0x00, 0x48, 0x8B, 0x45, 0x23, 0x48, 0x0F, 0xB6,
0x08, 0x48,
0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0x5E, 0x5A, 0x59, 0x48, 0x83, 0xF8,
0xFF, 0x74,
0x07, 0x48, 0x8B, 0x45, 0x23, 0x48, 0x29, 0xC8, 0x48, 0x83, 0xC4, 0x2B, 0x5D, 0xC3,
0xC7, 0x45,
0x1A, 0x00, 0x00, 0x00, 0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x25,
0xC7, 0x00,

0x00, 0x00, 0xB9, 0x40, 0x00, 0x00, 0x00, 0x48, 0x31, 0xD2, 0xF7, 0xF1, 0x89, 0x45,
0x0A, 0x83,
0xF8, 0x01, 0x75, 0x04, 0x83, 0x45, 0x1A, 0x01, 0x83, 0xF8, 0x02, 0x75, 0x04, 0x83,
0x45, 0x1A,
0x04, 0x89, 0x55, 0x0E, 0xC1, 0xE0, 0x06, 0x48, 0x01, 0xF0, 0x48, 0x05, 0x00, 0x20,
0x00, 0x00,
0x48, 0x8D, 0x04, 0xD0, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC3, 0x48, 0x8B, 0x45, 0x23,
0x0F, 0xB6,
0x40, 0x01, 0x83, 0xE0, 0x38, 0xC1, 0xE8, 0x03, 0x89, 0x45, 0x16, 0xC3, 0xC3, 0x83,
0x7D, 0x06,
0x20, 0x7C, 0x23, 0x83, 0x45, 0x1A, 0x01, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40,
0x02, 0x83,
0xE0, 0x07, 0x89, 0x45, 0x12, 0x83, 0x7D, 0x12, 0x05, 0x75, 0x0A, 0x83, 0x7D, 0x0A,
0x00, 0x75,
0x04, 0x83, 0x45, 0x1A, 0x04, 0xC3, 0xC3, 0x83, 0x7D, 0x06, 0x20, 0x7C, 0x05, 0x83,
0x45, 0x1A,
0x04, 0xC3, 0xC3, 0x83, 0x7D, 0x06, 0x10, 0x75, 0x05, 0x83, 0x45, 0x1A, 0x02, 0xC3,
0xC3, 0xE8,
0x5A, 0xFF, 0xFF, 0xFF, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23,
0x02, 0xC3,
0x48, 0xFF, 0x45, 0x23, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0x83, 0x7D, 0x02,
0x10, 0x75,
0x06, 0xE8, 0xD9, 0xFF, 0xFF, 0xFF, 0xC3, 0xE8, 0x51, 0x02, 0x00, 0x00, 0xC3, 0x83,
0x7D, 0x1E,
0x40, 0x75, 0x06, 0xE8, 0x45, 0x02, 0x00, 0x00, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xC3,
0x83, 0x7D,
0x02, 0x20, 0x7C, 0x06, 0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0x48, 0x83, 0x45, 0x23,
0x03, 0xC3,
0x83, 0x7D, 0x02, 0x40, 0x75, 0x06, 0x48, 0x83, 0x45, 0x23, 0x09, 0xC3, 0x83, 0x7D,
0x02, 0x20,
0x75, 0x06, 0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x03, 0xC3,
0xE8, 0x8C,
0xFF, 0xFF, 0xFF, 0x48, 0xFF, 0x45, 0x23, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x24,
0xC7, 0x45,
0x02, 0x40, 0x00, 0x00, 0x00, 0x48, 0xFF, 0x45, 0x23, 0x48, 0x8B, 0x45, 0x23, 0x48,
0x0F, 0xB6,
0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC7, 0x45, 0x02, 0x20,
0x00, 0x00,
0x00, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x25, 0x48,
0xFF, 0x45,
0x23, 0xFE, 0x45, 0x22, 0x80, 0x7D, 0x22, 0x0F, 0x75, 0x06, 0xE8, 0xBE, 0x01, 0x00,
0x00, 0xC3,
0x48, 0x8B, 0x45, 0x23, 0x48, 0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03,
0x00, 0xFF,
0xD0, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x01, 0xC3, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22,
0x80, 0x7D,
0x22, 0x0F, 0x75, 0x06, 0xE8, 0x94, 0x01, 0x00, 0x00, 0xC3, 0x48, 0x8B, 0x45, 0x23,
0x48, 0x0F,
0xB6, 0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC3, 0x83, 0x7D,
0x02, 0x20,
0x7C, 0x0B, 0xE8, 0xF8, 0xFE, 0xFF, 0xFF, 0x48, 0x83, 0x45, 0x23, 0x04, 0xC3, 0xE8,
0xED, 0xFE,

0xFF, 0xFF, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x06,
0xE8, 0x5A,
0x01, 0x00, 0x00, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0x48, 0x83, 0x45, 0x23,
0x04, 0xC3,
0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x06, 0xE8, 0x3C,
0x01, 0x00,
0x00, 0xC3, 0xE8, 0xB8, 0xFE, 0xFF, 0xFF, 0xC3, 0xE8, 0x11, 0xFE, 0xFF, 0xFF, 0x83,
0x7D, 0x0A,
0x03, 0x75, 0x06, 0xE8, 0xA7, 0xFE, 0xFF, 0xFF, 0xC3, 0xE8, 0x1F, 0x01, 0x00, 0x00,
0xC3, 0x48,
0x83, 0x45, 0x23, 0x03, 0xC3, 0x83, 0x7D, 0x06, 0x40, 0x75, 0x06, 0x48, 0x83, 0x45,
0x23, 0x09,
0xC3, 0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0x83, 0x7D, 0x06, 0x10, 0x75, 0x06, 0x48,
0x83, 0x45,
0x23, 0x03, 0xC3, 0x83, 0x7D, 0x06, 0x20, 0x75, 0x06, 0x48, 0x83, 0x45, 0x23, 0x05,
0xC3, 0x48,
0x83, 0x45, 0x23, 0x09, 0xC3, 0x80, 0x7D, 0x00, 0x01, 0x75, 0x06, 0xE8, 0x5F, 0xFE,
0xFF, 0xFF,
0xC3, 0xE8, 0xD7, 0x00, 0x00, 0x00, 0xC3, 0x80, 0x7D, 0x00, 0x01, 0x75, 0x06, 0xE8,
0x4D, 0xFE,
0xFF, 0xFF, 0xC3, 0x80, 0x7D, 0x01, 0x01, 0x75, 0x06, 0xE8, 0x41, 0xFE, 0xFF, 0xFF,
0xC3, 0x83,
0x7D, 0x02, 0x10, 0x75, 0x06, 0xE8, 0x35, 0xFE, 0xFF, 0xFF, 0xC3, 0xE8, 0xAD, 0x00,
0x00, 0x00,
0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x06, 0xE8, 0xA1, 0x00, 0x00, 0x00, 0xC3, 0x83,
0x7D, 0x02,
0x20, 0x75, 0x06, 0x48, 0x83, 0x45, 0x23, 0x07, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x05,
0xC3, 0xC3,
0x83, 0x7D, 0x02, 0x10, 0x74, 0x11, 0xE8, 0x63, 0xFD, 0xFF, 0xFF, 0x8B, 0x45, 0x1A,
0x01, 0x45,
0x23, 0x48, 0x83, 0x45, 0x23, 0x06, 0xC3, 0xE8, 0x52, 0xFD, 0xFF, 0xFF, 0x8B, 0x45,
0x1A, 0x01,
0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x04, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x06,
0xE8, 0x5A,
0x00, 0x00, 0x00, 0xC3, 0x83, 0x7D, 0x02, 0x20, 0x75, 0x06, 0x48, 0x83, 0x45, 0x23,
0x07, 0xC3,
0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0xE8, 0x6F, 0xFD, 0xFF, 0xFF, 0x83, 0x7D, 0x16,
0x00, 0x75,
0x06, 0xE8, 0xB9, 0xFD, 0xFF, 0xFF, 0xC3, 0xE8, 0x31, 0x00, 0x00, 0x00, 0xC3, 0x83,
0x7D, 0x1E,
0x40, 0x75, 0x06, 0x48, 0x83, 0x45, 0x23, 0x05, 0xC3, 0x83, 0x7D, 0x02, 0x20, 0x75,
0x06, 0x48,
0x83, 0x45, 0x23, 0x05, 0xC3, 0x48, 0x83, 0x45, 0x23, 0x03, 0xC3, 0x80, 0x7D, 0x00,
0x01, 0x75,
0x06, 0xE8, 0x89, 0xFD, 0xFF, 0xFF, 0xC3, 0xE8, 0x01, 0x00, 0x00, 0x00, 0xC3, 0x48,
0xB8, 0xFF,
0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x06,
0xE8, 0xEA,
0xFF, 0xFF, 0xFF, 0xC3, 0xE8, 0x66, 0xFD, 0xFF, 0xFF, 0x48, 0x83, 0x45, 0x23, 0x01,
0xC3, 0x83,
0x7D, 0x02, 0x20, 0x7C, 0x0B, 0xE8, 0x55, 0xFD, 0xFF, 0xFF, 0x48, 0x83, 0x45, 0x23,
0x04, 0xC3,

0xE8, 0x4A, 0xFD, 0xFF, 0xFF, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8, 0x9E, 0xFC,
0xFF, 0xFF,
0xE8, 0xE5, 0xFC, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x0C, 0x8B, 0x45, 0x1A,
0x01, 0x45,
0x23, 0x48, 0x83, 0x45, 0x23, 0x03, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x06, 0xE8,
0x9B, 0xFF,
0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02,
0xC3, 0x83,
0x7D, 0x02, 0x20, 0x7C, 0x34, 0xE8, 0x64, 0xFC, 0xFF, 0xFF, 0xE8, 0xAB, 0xFC, 0xFF,
0xFF, 0x83,
0x7D, 0x16, 0x00, 0x75, 0x0C, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45,
0x23, 0x06,
0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x06, 0xE8, 0x61, 0xFF, 0xFF, 0xFF, 0xC3, 0x8B,
0x45, 0x1A,
0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8, 0x30, 0xFC, 0xFF, 0xFF,
0xE8, 0x77,
0xFC, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x0C, 0x8B, 0x45, 0x1A, 0x01, 0x45,
0x23, 0x48,
0x83, 0x45, 0x23, 0x04, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x06, 0xE8, 0x2D, 0xFF,
0xFF, 0xFF,
0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8,
0xFC, 0xFB,
0xFF, 0xFF, 0xE8, 0x43, 0xFC, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x01, 0x7E, 0x06, 0xE8,
0x0B, 0xFF,
0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02,
0xC3, 0xE8,
0x26, 0xFC, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x06, 0x7E, 0x06, 0xE8, 0xEE, 0xFE, 0xFF,
0xFF, 0xC3,
0xE8, 0xC9, 0xFB, 0xFF, 0xFF, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45,
0x23, 0x02,
0xC3, 0xE8, 0xB8, 0xFB, 0xFF, 0xFF, 0xE8, 0xFF, 0xFB, 0xFF, 0xFF, 0x83, 0x7D, 0x16,
0x05, 0x7E,
0x06, 0xE8, 0xC7, 0xFE, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48,
0x83, 0x45,
0x23, 0x02, 0xC3, 0xE8, 0x96, 0xFB, 0xFF, 0xFF, 0xE8, 0xDD, 0xFB, 0xFF, 0xFF, 0x83,
0x7D, 0x16,
0x00, 0x75, 0x1A, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x85, 0xAC, 0x00, 0x00, 0x00, 0x83,
0x7D, 0x0E,
0x04, 0x0F, 0x8E, 0xA2, 0x00, 0x00, 0x00, 0xE8, 0x91, 0xFE, 0xFF, 0xFF, 0xC3, 0x83,
0x7D, 0x16,
0x01, 0x75, 0x1A, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x85, 0x8C, 0x00, 0x00, 0x00, 0x83,
0x7D, 0x0E,
0x01, 0x0F, 0x8E, 0x82, 0x00, 0x00, 0x00, 0xE8, 0x71, 0xFE, 0xFF, 0xFF, 0xC3, 0x83,
0x7D, 0x16,
0x02, 0x75, 0x10, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x85, 0x6C, 0x00, 0x00, 0x00, 0xE8,
0x5B, 0xFE,
0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75, 0x0C, 0x83, 0x7D, 0x0A, 0x03, 0x75,
0x5A, 0xE8,
0x49, 0xFE, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x0C, 0x83, 0x7D, 0x0A,
0x03, 0x75,
0x48, 0xE8, 0x37, 0xFE, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x05, 0x75, 0x06, 0xE8,
0x2B, 0xFE,

0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x06, 0x75, 0x0C, 0x83, 0x7D, 0x0A, 0x03, 0x75,
0x2A, 0xE8,
0x19, 0xFE, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x07, 0x75, 0x1E, 0x83, 0x7D, 0x0A,
0x03, 0x75,
0x18, 0x83, 0x7D, 0x1E, 0x40, 0x75, 0x0C, 0x83, 0x7D, 0x0E, 0x00, 0x74, 0x0C, 0xE8,
0xFB, 0xFD,
0xFF, 0xFF, 0xC3, 0xE8, 0xF5, 0xFD, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45,
0x23, 0x48,
0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8, 0xC4, 0xFA, 0xFF, 0xFF, 0xE8, 0x0B, 0xFB, 0xFF,
0xFF, 0x83,
0x7D, 0x16, 0x04, 0x7D, 0x06, 0xE8, 0xD3, 0xFD, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A,
0x01, 0x45,
0x23, 0x48, 0x83, 0x45, 0x23, 0x03, 0xC3, 0xE8, 0xA2, 0xFA, 0xFF, 0xFF, 0xE8, 0xE9,
0xFA, 0xFF,
0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x06, 0xE8, 0xB1, 0xFD, 0xFF, 0xFF, 0xC3, 0x83,
0x7D, 0x16,
0x02, 0x75, 0x06, 0xE8, 0xA5, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75,
0x06, 0xE8,
0x99, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x06, 0xE8, 0x8D, 0xFD,
0xFF, 0xFF,
0xC3, 0x83, 0x7D, 0x16, 0x05, 0x75, 0x06, 0xE8, 0x81, 0xFD, 0xFF, 0xFF, 0xC3, 0x83,
0x7D, 0x16,
0x07, 0x7E, 0x06, 0xE8, 0x75, 0xFD, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45,
0x23, 0x48,
0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8, 0x90, 0xFA, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x00,
0x75, 0x06,
0xE8, 0x58, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x06, 0xE8, 0x4C,
0xFD, 0xFF,
0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x02, 0x75, 0x11, 0xE8, 0x21, 0xFA, 0xFF, 0xFF, 0x83,
0x7D, 0x0A,
0x03, 0x74, 0x52, 0xE8, 0x35, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75,
0x06, 0xE8,
0x29, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x11, 0xE8, 0xFE, 0xF9,
0xFF, 0xFF,
0x83, 0x7D, 0x0A, 0x03, 0x74, 0x2F, 0xE8, 0x12, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D,
0x16, 0x05,
0x75, 0x06, 0xE8, 0x06, 0xFD, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x06, 0x75, 0x11,
0xE8, 0xDB,
0xF9, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x74, 0x0C, 0xE8, 0xEF, 0xFC, 0xFF, 0xFF,
0xC3, 0xE8,
0xE9, 0xFC, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45,
0x23, 0x03,
0xC3, 0xE8, 0x04, 0xFA, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x06, 0xE8, 0xCC,
0xFC, 0xFF,
0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x06, 0xE8, 0xC0, 0xFC, 0xFF, 0xFF, 0xC3,
0x83, 0x7D,
0x16, 0x02, 0x75, 0x11, 0xE8, 0x95, 0xF9, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x74,
0x52, 0xE8,
0xA9, 0xFC, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75, 0x06, 0xE8, 0x9D, 0xFC,
0xFF, 0xFF,
0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x11, 0xE8, 0x72, 0xF9, 0xFF, 0xFF, 0x83, 0x7D,
0x0A, 0x03,

0x74, 0x2F, 0xE8, 0x86, 0xFC, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x05, 0x75, 0x06,
0xE8, 0x7A,
0xFC, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x06, 0x75, 0x11, 0xE8, 0x4F, 0xF9, 0xFF,
0xFF, 0x83,
0x7D, 0x0A, 0x03, 0x74, 0x0C, 0xE8, 0x63, 0xFC, 0xFF, 0xFF, 0xC3, 0xE8, 0x5D, 0xFC,
0xFF, 0xFF,
0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x03, 0xC3, 0xE8,
0x78, 0xF9,
0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x06, 0xE8, 0x40, 0xFC, 0xFF, 0xFF, 0xC3,
0x83, 0x7D,
0x16, 0x01, 0x75, 0x06, 0xE8, 0x34, 0xFC, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x02,
0x75, 0x15,
0xE8, 0x09, 0xF9, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x84, 0x7B, 0x00, 0x00,
0x00, 0xE8,
0x19, 0xFC, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75, 0x1D, 0x83, 0x7D, 0x02,
0x10, 0x75,
0x11, 0xE8, 0xE8, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x74, 0x5E, 0xE8, 0xFC,
0xFB, 0xFF,
0xFF, 0xC3, 0xE8, 0xF6, 0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x06,
0xE8, 0xEA,
0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x05, 0x75, 0x06, 0xE8, 0xDE, 0xFB, 0xFF,
0xFF, 0xC3,
0x83, 0x7D, 0x16, 0x06, 0x75, 0x11, 0xE8, 0xB3, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x0A,
0x03, 0x74,
0x29, 0xE8, 0xC7, 0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x07, 0x75, 0x17, 0x83,
0x7D, 0x02,
0x10, 0x75, 0x11, 0xE8, 0x96, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x74, 0x0C,
0xE8, 0xAA,
0xFB, 0xFF, 0xFF, 0xC3, 0xE8, 0xA4, 0xFB, 0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01,
0x45, 0x23,
0x48, 0x83, 0x45, 0x23, 0x03, 0xC3, 0xE8, 0xBF, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x16,
0x00, 0x75,
0x15, 0xE8, 0x68, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x85, 0xA0, 0x00,
0x00, 0x00,
0xE8, 0x78, 0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x15, 0xE8, 0x4D,
0xF8, 0xFF,
0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x0F, 0x85, 0x85, 0x00, 0x00, 0x00, 0x00, 0xE8, 0x5D, 0xFB,
0xFF, 0xFF,
0xC3, 0x83, 0x7D, 0x16, 0x02, 0x75, 0x15, 0xE8, 0x32, 0xF8, 0xFF, 0xFF, 0x83, 0x7D,
0x0A, 0x03,
0x0F, 0x85, 0x6A, 0x00, 0x00, 0x00, 0xE8, 0x42, 0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D,
0x16, 0x03,
0x75, 0x11, 0xE8, 0x17, 0xF8, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x75, 0x53, 0xE8,
0x2B, 0xFB,
0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x04, 0x75, 0x06, 0xE8, 0x1F, 0xFB, 0xFF, 0xFF,
0xC3, 0x83,
0x7D, 0x16, 0x05, 0x75, 0x11, 0xE8, 0xF4, 0xF7, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03,
0x75, 0x30,
0xE8, 0x08, 0xFB, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x06, 0x75, 0x11, 0xE8, 0xDD,
0xF7, 0xFF,
0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x75, 0x19, 0xE8, 0xF1, 0xFA, 0xFF, 0xFF, 0xC3, 0x83,
0x7D, 0x16,

0x07, 0x7F, 0x07, 0xE8, 0xC6, 0xF7, 0xFF, 0xFF, 0xEB, 0x06, 0xE8, 0xDE, 0xFA, 0xFF,
0xFF, 0xC3,
0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xE8, 0xF9,
0xF7, 0xFF,
0xFF, 0x83, 0x7D, 0x16, 0x00, 0x75, 0x11, 0xE8, 0xA2, 0xF7, 0xFF, 0xFF, 0x83, 0x7D,
0x0A, 0x03,
0x75, 0x51, 0xE8, 0xB6, 0xFA, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x11,
0xE8, 0x8B,
0xF7, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x75, 0x3A, 0xE8, 0x9F, 0xFA, 0xFF, 0xFF,
0xC3, 0x83,
0x7D, 0x16, 0x02, 0x75, 0x11, 0xE8, 0x74, 0xF7, 0xFF, 0xFF, 0x83, 0x7D, 0x0A, 0x03,
0x75, 0x23,
0xE8, 0x88, 0xFA, 0xFF, 0xFF, 0xC3, 0x83, 0x7D, 0x16, 0x03, 0x75, 0x11, 0xE8, 0x5D,
0xF7, 0xFF,
0xFF, 0x83, 0x7D, 0x0A, 0x03, 0x75, 0x0C, 0xE8, 0x71, 0xFA, 0xFF, 0xFF, 0xC3, 0xE8,
0x6B, 0xFA,
0xFF, 0xFF, 0xC3, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02,
0xC3, 0x48,
0xFF, 0x45, 0x23, 0xC7, 0x45, 0x02, 0x10, 0x00, 0x00, 0x00, 0xFE, 0x45, 0x22, 0x80,
0x7D, 0x22,
0x0F, 0x75, 0x06, 0xE8, 0x45, 0xFA, 0xFF, 0xFF, 0xC3, 0x48, 0x8B, 0x45, 0x23, 0x48,
0x0F, 0xB6,
0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC7, 0x45, 0x02, 0x20,
0x00, 0x00,
0x00, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22, 0x80, 0x7D, 0x22, 0x0F, 0x75,
0x06, 0xE8,
0x19, 0xFA, 0xFF, 0xFF, 0xC3, 0x8B, 0x4D, 0x06, 0xD1, 0xE9, 0x89, 0x5D, 0x06, 0x48,
0x8B, 0x45,
0x23, 0x48, 0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0,
0x8B, 0x5D,
0x06, 0xD1, 0xE1, 0x89, 0x4D, 0x06, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22,
0x80, 0x7D,
0x22, 0x0F, 0x75, 0x06, 0xE8, 0xE4, 0xF9, 0xFF, 0xFF, 0xC3, 0x48, 0x8B, 0x45, 0x23,
0x0F, 0xB6,
0x00, 0x3C, 0xA4, 0x74, 0x12, 0x3C, 0xA7, 0x74, 0x0E, 0x3C, 0xAE, 0x74, 0x0A, 0x3C,
0xAF, 0x74,
0x06, 0x3C, 0x0F, 0x74, 0x02, 0xEB, 0x04, 0xC6, 0x45, 0x00, 0x01, 0x48, 0x8B, 0x45,
0x23, 0x48,
0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC6, 0x45,
0x00, 0x00,
0xC3, 0x48, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22, 0x80, 0x7D, 0x22, 0x0F, 0x75, 0x06,
0xE8, 0x9A,
0xF9, 0xFF, 0xFF, 0xC3, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x00, 0x3C, 0x90, 0x74,
0x3E, 0x3C,
0xA4, 0x74, 0x3A, 0x3C, 0xA5, 0x74, 0x36, 0x3C, 0xA6, 0x74, 0x32, 0x3C, 0xA7, 0x74,
0x2E, 0x3C,
0xAA, 0x74, 0x2A, 0x3C, 0xAB, 0x74, 0x26, 0x3C, 0xAC, 0x74, 0x22, 0x3C, 0xAD, 0x74,
0x1E, 0x3C,
0xAE, 0x74, 0x1A, 0x3C, 0xAF, 0x74, 0x16, 0x3C, 0x6C, 0x74, 0x12, 0x3C, 0x6D, 0x74,
0x0E, 0x3C,
0x6E, 0x74, 0x0A, 0x3C, 0x6F, 0x74, 0x06, 0x3C, 0x0F, 0x74, 0x02, 0xEB, 0x04, 0xC6,
0x45, 0x01,

0x01, 0x48, 0x8B, 0x45, 0x23, 0x48, 0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x04, 0xCE, 0x48,
0x03, 0x00,
0xFF, 0xD0, 0xC6, 0x45, 0x01, 0x00, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22,
0x80, 0x7D,
0x22, 0x0F, 0x75, 0x06, 0xE8, 0x24, 0xF9, 0xFF, 0xFF, 0xC3, 0x48, 0x8B, 0x45, 0x23,
0x48, 0x0F,
0xB6, 0x08, 0x48, 0x8D, 0x84, 0xCE, 0x00, 0x08, 0x00, 0x00, 0x48, 0x03, 0x00, 0xFF,
0xD0, 0xC3,
0x48, 0xFF, 0x45, 0x23, 0xFE, 0x45, 0x22, 0x80, 0x7D, 0x22, 0x0F, 0x75, 0x06, 0xE8,
0xFB, 0xF8,
0xFF, 0xFF, 0xC3, 0x48, 0x8B, 0x45, 0x23, 0x48, 0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x84,
0xCE, 0x00,
0x10, 0x00, 0x00, 0x48, 0x03, 0x00, 0xFF, 0xD0, 0xC3, 0x48, 0xFF, 0x45, 0x23, 0xFE,
0x45, 0x22,
0x80, 0x7D, 0x22, 0x0F, 0x75, 0x06, 0xE8, 0xD2, 0xF8, 0xFF, 0xFF, 0xC3, 0x48, 0x8B,
0x45, 0x23,
0x48, 0x0F, 0xB6, 0x08, 0x48, 0x8D, 0x84, 0xCE, 0x00, 0x18, 0x00, 0x00, 0x48, 0x03,
0x00, 0xFF,
0xD0, 0xC3, 0xC7, 0x45, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F,
0xB6, 0x40,
0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00, 0x7F, 0x11, 0xE8, 0xCD, 0xF5, 0xFF, 0xFF, 0x83,
0x7D, 0x16,
0x07, 0x7E, 0x06, 0xE8, 0x95, 0xF8, 0xFF, 0xFF, 0xC3, 0xE8, 0x70, 0xF5, 0xFF, 0xFF,
0x8B, 0x45,
0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xC7, 0x45, 0x1A, 0x00,
0x00, 0x00,
0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00,
0x7F, 0x17,
0xE8, 0x95, 0xF5, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x01, 0x75, 0x69, 0x83, 0x7D, 0x16,
0x07, 0x7E,
0x63, 0xE8, 0x57, 0xF8, 0xFF, 0xFF, 0xC3, 0x3D, 0xC0, 0x00, 0x00, 0x00, 0x7C, 0x56,
0x89, 0xC2,
0xC1, 0xEA, 0x04, 0x89, 0xC1, 0x83, 0xE1, 0x0F, 0x83, 0xFA, 0x0D, 0x75, 0x0B, 0x83,
0xF9, 0x00,
0x74, 0x42, 0xE8, 0x36, 0xF8, 0xFF, 0xFF, 0xC3, 0x83, 0xFA, 0x0E, 0x75, 0x37, 0x83,
0xF9, 0x02,
0x75, 0x06, 0xE8, 0x26, 0xF8, 0xFF, 0xFF, 0xC3, 0x83, 0xF9, 0x03, 0x75, 0x06, 0xE8,
0x1B, 0xF8,
0xFF, 0xFF, 0xC3, 0x83, 0xF9, 0x06, 0x75, 0x06, 0xE8, 0x10, 0xF8, 0xFF, 0xFF, 0xC3,
0x83, 0xF9,
0x07, 0x75, 0x06, 0xE8, 0x05, 0xF8, 0xFF, 0xFF, 0xC3, 0x83, 0xF9, 0x0F, 0x75, 0x06,
0xE8, 0xFA,
0xF7, 0xFF, 0xFF, 0xC3, 0xE8, 0xD5, 0xF4, 0xFF, 0xFF, 0x8B, 0x45, 0x1A, 0x01, 0x45,
0x23, 0x48,
0x83, 0x45, 0x23, 0x02, 0xC3, 0xC7, 0x45, 0x1A, 0x00, 0x00, 0x00, 0x00, 0x48, 0x8B,
0x45, 0x23,
0x0F, 0xB6, 0x40, 0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00, 0x7F, 0x11, 0xE8, 0xFA, 0xF4,
0xFF, 0xFF,
0x83, 0x7D, 0x16, 0x07, 0x7E, 0x32, 0xE8, 0xC2, 0xF7, 0xFF, 0xFF, 0xC3, 0x3D, 0xC0,
0x00, 0x00,
0x00, 0x7C, 0x25, 0x89, 0xC2, 0xC1, 0xEA, 0x04, 0x89, 0xC1, 0x83, 0xE1, 0x0F, 0x83,
0xFA, 0x0E,

0x75, 0x0B, 0x83, 0xF9, 0x09, 0x74, 0x11, 0xE8, 0xA1, 0xF7, 0xFF, 0xFF, 0xC3, 0x83,
0xFA, 0x0F,
0x75, 0x06, 0xE8, 0x96, 0xF7, 0xFF, 0xFF, 0xC3, 0xE8, 0x71, 0xF4, 0xFF, 0xFF, 0x8B,
0x45, 0x1A,
0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xC7, 0x45, 0x1A, 0x00, 0x00,
0x00, 0x00,
0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00, 0x7F,
0x1F, 0xE8,
0x96, 0xF4, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x04, 0x74, 0x0E, 0x83, 0x7D, 0x16, 0x06,
0x74, 0x08,
0x83, 0x7D, 0x16, 0x07, 0x7F, 0x02, 0xEB, 0x41, 0xE8, 0x50, 0xF7, 0xFF, 0xFF, 0xC3,
0x3D, 0xC0,
0x00, 0x00, 0x00, 0x7C, 0x34, 0x89, 0xC2, 0xC1, 0xEA, 0x04, 0x89, 0xC1, 0x83, 0xE1,
0x0F, 0x83,
0xFA, 0x0E, 0x75, 0x15, 0x83, 0xF9, 0x08, 0x7D, 0x20, 0x83, 0xF9, 0x03, 0x74, 0x1B,
0x83, 0xF9,
0x02, 0x74, 0x16, 0xE8, 0x25, 0xF7, 0xFF, 0xFF, 0xC3, 0x83, 0xFA, 0x0F, 0x75, 0x0B,
0x83, 0xF9,
0x08, 0x7C, 0x06, 0xE8, 0x15, 0xF7, 0xFF, 0xFF, 0xC3, 0xE8, 0xF0, 0xF3, 0xFF, 0xFF,
0x8B, 0x45,
0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xC7, 0x45, 0x1A, 0x00,
0x00, 0x00,
0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00,
0x7F, 0x11,
0xE8, 0x15, 0xF4, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x07, 0x7E, 0x22, 0xE8, 0xDD, 0xF6,
0xFF, 0xFF,
0xC3, 0x3D, 0xC0, 0x00, 0x00, 0x00, 0x7C, 0x15, 0x89, 0xC2, 0xC1, 0xEA, 0x04, 0x89,
0xC1, 0x83,
0xE1, 0x0F, 0x83, 0xFA, 0x0D, 0x75, 0x06, 0xE8, 0xC1, 0xF6, 0xFF, 0xFF, 0xC3, 0xE8,
0x9C, 0xF3,
0xFF, 0xFF, 0x8B, 0x45, 0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3,
0xC7, 0x45,
0x1A, 0x00, 0x00, 0x00, 0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x3D,
0xBF, 0x00,
0x00, 0x00, 0x7F, 0x19, 0xE8, 0xC1, 0xF3, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x05, 0x74,
0x08, 0x83,
0x7D, 0x16, 0x07, 0x7F, 0x02, 0xEB, 0x32, 0xE8, 0x81, 0xF6, 0xFF, 0xFF, 0xC3, 0x3D,
0xC0, 0x00,
0x00, 0x00, 0x7C, 0x25, 0x89, 0xC2, 0xC1, 0xEA, 0x04, 0x89, 0xC1, 0x83, 0xE1, 0x0F,
0x83, 0xFA,
0x0C, 0x75, 0x0B, 0x83, 0xF9, 0x08, 0x7C, 0x11, 0xE8, 0x60, 0xF6, 0xFF, 0xFF, 0xC3,
0x83, 0xFA,
0x0F, 0x75, 0x06, 0xE8, 0x55, 0xF6, 0xFF, 0xFF, 0xC3, 0xE8, 0x30, 0xF3, 0xFF, 0xFF,
0x8B, 0x45,
0x1A, 0x01, 0x45, 0x23, 0x48, 0x83, 0x45, 0x23, 0x02, 0xC3, 0xC7, 0x45, 0x1A, 0x00,
0x00, 0x00,
0x00, 0x48, 0x8B, 0x45, 0x23, 0x0F, 0xB6, 0x40, 0x01, 0x3D, 0xBF, 0x00, 0x00, 0x00,
0x7F, 0x11,
0xE8, 0x55, 0xF3, 0xFF, 0xFF, 0x83, 0x7D, 0x16, 0x07, 0x7E, 0x27, 0xE8, 0x1D, 0xF6,
0xFF, 0xFF,
0xC3, 0x3D, 0xC0, 0x00, 0x00, 0x00, 0x7C, 0x1A, 0x89, 0xC2, 0xC1, 0xEA, 0x04, 0x89,
0xC1, 0x83,

[illegible]

[illegible]

[illegible]

那么该如何调用呢？

调用其实很容易，首先调用 `lde_init()` 函数将功能载入到内存，然后通过 `lde_disasm()` 直接调用功能，在调用时第一个参数传入需要计算的内存地址，第二个参数是位数，如果传入0则表示计算32位汇编汇编，如果传入64则计算64位汇编长度。

```
#include "lyshark_lde64.h"
#include <ntifs.h>

// 计算地址处指令有多少字节
// address = 地址
// bits 32位驱动传入0 64传入64
typedef INT(*LDE_DISASM)(PVOID address, INT bits);

LDE_DISASM lde_disasm;

// 初始化引擎
VOID lde_init()
{
    lde_disasm = ExAllocatePool(NonPagedPool, 12800);
    memcpy(lde_disasm, szShellCode, 12800);
}

VOID UnDriver(PDRIVER_OBJECT driver)
{
    DbgPrint("驱动已卸载 \n");
}

NTSTATUS DriverEntry(IN PDRIVER_OBJECT Driver, PUNICODE_STRING RegistryPath)
{
    DbgPrint("hello lyshark.com \n");

    // 初始化反汇编引擎
    lde_init();

    UNICODE_STRING unstr;
    PVOID addr;

    RtlInitUnicodeString(&unstr, L"PsLookupProcessByProcessId");
    addr = MmGetSystemRoutineAddress(&unstr);
    DbgPrint("获取内存地址: 0x%p \n", addr);
}
```

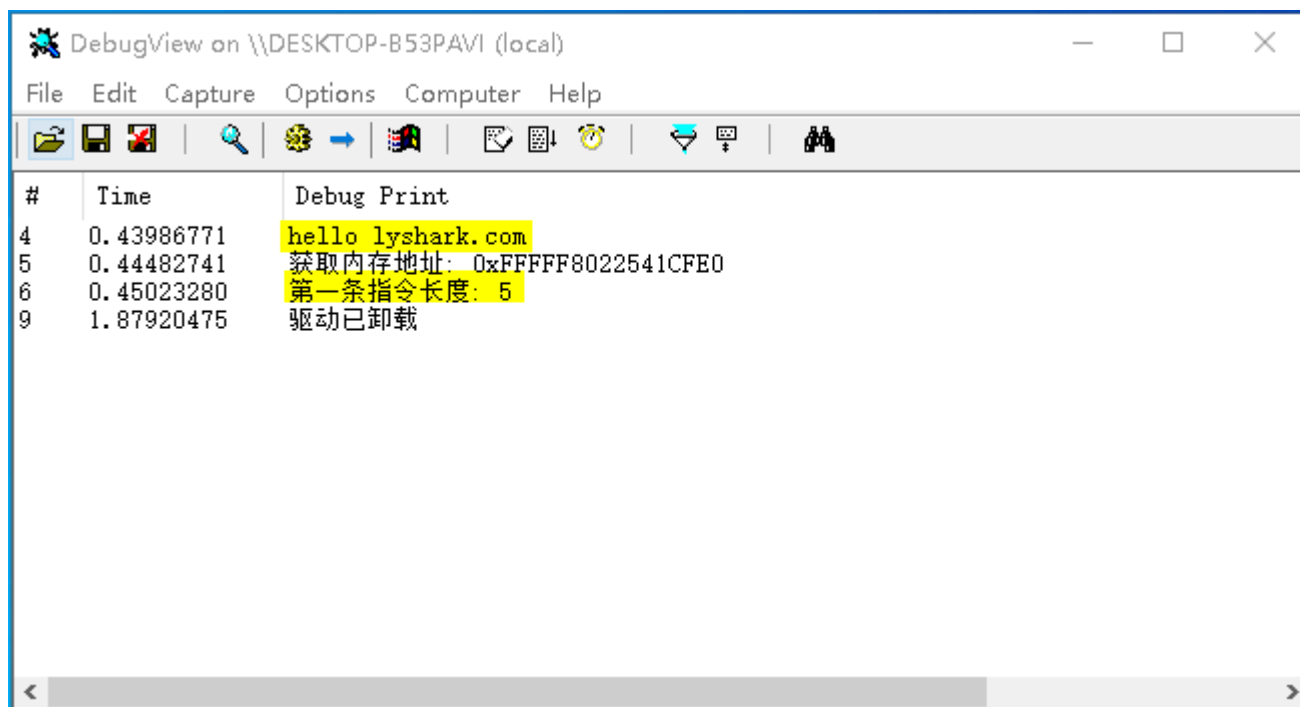
```

// 计算第一条汇编指令长度
INT asm_len = lde_disasm(addr, 64);
DbgPrint("第一条指令长度: %d \n", asm_len);

Driver->DriverUnload = UnDriver;
return STATUS_SUCCESS;
}

```

运行上方的驱动程序，即可得到 `PsLookupProcessByProcessId` 函数第一条指令的实际长度，输出效果如下；



如果我们需要 Hook 挂钩 则最常用的就是填充 `JMP` 跨4G跳转，该指令占用 14个字节 的内存长度，但我们无法保证 14个字节 就是一个完整的指令长度，有可能指令会被截断而导致执行异常，此时必须得到完整指令的长度，指令长度就需要大于等于14，所以代码中的计算应该这样来实现。

```

#include "lyshark_lde64.h"
#include <ntifs.h>

// 计算地址处指令有多少字节
// address = 地址
// bits 32位驱动传入0 64传入64
typedef INT(*LDE_DISASM)(PVOID address, INT bits);

LDE_DISASM lde_disasm;

// 初始化引擎
VOID lde_init()
{
    lde_disasm = ExAllocatePool(NonPagedPool, 12800);
    memcpy(lde_disasm, szShellCode, 12800);
}

VOID UnDriver(PDRIVER_OBJECT driver)

```

```

{
    DbgPrint("驱动已卸载 \n");
}

// 得到完整指令长度,避免截断
ULONG GetFullPatchSize(PUCHAR Address)
{
    ULONG LenCount = 0, Len = 0;

    // 至少需要14字节
    while (LenCount <= 14)
    {
        Len = Ide_disasm(Address, 64);
        Address = Address + Len;
        LenCount = LenCount + Len;
    }
    return LenCount;
}

NTSTATUS DriverEntry(IN PDRIVER_OBJECT Driver, PUNICODE_STRING RegistryPath)
{
    DbgPrint("hello lyshark.com \n");

    // 初始化反汇编引擎
    Ide_init();

    UNICODE_STRING unstr;
    PVOID addr;

    RtlInitUnicodeString(&unstr, L"PsLookupProcessByProcessId");
    addr = MmGetSystemRoutineAddress(&unstr);
    DbgPrint("获取内存地址: 0x%p \n", addr);

    ULONG count = GetFullPatchSize(addr);
    DbgPrint("完整指令长度: %d \n", count);

    Driver->DriverUnload = UnDriver;
    return STATUS_SUCCESS;
}

```

运行这个驱动程序，计算得到的结果与上图作比较，此处得到的才是一个完整的指令长度；

