[1. Source Code 3](#_Toc464834722)

[1-1. 编译出的exe 3](#_Toc464834723)

[1-2. 文件的大小 3](#_Toc464834724)

[1-2-1. Windows 的显示 3](#_Toc464834725)

[1-2-2. CFF Explorer中的显示 4](#_Toc464834726)

[1-2-3. Beyond Compare 中的显示 4](#_Toc464834727)

[2. Debug 和Release 文件的差异 5](#_Toc464834728)

[3. Beyond Compare中看到的 Exe 文件里的内容 9](#_Toc464834729)

[3-1. Dos 头及存根代码 9](#_Toc464834730)

[3-2. 一堆字符串符号 10](#_Toc464834731)

[3-2-1. Assembly Info 10](#_Toc464834732)

[3-3. 引用的Pdb文件及其路径 11](#_Toc464834733)

[3-4. 对mscoree.dll的调用 11](#_Toc464834734)

[3-5. Configuration Files 11](#_Toc464834735)

[4. PE 文件框架构成 12](#_Toc464834736)

[5. CFF Explorer 中看到的exe 文件内容 12](#_Toc464834737)

[5-1. Dos Header ： \_IMAGE\_DOS\_HEADER 12](#_Toc464834738)

[5-2. Dos Stub 13](#_Toc464834739)

[5-3. NT Header (PE Header): \_IMAGE\_NT\_HEADERS 14](#_Toc464834740)

[5-3-1. File Header : \_IMAGE\_FILE\_HEADER 14](#_Toc464834741)

[5-3-2. Optional Header:IMAGE\_OPTIONAL\_HEADER32 15](#_Toc464834742)

[5-3-3. Data Directories 17](#_Toc464834743)

[5-4. Section Table ： \_IMAGE\_SECTION\_HEADER 19](#_Toc464834744)

[5-5. .text 节 19](#_Toc464834745)

[5-6. .rsrc节 23](#_Toc464834746)

[5-7. .reloc 节 26](#_Toc464834747)

[6. 字节码 27](#_Toc464834748)

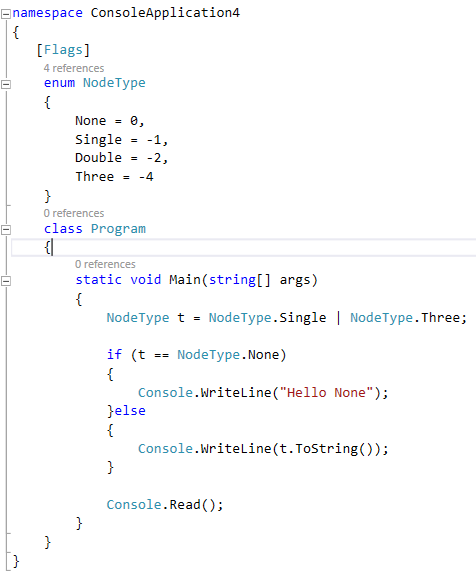
[6-1. 从Cerbero PE Insider 中看到的字节码 27](#_Toc464834749)

[6-2. 从ILDasm 中看到的字节码 27](#_Toc464834750)

[6-2-1. Manifest 28](#_Toc464834751)

# Source Code

详见<ConsoleApplication4>



## 编译出的exe

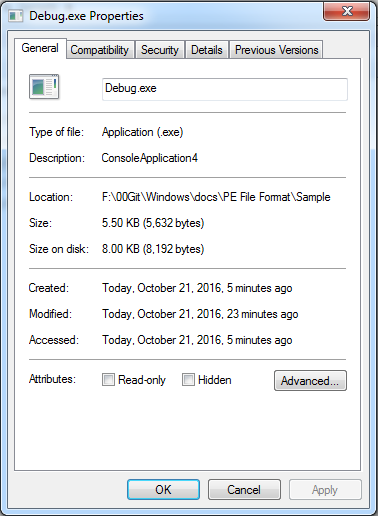
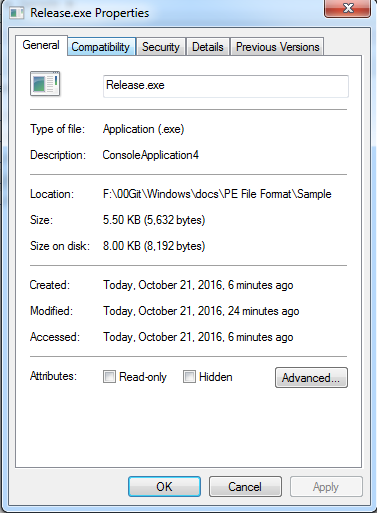
Debug.exe

Release.exe

## 文件的大小

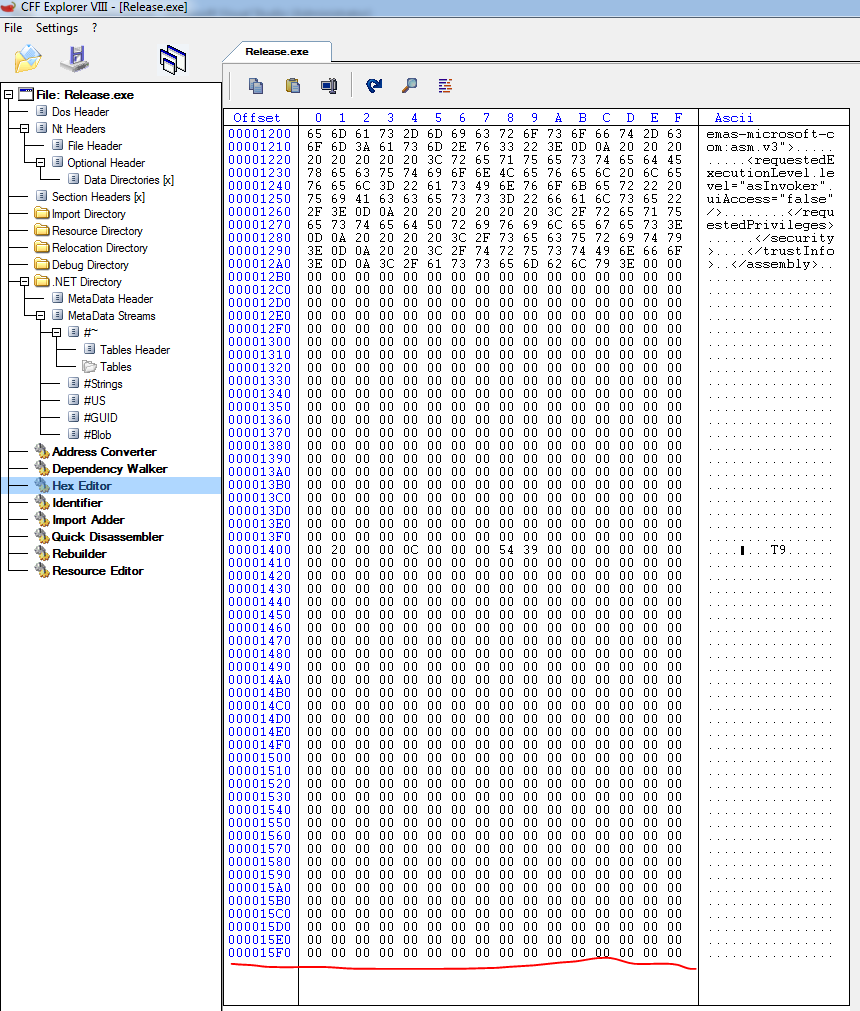
### Windows 的显示

Debug.exe 和Release.exe的文件大小都是5632Bytes，转换为16进制也就是0x1600

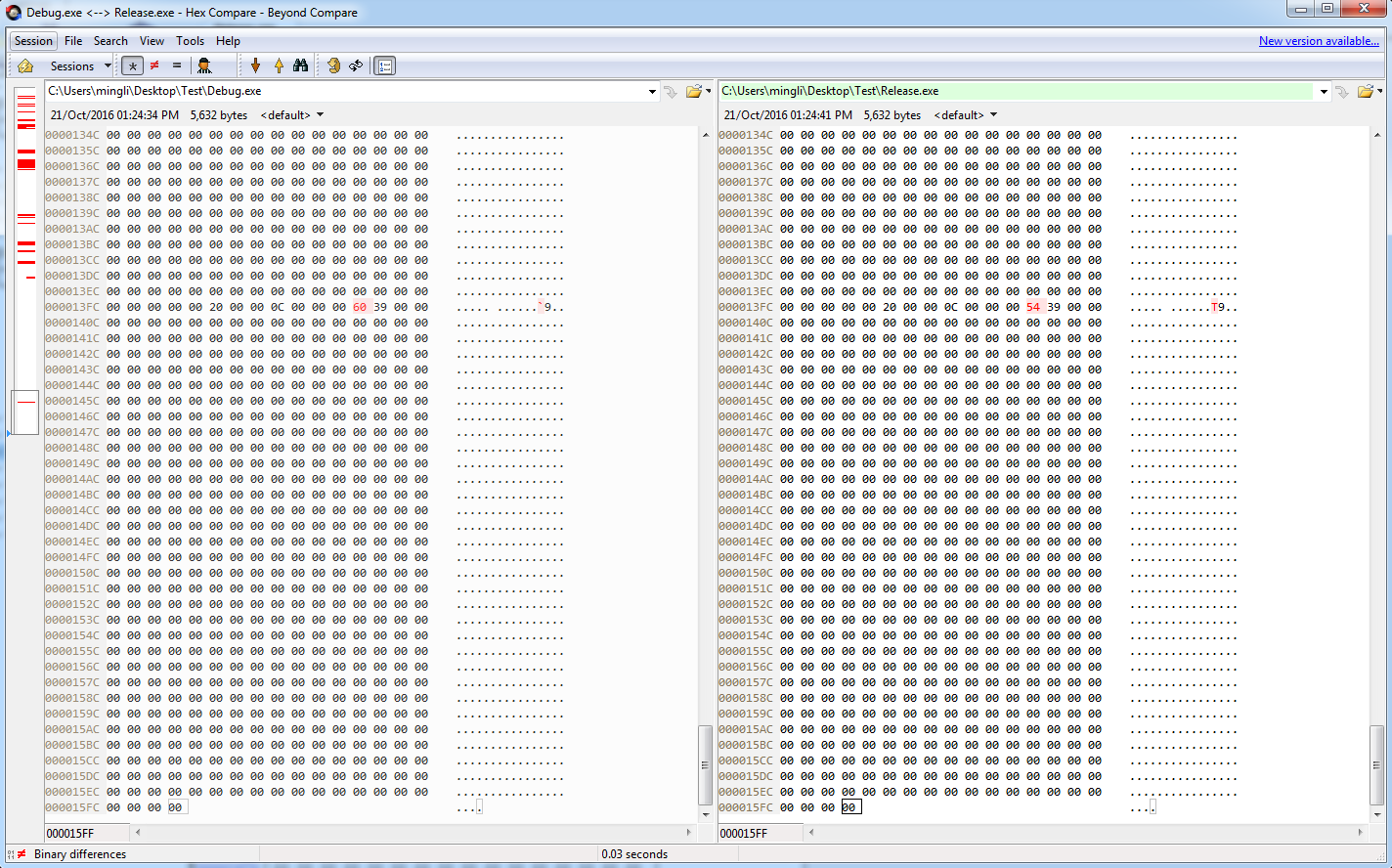
### CFF Explorer中的显示

在CFF Explorer 中看到的文件大小，刚好就是偏移到0x15FF位置，既有0x1600Bytes

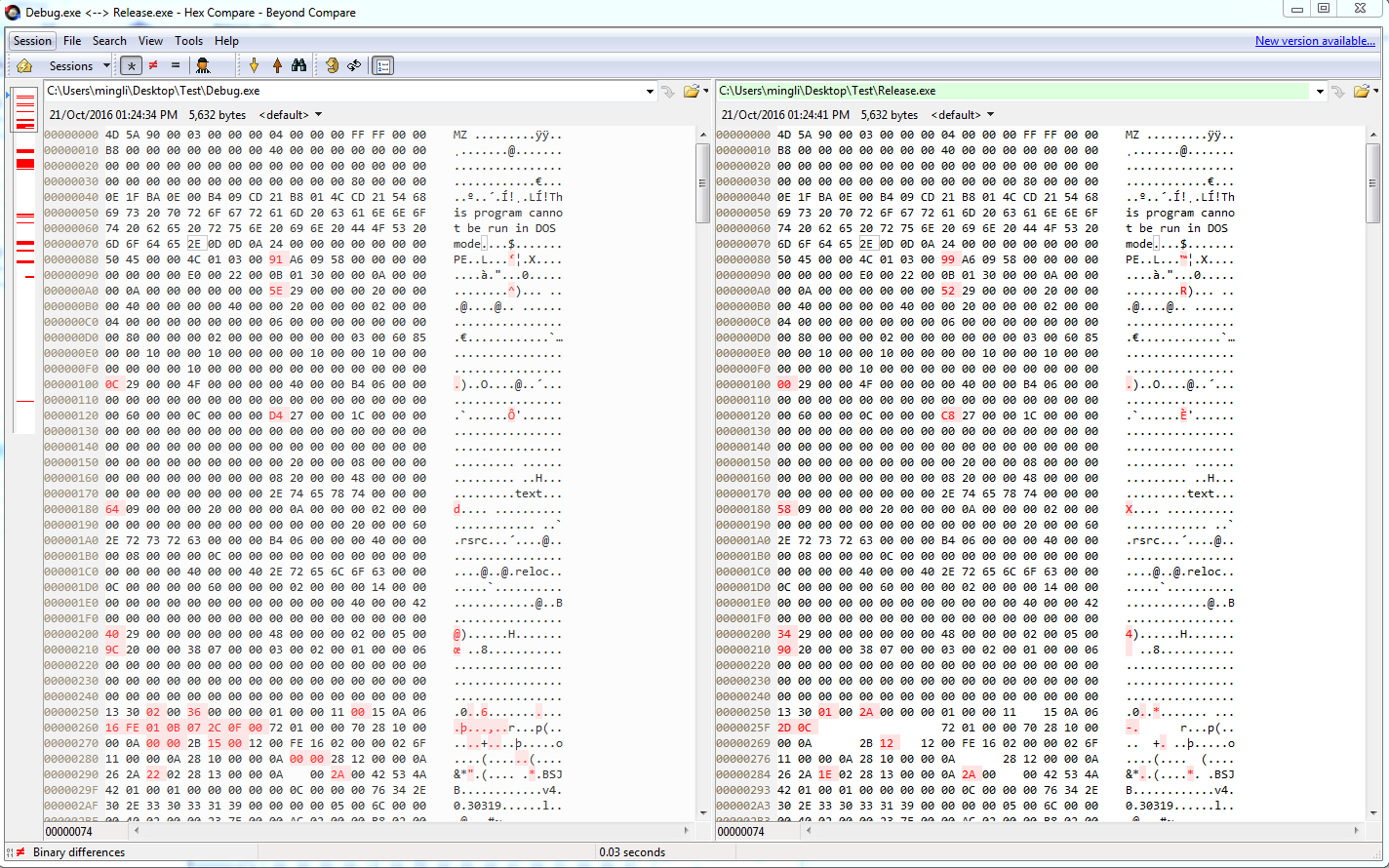


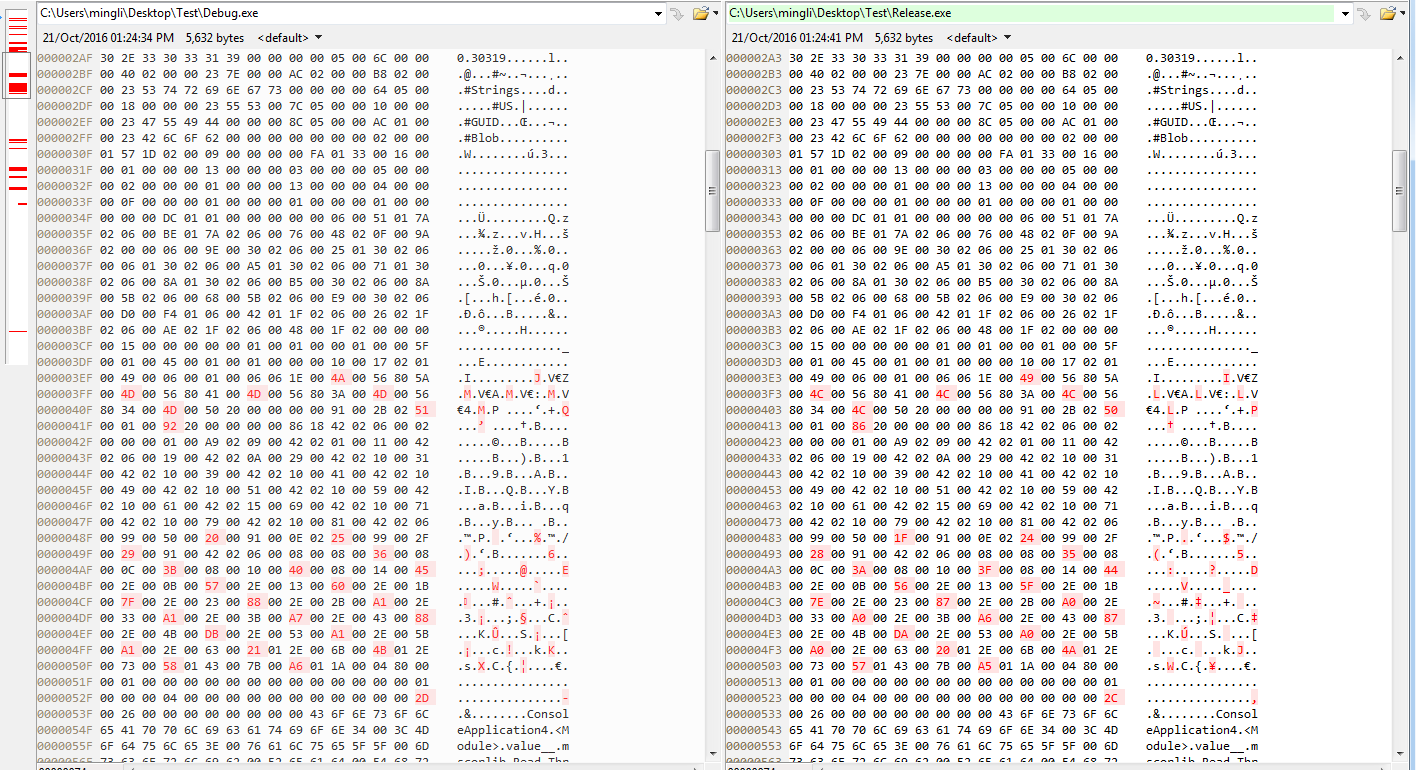
### Beyond Compare 中的显示

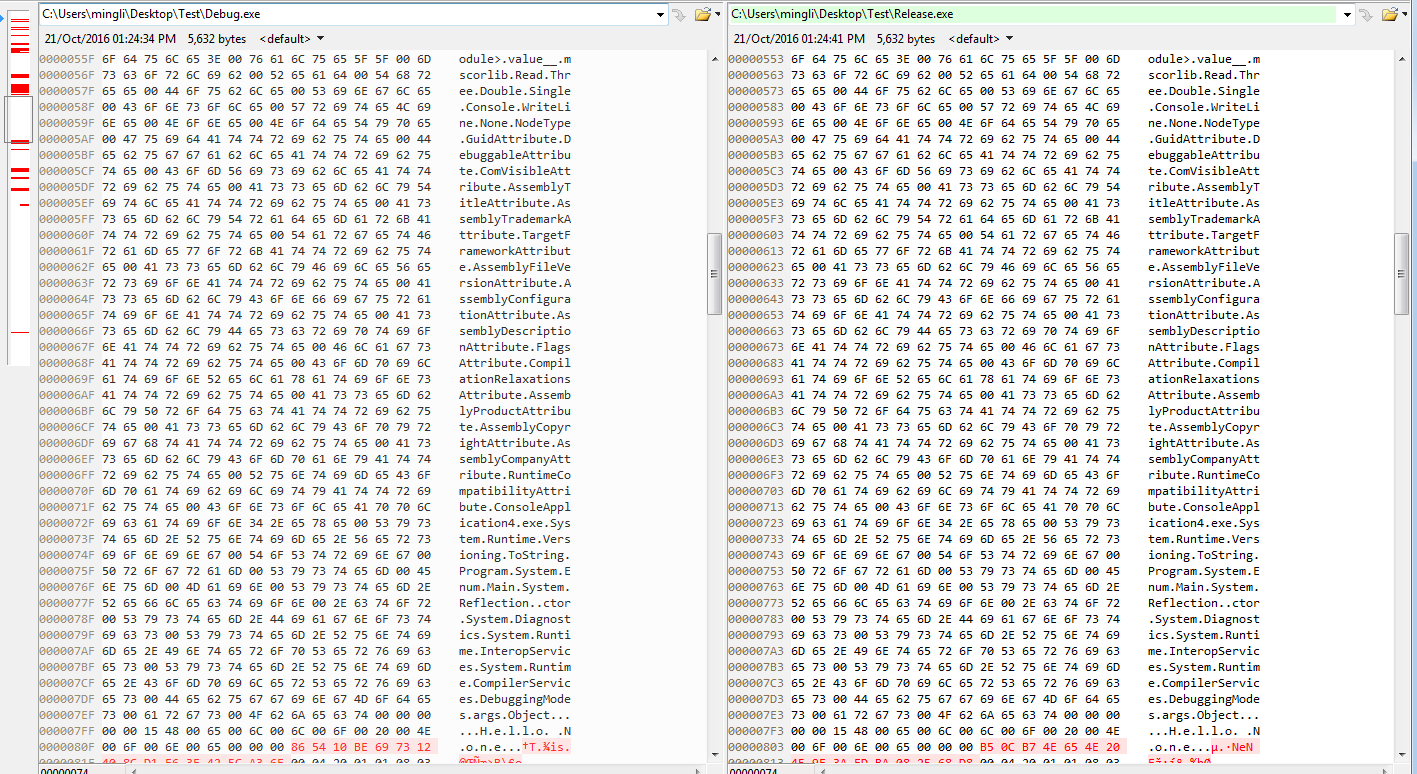
也是偏移到0x15FF的位置

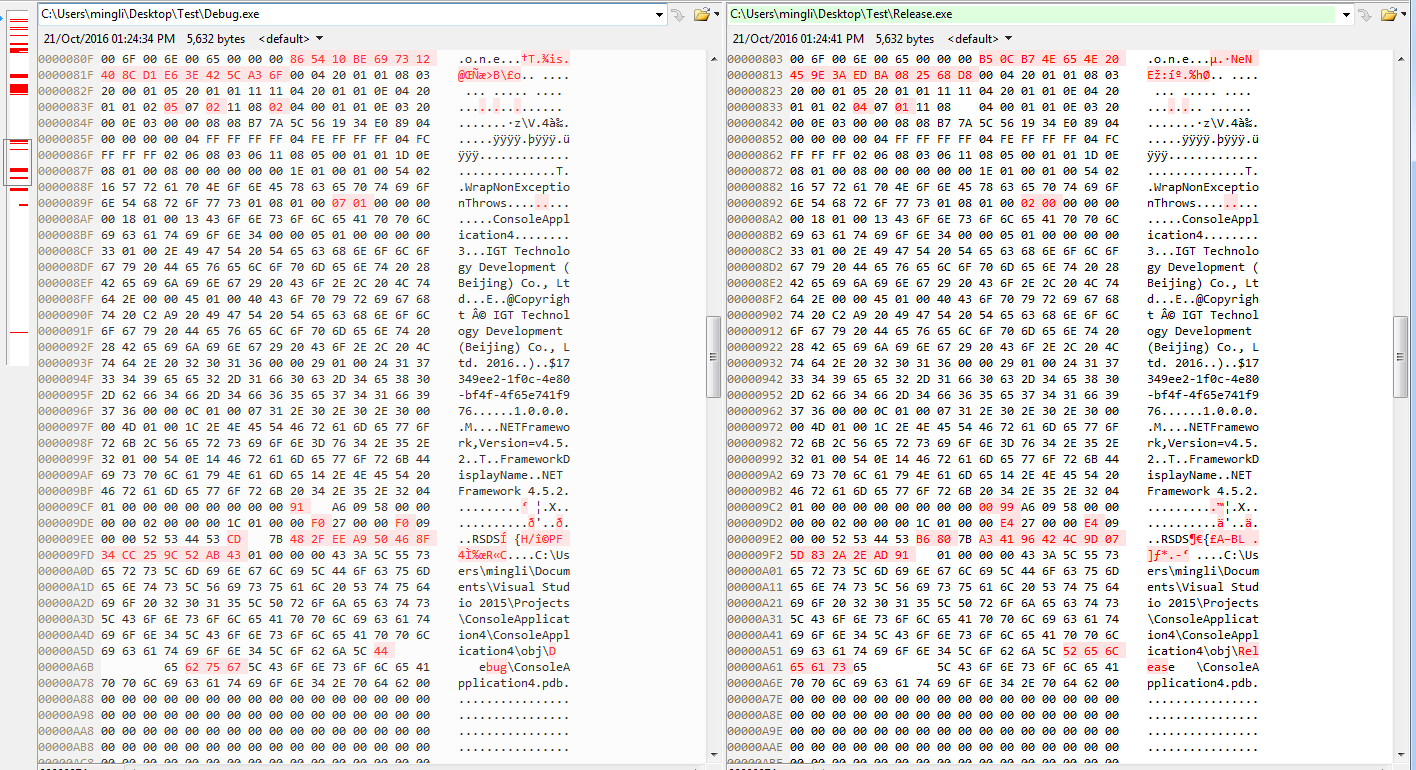


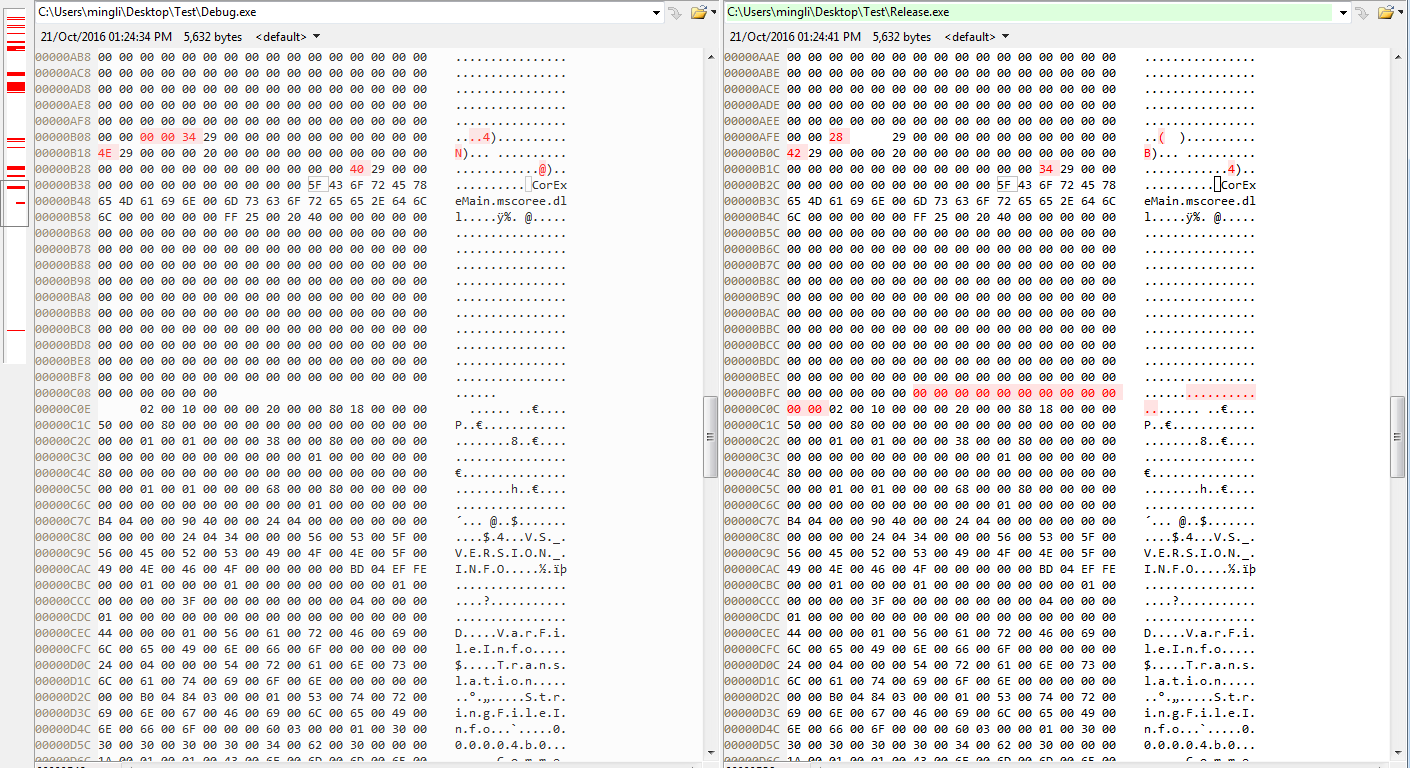
# Debug 和Release 文件的差异

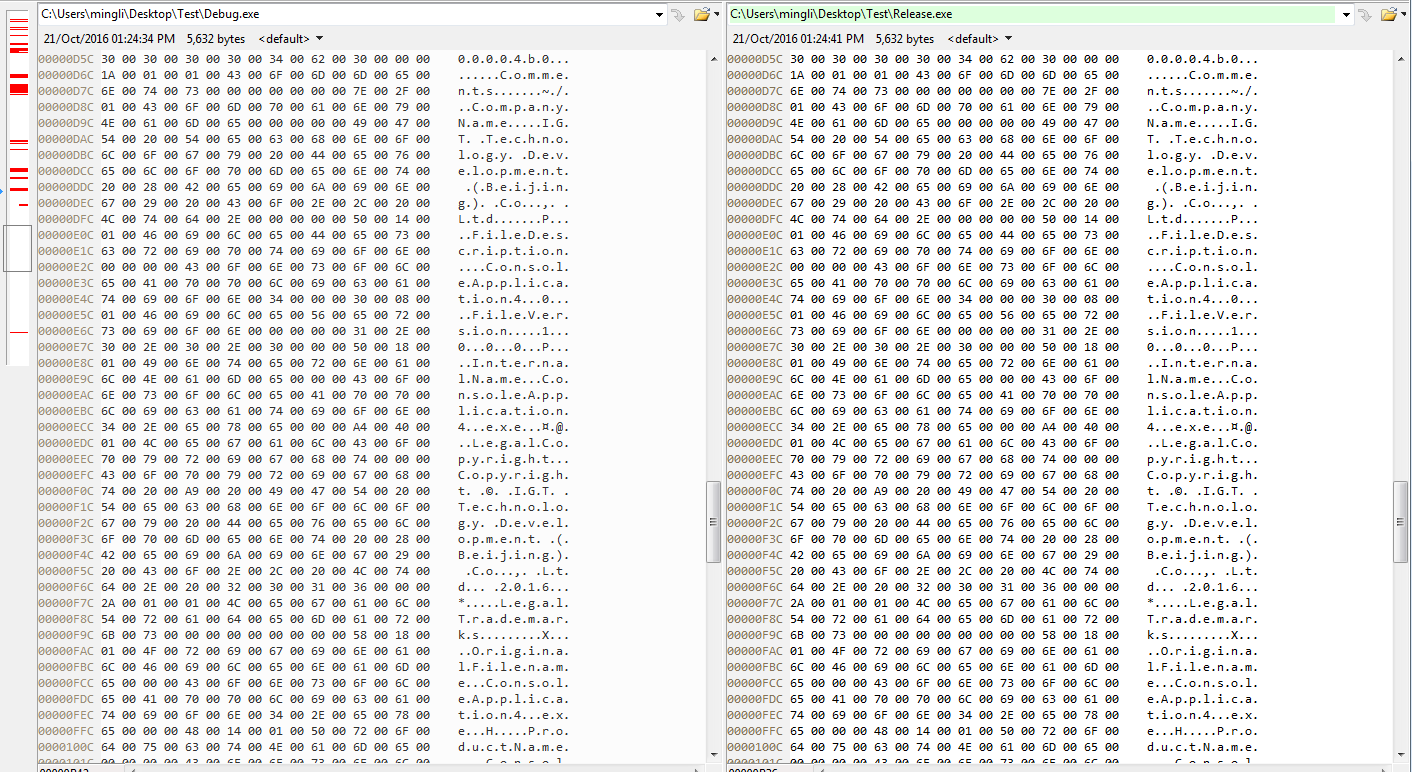


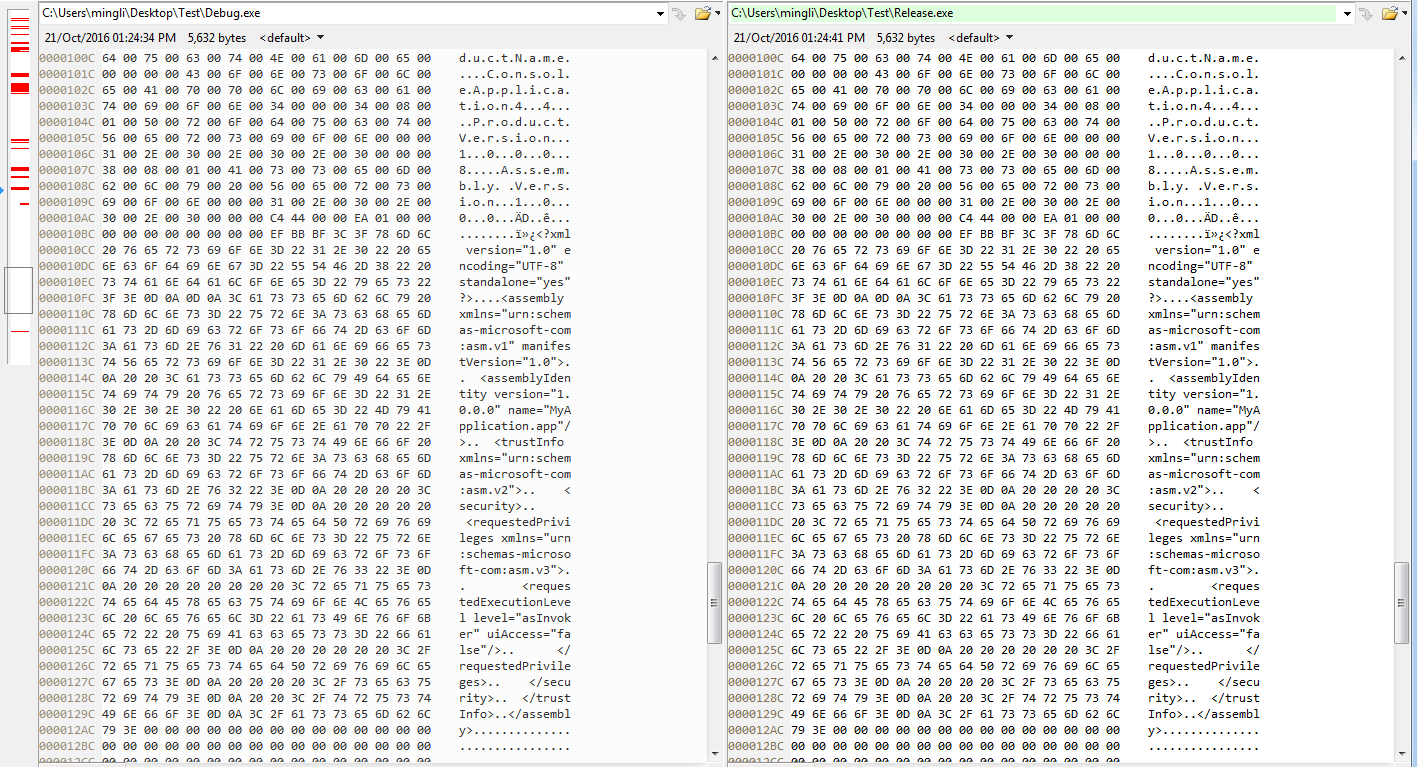


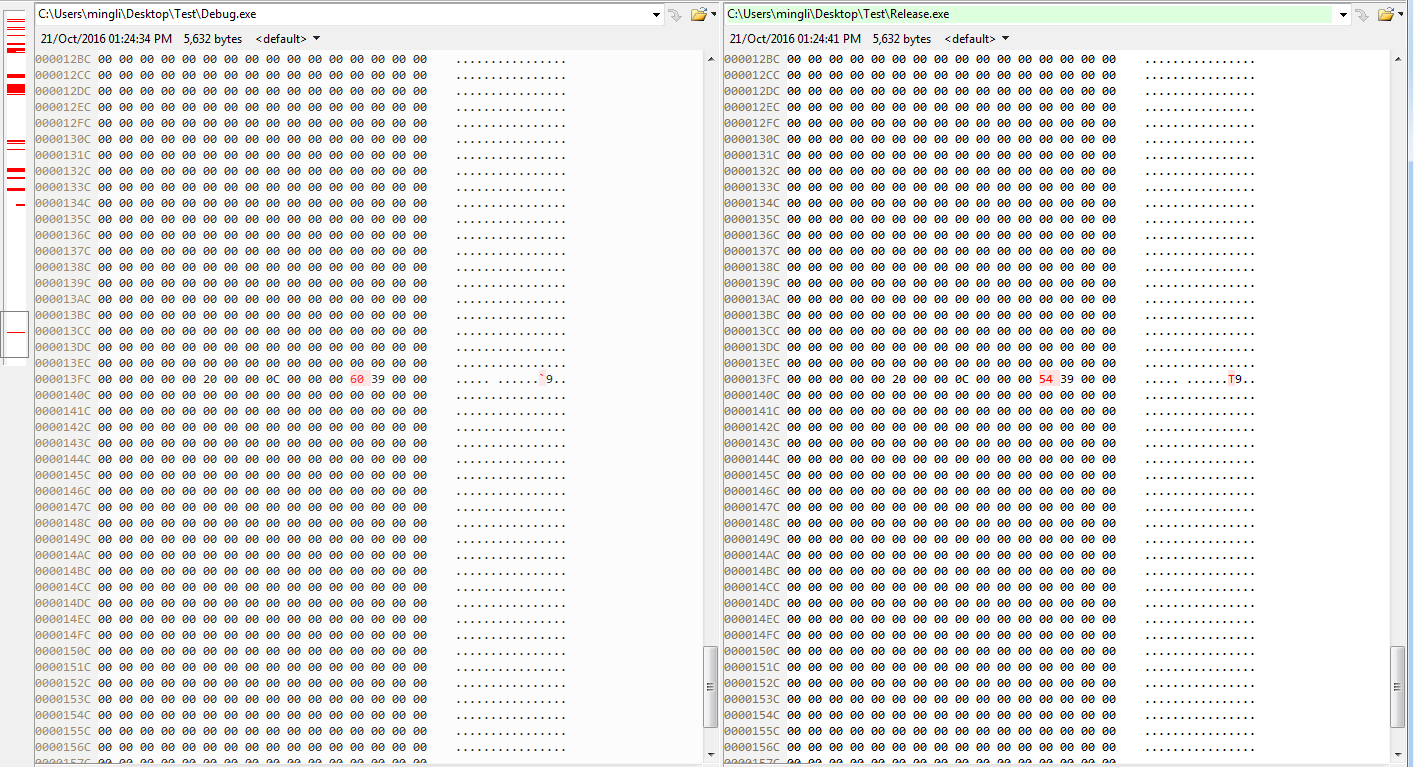


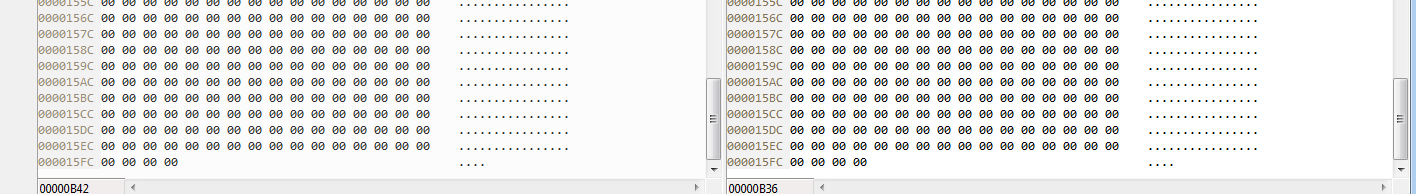








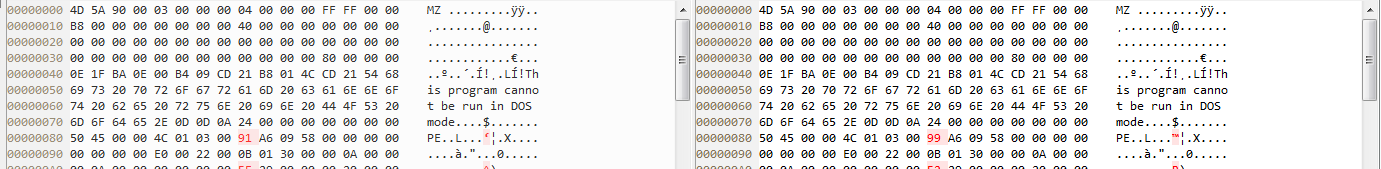




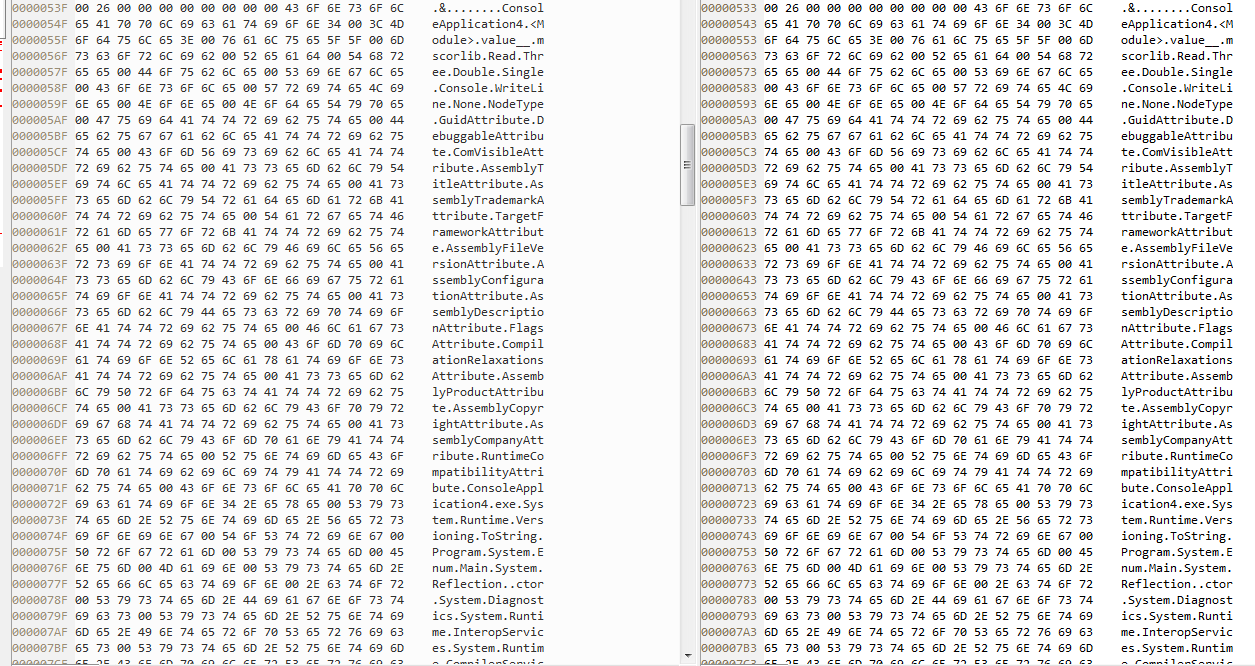
# Beyond Compare中看到的 Exe 文件里的内容

## Dos 头及存根代码

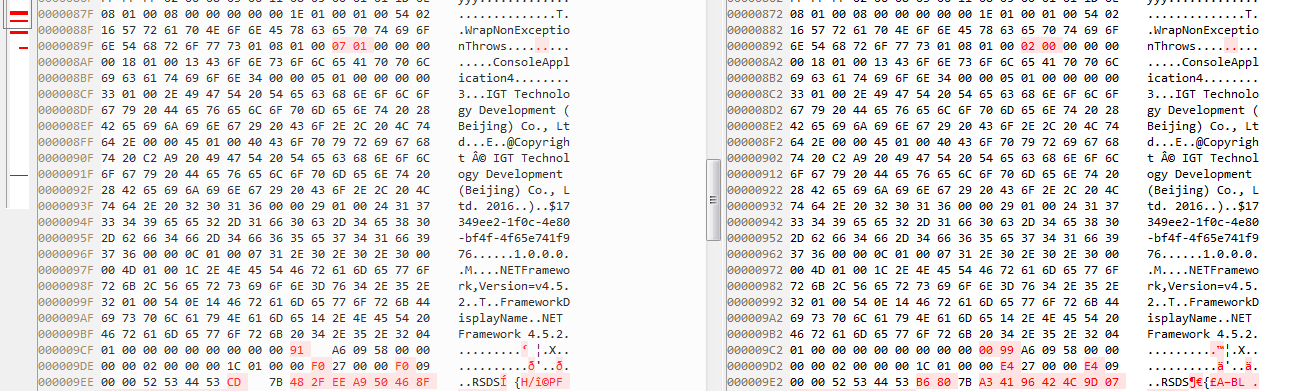
This program cannot be run in Dos mode



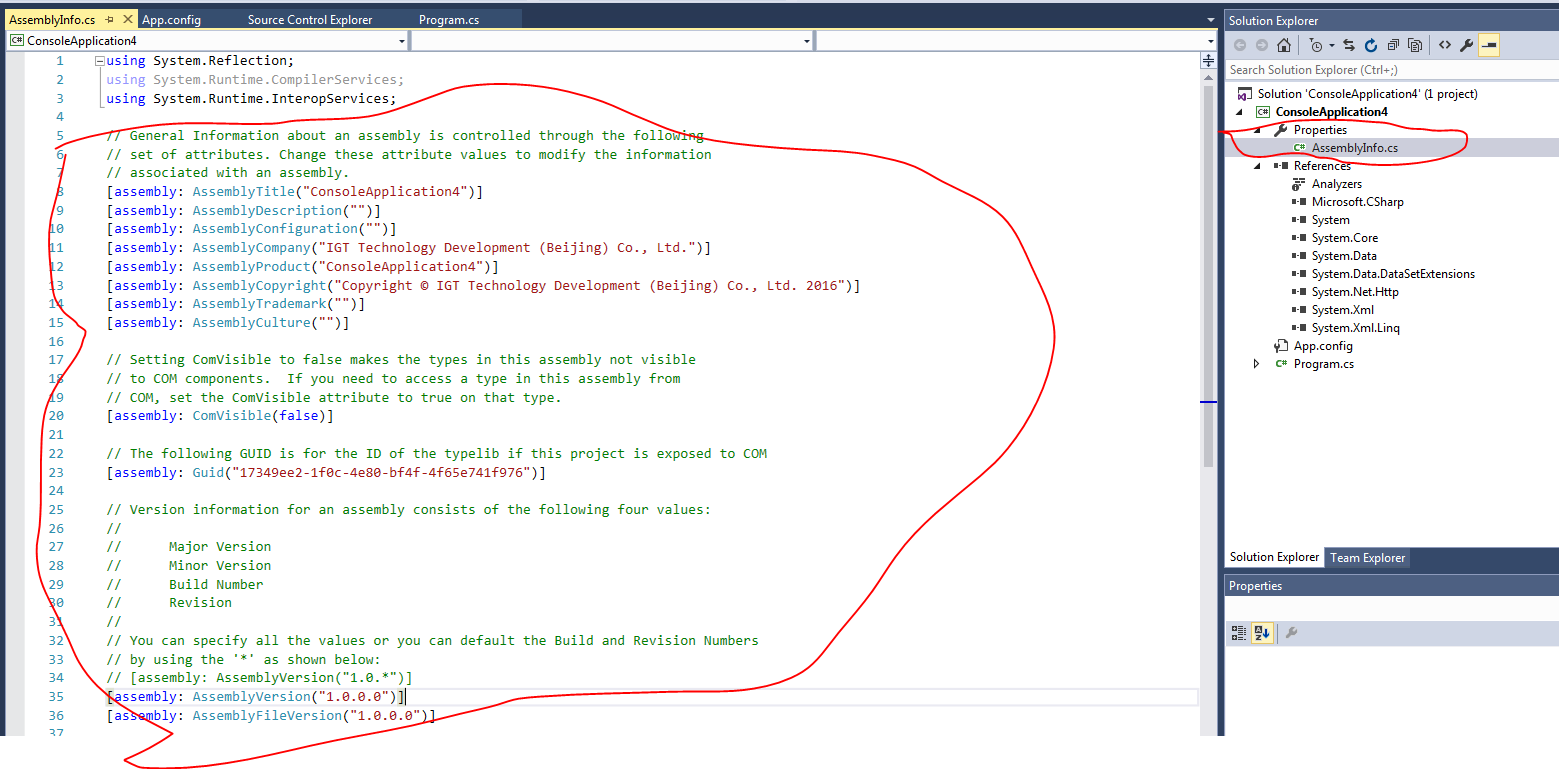
## 一堆字符串符号



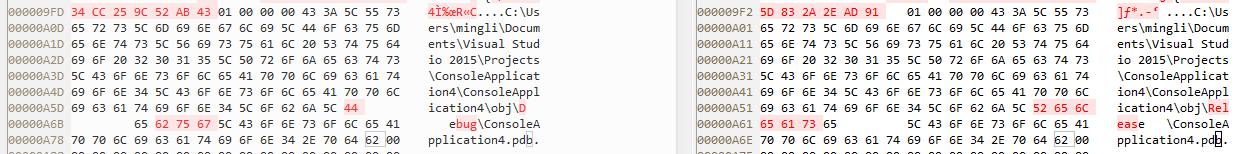
### Assembly Info



就是我们的AssemblyInfo.cs中的设置



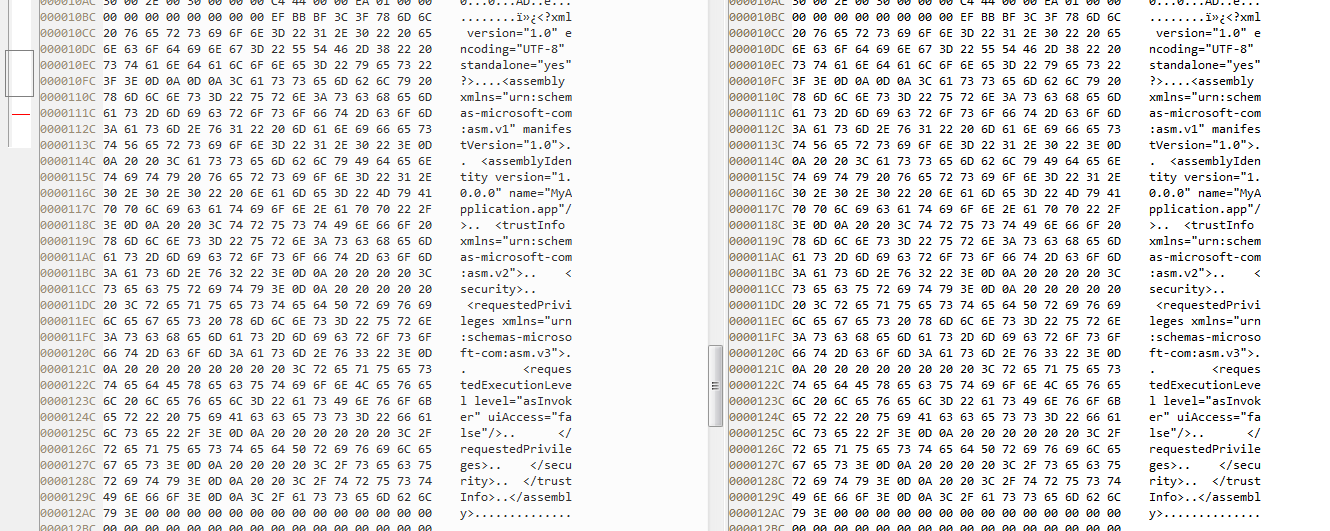
## 引用的Pdb文件及其路径

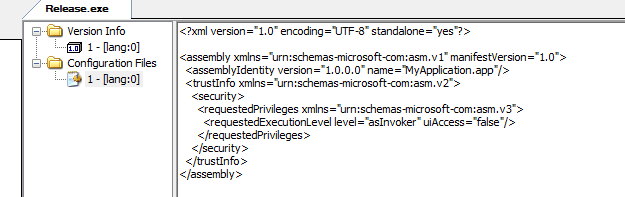


## 对mscoree.dll的调用

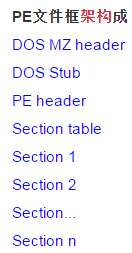


## Configuration Files



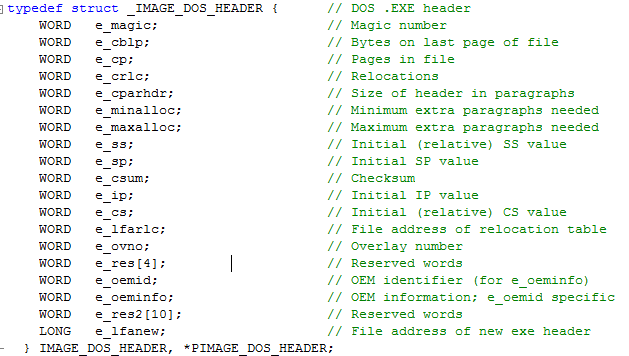


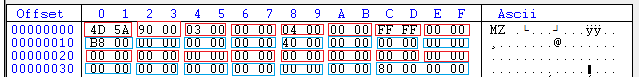
# PE 文件框架构成

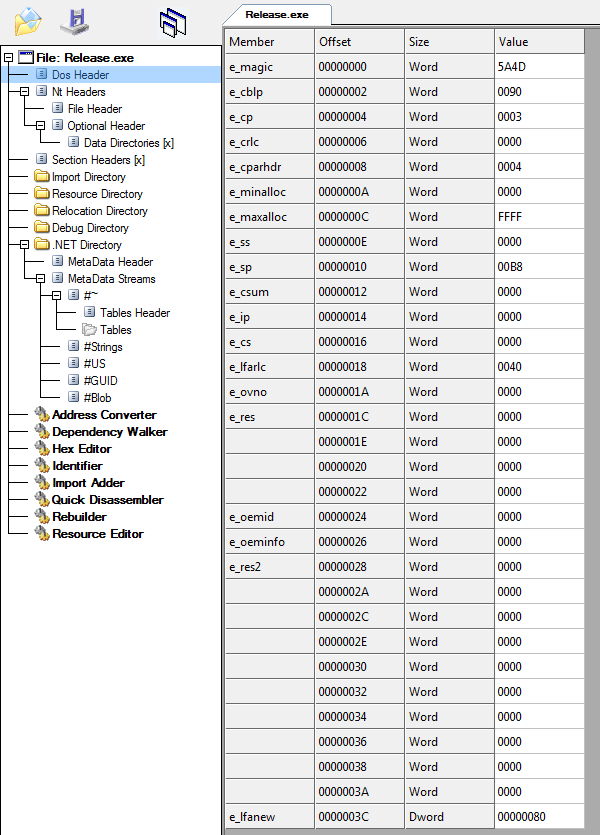


# CFF Explorer 中看到的exe 文件内容

## Dos Header ： \_IMAGE\_DOS\_HEADER



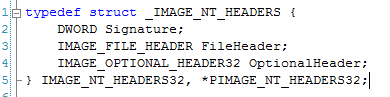




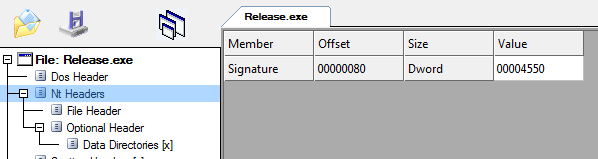
## Dos Stub



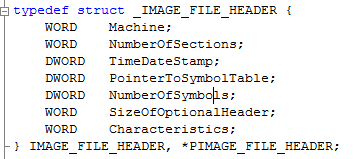
## NT Header (PE Header): \_IMAGE\_NT\_HEADERS



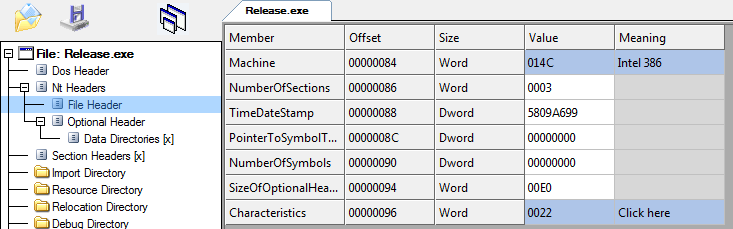




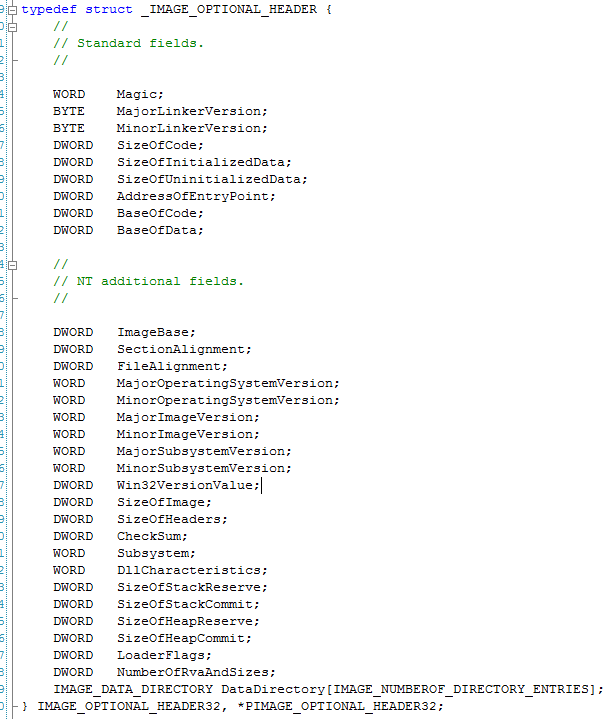
### File Header : \_IMAGE\_FILE\_HEADER

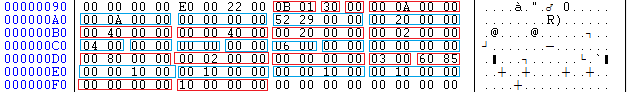


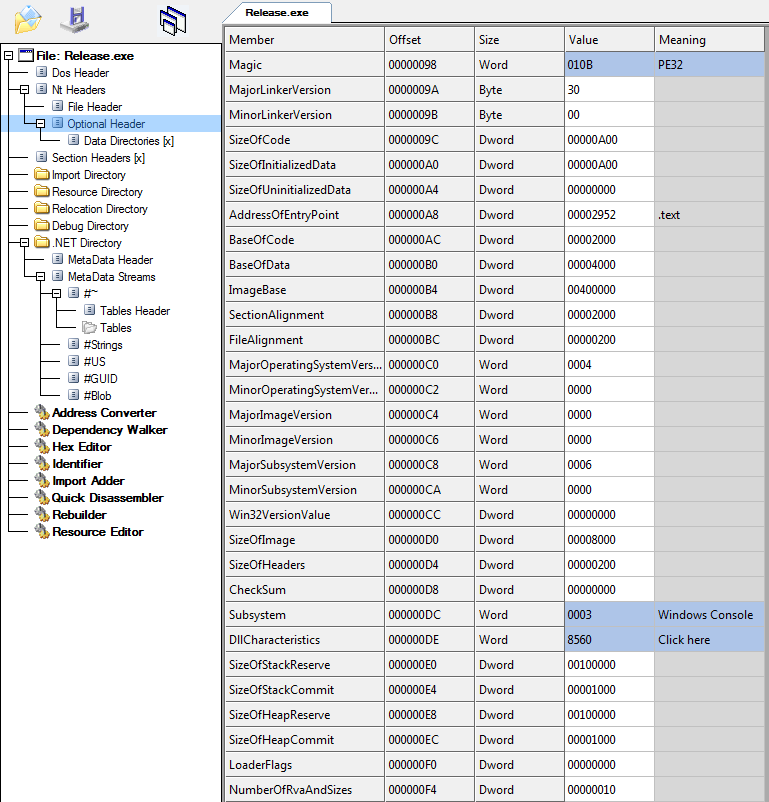




### Optional Header:IMAGE\_OPTIONAL\_HEADER32





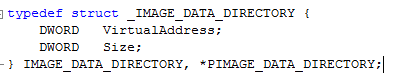


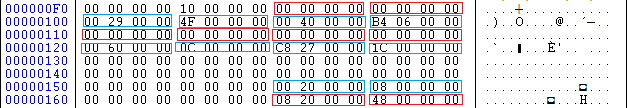
**保留栈大小： 1M Bytes = 1024K Bytes = 1024 \* 1024 = 1048576 Bytes = 0x100000 Bytes**

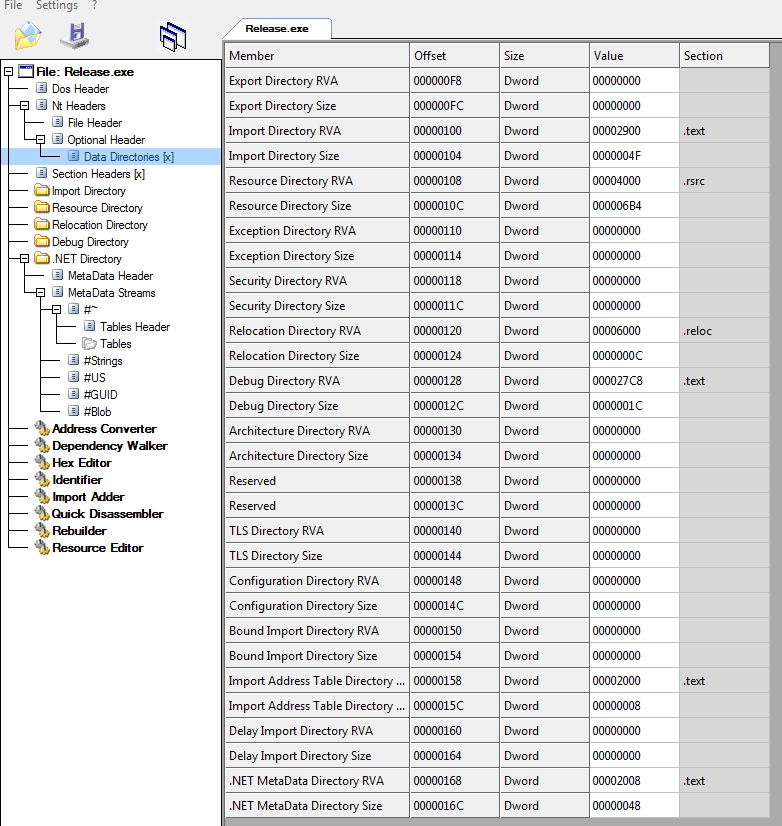
**提交栈大小： 4K Bytes = 1024 \* 4 = 4096 Bytes = 0x1000**

### Data Directories

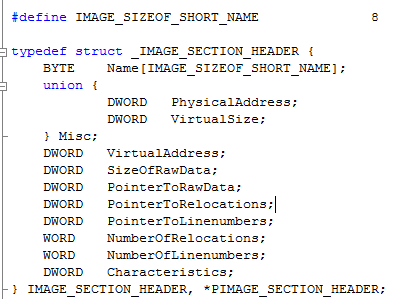


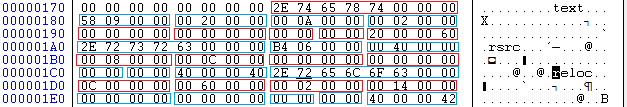


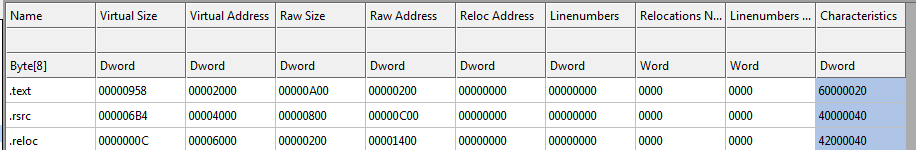




## Section Table ： \_IMAGE\_SECTION\_HEADER





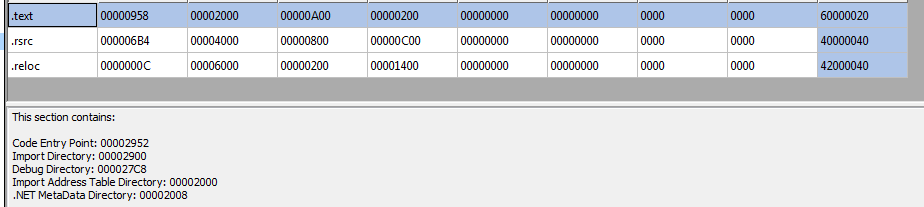


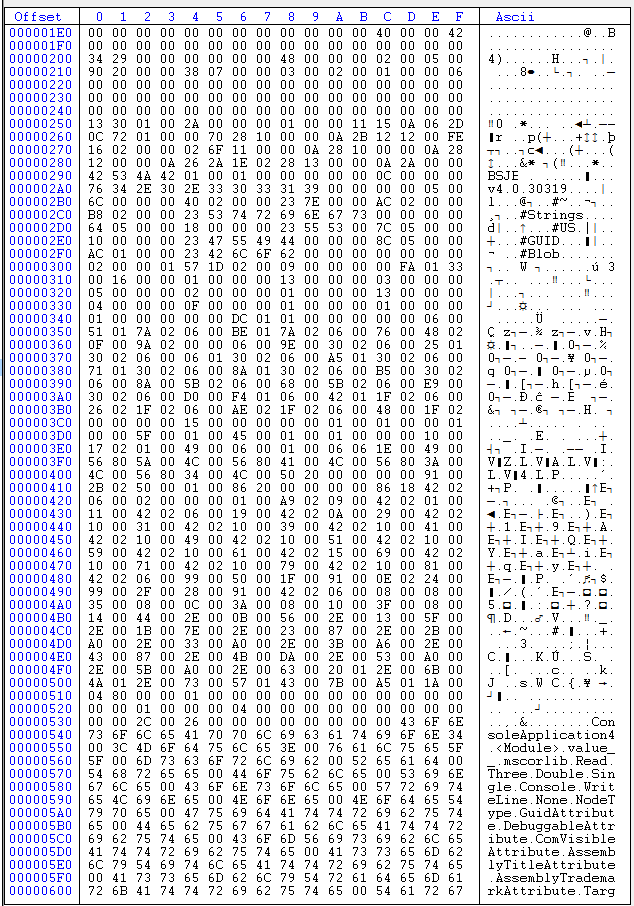
## .text 节

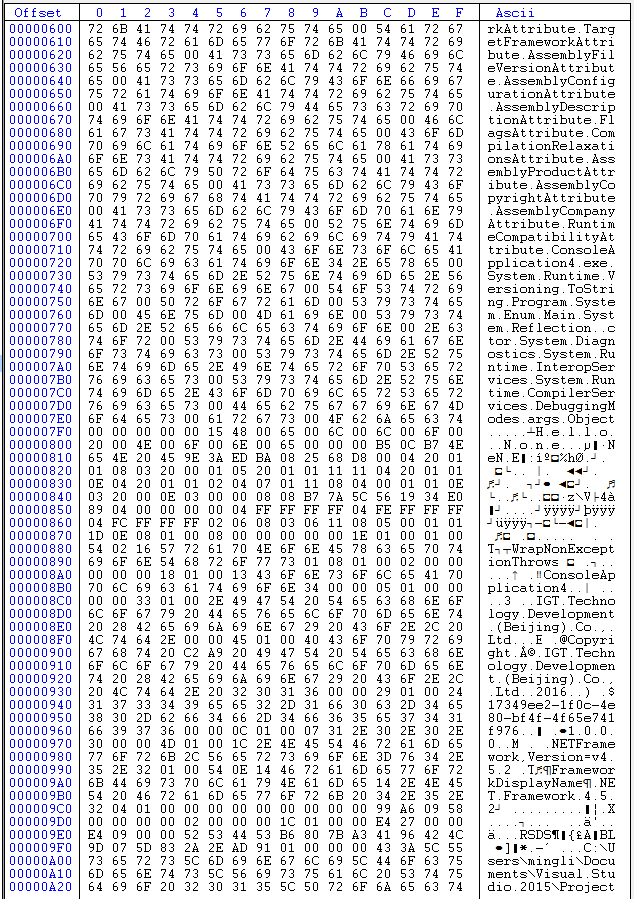
从1F0 到 1FF是填充数据，全部是0

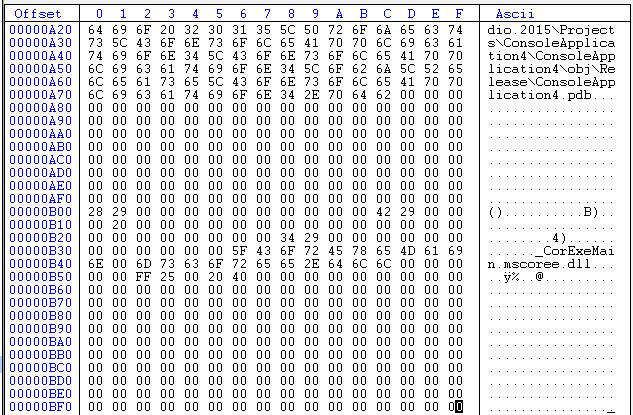
.text 节从200 开始，到BF0结束

包含 Code Entry Point ，Import Directory， .NET MetaData Directory, etc.



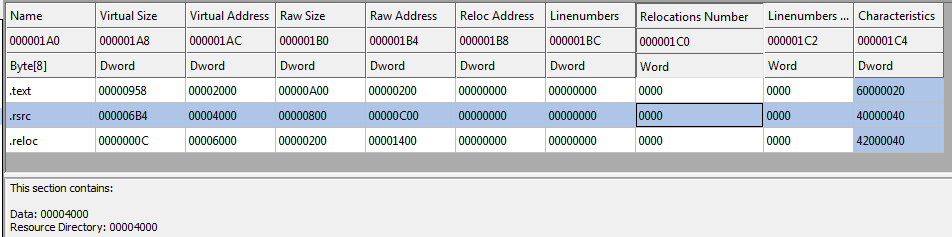


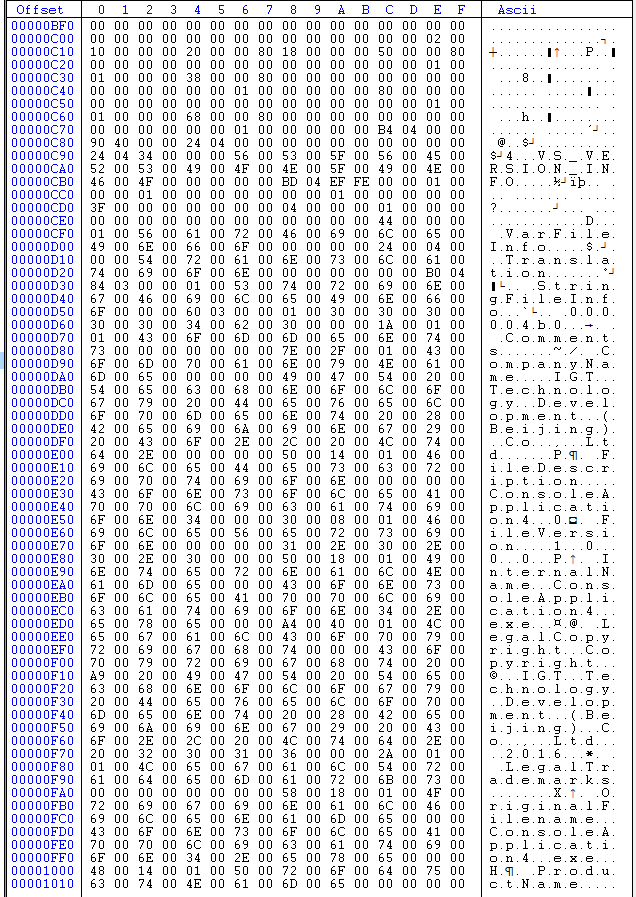


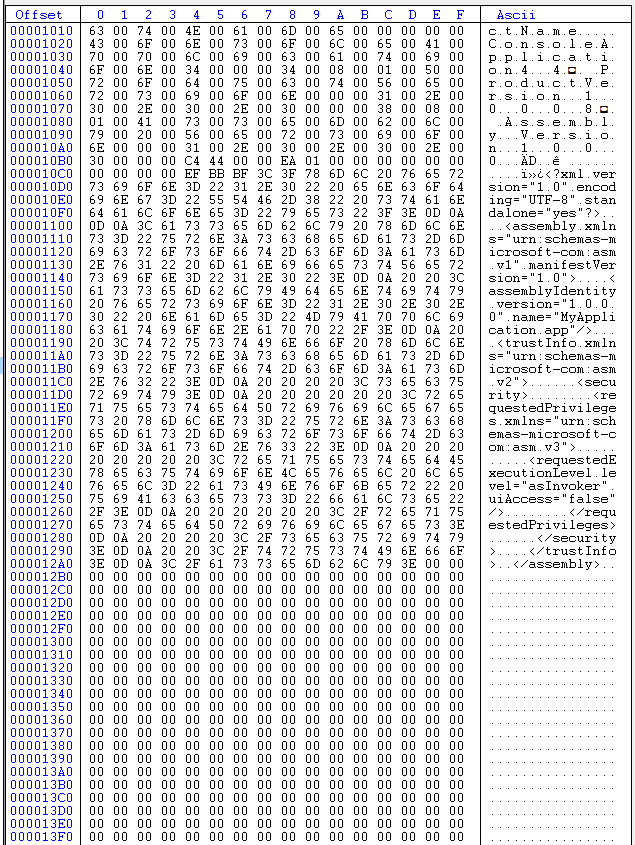


## .rsrc节

从 C00开始，13F0结束

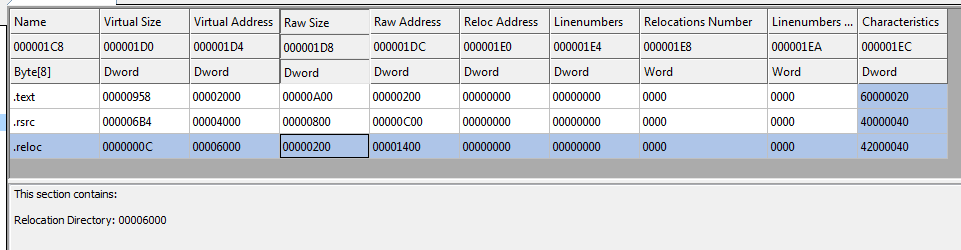


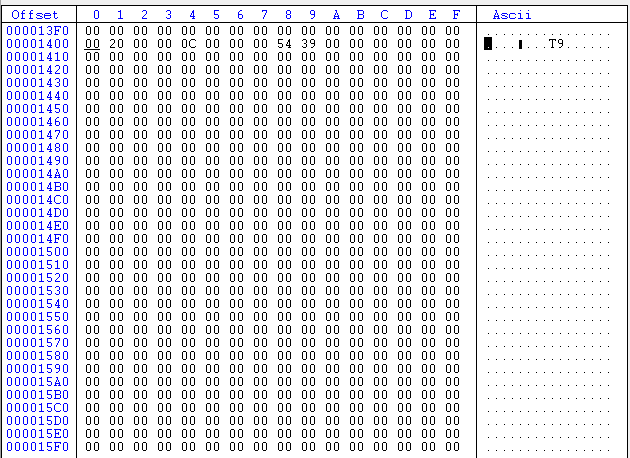




## .reloc 节

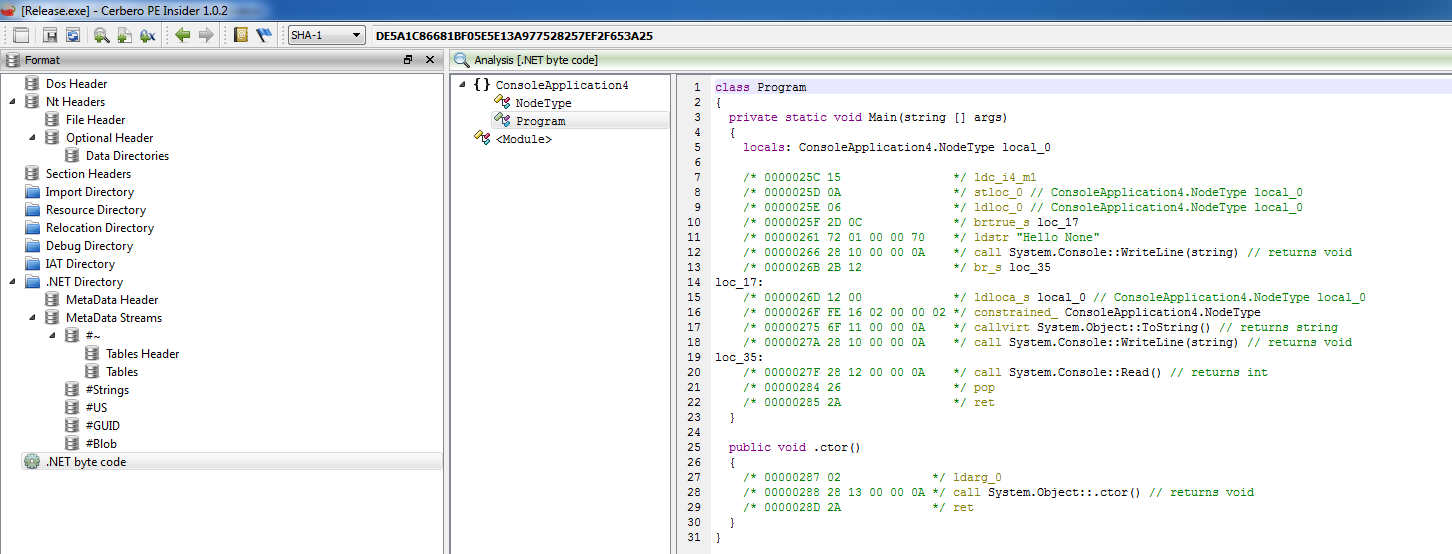
从1400 开始，到15F0结束



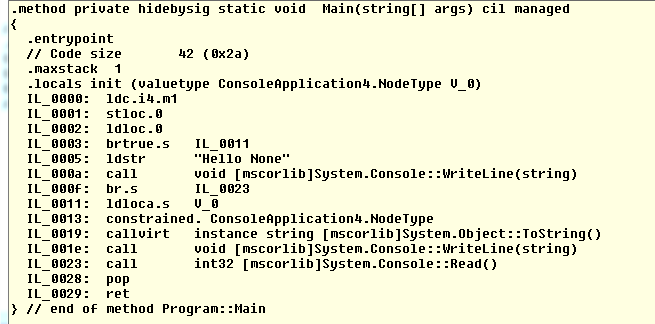


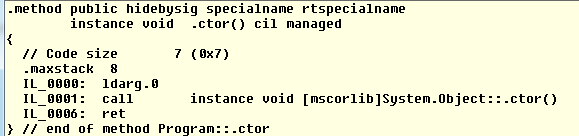
# 字节码

## 从Cerbero PE Insider 中看到的字节码



## 从ILDasm 中看到的字节码





### Manifest

