StudyPE+ (x86) / (x64) [PE32 & PE64 查看/分析集成工具]

目录

【软件说明】 4
【基本操作说明】 5
【打开一个文件】 6
标签页面说明 7
【概况页面】 7
替换图标 8
改变基址 9
额外数据处理 9
特征码分析 9
密码学分析 9
【PE 头页面】 10
【数据表页面】 11
在位编辑 12
【区段页面】 12
清理空区段 13
添加区段 14
插入区段 14
删除区段 14
编辑区段 14
在位编辑区段 15
替换区段 15
向下合并区段 15
扩大最后一个区段 15
追加数字签名 / 附加数据 15
查看、删除，另存 数字签名 / 附加数据 15
【导入表页面】 15
添加 APi 16
其他 17
【导出表页面】 17
增加 / 删除导出函数 18

在位编辑 19
其他 19
【资源页面】 19
替换图标 20
另存资源 20
【重定位页面】 21
【异常页面】 22
【.net 页面】 22
【其他 PE 相关功能】 23
PE 清理工具 24
PE 重建工具 24
PE 文件的 Asm 分析功能 25
Asm 编辑功能 26
汇编对比功能 27
汇编代码转 Hex 代码工具 29
文件搜索功能 30
插件功能 31
【其他功能】 32
十六进制编辑窗口 32
大数进制转换功能 32
进程功能 33
【还没有说到的菜单项】 35
参数设置 35
输出文件信息 35
最近打开的文件 35
【附加说明】 36
务必联系我 36
版权信息 36
参考资料 36
感谢名单 37

【软件说明】

主要功能：

■支持 PE32、PE64、.net PE，提供丰富的 PE 分析功能。

■提供丰富的 PE 编辑功能。

■提供 RVA FOA 互相转换功能。

■提供 PE 反汇编及反汇编编辑、比较功能。

■提供 PE 内多种数据搜索功能。

■有限的查壳功能。

■有限的 PE 资源查看处理功能。

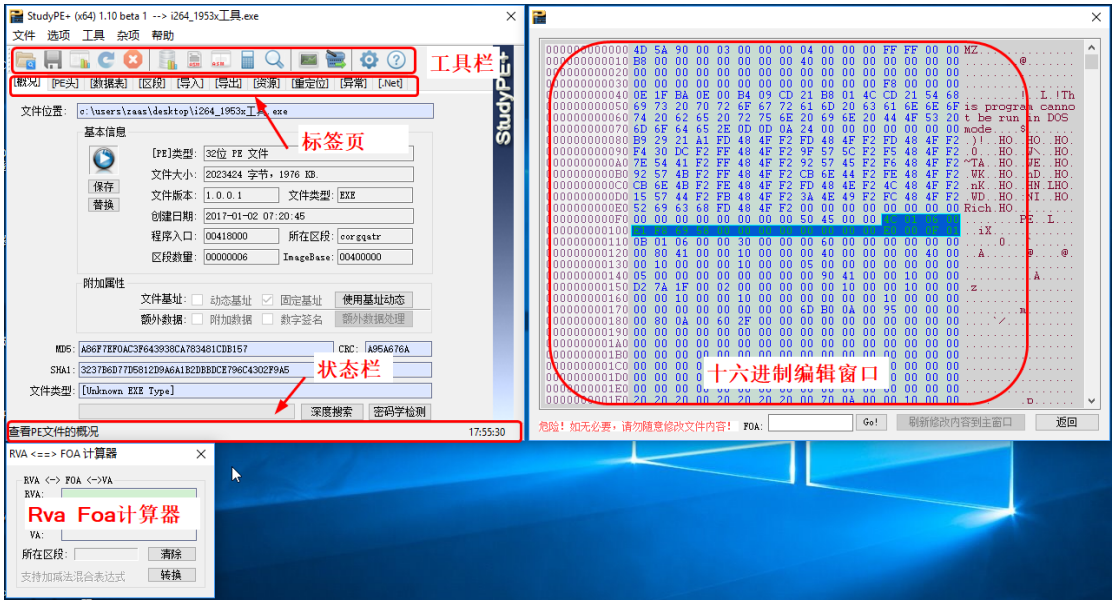
■有限的图片及文本格式文件查看功能。

==========

软件的主要窗口如下图所示。十六进制窗口和 Rva 计算取窗口以磁性窗口的方式吸附在主窗口上。当然你可以随意拖动他们或者很方便的关闭、打开他们。

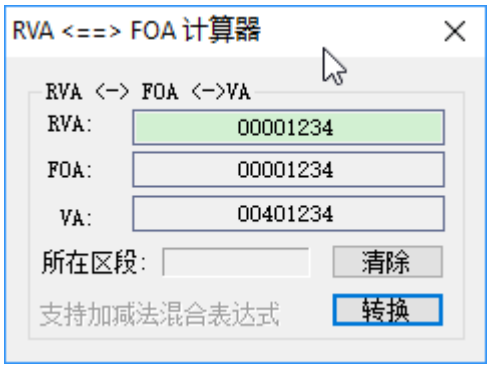
工具栏是一些常用工具的快捷打开方式。你可以把鼠标停留在工具栏的按钮上边，以便查看这些按钮都是什么功能。

状态栏会经常提示你的操作是否成功，如果你嫌他聒噪，你可以通过菜单的【选项】-【状态栏】打开或者关闭它。



在破解或者调试软件的过程中，我们常常需要在文件地址 FOa 和软件装载地址 Rva 以及运行的实际地址 Va 中转换，这个浮动窗口可以让你随时随地的转换这几个数据。

这个窗口可以随时从工具栏的按钮中打开或者关闭。



【基本操作说明】

1. 所有含有列表的页面都可以使用右键菜单选择相应的功能。
2. 大多数显示的图片都可以使用右键菜单选择相应的功能。
3. 所有的表格都可以【双击鼠标中键】复制整个表格到剪贴板。
4. 所有的表格都可以【双击鼠标右键】复制当前行到剪贴板。
5. 部分表格具有在位编辑的功能，你可以直接编辑列表框中的数据，但是并不是所有列表框均有这样的功能，下边详细介绍中会说明哪些列表框可以直接编辑。

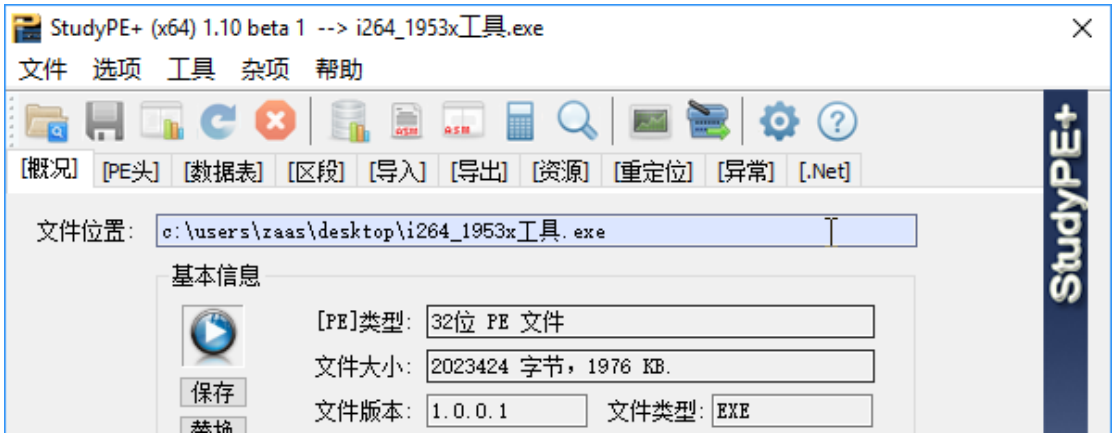
6. 在【十六进制编辑窗口】打开的状态下，【鼠标左键】点击任何表格有效行都可以在【十六进制编辑窗口】看到对应的数据。
7. 大多数文本框都处于只读状态，你可以复制数据，但是不可以直接修改它。如果你确实想要修改，请在【十六进制编辑窗口】中修改。
8. 大多数编辑 PE 的功能、PE 相关工具及进程相关工具都有对应的菜单，你也可以从主界面的菜单选择使用它们。

【打开一个文件】

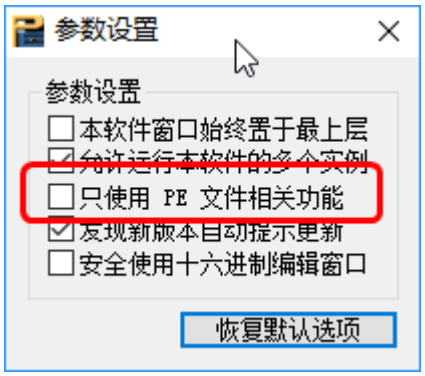
你可以通过拖拽拖入一个文件或者菜单：【文件】- 【打开文件】或者点击工具栏图标的方式打开一个文件进行分析。如果是 PE 文件或者 PE 的快捷方式，程序会对直接 PE 展开详细分析。

如果是文本文件，或者是图形文件，本工具是一个基本的图片查看工具。

如果是其他文件，本工具将显示其十六进制代码。



当然你也可以选择只关注 PE 的功能。你可以通过菜单的【选项】-【参数设置】或者工具栏的【设置】按钮，打开参数设置对话框，选择只使用 PE 相关的功能。



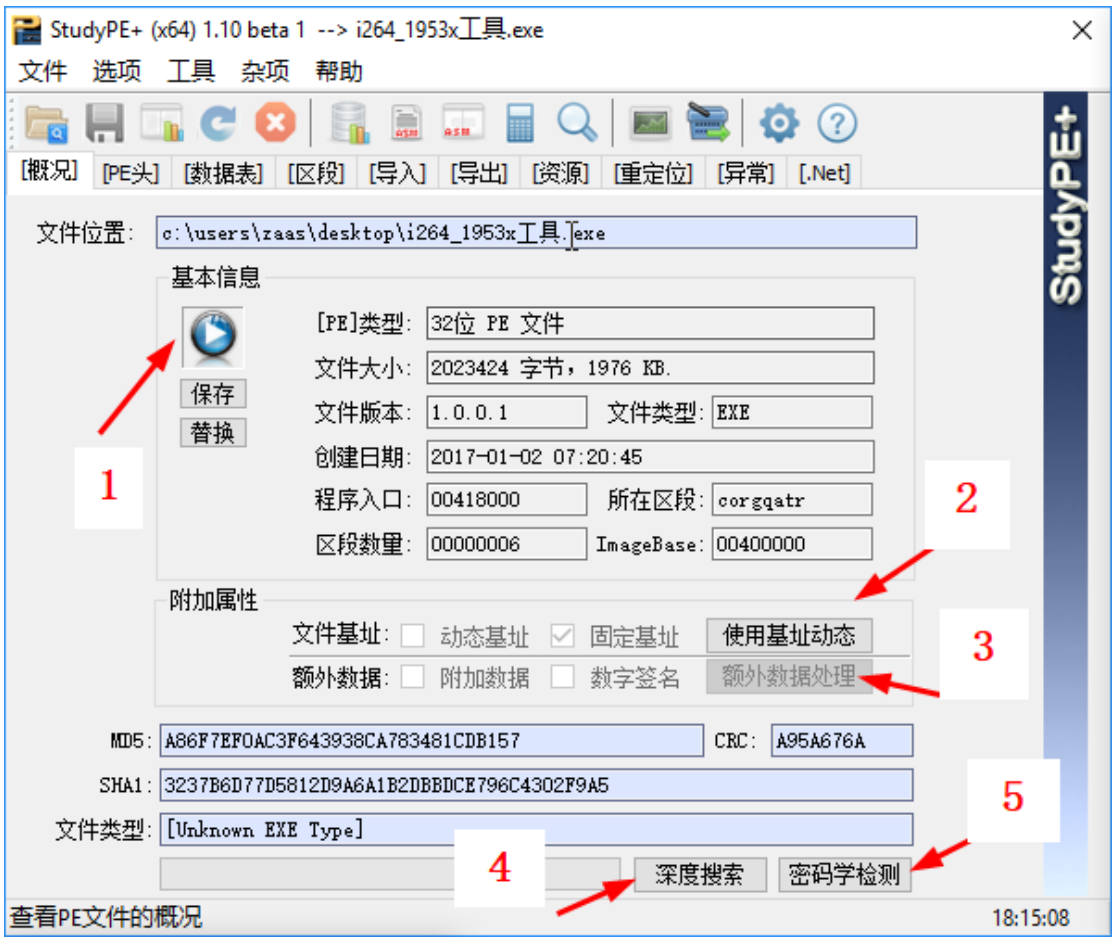
参数设置对话框还有一些其他的设置。当然他们很容易理解。比如【安全使用十六进制窗口】，它意味着十六进制窗口的数据只能看，不能编辑。

标签页面说明

PE 文件的详细通过标签页的方式展示。

【概况页面】

这里展示了你打开的 PE 文件的一些基本信息。这都很容易理解。



替换图标

1. PE 文件的图标，你可以【保存】或者【替换】它。

一共需要 4 个步骤：

1.1 选择要替换的图标。

1.2 选择一个图标文件。你可以选择【拖拽】或者【浏览】。

1.3 选择图标文件中的一个图标。

1.4 点击确定替换。

本功能支持 ICO 格式和 PNG 格式的图标。但是要注意，新图标文件大小不能超过原有图标文件大小。这些基本信息都在对话框上显示着呢。需要说明的是，显示哪个图标是系统自己决定的，如果你选择的不是系统显示的图标，替换后并不能让系统显示你替换后的 PE 文件图标。

改变基址

2. 你可以看到 PE 文件使用的是固定基址还是动态基址，你也可以随意改变 PE 的基址使用方式

额外数据处理

3. 你可以很直观的看到 PE 文件有没有附加数据或者数字签名，如果你不喜欢他们，你可以直接把他们删除。或者，你可以在【区段】页面选择进一步处理它们。

特征码分析

4. 在这个页面，你已经看到 PE 文件可能的加壳类型了，如果初步检查没有结果，或许你想进一步看看软件有没有加壳或者是用什么语言编译的，你可以点击这个按钮。它会在 userdb 文件里进一步搜索 PE 文件的特征码，当然这会相对比较耗时。

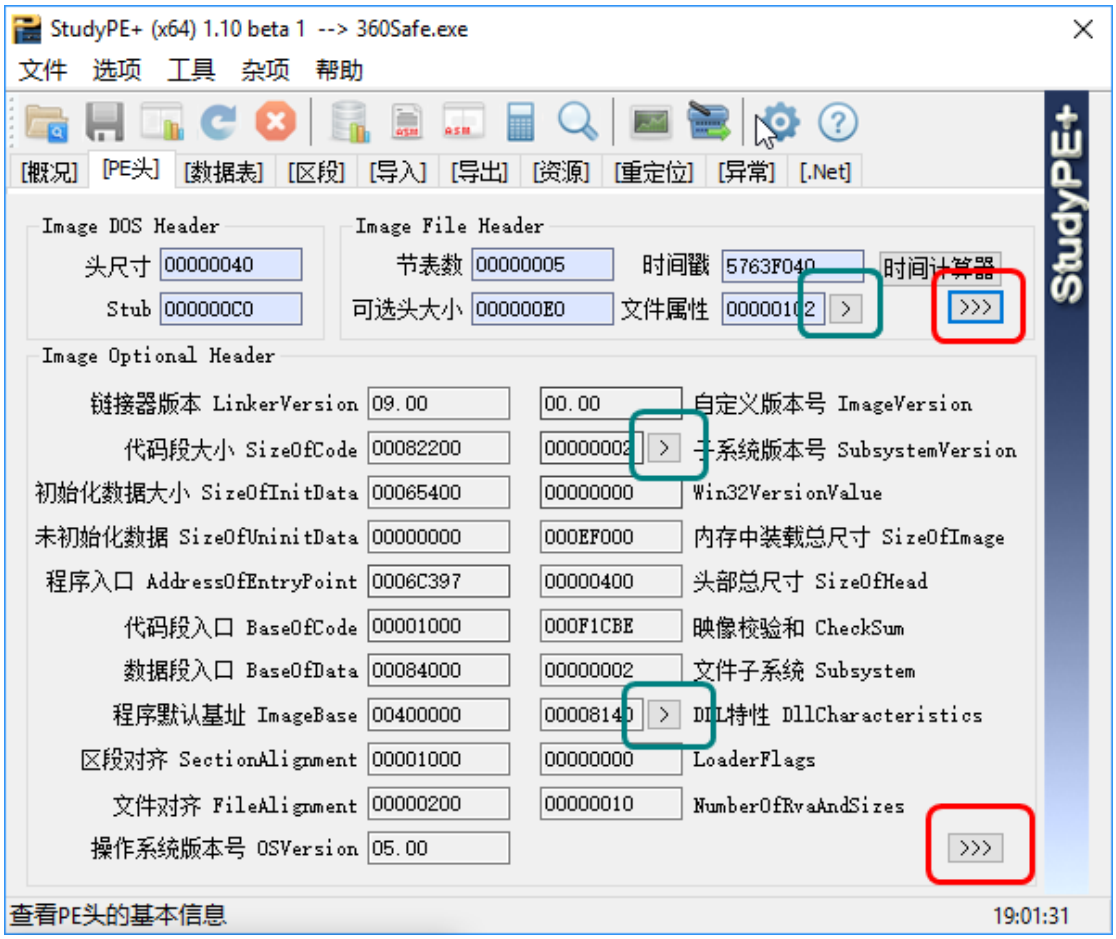
密码学分析

5. 如果你想知道这个 PE 文件里边用了什么样的密码学工具，你可以点击这个按钮，搜索一下文件里的密码学特征码，这样你在破解这个 PE 文件的时候就心中有数，可能软件的注册方式是用了这些 MD5，SHA512 或者其他的，谁知道呢。

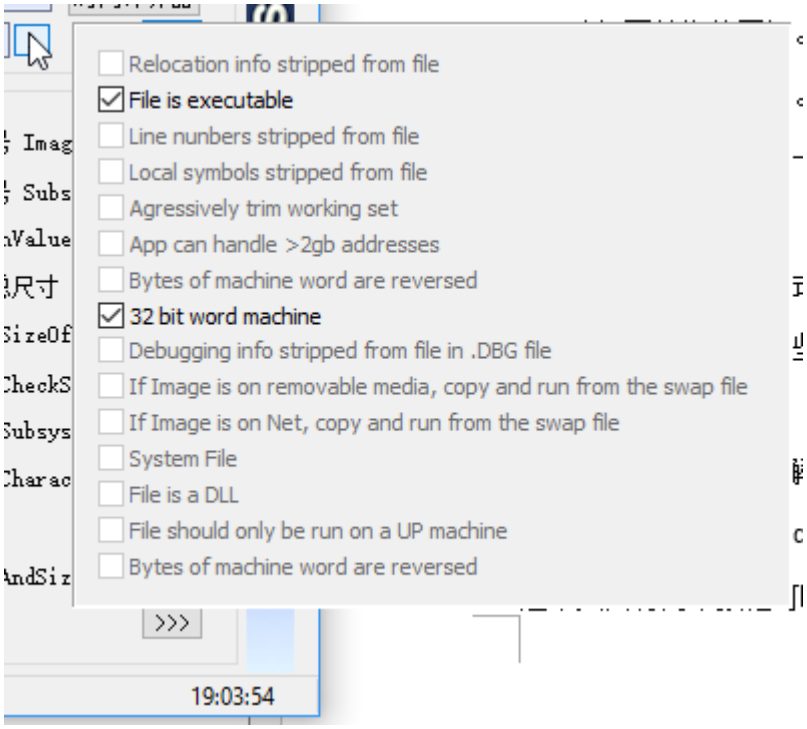
【PE 头页面】

如果你对 PE 文件不了解，没关系。你可以从这个页面得到这个 PE 文件的 Dos header，File header 和 Optional Header 的基本信息。

这个页面有两个按钮可以直接定位到【十六进制编辑窗口】的相关部位，方便你学习和研究它们。

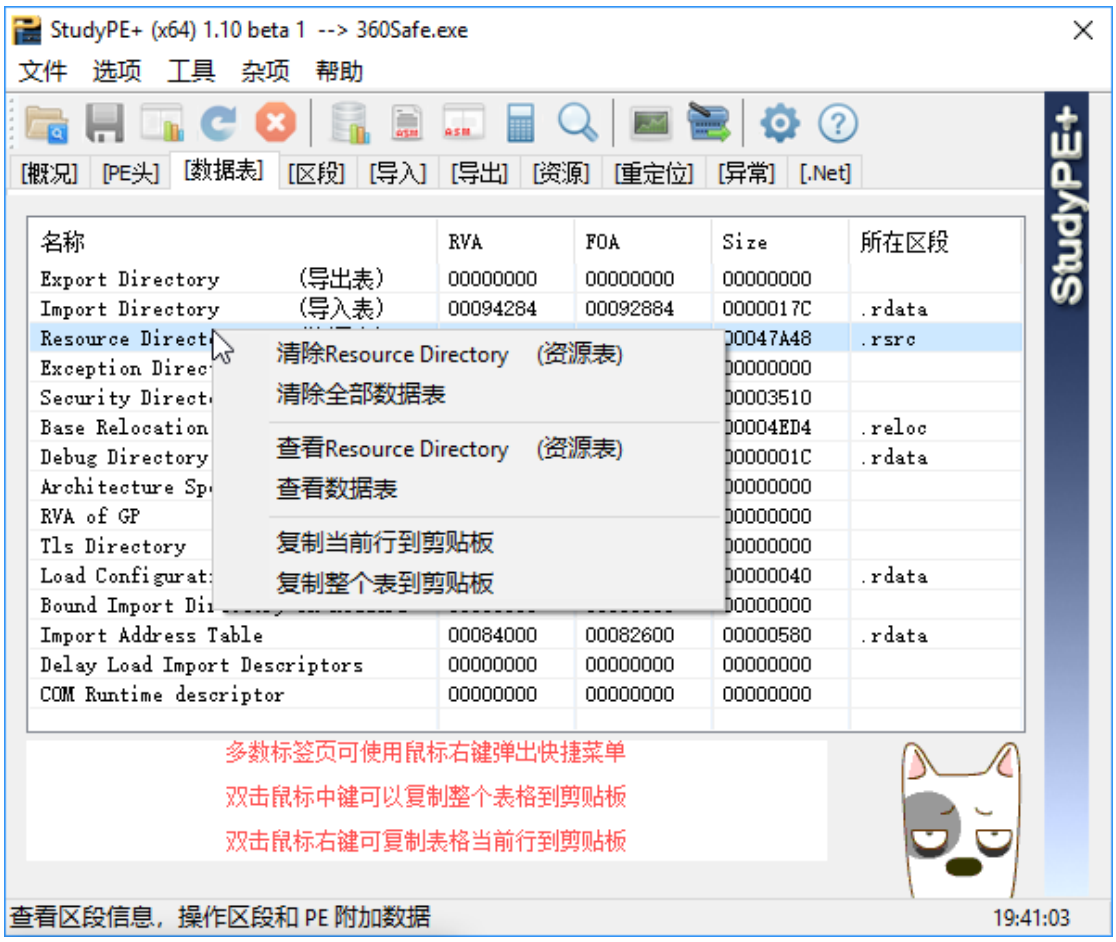


此外还有几个小的按钮会用浮动窗口的方式展现出这几个数据的含义，当你把鼠标移动到这几个按钮上他们就会自动浮现。



【数据表页面】

你可以用【右键菜单】选择查看、复制或者清除当前数据表项以及全部数据表。



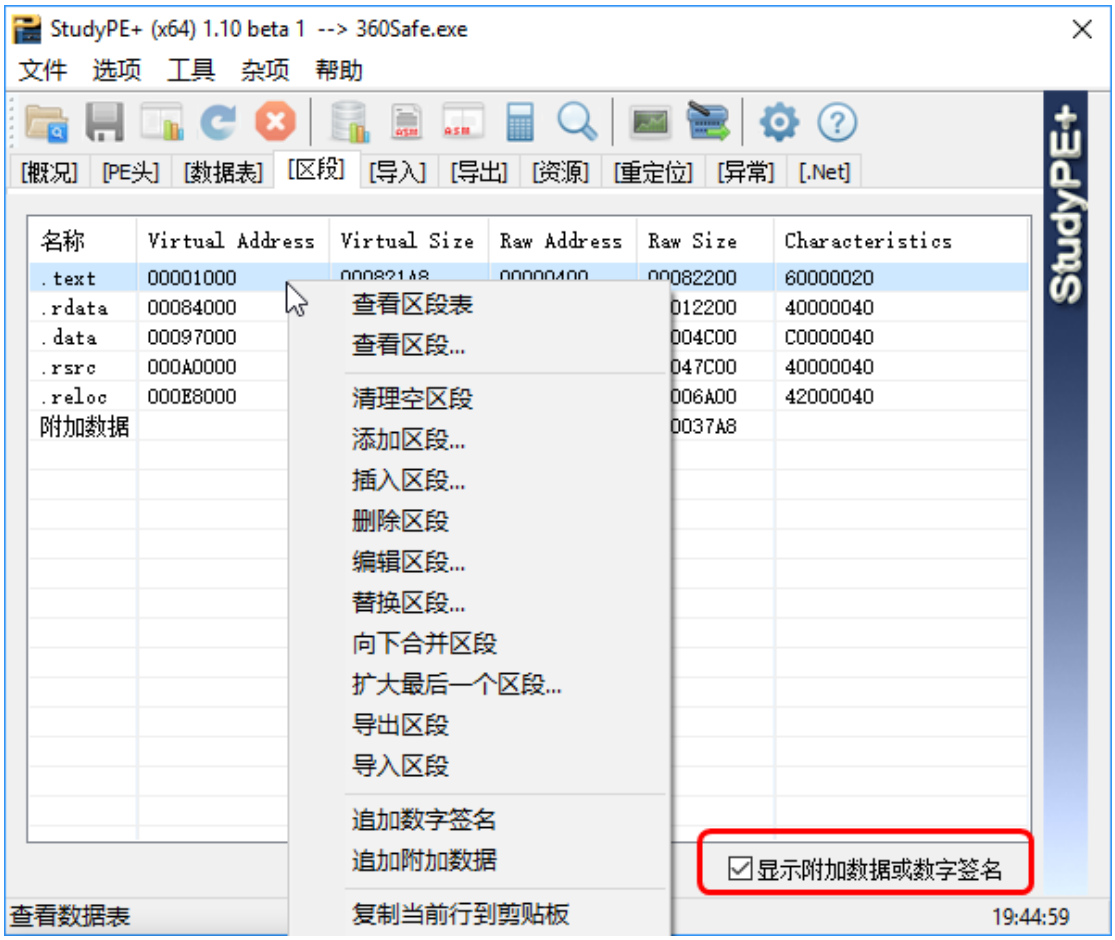
在位编辑

需要说明的是，数据表支持在位编辑。但是你只能编辑 rva 和 size 两项，其他项依赖于这两项的数据，所以不可以随意更改。

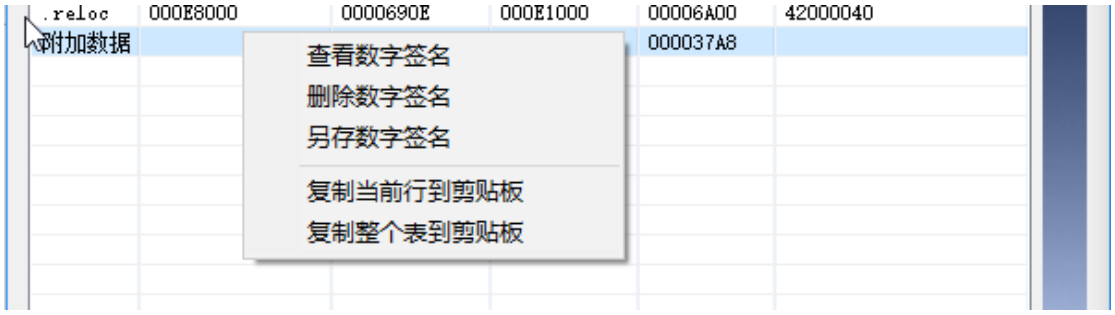
【区段页面】

右键菜单提供了丰富的区段编辑功能。当然程序主菜单也提供了这些功能的另一个快捷使

用方式。需要说明的是，有些功能依赖于你选择了列表中的哪一行数据，如果你没有选择任何一行，它不会起作用。



选中【显示附加数据或数字签名】会在列表中显示对应的数据（如果有的话），当它显示出来的时候，【鼠标右键】点击这一行的时候，会出现不同的菜单。



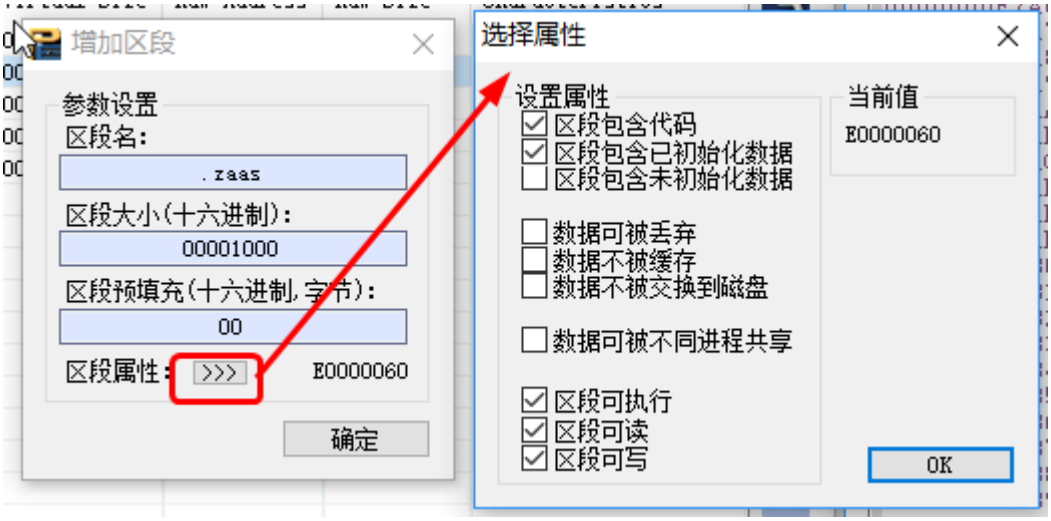
区段操作基本上全部属于危险操作，稍有不慎会导致程序崩溃。请谨慎选择。

清理空区段

有些 PE 文件空区段不可清理，清理之后会导致它无法运行。

添加区段

添加区段的对话框将会弹出。需要说明的是区段属性可以在点击按钮之后弹出选择区段属性对话框，可以直观的选择你需要的区段属性。如果你乐意，可以设置【区段预填充】，这样你新增的区段就会用你指定的字符填满。



插入区段

将在你指定的行之下增加一个区段。后边的区段将依次后移。

删除区段

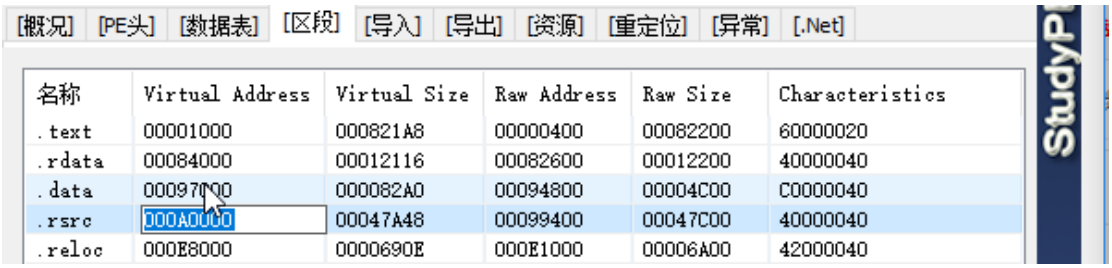
你选择的区段将会被删除。

编辑区段

区段的所有字段均可编辑，同样，你还可以人机交互的选择区段属性。

在位编辑区段

区段页面你还有另一种选择—不需要打开任何新的对话框，直接在列表中编辑数据。此时数据检查必须你自己把握，需要你对区段的信息具有相当的熟悉程度。



替换区段

打开一个文件，用文件中的数据替换区段中的数据。

向下合并区段

将你选择的区段和下一个区段合并。

扩大最后一个区段

参见【添加区段】

追加数字签名 / 附加数据

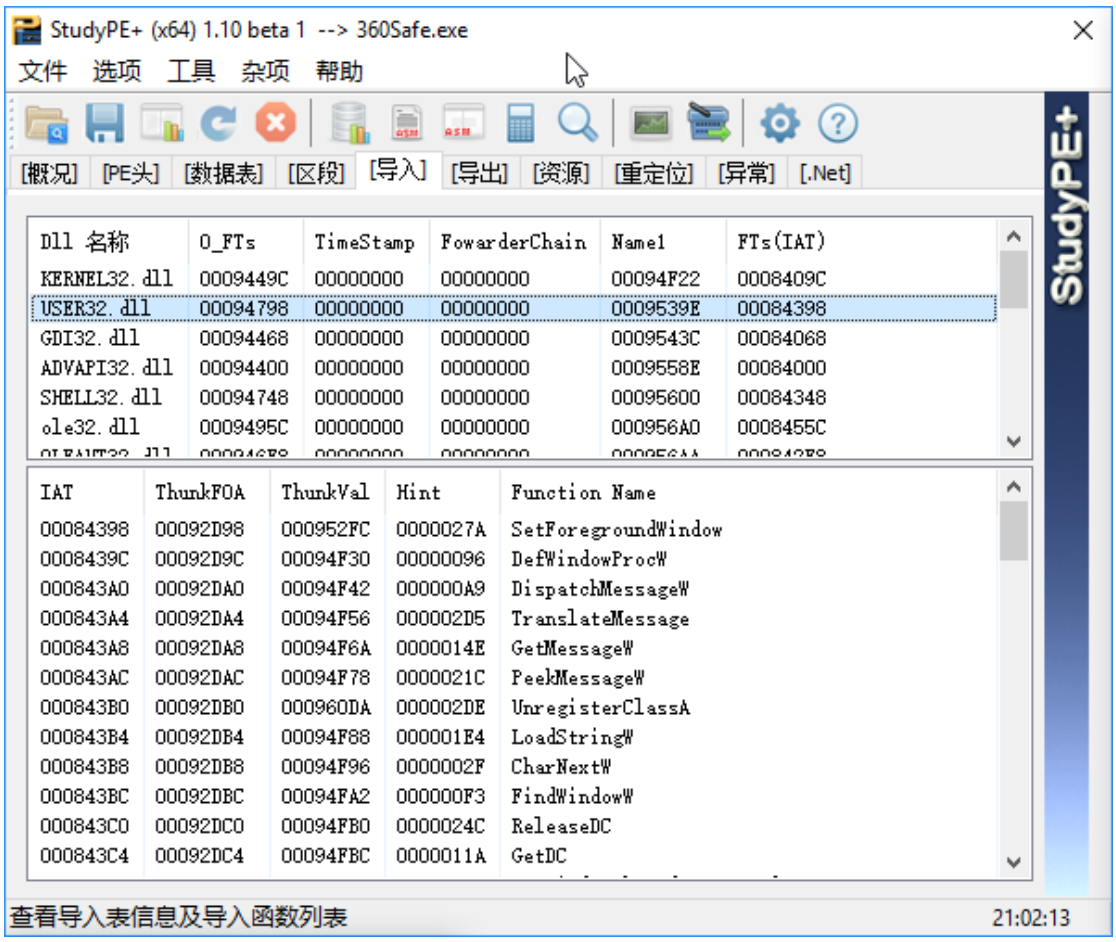
没什么好说的，很清晰的功能。

查看、删除，另存 数字签名 / 附加数据

没什么好说的，很清晰的功能。

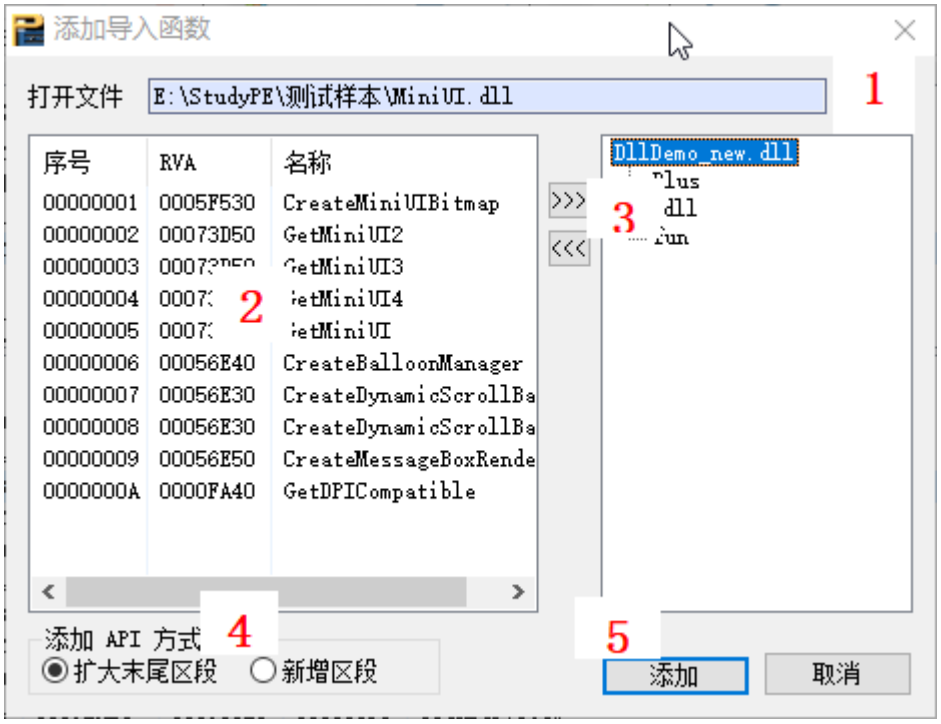
【导入表页面】

查看、增加、编辑导入表。点击导入 dll 可以马上看到从该 dl 中导入的函数。国际惯例，有名字的导入函数显示其名称，没有名称只有序号的函数其 hint 和名称显示为“-”。



添加 APi

本页面最重要的附加功能就是增加导入函数了。本工具支持一次性添加多个导入 dll 的多个导入函数，请按照以下步骤完成本项操作。



1.1 用拖拽或者浏览的方式打开一个带有带出函数的 dll 或者 exe

1.2 选择你想要添加的函数（支持 Shift + 鼠标左键多选以及双击函数列表项添加到右边列表）；

1.3 点击按钮添加到右边列表（如果想要删掉的可以点击删除）

1.4 选择添加的方式：扩大末尾区段或者直接新建一个区段，两者功能上没有区别，只是 Pe 文件格式上的不同而已。默认为扩大末尾区段方式。

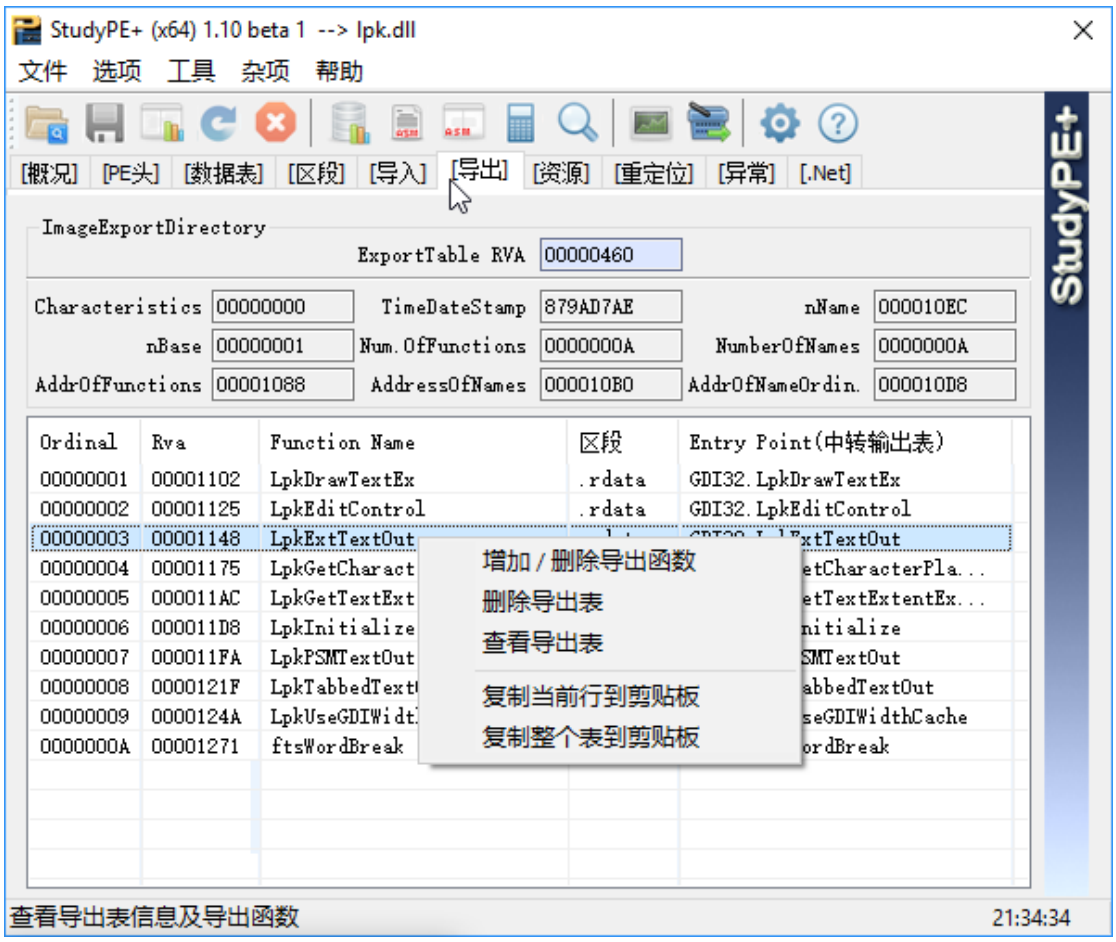
1.5 点击【添加】

其他

其他功能都很一目了然，不再赘述。

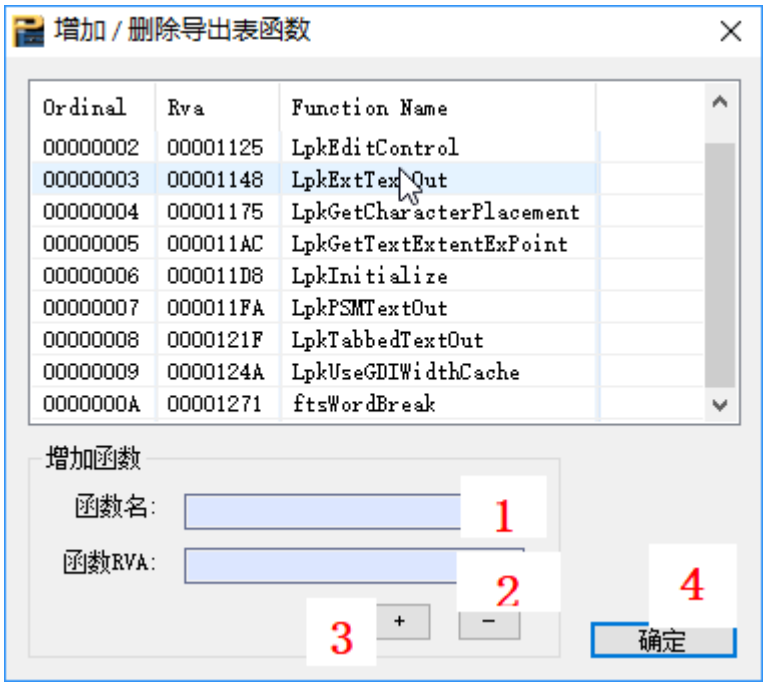
【导出表页面】

查看、增加、编辑导出表。对于特殊的 dll（比如 lpk.dll）中转输出表可以直接分析实际的输出表 dll 及函数位置。



增加 / 删除导出函数

同样，本页面最重要的功能还是【增加 / 删除导出函数】。需要说明的是，【增加 / 删除导出函数】只支持以函数名为导出的方式，而且，函数 rva 需要你对软件调试完全熟悉并且知道你在干什么。



本操作需要 4 个步骤：

1.1 输入函数名

1.2 输入函数 rva

1.3 点击增加“+”

1.4 确定。当然你也可以点击“X”取消，本操作将不被执行。

在位编辑

导出函数页面支持在位编辑。但是，只有 rva 项和 function name 可以编辑。因为表格中其他项均依赖于这两项内容，所以不可以直接编辑。

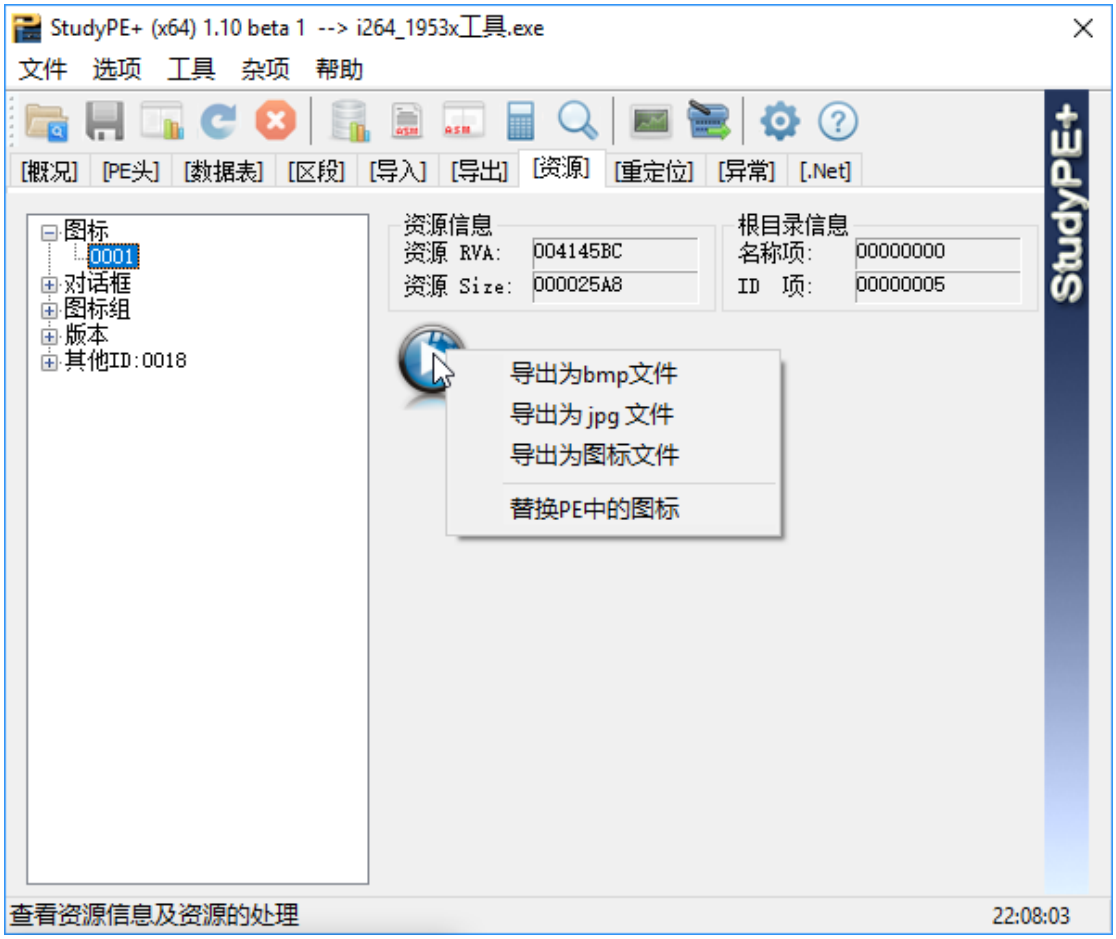
其他

其他功能都很一目了然，不再赘述。

【资源页面】

本页面用于展示、编辑 PE 文件里的资源。点击每项资源都可以显示其内容。如果是图形资源或者图标或者光标资源，直接显示其图片；如果是菜单资源、版本资源及其他文本资源，尽量显示其文本信息如果是图标组资源、光标组资源，用表格的形式显示其内容。实在没办

法分析的资源及对话框资源，用十六进制代码显示资源内容。同样的，列表资源可以用【基本操作说明】章节里说到的方式进行复制、查看及保存。部分加壳 PE 的资源无法显示，这是正常现象。

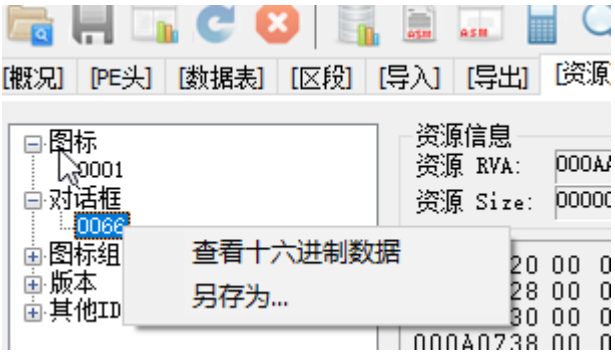


替换图标

这里的替换图标方式与【概况】页面不同。如果【概况】页面替换失败，请从这里替换。

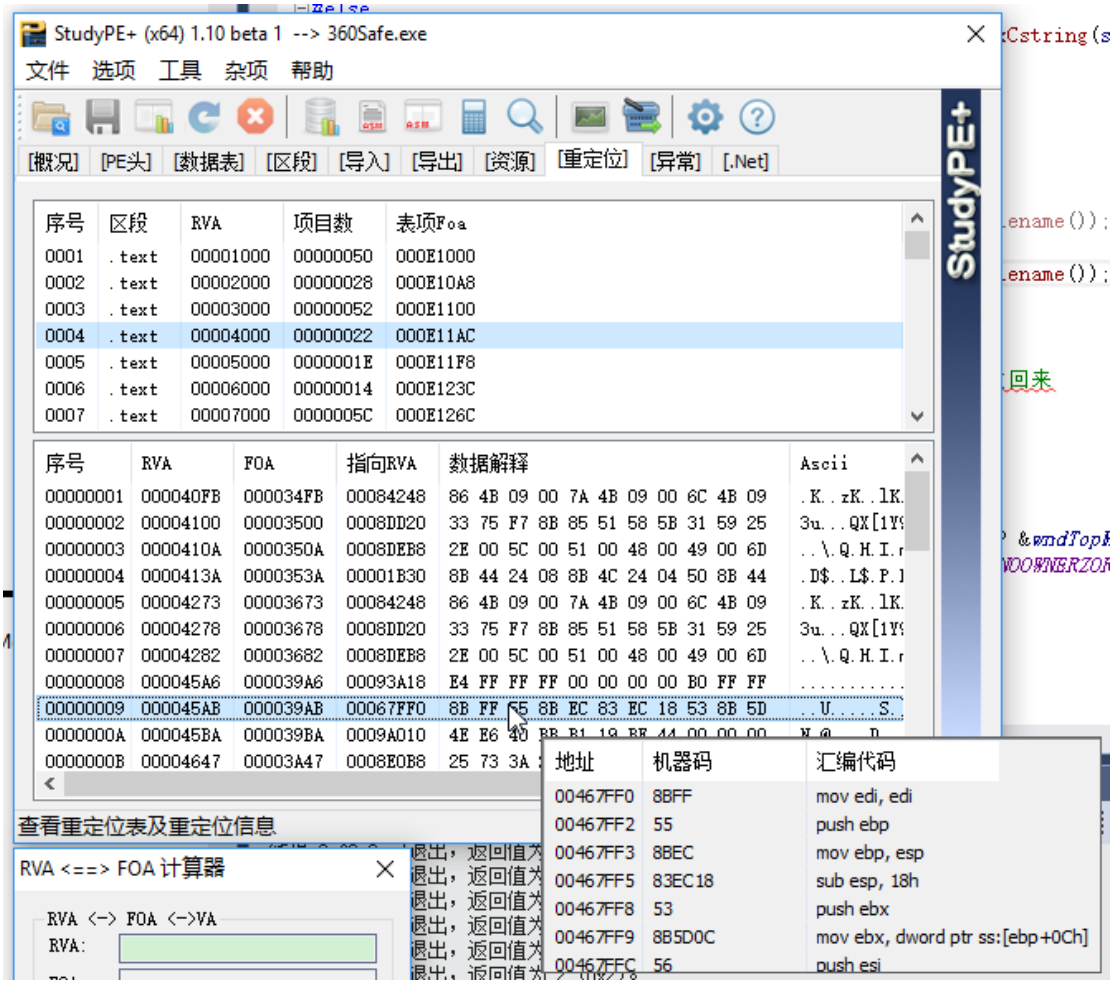
另存资源

各种资源均可以保存成单独的文件。对于图形文件（包括图标和光标文件），保存后的信息是可以直接用图形浏览软件打开的，兑取其他资源，保存的只是其 16 进制数据。如果图形信息非法，你得到的也只是其 16 进制数据。



【重定位页面】

顾名思义，重定位页面展示 PE 文件的重定位信息。Exe 文件的重定位信息可有可无，所以菜单里有删除重定位信息的选项。此外重定位信息的数据解释同样以浮动窗口的样式显示其汇编代码，如果重定位到某个函数地址的话。

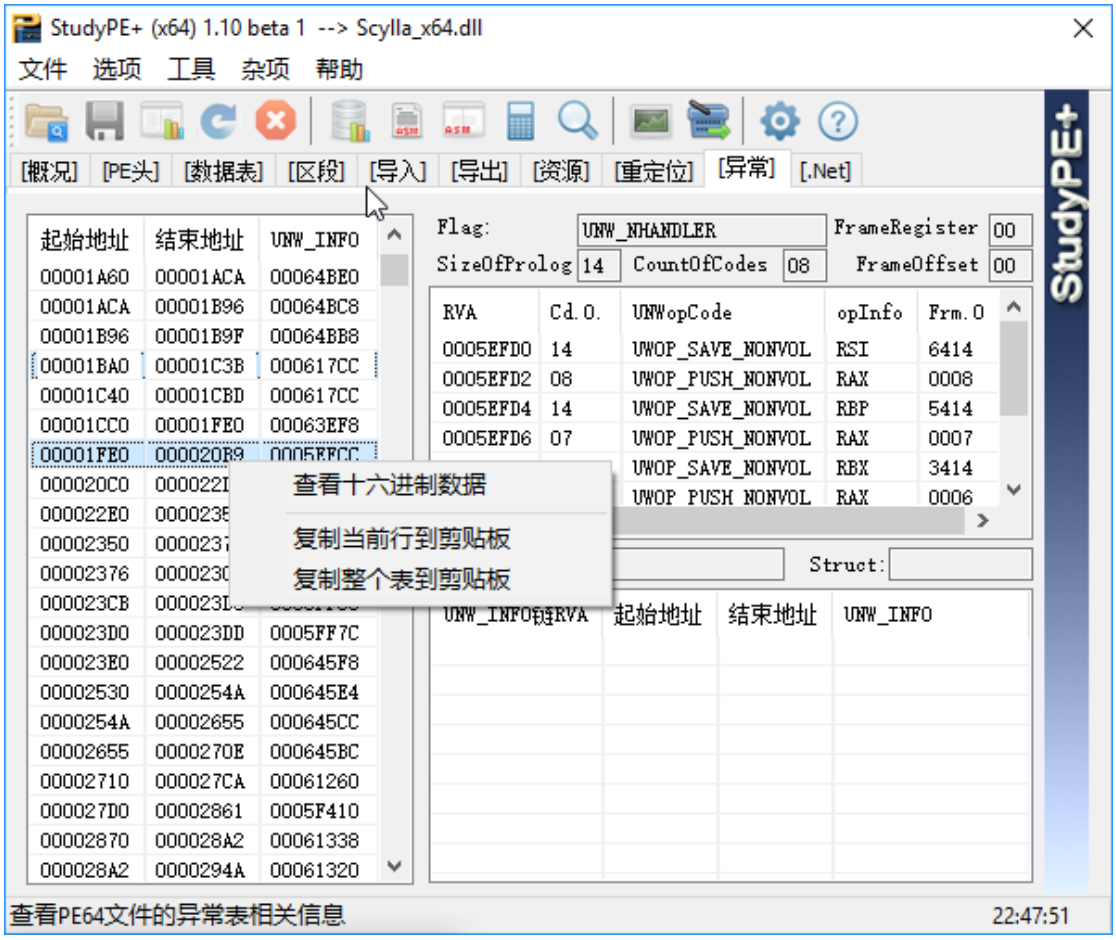


特别说明

如果鼠标移开而数据解释小窗口未能自动消失，请点击一下小窗口或者按 ESC，小窗口就会关闭。

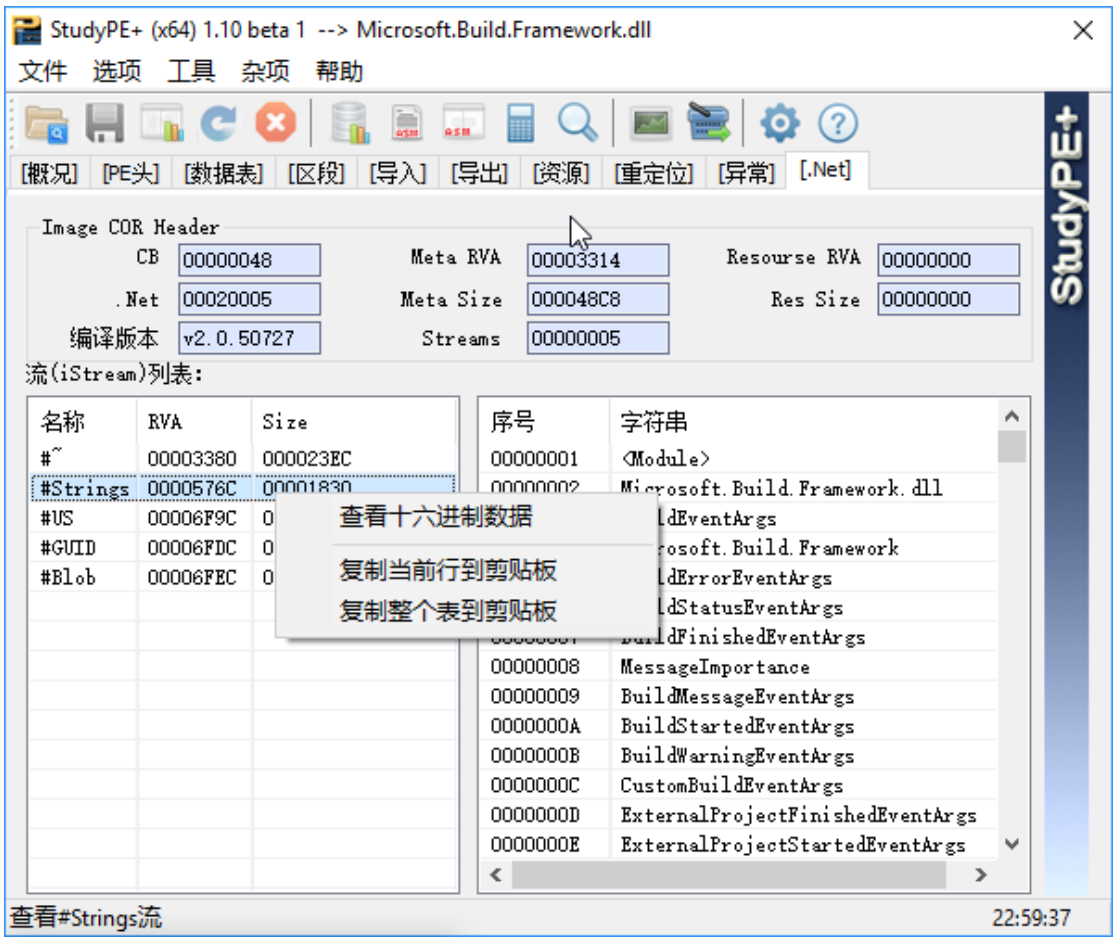
【异常页面】

本页面展示 PE 文件的异常信息。需要特别说明的是，x86 文件没有异常表的信息，本页面及用于 x64 的 PE 文件。



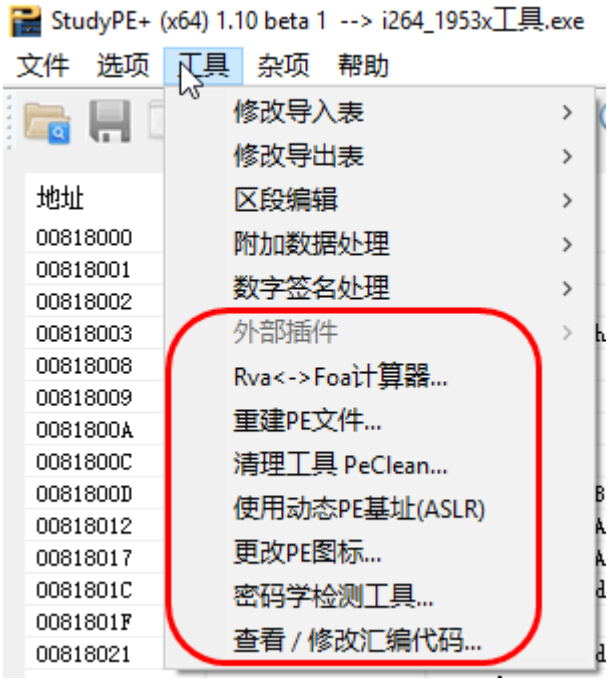
【.net 页面】

本页面展示.net Framework 文件的基本信息。正如大家所知道的，.net PE 和正常的 PE 并不一样，目前本工具只分析了#strings 流的信息，下一步的工作中将会对.net PE 进行深入分析。



【其他 PE 相关功能】

本软件还具有丰富的 PE 相关其他功能。这些功能不依赖于某一项操作，所以放在单独的位置。你可以从菜单选择使用他们，有些可以从工具栏图标快捷使用。当你打开了一个 PE 文件，【工具】菜单就会自动显示出来。



PE 清理工具

工具位置：菜单 - 【工具】- 【清理工具 Peclean...】

PE 文件里边包含了大量的无用信息，而他们是可以清理的。当然 PE 文件千差万别，可能有些信息清除掉会导致 PE 无法运行，所以请谨慎选择要清理的选项。如果清理后的 PE 无法运行，请减少选项或者一项一项去实验直到找到最佳选项为止。清理选项如下图所示：

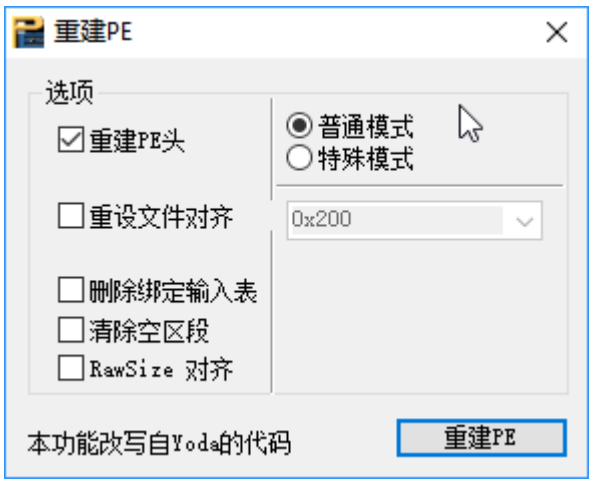
PE 重建工具

工具位置：菜单 - 【工具】- 【重建 PE 文件...】

你还可以更进一步选择重建 PE 工具。使用重建 PE 工具可以有效的减小问价大小。

如果你了解 PE 文件，这些选项都一目了然。唯一需要解释的是：

【普通模式】下 dos 头维持原有大小，【特殊模式】连 Dos 头都被清理掉，只保留最有必要的 0xc 个字节。Dos 头的其他数据已经没有存在的必要，这也是我在【PE 头页面】只显示两项 Dos header 数据的原因。

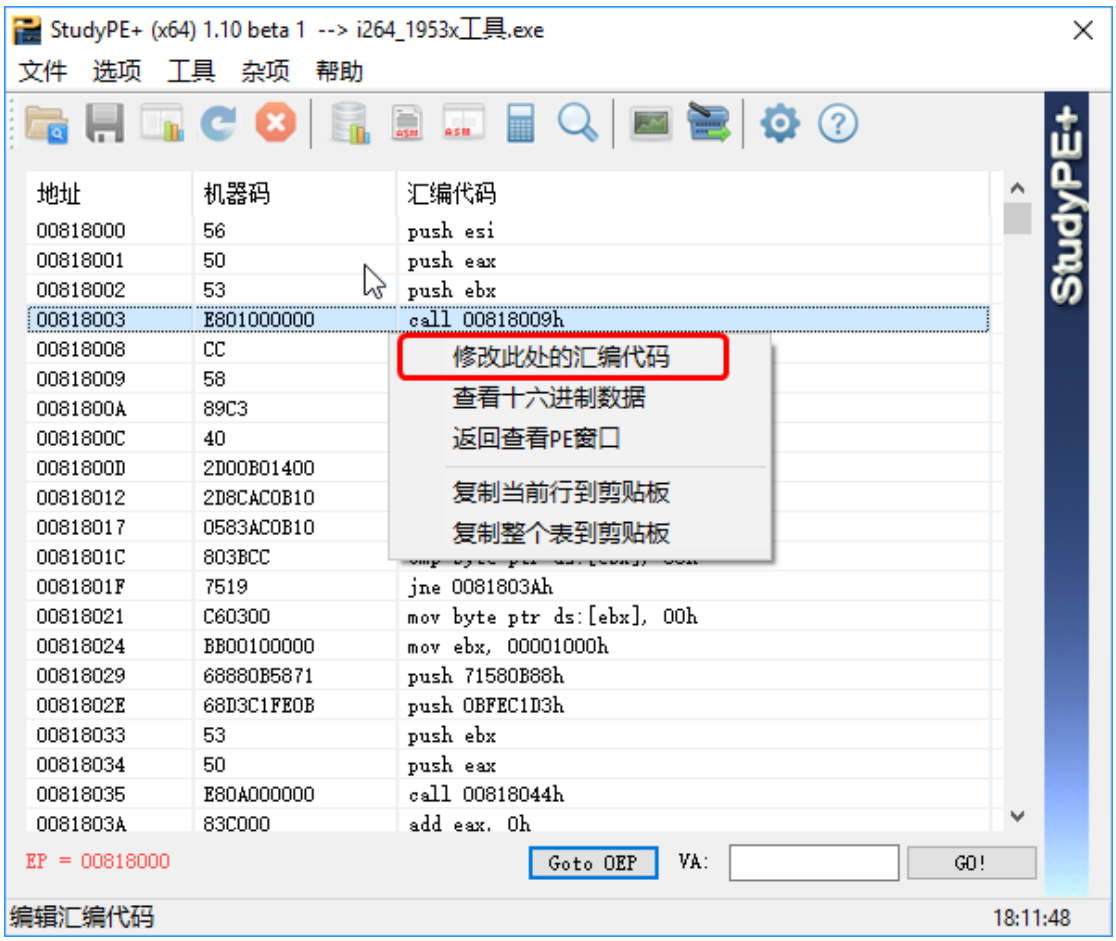


PE 文件的 Asm 分析功能

工具位置：菜单 - 【工具】- 【查看 / 修改汇编代码...】

或者选择从工具栏直接打开它。

这里的反汇编引擎为 BeaEngine，无论 x86 还是 x64 都能正常反汇编。按照大家使用 OD 的习惯，汇编代码跳转方式选择输入 Va 的方式。Goto OEP 这里跳转到的是 PE 头里边指定的 EP，并不是指脱壳后的 OEP，抱歉让有些期望自动脱壳的朋友失望了。



Asm 编辑功能

工具位置：反汇编窗口【右键】 - 【修改此处的汇编代码...】

选择之后会打开另一个窗口，在合格窗口里你可以输入自己期望的汇编代码。需要说明的是，这里你可以按着【Shift】键对汇编表格多选，选中的内容都可以显示到修改汇编代码对话框。

输入汇编代码的时候请注意，十六进制数据必须以后缀 h 的方式输入，就如同汇编代码显示的那样。比如：

mov eax,1234h

jmp 401000h

如果你输入的汇编代码是合法的，你将在【Opcode】编辑框里看到成功转换出来的 hex 代码。如果失败了，请注意观察主窗口的状态栏给出的错误原因，然后再试一次。

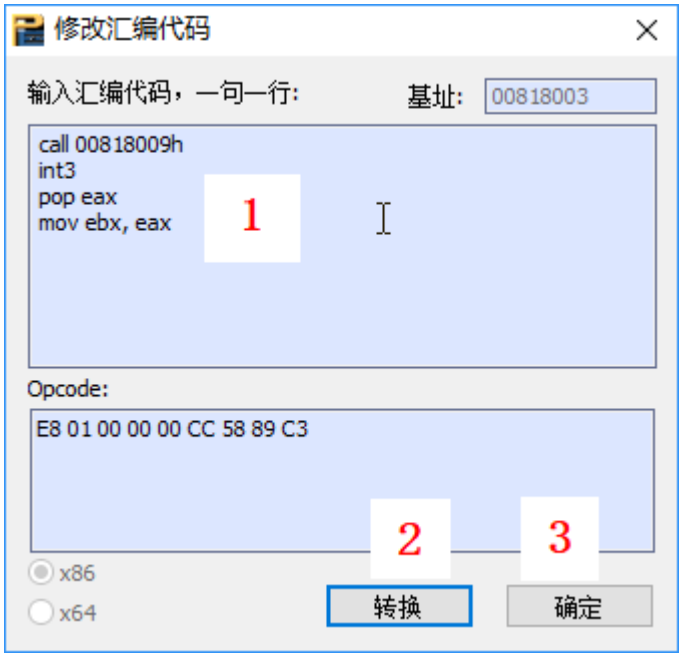
这里你只需要三个步骤：

输入汇编代码。

点击转换。

点击确定（如果能成功转换的话）。

然后你就可以在【查看 / 修改汇编代码页面】看到你修改后的成果。



想要修改汇编代码还有另一个途径。前提是你知道你要修改的汇编代码对应的 hex 代码。在未选中【安全使用十六进制编辑窗口】的条件下，从【查看 / 修改汇编代码页面】使用【右键菜单】选择【】，然后直接修改 hex 码，点击【刷新修改内容到主窗口】，即可即时看到你修改的效果。

注意：你想要替换的汇编代码的 Opcode 长度应该和原汇编代码的 Opcode 长度一致，否则不能保证 PE 文件运行会不会出错。如果长度不一致，请手动补充 Nop 或者在【十六进制编辑窗口】手动输入 0x90。

在后续版本中可能我会增加自动补充 Nop 的功能。

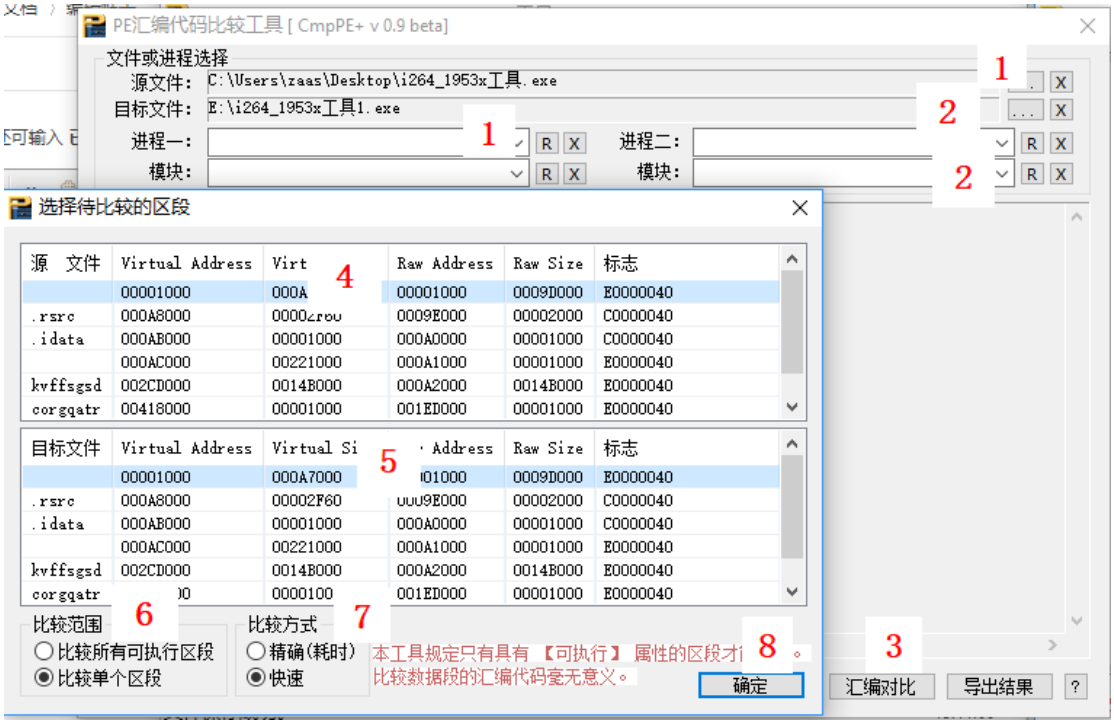
汇编对比功能

工具位置：菜单- 【杂项】 - 【汇编代码比较...】

现在你眼前摆着两个文件，一个是原始文件，另一个是破解过的文件。你迫切想要知道，别人的破解修改了原始文件的什么地方，是不是？好吧，这个工具可以给你答案。（如果别人为了保护自己的知识产权，对修改后的文件加了壳或者其他保护措施，本工具无法比较出正

确的结果）

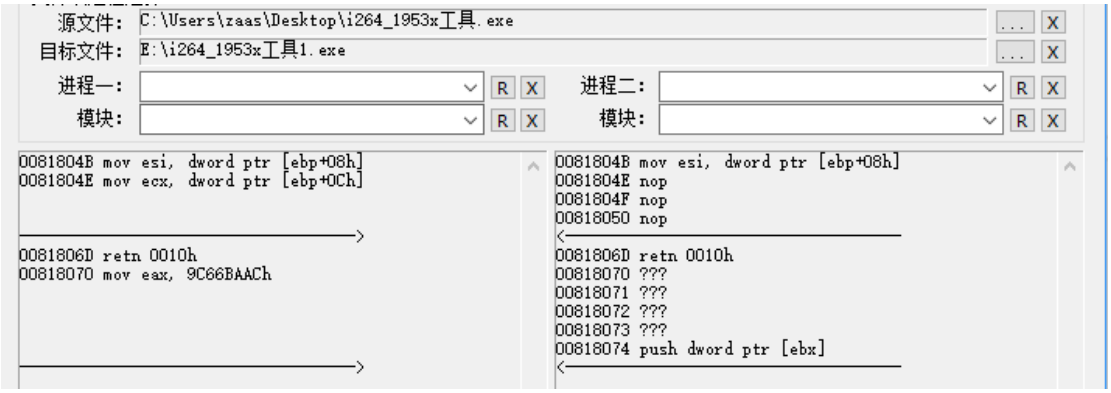
这里不单纯可以比较两个 PE 文件，也可以比较进程以及进程中的模块。本工具预设只能对比具有可执行属性的区段，而且两者 Rva 一致。如果两个区段大小不等，按照较小的那个进行比较。（比较数据区段的汇编代码毫无意义，比对 rva 不同的汇编代码简直不可理喻，对吧？那里你可以直接比较十六进制代码。如过需要，下个版本我可以另外提供一个比较十六进制代码的工具）



你可以通过以下步骤实现汇编对比。

1. 选择源文件或者一个进程或者进程的一个模块；
2. 选择目标文件或者目标进程或者目标进程的一个模块；
3. 点击【汇编对比】按钮
4. 在弹出的对话框中选择源文件中想要比较的区段；
5. 在弹出的对话框中选择目标文件中想要比较的区段；
6. 设置比较范围；
7. 设置比较方式
8. 点击【确定】开始比较。

比较结果将在对话框中的编辑框里展示。你可以清除或者保存对比结果。



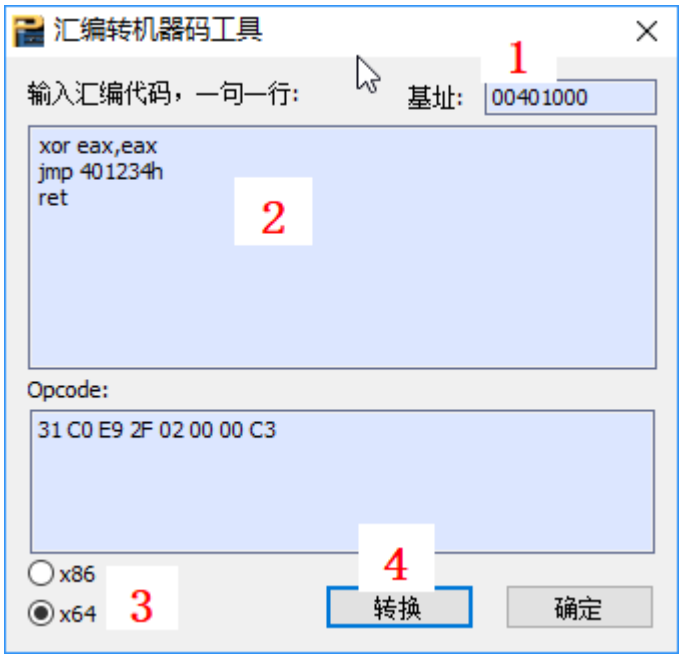
汇编代码转 Hex 代码工具

工具位置：菜单- 【杂项】 - 【汇编代码转机器码...】

你并不是必须打开一个 PE 文件才能做汇编代码到机器码的转换。你也可以直接输入汇编代码，求得其机器码用于在其他软件中的修改。那么你可以使用这个工具。后续要不要写一个不依赖于 PE 文件的机器码转汇编代码的工具？我以前写过一个把字符串转换为汇编代码，用于在 OD / x64Dbg / Ida 中直接粘贴的工具要不要继承到本软件中来？思考中...

好吧，你还是需要 4 个步骤：

1. 如果你要转换的汇编代码包含地址，请务必设置修改的基址。
2. 输入汇编代码。
3. 选择转换的模式是 x86 还是 x64；
4. 点击转换按钮。同样，如果汇编代码能成功转换的话，你会看到结果，否则请注意观察主窗口的状态栏给出的错误原因，然后再试一次。



文件搜索功能

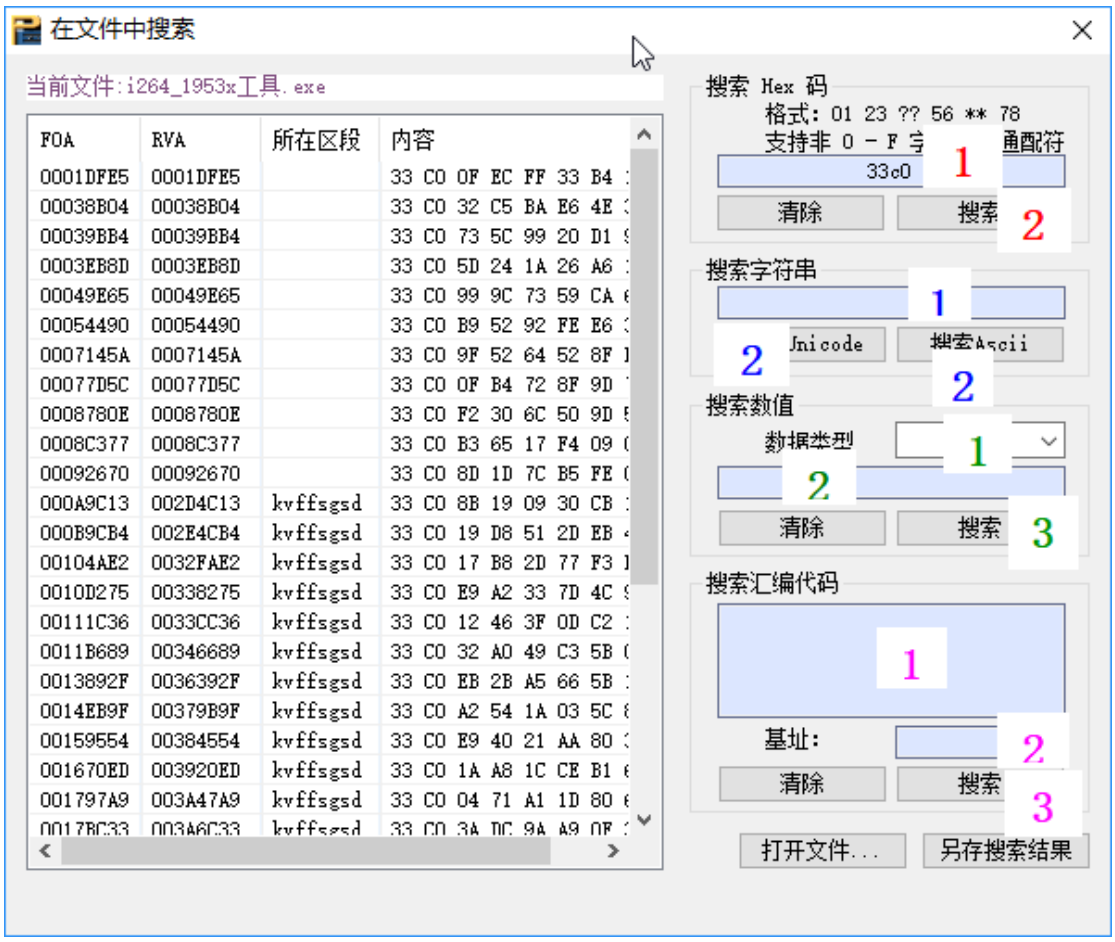
工具位置：菜单- 【杂项】 - 【在文件中搜索...】

如果你打开了一个 PE 文件，本功能自动在这个 PE 文件中展开搜索。当然你也可以通过【拖拽】或者【浏览】打开一个新的文件进行搜索。

如图所示，你可以选择搜索十六进制代码、常数、unicode 字符串、ansi 字符串或者汇编代码。他们的搜索方式大同小异，步骤最多有三个：

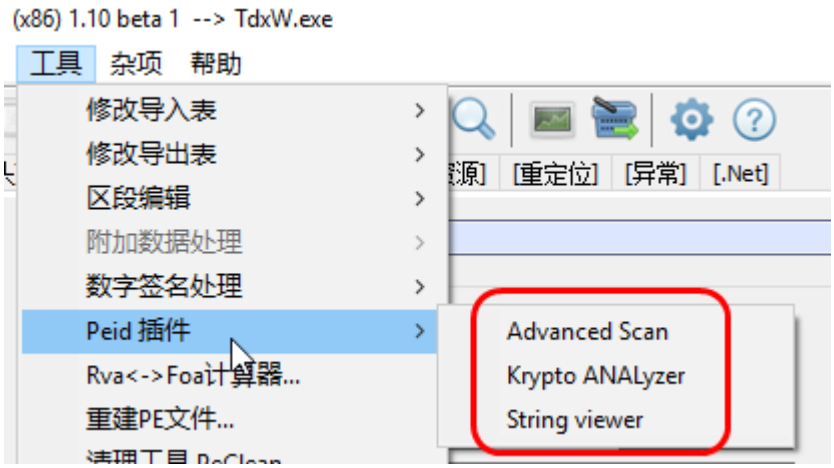
1. 选择数据类型或者基址（如果需要的话）
2. 输入想要搜索的内容
3. 点击【搜索】

输入的注意事项要么直接有说明，要么请参见汇编代码部分的说明。搜索结果将在左半部分展示出来，你可以清除掉或者保存搜索结果。当然你也可以用【基本操作说明】里的方法复制到剪贴板。



插件功能

本程序直接集成 Scylla，对应的 x86 版本支持 Scylla_x86，x64 版本支持 Scylla_x64。对于 x86 版，直接支持 Peid 的插件，你可以把你想要加载的 Peid 插件 copy 到本软件所在的 plugins_x86 文件夹下。本软件启动时，就能自动加载它们。需要注意的是某些 Peid 插件编写不规范，有可能会导致本软件崩溃。如果这种情况发生，请移除（删除）相应的插件。

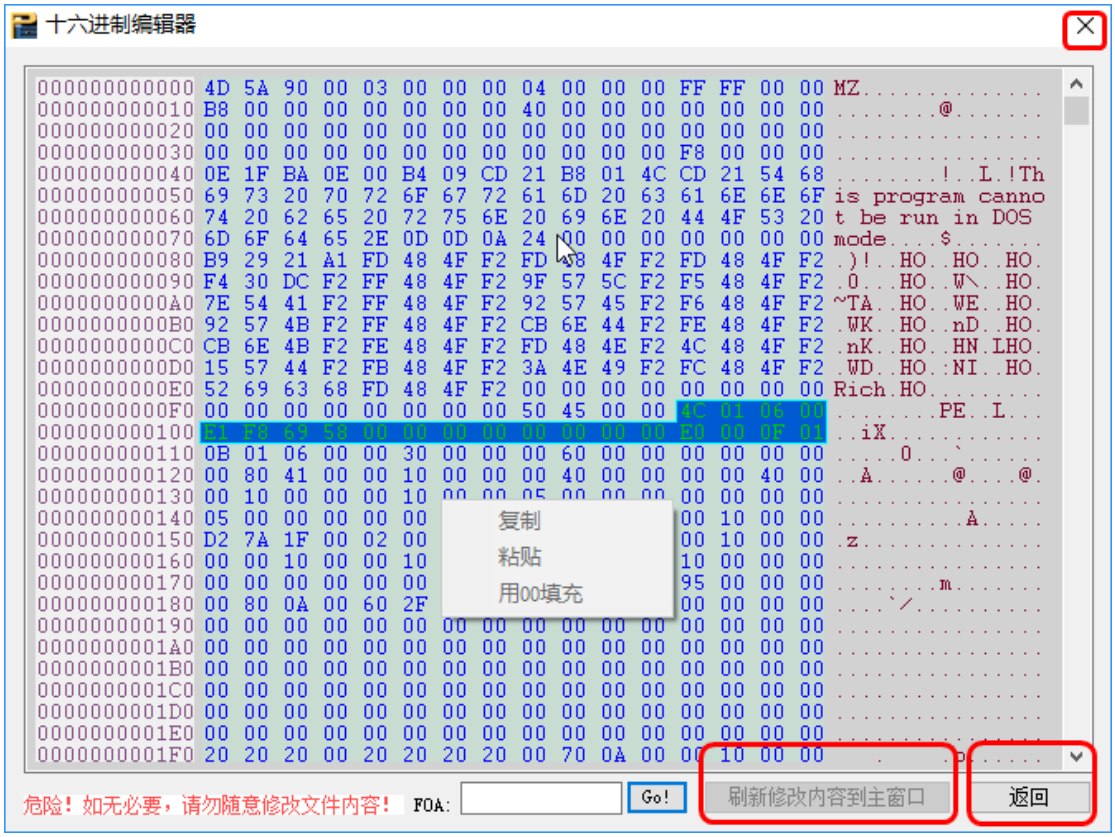


【其他功能】

除了以上功能以外，本软件还集成了以下相关功能。

十六进制编辑窗口

如上所述，十六进制编辑窗口是本软件不可分割的一部分。通常情况下它以磁性窗口的形势吸附在主窗口右侧，当然你也可以移动它让它吸附到主窗口的其他部位或者直接放在一边。你可以从菜单【选项】--【参数设置】--永久设置【安全使用十六进制编辑窗口】，也可以通过菜单【选项】--【安全使用十六进制编辑窗口】临时设置十六进制是否可以编辑。当你在十六进制窗口编辑完成后，请务必记得点击【刷新修改内容到主窗口】或者点击【X】按钮或者【返回】按钮以应用你的修改，否则你的修改将被抛弃。当你修改了十六进制窗口的数据，【刷新修改内容到主窗口】将变得可用。



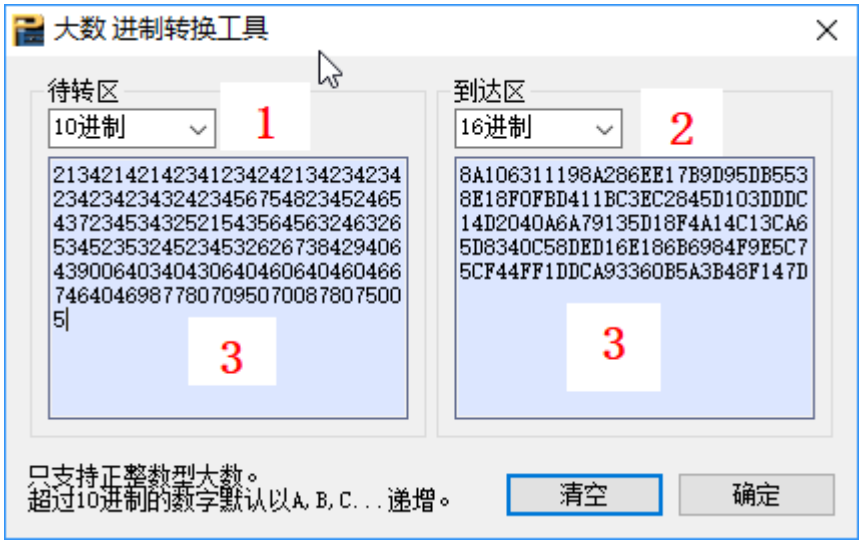
大数进制转换功能

工具位置：菜单- 【杂项】 - 【大数进制转换器...】

通常情况下你用不到这个工具。然而当你发现程序中给出了一个大数，比如 Sha256 计算或者 PE 文件中有这样的数据时，或许你需要知道这个数究竟是多少。

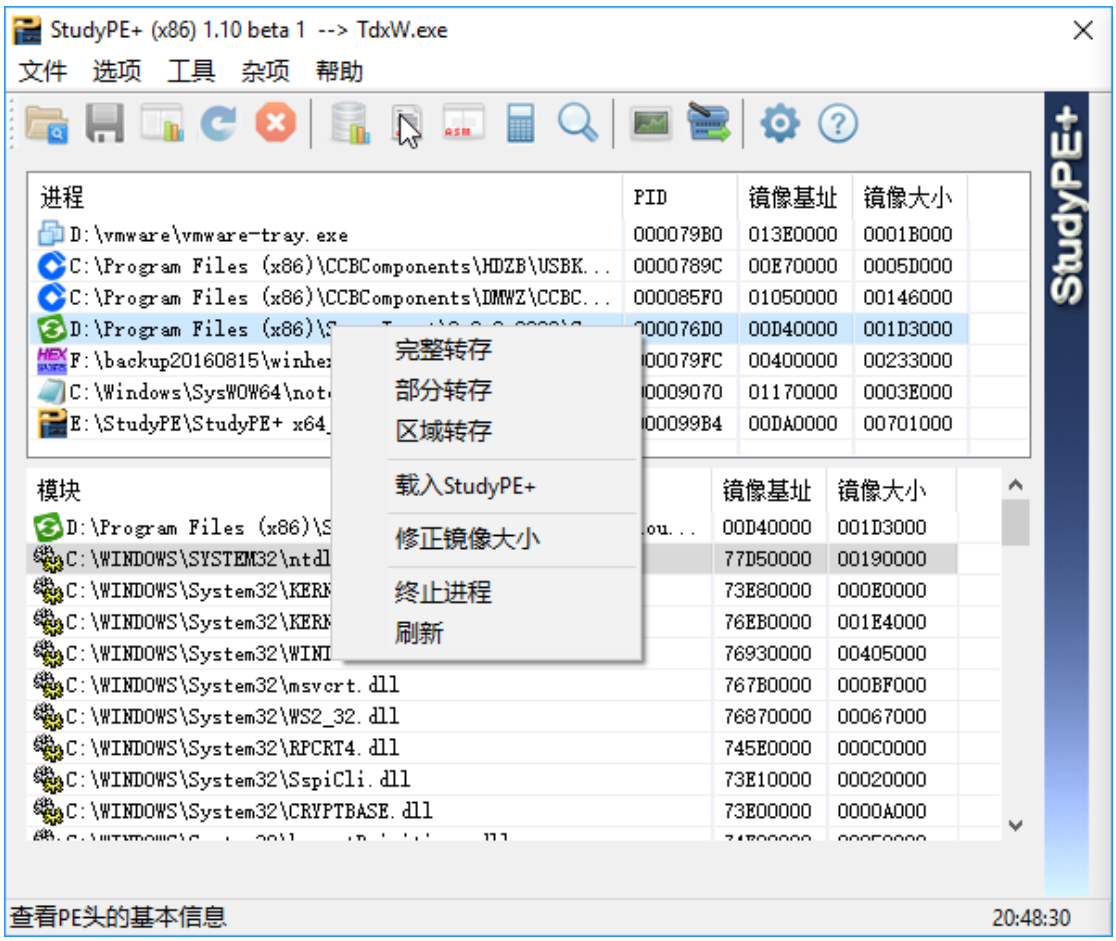
本工具支持 2-32 位的进制转换。

它的使用方法极其简单，不再多说了。

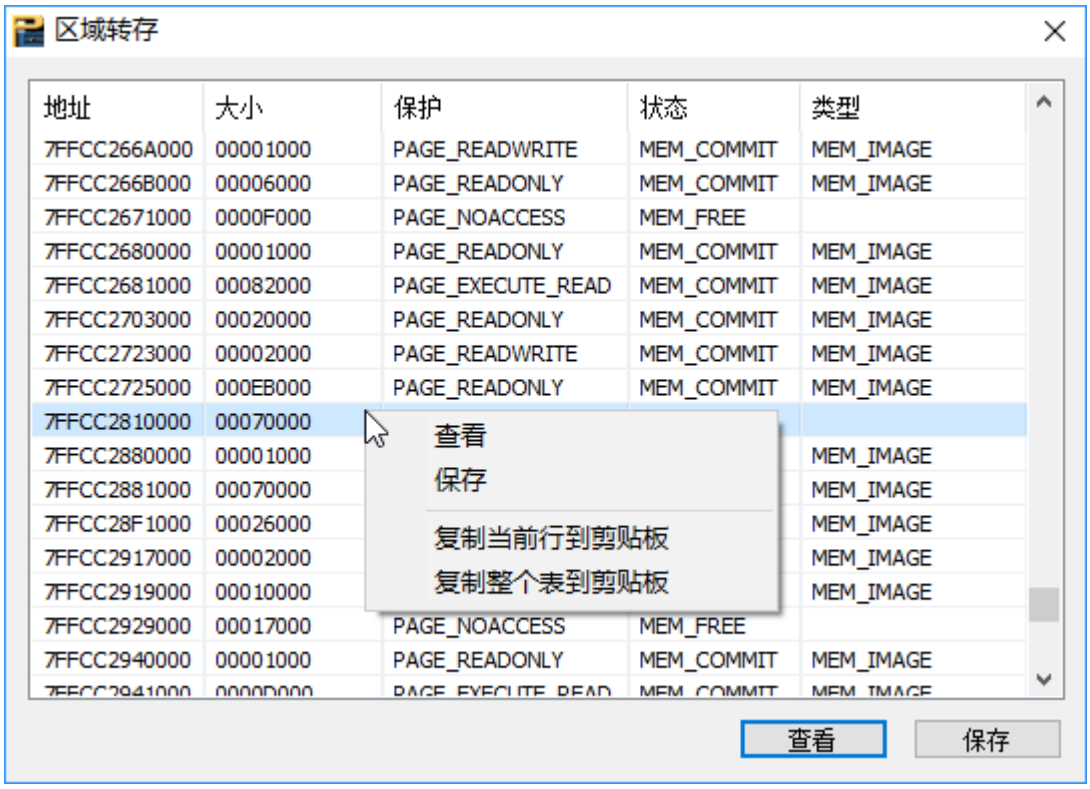


进程功能

本功能完美复制了 LordPE 的功能。众所周知，在 Win10 或者其他 x64 系统中 LordPE 不能很好的运行，本软件则毫无问题。此外，你也可以通过右键菜单直接把进程中的 PE 文件直接载入本软件进行分析。



象 LordPE 一样，你也可以转存相应的数据到文件。这里需要特别说明的是【区域转存】，你一样可以在十六进制窗口中查看或者转存所有可以看的区域。对于具有 PAGE_NOACCESS 属性的区段，很遗憾，我们没有权限查看。



【还没有说到的菜单项】

参数设置

工具位置：【选项】 - 【参数设置】

已经在前边说过了。其他几个选项都很直观，没有什么需要特别说明的。

输出文件信息

工具位置：【文件】 - 【输出文件信息】

你可以把 PE 文件的基本信息以文本文件的方式转存出来以便将来和其他信息对比。它将会弹出一个磁性窗口吸附在主窗口的右侧，跟其他磁性窗口一样，你一样可以随意拖动它。

最近打开的文件

工具位置：【文件】 - 菜单栏最下边的 5 项菜单。这是你曾经查看过的文件，你可以更加方便的再次打开这些文件进行分析。

【附加说明】

务必联系我

StudyPE 完善 QQ 群 790980160

Facebook group: https://www.facebook.com/groups/385475628805532/

我的邮箱：zaas2015@163.com

如果你发现了软件的 bug，请大家在反馈 bug 的时候，请一并把有问题的文件和问题描述 txt 打包上传至群共享或发至我的有限。感谢大家的反馈和对 StudyPe 的支持。

版权信息

参考资料

PE 权威指南
加密与解密 3
OllyDbg
Google
Butterinsect
Oleg Bykov
Ch.Kuendig
CxImage
M.o.D. and yoda
BeaEngine
lordPE
github.com
www.codeproject.com
www.csdn.com
www.chinaPYG.com
bbs.Pediy.com
Guilfanov
Pezcode
A.S.L

Keystone

感谢名单

感谢以上参考资料涉及到的人员
以及编程指导：
Nisy
Knuth 学徒
Komany
以及以下测试人员：
Csjwaman
Cwz
cxj98
bambooqj
Taoist/ka
Wan
small-Q
沉默是金
Cwx
以及
StudyPE 完善群的全体成员