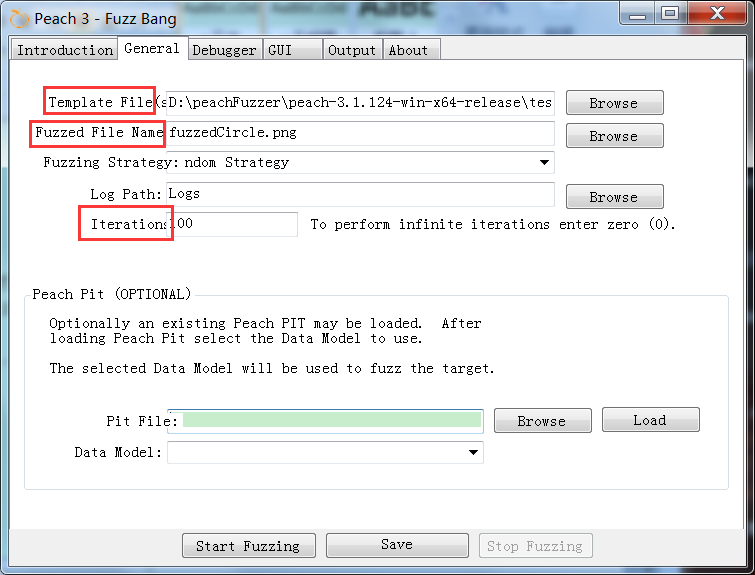
2018/10.1~10.7

关于PIT文件和V2、V3对比可以参照

D:\peachFuzzer\peach-3.1.124-win-x64-release\fuzz\_png\_test.xml

这个文档放GUI的过程：



Gereral：

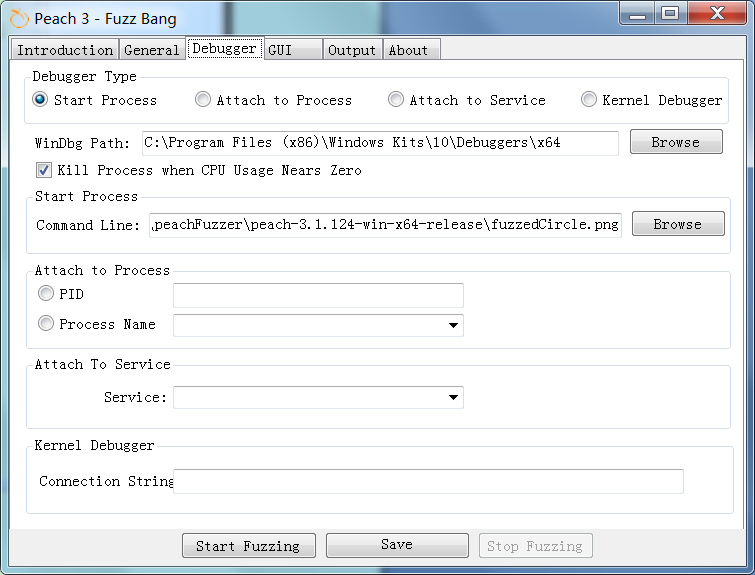
Fuzzed File name要和Debugger.Start Process 第二个参数名字一致

例如：我早General的Fuzzed File Name写为fuzzedCircle.png，那么我在Debugger.Start Process.Command Line里就要写

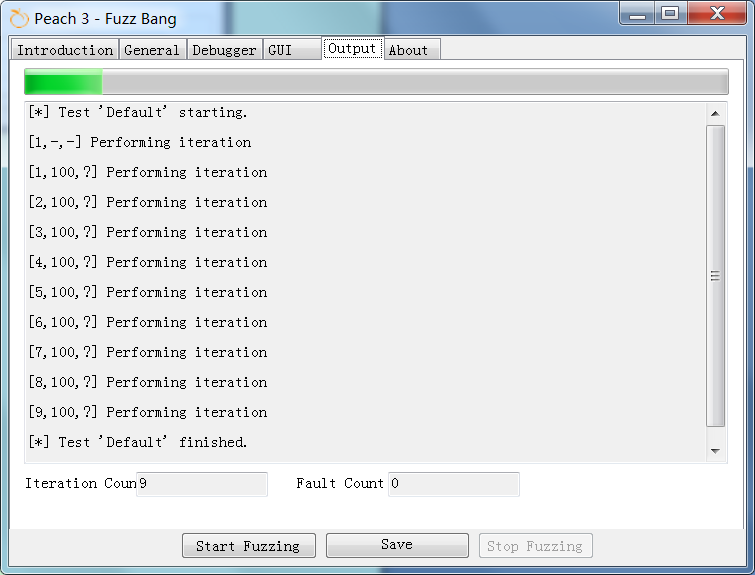
C:\Program Files (x86)\2345Soft\2345Pic\2345PicViewer.exe （空格）

D:\peachFuzzer\peach-3.1.124-win-x64-release\fuzzedCircle.png（因为我这里是以2345viewer为例，所以目标程序就以他为例）

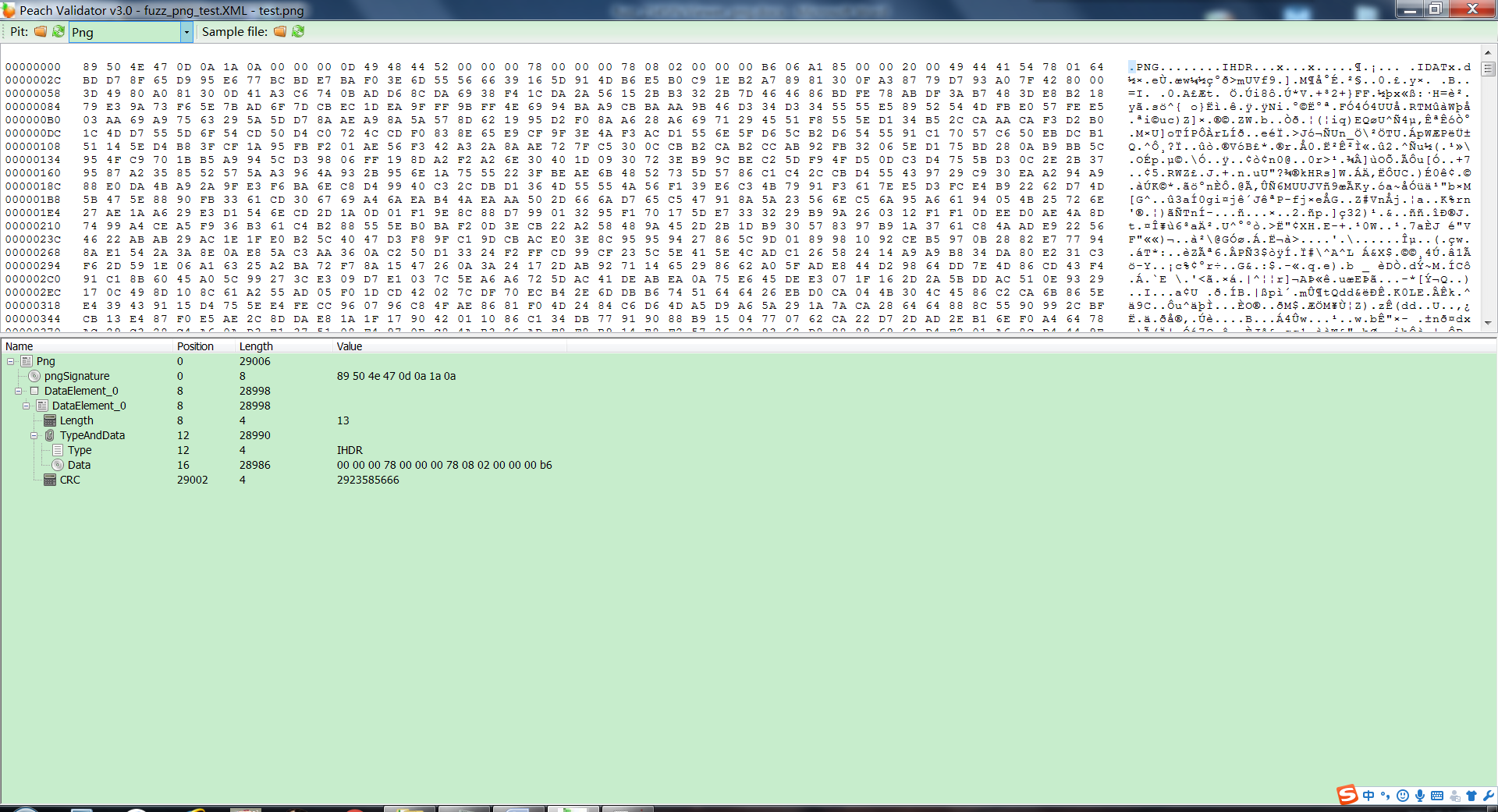
这块的PIT文件竟然是可选的？这里我有点奇怪？难道Peach 3已经能自动根据文件生成pit文件了吗？



运行实例：



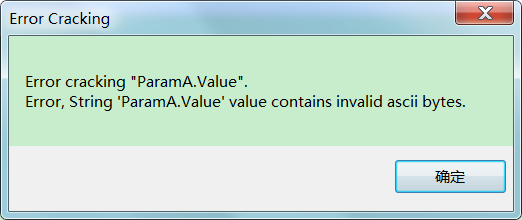
然后是Peach Validator

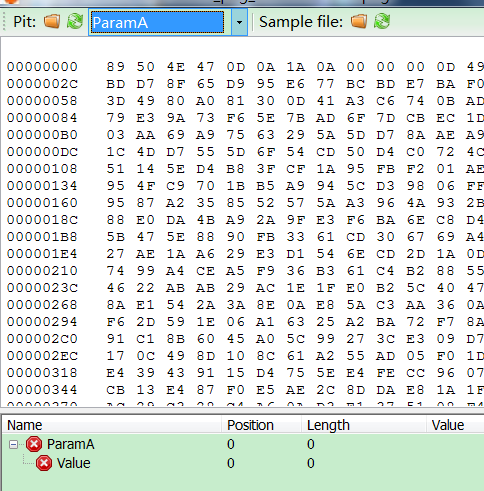




一个自己写的pit文件，和一个sample 文件，

我调试了一下我写的png.xml，发现好像还是名为ParamA的datamodel的问题。（待解决）





附：

GUI的参数(到时候直接复制进去就可以了)

general：

D:\peachFuzzer\peach-3.1.124-win-x64-release\test.png

fuzzedCircle.png

Debugger:

C:\Program Files (x86)\Windows Kits\10\Debuggers\x64

C:\Program Files (x86)\2345Soft\2345Pic\2345PicViewer.exe D:\peachFuzzer\peach-3.1.124-win-x64-release\fuzzedCircle.png