

软件简介

大蒜 1.3 版本说明:

- 1.解决了 104 结构解析的 bug。
- 2.强化了 201 结构的解析。
- 3.增加了 105,106 结构的解析。
- 4.修改了核心引擎，分析更快。
- 5.增加了版权限制

软件新增功能还不稳定，很在乎的不要考虑。

白皮蒜下载地址：<http://www.asm64.com/IFFA/IFFA1.3.zip>

大蒜 1.3 软件简介

说明	大蒜 1.3 版本说明：1. 解决了 104 结构解析的 bug。2. 强化了 201 结构的解析。3 增加了 105, 106 结构的解析。4 修改了核心引擎，分析更快。			
软件属于光刃个人所有，未经光刃授权使用软件均属于违法行为!!! 本人保留追究法律责任的权力!	版本	白皮蒜	紫皮蒜	独头蒜
	文件格式	是	是	是
	网络协议	是	是	是
	自动分析	是	是	是
	交互式分析	是	是	是
	命令修改属性	是	是	是
	深入自动分析	否	是	是
	文件大小限制	1KB	2KB	4KB
(授权限该版本，时效 3 个月，过期主动删除。升级后无效。如授权后 7 天内产品升级，可申请新版本)	授权方式 1	免费	1. 转发朋友圈获得 10 个赞。 2. 转发 100 人技术群 1 次。 【满足其一】	1. 转发朋友圈获得 10 个赞。 2. 转发 100 人技术群 1 次。 3. 写一篇使用申请书，包括对软件的看法，不得少于 200 字。 【同时满足】
	授权方式 2		提出有效 bug 或者有效建议等对产品发展有帮助的信息的。酌情授权紫皮蒜版或者独头蒜版。	
	授权方式 3		原创使用文档并发布（请在满足相应法律法规前提下发布，违规信息由提交者自己承担）（根据质量确定紫皮蒜版本或者白皮蒜版本）	

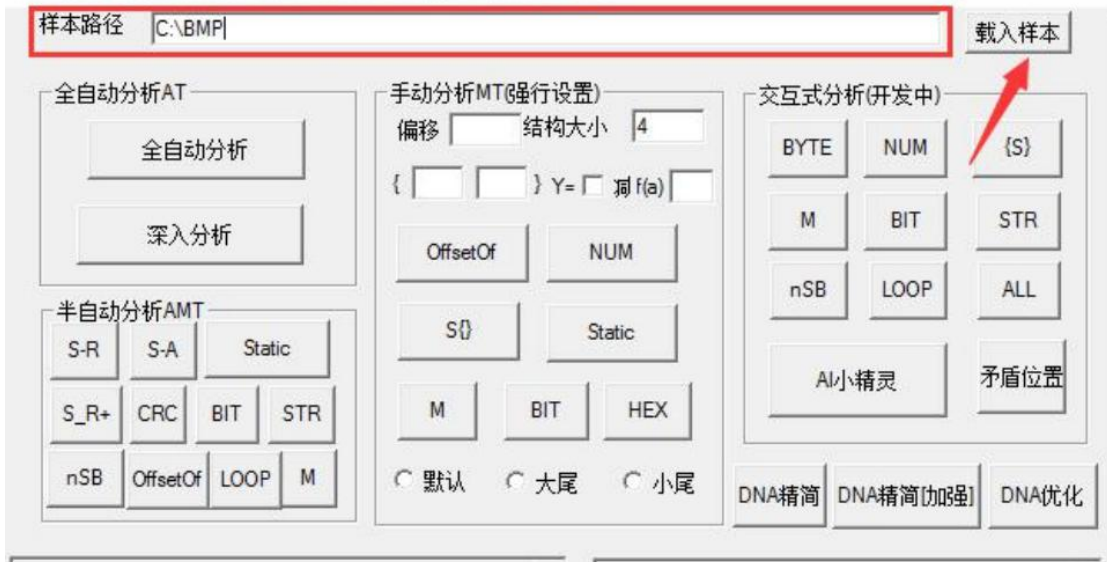
使用简介

下面用一个例子来演示大蒜

样本为画图板生成的 32*16 的图片，3 种不同颜色。（该例子白皮蒜无权测试，需要使用紫皮蒜和独头蒜方可）

1 启动软件，输入样本路径。点击载入

大蒜 (交互式样本分析系统) by 光刃 www.asm64.com/IFFA



2 选择全自动分析。

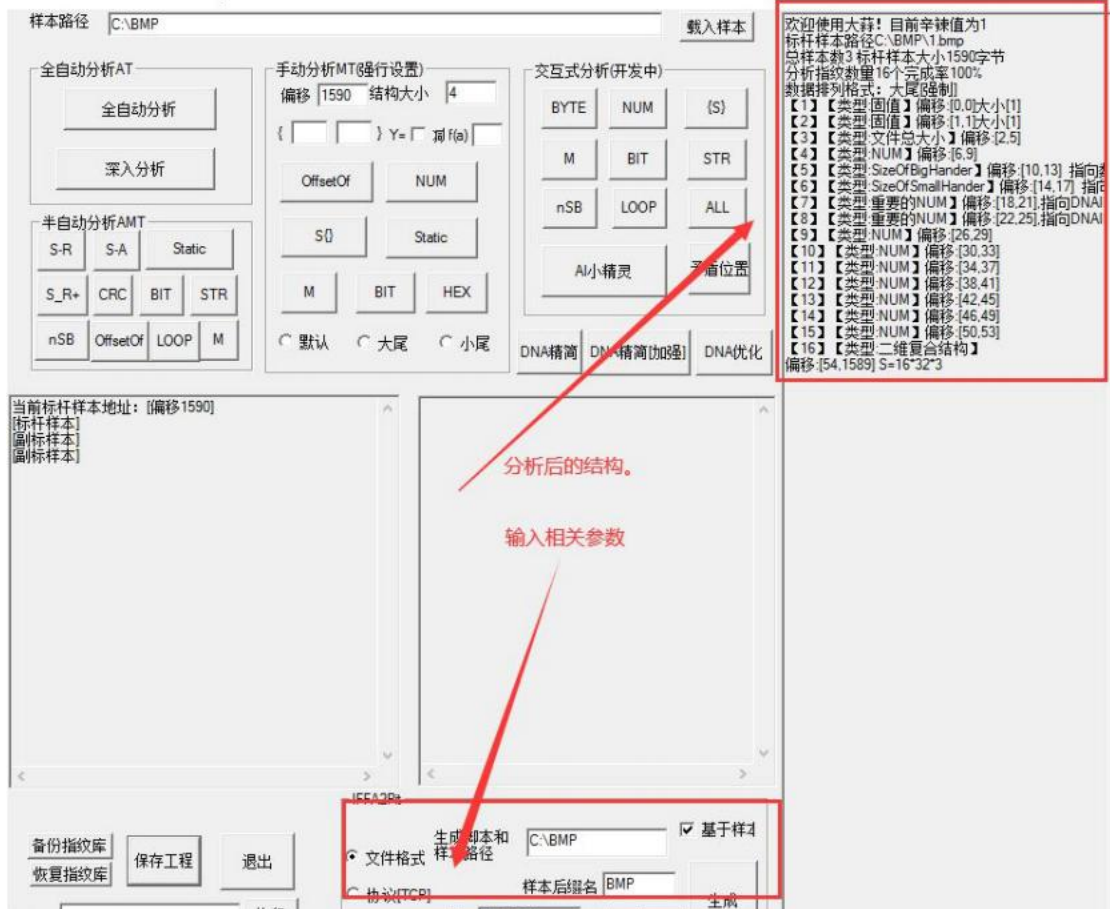
大蒜 (交互式样本分析系统) by 光刃 www.asm64.com/IFFA



3 完成分析后，选择深入分析(白皮蒜无该使用权)。



4 深入分析后, 按照格式输出 pit.



5 生成的 pit 脚本如下

```
<?xml version="1.0" encoding="utf-8"?><Peach xmlns="http://peachfuzzer.com/2012/Peach"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://peachfuzzer.com/2012/Peach ../peach.xsd">
<DataModel name="IFFA_data">
<!--write by IFFA..www.asm64.com QQ 群: 539069279 关注微信公众号 IFFA64 获取最新信息。 -->
<!--Create time 2021-10-5 14:7-->
<Block name = "1">
<Blob valueType = "hex" token="true" mutable="false" length = "1" value = "42 " />
<Blob valueType = "hex" token="true" mutable="false" length = "1" value = "4D " />
<Number
size = "32" mutable="false">
<Relation type = "size" of = "IFFA_data"
/>
</Number>
<Number size="32" />
<Number
mutable="false" size="32" >
<Relation type="size" of="1" />
</Number><Block name = "2">
<Number
mutable="false" size="32" >
<Relation type="size" of="2" />
</Number>
<Number mutable="false" size="32" >
<Relation type="size" of="X54" />
</Number>
<Number mutable="false" size="32" >
<Relation type="size" of="Y54" />
</Number>
<Number size="32" />
<Number size="32" />
<Number size="32" />
<Number size="32" />
<Number size="32" />
<Number size="32" />
<Number size="32" />
<Number size="32" />
</Block>
</Block>
<Block name="X54" minOccurs="1" maxOccurs="16" >
<Block name="Y54" minOccurs="1" maxOccurs="32" >
<Blob valueType="hex" length="3"
/>
</Block>
</Block>
</DataModel>
```

```

<StateModel name="State" initialState="State1">
<State name="State1">
<Action type="output">
<DataModel ref="IFFA_data"/>
<Data fileName="C:\BMP\1.bmp" /></Action>
</State>
</StateModel>
<Test name="Default">
<StateModel ref="State"/>
<Publisher class="FilePerIteration">
<Param name="FileName" value="C:\BMP\{0}.BMP"/>
</Publisher>
</Test>
</Peach>

```

[1014,-,-] Performing iteration	3. bmp	30. BMP	57. BMP
[*] Fuzzing: IFFA_data.X54.X54_1.Y54.Y54_2.DataElement	4. BMP	31. BMP	58. BMP
[*] Mutator: DataElementDuplicateMutator	5. BMP	32. BMP	59. BMP
[*] Fuzzing: IFFA_data.1.2.DataElement_11	6. BMP	33. BMP	60. BMP
[*] Mutator: NumericalVarianceMutator	7. BMP	34. BMP	61. BMP
	8. BMP	35. BMP	62. BMP
[1015,-,-] Performing iteration	9. BMP	36. BMP	63. BMP
[*] Fuzzing: IFFA_data.X54	10. BMP	37. BMP	64. BMP
[*] Mutator: DataElementDuplicateMutator	11. BMP	38. BMP	65. BMP
[*] Fuzzing: IFFA_data.X54.X54_1	12. BMP	39. BMP	66. BMP
[*] Mutator: DataElementRemoveMutator	13. BMP	40. BMP	67. BMP
	14. BMP	41. BMP	68. BMP
[1016,-,-] Performing iteration	15. BMP	42. BMP	69. BMP
[*] Fuzzing: IFFA_data.X54.X54.Y54.Y54_3	16. BMP	43. BMP	70. BMP
[*] Mutator: DataElementDuplicateMutator	17. BMP	44. BMP	71. BMP
[*] Fuzzing: IFFA_data.X54.X54.Y54	18. BMP	45. BMP	72. BMP
[*] Mutator: DataElementRemoveMutator	19. BMP	46. BMP	73. BMP
[*] Fuzzing: IFFA_data.X54.X54_1.Y54.Y54_4	20. BMP	47. BMP	74. BMP
[*] Mutator: DataElementRemoveMutator	21. BMP	48. BMP	75. BMP
[*] Fuzzing: IFFA_data.1.2.DataElement_10	22. BMP	49. BMP	76. BMP
[*] Mutator: DataElementRemoveMutator	23. BMP	50. BMP	77. BMP
[*] Fuzzing: IFFA_data.X54.X54_1.Y54.Y54.DataElement			
[*] Mutator: BlobBitFlipperMutator			