MPLabX 中 PIC18 的反汇编器或反编译器?

页: < 1 2 3 > • 显示第 2 页，共 3 页

作者 Essentials Only 完整版 邮政

伏洛基

回复: MPLabX 中 PIC18 的反汇编器或反编译器? • 2015 年 5 月 14 日星期四 4:00 AM （固定链接）

乔，唉!

★★★★★

帖子总数: 6815

奖励积分: 0

加入时间: 2007 年 10 月 15 日

地点: 德国

状态: 离线

> 行地址操作码 *DisAssy 1*
> *00000 6A00 CLRF 0x0, ACCESS* 这是复位向量
> *2 00002 EF4F GOTO 0x49E* 转到主、初始化或启动?
> ~~*3 00004 F002 NOP*~~ 第二个字 *for goto*
> ~~*4 00006 FFFF NOP*~~ 只是一个未编程的字
> *5 00008 EF34 GOTO 0x1E468* 中断向量
> ~~*6 0000A F0F2 NOP*~~ 第二个字 *for goto*
> ...

+2 (2)

您的原始代码是用 C 语言还是汇编语言编写的?
如果组装，绝对或可重定位?

无论如何，如果你想以可重定位的方式"反汇编"代码，它看起来像这个

```
RESET_VECTOR 代码 0x0000
        CLRF 0x0, ACCESS 这是重置向量
        GOTO 0x49E goto main, init 或 startup ?
INTERRUPT_VECTOR 代码 0x0008
        GOTO 0x1E468            中断向量
...
```

乌巴斯!

#21

克罗斯兰

回复: MPLabX 中 PIC18 的反汇编器或反编译器? • 2015 年 5 月 14 日星期四 4:06 AM （永久链接）

> 伏洛基
>
> 行地址操作码 *DisAssy 1*
> *00000 6A00 CLRF 0x0, ACCESS* 这是复位向量

+1 (1)

超级会员

总帖子数：2831

奖励积分：0

加入时间：2005 年 5 月 11 日

地点：英国沃克斯

状态：离线

> *2 00002 EF4F GOTO 0x49E* 转到主、初始化或启动?
> ~~*3 00004 F002 NOP*~~ 第二个字 *for goto*
> ~~*4 00006 FFFF NOP*~~ 只是一个未编程的字
> *5 00008 EF34 GOTO 0x1E468* 中断向量
> ~~*6 0000A F0F2 NOP*~~ 第二个字 *for goto*
> ...

你没有帮助 ypurself :)

地址 6 的第二个 NOP 是真实的，将向量放在地址 8 是必要的填充。

#22

伏洛基

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 4:11 （固定链接）

我会说向量放在 0x0008 处，因此 0x0006 只剩下 ffff
最后它是相同的 ;-)

+2 (2)

乌巴斯!

乔，唉!

帖子总数：6815

奖励积分：0

加入时间：2007 年 10 月 15 日

地点：德国

状态：离线

#23

达里奥

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 4:49 （永久链接）

OP 想要一个显示 GOTO 和 CALL 以及单个助记符的反汇编程序。
有人请写这样的东西，我们就完成了 （不关心关于跳过等的 Microchip 细节.....）

+3 (3)

热那亚 :D :D ！ 去做

Allmächtig。

帖子总数：54081

奖励积分：0

加入时间：2006 年 2 月 25 日

地点：Oesterreich

状态：离线

#24

伏洛基

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 5:13 （固定链接）

乔，唉！

★★★★★

帖子总数：6815

奖励积分：0

加入时间：2007 年 10 月 15 日

地点：德国

状态：离线

> 达里奥
>
> *OP* 想要一个显示 *GOTO* 和 *CALL* 以及单个助记符的反汇编程序。
> 有人请写这样的东西，我们就完成了（不关心关于跳过等的 *Microchip* 细节……）

+1 (3)

猜猜我们可以做到——但它有什么用呢？

如果您知道该程序的作用，则最好将其编写为新的；-)

乌巴斯！

#25

库兹曼

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 5:25 （固定链接）

网络上的一个人

★★★★★

总帖子数：19924

奖励积分：0

加入时间：2008 年 1 月 17 日

地点：0

状态：在线

+4 (4)

如果您知道该程序的作用，则最好将其编写为新的；-)

我想这就是问题所在。他们不知道它做了什么。
并希望守则能提供一些答案。

#26

达里奥

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 5:55 （固定链接）

Allmächtig。

★★★★★

帖子总数：54081

奖励积分：0

加入时间：2006 年 2 月 25 日

地点：Oesterreich

状态：离线

0

热那亚 :D :D ！ 去做

#27

蒂梅克

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 7:15 （固定链接）

超级会员

★★★★★

总帖子数：1216

奖励积分：0

加入时间：2007 年 11 月 26 日

地点：台湾

状态：离线

+2 (2)

我编写了一个简单的 C# 程序来自动为 PIC18 和 PIC24 的调用和跳转添加标签。用户可以在查看汇编代码后创建地址-标签映射表，使标签更有意义。

至于NOP，可能不是什么大问题，因为我们已经知道了，然后我们可以处理它……

我的程序只是为了帮助我更好地理解汇编代码的流程，所以现在还没有准备好发送用于编译的解释代码，但无论如何都可以完成。

如果您的 HEX 不是专有的，您可以在此处发布。我可以尝试得到一些初步的结果。或者您可以发布部分 HEX 进行一些测试。如果测试没问题，我不介意在这里发布我的代码。所以以后可以自己DIY。

++ 顺便说一句，你可以看看下面的线程，这就是我为 PIC24

http://www.microchip.com/forums/m861426.aspx所做的

帖子由 timijk 编辑 - 2015 年 5 月 14 日星期四上午 7:33

#28

里克

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四上午 7:38 （固定链接）

超级会员

★★★★★

总帖子数：35294

奖励积分：0

加入时间：2003 年 11 月 8 日

地点：澳大利亚，墨尔本

状态：离线

+2 (2)

有几个人在这里非常血腥。
OP已经明确表示他想将十六进制代码反汇编成可以重新组装的汇编源代码。
MPLAB 反汇编程序不适合这种情况，特别是因为它在两个字节的 PIC18 GOTO/CALL 指令中显示了嵌入式 NOP。它实际上只是作为调试辅助工具。
虽然我同意尝试对十六进制文件进行逆向工程，特别是如果它是优化编译器的输出，将是一项非常艰巨的任务，但当他明白指令集时告诉他阅读数据表并没有帮助。

我还在：PicForum上发帖

要获得有用的答案，请始终说明您使用的是哪个 PIC!

#29

伏洛基

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 7:39 （固定链接）

乔，唉!

★★★★★

帖子总数：6815

奖励积分：0

加入时间：2007 年 10 月 15 日

地点：德国

+2 (2)

> 多名意志
>
> 我意识到我可以编写自己的反汇编程序，但如果已经存在的话，我会尽量避免花费时间和精力。或者，如果有人可以引导我使用可在 *PIC18F* 上运行的廉价（免费也很好）反编译器（即生成 *C* 代码），那将是非常棒的。搜索互联网并没有产生任何结果，我觉得在工作计算机上下载和执行是安全的。

…产生C代码大声笑：

他不觉得节省眨眼：

状态：离线

问：**谁**需要这样的工具？
（（（（这是要求的正确地方吗？））））

乌巴斯！

#30

多名意志

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 7:52 （固定链接）

新成员

帐子总数：10
奖励积分：0
加入时间：2015 年 5 月 14 日
地点：0
状态：离线

> 克罗斯兰
>
> *PIC* 架构最初是每个字一个指令。为了增加额外的功能，*Microchip* 创建了需要第二个字的新指令字，例如 *GOTO*。第二个词，孤立地理解<...>

0

我并不是说 GOTO 需要两个词。然而，显然这个线程中没有其他人知道"真正的"反汇编程序的工作是什么。它的工作是生成一个汇编列表，当通过汇编器时将生成与最初给出的相同的二进制文件（或在本例中为 Intel Hex 格式的文件）。在你大发雷霆并告诉我我不知道我在说什么之前，我的几个硕士项目正在构建其中的几个，更不用说我与其他几个项目（非PIC）一起工作了作为我工作的一部分，我每天都在做建筑。所以我知道它们存在，我知道"真实"世界理解并同意我的定义。我再说一遍：f(g(x)) -> x

我有点惊讶和难过，我的第一次尝试并没有在这个董事会上找到同事之间的明智讨论，而是无知、任性和懒惰。为什么人们觉得有必要假装他们知道某事并大声说出来，而不是在他们对讨论没有任何有用的贡献时继续前进？

对于将来遇到此线程的任何人，我正在编写自己的（实际上此时已接近完成），如果我能说服我的工作让我分享它，我将在此处发布链接或其他内容.

-将要

#31

里克

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 8:01 （固定链接）

超级会员

总帖子数：35294
奖励积分：0
加入时间：2003 年 11 月 8 日
地点：澳大利亚，墨尔本
状态：离线

没有人？
我想你会在这个主题的第二页上找到至少两个理解的人。:)

+3 (3)

我还在：PicForum上发帖
要获得有用的答案，请始终说明您使用的是哪个 PIC！

#32

多名意志

新成员

帖子总数：10

奖励积分：0

加入时间：2015 年 5 月 14 日

地点：0

状态：离线

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 8:18 （永久链接）

0

我向 ric 和第 2 页上真正理解的其他人道歉，由于某种原因，我错过了第二页的大部分讨论（没有电子邮件通知和在树形视图中阅读，现在已修复）。

对于好奇的人，我将逆向工程作为我日常工作的一部分（有时作为一种爱好；我知道，很奇怪）。当您拥有的只是二进制/英特尔 Hex 文件时，有许多合法（以及一些非法/非法）的理由进行逆向工程。有时是为了进行安全审计，有时是因为您认为工具链中可能存在错误（有时确实会发生），有时是为了了解它打算在其上运行的硬件，有时是在这种情况下，分包商或其他遗留编码器将一堆热气腾腾的无证位倾倒在您的腿上，然后立即走开，离开管理层，决定让您“更好”地弄清楚他们做了什么，而不是试图强迫原作者制作文档/源代码。长话短说，A公司确实为B公司工作，B公司认为他们做得很差，A公司拒绝提供来源/文件。所以 B 公司去找 C 公司（我）并要求他们重新审视 A 公司做了什么（因为 B 公司拥有它并且可以合法地这样做），我跳上论坛并开始了一场激烈的战争。:)

最后一个可能发生的原因有很多，而且它发生的频率比你想象的要频繁得多。事实上，我现在正在进行两个半项目，这正是这种情况……但是，嘿，有报酬的工作等等。

哦，我知道反编译器（例如 C 代码）很少见，好的反编译器更罕见，但它们确实存在于某些体系结构中，因此认为它们可以存在于 PIC18 中并不难。哎呀，在 1999 年到 2005 年之间，我不相信 PIC 上有一个好的 C 编译器，但是目前的收成变得好多了。

帖子由 WillOfManyNames 编辑 - 2015 年 5 月 14 日星期四晚上 8:21

#33

克罗斯兰

超级会员

总帖子数：2831

奖励积分：0

加入时间：2005 年 5 月 11 日

地点：英国沃克斯

状态：离线

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 9:00 （固定链接）

+3 (3)

> 多名意志
>
> 然而，显然这个线程中没有其他人知道“真正的”反汇编程序的工作是什么。它的工作是生成一个汇编列表，当通过汇编器时将生成与最初给出的相同的二进制文件（或在本例中为 *Intel Hex* 格式的文件）。

谁说的?

在您提供权威参考之前，我更喜欢维基百科的定义“反汇编，反汇编程序的输出，通常被格式化为人类可读性，而不是适合输入到汇编程序”。

#34

吉姆尼克森

用户 452

总帖子：7172

奖励积分：0

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 9:24 （固定链接）

+1 (1)

根据我的经验，大多数使用嵌入式处理器的系统都有可以记录/测量的输入和输出。
对输入进行明确定义的更改会导致输出发生更改。
我经常发现，当我看到一个没有源代码/文档的新系统时，为现有处理器编写新代码或替换它会更快。

加入时间：2003 年 11 月 8 日

地点：加利福尼亚州圣地亚哥

状态：离线

Jim.Nickerson

擅长使用 Microchip 产品进行设计。点击此处访问 Microchip Technology 网站了解更多信息

#35

1和0

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 9:52 （固定链接）

+2 (2)

访问被拒绝

帖子总数：15304

奖励积分：0

加入时间：2007 年 5 月 7 日

地点：哈利的灰质

状态：离线

正如我在第 1 页的帖子 #15中所说：

> 1和0
>
> 是的，如果你想创建一个汇编源代码，你必须去掉双字指令的 *NOP*。“反汇编列表”用于调试，例如单步等；它并不是要创建汇编源代码。
>
> 在我之前发布的那个线程中有一个名为“*unPIC*”的反汇编工具的链接。*<edit>* *http://www.microchip.com/.../FindPost/611989* 但我认为它适用于 *PIC16* 设备。*</edit>*
>
> *<edit>* 免责声明：我从来没有使用过那个“工具”，所以.....无论如何，我发现逆向工程时从头开始更容易。

PIC18 器件有四个双字指令（CALL、GOTO、LFSR 和 MOVFF），其中第二个字是 NOP。要从 MPLAB 的反汇编列表中生成可重新汇编的汇编源代码，您需要删除这些 NOP。编写一个脚本来按摩它，或者甚至 Excel 可以处理它。要获得可修改的源，所有 BRA、CALL、GOTO 和 RCALL 目标都需要转换为命名标签。然后您将需要添加，例如：

```
列表 p = 18f2520 #include < p18f2520 。公司> ; 在此处插入配置位；在此处插入用户 ID ；在此处插
```

无论如何，“反编译”成诸如 C 之类的高级语言将是一项非常艰巨的任务。虽然这并非不可能，但我认为 C 反编译器生成的 C 代码很少有用。您需要了解用于生成 hex 文件的 C 编译器的内部细节。每个 C 编译器以及可能的每个版本都有一组不同的优化并生成不同样式的操作码。此外，正如前面提到的，在程序内存中存在可以解释为代码的字符串或数据表会使反编译器感到困惑——更不用说由编译器错误生成的代码了。

> “问题在于，通过优化编译器，编译器的
> 给定输出具有无限（或大约；）数量的
> 可能源程序。事实是，反编译器可以生成
> 完全有效的 *C* 代码，这对正常来说几乎没有任何意义人类。”

#36

克罗斯兰

超级会员

★★★★★

总帖子数：2831

奖励积分：0

加入时间：2005 年 5 月 11 日

地点：英国沃克斯

状态：离线

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 10:02 （固定链接）

> 1和0
>
> "事实是，反编译器可以生成完全有效的 *C* 代码，这对普通人来说几乎没有任何意义。"

+5 (5)

谁需要反编译器来做到这一点:)

#37

1和0

访问被拒绝

★★★★★

帖子总数：15304

奖励积分：0

加入时间：2007 年 5 月 7 日

地点：哈利的灰质

状态：离线

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 10:17 （永久链接）

> 克罗斯兰
>
> 谁需要反编译器来做到这一点*:)*

+3 (3)

也许……国际混淆 C 代码竞赛格林先生：

#38

北盖

超级会员

★★★★★

总帖子数：7337

奖励积分：0

加入时间：2014 年 2 月 24 日

地点：加拿大北部

状态：离线

回复：MPLabX 中 PIC18 的反汇编器或反编译器？ • 2015 年 5 月 14 日星期四晚上 10:31 （固定链接）

+3 (3)

在 PIC16/18 上，变量位于存储库中，反汇编程序很难找出您正在访问的存储库。因此，即使是可重新编译的反汇编代码，使用它也可能不是那么容易。

A公司设计了算法（所以这对他们来说不是秘密）。B 公司写了一个糟糕的代码（毫无价值）。现在，A 公司在试图反汇编这个毫无价值的代码时投入了大量资金。他们聘请 C 公司来做这件事。公司 C 可以建议公司 A 为已知算法编写好的代码比修改现有的坏代码更便宜和更好，即使源存在，更不用说需要反汇编了。

北方软件公司

#39

1和0

回复：MPLabX 中 PIC18 的反汇编器或反编译器? • 2015 年 5 月 14 日星期四晚上 10:46 （固定链接）

访问被拒绝

★★★★★

帖子总数：15304

奖励积分：0

加入时间：2007 年 5 月 7 日

地点：哈利的灰质

状态：离线

> 北盖
>
> …即使源代码存在，为已知算法编写好的代码也比修改现有的坏代码更便宜和更好，更不用说需要反汇编了。

+3 (3)

去过那里……并且在更短的时间内完成了它。咧嘴一笑：

#40

页： < 1 2 3 > • 显示第 2 页，共 3 页

主页 » 所有论坛 » [开发工具] » MPLAB X IDE » MPLabX 中 PIC18 的反汇编器或反编译器?

跳转到： 跳到

最新的帖子

无法测量频率；我只得到 25536 的输出
优化和数学库
警告：(751) 常量表达式中的算术溢出
提问 flash NOR 内存芯片
检测usart何时发送最后一个字节进行485...
READTIMER0() PIC18F26Q10
基于 PIC32MX2 的约 10 美元示波器和逻...
PIC32MK EEPROM 写操作
AT42QT1245 彻底死机
MCP794xx 库未出现

活跃帖子

无法测量频率；我只得到 25536 的输出
提问 flash NOR 内存芯片
READTIMER0() PIC18F26Q10
基于 PIC32MX2 的约 10 美元示波器和逻...
PIC32MK EEPROM 写操作
MCC 库安装
问题 RTCC MCP794xx mcc lib
[已修复] 将整个引导加载程序放入 RAM
MCC TCP/IP 精简版错误?
写入 PIC16F15345 存储区闪存不起作用

所有常见问题解答

为什么我的 PIC32 运行速度比预期慢?
国家发展委员会
MPLAB XC32 v4.10 发布

产品 应用 设计支持 训练 样品和购买 关于我们 联系我们 合法的 投资者 职业生涯