



^ 上一个主题

下一个主题 v

反编译 PIC

页: > • 显示第 1 页, 共 2 页

作者

Essentials Only

完整版

邮政 ^

元

2020 年 7 月 12 日星期日下午 6:06 (永久链接)



反编译 PIC

0

您好:

有没有用C#或者Java反编译PIC16F84A的源码?

问候。

高级会员



总帖子: 153

奖励积分: 0

加入时间: 2008 年 2 月 11 日

地点: 西班牙

状态: 离线

<http://electronica-pic.blogspot.com>中的电子 PIC

#1

21 条回复 • 相关主题

- PIC16是否兼容“Explorer 8开发板”
- 带有 PIC18F97J60 的 Picdem net 2 开发板
- PIC18LF25K50 的引导加载程序 - 起点
- 16F84 H桥电机控制
- pic/rf 的奇怪问题 - 坏 pic 系列?
- PIC18F97J60 源代码
- pic微控制器教程的完整列表
- 错误 [1109] 重新声明中的类型不匹配
- PIC PIC 可以 PIC 吗?

卡特拉

回复: 反编译一张图片 • 2020 年 7 月 12 日星期日晚上 9:26 (永久链接)



当你说反编译PIC时, 你到底是什么意思? PIC的免费开源编译器...?



-1 (1)

超级会员



面向爱好者和学生的免费在线微控制器教程和项目。从初学者到高级。网站: www.studentcompanion.co.za

YouTube 教程: <https://www.youtube.com/StudentCompanionSA>

总职位：2009

奖励积分：0

加入时间：2013 年 6 月 11 日

地点：南非

状态：离线

元



高级会员

★★★★★

总帖子：153

奖励积分：0

加入时间：2008 年 2 月 11 日

地点：西班牙

状态：离线

📄 回复：反编译一张图片 • 2020 年 7 月 12 日星期日晚上 9:58 （永久链接）

从 hex 文件到 asm 会发生什么。

+1 (1)

<http://electronica-pic.blogspot.com>中的电子 PIC

#3

库兹曼



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：离线

📄 回复：反编译一张图片 • 2020 年 7 月 12 日星期日晚上 10:02 （永久链接）

该软件通常被称为“反汇编程序”。

+3 (3)

#4

upand_at_them



超级会员

★★★★★

总帖子：915

📄 回复：反编译一张图片 • 2020 年 7 月 12 日星期日晚上 10:19 （固定链接）

十六进制 -> 程序集？ ...是的
十六进制 -> 其他什么？ ...否

+2 (2)

#5

奖励积分: 0

加入时间: 2005 年 5 月 16 日

地点: 宾夕法尼亚

状态: 离线

元



高级会员

★★★★★

总帖子: 153

奖励积分: 0

加入时间: 2008 年 2 月 11 日

地点: 西班牙

状态: 离线

回复: 反编译一张图片 • 2020 年 7 月 12 日 星期日晚上 10:19 (固定链接)

是的。

0

<http://electronica-pic.blogspot.com>中的电子 PIC

#6

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: 反编译一张图片 • 2020 年 7 月 12 日 星期日晚上 11:10 (永久链接)

在 MPLAB 中, 导入您的 hex 文件并查看程序存储器 (反汇编列表)。

+1 (1)

#7

元



高级会员

★★★★★

总帖子: 153

奖励积分: 0

回复: 反编译一张图片 • 2020 年 7 月 13 日, 星期一 1:08 AM (永久链接)

在 MPLAB 中我不喜欢它, 因为操作数用数字显示给你。例如:

0

0:	16 83	bsf 0x03, 5
1:	01 86	clrf 0x06
2:	30 1F	movlw 0x1F
3:	00 85	movwf 0x05
4:	12 83	bcf 0x03, 5
5:	10 06	bcf 0x06, 0

加入时间：2008 年 2 月 11 日

地点：西班牙

状态：离线

使用 Visual C# 我想将其编程为如下所示：

```
0:    16 83      bsf STATUS, RPO
1:    01 86      clrf TRISB
2:    30 1F      movlw 0x1F
3:    00 85      movwf TRISA
4:    12 83      bcf STATUS, RPO
5:    10 06      bcf PORTB, 0
```

你明白我想做什么吗？

谢谢。

<http://electronica-pic.blogspot.com>中的电子 PIC

#8

W4GNS。

回复：反编译一张图片 • 2020 年 7 月 13 日，星期一，凌晨 1:34 （固定链接）



茫然不知所措
★★★★★

帖子总数：75
奖励积分：0

加入时间：2009 年 11 月 17 日
状态：离线

<https://www.nsa.gov/resources/everyone/ghidra/>

👍👎

0

#9

北盖

回复：反编译一张图片 • 2020 年 7 月 13 日，星期一，凌晨 3:01 （固定链接）



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

“

你明白我想做什么吗？

”

元

👍👎

+1 (1)

这些符号取决于选择的银行，仅通过查看指令代码是无法分辨的。

[北方软件公司](#)

#10

元



高级会员
★★★★★
总帖子: 153
奖励积分: 0
加入时间: 2008 年 2 月 11 日
地点: 西班牙
状态: 离线

回复: 反编译一张图片 • 2020 年 7 月 13 日星期一凌晨 3:08

精确的。有个窍门。
程序会查看您所在的存储区。在这种情况下, PIC16F84A 只有两个存储区。

C# 必须读取该银行此时找到的次数, 然后应用相应的指令。


👍👎

0

<http://electronica-pic.blogspot.com>中的电子 PIC

#11

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: 反编译一张图片 • 2020 年 7 月 13 日星期一凌晨 3:33 (固定链接)

“
精确的。有个窍门。
程序会查看您所在的存储区。在这种情况下, PIC16F84A 只有两个存储区。

C# 必须读取该银行此时找到的次数, 然后应用相应的指令。
”

元

👍👎

+1 (1)

您将不得不编写一个“智能”反汇编程序, 这绝非易事!

#12

元



高级会员
★★★★★
总帖子: 153
奖励积分: 0
加入时间: 2008 年 2 月 11 日
地点: 西班牙
状态: 离线

回复: 反编译一张图片 • 2020 年 7 月 13 日星期一凌晨 3:58 (固定链接)

这不容易, 也不是不可能。编译器知道它编译了什么。反编译时你必须帮助他。

尝试按照以下步骤操作。

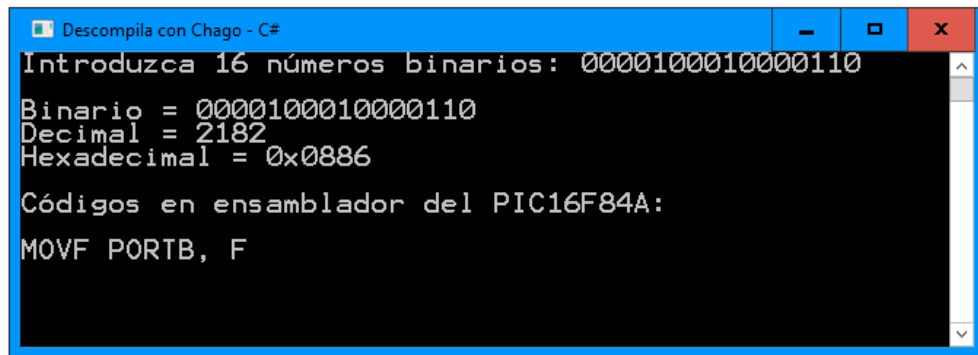
总之

👍👎

-1 (1)

```
MOVF PORTB , F  
  
MOVF H '0006' , H '0001'  
  
00001000 1 000 0110
```

FIGURA 7-1: FORMATO GENERAL DE INSTRUCCIONES



然后我把它改编成英语。

[下载](#)

;))

<http://electronica-pic.blogspot.com> 中的电子 PIC

#13

里克



超级会员



总帖子数: 35294

奖励积分: 0

加入时间: 2003 年 11 月 8 日

回复: 反编译一张图片 • 2020 年 7 月 13 日, 星期一 4:44 AM (永久链接)

你把它简化了。

您的反汇编程序必须完全模拟 PIC 的操作, 并执行整个程序, 跟踪库选择位的状态。您并不总是在内存访问之前的指令中立即包含银行选择代码, 它们可能在从其他地方的 GOTO 或 CALL 之前执行。



+5 (5)

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!

#14

地点: 澳大利亚, 墨尔本
状态: 离线

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: 反编译一张图片 • 2020 年 7 月 13 日星期一上午 5:14 (固定链接)

“

这不容易, 也不是不可能。

元

”



+2 (2)

银行选择是运行时的。同一位置的同一指令可能会以不同的通道访问不同的存储体。我做到了:) 所以, 确实存在完全不可能的情况。在某些情况下, 您可以做出很好的猜测, 而在其他情况下则不能。当然, 你需要智慧来区分这些情况。

[北方软件公司](#)

#15

元



高级会员



总帖子: 153

奖励积分: 0

加入时间: 2008 年 2 月 11
日

地点: 西班牙

状态: 离线

回复: 反编译一张图片 • 2020 年 7 月 13 日, 星期一 5:22 AM (永久链接)

不需要模拟器。

只需读入十六进制, 如果有
16 83 bsf STATE, RPO

和
12 83 bcf STATE, RPO的另一个操作码,

C#程序就多了一个。

<http://electronica-pic.blogspot.com>中的电子 PIC



-2 (2)

#16

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: 反编译一张图片 • 2020 年 7 月 13 日星期一上午 5:38 (固定链接)

“

不需要模拟器。

只需读取十六进制, 如果有
16 83 bsf STATE, RPO

和
12 83 bcf STATE, RPO的另一个操作码

元


”



+1 (1)

您假设从低地址到高地址的线性操作。通常情况并非如此, 尤其是当 hex 文件是由“有经验的”程序员编写的汇编代码创建时。如前所述, 银行指令通常不位于内存访问指令之前。

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: 反编译一张图片 • 2020 年 7 月 13 日星期一上午 5:55 (固定链接)

例如,

```
bsf STATUS , RP0
clrf TRISB
goto label
clrf PORTB
```

PORTB 和 TRISB 具有相同的偏移地址, 那么您的反汇编程序会将其视为 PORTB 还是 TRISB? 这只是一个简单的例子, 还有其他更困难的情况, 比如 NorthGuy 描述的不同指令可以访问两个或更多不同的寄存器。我也这样做了。;)

👍👎

+2 (2)

#18

里克



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

回复: 反编译一张图片 • 2020 年 7 月 13 日星期一上午 6:04 (固定链接)

“

不需要模拟器。

只需读取十六进制, 如果有

16 83 bsf STATE, RP0

和

12 83 bcf STATE, RP0的另一个操作码

”

所以你根本没看懂我的描述。您实际上有多少PIC16F汇编代码的经验?

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!

👍👎

+2 (2)

#19

元



高级会员

★★★★★

总帖子: 153

奖励积分: 0

加入时间: 2008 年 2 月 11 日

地点: 西班牙

回复: 反编译一张图片 • 2020 年 7 月 13 日星期一上午 6:12 (固定链接)

我已经理解他们了。

所以做不到。

<http://electronica-pic.blogspot.com>中的电子 PIC

👍👎

0

#20

状态: 离线

页: 1 2 > • 显示第 1 页, 共 2 页

主页 » 所有论坛 » [8 位微控制器] » PIC 微控制器 (PIC10F、PIC12F、PIC16F、PIC18F) » 反编译 PIC

跳转到: --- PIC Microcontrollers (PIC10F, PIC12F, PIC16F, PIC18F)

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