# 关于Intel DCI调试的研究记录

## 1：下载并安装ISS (Intel System Studio)

### 1.1注意事项

**为了接下来一切功能的正常运作，请务必在当前主机先安装ISS**

**否则你将无法正常识别到Intel DCI设备，其主要原因是Intel DCI设备需要的驱动**

**只能在安装ISS的时候打上。**

### 1.2无用介绍

Intel System Studio 2020是英特尔公司推出的一款功能强大的工具包（极速下载站提供），可以提高基于英特尔的物联网系统的可靠性和性能。先进的调试，跟踪和分析功能可帮助您开发IoT解决方案或嵌入式应用程序。该套件非常适合包括图像，机器学习，存储，通信和运输用途在内的高要求处理。并从Windows \*主机进行了交叉开发，并为所有IA平台提供了扩展的JTAG调试支持。新的基于代理的UEFI调试可帮助系统开发人员加快产品上市时间，并增强这些日益复杂的嵌入式和移动系统的可靠性。Eclipse \*集成和交叉构建功能可通过Intel System Studio加快系统开发速度。

### 1.3下载地址

ISS (windows调试版)安装镜像以及license下载地址：

<https://registrationcenter-download.intel.com/akdlm/irc_nas/16258/system_studio_2020_windows_target_ultimate_edition_offline.iso>

<https://dynamicinstaller.intel.com/api/v2/license>

度盘下载地址 (code：t0fw)：

<https://pan.baidu.com/s/1sz9SzZtkOIwT_EZnnfgAqg>

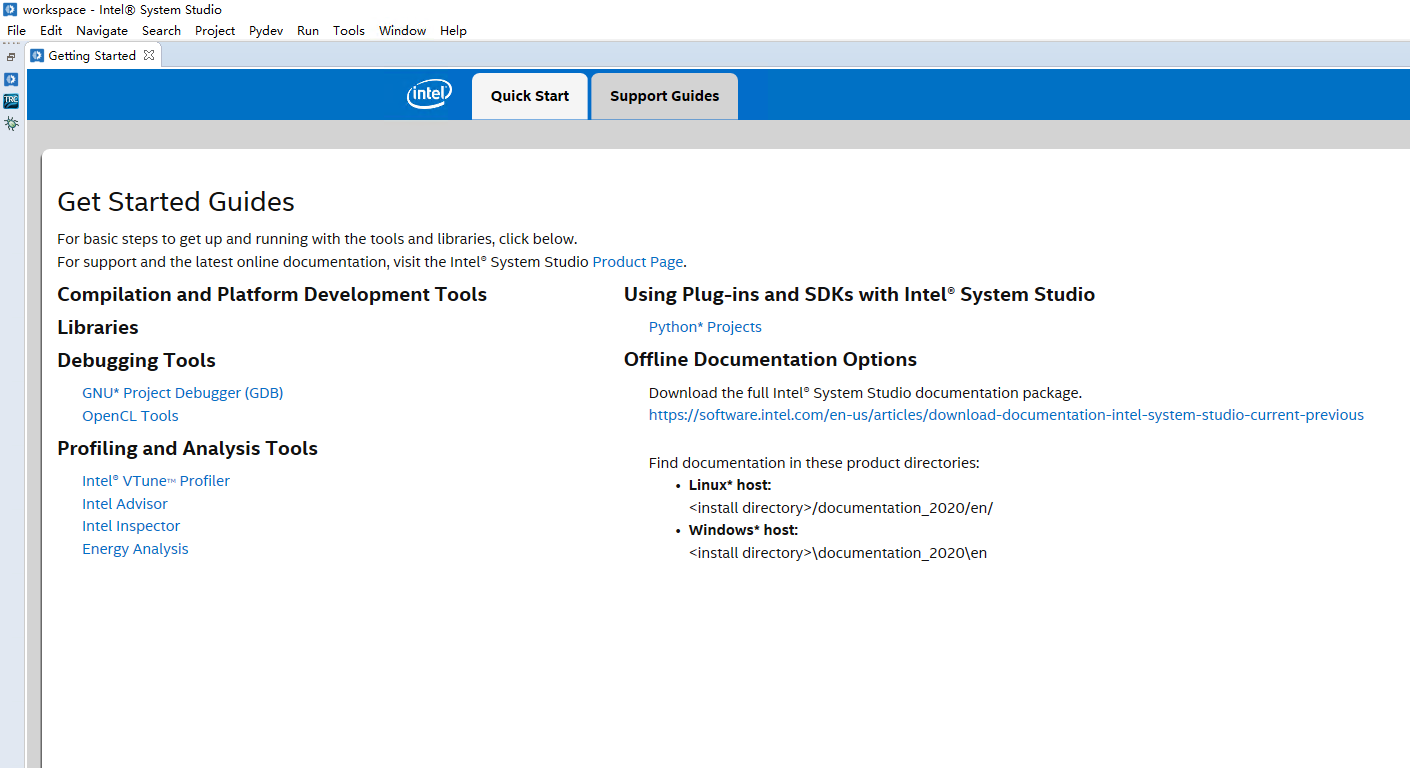
### 1.4安装 ISS

### 

下载之后得到这两个文件，在windows内直接双击打开4G大小的安装镜像



然后运行install.exe，接下来只需要一路点Next 就可以安装上了。



接下来就可以关闭ISS了，进行下一步操作

## 2：购买合适的硬件搭配

### 2.1廉价改造一根调试线

ITPDCI调试线其实是USB3.0公对公线，如下图进口货(智商税)所示。



但它又和一般的USB3.0公对公有所不同

其内部的Power 和USB1/2的部分是没有连同的。

而其价格也是不菲，在某宝上需要花费200 rmb才能买到，有时候还要等进货。

通过阅读这篇文章：

<https://www.lab-z.com/ccadbc/>

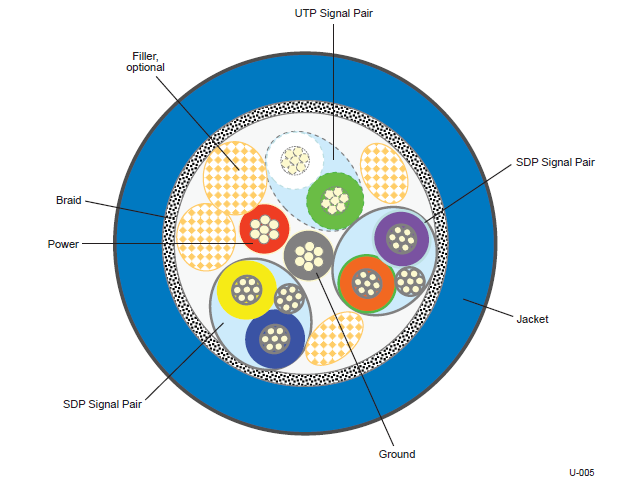
发现其实Windbg的调试线也是可以作为DCI调试线使用的

再后来又阅读这篇文章：

<https://www.mobibrw.com/2014/1469>

发现其实这个线非常好改 我们摘取简要部分介绍

USB3.0内部线缆颜色图如下所示



Power线为红色

USB1/2是两根线，也就是D+ &D- (UTP Signal Pair),颜色是白色和绿色

也就是说，我们只需要去某宝买一条20包邮的USB3.0公对公的线

拆开内部，把其中的 红、绿、白 三根线剪断就可以获得一根DCI调试线

经过笔者自行支付智商税买一根正版线

以及另外购买一根USB3.0 公对公线测试

魔改出来的线和正版线使用起来并没有什么差别

### 2.2主板和CPU的选择

这里是比较重要的一个环节，需要主板和CPU匹配，才能正常进行调试。

笔者本身玩过魔改，尝试过使用100系主板上八代ES (QNCT)

最终只能成功连接，但不可以调试（据说可以通过Intel DAL调试，但我并没有弄明白）

当前支持调试的酷睿组合如下

格式 CPU架构 / 主板芯片组

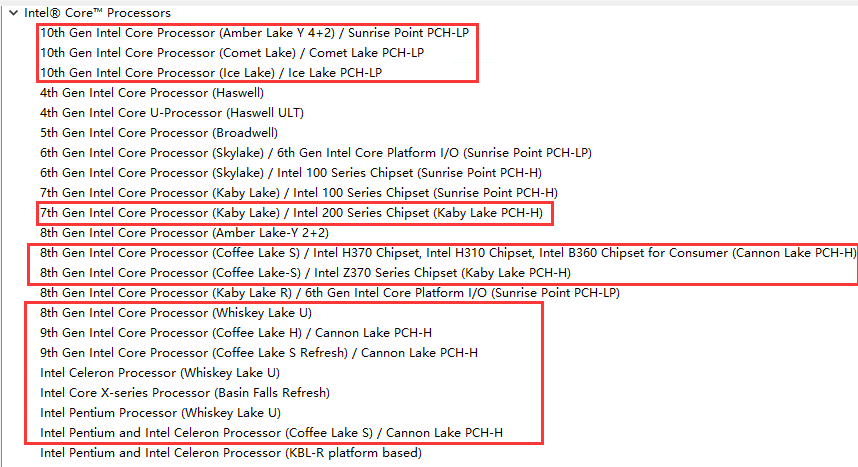
**其中只有红框选中的组合是支持USB3.0 DCI 调试的**

**而且必须要板U对应**

**如果你是100系主板(H110 B150 Z170 ....)**

**魔改上了8/9代的 正版/ES版 CPU ，都是不可以作为被调试机使用的。**

**在ISS (Intel System Studio)中，没有合适的组合可以调试他们，所以必须要板U对应**



目前可以抄的作业：

华擎H370M itx AC + i7 8700 来源:<https://www.4hou.com/posts/pRmV>

微星 Z390A PRO + i7 9700k 来源：笔者亲测

猜测可行的廉价方案：

酷睿：

任意大厂H310 + i3 9100

任意大厂H410 + i 3 10100

赛扬 (Apollo Lake)板U集成一体：(笔者自行购买一台笔记本测试过了，不行)

锐角云 N3450

任意厂家 J3455 / J3355 / J3355E / J4205 / N4200 / N4200E

**PS：理论上只要是 板U对应就可以**

**Z370 / B360 / B365 / H310 对应 酷睿八代正版U**

**Z390 对应 酷睿九代正版**

## 3：修改BIOS设置开启DCI和PT

### 3.1名词介绍

DCI 全称  Direct Connect Interface，是Intel在芯片组和CPU上预留的一个调试接口。

PT 全称 Processor Trace 字面意思 处理器跟踪

有关PT的更多介绍可以移步这里：<https://bbs.pediy.com/thread-266903.htm>

### 3.2如何开启DCI和PT

目前支持DCI和PT的主板，默认都会把这些选项在BIOS中隐藏起来。

为了开启它们，我们有以下三种途径可走

1：修改BIOS强行开启

2：在UEFI shell 下写入BIOS NVRAM 临时开启

3：使用Intel Flash Image Tool重新编译bios（笔者测试并没有什么卵用，甚至还把bios刷坏）

这里讲一下前两种方法

警告：

由于目前大部分厂家的BIOS都是AMI的，所以后续的内容也仅仅讲AMI的BIOS修改方法

### 3.3必要的工具准备

**软件部分**：

1：AFUWIN

AFUWIN是一个可以在windows系统内备份/刷入BIOS的软件，但需要下载对应的版本才可以正常操作，否则打开就会让电脑死机。

2：AMIBCP

AMIBCP是AMI BIOS修改软件，他可以解锁部分BIOS功能，但也需要下载对应的版本才可以正常修改BIOS。

3：UEFITooL&Universal IFR Extractor

UEFITool是民间大神写的BIOS解析工具，可以提取BIOS中的关键节点导出到文件，但提取内容是加密的。

Universal IFR Extractor 是与之对应的解密软件，它可以把UEFITool导出的文件解密成人类可阅读的txt格式。

这个工具组合的重要点在于，它们可以获取到某个BIOS设置在NVRAM中的偏移量，比如BIOS Lock偏移量为 Offset：0x7D8; Size:：1; 0x01 lock 0x00 unlock; 。

但是，事实上，每个BIOS的NVRAM偏移量都不相同，所以必须要用这个工具手动去获取。

4：工具打包下载地址

在上面ISS分享地址同文件夹下的 AMI(BIOS Tool).rar

当前分享的版本，适用于 100 200 300 400系主板，基本上涵盖了678910代CPU。

如果不好使，少侠自行Google Baidu SMXDIY 找找。

**硬件部分**(本部分不是必须，但有条件的还是要准备一下)：

1：一个空闲的U盘

这个U盘的作用是用来进入UEFI shell 直接改写BIOS NVRAM 临时开启BIOS功能

好处是，如果改写有误，可以清除CMOS还原一切设置，而不伤BIOS。

2：第二台电脑

改BIOS本就逆天而行，偶有失手也正常，第二台电脑可以配合编程器救回主板。

3：CH341 BIOS编程器

编程器是你的第二道防线，如果刷入BIOS有误并且无法正常开机，你可以使用第二台电脑，把原厂BIOS重新刷入主板救砖。

4：备用BIOS芯片和电烙铁

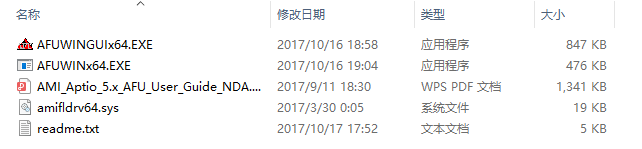
本来是不必要的，但是为了防止你手笨搞坏BIOS芯片，这是最后一道防线，如果你彻底刷坏了BIOS 可以用烙铁（或者风枪）把原BIOS取下，焊接上新BIOS芯片，然后再继续试验。

### 3.4 使用AMIBCP&AFUWIN修改BIOS

解压工具压缩包，得到如下文件

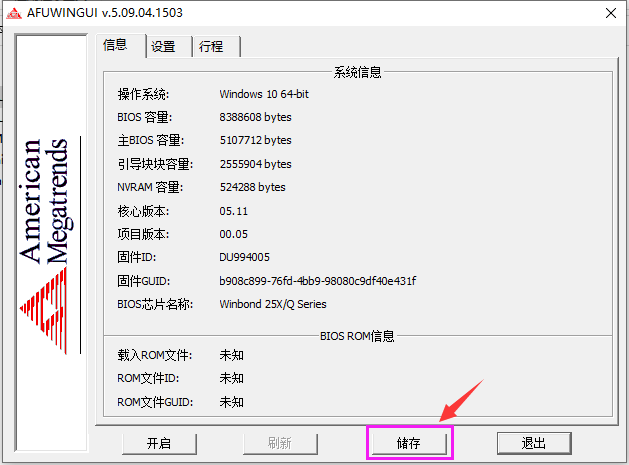


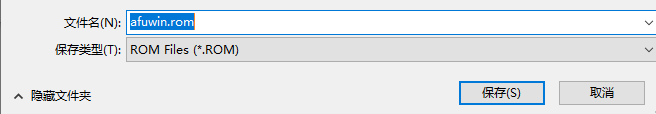
打开 AfuWin64文件夹



然后运行 AFUWINGUIx64.EXE

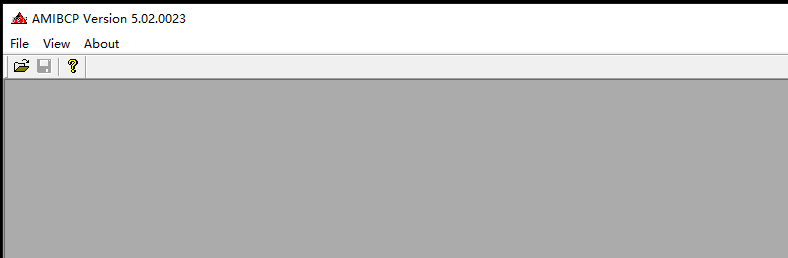
点击储存按键，就可以把当前BIOS备份到文件





回到上一级目录

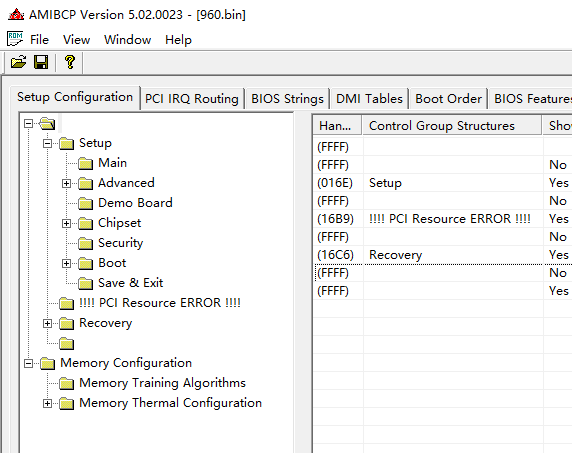
打开AMIBCP



把刚刚备份的BIOS文件拖进去

拖不进去的，直接点File->Open 选择文件打开

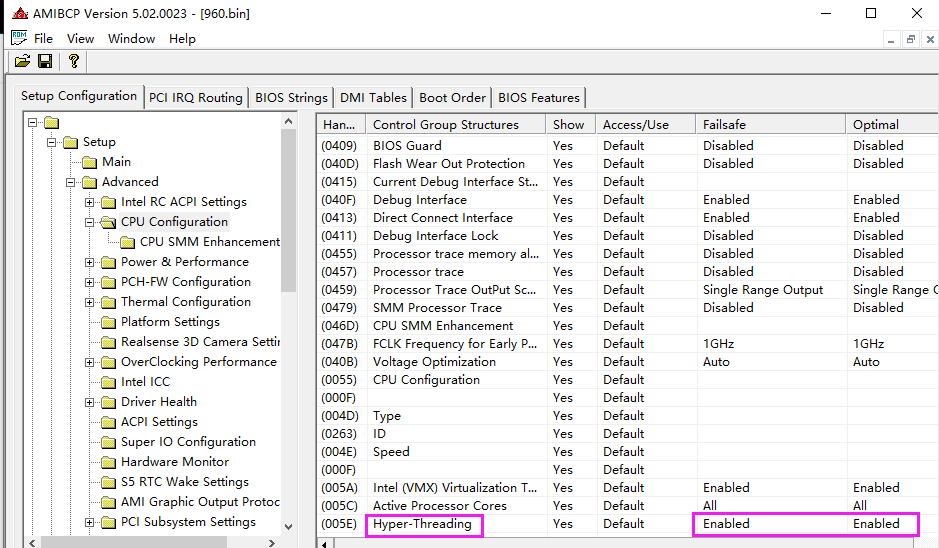
打开之后，就可以随便点点看看了。



例子：

你想开启超线程的时候，只需要把Hyper-Threading 修改为Enabled即可

要把Failsafe 和 Optimal这两列都改成 Enabled



接下来就是开启DCI选项

从树里找到

IED或者Intel Enhanced Debug 修改为 Enabled

CPU Run Control 修改为 Enabled

CPU Run Control Lock 修改为 Enabled

Platform Debug Consent 修改为 USB3

xDCI Support 修改为 Enabled

DCI 或者 Direct Connect Interface 修改为 Enabled

DCI Lock或者 Debug Interface Lock 修改为 Disabled

PCH Trace Hub Enable Mode 修改为 Host Debugger

Processor trace memory allocation 修改为 4k

Processor trace 修改为 Enabled

Processor Trace OutPut Scheme 修改为 ToPA Output

SMM Processor trace 修改为 Enabled

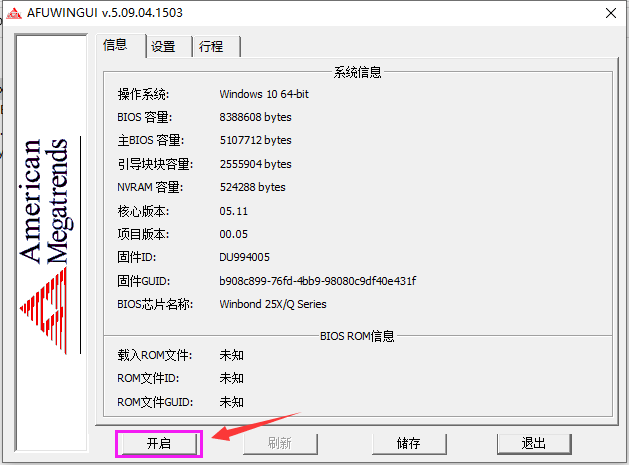
Probeless Trace 修改为 Enabled

Memory Trace 修改为 Enabled

以上内容并不是全都可以找到，能找到多少就改多少。

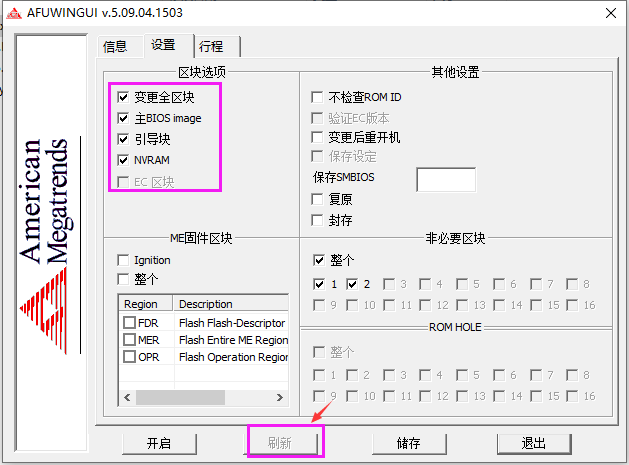
修改完成之后保存BIOS到新文件，原BIOS最好在其他电脑备份一下，用来救砖。

然后你就可以再次使用AfuWin64 把修改后的BIOS刷入主板



点击开启后，它会让你选择要刷入的BIOS

选择好后，勾选全部区块，再点击刷新就好了



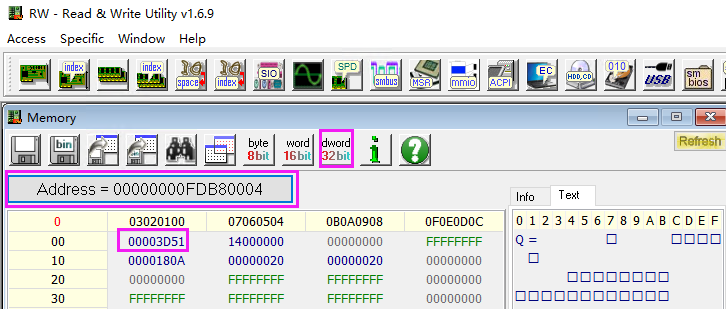
等待一段时间后，BIOS就会刷入成功

如果刷入成功，那么立刻重启，开机狂按Del进入BIOS

选择恢复出厂设置，然后再把Boot 重新设置一下就好了。

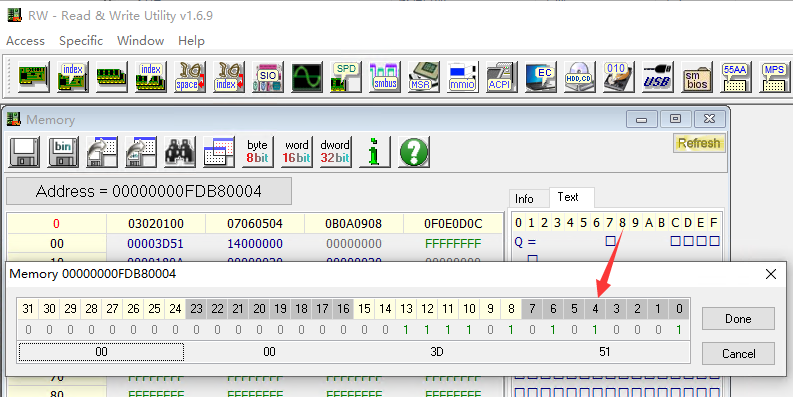
开机后，可以在系统内打开 RW-Everything工具（百度下载）

选择 Memory，查看地址 0xFDB80004 大小选择 dword 32bit



然后双击 00 行 第一个数值

可以看到完整的bit位



注意看bit4

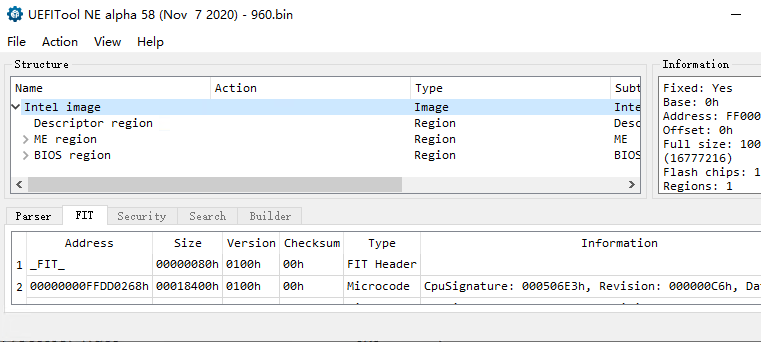
如果为1 则代表已经成功开启DCI

但是要注意的是 这里只是说明你成功开启了DCI，并不能看到PT等功能是否开启

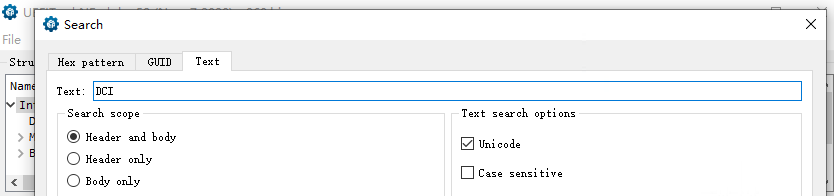
要测试PT是否开启，自行找其他工具测试。

### 3.5 使用UEFITool提取BIOS设置偏移量

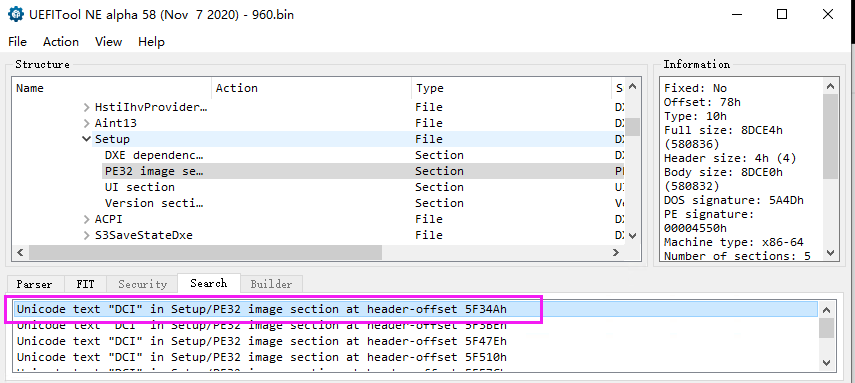
这是第二种方法，首先打开UEFITool并把BIOS文件拖进去



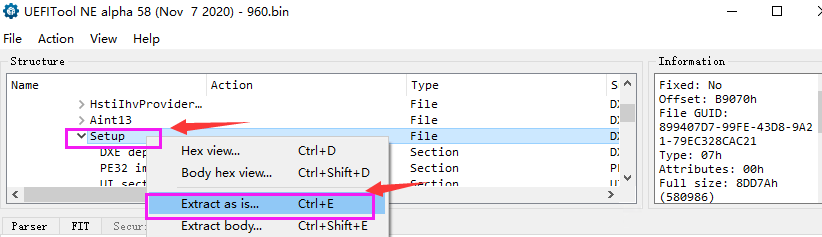
然后CTRL+F搜索 DCI



搜索到之后，随便挑一个鼠标点一下，就会跳到对应的位置



然后右击导出

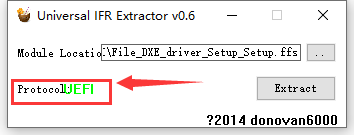


导出后可以获得一个.ffs的文件

然后我们打开Universal IFR Extractor.exe 把ffs文件路径填进去

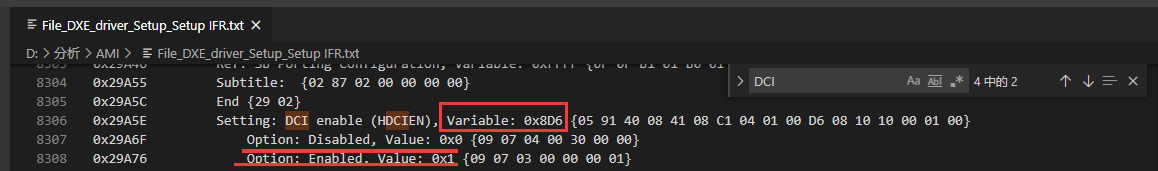
如果可以正常识别，左下角会有绿色的UEFI

然后我们直接点击 Extract导出即可



导出后，用文本编辑工具打开txt

搜索相应的设置



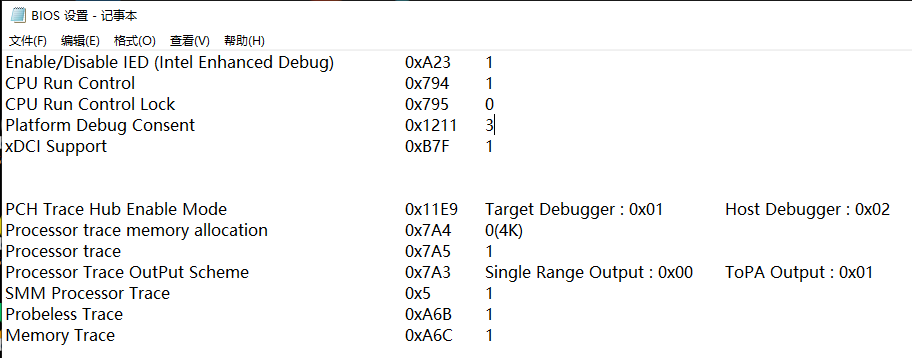
这张截图仅仅是例子

Variable 就是偏移量

Option 就是设置值

把我们需要的偏移量都找到，并记录下来

最终得到了如下内容



### 3.6制作UEFI shell U盘修改BIOS NVRAM

准备好一个空U盘，完全格式化，分区类型为FAT32

然后把UEFI shell.rar解压到U盘根目录



UEFI shell.rar也在上面的度盘链接里。

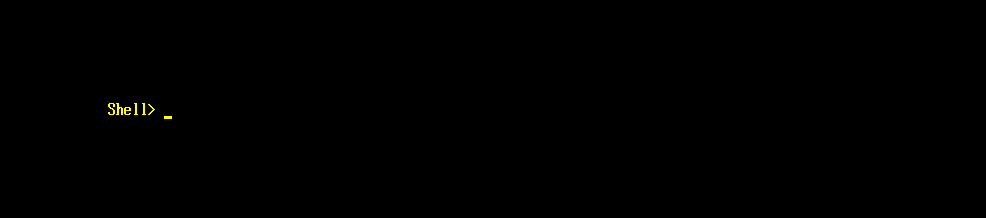
放进去之后，U盘就做好了

然后重启系统，开机狂按DEL

进入BIOS后，修改Boot选项

Boot首选项改为 UEFI :xxxxxx (后面一般都是你的U盘名字+容量，自己判断)

修好好Boot之后保存设置，再次重启

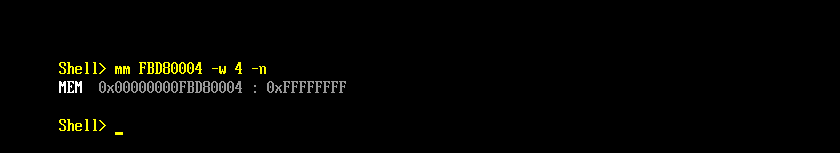


就可以看到shell 控制台了

在这里，可以允许你写一写简单的命令

比如

mm命令



这里的mm命令其实和 RW-Everything一样，都是在读取物理内存

但这都不重要，重要的是，修改bios设置命令

例如 DCI 开启的偏移是 0x7B0 那么命令就是

ami 0x7B0 0x01



之后我们再依次把之前获取到的偏移

全都设置为指定的值就可以

全部修改完成后

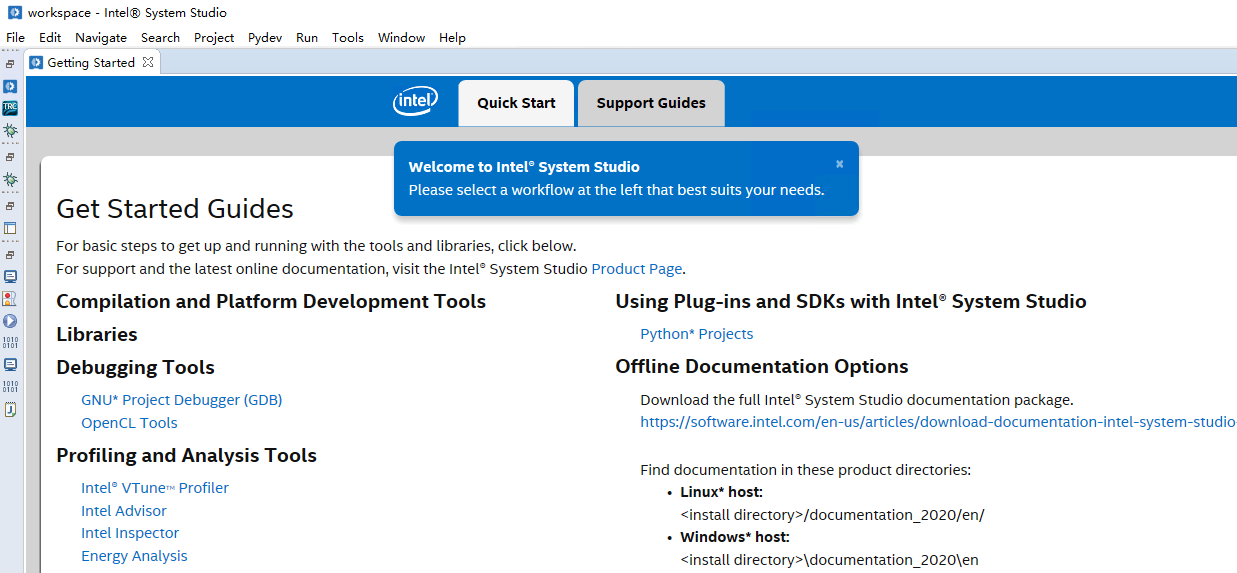
直接Ctrl+Alt+Del 重启

然后进BIOS 把Boot选项改回你原来的系统就好了

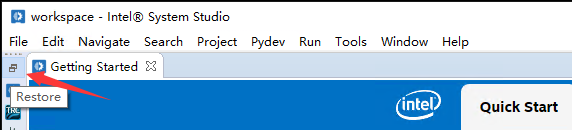
## 4：ISS的连接与调试

### 4.1设置ISS链接

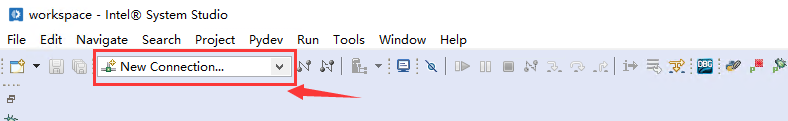
打开ISS



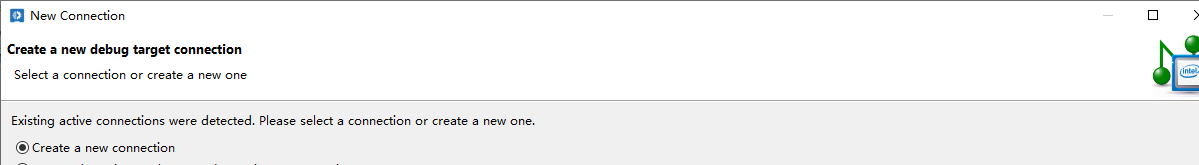
点击Restore



点击创建新链接



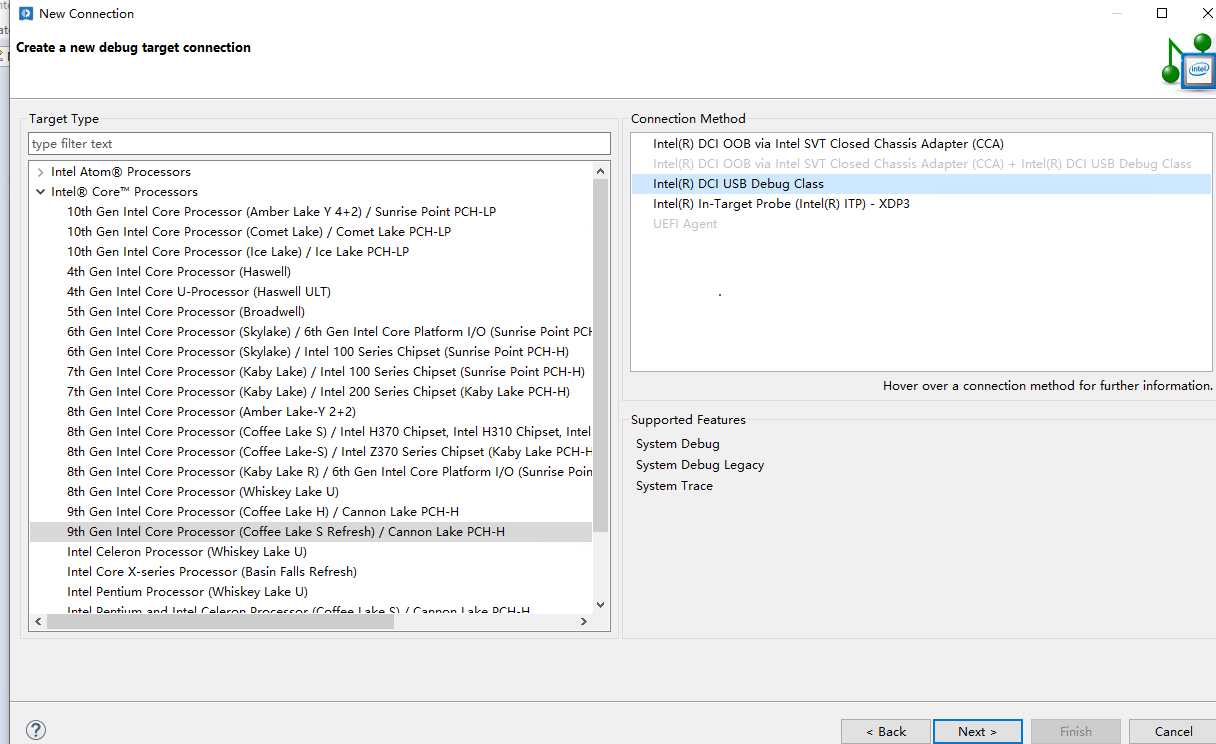
然后



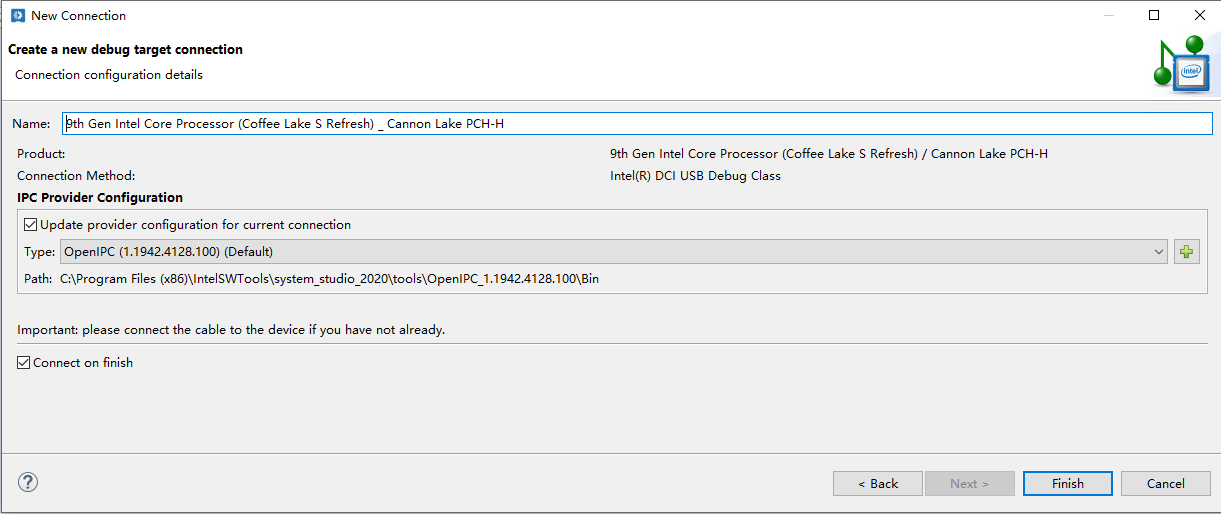
选择自己对应的板U组合

笔者这里是9代+Z390，所以这样选

右边记得点一下 DCI USB Debug Class

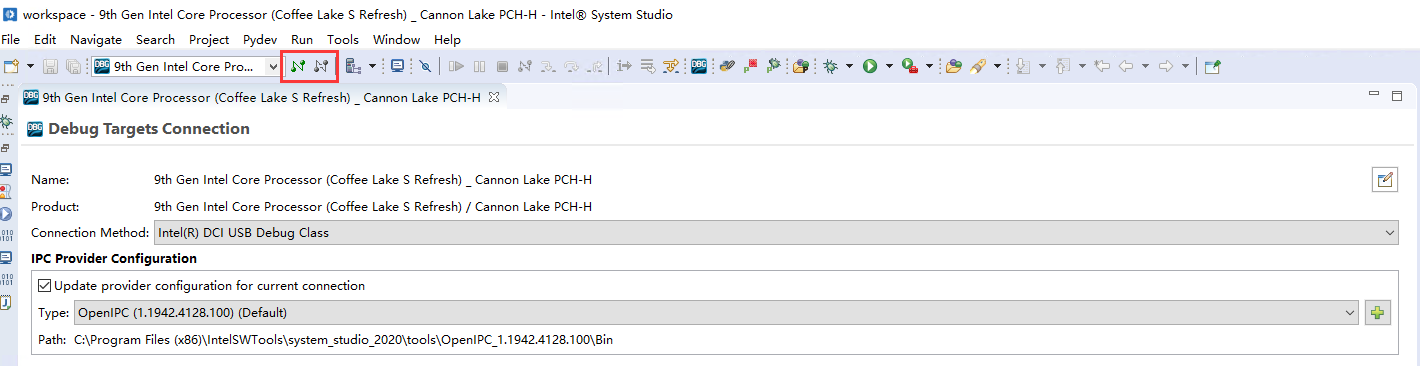


最后



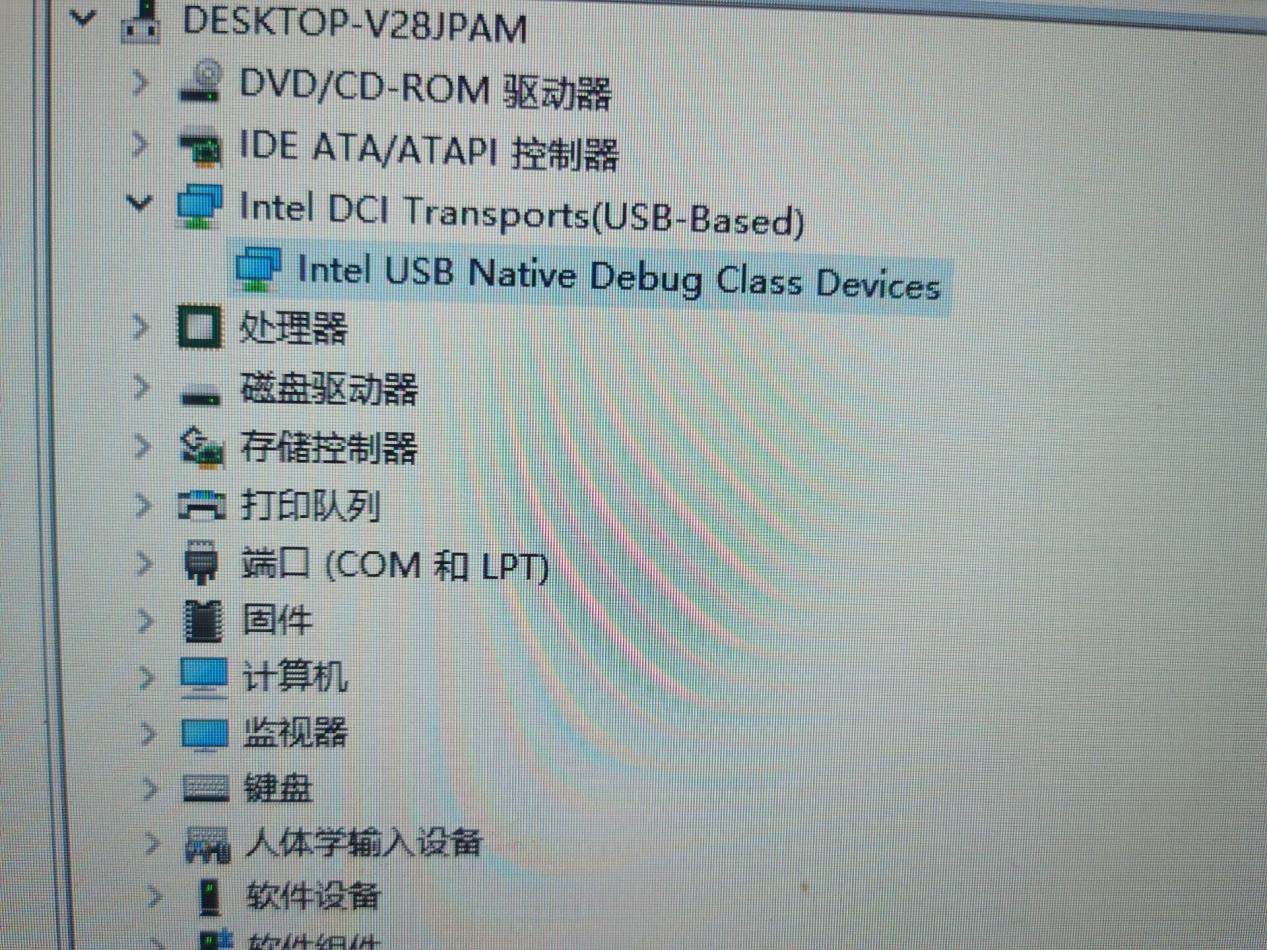
按下Finish后，ISS会自动链接目标

红框里的两个按钮分别是 链接和断开



当然，在你链接失败时，你要检查一下，你的DBC调试线是否有插好

如果插好了，可以在本地系统看到一个DCI设备



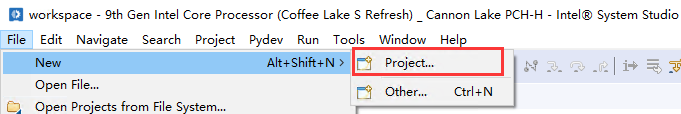
链接成功后会有一条日志



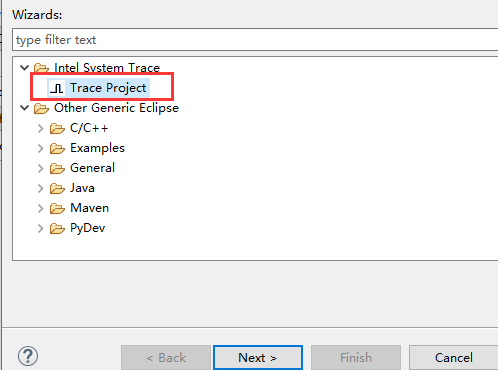
代表已经链接成功

### 4.2创建调试项目

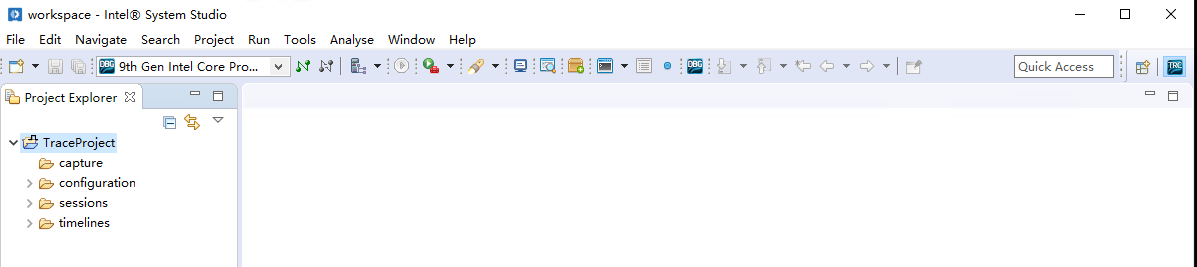
创建项目



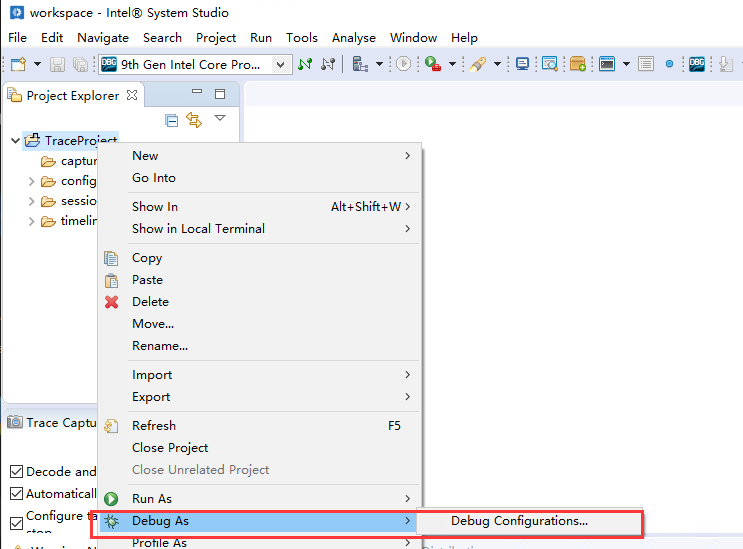
选择Trace Project



一路Next

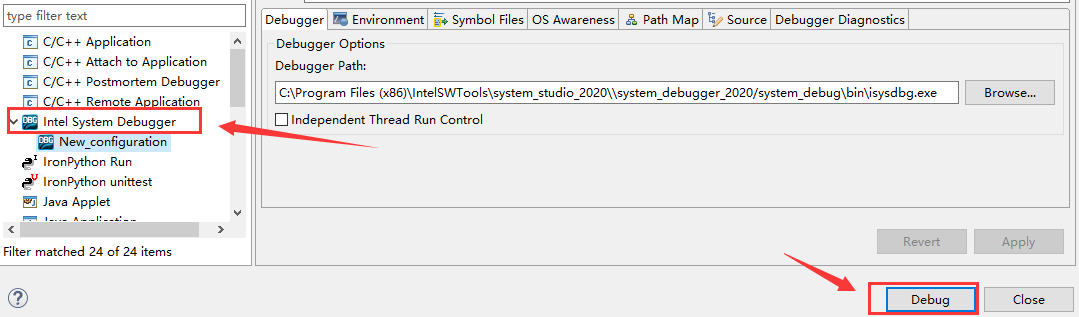


然后设置调试类型

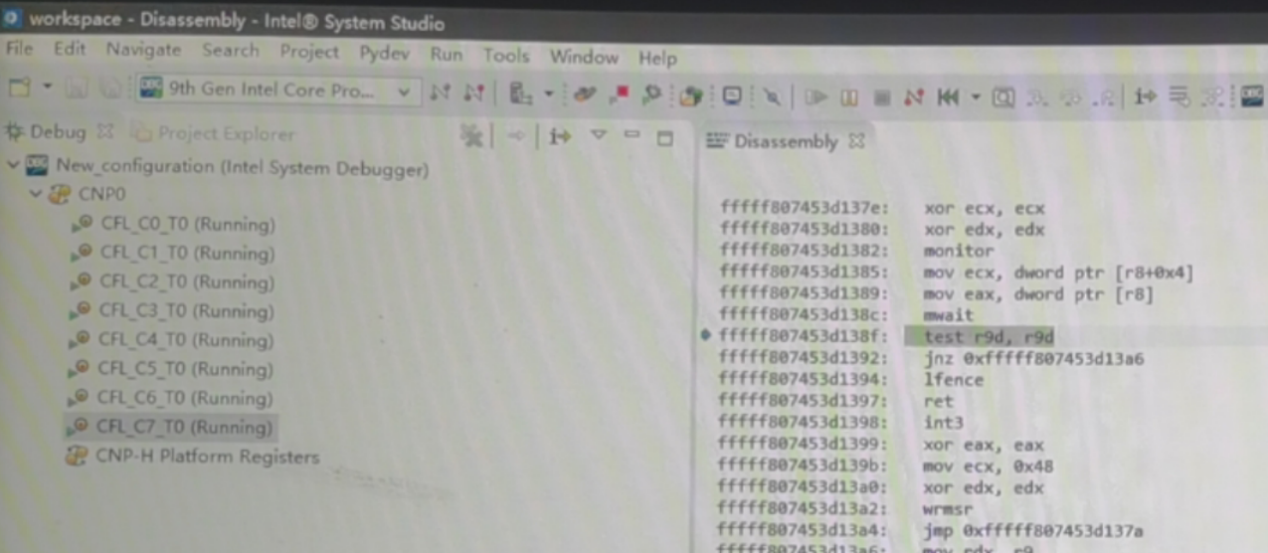


选择 Intel System Debug

点Debug



左侧就会出现CPU列表



随便选一个鼠标右击 suspend 就可以暂停了

右侧是反汇编代码

别问我为什么有的图很糊

因为我用这个拍的



大致就是这样，剩下的内容以后有空再研究

——BY 看雪 万剑归宗