

“羊习习”的专栏

做才能得到，守才是幸福

[目录视图](#)[摘要视图](#)[RSS 订阅](#)

个人资料



羊习习、

[+ 加关注](#) [发私信](#)

访问： 9477次

积分： 260

等级： [BLOG > 2](#)

[为什么未来是全栈工程师的世界](#) [前端精品课程免费看，写课评赢心动大礼！](#) [JavaScript知识库发布](#)

[快速回复](#)

原 如何利用JClassLib修改.class文件

标签： [Android](#) [jclasslib](#) [反编译](#)

2013-11-08 14:27 2793人阅读 评论(2) [收藏](#) [举报](#)

分类： [Android反编译](#)

| 版权声明：本文为博主原创文章，未经博主允许不得转载。

最近在学习逆向分析和反编译，无意之中了解到了**JClassLib**。**JClassLib**不但是一个字节码阅读器而且还包含一个类库允许开发者读取,修改,写入**Java Class**文件与字节码。其他的用途我就不说了，先看一下效果。

第一步、准备下载工具，一个是jd-gui，阅读jar包和.class源码的工具，jclasslib就修改.class文件的包

排名：千里之外

原创：16篇 转载：2篇

译文：0篇 评论：5条

文章搜索

文章分类

Android (6)

Android问题解决 (6)

Android反编译 (1)

Android界面 (3)

FTP (1)

Android Studio (1)

文章存档

2015年12月 (1)

2015年11月 (4)

2015年01月 (4)

2014年11月 (1)

2014年09月 (1)

展开

阅读排行

如何利用JClassLib修改. (2792)

Fragment中startActivityF (728)

下载地址

第二步、示范

1、比如说这个就是原来的java文件，很简单就是输出 google 这个字符串

```
[html] view plain copy print ?
01. package com.qx;
02.
03. public class Main {
04.     public static void main(String[] args) {
05.         print();
06.     }
07.
08.     static void print() {
09.         System.out.println("google");
10.     }
11. }
```

HTML

2、编译之后，控制台执行结果为 google，为什么用 javac -d . Main.java 去编译java文件，这个我就不解释了，不懂的话去恶补一下

3、找到Main.class文件，并用 jd-gui打开，效果如下

4、在这里很明显看到源码，可惜不能修改呀，现在就准备修改工具，搞定它。解压 jclasslib，目录如下

5、在eclipse里面创建一个java工程，然后把src文件覆盖到工程目录下，并且执行 BrowserApplication.java，得到一个工具叫做Bytecode viewer，如下图

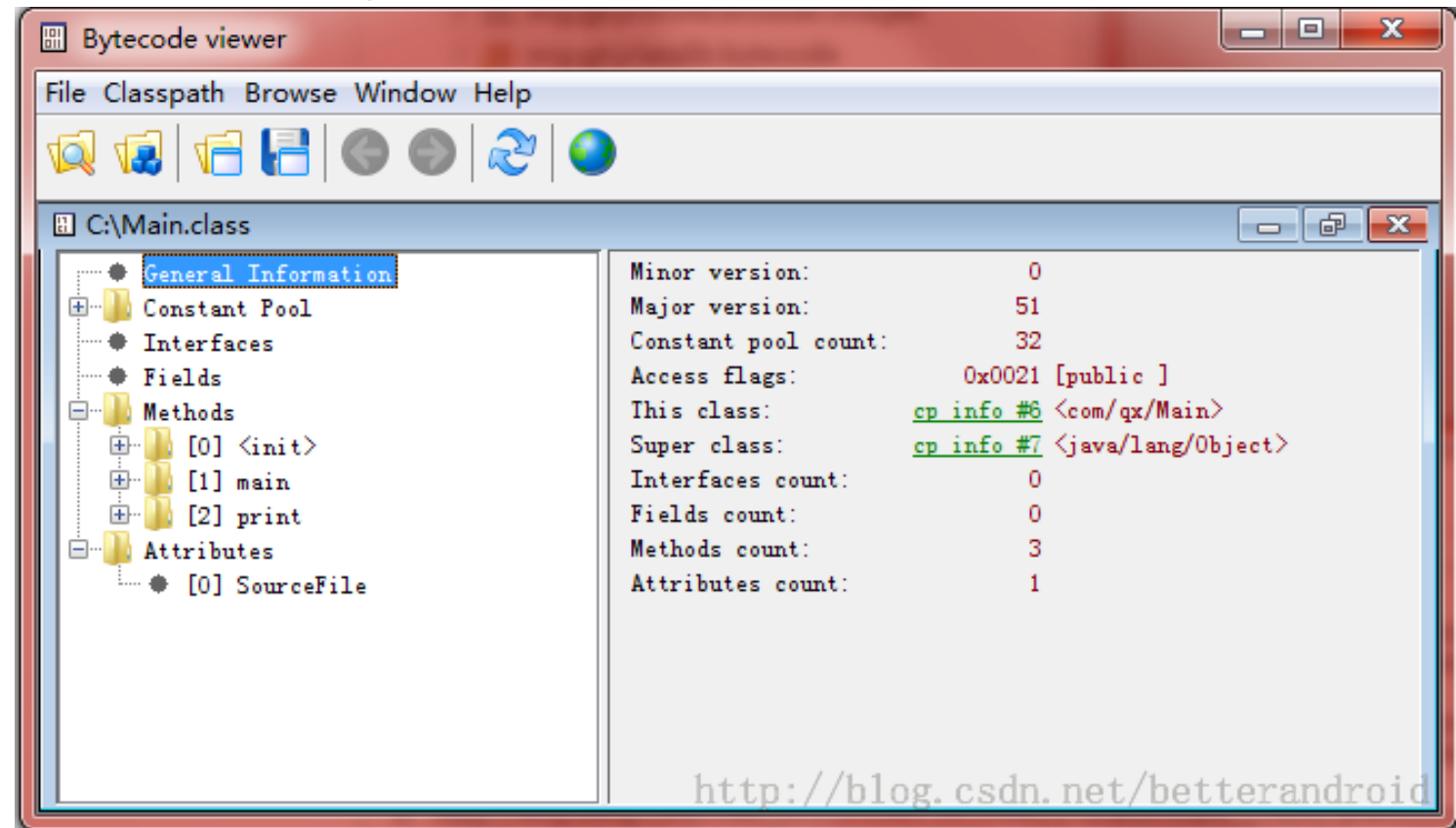
6、现在咱们可以利用工具找到我们修改的部分，我们就是要修改Main.class文件中 google，修改成 baidu。

Android调用已安装市场 (720)
java.lang.SecurityExcept (645)
android studio Gradle如 (608)
"Syntax error on tokens, (535)
ADB server didn't ACK之 (465)
ScrollView下嵌套Gridvie (435)
onWindowFocusChangi (342)
仿微信，自定义加载中透 (331)

评论排行

Android调用已安装市场 (2)
如何利用JClassLib修改. (2)
Fragment中startActivityF (1)
如何创建渐变阴影，记一 (0)
ScrollView下嵌套Gridvie (0)
仿微信，自定义加载中透 (0)
软件版本命名规范 (0)
onWindowFocusChangi (0)
"Syntax error on tokens, (0)
Android中Shane的使用 (0)

结构目录很清楚，methods就是方法，print是打印google字符串的方法，main是主函数，在这里我们找到print并打开



7、打开code，我们会看到第二行 lbc #4 <google>,这时我们点击#4

最新评论

Android调用已安装市场平台（如羊习习、@wdmxzf:手机里面要安装相关的应用市场才能够显示出来。

Android调用已安装市场平台（如wdmxzf:为什么弹不出来呢？

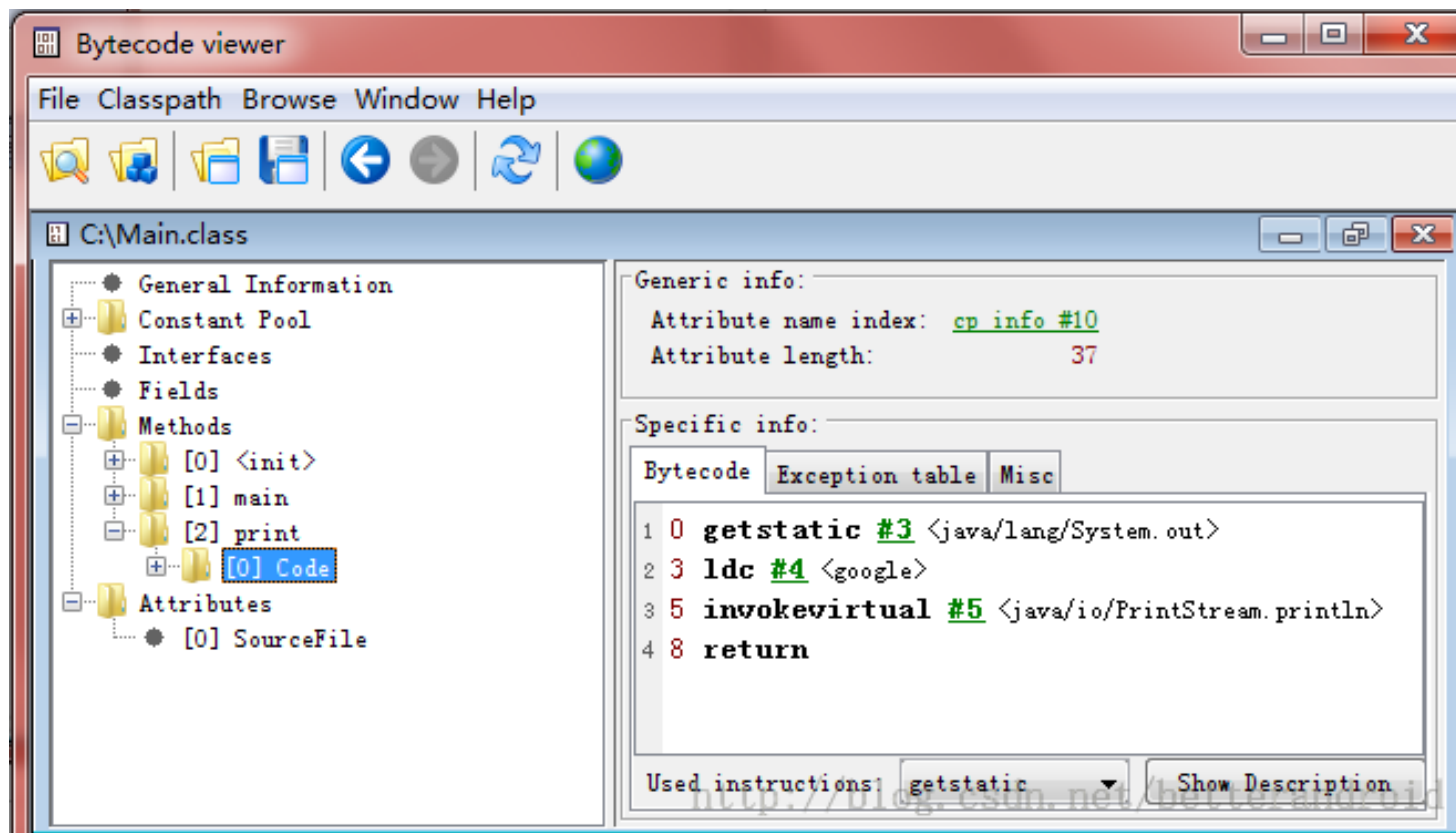
Fragment中startActivityForResult qq_22211053:你的方法我也试了一下，还是不执行啊，你的isFresh是不是设置的默认false？

如何利用JClassLib修改.class文 Akishimo:我要从一个method里删掉几句，该怎么做？？？

如何利用JClassLib修改.class文 Akishimo:怎么删除代码

推荐文章

*Xcode 调试方法总结



8、这个效果如下，通过这个，我们知道google字符串的地址在哪里了，在#21，这个时候 点击 cp info #21

*Android框架设计模式 (三)

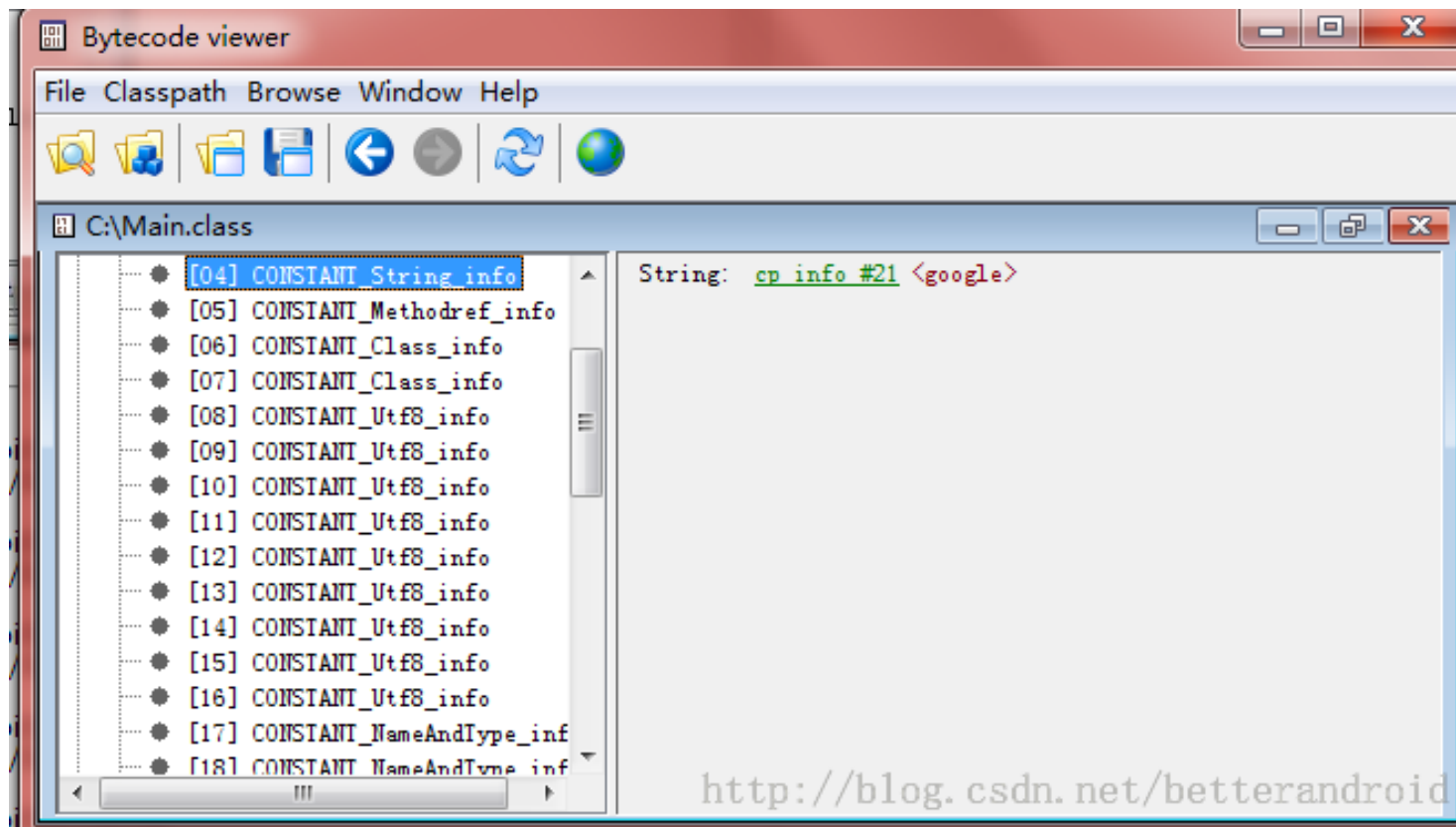
——Observer Method

*浅谈Storm流式处理框架

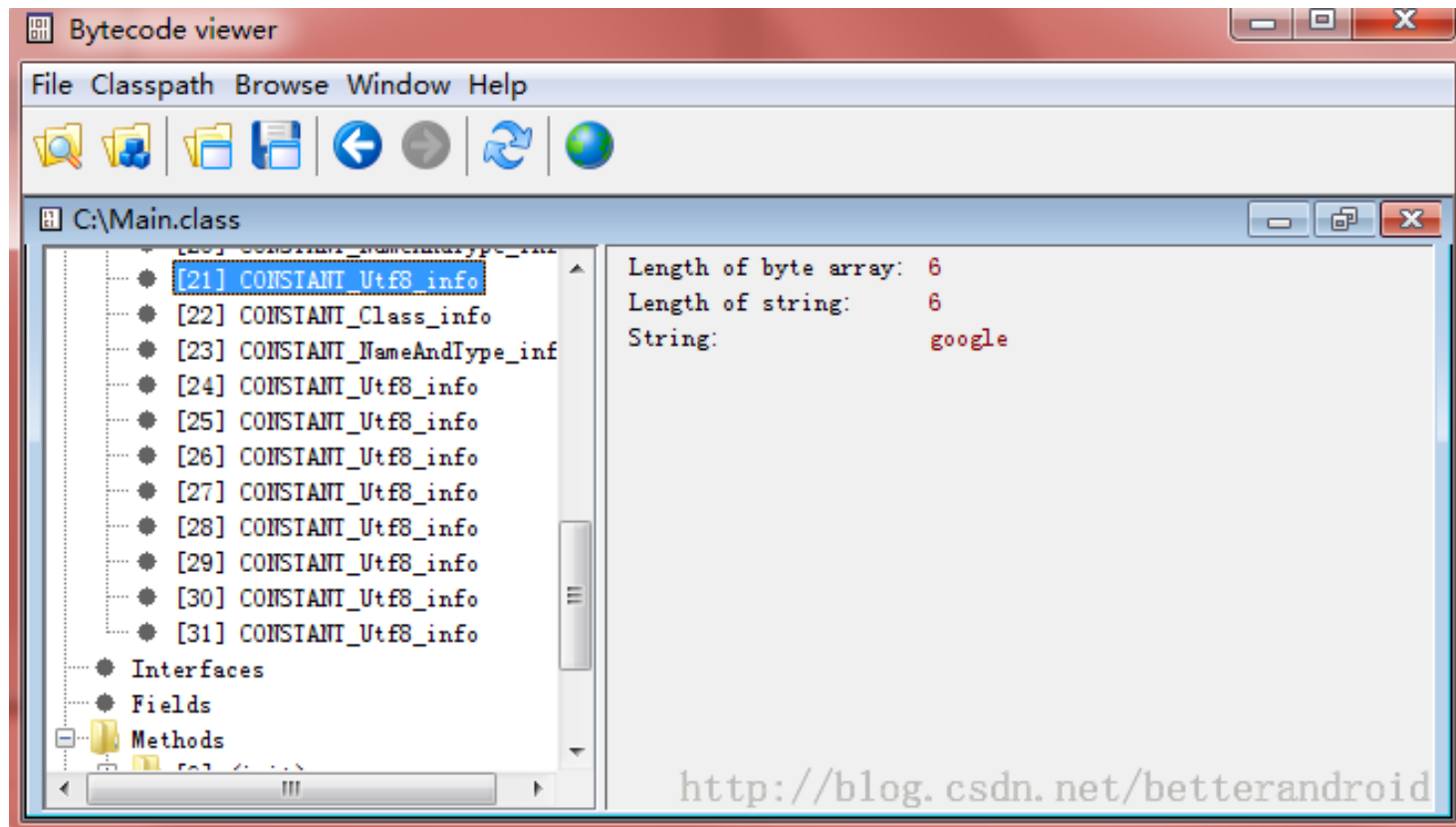
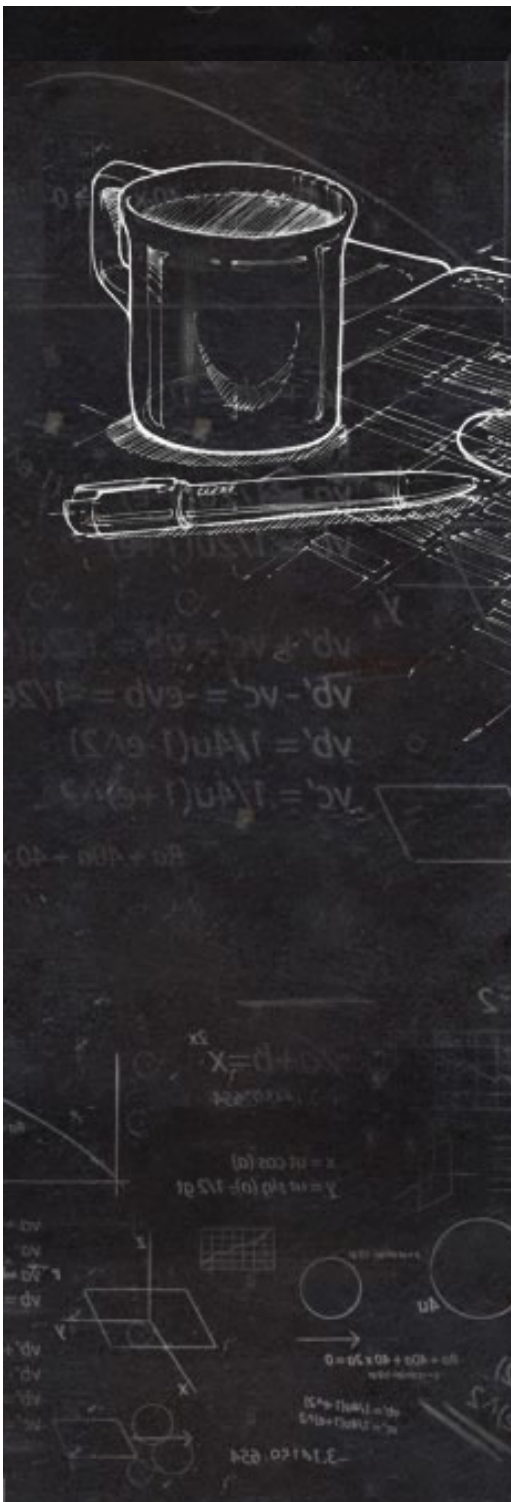
*有关深度学习领域的几点想法

*管理Java垃圾回收的五个建议

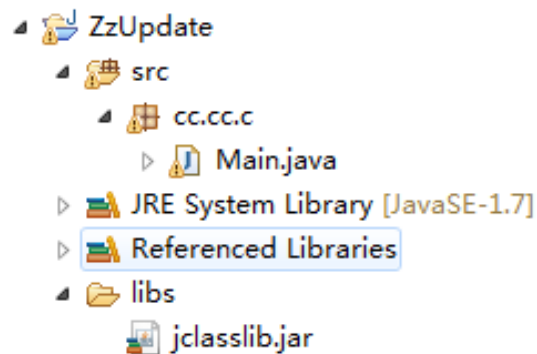
*大数据并发问题



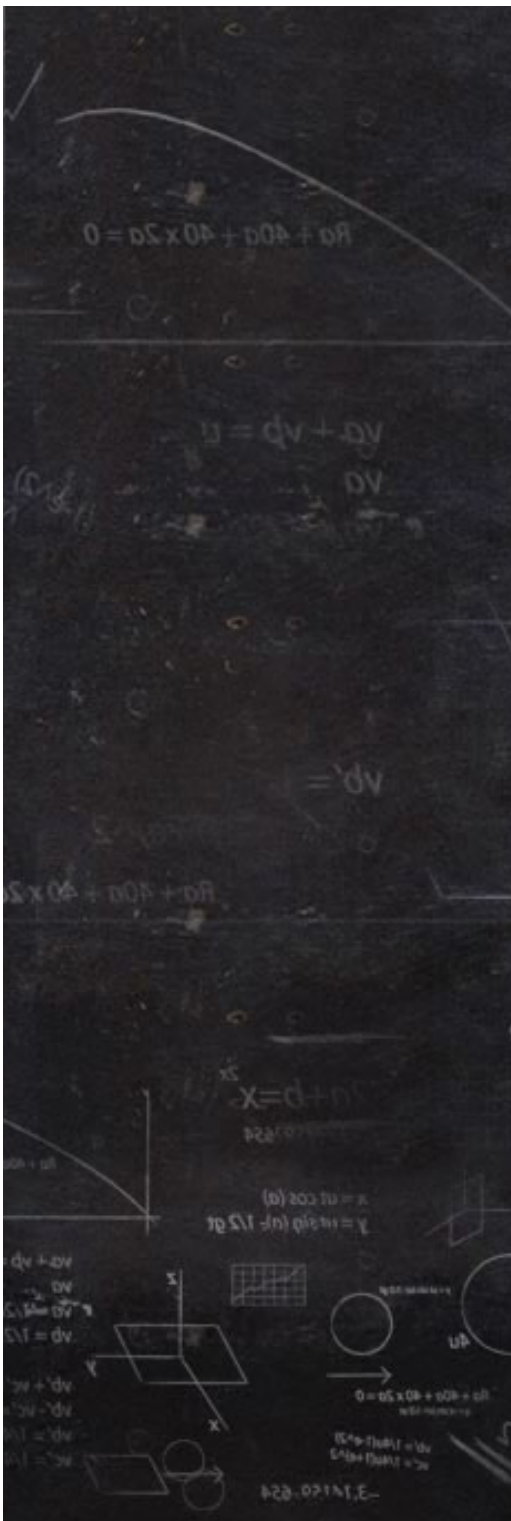
9、这时，我们看到的google字符是在[21]这个位置，并且CONSTANT_Utf-8_info，这些信息待会修改的时候 很有用。



10、现在我们可以用代码去把 google 修改成 baidu。首先创建一个工程，把刚刚下载 jclasslib 文件夹下 bin 目录下 jclasslib.jar 引入，如下图



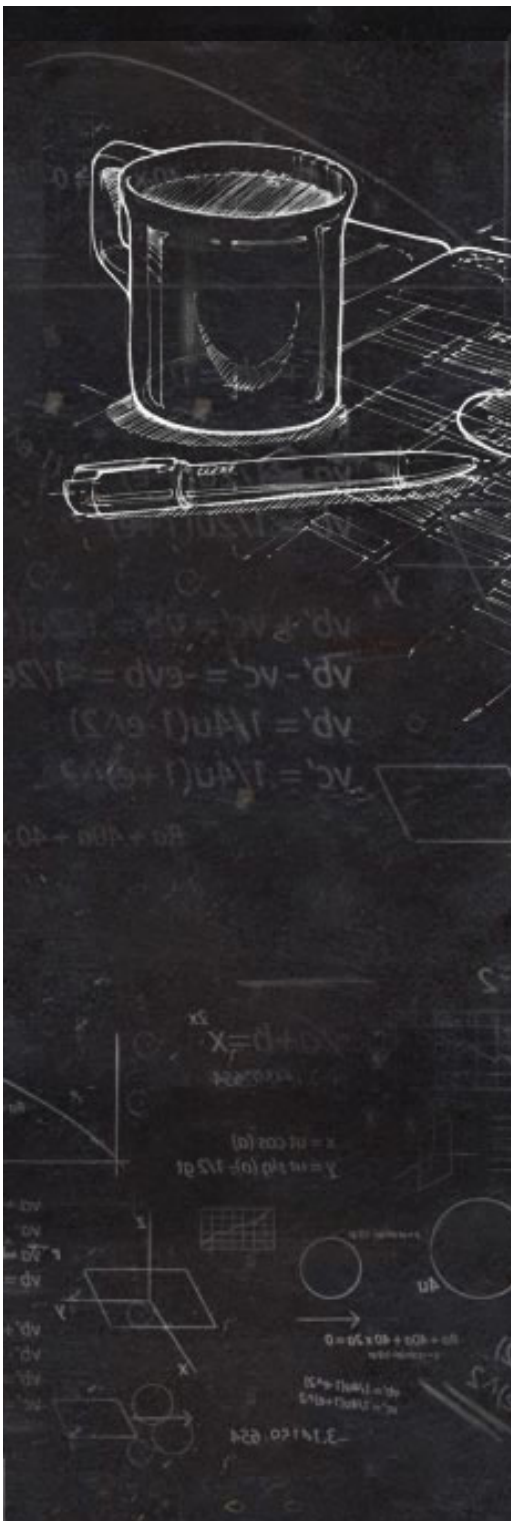
11、Main.java 函数代码如下



[java] view plain copy print ?

JAVA

```
01. package cc.cc.c;
02.
03. import java.io.*;
04. import org.gjt.jcclib.io.ClassFileWriter;
05. import org.gjt.jcclib.structures.CPInfo;
06. import org.gjt.jcclib.structures.ClassFile;
07. import org.gjt.jcclib.structures.constants.ConstantUtf8Info;
08.
09. public class Main {
10.     public static void main(String[] args) throws Exception {
11.
12.         String filePath = "C:\\Main.class";
13.         FileInputStream fis = new FileInputStream(filePath);
14.         DataInput di = new DataInputStream(fis);
15.         ClassFile cf = new ClassFile();
16.         cf.read(di);
17.         CPInfo[] infos = cf.getConstantPool();
18.
19.         int count = infos.length;
20.         for (int i = 0; i < count; i++) {
21.             if (infos[i] != null) {
22.                 System.out.print(i);
23.                 System.out.print(" = ");
24.                 System.out.print(infos[i].getVerbose());
25.                 System.out.print(" = ");
26.                 System.out.println(infos[i].getTagVerbose());
27.                 if (i == 21) { //刚刚找到的是21位置
28.                     ConstantUtf8Info uInfo = (ConstantUtf8Info) infos[i]; //刚刚那里是
CONSTANT_Utf-8_info所以这里要用这个
29.                     uInfo.setBytes("baidu".getBytes());
30.                     infos[i] = uInfo;
31.                 }
32.             }
33.         }
34.         //这种方式也可以，一样的
35.         /* if(infos[count] != null) {
36.             ConstantUtf8Info uInfo = (ConstantUtf8Info) infos[i]; //刚刚那里是
```



```
CONSTANT_Utf-8_info所以这里要用这个
37.         uInfo.setBytes("baidu".getBytes());
38.         infos[count] = uInfo;
39.     }*/
40.
41.     cf.setConstantPool(infos);
42.     fis.close();
43.     File f = new File(filePath);
44.     ClassFileWriter.writeFile(f, cf);
45. }
46. }
```

12、不报错，就代表成功了，然后再执行Main.class文件

```
C:\>java com.qx.Main
google

C:\>java com.qx.Main
baidu

C:\>■
```

这个时候，我们就把class文件中google修改成baidu了，怎么用这个工具就看你怎么玩了，有什么问题请随时留言。

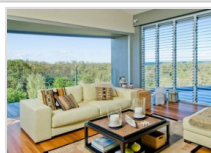


顶
0

踩
0

猜你在找

- Java基础核心技术：IO(day15-day16)
- Android开发精品课程【Java核心知识】
- 深入浅出Java的反射
- 深入浅出Java5新特性
- JavaSE聊天案例



澳大利亚买房



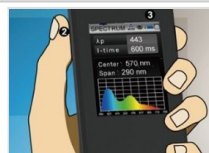
app开发报价



新西兰移民条



立体车库



手持光谱仪



进销存管理



治疗痘印推广

查看评论

2楼 Akishimo 2015-07-10 17:35发表



我要从一个method里删掉几句，该怎么做???

1楼 Akishimo 2015-07-10 17:35发表



怎么删除代码

您还没有登录,请[\[登录\]](#)或[\[注册\]](#)

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

核心技术类目



全部主题 Hadoop AWS 移动游戏 Java Android iOS Swift 智能硬件 Docker OpenStack
VPN Spark ERP IE10 Eclipse CRM JavaScript 数据库 UML components Windows Mobile Rails QEM
BI HTML5 Spring Apache .NET API HTML SDK
Splashtop UML components Windows Mobile Rails QEM
FTC coremail OPhone CouchBase 云计算 iOS6 Rack
Maemo Compuware 大数据 aptech Perl Tornado Rub
Pure Solr Angular Cloud Foundry Redis Scala Django

关闭



[公司简介](#) | [招贤纳士](#) | [广告服务](#) | [银行汇款帐号](#) | [联系方式](#) | [版权声明](#) | [法律顾问](#) | [问题报告](#) | [合作](#)

网站客服 杂志客服 微博客服 webmaster@csdn.net 400-600-2320 | 北京创新乐知信息技术有限公司

京 ICP 证 09002463 号 | Copyright © 1999-2014, CSDN.NET, All Rights Reserved

