“羊习习”的专栏

做才能得到，守才是幸福

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

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

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. }
```

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

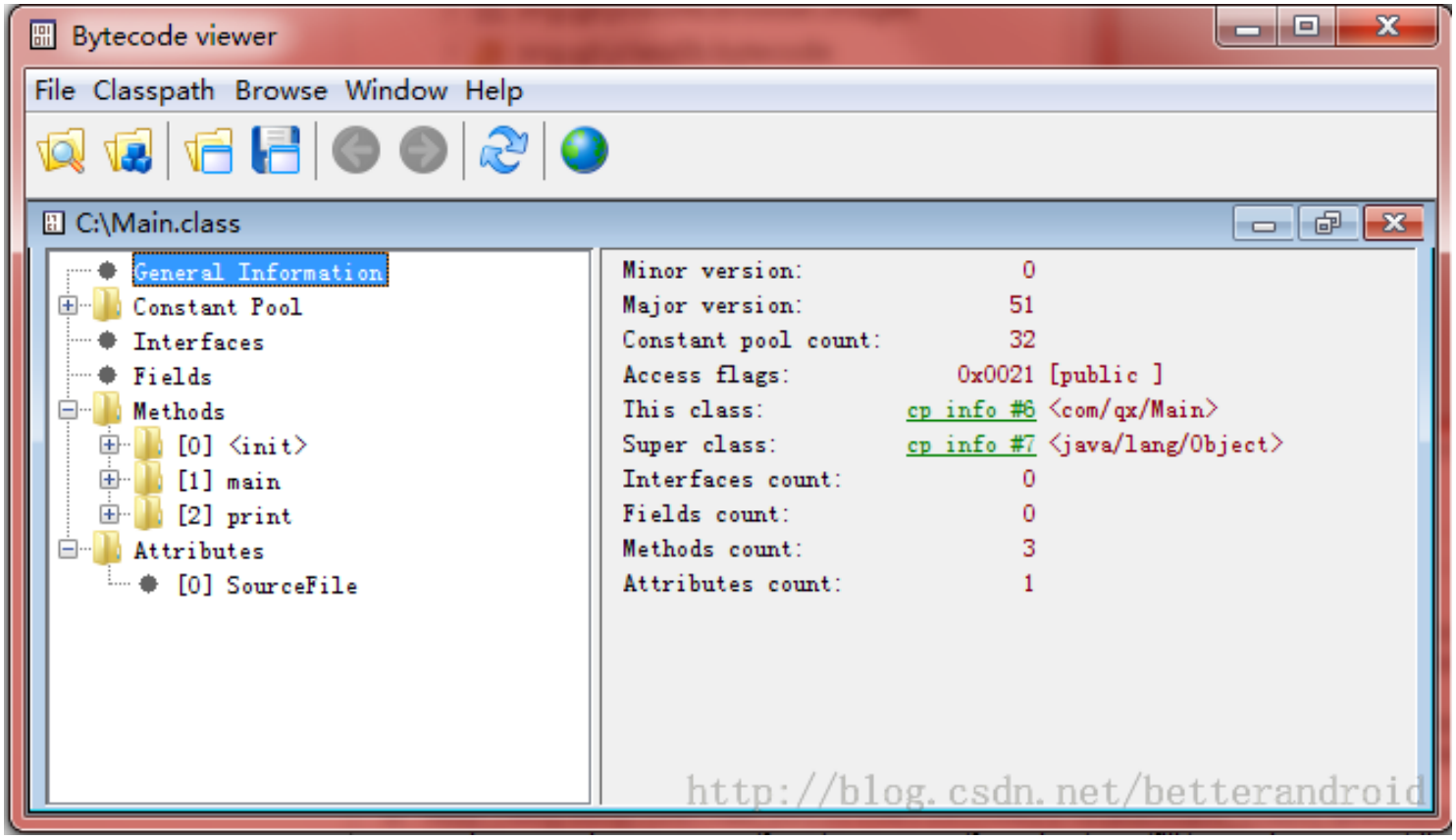
4、在这里很明显看到源码，可惜不能修改呀，现在就准备修改工具，搞定它。解压jclasslib，目录如下

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。

评论排行

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（如羊习习丶: @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？

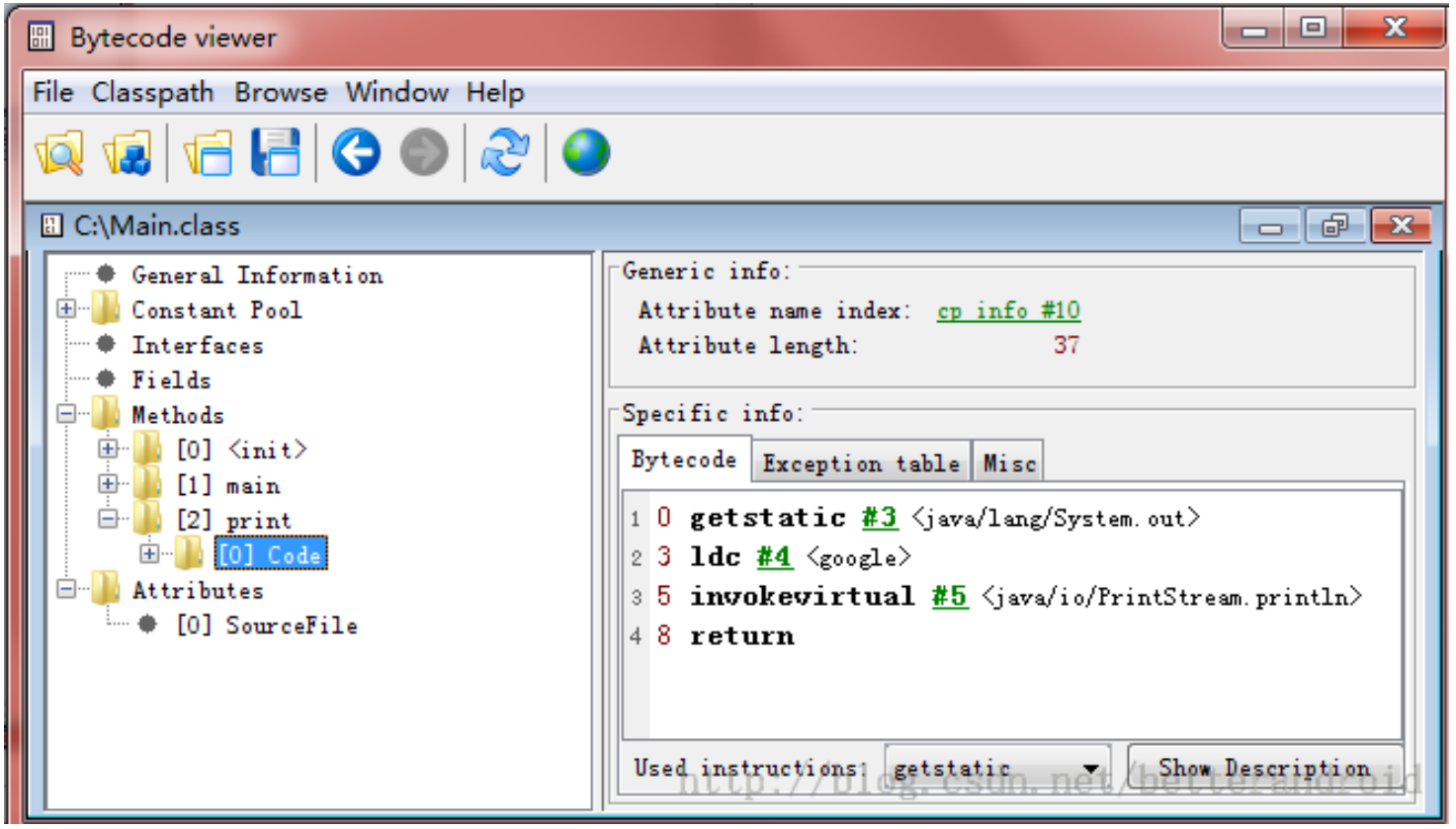
Fragment中startActivityForResu qq_22211053: 你的方法我也试了一下，还是不执行啊，你的isFresh是不是设置的默认false？

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

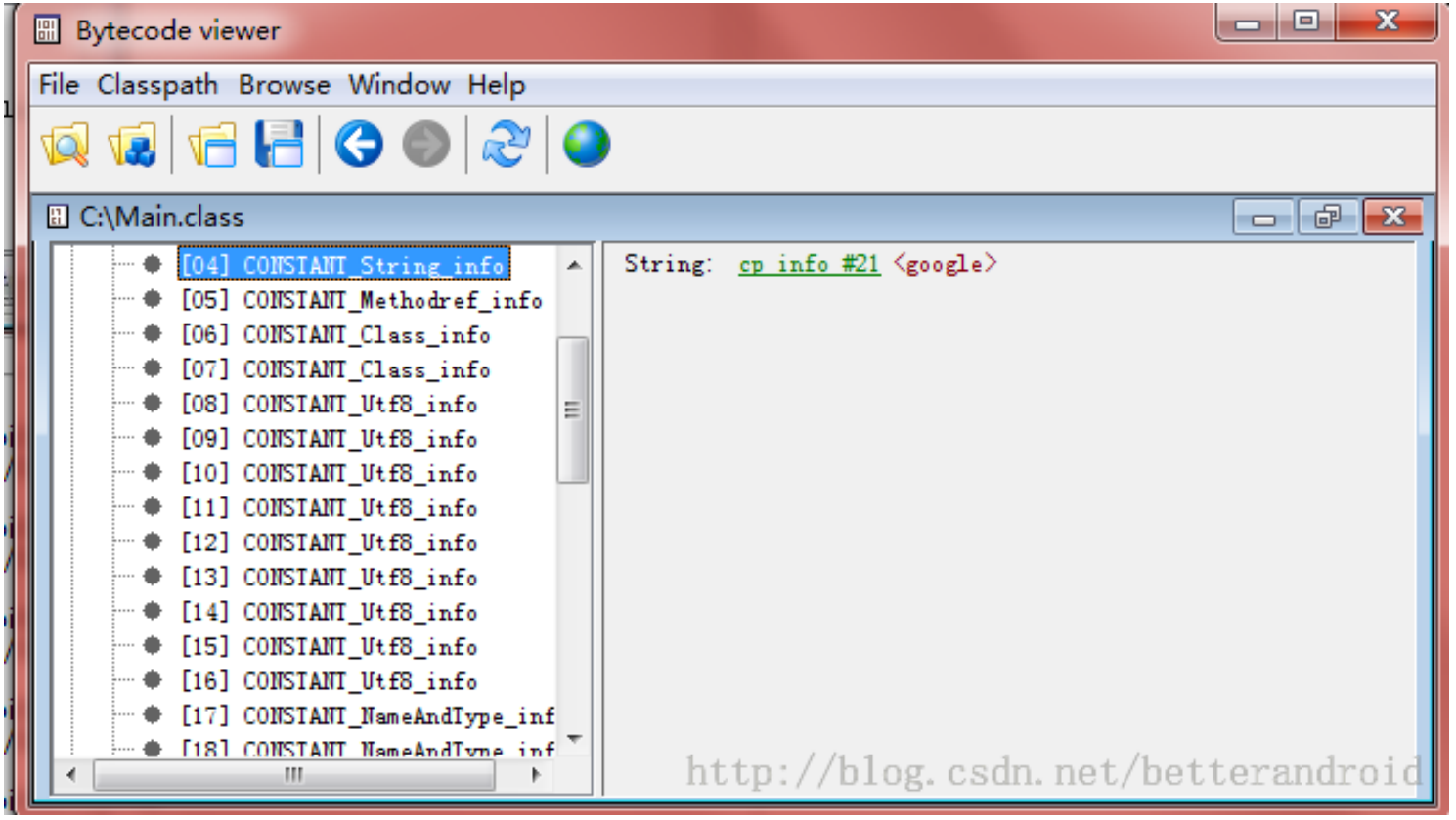
*Android框架设计模式（三）——Observer Method

*浅谈Storm流式处理框架

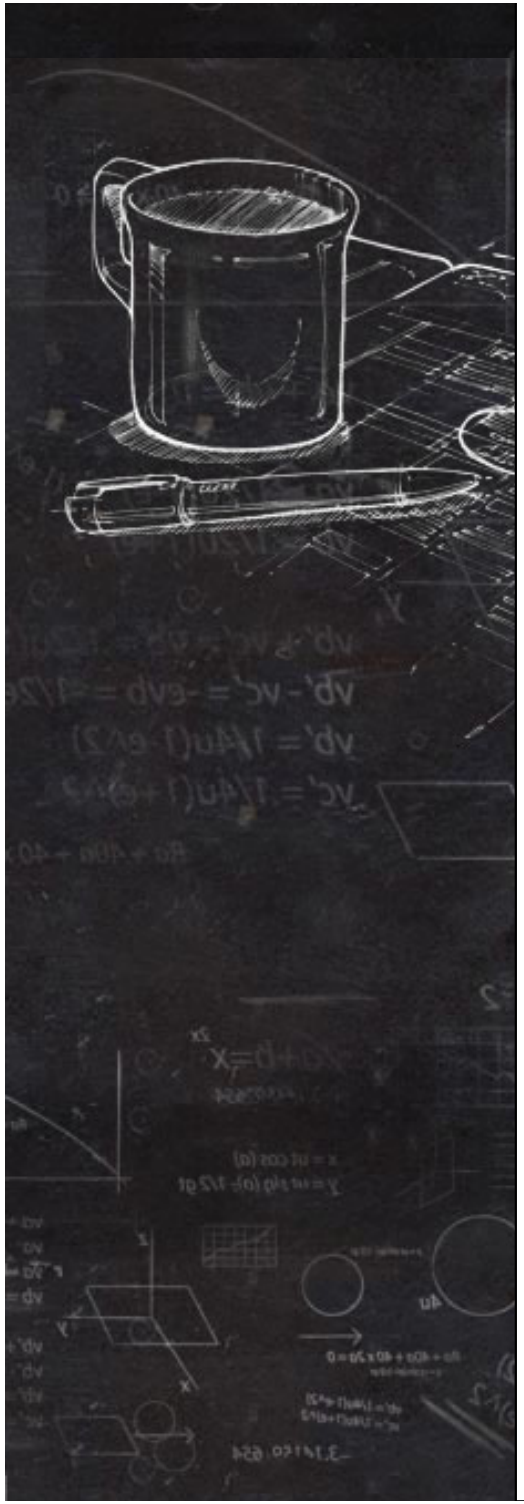
*有关深度学习领域的几点想法

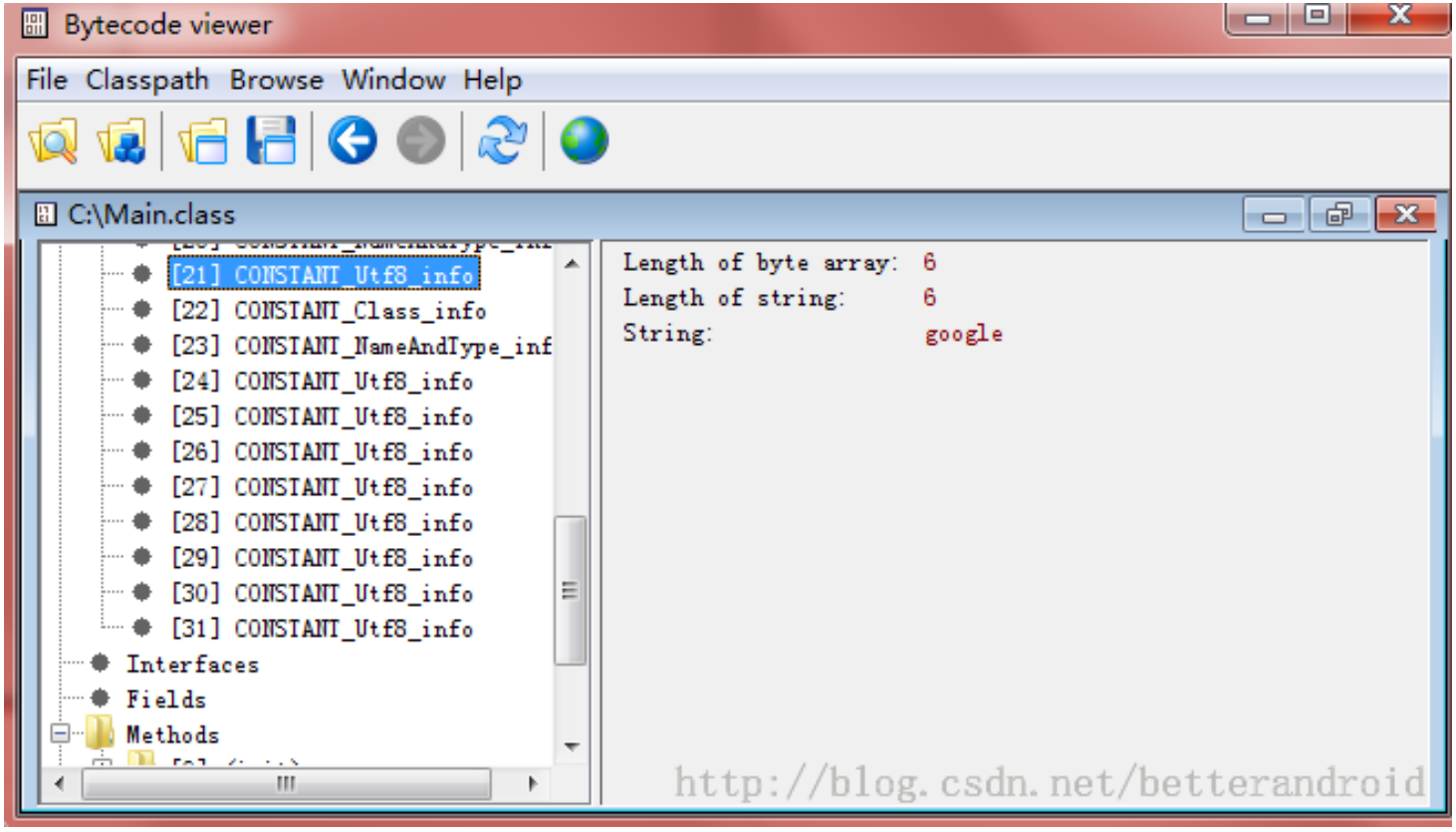
* 管理Java垃圾回收的五个建议

* 大数据并发问题

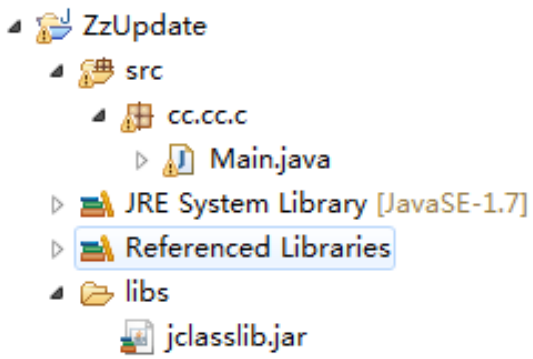


9、这时，我们看到的google字符是在[21]这个位置，并且CONSTANT_Utf-8_info，这些信息待会修改的时候 很有用。

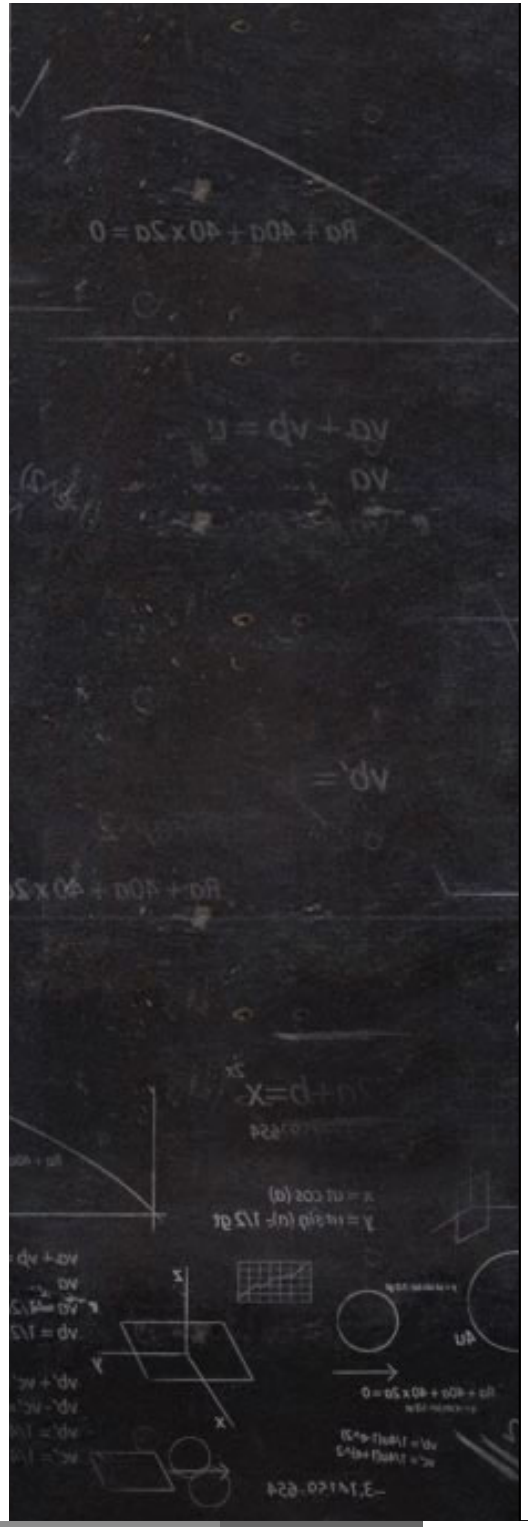




10、现在我们可以用代码去把 google 修改成 baidu。首先创建一个工程，把刚刚下载 jclasslib文件夹下bin目录下jclasslib.jar引入，如下图



11、Main.java函数代码如下



[java] view plain copy print ?

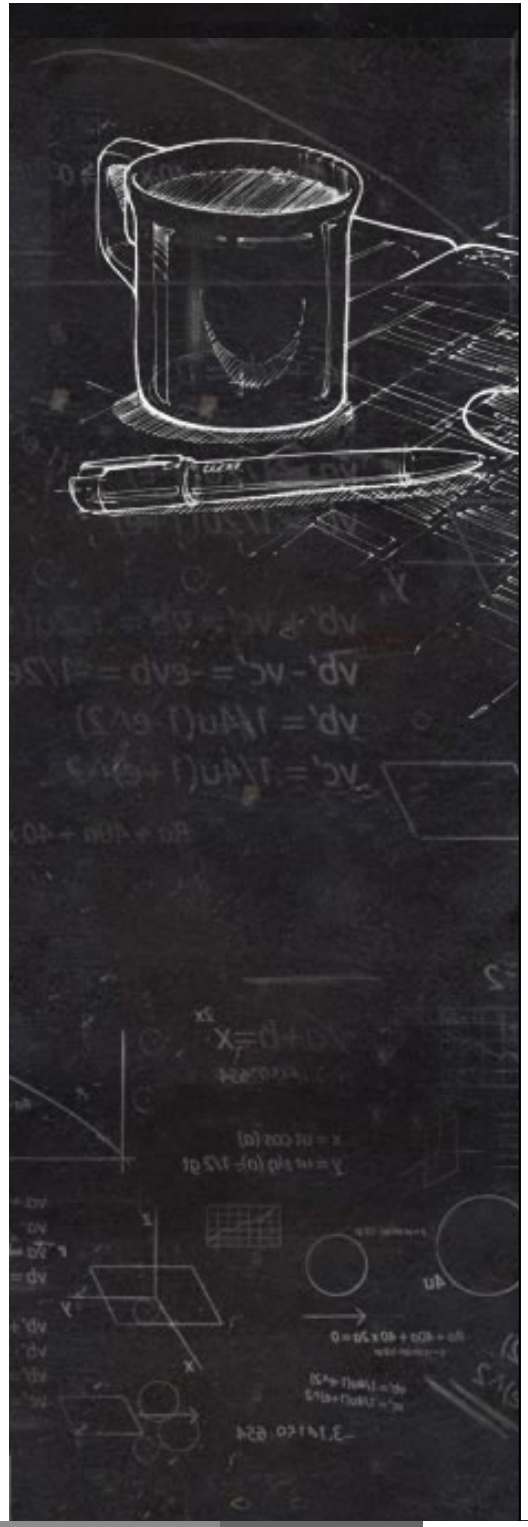
```java
package cc.cc.c;

import java.io.*;
import org.gjt.jclasslib.io.ClassFileWriter;
import org.gjt.jclasslib.structures.CPInfo;
import org.gjt.jclasslib.structures.ClassFile;
import org.gjt.jclasslib.structures.constants.ConstantUtf8Info;

public class Main {
    public static void main(String[] args) throws Exception {

        String filePath = "C:\\Main.class";
        FileInputStream fis = new FileInputStream(filePath);
        DataInput di = new DataInputStream(fis);
        ClassFile cf = new ClassFile();
        cf.read(di);
        CPInfo[] infos = cf.getConstantPool();

        int count = infos.length;
        for (int i = 0; i < count; i++) {
            if (infos[i] != null) {
                System.out.print(i);
                System.out.print(" = ");
                System.out.print(infos[i].getVerbose());
                System.out.print(" = ");
                System.out.println(infos[i].getTagVerbose());
                if (i == 21) {//刚刚找到的是21位置
                    ConstantUtf8Info uInfo = (ConstantUtf8Info) infos[i]; //刚刚那里是CONSTANT_Utf-8_info所以这里要用这个
                    uInfo.setBytes("baidu".getBytes());
                    infos[i] = uInfo;
                }
            }
        }
        //这种方式也可以，一样的
/*      if(infos[count] != null) {
            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.writeToFile(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。

上一篇 onWindowFocusChanged
下一篇 软件版本命名规范

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

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