# ReadRecord使用说明

ReadRecord用来读取执行记录文件，方法是按照记录格式对数据进行逐条解析，使用简介如下。

将ReadRecord.tar.gz在linux系统下解压得到ReadRecord可执行文件。

命令行：ReadRecord filename startid number output\_type

说明 ： ReadRecord 程序名

filename 记录文件路径

startid 所要读取的记录的起始序号（从1开始计数 ）

number 要读取的数据条目数量（number+1），输入0读取startid后面的全部

output\_type 按需求输出数据，模式如下表1所示

表 1输出模式表

|  |  |
| --- | --- |
| output\_type | 说明 |
| 1 | 输出 id, tid, eip, 汇编指令基本信息 |
| 2 | 输出 id, eip, 汇编指令，eax，ecx，edx，ebx数据 |
| 3 | 输出 id, eip, 汇编指令，esp，ebp，edi，esi数据 |
| 4 | 2和3 的叠加 |
| 5 | 输出id, eip, 汇编指令，3个操作数的值  （操作数为寄存器时忽略该值，部分未使用的opVal[i]值也为0） |
| 6 | 2，3，和5的叠加 |

例子如下图1 所示:

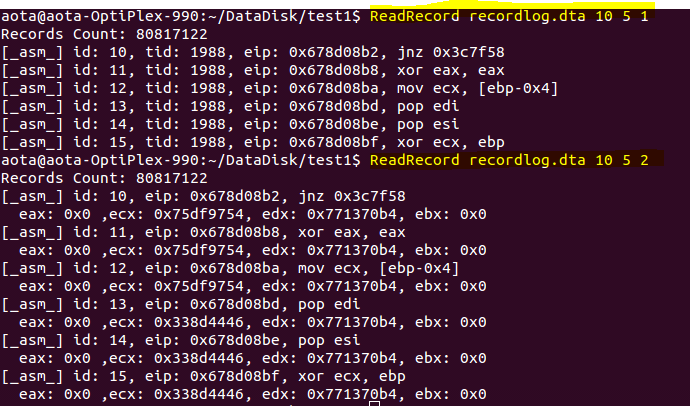


图 1 使用样例