汇编那些事

Tips on Assembly Language

张华平 副教授 博士

Email: kevinzhang@bit.edu.cn

Website: http://www.nlpir.org/

@ICTCLAS张华平博士

大数据搜索与挖掘实验室

2016-9

课程微信群（一周后过期）

汇编课程2016年

该二维码7天内(9月27日前)有效，重新进入将更新

从Apple密码门开始…

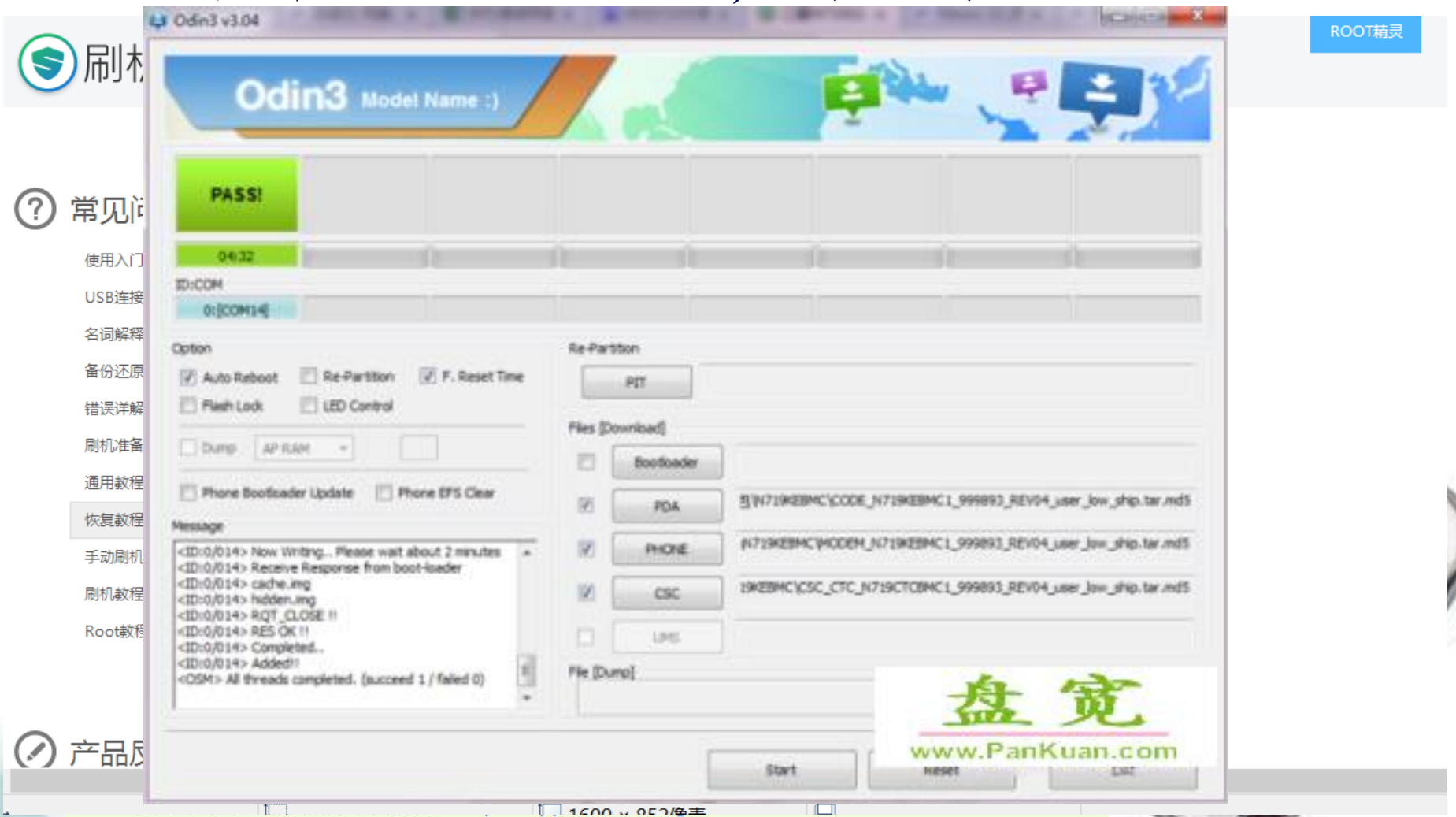
从棱镜项目看汇编...


返回央视网
首页
电视
电影
电视剧
动画片
纪录片
原创
游戏
爱西柚
动画片库
高清动画
央视热播
动画播出时间表
搞笑片
亲子片
怀旧片
口袋动画影院
动画电影
预告片花
热播榜
CCTV
新闻联播
焦点访谈
晚间新闻
新闻30分
朝闻天下
舞出我人生
百家讲坛
星光大道
今日说法
开讲啦
直播中国
CCTV-5
CCTV-1
CCTV-新闻
BTV体育
CCTV-3
CCTV-4亚洲
CCTV-6
CCTV-2
东方卫视
CCTV-9
中国网络电视台 > 环球记者连线 > 《环球记者连线》 20130614


正在播出:《环球记者连线》20130702
CCTV 13
新 闻
CNTV
北京理工大学计算机学院副教授 张华平
电话采访
环球记者连线
00:54
区失业率达到１２．１％，比修订过的４月份
00:44

合约机的坑里木有汇编老师...

- 大家掉过合约机的坑，有木有？



闲话教育

兴趣第一

- 感兴趣找方法，不感兴趣找借口；
- 教育第一原则是培养对科学或者具体学科的兴趣，扼杀青年的兴趣，罪莫大焉；
- 再好的学问，以面目可憎的形象出现，年轻人也不可能接受。佛家无色无相，却幻化万象，以渡众生。

闲话教育

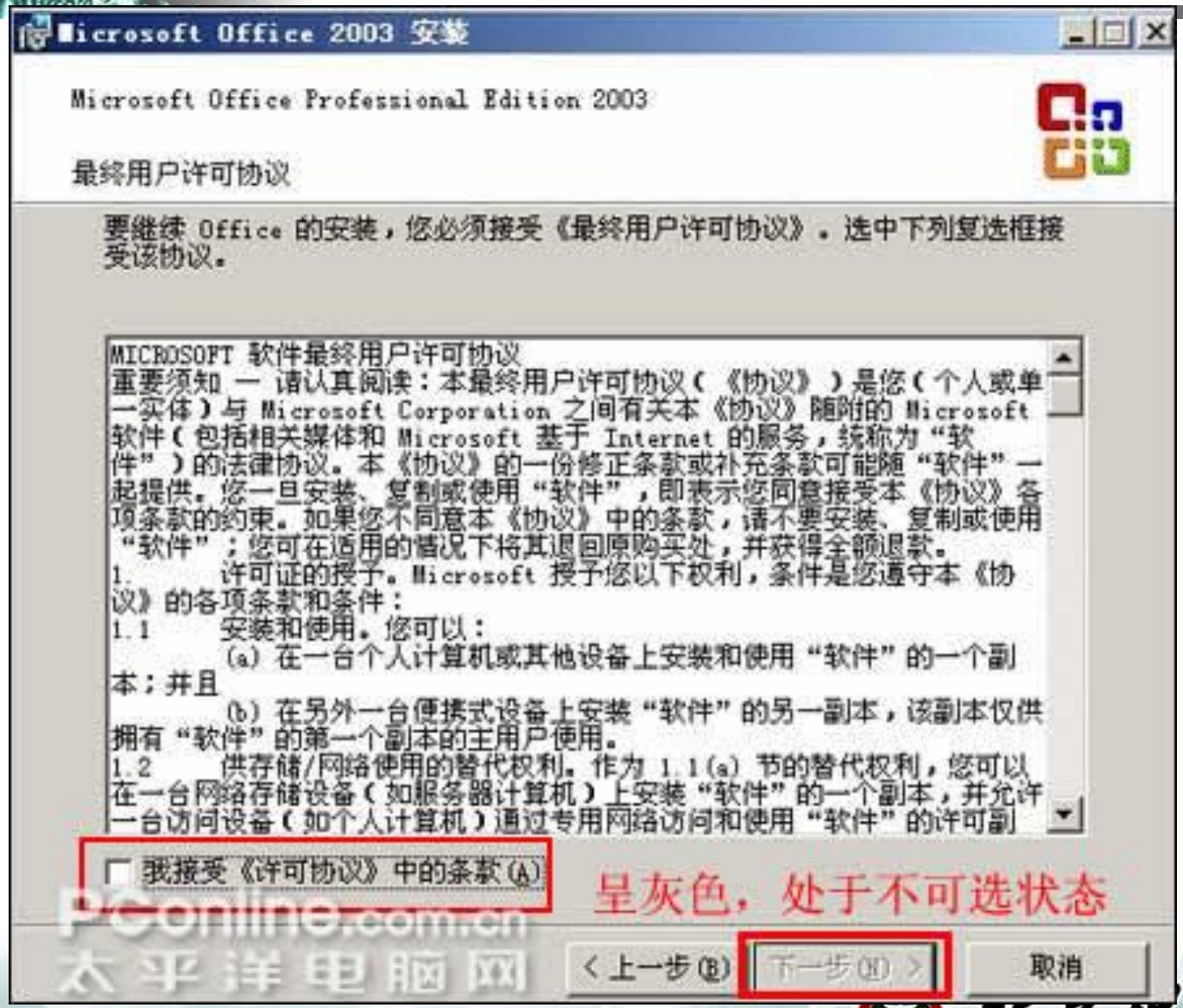
知行合一

- 明 王守仁《传习录》卷 教育家：陶行知
- 王守仁，号阳明先生，中国明代最著名的思想家、哲学家、文学家和军事家。陆王心学之集大成者，非但精通儒家、佛家、道家，而且能够统军征战，是中国历史上罕见的全能大儒。封“先儒”，奉祀孔庙东庑第58位。
- 计算机科学尤其强调知行合一。

闲话汇编

- 汇编不会编；其实汇编都会编；
- 计算机专业与非专业之三大差别：数据结构、汇编、编译；
  - 数据结构：解决问题的算法-原理；
  - 编译：软件如何编译，如何优化；
  - 汇编：软件更懂硬件；
- 1946年计算机发明以来，过去了60多年，高级语言已经可见即可得，为什么还要学汇编？

软件许可协议



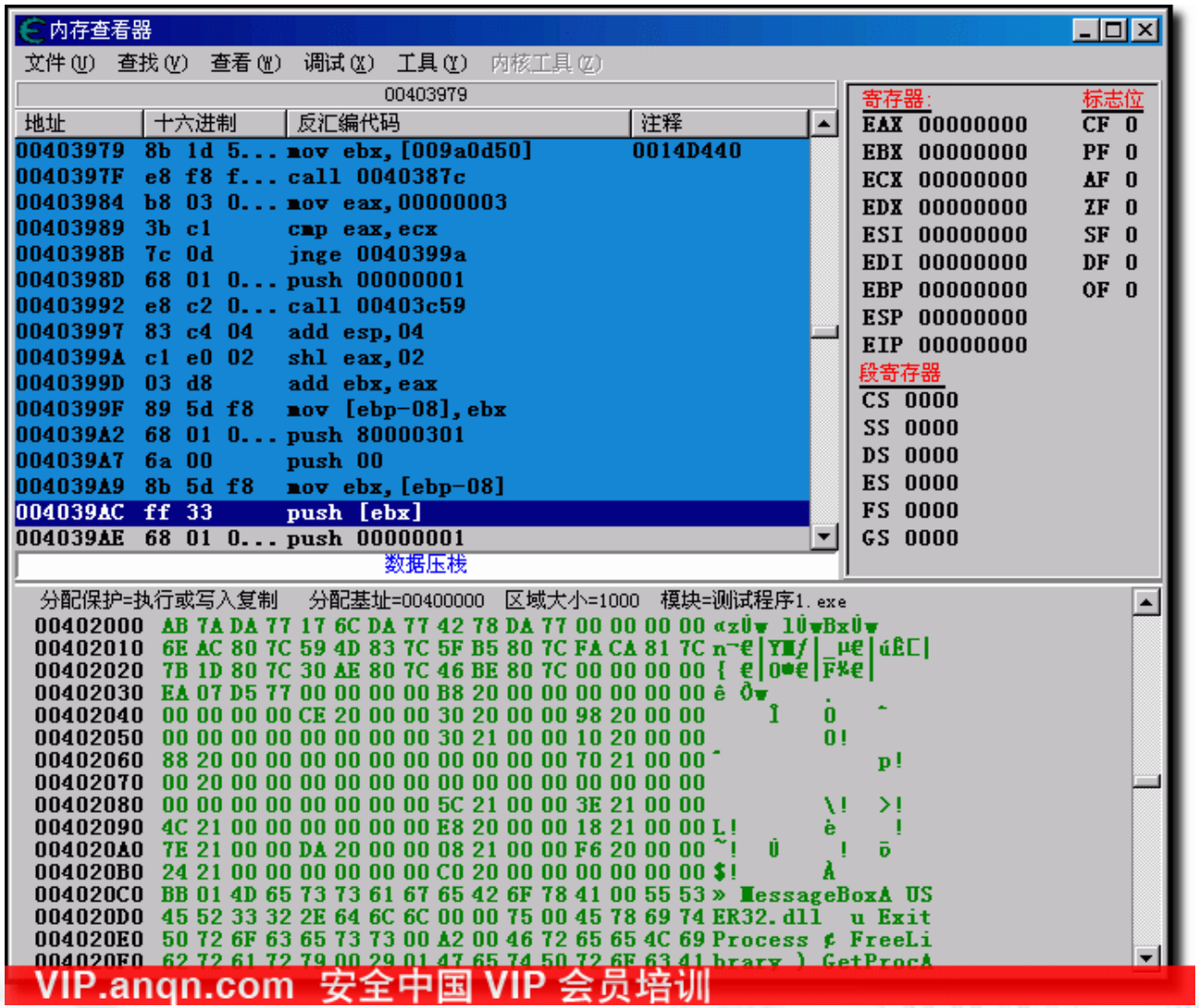
为什么都有下面这一条？

4. 对反向工程、反编译和反汇编的限制。您不得对"软件"进行反向工程、反编译或反汇编，除非适用法律明示允许，并仅在适用法律明示允许的范围内从事上述活动。

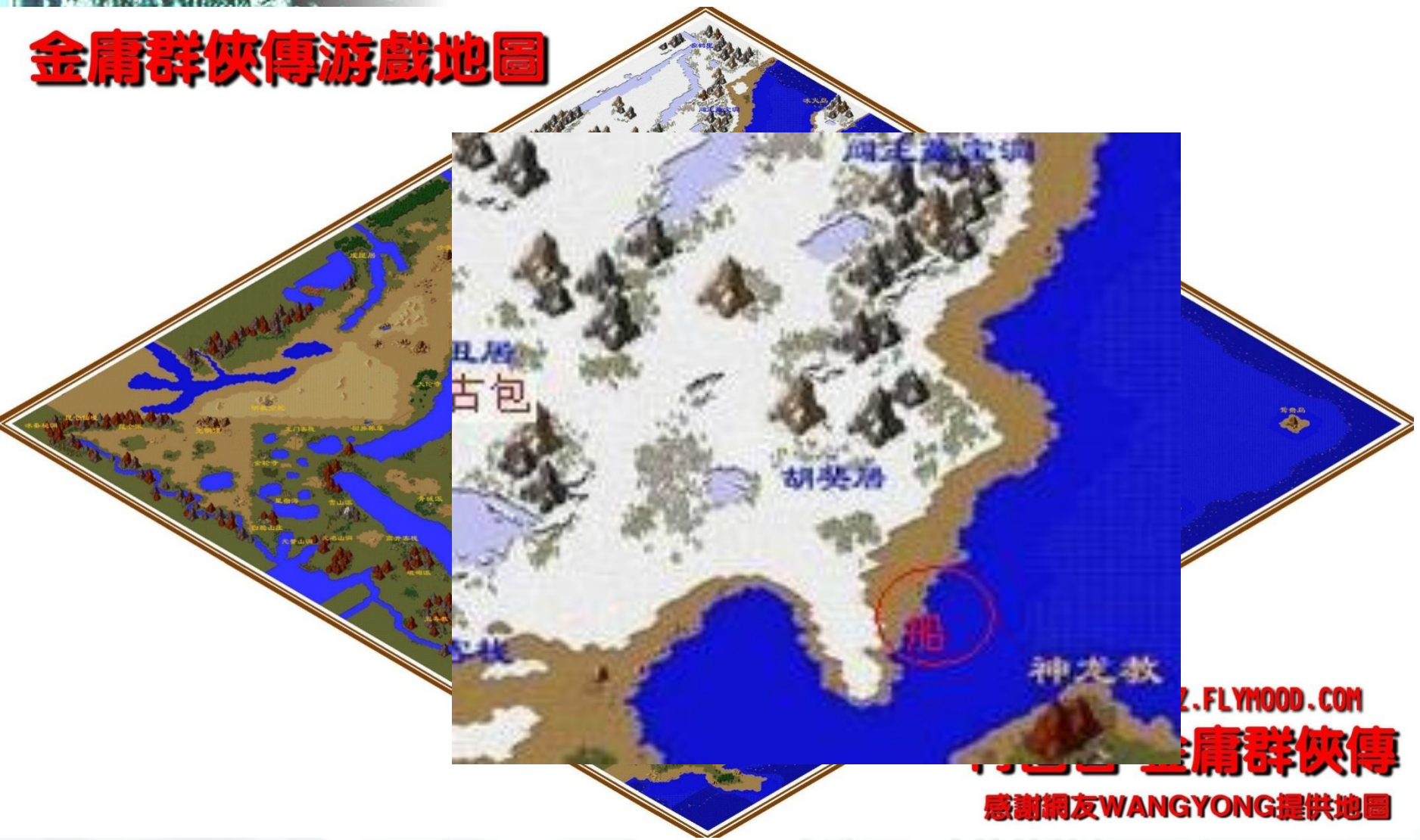
debug

```
08048414 <main>:
 8048414:       55                      push   %ebp
 8048415:       89 e5                   mov    %esp,%ebp
 8048417:       83 e4 f0                and    $0xfffffff0,%esp
 804841a:       83 ec 20                sub    $0x20,%esp
 804841d:       c7 44 24 1c 03 00 00    movl   $0x3,0x1c(%esp)
 8048424:       00
 8048425:       8b 44 24 1c             mov    0x1c(%esp),%eax
 8048429:       01 c0                   add    %eax,%eax
 804842b:       83 44 24 1c 01          addl   $0x1,0x1c(%esp)
 8048430:       03 44 24 1c             add    0x1c(%esp),%eax
 8048434:       89 44 24 18             mov    %eax,0x18(%esp)
 8048438:       83 44 24 1c 01          addl   $0x1,0x1c(%esp)
 804843d:       83 44 24 1c 01          addl   $0x1,0x1c(%esp)
 8048442:       b8 30 85 04 08          mov    $0x8048530,%eax
 8048447:       8b 54 24 18             mov    0x18(%esp),%edx
 804844b:       89 54 24 08             mov    %edx,0x8(%esp)
 804844f:       8b 54 24 1c             mov    0x1c(%esp),%edx
 8048453:       89 54 24 04             mov    %edx,0x4(%esp)
 8048457:       89 04 24                mov    %eax,(%esp)
 804845a:       e8 e1 fe ff ff          call   8048340 <printf@plt>
 804845f:       c7 04 24 00 00 00 00    movl   $0x0,(%esp)
 8048466:       e8 e5 fe ff ff          call   8048350 <exit@plt>
 804846b:       90                      nop
```

win-debug工具



金庸群侠传的故事



密码破译的故事

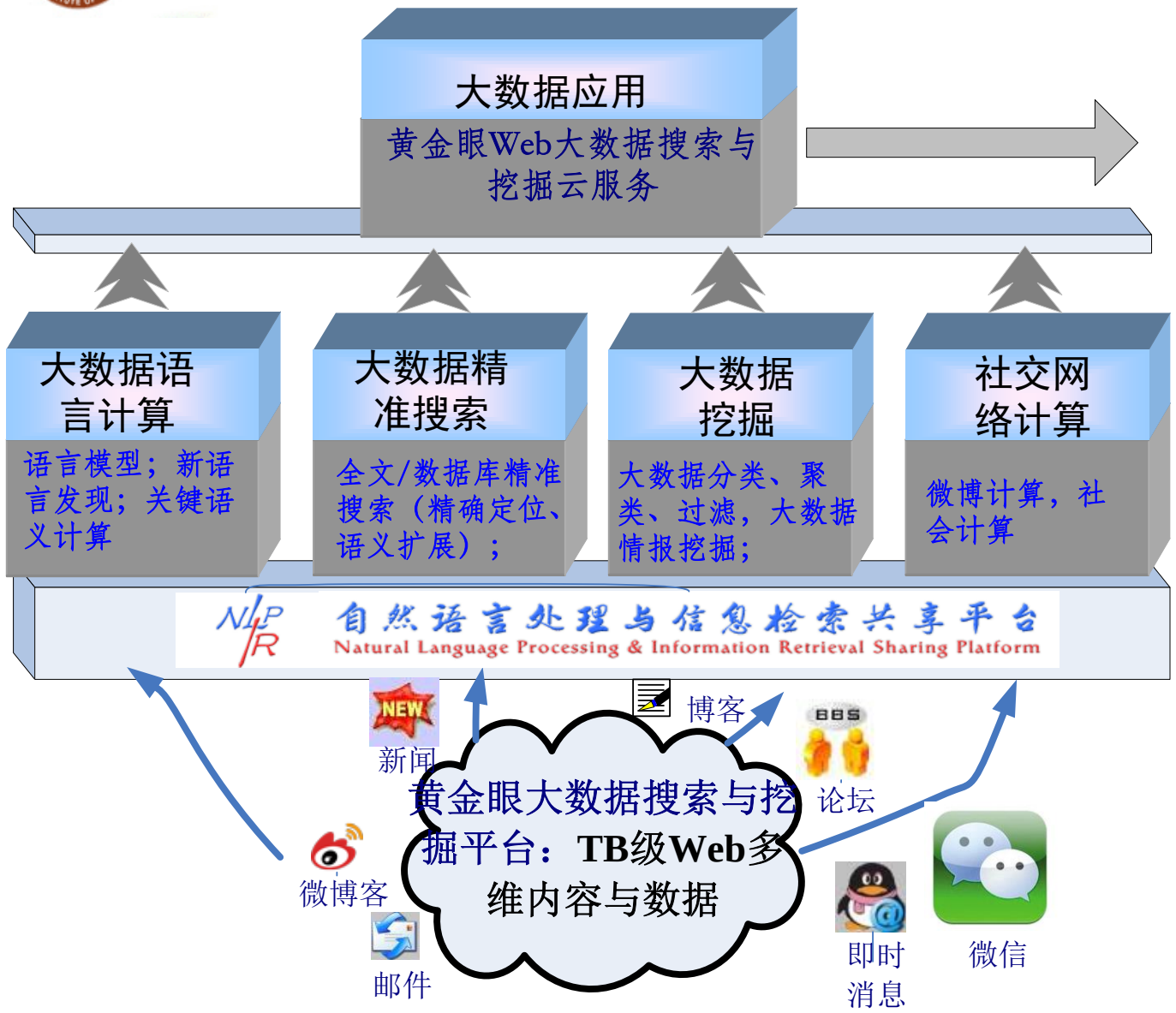
```
00007f70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007f80h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007f90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007fa0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007fb0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007fc0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007fd0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007fe0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007ff0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00008000h: 00 00 00 00 00 00 00 00 00 00 00 00 C1 1C 40 00 ; ............?@.
00008010h: B4 42 40 00 00 00 00 00 00 00 00 00 66 1D 40 00 ; 碆@.........f.@.
00008020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00008030h: 59 6F 75 20 61 72 65 20 69 6E 76 61 6C 69 64 21 ; You are invalid!
00008040h: 0A 00 00 00 48 65 6C 6C 6F 20 57 6F 72 6C 64 21 ; ....Hello World!
00008050h: 0A 00 00 00 59 6F 75 20 61 72 65 20 76 61 6C 69 ; ....You are vali
00008060h: 64 21 0A 00 42 49 54 00 25 73 00 00 50 6C 65 61 ; d!..BIT.%s..Plea
00008070h: 73 65 20 69 6E 70 75 74 20 70 61 73 73 77 6F 72 ; se input passwor
00008080h: 64 3A 0A 00 E9 26 40 00 01 00 00 00 20 09 2D 0D ; d:..?@..... .-.
00008090h: 5D 00 00 00 5D 00 00 00 60 AE 40 00 00 00 00 00 ; ]...]...`胤.....
000080a0h: 60 AE 40 00 01 01 00 00 00 00 00 00 00 00 00 00 ; `胤.............
000080b0h: 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000080c0h: 00 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 ; ................
000080d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000080e0h: 00 00 00 00 02 00 00 00 02 00 00 00 00 00 00 00 ; ................
000080f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00008100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00008110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

病毒如何检测识别？

- 基于机器学习的计算机恶意程序检测模型构建与实现–胡巍巍 学号：20082892
- 可执行程序转换为汇编代码，进行训练，特征识别，分类识别。

种类	频率	相对频率	提高
后门	96.63%	96.79%	0.16%
构造器	94.49%	94.92%	0.43%
木马	94.65%	95.88%	1.24%
病毒	97.23%	97.24%	0.01%
蠕虫	95.00%	95.73%	0.73%
其他	94.45%	95.12%	0.67%
平均	95.41%	95.95%	0.54%

北京理工大学 大数据搜索与挖掘实验室（BDSM@BIT）



中央网信办、央行
情报分析与风险控制

工信部、安全部
242及安全情报监测

河北科技支撑计划
海量异构文本挖掘

新疆高新技术计划
新疆维文舆情监测预警

973课题
社交网络分析基础研究

国家自然科学基金
基于主体个性化的微博情感分析算法研究

员工与学生

感谢关注聆听！

张华平
Email: kevinzhang@bit.edu.cn
微博：@ICTCLAS张华平博士
实验室官网：
http://www.nlpir.org

大数据千人会