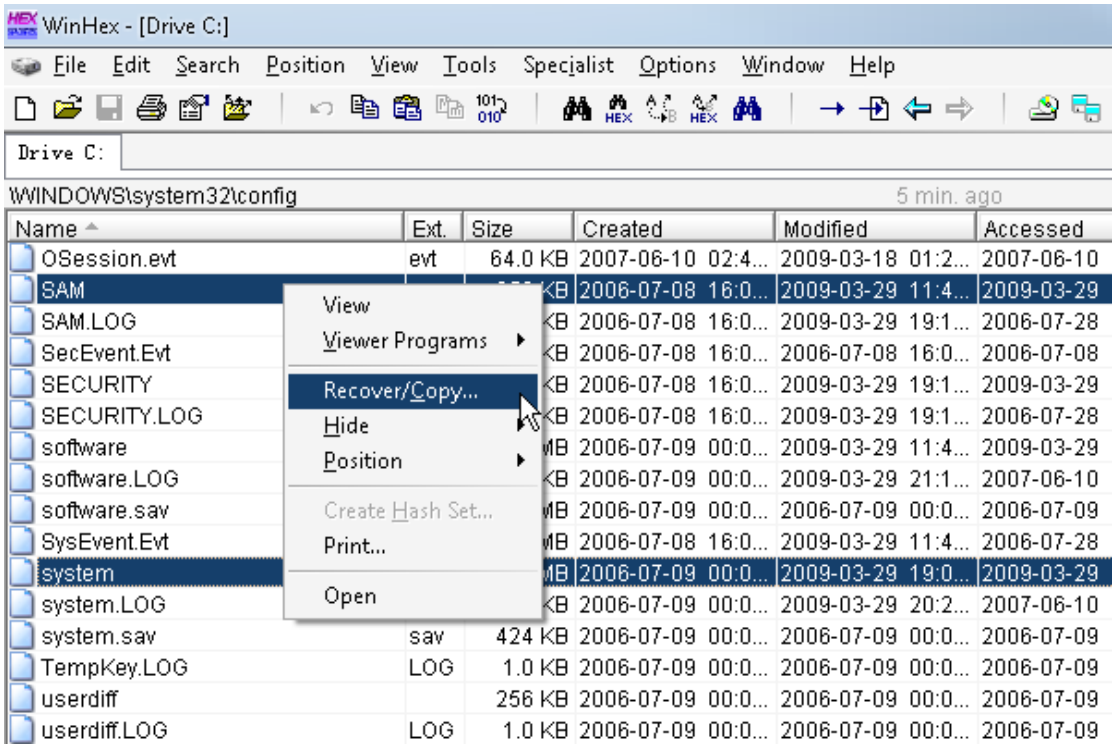
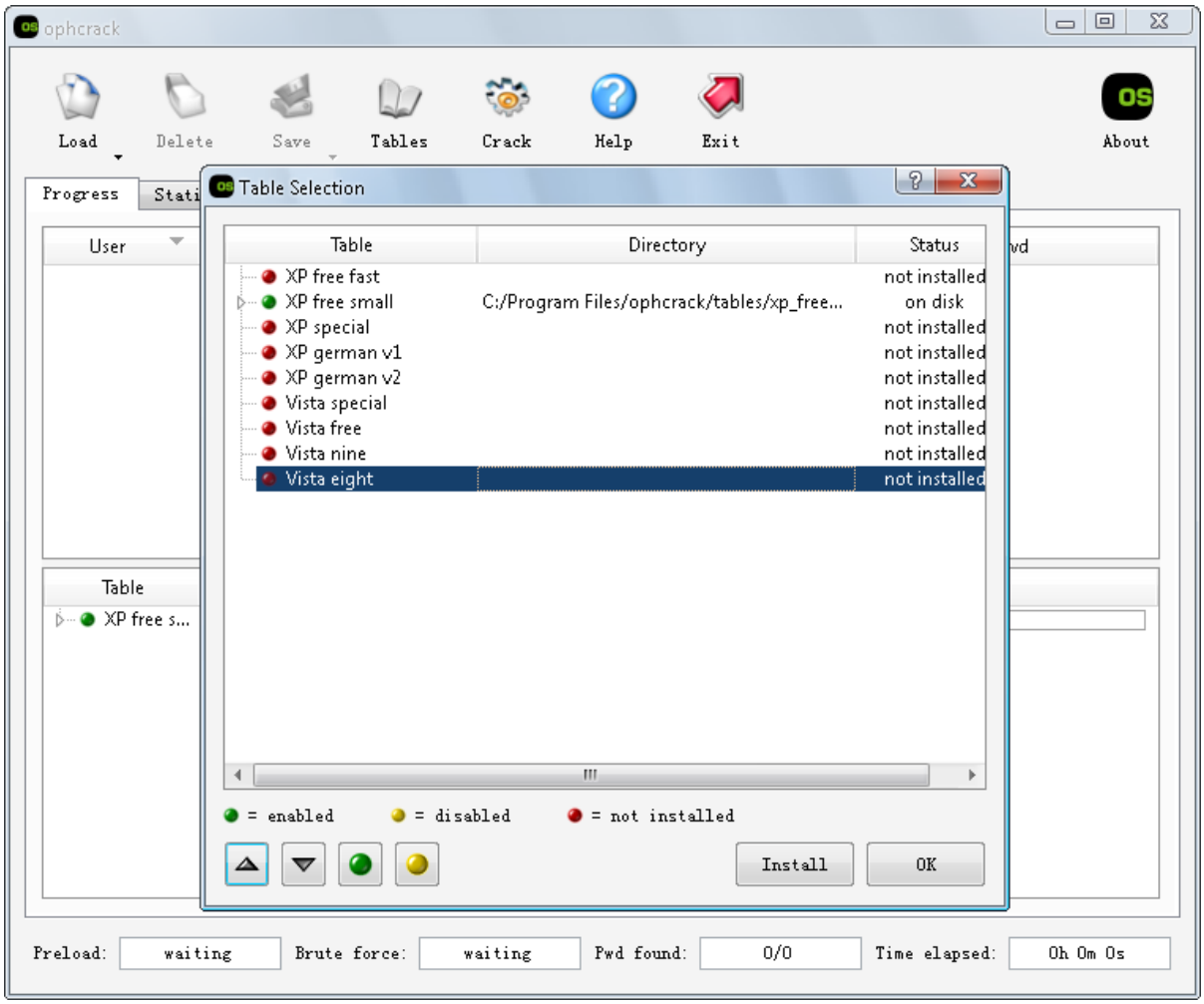
首先做一下准备工作
我们知道 windows 登录密码是储存在 C:\WINDOWS\system32\config 文件夹内的 sam 文件和 system 文件
当然直接复制粘贴是不行的
我们可以借助 winhex 来实现 sam 文件的复制和粘贴



利用 winhex 复制 sam 文件和 system 文件到 test 文件夹下备用

接下来请出今天主角
ophcrack http://www.xdowns.com/soft/8/114/2007/Soft_39348.html
把她下载安装一下
安装时会提示下载字典文件,选择最小的字典文件即可
当然也可以直接跳过,因为字典文件是可以在 ophcrack 官网上直接下载的

装完 ophcrack 后运行,点击 tables-->install 导入字典文件

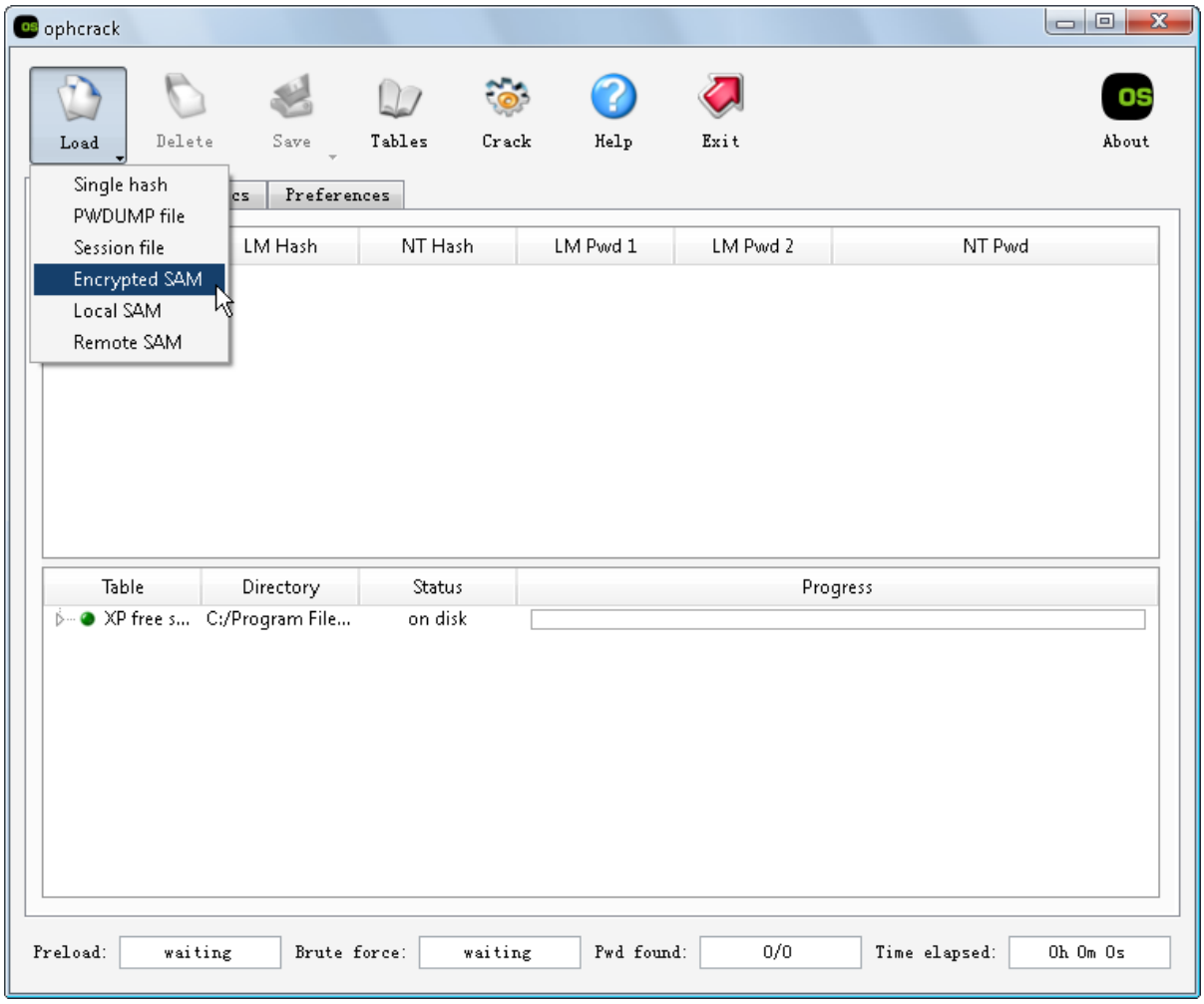


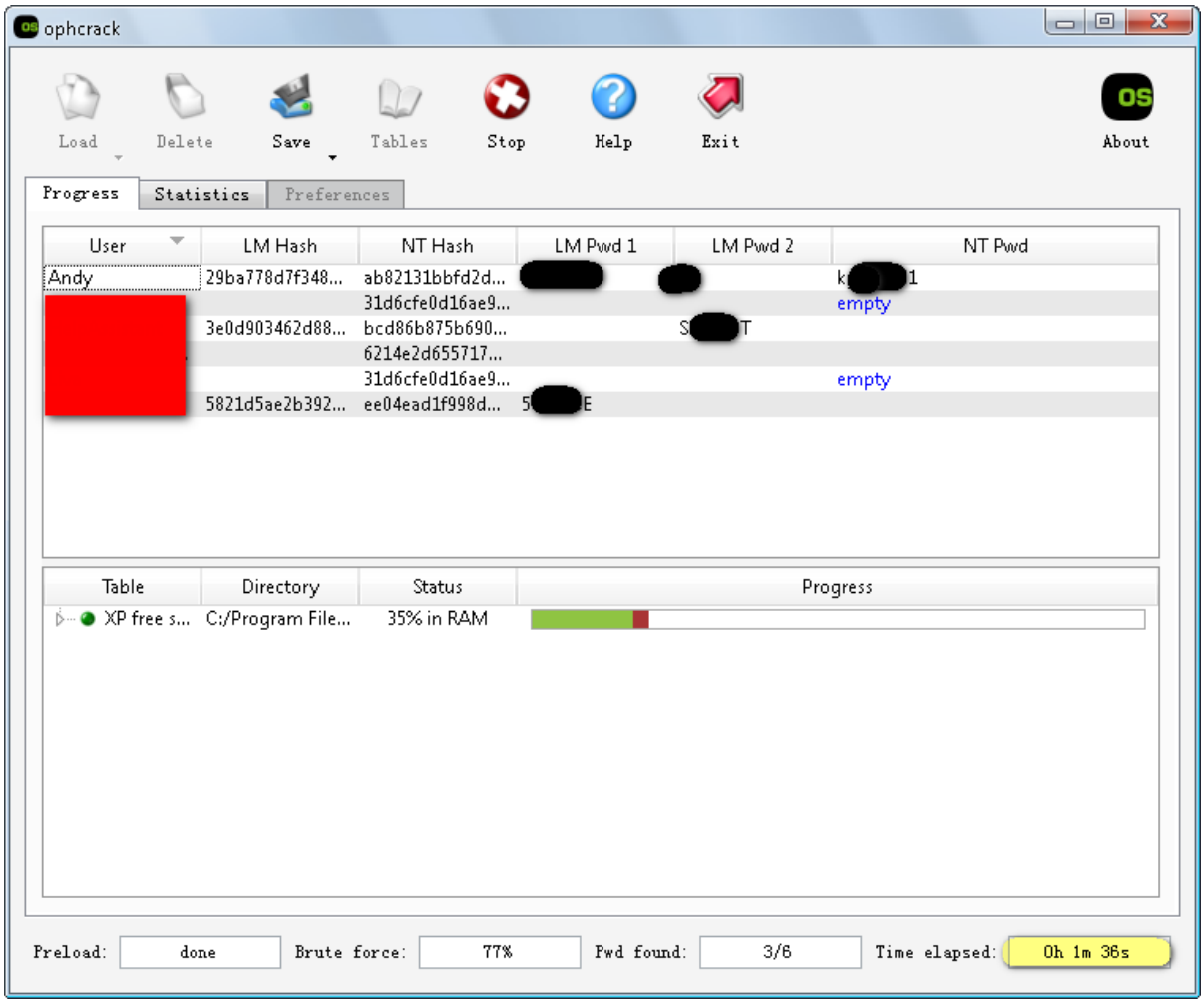
接下来就是破解了

运行 ophcrack 点击 load-->encrypted sam-->再选择刚才准备好的 sam 文件

之后点 crack 等着就好了

我的密码只用了 1 分半钟就跑出来了...汗.....


ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Single hash
PWDUMP file
Session file
Encrypted SAM
Local SAM
Remote SAM
Preferences
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Table
Directory
Status
Progress
XP free s...
C:/Program File...
on disk
Preload:
waiting
Brute force:
waiting
Pwd found:
0/0
Time elapsed:
0h 0m 0s



如果你的 windows 密码设置的比较强壮 ophcrack 跑不出来的话还有更暴力的
就是直接对 msv1_0.dll 施暴
此文件在 C:\WINDOWS\system32 文件夹内
我已经修改好
直接用 replacer 替换就可以了
重启后再次登陆的时候已经不需要密码了