全部的回忆：优化 Windows PIN 的恢复过程

© 2020 Passcape Software
Passcape Software

© 2020 Passcape Software

1 全部的回忆：优化 Windows PIN 的恢复过程

1.1 摘要

PIN是指个人识别号码。但它不仅仅是一个数字。它最早出现在Windows 8中，并在Windows 10中成为一种普遍的登录方式。与密码认证相比，PIN有很多优点。只要阅读 MS的文章，就可以获得更详细的相关信息。

1.2 恢复 Windows PIN

1.2.1 Windows PIN安全

对于那些懒得看文章的人来说：PIN码的主要优点之一是它更难破解。与 NTLM 密码 hash值相比，难度大约是100000倍。 因此，常规的恢复Windows密码的方法并不适合用于PIN码的解密。在这篇文章中，我们将展示如何使用新版本的 Reset Windows Password来减少恢复一些PIN码所需的时间。

1.2.2 根据日期恢复PIN

我们注意到，很多用户使用出生日期创建他们的Windows PIN码。他们自己的、亲戚的、宠物的，都无所谓。通常，这种PIN码由6个或8个数字组成。例如，12061999，05112018，等等。然而，即使是这样简单但被遗忘的PIN码也很难猜到，假设你在一个普通的CPU上每秒钟最多能猜到200-250次。

因此，解密一个8位数的PIN码需要10^8/200=500000秒或超过5天的时间！ 让我们把这个时间减少到一些合理的值，比如说最多5小时。为此，我们需要一个 掩码攻击 。

1.2.3 优化恢复过程

我想到的第一件事是设置一个数字掩码，即第一个字符是数字，第二个字符也是数字，例如：如下示例

%d%d%d%d%d%d%d%d

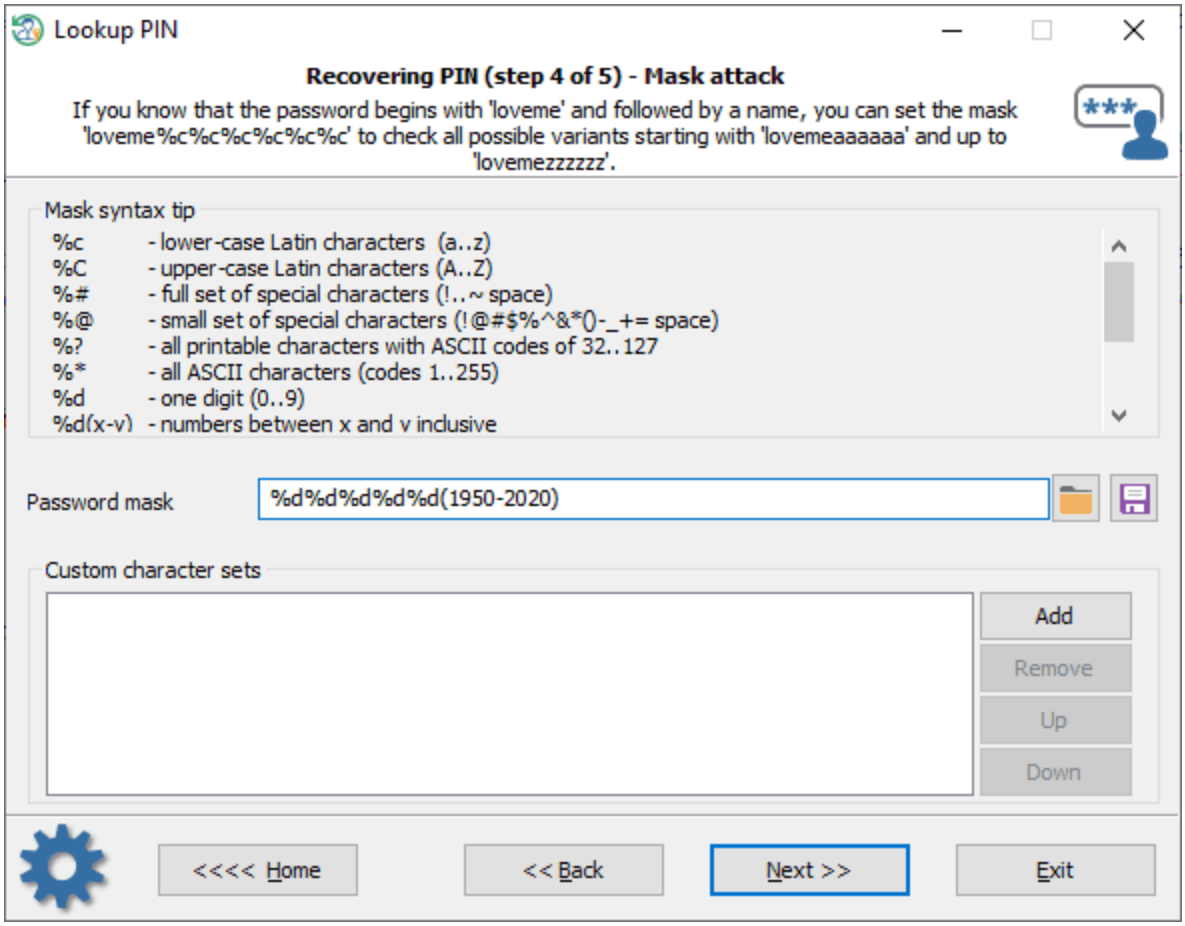
请注意，%d表示密码中的一个数字。总共8个数字。
这个掩码给了我们100 000 000种组合。要检查所有的组合需要5天时间，这就太多了。

假设1：最后四位数字应该是年份
我们需要：将最后四位数字限制在某个年份范围内
执行_1: **%d%d%d%d%d%d(1800-2030)**
%d(1800-2030)表示我们将检查从1800到2030的数字

很难想象有人会在19世纪出生，那么，更严格的限制呢？

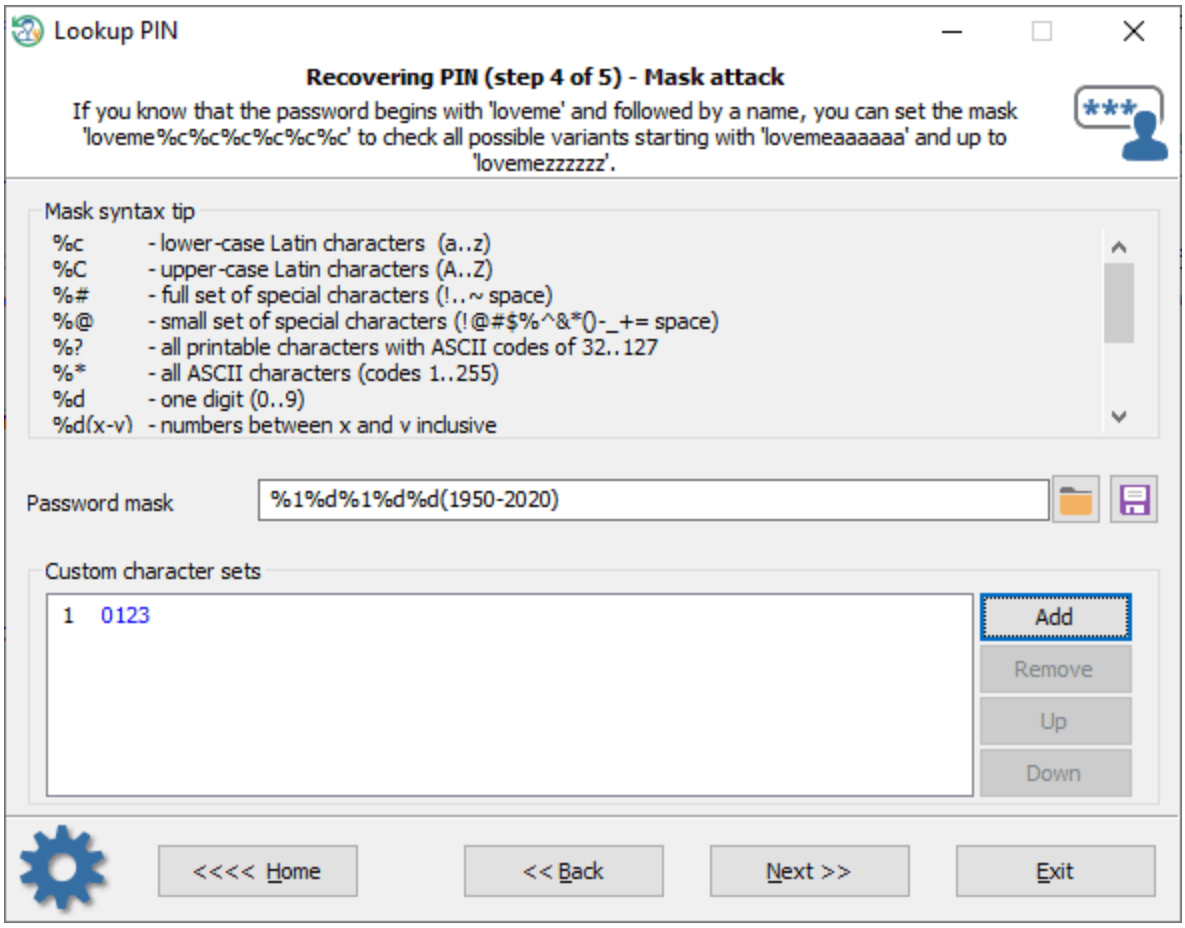
© 2020 Passcape Software

执行2: %d%d%d%d%d%d(1950-2020)
试想一下，我们已经将搜索范围从100 000 000减少到710 000。现在我们可以在不到一天的时间内完成所有的密码组合。



好了，现在是更难一点的事情。
假设 2: 前两个数字和后两个数字应该是一天和一个月。或者反之亦然。在一些国家使用mmddyyyy格式，在另一些国家使用相反的格式，即ddmmyyyy。总之，第一个和第三个数字都可以是0、1、2或3。
执行 1: **%1%d%1%d%d%d(1950-2020)**
其中%1是以下自定义字符集：0123

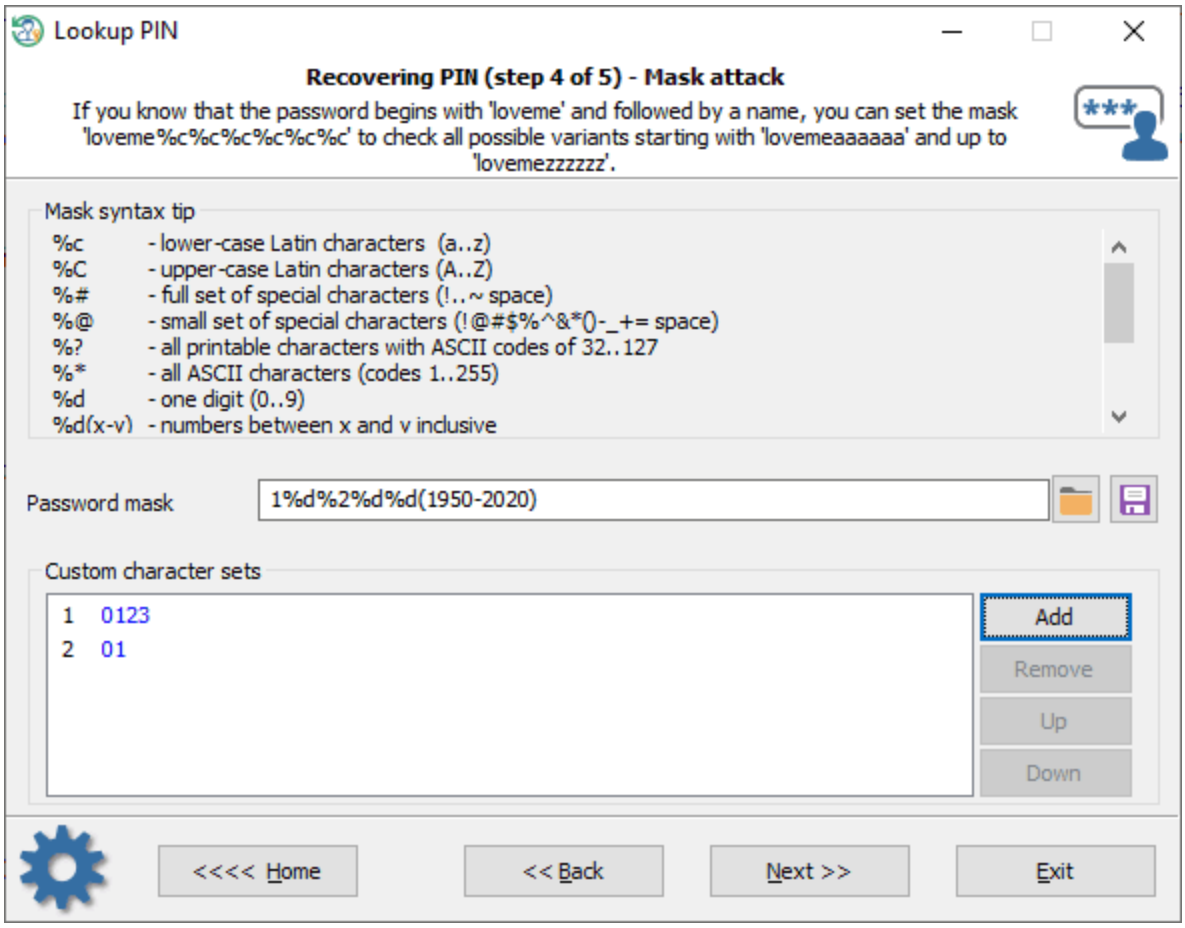
© 2020 Passcape Software



需要更严格的限制吗？

执行 2: **%1%d%2%d%d(1950-2020)**
其中%1等于0123, %2为0或1

© 2020 Passcape Software



现在总共只有56800个组合。

1.3 总结

好吧，你明白了这个意思。同样的技术也可以应用于恢复6位数的PIN。

照顾好自己，保证你的数据安全!

© 2020 Passcape Software