



IE7 密码恢复

北京天宇宁企业技术秘密保护咨询服务中心

电子证据调查文摘汇编

2009年9月

IE7 密码恢复

简介

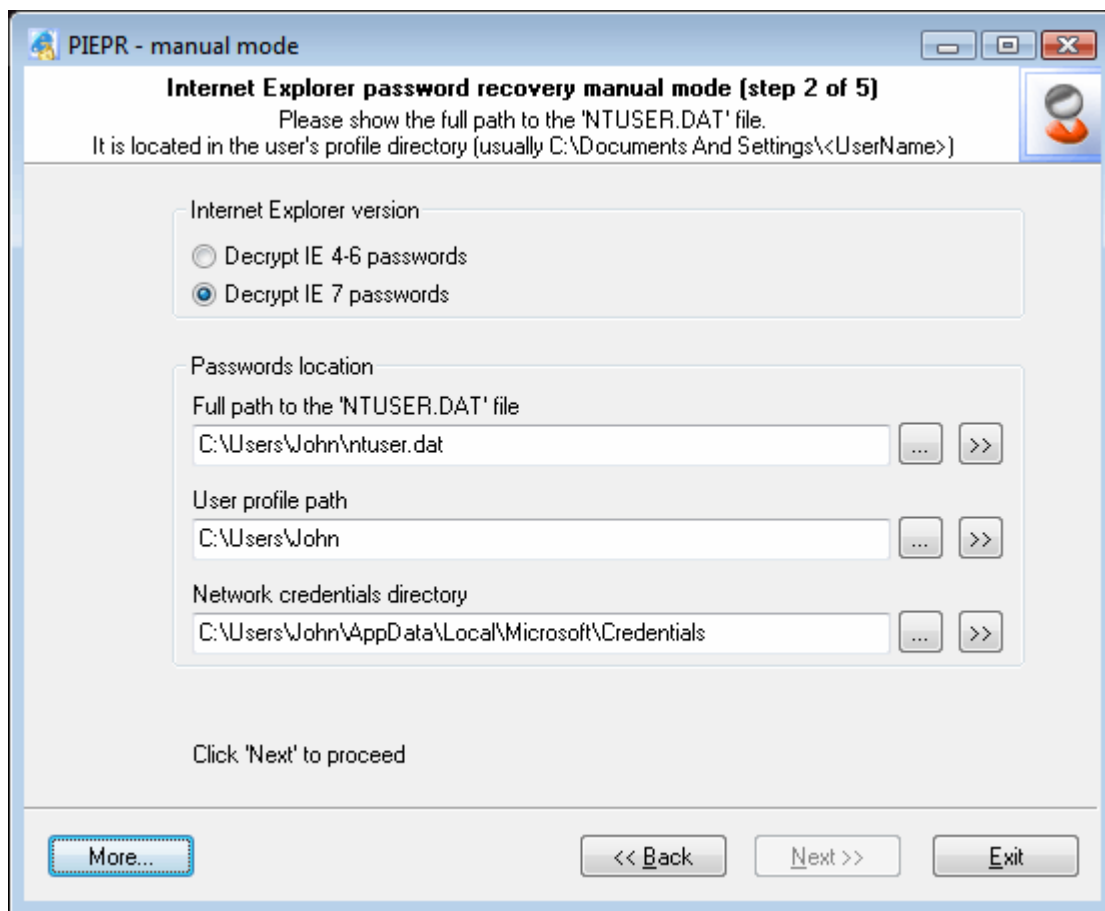
与其兄弟版本不同，IE7 新版使用了完全不同的对隐私数据加密的概念，即“不保存加密密钥”。这使得恢复该类型的口令难上加难，尤其是在自动模式下。因此，为了确保对口令的完全恢复，我们在应用程序向导里添加了手动操作模式。这使得恢复工作更加灵活，因为它使用了一些特别设计的算法并允许抓取密钥，这在自动模式中是无法实现的。

配置给 IE7 的手动模式可以在理论上分为 5 部分或者 PIEPR 5 步向导。更加精确的说，是 4 步，在第一步中你将选择操作模式。

步骤 1: 选择手动操作模式



步骤 2: 设定数据位置



手动恢复的第二步，你会被提示输入三个用于口令恢复工作必需的参数。实际上，软件会尝试自动获得所有的必需数据。不过，如果自动获取失败的话，它将会要求你手动输入这些必需的数据：

1. **注册表文件路径**(ntuser.dat)，它位于用户的信息目录中。用户的注册表中保存了三类已加密的 IE7 口令（总共有 4 个）。在 Windows XP-2003 中，指向该文件的路径通常是这样的：*C:\Documents And Settings\%USER%\ntuser.dat*，其中 *%USER%* 代表你的账户名。在 Vista 系统中，默认路径可能看起来有所不同：*C:\Users\%USER%\ntuser.dat*。该参数是强制性的，必须要输入才能使恢复工作继续。
2. **指向用户注册信息的路径**（可选参数）。软件通常通过用户注册表的位置自动能够检测到该路径(见上文)。用户的注册信息的文件夹是在下一步中将出现的一些选项的自动检测的开始点。如果没有设置该参数，恢复向导将不能在第三步中找出指向用户的 **Master Key** 的路径，而且进一步的恢复工作也只有在该参数已被提供的前提下才能进行。
3. **网络证书目录**（可选项）。Windows 证书管理器创建并管理这个文件夹，在其中保存了许多应用程序的隐私数据。这其中可能包含了域和 LAN 口令、.Net Passport 账户、Exchange 服务器的口令、认证证书等等。所有这些数据都已被加密并保存在网络证书目录里。在我们的案例中，我们特别关注 IE7 的网站口令，它也被称作

Wininet 证书。关于 Wininet 证书的更多信息，请查看我们关于 IE 口令的其他文章。在 Windows XP-2003 中, Wininet 证书可被保存在两个不同的目录里：

C:\Documents And Settings\%USER%\Application

Data\Microsoft\Credentials\%SID%

或者

C:\Documents And Settings\%USER%\Local Settings\Application

Data\Microsoft\Credentials\%SID%。

请注意 %USER% 代表你的 Windows 账户名， %SID% 是用户的 SID。

在 Vista 系统中，SID 并没有用到网络证书目录名中，所以指向已加密的 Wininet 证书数据的路径可能有一些不同，它们是：

C:\Users\%USER%\AppData\Local\Microsoft\Credentials 和




C:\Users\%USER%\AppData\Roaming\Microsoft\Credentials。

以下是两个指向网络证书目录的实际案件中的路径名：

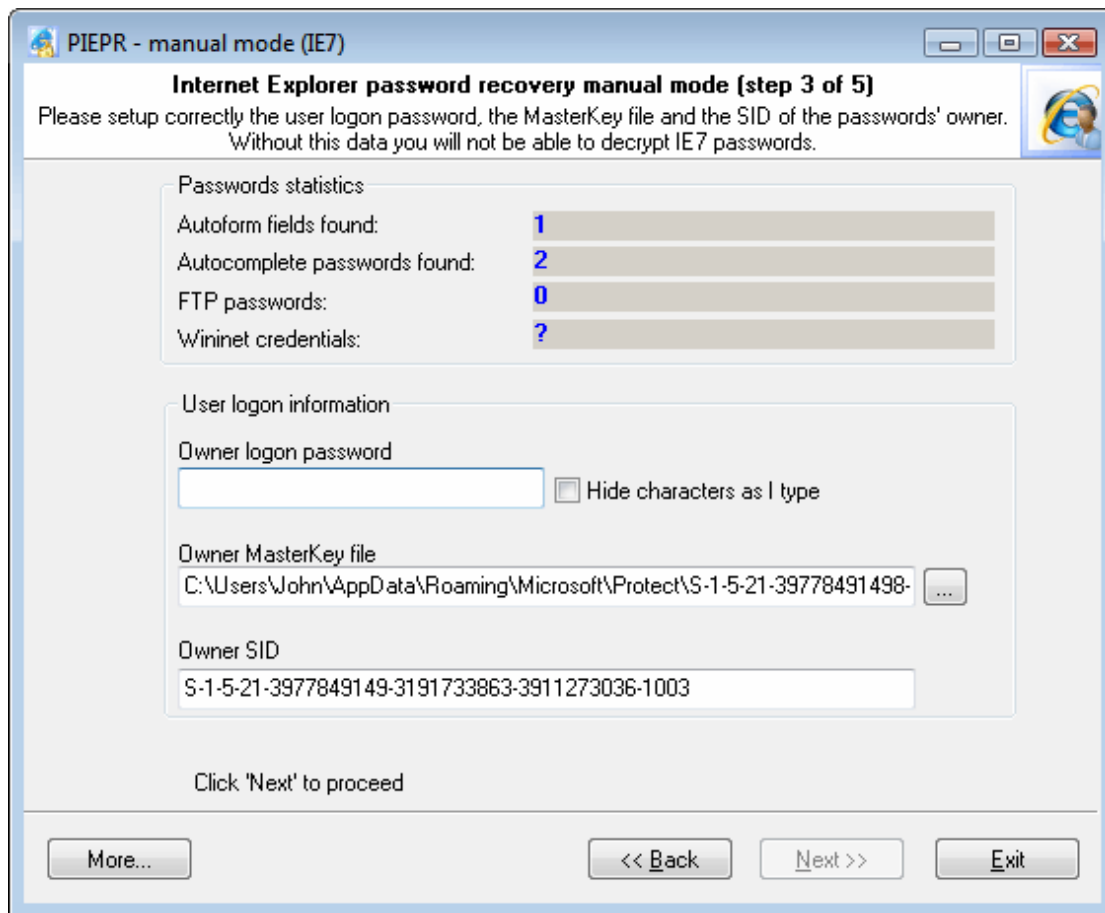
C:\Users\John\AppData\Local\Microsoft\Credentials

D:\Documents and Settings\Kate\Application

Data\Microsoft\Credentials\S-1-5-21-1927147842-1992852531-225342917-1003。

使用  键寻找本地用户的网络证书目录非常方便。当你点击  按钮，你将会被提示选择所需的本地用户的个人资料，而且软件也将自动选择与此相应的网络证书目录。如果恢复工作中所要求的数据需要从其它电脑上得到，你就必须手动输入指向网络证书目录的路径（通过点击按钮 ）。

步骤 3：恢复用户的 Master Key。显示出找到的口令。



在第三步中，恢复向导会尝试从你之前提供的数据中找出是否存在任何 IE7 的口令及其数量。此处会口令统计会显示出找到的口令信息数量（但还没有进行恢复）。

软件可以找出大量有效的 Wininet 证书，但前提是：

- 在向导程序之前的步骤中输入了正确的网络证书目录参数。
- 在用户登录信息对话框中完成所有选项，包括用户口令。

通常，软件将自动找到用户 *MasterKey* 文件和用户 *SID*。当然，你也可以手动操作。根据默认，用户的 *Master Key* 文件保存在如下文件夹中：

Windows XP-2003:

C:\Documents and Settings\%USER%\Application Data\Microsoft\Protect\%SID%

Vista:

C:\Users\%USER%\AppData\Roaming\Microsoft\Protect\%SID%

Owner *SID* 参数通常与 *%SID%* 文件夹名一样。只要在 User Logon Information 段中输入了正确的口令，软件就会计算 Wininet 证书的数量，而且按钮 'Next >>' 即下一步键将可用，然后你可以继续向导程序的下一步--寻找加密密钥。

步骤 4: 搜集加密密钥

搜集加密密钥是整个恢复过程中最关键最具决定性的一步。如上文中提到的, 在 IE7 中的加密机制是有意被设计成: 在任何有可能的时候, 应用程序都不会在本地计算机上保存加密密钥。所以, 当你开始搜索密钥之前, 你必须先了解 IE 对口令加密和数据加密的操作概念。暂时, 你可以忘记 **FTP** 和 **Wininet 口令**, 从恢复向导的第四步开始, 软件已有了足够的信息来恢复这些密码。

在 IE7 中的自动完成口令的加密算法如下:

1. 在第一次访问某网页时, 用户一旦输入了口令, IE 就会保存当前网页的**网址**并计算该地址的哈希值 **hash=SHA(URL)**。
2. 上一步保存的**网址**(一个基于 Unicode 的文本字符串)被作为加密密钥使用。该密钥被用来通过强大的加密算法(DPAPI) 对口令进行加密。已加密的口令=DPAPI (URL, 口令)。
3. 已加密的口令与哈希值一起, 被保存在用户的注册表中。
4. **网址**将被认为不再需要而清除。

上述唯一能够得出的结论是: 除非有人知道原始网址, 否则将不能恢复口令, 而且, 仅根据网址哈希值来破解口令也是不可能的。另一方面, 并不是总是需要将加密密钥(网址)都保存在本地计算机上。

但是 IE 究竟是怎样恢复其自身的口令的呢? - 其实很简单:

当再次访问该网站时, IE 会再一次计算**该网址**的哈希值, 然后它会将得到的哈希值与保存在注册表中的值(哈希值+已加密的口令)进行对比校验。如果其中一项哈希值匹配, 与之关联的加密的口令将被恢复出来。

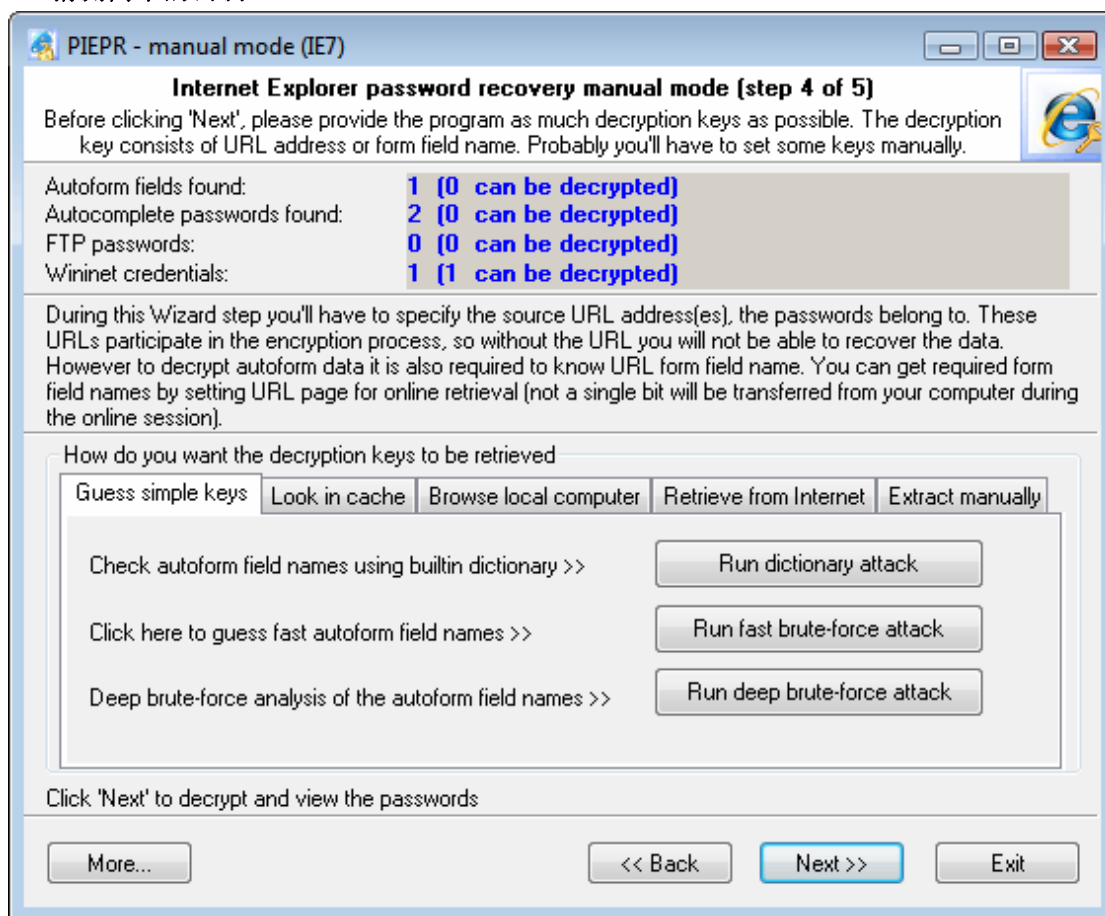
对**自动完成数据**的加密采取了一个稍有不同的方式。比如说, 认证页面有输入登录用户和口令的字段, 登陆用户和口令采用不同的加密方式。最根本的不同即是软件给加密密钥的域名采用了 HTML 形式而不是 URL。让我们来看一份包含有登陆用户和口令的html 文件样本。

```
<table><tr>
<td><input type="text" name="loginname" value=""><br></td>
<td><input type="password" name="pwd" value=""><br></td>
</tr></table>
```

在本例中, 字段名和密钥将以文本形式 loginname。此外, 自动完成数据的加密机制和加密口令的机制是完全相同的。

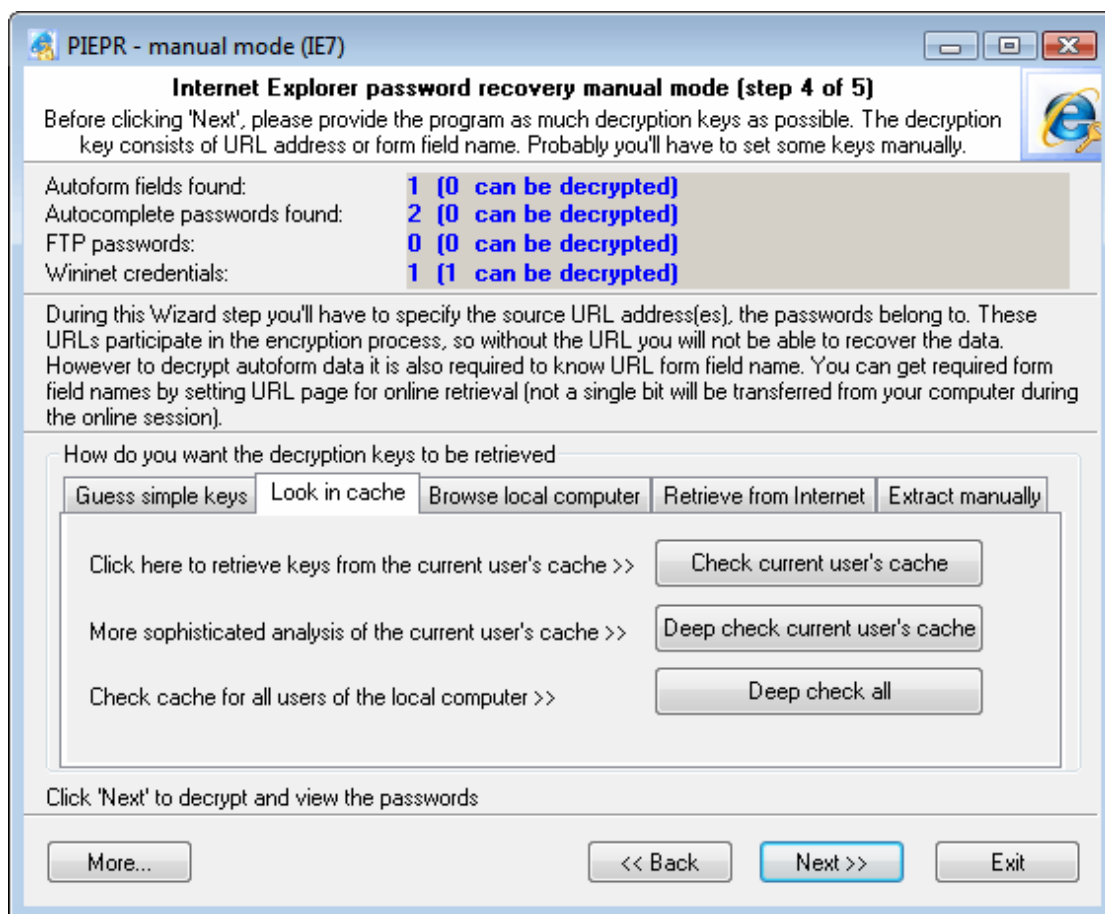
因此, 为了在 IE7 中对自动完成的用户名和自动完成的口令进行恢复工作, 我们需要使创建一个策略。在截图上的五个栏目就是你可以采用的五种恢复加密密钥的方法。这些密钥被用来恢复找到的口令。所恢复的口令数量直接取决于你在这一步中的成果, 所以, 以下是关于每种方法的简述。

1. 猜测简单的密钥



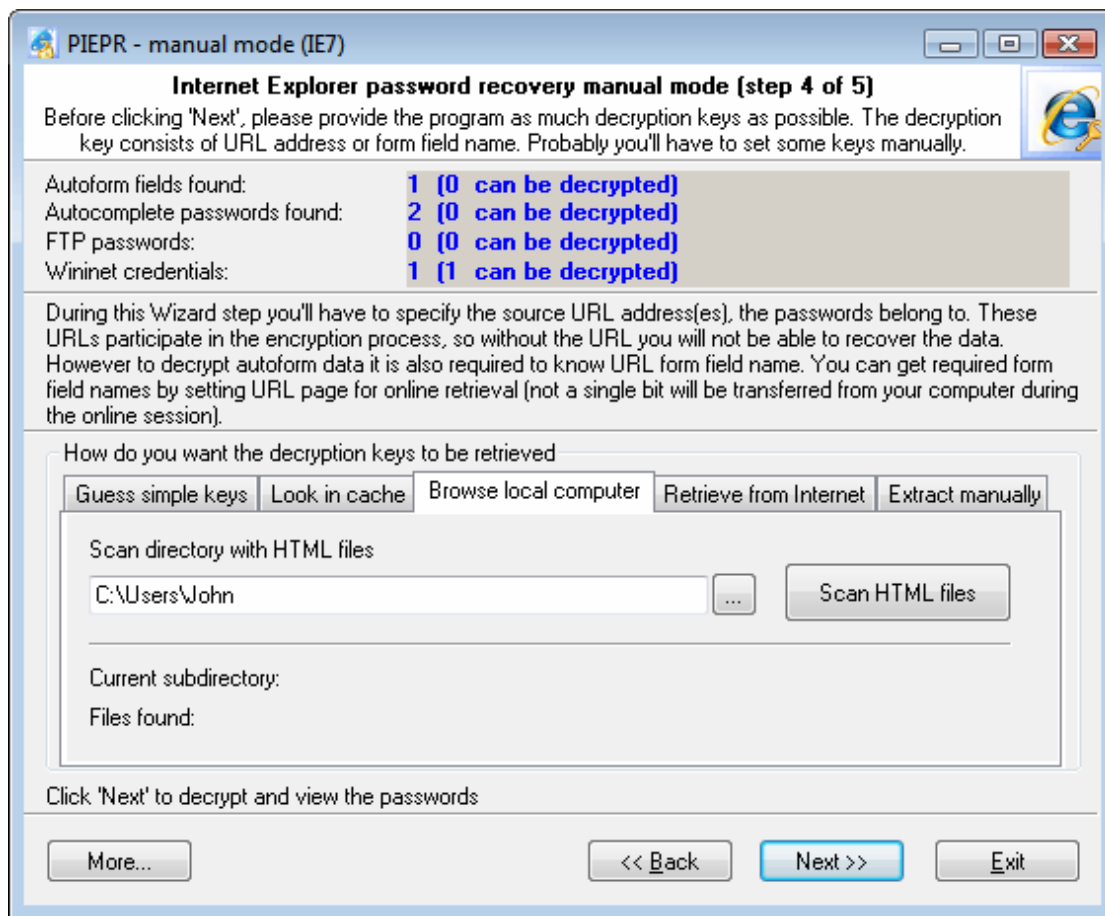
这种方法通过词典或者暴力攻击来找到自动完成的加密密钥。当你点击了运行字典攻击的选项之后，软件将利用其内置的字典配合运行程序开始搜寻密钥。如果你想使用你自己的字典，只要将其命名为 *custom.dic* 并将其复制到程序的安装字典目录中即可。你也可以尝试暴力攻击，这时软件将核对所有的字母和数字的组合以找到密码。但是，这种方法的主要缺点就是它只对短的密码（最多 6 位）较有效率。在该软件的下一版本中，我们计划将设计一种新类型的智能变化攻击方式（smart mutations）。

2. 在缓存中搜索



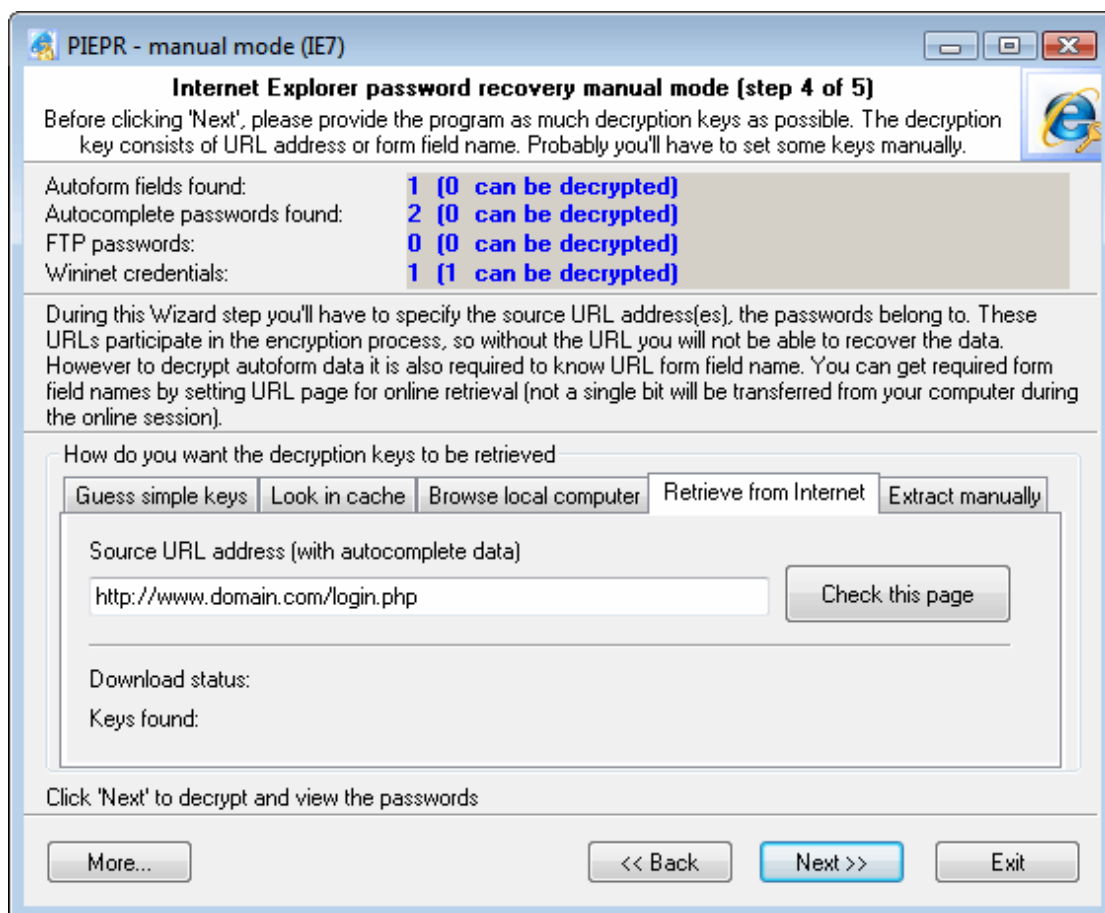
在这一栏中，你可以试图在本地计算机的缓存中搜寻你丢失的 IE 密钥（密码和表单）。当你点击了 **Check Current User's Cache** 键后，应用程序将开始在缓存中快速搜寻密钥。如需展开深度搜索，你要点击 **Deep Check Current User's Cache** 键。尽管此选项速度较慢，但主要的优点在于能独立于 Windows API 各项功能之外进行搜索。最慢但最为有效的方法是第三类 (**Deep Check All**)，该选项将在本地计算机的所有用户缓存中进行搜索。

3. 浏览本地计算机



这一栏只支持搜寻自动完成的加密密码。使用该项时，你需要指定指向 HTML 文件的文件夹的路径。这些文件是什么并不重要，关键在于需要收集尽可能多的文件。这些文件夹，有可能是一个类似于 Internet Explorer cache 的目录。例如，可以是其他浏览器的 html 文件的缓存目录，像 Opera 浏览器一样，将所有访问过的页面保存在一个特殊的位置（通常是 *C:\Documents and Settings\%USER%\Application Data\Opera\Opera\profile\cache4*）。一旦指定了文件夹，你就可以开始扫描 HTML 文件并核实所有找到的自动表单名。这些自动表单名称通常是与你要找的一致。

4. 从 Internet 获得

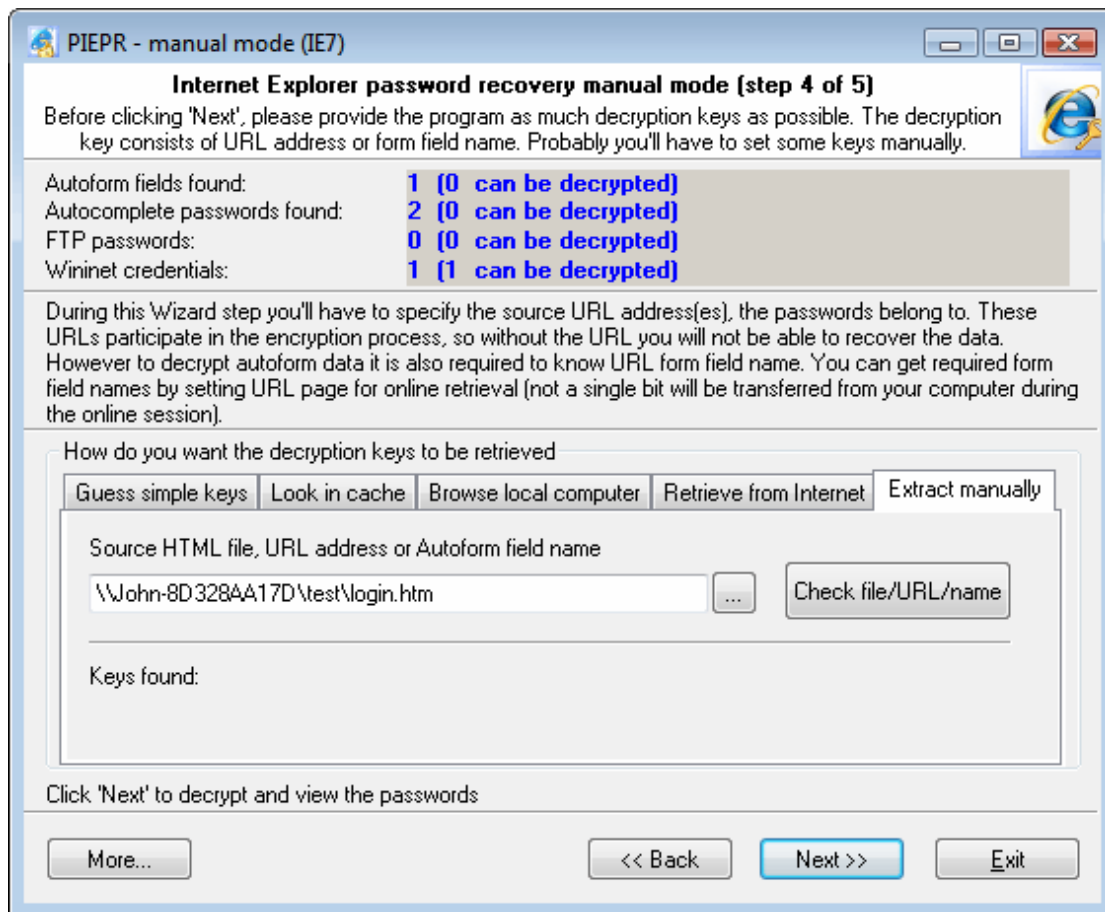


如果你尚有一些密码项目依然没有恢复成功(从上方的统计数据对话框可以知道结果), 这一选栏可能是你最后的选择了。

输入你需要恢复口令的页面的网址 (你只需要从浏览器的地址栏中复制过来就行了), 然后点击 **Check this page**, 软件将会进行如下两项操作。

首先它将会核对该网址是否是恢复**自动完成口令 (Autocomplete)**的密钥。然后, 将它将指定页面下载, 并检查是否是**自动完成表单 (Autoform)**的口令。在新的版本中, 软件将可能支持 URL 列表。

5. 手动恢复



最后一项。你并不需要联网进行，但是，你需要明确以下事项：

- HTML 文件 - 搜寻自动完成表单 (Autoform) 加密密钥
- URL 网址地址 - 校验自动完成 (AutoComplete) 密钥
- HTML 表格的特殊域名 - 校验自动完成表单 (Autoform) 加密密钥

对这些栏目的选择是根据其各自不同的效率。最有效的方法是字典攻击，从来猜测简单的口令。接下来是搜索 Internet Explorer 缓存文件，处理 html 文件，从互联网互联网获取，最后是手动恢复。如果其中一项没有达到目的，点击 'Next >>' 尝试其它所有选项。

步骤 5: 恢复数据

在最后一步中，向导程序会分析所有获取的密钥，并恢复原始的已加密数据。

