Internet Explorer 7- 9

1

Internet Explorer 7 (IE8 - IE9
)
!

,

[Passcape Internet Explorer Password Recovery](). ,
- , ,
.

5 5 . 4,
.

1. .
2. .
3. . .
4. .
5. .

, ...

2   1:

1   .   .

3   2:

,   ,
,   .   ,
,   ,   :

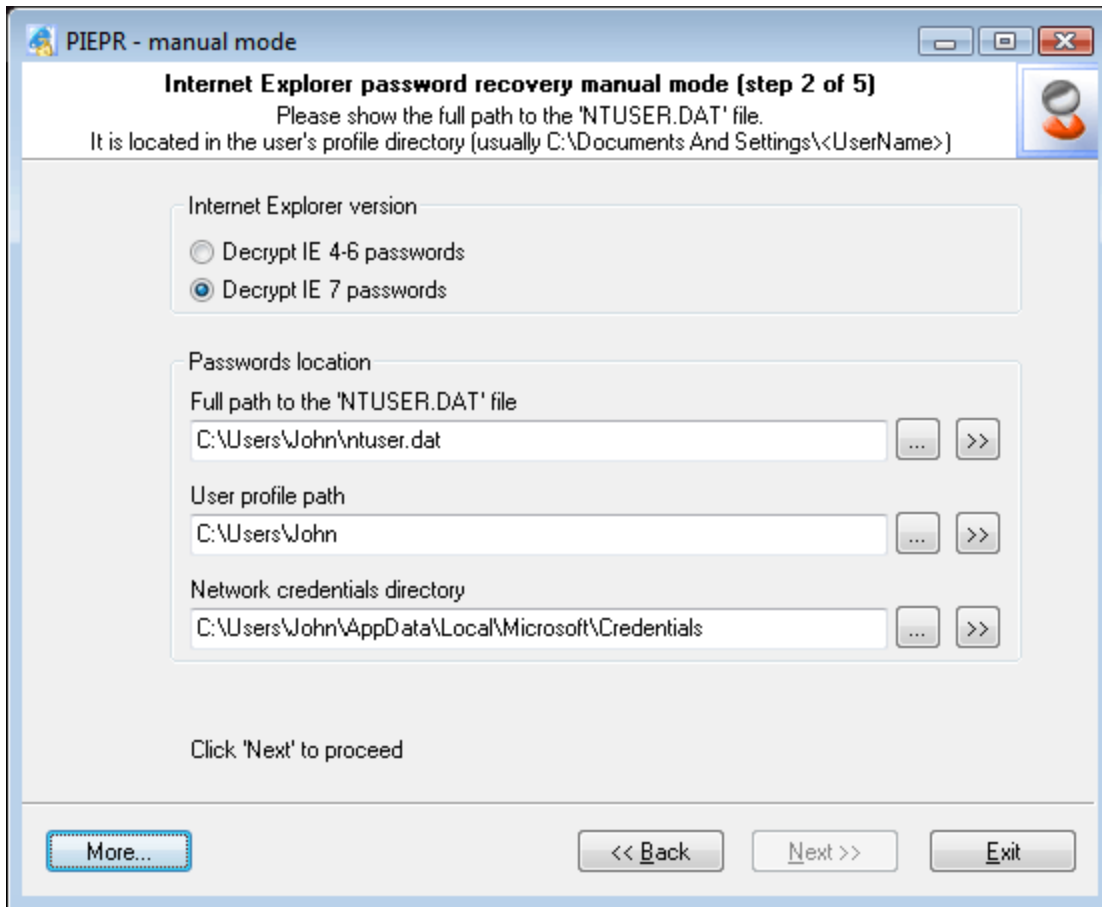1.   ntuser.dat,
.   IE 7-8 (4).   Windows XP-2003
: *C:\Documents And Settings\%*
USER%\ntuser.dat,   *%USER%* -   .   Vista
-          : *C:\Users\%USER%\ntuser.dat*.

.

2.   -   .
(.   ).

,   .
,
.

3. **Network credentials directory** -   . Windows Credentials
Manager   ,

.   ,   ,
Windows Live (.Net Passport),   Exchange   . .,
             Network Credentials Directory.   ,   ,   Web
             Internet Explorer 7   ,   Wininet
Credentials.   Wininet Credentials
             IE.

   Windows XP-2003 Wininet Credentials   :
C:\Documents And Settings\%USER%\Application Data\Microsoft\Credentials\%SID%

C:\Documents And Settings\%USER%\Local Settings\Application Data\Microsoft\Credentials\%SID%.

             %USER% -   Windows,   *%SID%* -
             SID   ,   .

   Windows Vista SID   Network Credentials Directory   ,
                              Wininet Credentials   :

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

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

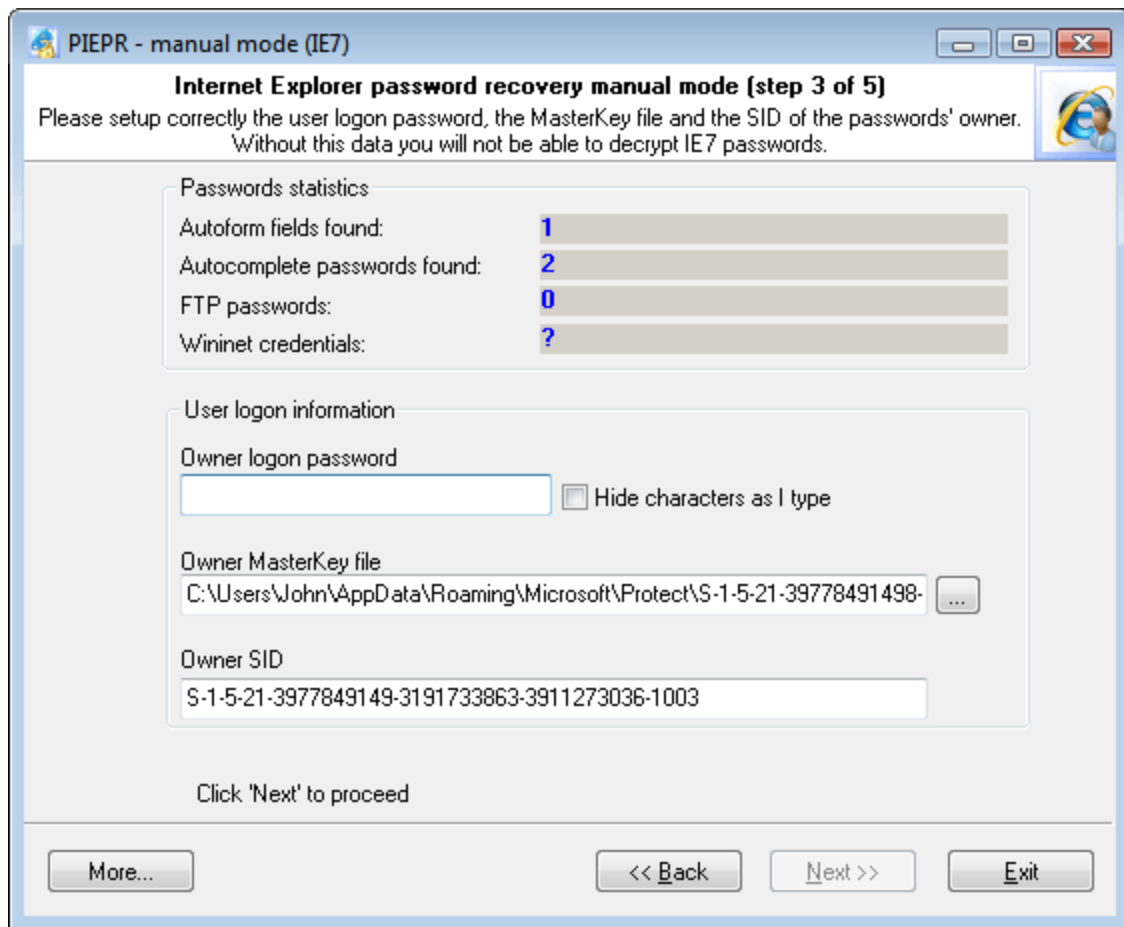   Network Credentials Directory:
C:\Users\John\AppData\Local\Microsoft\Credentials
D:\Documents   and   Settings\Kate\Application   Data\Microsoft\Credentials\   S-1-5-21-1927147842-
1992852531-225342917-1003.

                     Network   Credentials   Directory
                              [>>] ,

                                                                         ,   .
             Network Credentials Directory,   .
                                                                 ,   Network Credentials
Directory,   ,   [...].

4   3:   ,

,   ,
Internet
Explorer.   'Password *Statistics*'   ,
                              .   Wininet Credentials
                    ,   :

-                              'Network Credentials Directory'

-                        'User   logon   information',

        ,   *'Owner MasterKey file'*   *'Owner SID'*
                                                        .
        .   :
Windows XP-2003:
C:\Documents and Settings\%USER%\Application Data\Microsoft\Protect\%SID%
Windows Vista+:
C:\Users\%USER%\AppData\Roaming\Microsoft\Protect\%SID%

Owner SID, , %SID%.

, 'User logon information',
Wininet credentials, 'Next >>'
- .

5 4:

.
Internet Explorer 7 ,
.
, , IE,
.
FTP Wininet , , .
, .

, IE 7
:

1. Web , , ,
Internet Explorer URL
hash=sha(URL).
2. URL (Unicode),
.
DPAPI :
EncryptedPassword=DPAPI(URL,password).
3. EncryptedPassword hash,
.
4. URL .

:
URL , . . URL
. , (URL)
.

Internet Explorer? :

, IE **hash URL** .
(**hash + EncryptedPassword**),
. , ,
, , ,
, URL .

.
, ,

,   .
URL   html   ,
html   ,
.

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

loginname.
.

,   IE 7,
.
,   ,   ,
(,
).   ,   ,   .
.   ,   .

5.1

.   'Run
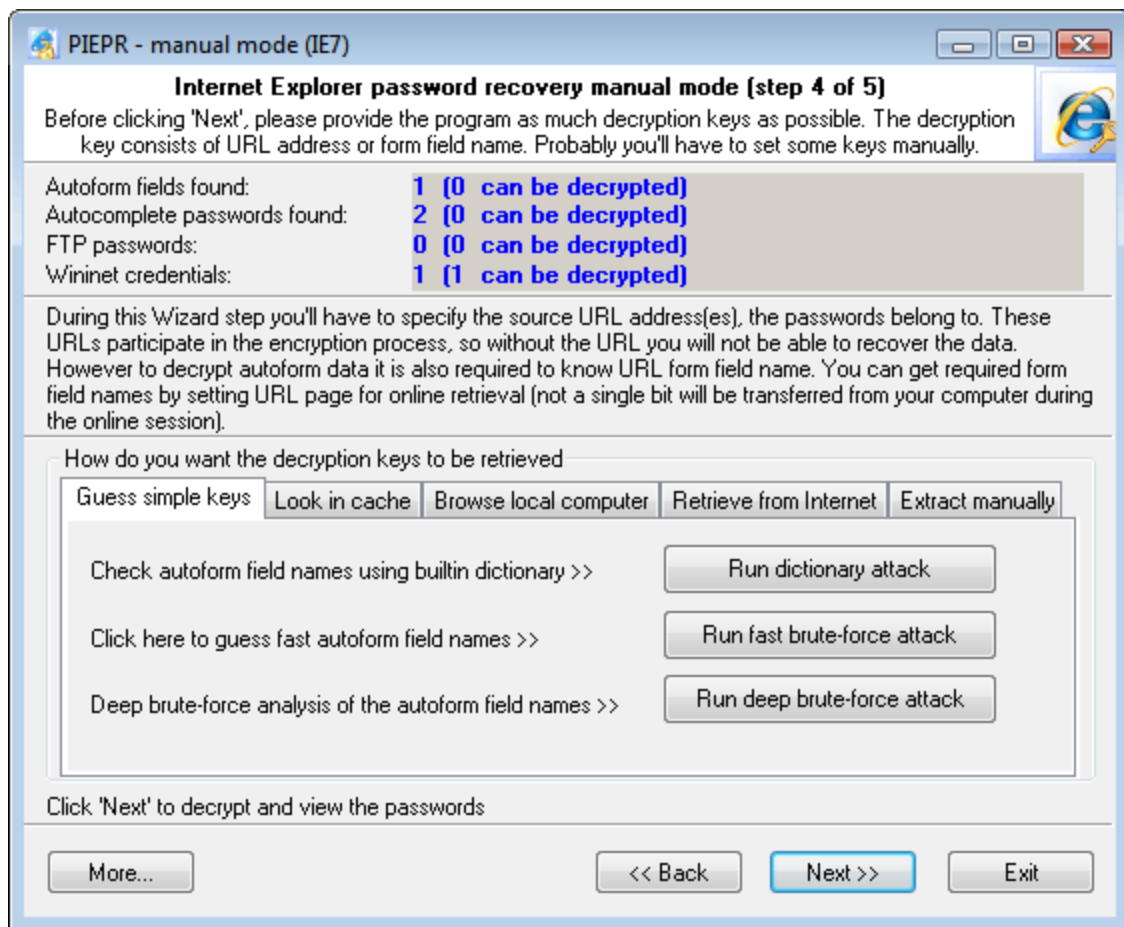dictionary   attack'   ,   ,
.   .   ,
.   ,
(5   )   .
,   **smart mutations**.

5.2

(,
)   IE   .   'Check current
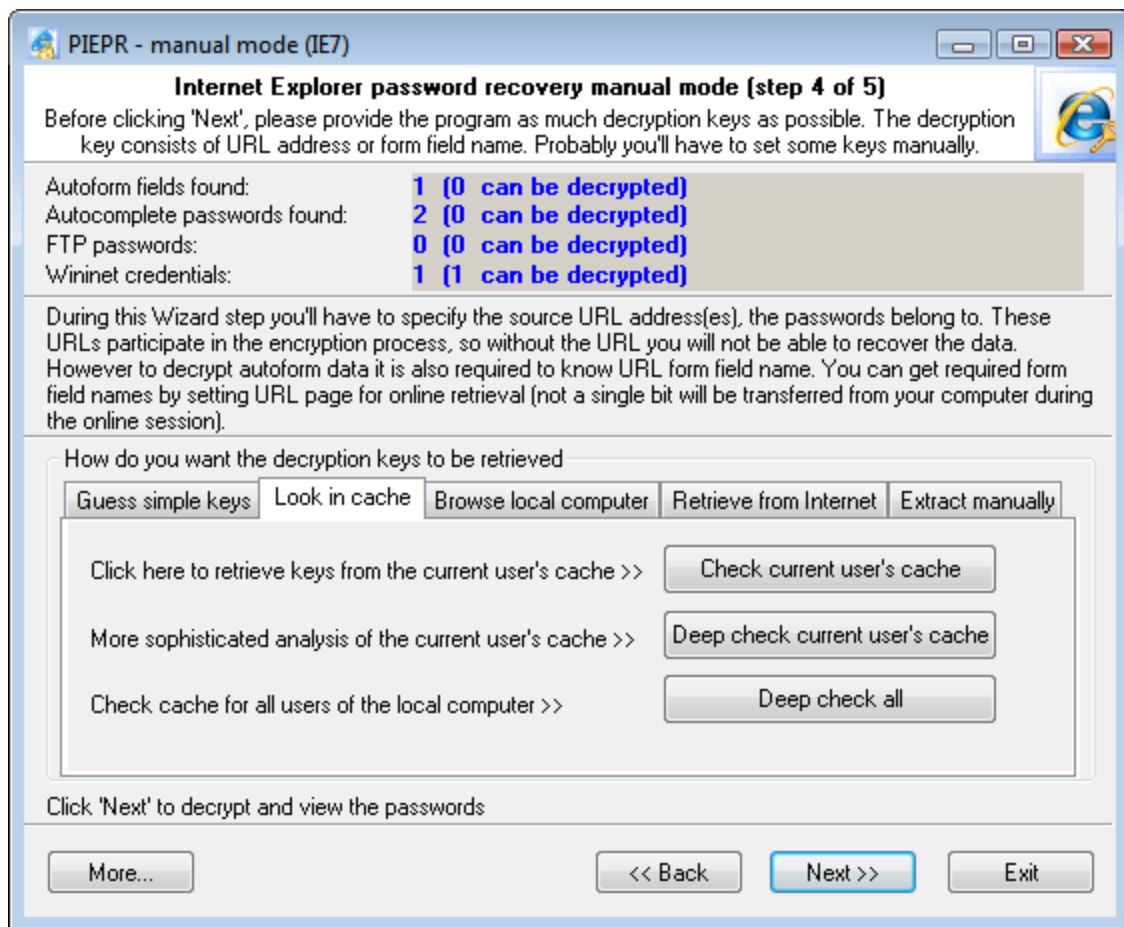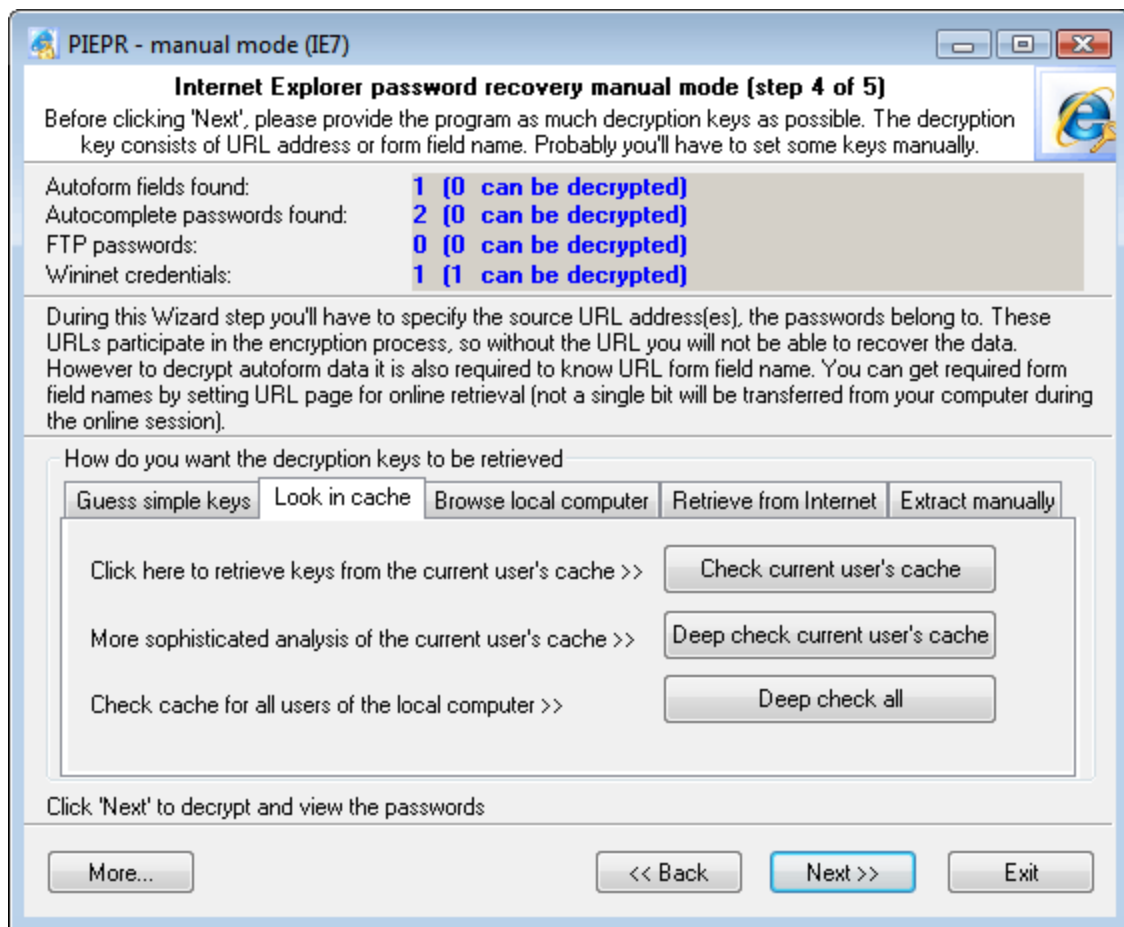user's cache'   .
                                                                            'deep check current user's
cache'.   ,   ,   Windows
API.   ,
                            ,   'deep check all',
                                                                    .

5.3

.
html   .   .   ,
.   ,   Internet Explorer,
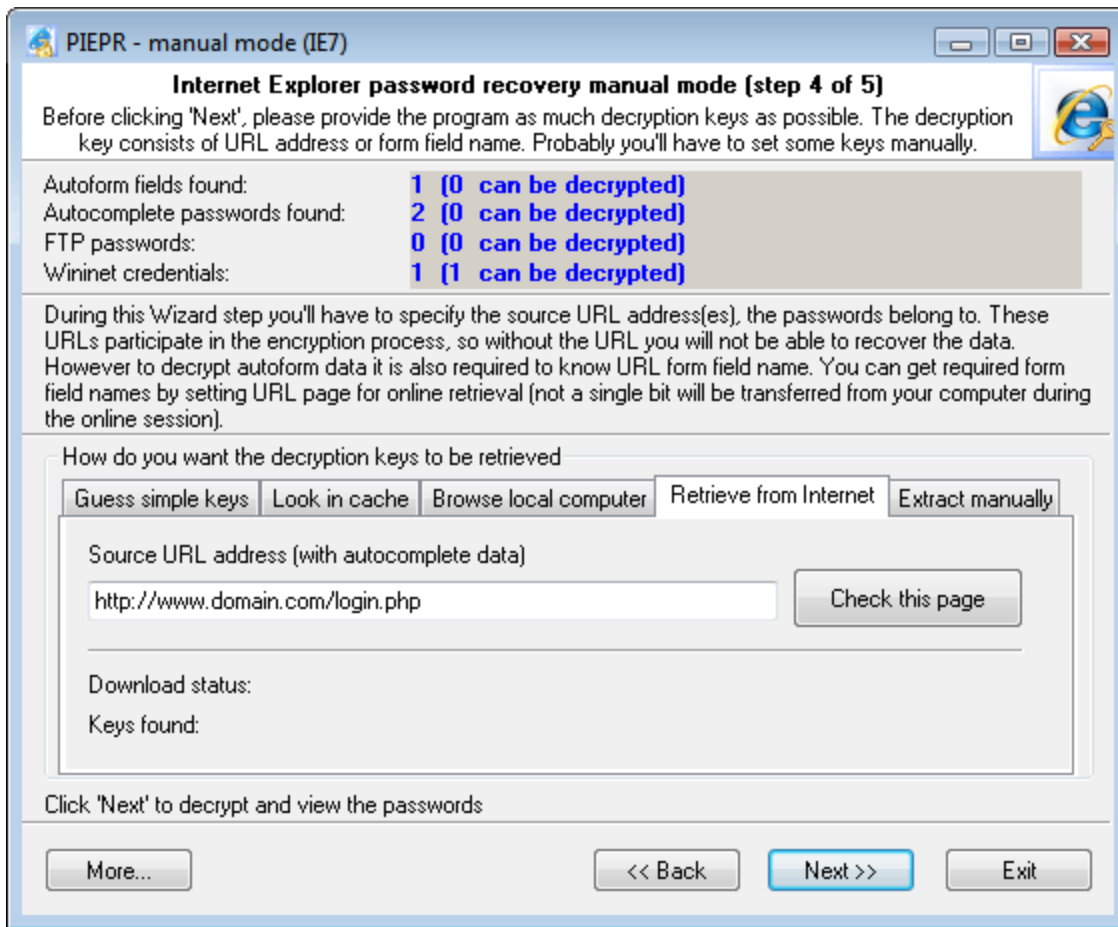,   html   .
, Opera   (   )
(C:\Documents and Settings\%USER%\Application
Data\Opera\Opera\profile\cache4).   ,   ,
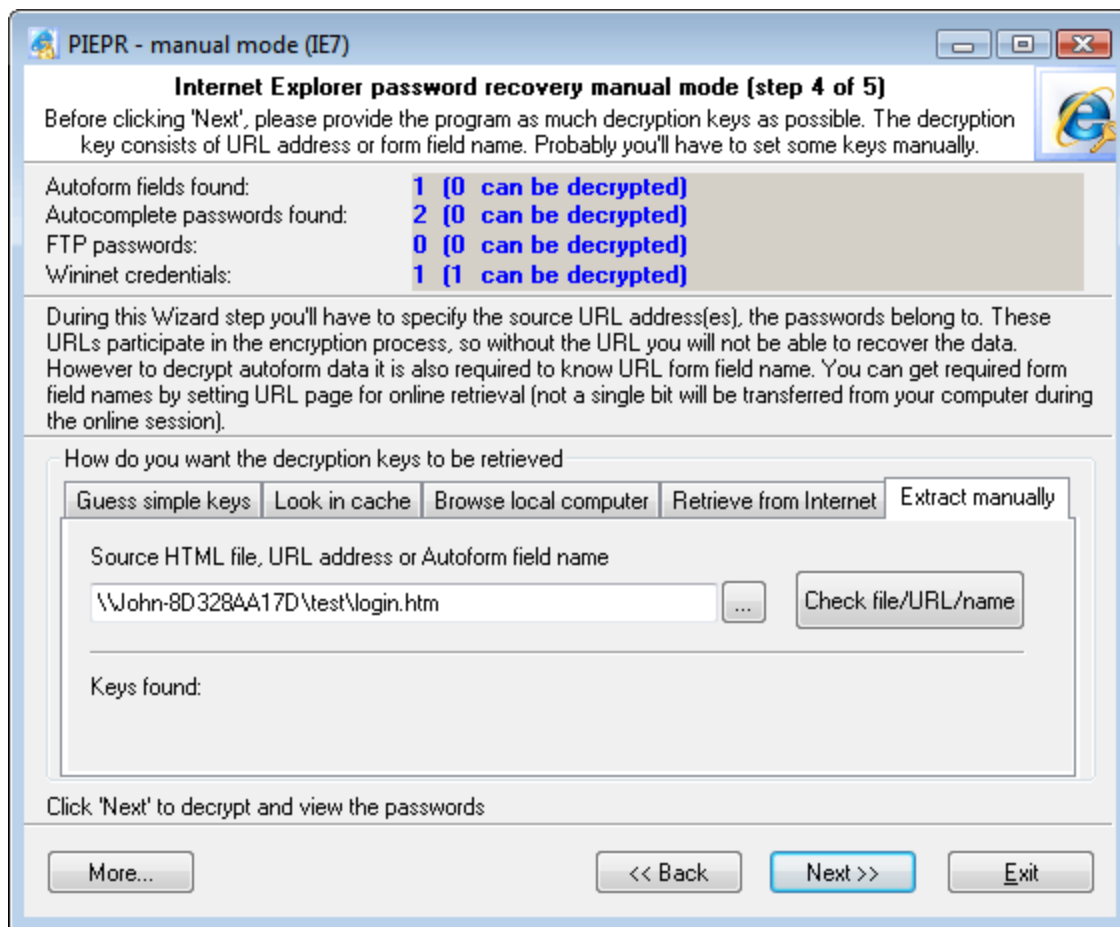html
.   ,   .

5.4

(   ),
-   .   **URL**   (,
,   ),
,   'Check this page'.
.   -   ,   URL,
.   -   ,
,
.   ,   ,
.

5.5

         ,   ,   .
            ,   :

- **html**   -
-          **URL** -
-   **html**   -   .

                                                     .
                       -   Guess simple keys,
         IE,   html   ,   ,   ,   . '*Next
>>*',   .

6   5:

.