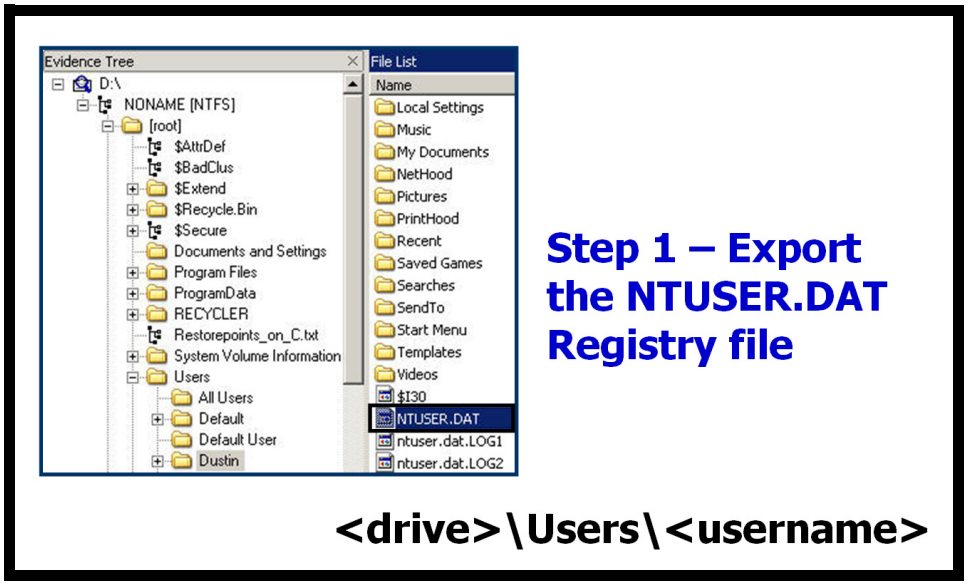
# Steps for Decrypting IntelliForms Data in Windows Vista

This appendix reviews the process required to decrypt the protected information located in the IntelliForms subkey.

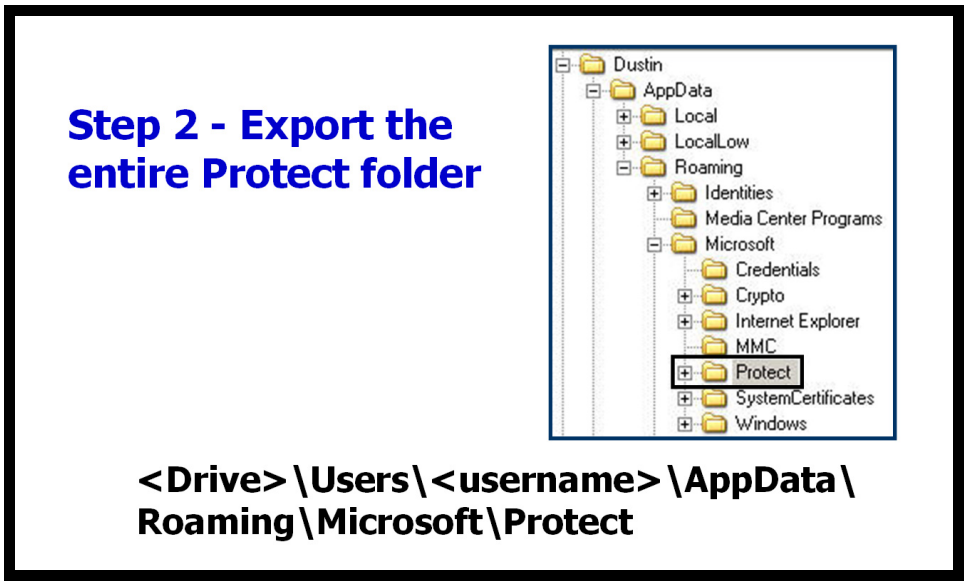
## STEP 1—EXPORT THE NTUSER.DAT REGISTRY FILE




Create a folder to hold the necessary objects and export the NTUSER.DAT of the particular user of interest to this folder. The NTUSER.DAT in Vista is located at:

C:\Users\<*username*>

## STEP 2—EXPORT THE ENTIRE PROTECT FOLDER



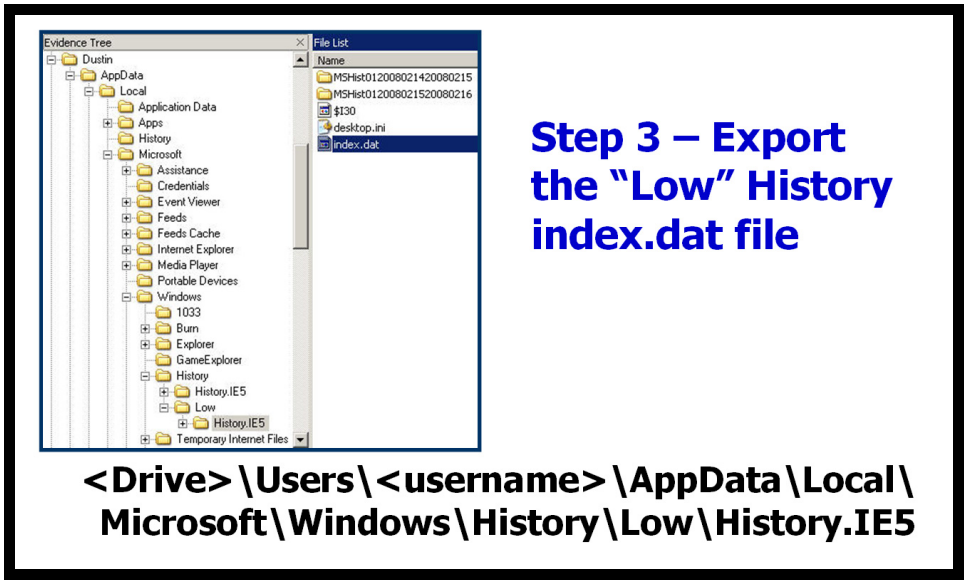

In Windows Vista, the Protect folder is located at:

C:\Users\<*username*>\AppData\Roaming\Microsoft\Protect

In Windows XP, this path would be:

C:\Document and Settings\<*username*>\Application Data\Microsoft\Protect

## STEP 3—EXPORT THE "LOW" HISTORY INDEX.DAT FILE




One of the pieces of entropy for Web login passwords is the actual URL that the password was entered into. In order to harvest as many URLs as

possible, use that users History index.dat. Export the one located in the Low folder, as this will likely have the most up to date URLs. By exporting this file, then later pointing PRTK to it, PRTK will carve all of the URLs from the file and use them like a dictionary to attack any stored passwords.

If this doesn't work, more URLs should be carved from the system and placed into a file. PRTK can be pointed to the file to harvest the URLs for testing.

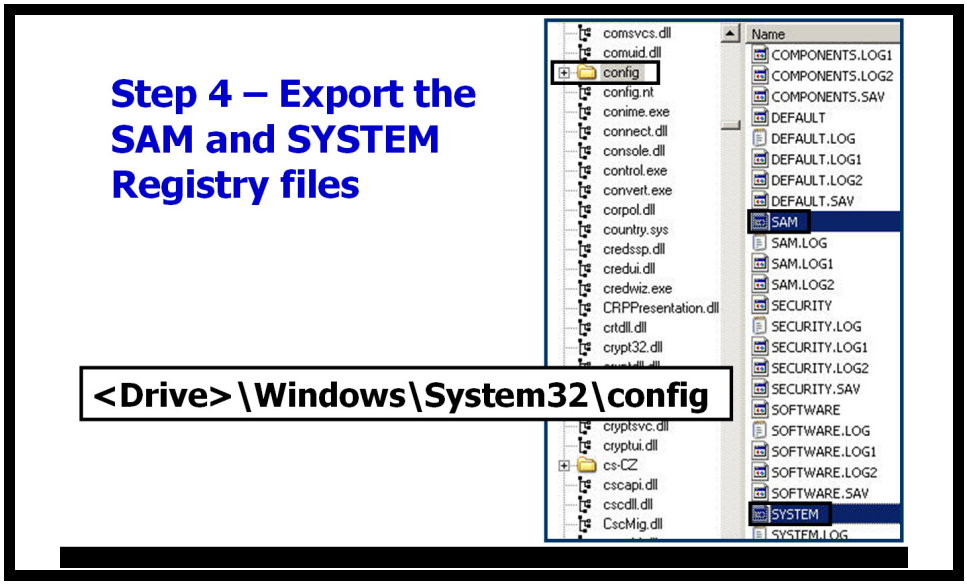
In Windows Vista, the Low history is located at:

C:\Users\<*username*>\AppData\Local\Microsoft\Windows\History\Low\History.IE5

In Windows XP, use:

C:\Documents and Settings\<*username*>\Local Settings\History\History.IE5

## Step 4—Export the SAM and SYSTEM Registry files

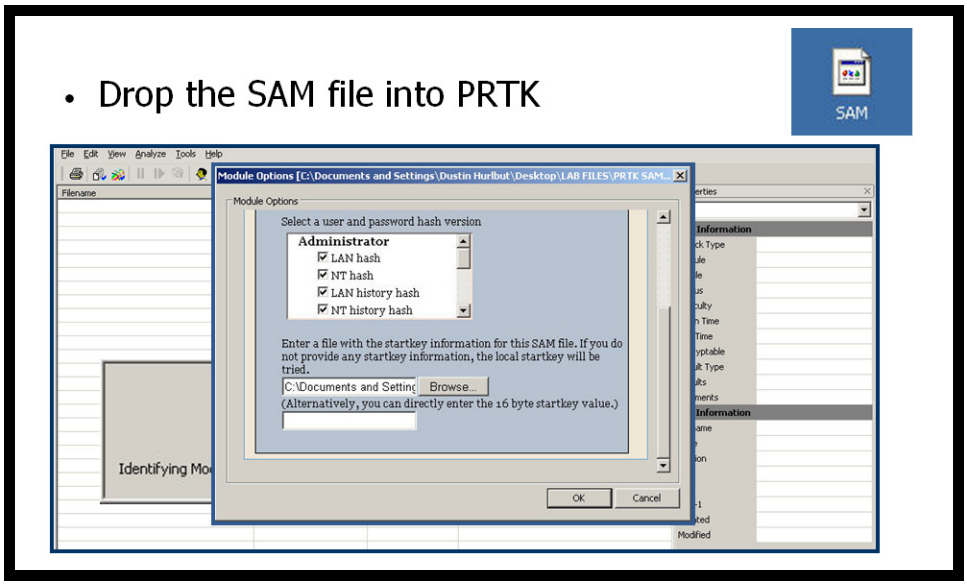



The SAM and SYSTEM registry files will be needed in order to break the user's login password prior to breaking the protected data in the IntelliForms.

The SAM and SYSTEM registry files are in the same location:

C:\Windows\System32\config

## Step 5—Break the User's Login Password




To break the user's login password:

1 Drag-and-drop the SAM file into PRTK.

After PRTK identifies the SAM file it will display a dialog box requesting further information.

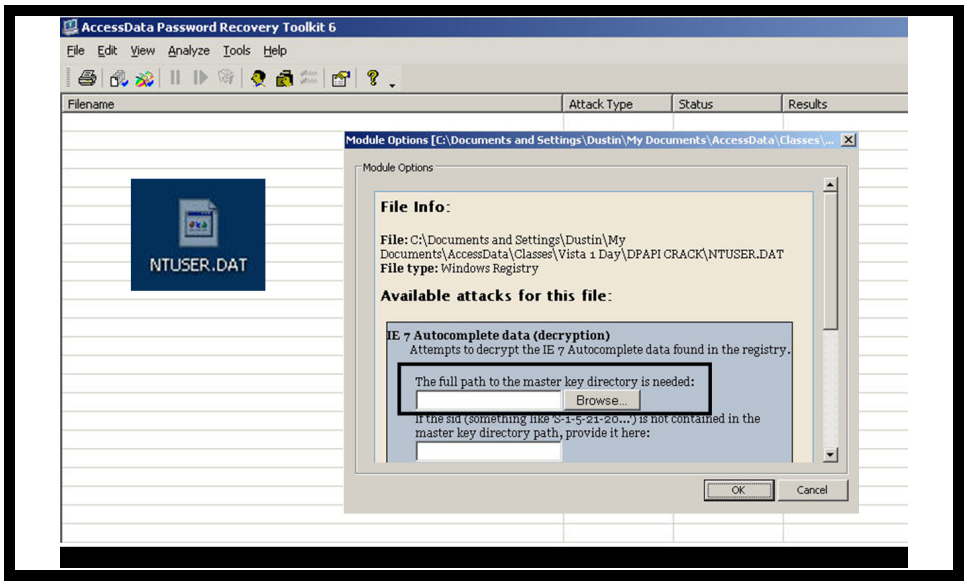
2 Select the user(s) whose password(s) you want to break.

3 Next, below the usernames, browse to the location of the exported SYSTEM file from the suspect's system. PRTK needs this file to harvest the Syskey which protects the SAM file.

4 Click **OK**.

5 PRTK will next request an attack profile. It is preferable to use the full text index from the suspect's system as one of the dictionaries in this attack. Also include any other pertinent dictionaries, including a biographical dictionary if available. Create the profile including the dictionaries, languages, characters, and levels desired and break out the user's login password.

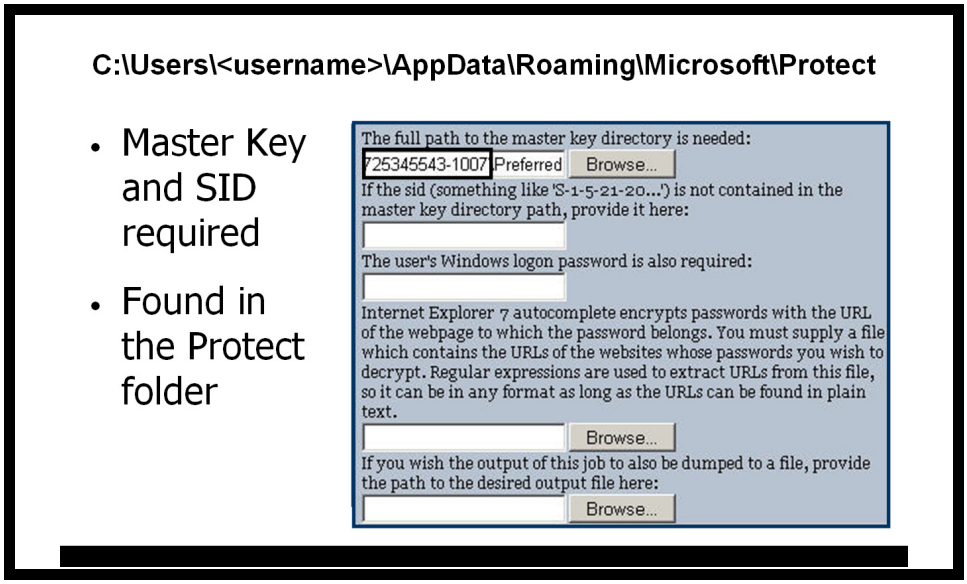
## Step 6—Create a Text File to Output the Results To




Once the three objects are in the folder, create a text file to output the results to. This file will contain all of the data that is retrievable from the IntelliForms. The data can be viewed in PRTK, but the text file makes it easier to collate and place into the final FTK report.

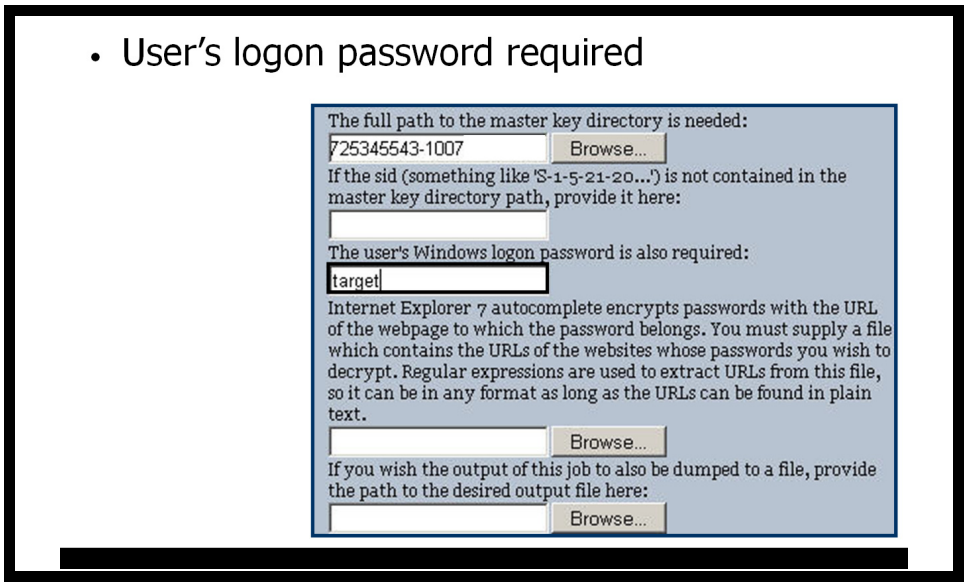
Drop the NTUSER.DAT file into PRTK. PRTK will identify the data in the file and report whether or not breakable data exists. If no data is in the IntelliForms to break, PRTK will return a dialog box indicating the that file is unidentifiable. If data is available, PRTK will display the **Module Options** dialog box. Use this box to point to the required objects.

## STEP 7—SPECIFY THE USER'S MASTER KEY AND SID



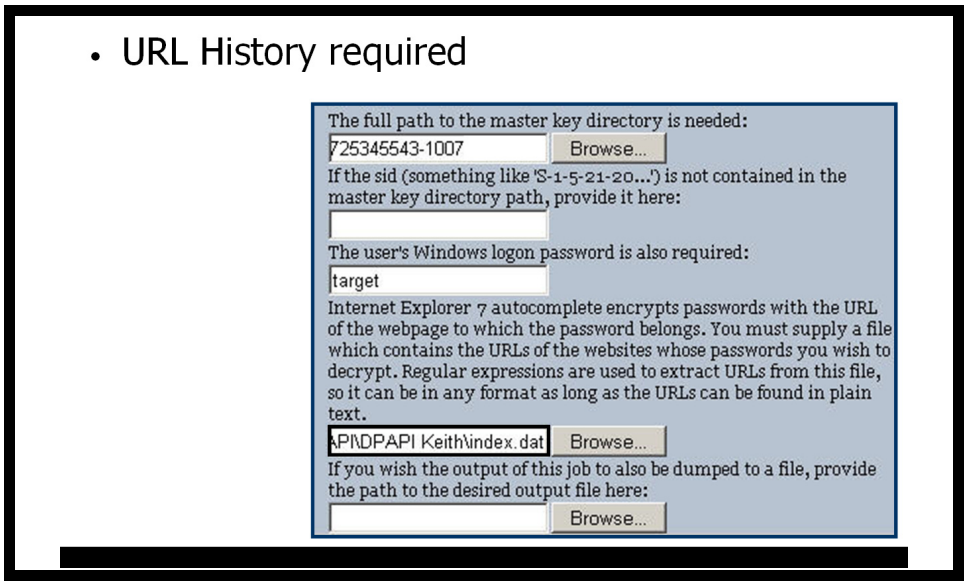
The first entry is the Protect folder. Browse to the folder you placed it into and open the Protect folder. Click the user's SID, then the Preferred file. Once this is done, you will have the full path entered into the text box. Navigate to the end of the path and delete the "Preferred" from the preferred file. This will leave the full path with the SID intact, which is what PRTK needs to harvest the key data.

## Step 8—Enter the User's Login Password



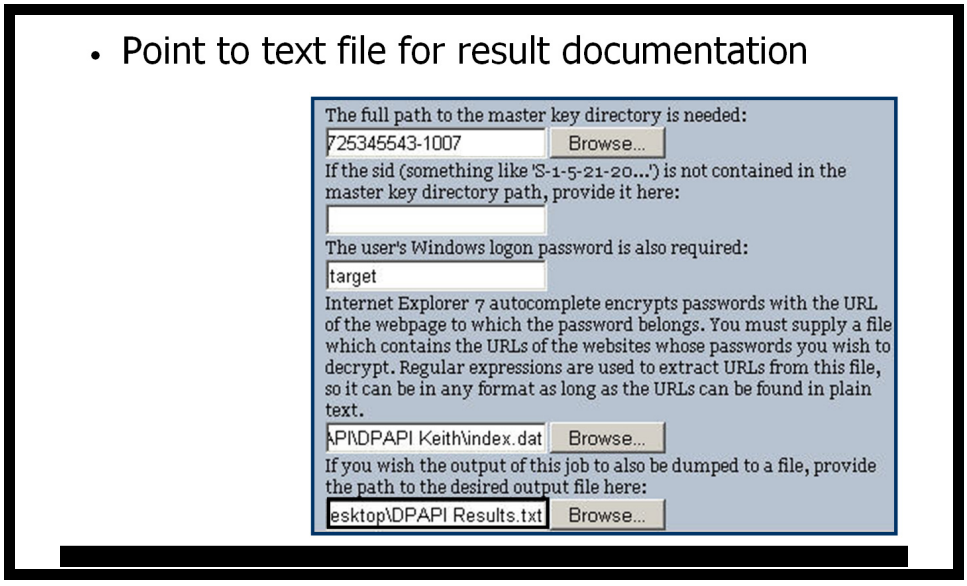

The next requirement is the user's login password. Enter it into the password text box.

## Step 9—Browse to the User's URL History File



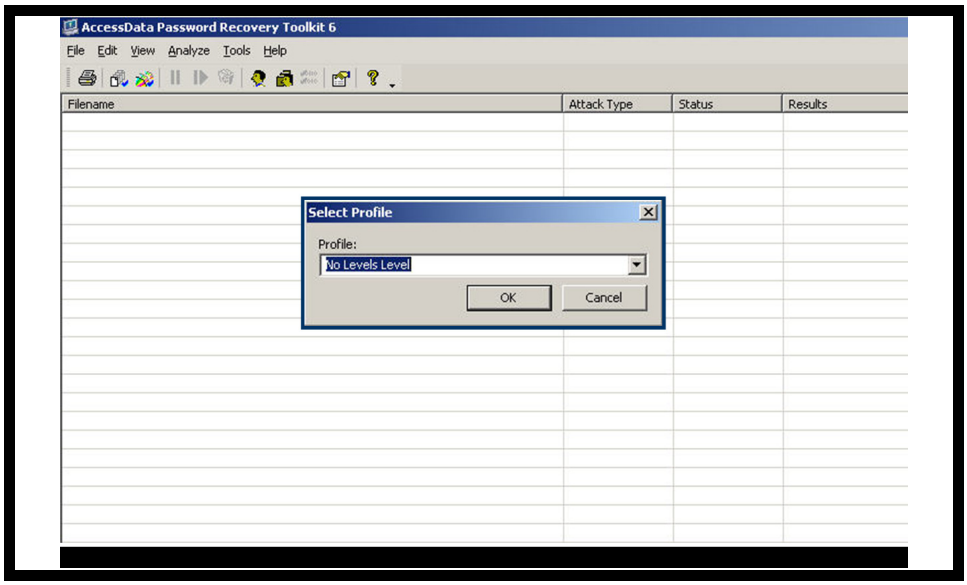

Browse to the index.dat harvested from the suspect's system.

## Step 10—Point to the Text File for Result Documentation




Browse to the text file that you created to hold the attack's results.

## Step 11—Select an Attack Profile

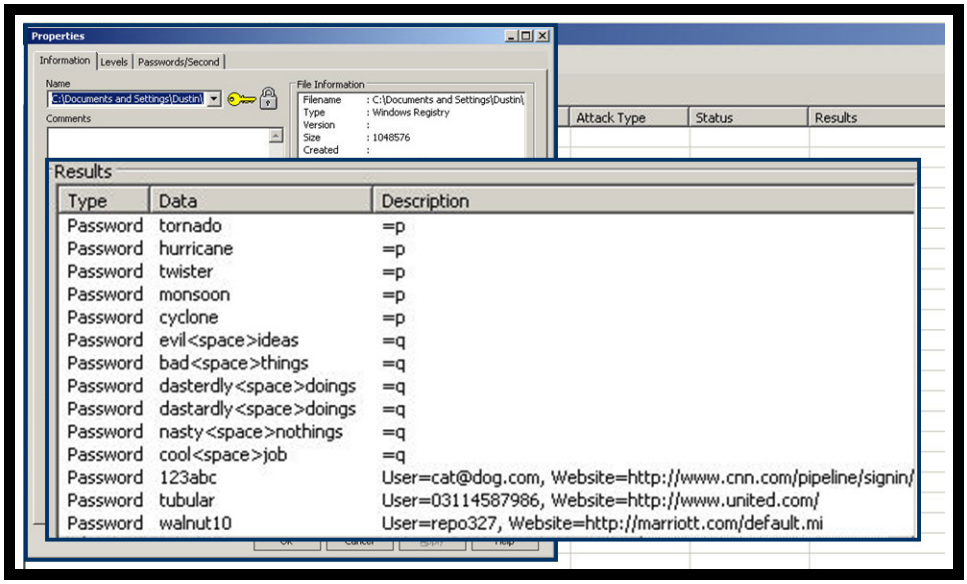



Once you have pointed to the text file, click **OK**.

PRTK will prompt you for the attack profile.

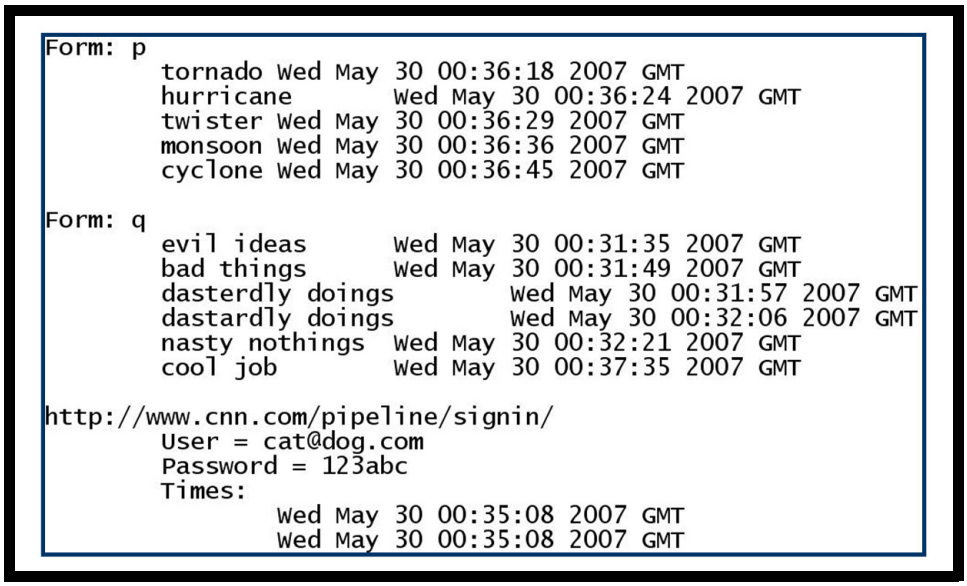
PRTK uses the objects that you supplied to it to break whatever it can from the IntelliForms registry subkey. This is a decryption attack, since the login password has been supplied. Any profile can be used; even a profile with no dictionaries, characters, or languages can be applied. All PRTK needs is a single level to initiate itself and break the data.

## STEP 12—VIEW THE RESULTS



The results are visible in PRTK; however, it is better to view them in the text file used to hold the results of the attack.

## STEP 13—VIEW THE RESULTS



```
Form: p
        tornado Wed May 30 00:36:18 2007 GMT
        hurricane       Wed May 30 00:36:24 2007 GMT
        twister Wed May 30 00:36:29 2007 GMT
        monsoon Wed May 30 00:36:36 2007 GMT
        cyclone Wed May 30 00:36:45 2007 GMT

Form: q
        evil ideas      Wed May 30 00:31:35 2007 GMT
        bad things      Wed May 30 00:31:49 2007 GMT
        dasterdly doings        Wed May 30 00:31:57 2007 GMT
        dastardly doings        Wed May 30 00:32:06 2007 GMT
        nasty nothings  Wed May 30 00:32:21 2007 GMT
        cool job        Wed May 30 00:37:35 2007 GMT

http://www.cnn.com/pipeline/signin/
        User = cat@dog.com
        Password = 123abc
        Times:
                Wed May 30 00:35:08 2007 GMT
                Wed May 30 00:35:08 2007 GMT
```

The text file will show the different passwords, search terms, and form data that PRTK was able to decrypt. Any other data that was still encrypted, such as a password that required a URL that wasn't in the History index.dat, will also be indicated.