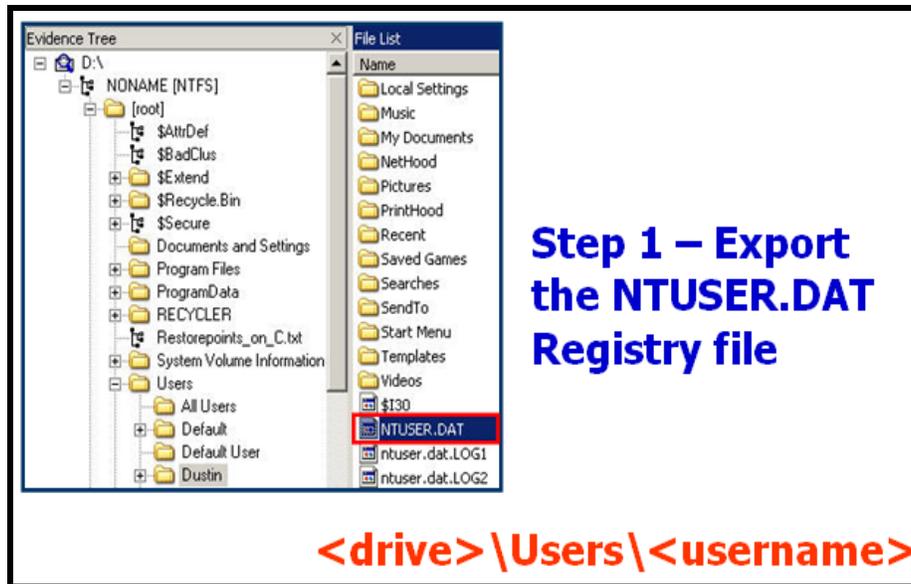


# Steps for Decrypting Intelliforms Data

## Step 1 – Export the NTUSER.DAT Registry File



Create a folder to hold the necessary registry objects, and then export the user's NTUSER.DAT file to this folder. In Windows Vista, the NTUSER.DAT file is located at:

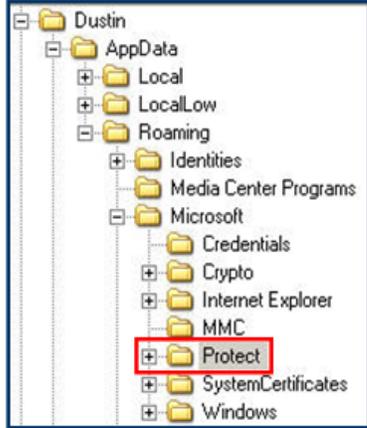
*drive:\Users\username*

In Windows XP, this path is located at:

*drive:\Document and Settings\username*

## Step 2 – Export the Entire Protect Folder

**Step 2 – Export the entire Protect folder**



**<Drive>\Users\<username>\AppData\  
Roaming\Microsoft\Protect**

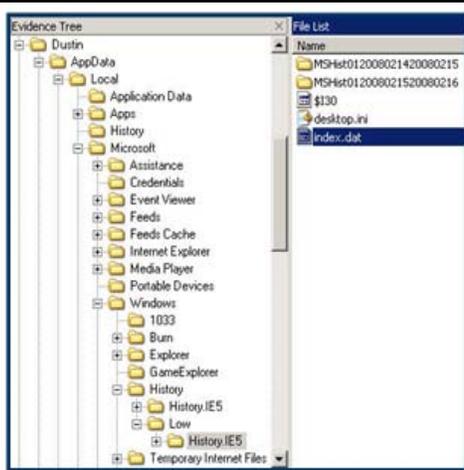
Export the entire Protect folder to your evidence folder. In Windows Vista, the Protect folder is located at:

*drive:\Users\username\AppData\ Roaming\Microsoft\Protect*

In Windows XP, this path is located at:

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

## Step 3 – Export the “Low” History index.dat File



**Step 3 – Export the “Low” History index.dat file**

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

One of the pieces of entropy for Web logon passwords is the actual URL that the password was entered into. To harvest as many URLs as possible, use that user's History index.dat file. Export the index.dat file located in the Low folder because this file is likely to have the most up-to-date URLs. By exporting this file and later pointing PRTK to it, PRTK carves all of the URLs from it and uses 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.

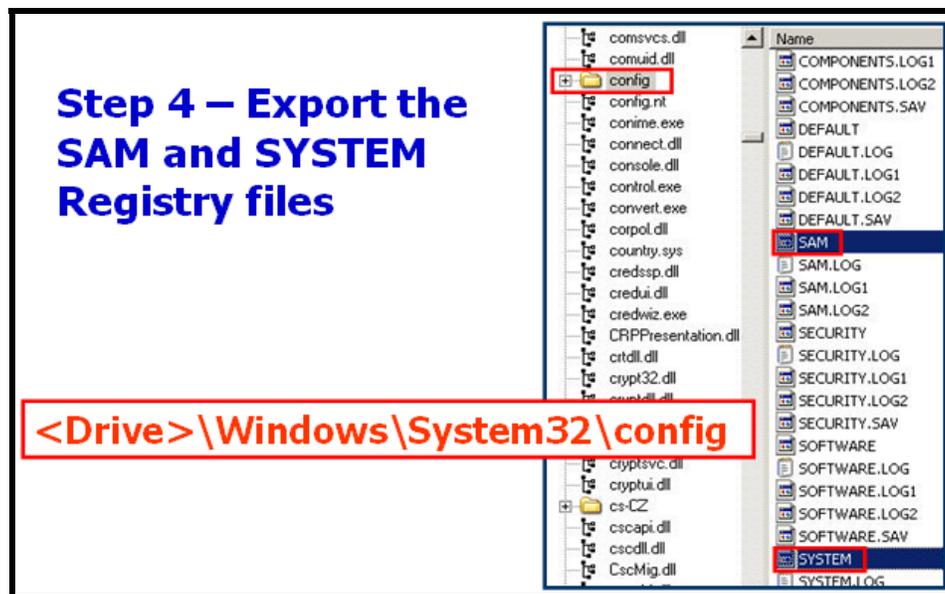
In Windows Vista, the Low history is located at:

*drive:\Users\username\AppData\Microsoft\Windows\History\Low\History.IE5.*

In Windows XP, the history is located at:

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

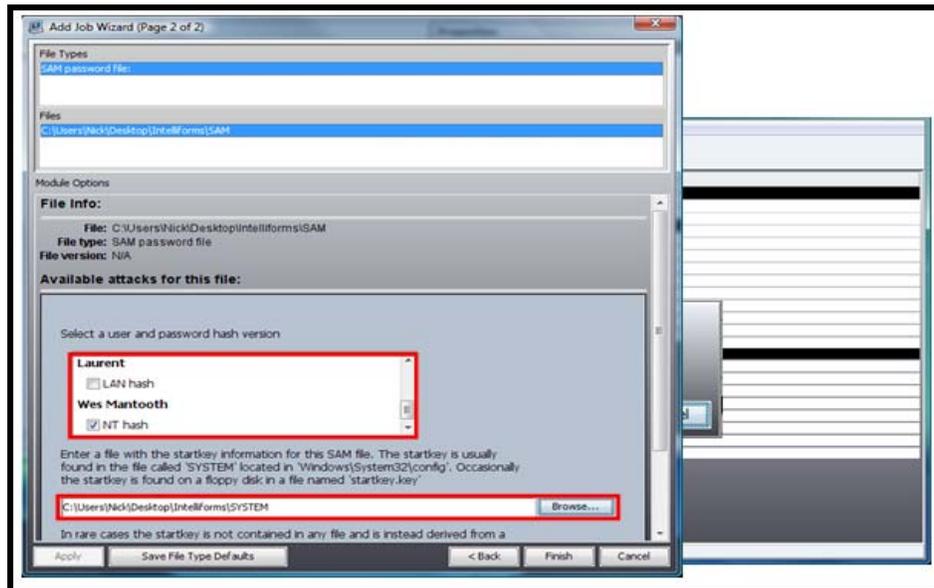
#### Step 4 – Export the SAM and SYSTEM Registry Files



Export the SAM and SYSTEM Registry files. They need to break the user's logon password prior to breaking the protected data in the IntelliForms.

The SAM and SYSTEM Registry files are located in the same location, *drive:\Windows\System32\config*.

## Step 5 – Break the User’s Login Password



To break the user’s logon password:

1. Drag and drop the SAM file into PRTK.

After PRTK identifies the SAM file, it displays a dialog box requesting an attack profile.

Create the profile including the dictionaries, languages, characters, and levels desired, then break out the user’s logon password.

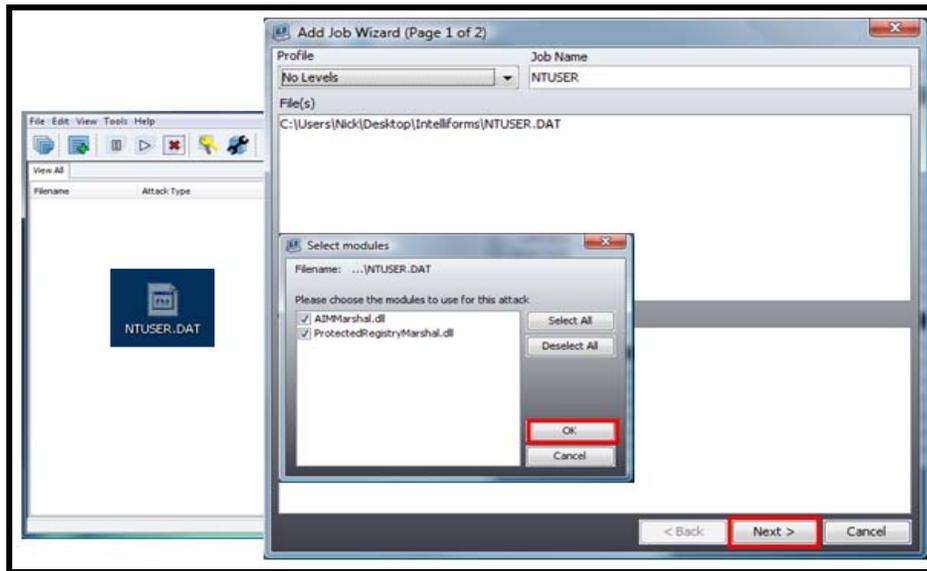
It is preferable to use the full text index from the suspect’s system as one of the dictionaries in this attack. Also include any other pertinent dictionaries including a Biographical Dictionary, if available.

2. Click **Next**.
3. Select the users whose passwords you want to break.
4. 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.

5. Click **Finish**.

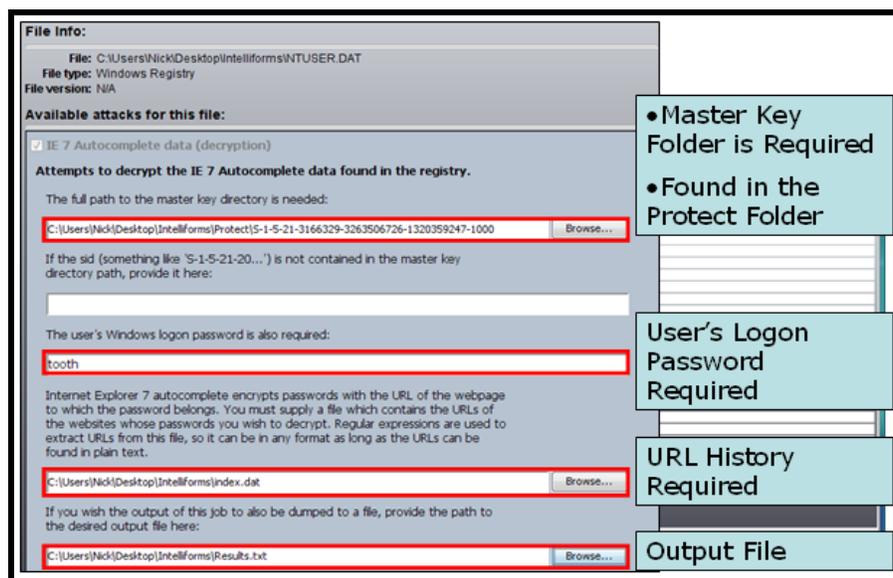
## Step 6 – Breaking Intelliforms



Drop the NTUSER.DAT file into PRTK. PRTK identifies the data in the file and reports whether breakable data exists or not. If no data is in the IntelliForms to break, PRTK returns a message indicating the file is unidentifiable. If data is available, PRTK displays the Module Options dialog. Use this dialog to point to the required objects.

PRTK then asks for the attack profile. Select an attack profile, then click **OK**. Any profile can be used.

## Step 7 – Specify the User’s Master Key, Login Password, URL History and Output File



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

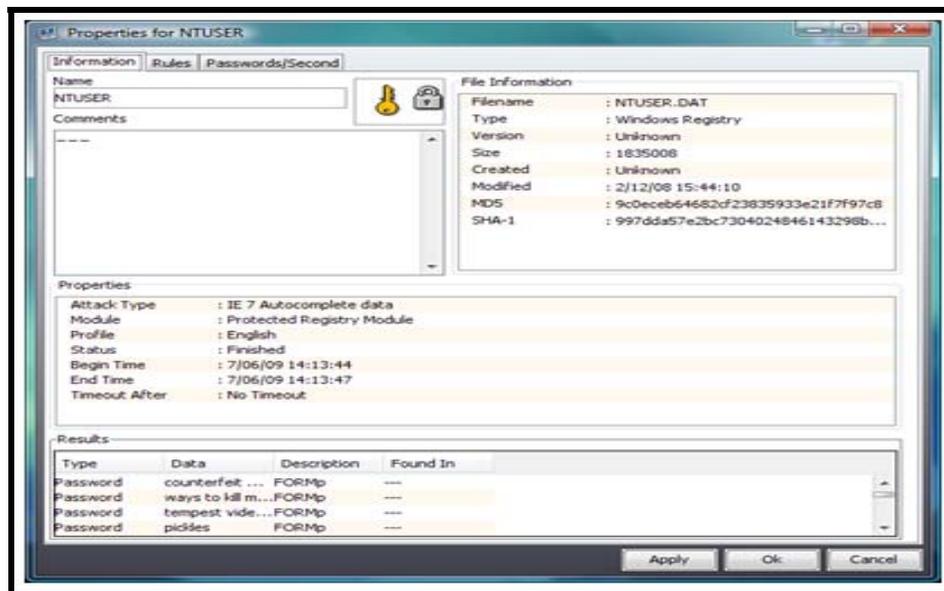
The second requirement is the user's logon password. Type it into the password text box.

The third requirement is to browse to the index.dat harvested from the suspect's system.

The fourth requirement is to browse to the text file you created to hold the attack's results, then click **OK**. Once the three objects are in the folder, create a text file to output the results to. This file contains 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.

PRTK uses the registry objects you supplied to recover whatever it can from the IntelliForms Registry subkey. This is a decryption attack since the logon password has been supplied.

## Step 8 – Viewing 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. The text file has more visible space for easier viewing than the results area in PRTK, especially when multiple passwords, form data items and search terms are recovered. This text file can also be added as a supplementary item in your FTK report.

```
Form: query
I am searching on MAMMA.com Tue Apr 10 20:10:07 2007 GMT
fake auto insurance Tue Apr 10 20:10:53 2007 GMT
fake license plates Tue Apr 10 20:11:18 2007 GMT
change your identity Tue Apr 10 20:11:40 2007 GMT
I am searching for terrible stuff on Lycos.com Sun Aug 05 09:14:19 2007 GMT

Form: qkw
I am searching for bad stuff in DogPile.com Sun Aug 05 09:12:00 2007 GMT

Form: name
ken wed Apr 11 06:41:34 2007 GMT

https://my.screenname.aol.com/_cqr/login/login.psp
User = mantooth2007
Password = wes2007
Times:
Sun Aug 05 09:08:50 2007 GMT
Sun Aug 05 09:08:50 2007 GMT
Sun Aug 05 09:09:48 2007 GMT
Sun Aug 05 09:09:48 2007 GMT

https://webauth.comcast.net/auth/login
User = dollarhyde86
Password = toothfairy
Times:
Sun Aug 05 09:08:07 2007 GMT
Sun Aug 05 09:08:07 2007 GMT

https://www.google.com/accounts/servicelogin
User = smee.rox
Password = mynameismud
Times:
Sun Aug 05 09:07:06 2007 GMT
Sun Aug 05 09:07:06 2007 GMT

http://www.marriott.com/default.mi
User = 00987654321
Password = R3@llyh@rdPa$$word
Times:
Sun Aug 05 11:14:10 2007 GMT
Sun Aug 05 11:14:10 2007 GMT
```

The text file shows 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, is also indicated.