ACCESSDATA SUPPLEMENTAL APPENDIX

Steps for Successful Password Recovery

1. In AccessData® Forensic Toolkit®, identify the encrypted files. They are located in the Overview tab > File Status > Encrypted Files container.

> **Note:** Be sure to select the Actual Files filter if exporting any document that has associated metadata. If encrypted metadata objects are exported and dropped into PRTK, they will fail.

2. Export the encrypted files from the FTK case to an external directory.

> **Note:** Do not export any EFS encrypted files, they must be decrypted inside FTK.

3. In FTK, export the Full Text Index by clicking **File > Export Word List**.

4. Skip the Select registry files windows and push the **Export** button.

> **Note**: In the Select registry files window, selecting the appropriate Registry files was for a system using IE6, which gave us access to protected storage passwords in the NTUSER.dat files. This is no longer used in modern versions of Microsoft's Internet Explorer.

5. Select a directory to export the word list to and name it with the *case_name,* click **Save**.

> **Note:** Place it in the following path, and PRTK will recognize it when importing.
>
> **C:\ProgramData\AccessData\PR\dictionaries**

6. In PRTK, import word lists such as text dictionaries to create a Code Page and Unicode Dictionary compatible with PRTK.
   a. Click Tools > Dictionary Tools.
   b. Navigate to the exported word list text file, click Select Source File.
   c. Click Generate.

7. To create a Biographical Dictionary from the Dictionary Import Utility window, click **Dictionary Tools > Biographical Dictionary Generator**.
   Enter the information into the correct field pull down list. When complete, click the Generator tab and click **Generate**. This will create a Code Page, Unicode, and XML (as-is) dictionaries.

8. In PRTK, set up an Attack Profile to utilize the desired dictionaries, languages, characters and rules.

   a. Click **Edit > Profiles**.

   b. Select the PRTK profile and select **Edit**.

c. Rename the profile to the *case name*.

d. Ensure the correct Language and Character Groups are selected.

e. In the Dictionaries pane, include the custom dictionaries you have created by placing a check in the box.

Note: Dictionaries are used in PRTK/DNA with the first used on top. To change the arrangement, click on the **Order** tab and move the dictionaries into the desired order.

f. Select the levels you want to apply to each dictionary and designate their order.

g. When finished, click **OK** to save the custom profile.

h. Close the Profile window.

8. Add the encrypted file(s) to PRTK by either dragging and dropping the file(s) onto the PRTK interface window or select **File > Add Files**..

9. In the Add Job Wizard (Page1 of 2) window, select the custom profile you created and click **Next**.

10. Select the type of attack(s) you want to perform on the file(s) in the Add Job Wizard (Page 2 of 2), click **Finish**.

11. When the passwords are recovered, right-click on the file(s) and select **Decrypt**. Save the decrypted file in an external folder.

12. To add the decrypted files back into FTK, use the Add Evidence: Click **Evidence > Add/Remove**.

13. If you are decrypting Microsoft Office files, EFS files, and/or Lotus Notes files, you can accomplish this inside of FTK without adding the files back into the case manually.

a. Click **Tools > Decrypt Files**.

b. Enter the password manually or copy and paste the password from PRTK.

c. Click **Set Password**.

d. Enter the password(s) and click **OK**.

e. Click **Decrypt**.

The file(s) that are decrypted inside of FTK will be located in the Overview tab > File Status > Decrypted Files container. Decrypted files will appear as child versions of the encrypted parent file.