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.

2. Export the encrypted files from the FTK case to an external directory.
   Note: Do not export any EFS encrypted files.

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

4. In the Select registry files window, select the appropriate Registry files.
   It is recommended to select the NTUSER.DAT Registry files, click **Export**.

   Note: You can use Registry Viewer to export word lists from Registry files outside of the case.

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

6. In PRTK import Word lists such as 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**.

   d. (Optional) 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.

7. In PRTK, set up a Dictionary Profile.

    a. Click **Edit** > **Profiles**.

    b. Select the PRTK profile and select **New from Selected**.

    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.

    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 window, select the custom profile you created, click **Next**.

10. Select the type of attack(s) you want to perform on the file(s), click **Finish**.

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

12. When the passwords are recovered, there are several options to add or decrypt the file in FTK:

    a. Option 1 (Manually adding the file back to FTK)

        i. Right-click on the file(s) and select **Decrypt**.

        ii. Save the decrypted file in an external folder.

        iii. Add the decrypted files back into FTK, use the Add Evidence Wizard to add the contents of the decrypted file(s) back into your FTK case.

        iv. Click **Evidence** > **Add/Remove**.

b. Option 2 (To add the file back with Add Decrypted File)

   Note: This will work only for Microsoft Office files, Lotus Notes (whole NSF), Lotus Notes (notes/emails), S/MIME PKCS7, and EFS. See item #13 for more details.

   i. In PRTK, right-click on the file(s) and select **Decrypt**.

   ii. Save the decrypted file in an external folder.

   iii. In FTK, return to the Encrypted container and right click on the file you want to decrypt.

   iv. Select **Add Decrypted File.**

   v. Browse to the location where the decrypted file is located. Select and click **OK**.

c. Option 3 (Using the FTK decryption functionality)

   i. In PRTK, right-click on the file and select **Copy Passwords to Clipboard**.

   ii. In FTK, click on **Tools** > **Decrypt Files**.

   iii. Click **Set Passwords**.

   iv. In the Encrypted Passwords dialog, paste in the password.

   v. Click **OK**, then click **Decrypt.**

d. Option 4 (Auto Decrypt)

   i. In FTK, right-click on the encrypted file.

   ii. Select **Auto Decrypt**.

   This will automatically export a wordlist and in PRTK it will create the necessary dictionaries and profile.

   iii. The process will begin in PRTK. If the password is found, the file will automatically be decrypted in FTK.

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 **Save Password**.

    d. Ensure the appropriate Decrypt File Types box is checked.

    e. Click **Decrypt**.

    The file(s) that are decrypted inside of FTK will be located in the Overview tab, File Status, Decrypted Files container.