

ACCESSDATA SUPPLEMENTAL APPENDIX

Steps for Successful Password Recovery—FTK 2

- 1 In AccessData® Forensic Toolkit® (FTK®), identify the encrypted files.

They are located in the Encrypted Files container of the FTK Overview tab.

- 2 Export the encrypted files from the FTK case to an external directory.
- 3 In FTK, export the Full Text Index by clicking **File > Export Word List**.

Give the word list a descriptive name that refers to your case. Include registry files that contain Protected Storage in your export.

Use the default location (the PRTK6 folder) and name (*case_name*).

- 4 In Password Recovery Toolkit® (PRTK®), click **Tools > Dictionary Tools** and import the word list as a dictionary. Also use the Biographical Dictionary Generator to generate a biographical dictionary.
- 5 (Conditional) If you have additional information that might be useful in the password recovery, create a user-defined dictionary in a text file.

Consider guerrilla tactics such as using HTT Track and Passphrase Generator to index the subject's favorite Web sites or to process potential words that can be combined into passphrases. You can then export the Web index to create another user-defined dictionary.

- 6 Use Registry Viewer® or FTK 2 to export word lists from applicable registry files if you did not do this in Step 3.
- 7 In PRTK, import word lists such as dictionaries to create codepage and Unicode dictionaries that are compatible with PRTK.
 - 7a Click **Tools > Dictionary Tools > Import**.
 - 7b Navigate to the text file.
 - 7c (Optional) Provide a file description.
 - 7d Click **Import**.

- 8 In PRTK, set up a dictionary profile.
 - 8a Click **Edit > Profiles > New**.
 - 8b Select the dictionaries that you want to use.
 - 8c Select the levels that you want to apply to each dictionary and designate their order.
- 9 (Conditional) If necessary, click **Edit > Profiles > New** to create new levels.
- 10 Include the custom levels in your dictionary profile.
- 11 Add the encrypted files to PRTK and recover the passwords.

Depending on the file type, you may select the types of cracks PRTK performs.
- 12 When passwords are recovered, open the corresponding files, remove the passwords, and use the Save As option to save the decrypted files to an external folder.
- 13 In FTK 2, click **Evidence > Add/Remove** to add the contents of the decrypted files folder back to your case.

Important: Ensure each file is closed before adding it as evidence.

- 14 Continue the investigation, remembering the “AccessData Attack Methodology” attack methodology.
- 15 Index the decrypted files you add to the case.
- 16 Export the updated case index and import as a new dictionary in PRTK.

Use the default location (the PRTK6 folder) and name (*case_name*).
- 17 Add the Full-Text Index dictionary to the dictionary profile.
- 18 Resume the dictionary attack.
- 19 Decrypt EFS files in FTK.

To decrypt EFS files, you can select the **Decrypt EFS Passwords** process as you add evidence to your case, or you can click **Tools > Add Passwords** and then **Tools > Decrypt Files**.

If FTK does not decrypt the EFS files, you might have a Windows XP SP1 or later system. In this case, you must first break the logon password from the SAM file. Add the SAM file to PRTK and, when prompted, point to the SYSTEM file to obtain the SysKey.

PRTK then conducts a dictionary attack against the SAM file to obtain the logon password. Make sure all the dictionaries are included in the PRTK dictionary profile before starting this procedure. When you obtain the logon password, return to FTK, click **Tools > Add Passwords**, then follow the procedure to decrypt the EFS files.

