AccessData®

# PRTK

Password Recovery ToolKit

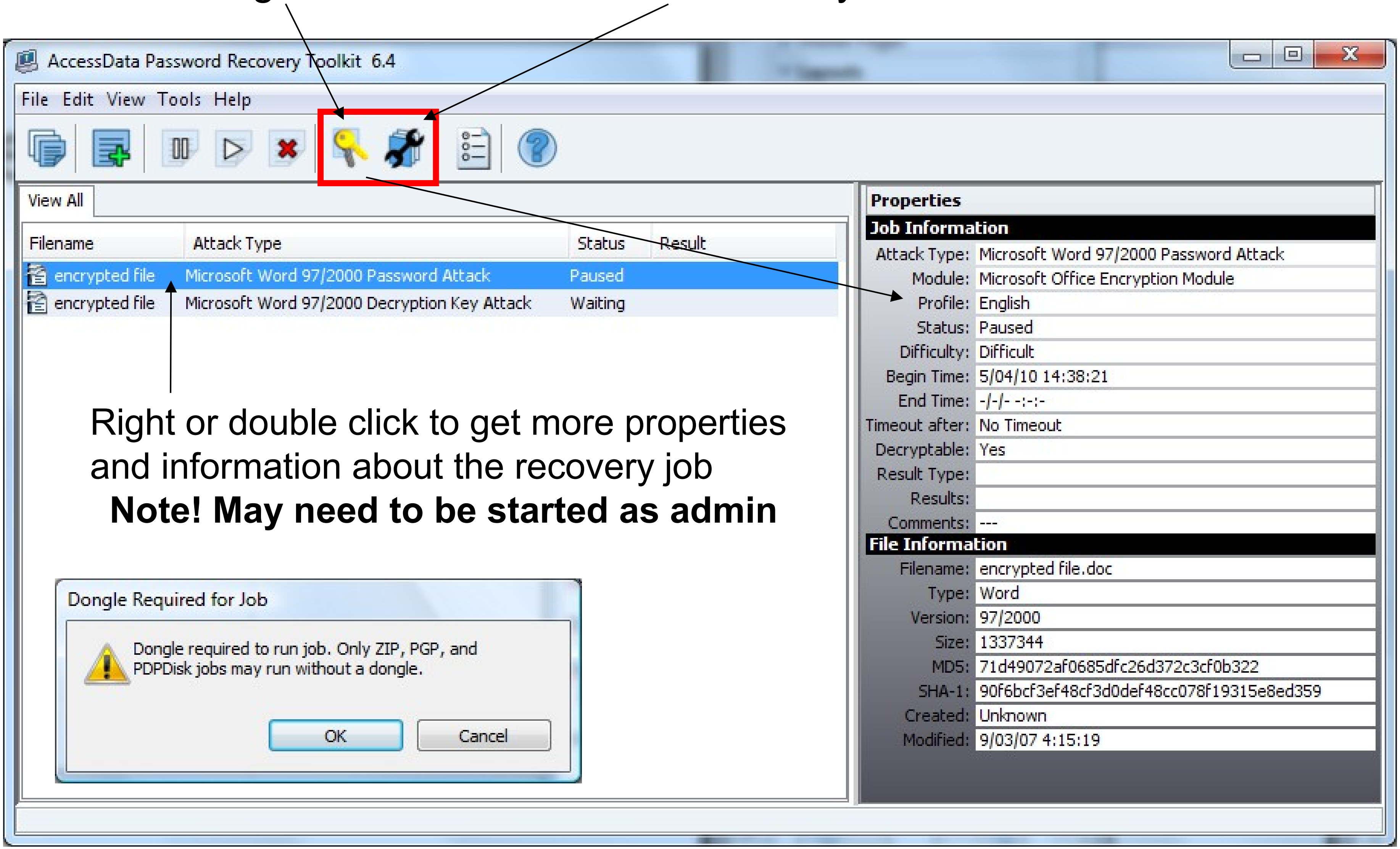
EFS (Encrypting File System)

http://en.wikipedia.org/wiki/Encrypting_File_System

# PRTK Overview - Interface

Manage Profiles...

Dictionary Tools...



| Filename | Attack Type | Status | Result |
|---|---|---|---|
| encrypted file | Microsoft Word 97/2000 Password Attack | Paused | |
| encrypted file | Microsoft Word 97/2000 Decryption Key Attack | Waiting | |

**Job Information**

| | |
|---|---|
| Attack Type: | Microsoft Word 97/2000 Password Attack |
| Module: | Microsoft Office Encryption Module |
| Profile: | English |
| Status: | Paused |
| Difficulty: | Difficult |
| Begin Time: | 5/04/10 14:38:21 |
| End Time: | -/-/- -:-:- |
| Timeout after: | No Timeout |
| Decryptable: | Yes |
| Result Type: | |
| Results: | |
| Comments: | --- |

**File Information**

| | |
|---|---|
| Filename: | encrypted file.doc |
| Type: | Word |
| Version: | 97/2000 |
| Size: | 1337344 |
| MD5: | 71d49072af0685dfc26d372c3cf0b322 |
| SHA-1: | 90f6bcf3ef48cf3d0def48cc078f19315e8ed359 |
| Created: | Unknown |
| Modified: | 9/03/07 4:15:19 |

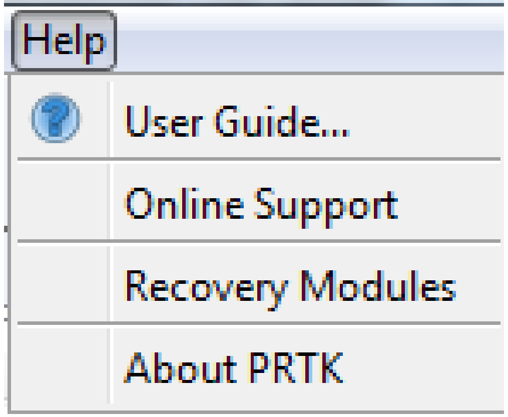
Right or double click to get more properties and information about the recovery job

**Note! May need to be started as admin**

Dongle Required for Job

Dongle required to run job. Only ZIP, PGP, and PDPDisk jobs may run without a dongle.

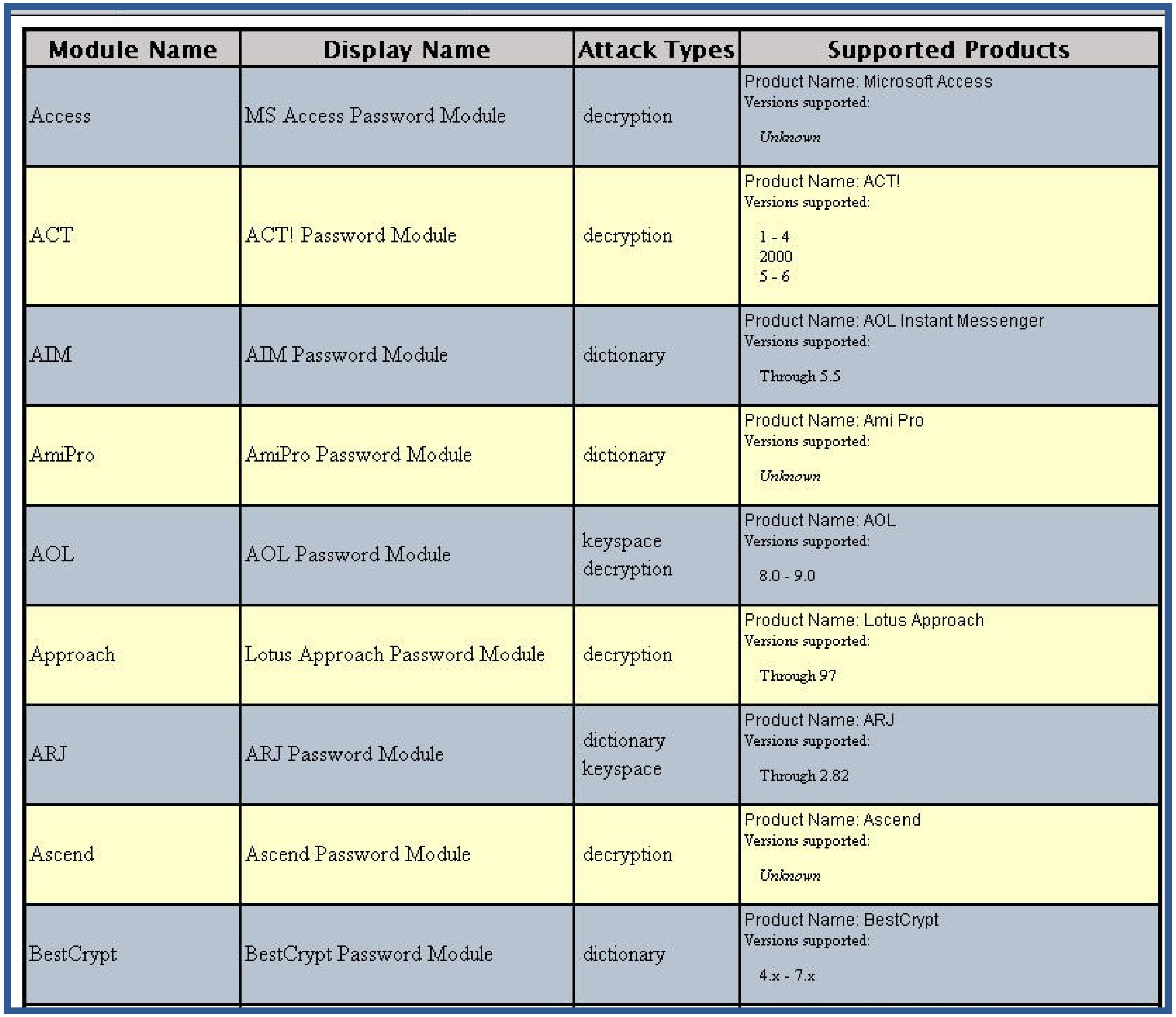
# PRTK Overview - Modules



**Help > User Guide...**
**F1 - Very good!**

**Recovery Modules →**

**RM listing is also available in the user guide**

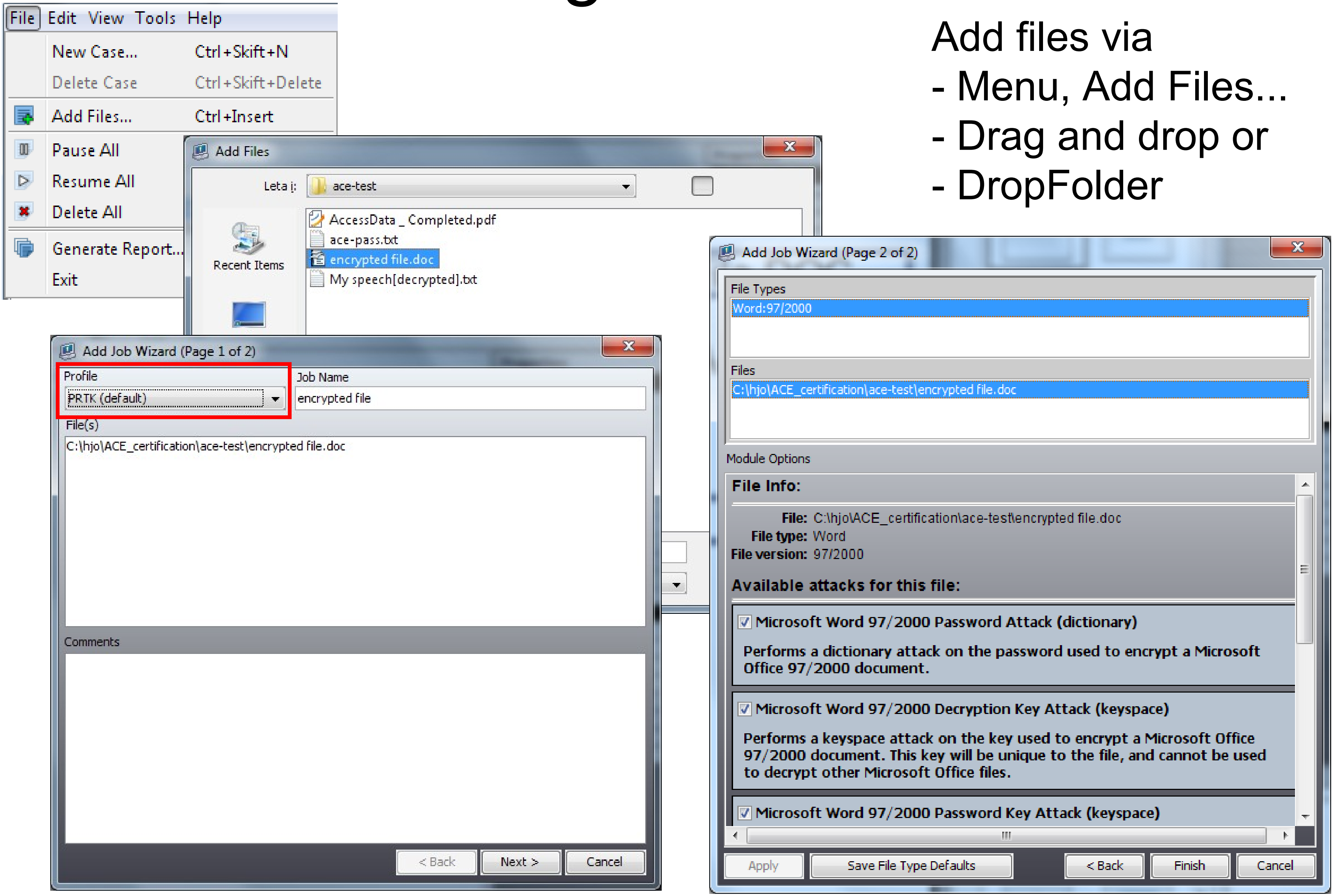


| Module Name | Display Name | Attack Types | Supported Products |
|---|---|---|---|
| Access | MS Access Password Module | decryption | Product Name: Microsoft Access<br>Versions supported:<br>*Unknown* |
| ACT | ACT! Password Module | decryption | Product Name: ACT!<br>Versions supported:<br>1 - 4<br>2000<br>5 - 6 |
| AIM | AIM Password Module | dictionary | Product Name: AOL Instant Messenger<br>Versions supported:<br>Through 5.5 |
| AmiPro | AmiPro Password Module | dictionary | Product Name: Ami Pro<br>Versions supported:<br>*Unknown* |
| AOL | AOL Password Module | keyspace<br>decryption | Product Name: AOL<br>Versions supported:<br>8.0 - 9.0 |
| Approach | Lotus Approach Password Module | decryption | Product Name: Lotus Approach<br>Versions supported:<br>Through 97 |
| ARJ | ARJ Password Module | dictionary<br>keyspace | Product Name: ARJ<br>Versions supported:<br>Through 2.82 |
| Ascend | Ascend Password Module | decryption | Product Name: Ascend<br>Versions supported:<br>*Unknown* |
| BestCrypt | BestCrypt Password Module | dictionary | Product Name: BestCrypt<br>Versions supported:<br>4.x - 7.x |

Goes on to Z … ~ 110 modules

# Starting a Session

Add files via
- Menu, Add Files...
- Drag and drop or
- DropFolder



Leta i: ace-test

AccessData _ Completed.pdf
ace-pass.txt
encrypted file.doc
My speech[decrypted].txt

Profile: PRTK (default)

Job Name: encrypted file

File(s): C:\hjo\ACE_certification\ace-test\encrypted file.doc

Comments

File Types: Word:97/2000

Files: C:\hjo\ACE_certification\ace-test\encrypted file.doc

Module Options

**File Info:**

**File:** C:\hjo\ACE_certification\ace-test\encrypted file.doc
**File type:** Word
**File version:** 97/2000

**Available attacks for this file:**

☑ **Microsoft Word 97/2000 Password Attack (dictionary)**

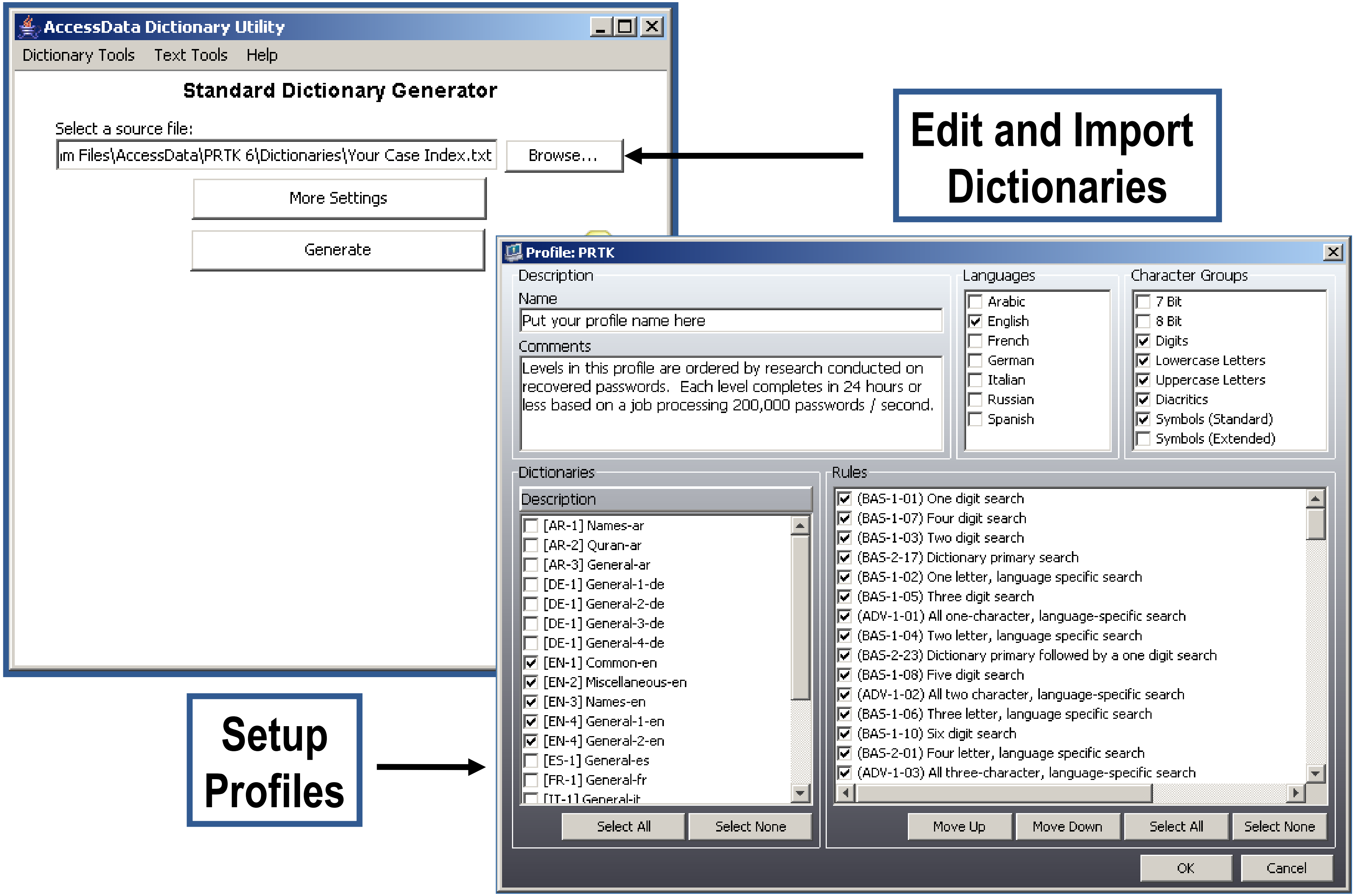
**Performs a dictionary attack on the password used to encrypt a Microsoft Office 97/2000 document.**

☑ **Microsoft Word 97/2000 Decryption Key Attack (keyspace)**

**Performs a keyspace attack on the key used to encrypt a Microsoft Office 97/2000 document. This key will be unique to the file, and cannot be used to decrypt other Microsoft Office files.**

☑ **Microsoft Word 97/2000 Password Key Attack (keyspace)**

# Setup Options



AccessData Dictionary Utility

**Standard Dictionary Generator**

Select a source file: im Files\AccessData\PRTK 6\Dictionaries\Your Case Index.txt

Profile: PRTK

Description

Name: Put your profile name here

Comments: Levels in this profile are ordered by research conducted on recovered passwords. Each level completes in 24 hours or less based on a job processing 200,000 passwords / second.

Languages

- □ Arabic
- ☑ English
- □ French
- □ German
- □ Italian
- □ Russian
- □ Spanish

Character Groups

- □ 7 Bit
- □ 8 Bit
- ☑ Digits
- ☑ Lowercase Letters
- ☑ Uppercase Letters
- ☑ Diacritics
- ☑ Symbols (Standard)
- □ Symbols (Extended)

Dictionaries

Description

- □ [AR-1] Names-ar
- □ [AR-2] Quran-ar
- □ [AR-3] General-ar
- □ [DE-1] General-1-de
- □ [DE-1] General-2-de
- □ [DE-1] General-3-de
- □ [DE-1] General-4-de
- ☑ [EN-1] Common-en
- ☑ [EN-2] Miscellaneous-en
- ☑ [EN-3] Names-en
- ☑ [EN-4] General-1-en
- ☑ [EN-4] General-2-en
- □ [ES-1] General-es
- □ [FR-1] General-fr
- □ [IT-1] General-it

Rules

- ☑ (BAS-1-01) One digit search
- ☑ (BAS-1-07) Four digit search
- ☑ (BAS-1-03) Two digit search
- ☑ (BAS-2-17) Dictionary primary search
- ☑ (BAS-1-02) One letter, language specific search
- ☑ (BAS-1-05) Three digit search
- ☑ (ADV-1-01) All one-character, language-specific search
- ☑ (BAS-1-04) Two letter, language specific search
- ☑ (BAS-2-23) Dictionary primary followed by a one digit search
- ☑ (BAS-1-08) Five digit search
- ☑ (ADV-1-02) All two character, language-specific search
- ☑ (BAS-1-06) Three letter, language specific search
- ☑ (BAS-1-10) Six digit search
- ☑ (BAS-2-01) Four letter, language specific search
- ☑ (ADV-1-03) All three-character, language-specific search

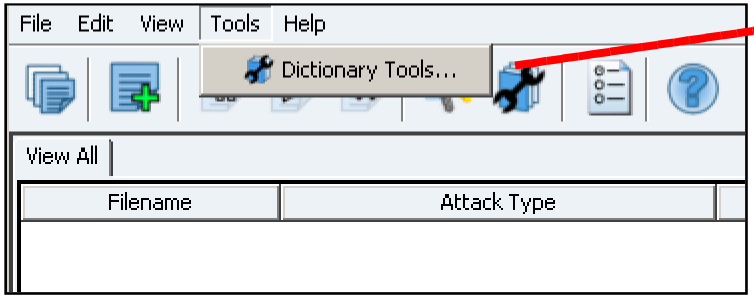
**Edit and Import Dictionaries**

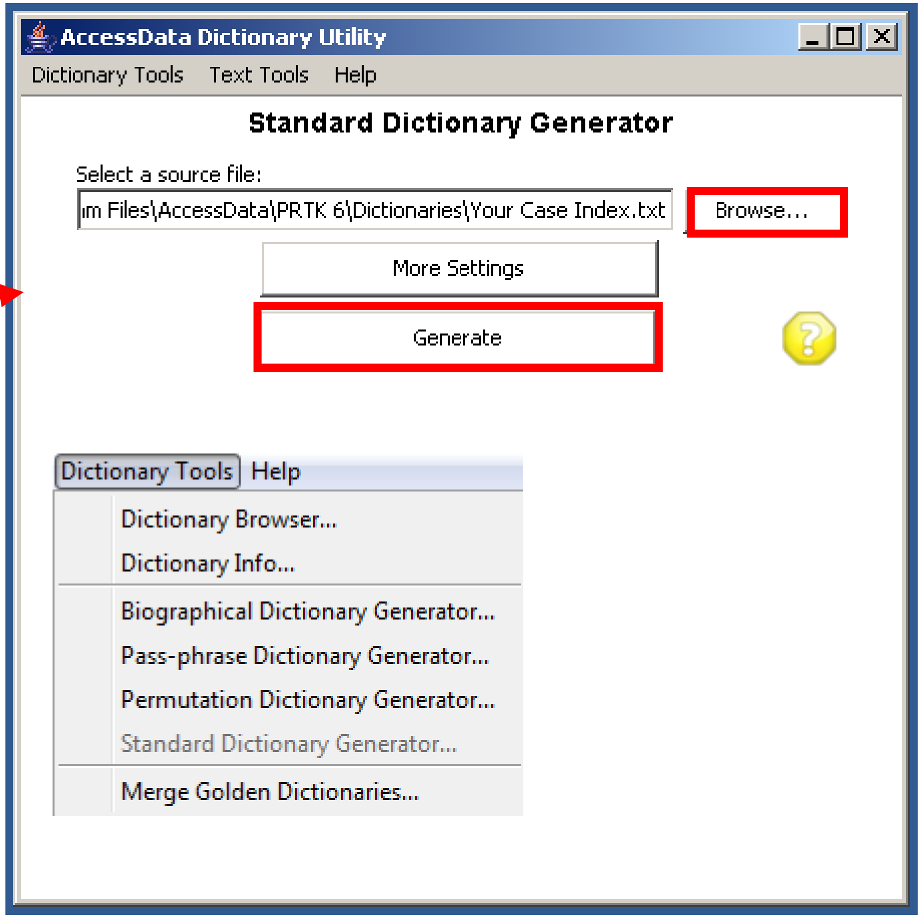
**Setup Profiles**

# Importing a new dictionary

## Add new dictionaries (from your word lists)

- Full-text index from FTK
- Other user-created text file

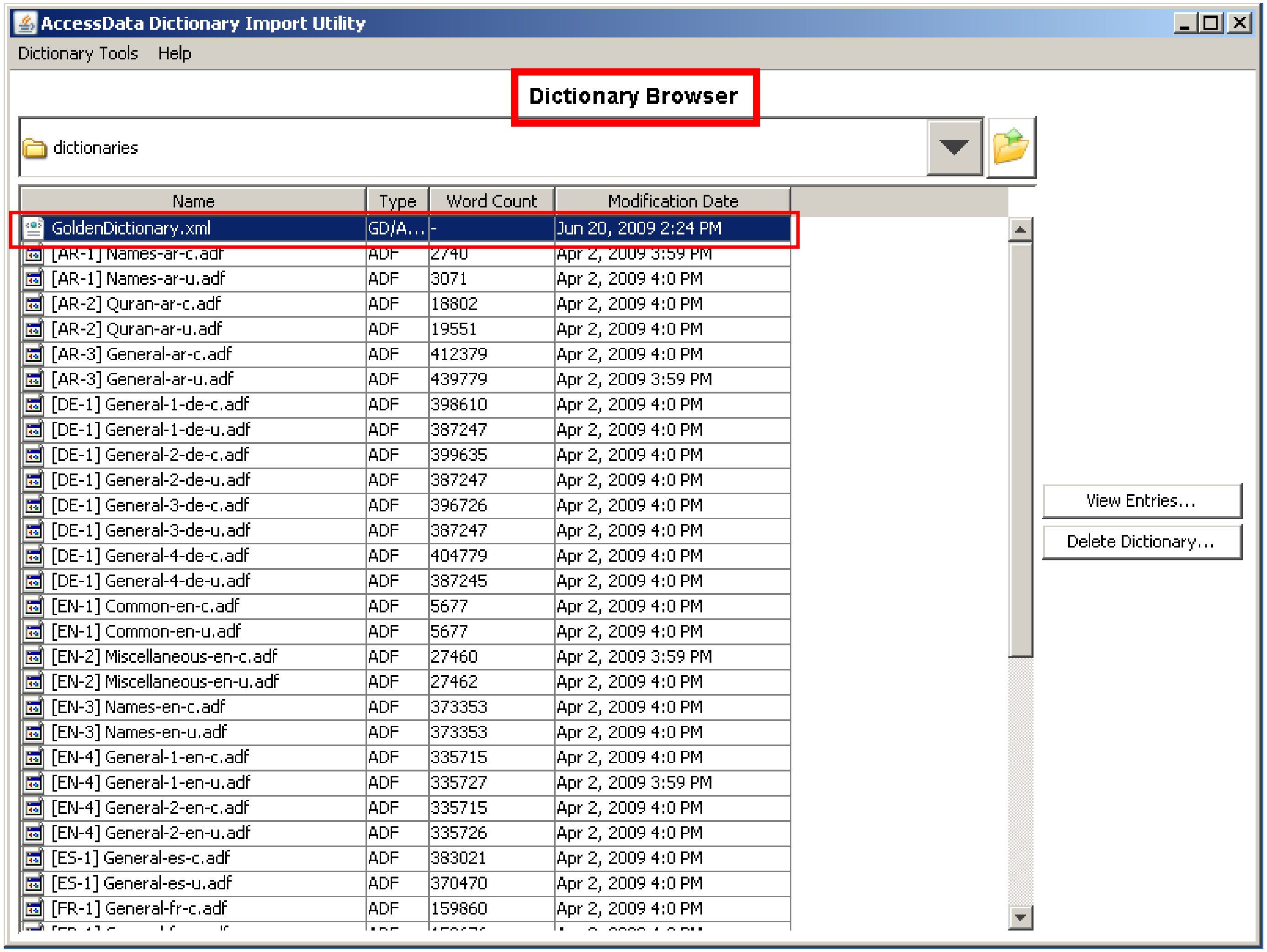



AccessData Dictionary Utility
Dictionary Tools
Text Tools
Help
Standard Dictionary Generator
Browse...
More Settings
Generate
Dictionary Tools
Help
Dictionary Browser...
Dictionary Info...
Biographical Dictionary Generator...
Pass-phrase Dictionary Generator...
Permutation Dictionary Generator...
Standard Dictionary Generator...
Merge Golden Dictionaries...

Select a source file: ım Files\AccessData\PRTK 6\Dictionaries\Your Case Index.txt

”More Settings” button depends on dictionary type, contains
- Dictionary Settings
- Word Settings

# Importing a new dictionary

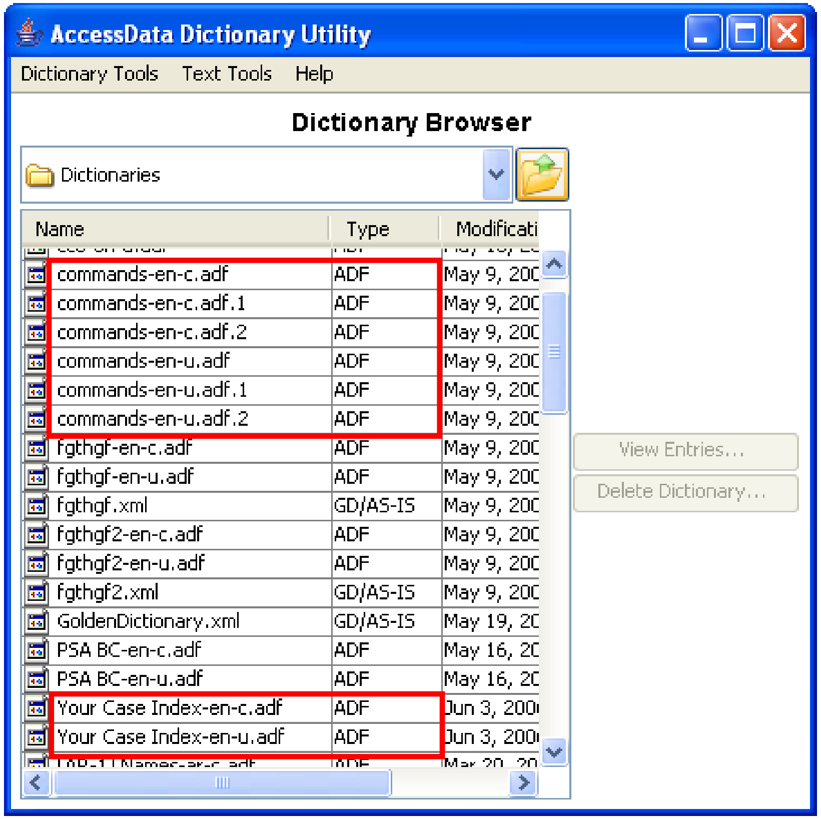


| Name | Type | Word Count | Modification Date |
|---|---|---|---|
| GoldenDictionary.xml | GD/A... | - | Jun 20, 2009 2:24 PM |
| [AR-1] Names-ar-c.adf | ADF | 2740 | Apr 2, 2009 3:59 PM |
| [AR-1] Names-ar-u.adf | ADF | 3071 | Apr 2, 2009 4:0 PM |
| [AR-2] Quran-ar-c.adf | ADF | 18802 | Apr 2, 2009 4:0 PM |
| [AR-2] Quran-ar-u.adf | ADF | 19551 | Apr 2, 2009 4:0 PM |
| [AR-3] General-ar-c.adf | ADF | 412379 | Apr 2, 2009 4:0 PM |
| [AR-3] General-ar-u.adf | ADF | 439779 | Apr 2, 2009 3:59 PM |
| [DE-1] General-1-de-c.adf | ADF | 398610 | Apr 2, 2009 4:0 PM |
| [DE-1] General-1-de-u.adf | ADF | 387247 | Apr 2, 2009 4:0 PM |
| [DE-1] General-2-de-c.adf | ADF | 399635 | Apr 2, 2009 4:0 PM |
| [DE-1] General-2-de-u.adf | ADF | 387247 | Apr 2, 2009 4:0 PM |
| [DE-1] General-3-de-c.adf | ADF | 396726 | Apr 2, 2009 4:0 PM |
| [DE-1] General-3-de-u.adf | ADF | 387247 | Apr 2, 2009 4:0 PM |
| [DE-1] General-4-de-c.adf | ADF | 404779 | Apr 2, 2009 4:0 PM |
| [DE-1] General-4-de-u.adf | ADF | 387245 | Apr 2, 2009 4:0 PM |
| [EN-1] Common-en-c.adf | ADF | 5677 | Apr 2, 2009 4:0 PM |
| [EN-1] Common-en-u.adf | ADF | 5677 | Apr 2, 2009 4:0 PM |
| [EN-2] Miscellaneous-en-c.adf | ADF | 27460 | Apr 2, 2009 3:59 PM |
| [EN-2] Miscellaneous-en-u.adf | ADF | 27462 | Apr 2, 2009 4:0 PM |
| [EN-3] Names-en-c.adf | ADF | 373353 | Apr 2, 2009 4:0 PM |
| [EN-3] Names-en-u.adf | ADF | 373353 | Apr 2, 2009 4:0 PM |
| [EN-4] General-1-en-c.adf | ADF | 335715 | Apr 2, 2009 4:0 PM |
| [EN-4] General-1-en-u.adf | ADF | 335727 | Apr 2, 2009 3:59 PM |
| [EN-4] General-2-en-c.adf | ADF | 335715 | Apr 2, 2009 4:0 PM |
| [EN-4] General-2-en-u.adf | ADF | 335726 | Apr 2, 2009 4:0 PM |
| [ES-1] General-es-c.adf | ADF | 383021 | Apr 2, 2009 4:0 PM |
| [ES-1] General-es-u.adf | ADF | 370470 | Apr 2, 2009 4:0 PM |
| [FR-1] General-fr-c.adf | ADF | 159860 | Apr 2, 2009 4:0 PM |

**Windows Vista/7**
**C:\ProgramData\AccessData\PR\dictionaries**

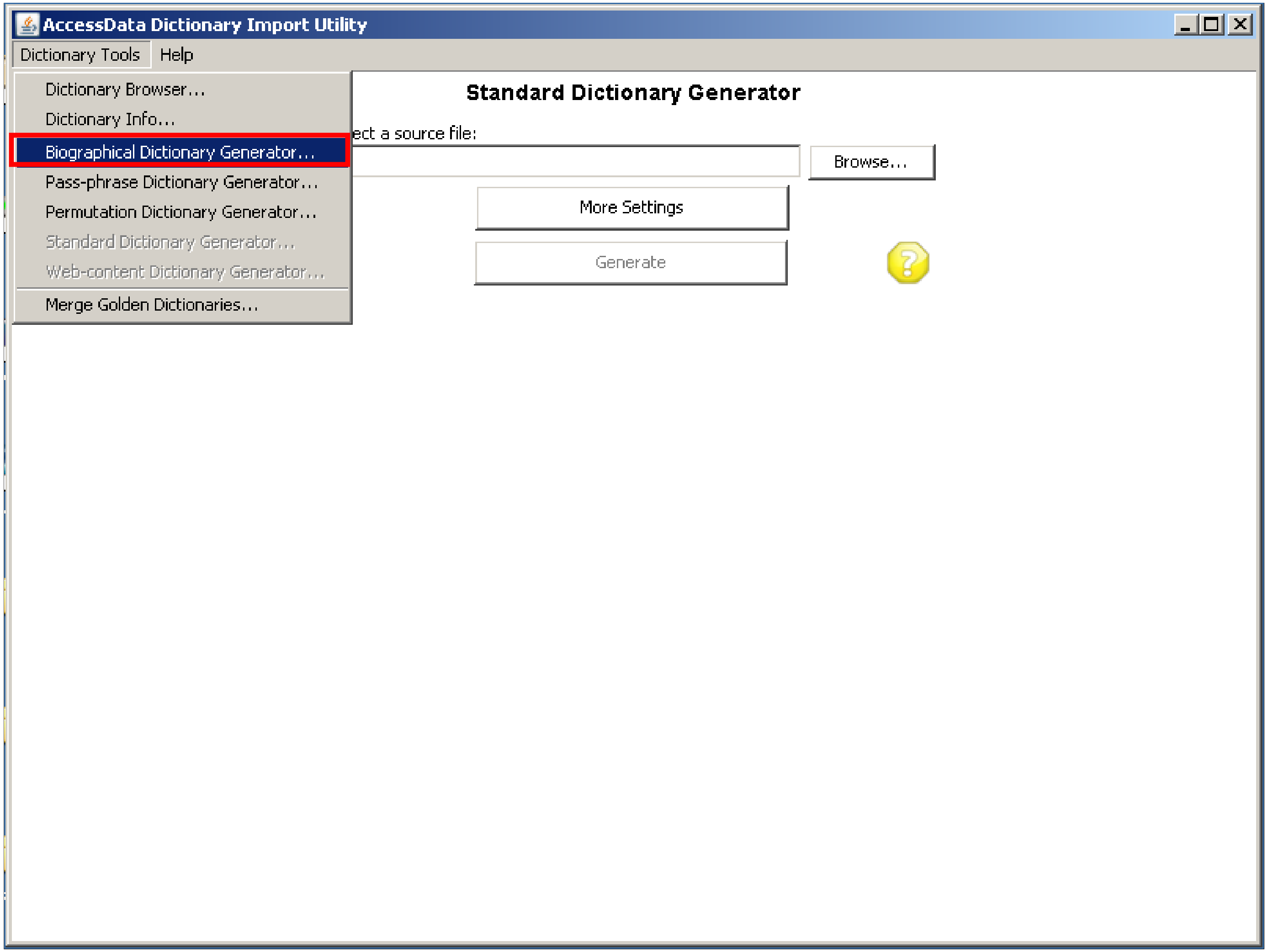
# Importing a new dictionary

- Codepage (-c) and Unicode (-u)
- Large dictionaries segmented at 500,000 words

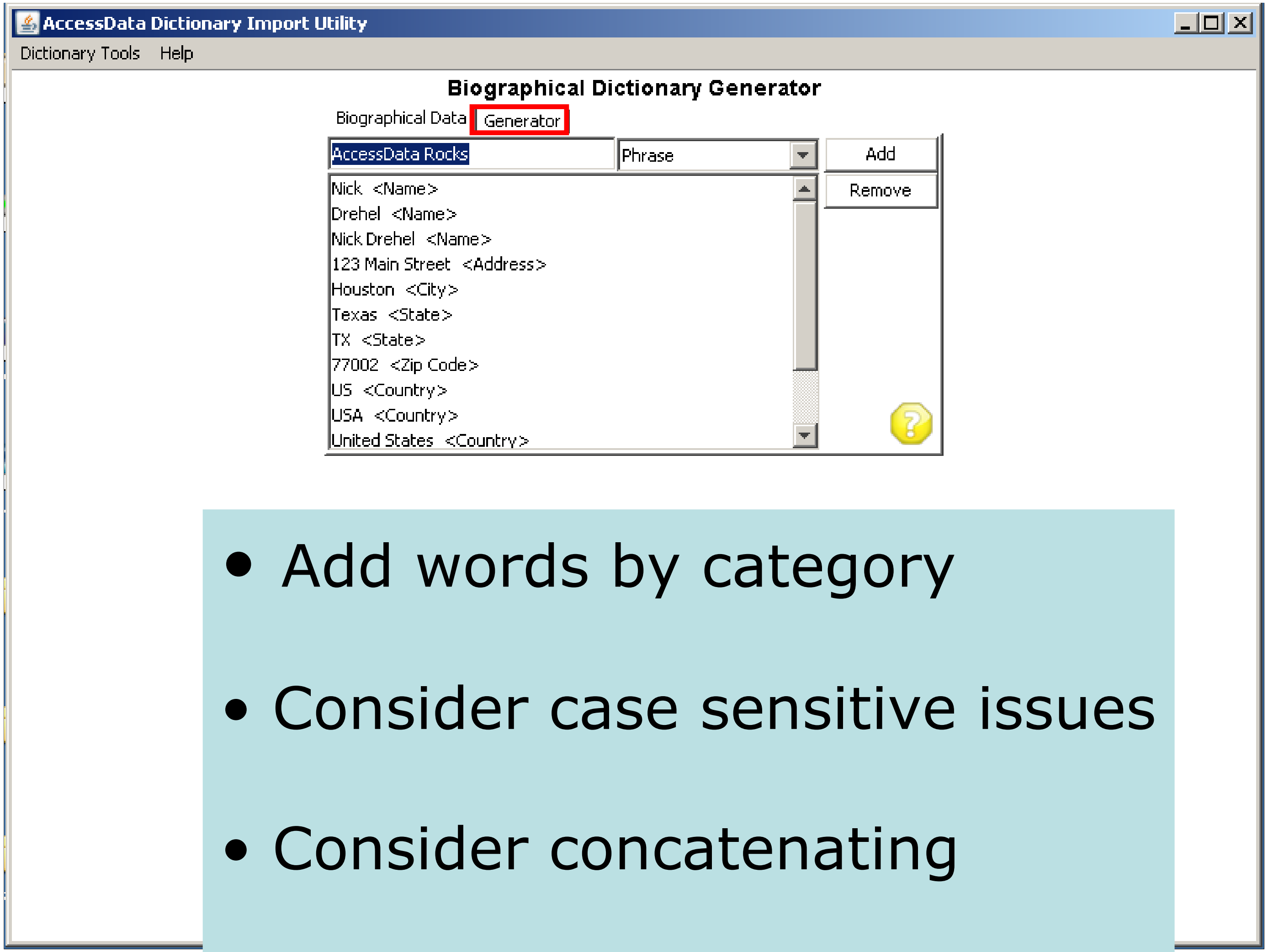


| Name | Type | Modificati |
|---|---|---|
| commands-en-c.adf | ADF | May 9, 200 |
| commands-en-c.adf.1 | ADF | May 9, 200 |
| commands-en-c.adf.2 | ADF | May 9, 200 |
| commands-en-u.adf | ADF | May 9, 200 |
| commands-en-u.adf.1 | ADF | May 9, 200 |
| commands-en-u.adf.2 | ADF | May 9, 200 |
| fgthgf-en-c.adf | ADF | May 9, 200 |
| fgthgf-en-u.adf | ADF | May 9, 200 |
| fgthgf.xml | GD/AS-IS | May 9, 200 |
| fgthgf2-en-c.adf | ADF | May 9, 200 |
| fgthgf2-en-u.adf | ADF | May 9, 200 |
| fgthgf2.xml | GD/AS-IS | May 9, 200 |
| GoldenDictionary.xml | GD/AS-IS | May 19, 20 |
| PSA BC-en-c.adf | ADF | May 16, 20 |
| PSA BC-en-u.adf | ADF | May 16, 20 |
| Your Case Index-en-c.adf | ADF | Jun 3, 200 |
| Your Case Index-en-u.adf | ADF | Jun 3, 200 |

# Biographical Dictionary


AccessData Dictionary Import Utility
Dictionary Tools
Help
Dictionary Browser...
Dictionary Info...
Biographical Dictionary Generator...
Pass-phrase Dictionary Generator...
Permutation Dictionary Generator...
Standard Dictionary Generator...
Web-content Dictionary Generator...
Merge Golden Dictionaries...
Standard Dictionary Generator
ect a source file:
Browse...
More Settings
Generate

# Biographical Dictionary


AccessData Dictionary Import Utility
Dictionary Tools
Help
Biographical Dictionary Generator
Biographical Data
Generator
Add
Remove

AccessData Rocks

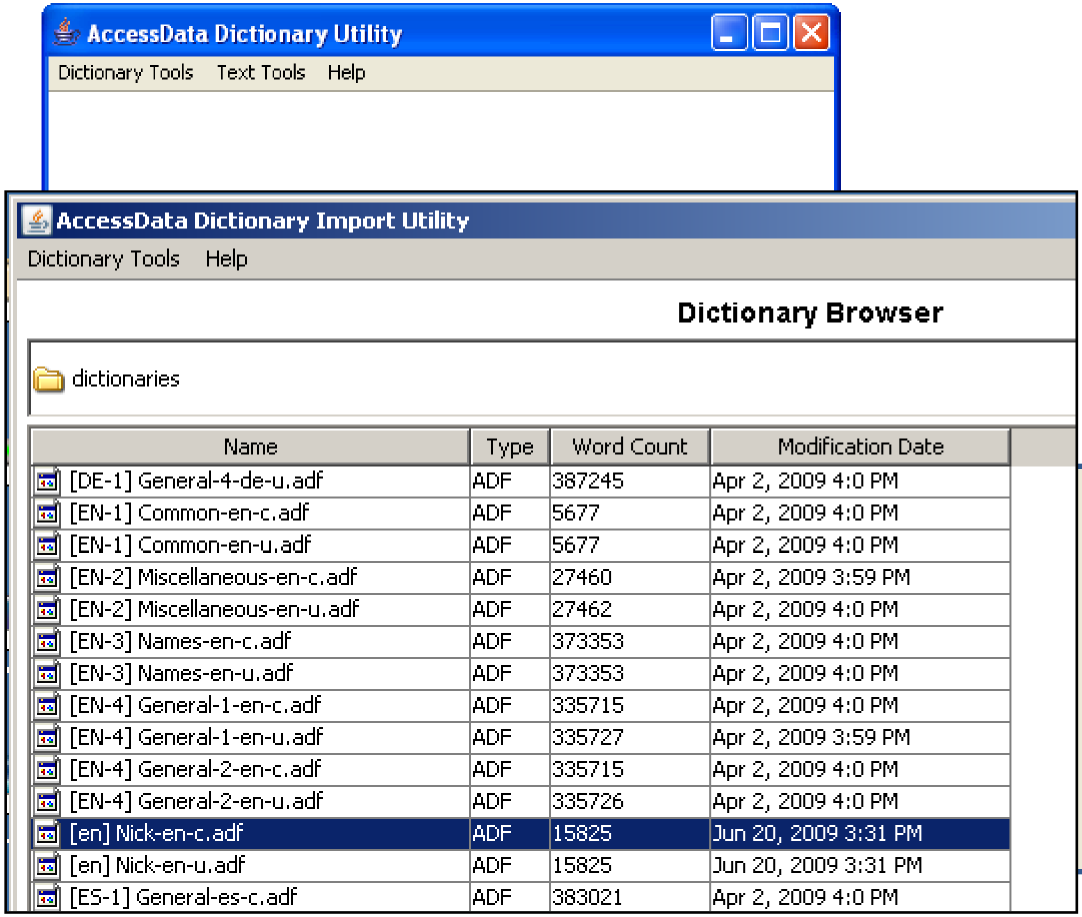
Phrase

Nick <Name>
Drehel <Name>
Nick Drehel <Name>
123 Main Street <Address>
Houston <City>
Texas <State>
TX <State>
77002 <Zip Code>
US <Country>
USA <Country>
United States <Country>

- Add words by category
- Consider case sensitive issues
- Consider concatenating
- Generate when complete

# Biographical Dictionary

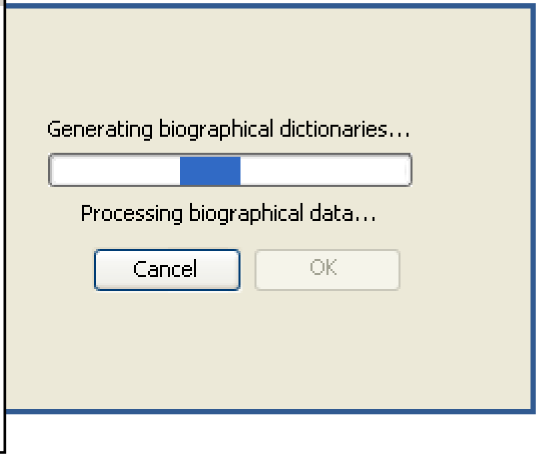
**The 14 entries generated almost 16,000 words in the dictionary!**



| Name | Type | Word Count | Modification Date |
|---|---|---|---|
| [DE-1] General-4-de-u.adf | ADF | 387245 | Apr 2, 2009 4:0 PM |
| [EN-1] Common-en-c.adf | ADF | 5677 | Apr 2, 2009 4:0 PM |
| [EN-1] Common-en-u.adf | ADF | 5677 | Apr 2, 2009 4:0 PM |
| [EN-2] Miscellaneous-en-c.adf | ADF | 27460 | Apr 2, 2009 3:59 PM |
| [EN-2] Miscellaneous-en-u.adf | ADF | 27462 | Apr 2, 2009 4:0 PM |
| [EN-3] Names-en-c.adf | ADF | 373353 | Apr 2, 2009 4:0 PM |
| [EN-3] Names-en-u.adf | ADF | 373353 | Apr 2, 2009 4:0 PM |
| [EN-4] General-1-en-c.adf | ADF | 335715 | Apr 2, 2009 4:0 PM |
| [EN-4] General-1-en-u.adf | ADF | 335727 | Apr 2, 2009 3:59 PM |
| [EN-4] General-2-en-c.adf | ADF | 335715 | Apr 2, 2009 4:0 PM |
| [EN-4] General-2-en-u.adf | ADF | 335726 | Apr 2, 2009 4:0 PM |
| [en] Nick-en-c.adf | ADF | 15825 | Jun 20, 2009 3:31 PM |
| [en] Nick-en-u.adf | ADF | 15825 | Jun 20, 2009 3:31 PM |
| [ES-1] General-es-c.adf | ADF | 383021 | Apr 2, 2009 4:0 PM |

## Results in:

- Codepage
- Unicode
- XML (AS-IS)



Generating biographical dictionaries...

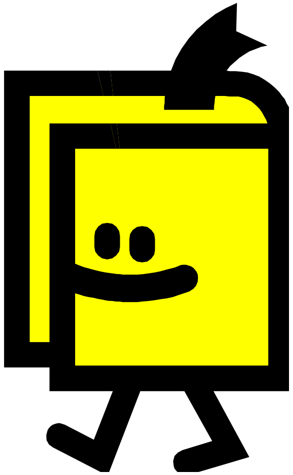
Processing biographical data...

# Other dictionaries & Golden Dictionary

- Permutation Dictionary
  - Builds dictionaries by using permutations of words from a word list file
- Pass-phrase Dictionary
  - Builds dictionaries from a phrase file

**Attack Level**

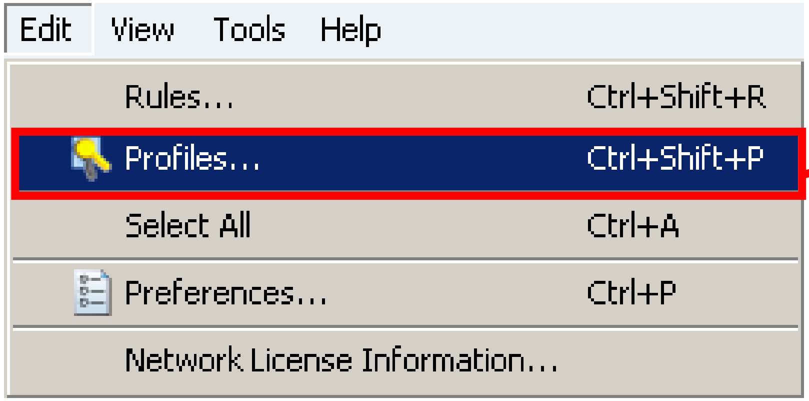
**GoldenDictionary.xml = Golden Dictionary**

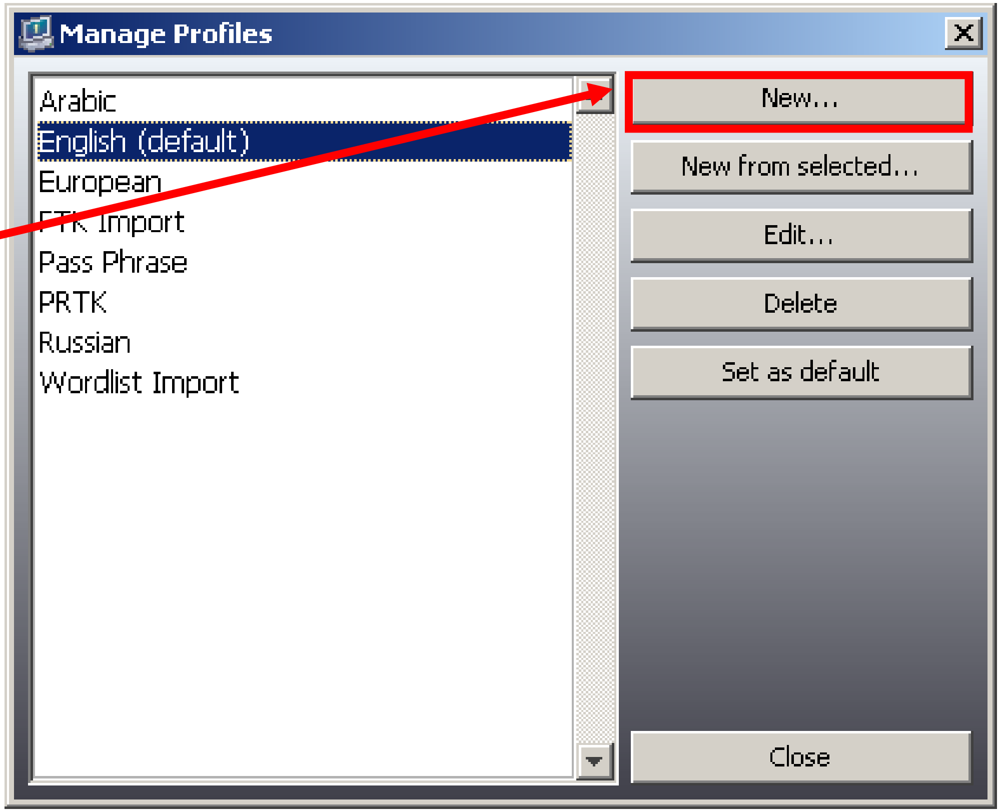


**Windows Vista/7**
**C:\ProgramData\AccessData\PR\dictionaries**

# Setting Up a New Profile

Set up a customized profile to dictate how PRTK attacks the encrypted file

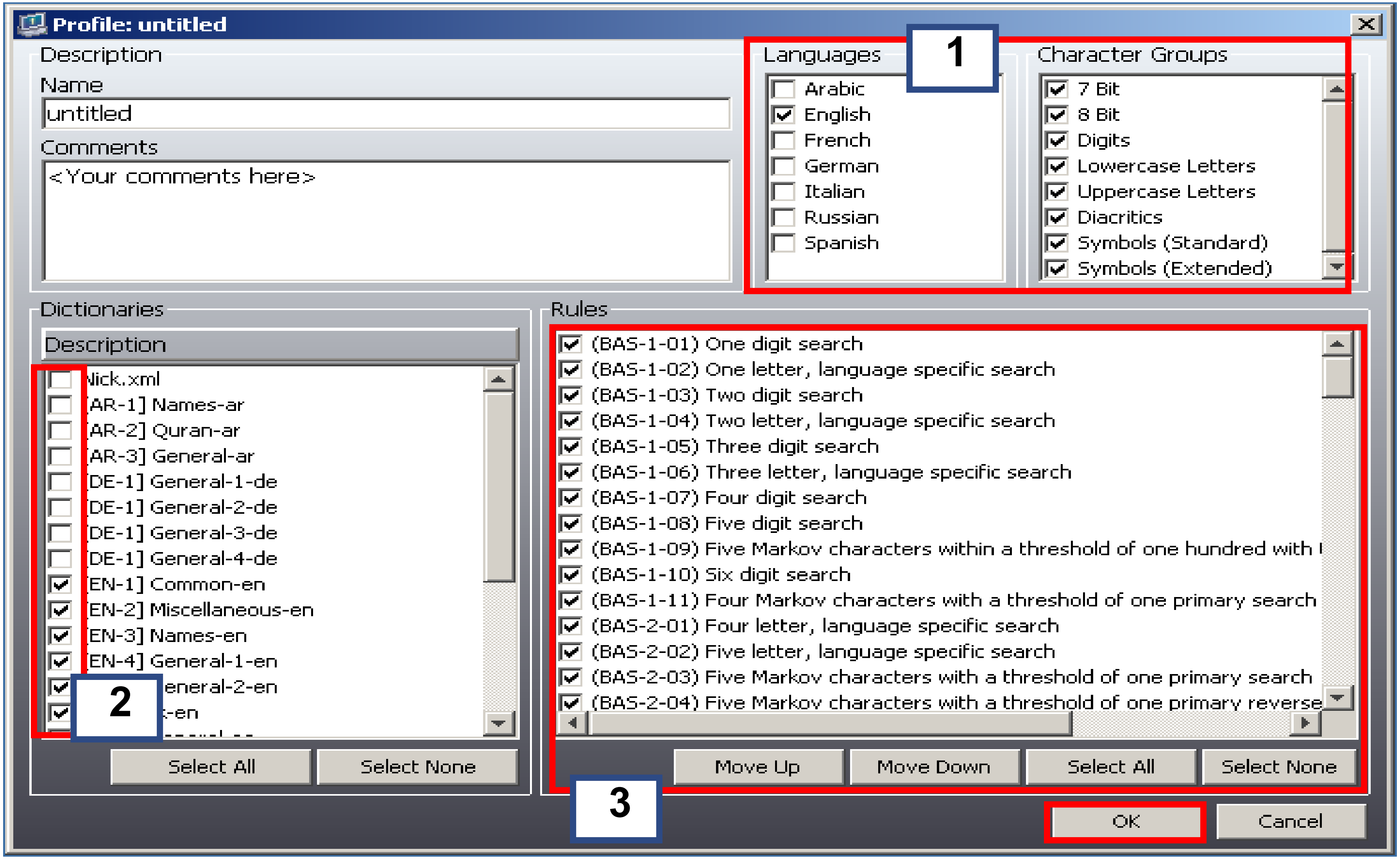




Använd **PRTK** profile och
**New from selected...**
Lägg till eventuellt **eget dictionary från word list**
Spara din nya profil
Nu är det svårt att misslyckas!

**BAS-2-17 Dictionary primary search**

# Setting Up a New Profile



**Profile: untitled**

Description

Name: untitled

Comments: <Your comments here>

Languages

- □ Arabic
- ☑ English
- □ French
- □ German
- □ Italian
- □ Russian
- □ Spanish

Character Groups

- ☑ 7 Bit
- ☑ 8 Bit
- ☑ Digits
- ☑ Lowercase Letters
- ☑ Uppercase Letters
- ☑ Diacritics
- ☑ Symbols (Standard)
- ☑ Symbols (Extended)

Dictionaries

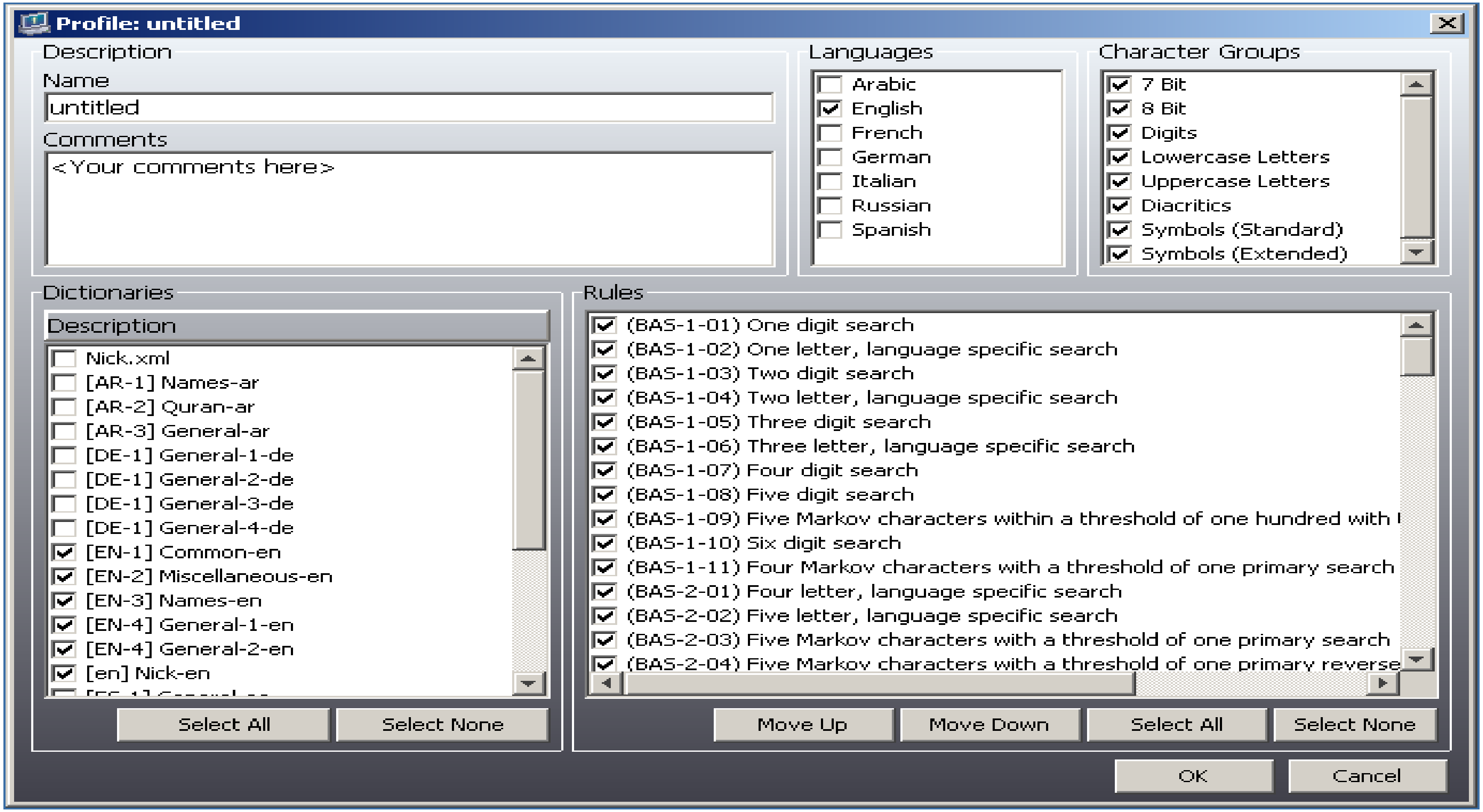
Description

- □ Nick.xml
- □ AR-1] Names-ar
- □ AR-2] Quran-ar
- □ AR-3] General-ar
- □ DE-1] General-1-de
- □ DE-1] General-2-de
- □ DE-1] General-3-de
- □ DE-1] General-4-de
- ☑ EN-1] Common-en
- ☑ EN-2] Miscellaneous-en
- ☑ EN-3] Names-en
- ☑ EN-4] General-1-en
- ☑ eneral-2-en
- ☑ -en

Rules

- ☑ (BAS-1-01) One digit search
- ☑ (BAS-1-02) One letter, language specific search
- ☑ (BAS-1-03) Two digit search
- ☑ (BAS-1-04) Two letter, language specific search
- ☑ (BAS-1-05) Three digit search
- ☑ (BAS-1-06) Three letter, language specific search
- ☑ (BAS-1-07) Four digit search
- ☑ (BAS-1-08) Five digit search
- ☑ (BAS-1-09) Five Markov characters within a threshold of one hundred with
- ☑ (BAS-1-10) Six digit search
- ☑ (BAS-1-11) Four Markov characters with a threshold of one primary search
- ☑ (BAS-2-01) Four letter, language specific search
- ☑ (BAS-2-02) Five letter, language specific search
- ☑ (BAS-2-03) Five Markov characters with a threshold of one primary search
- ☑ (BAS-2-04) Five Markov characters with a threshold of one primary reverse

# The New Profile



**Profile: untitled**

Description

Name: untitled

Comments: <Your comments here>

Languages

- □ Arabic
- ☑ English
- □ French
- □ German
- □ Italian
- □ Russian
- □ Spanish

Character Groups

- ☑ 7 Bit
- ☑ 8 Bit
- ☑ Digits
- ☑ Lowercase Letters
- ☑ Uppercase Letters
- ☑ Diacritics
- ☑ Symbols (Standard)
- ☑ Symbols (Extended)

Dictionaries

Description

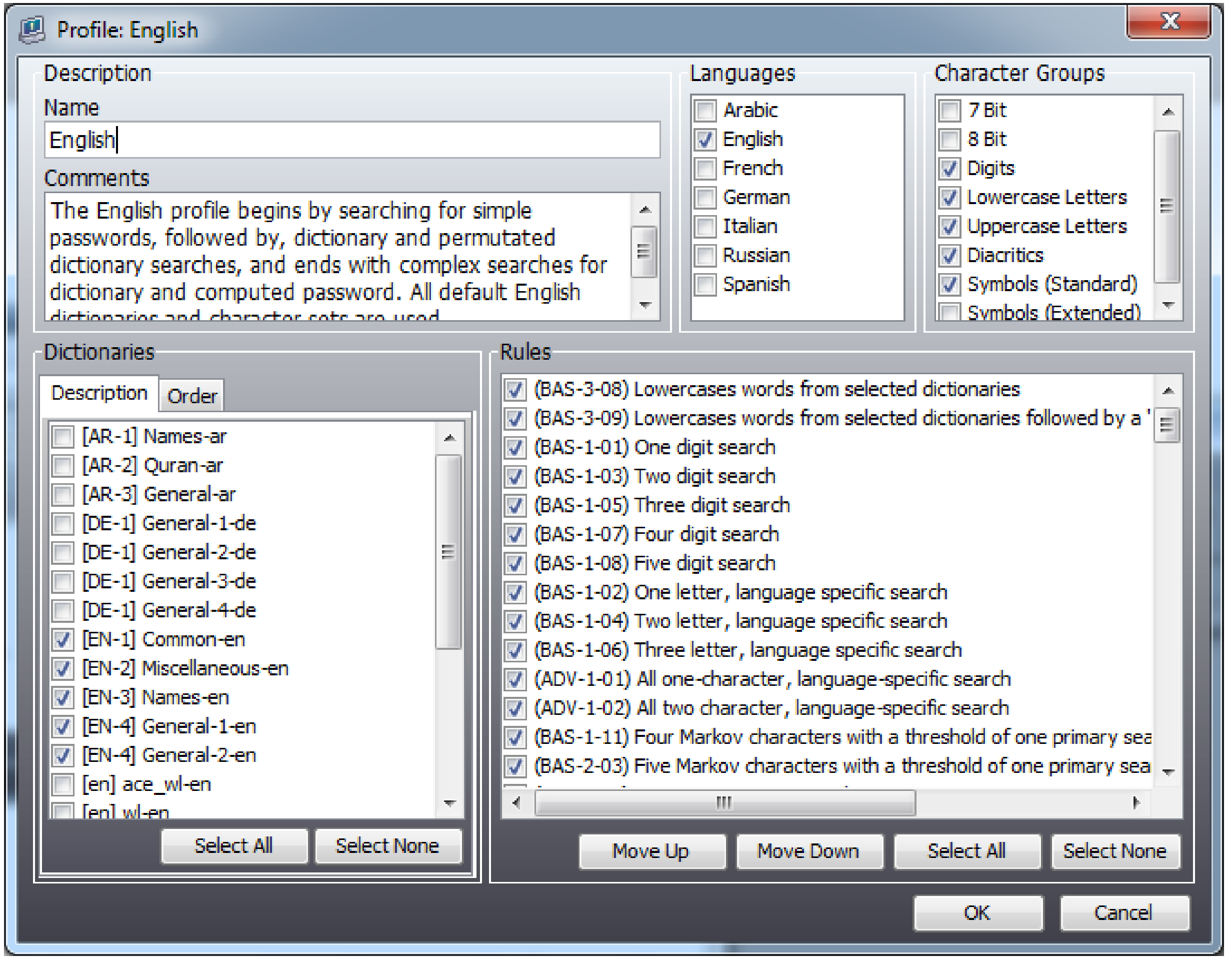
- □ Nick.xml
- □ [AR-1] Names-ar
- □ [AR-2] Quran-ar
- □ [AR-3] General-ar
- □ [DE-1] General-1-de
- □ [DE-1] General-2-de
- □ [DE-1] General-3-de
- □ [DE-1] General-4-de
- ☑ [EN-1] Common-en
- ☑ [EN-2] Miscellaneous-en
- ☑ [EN-3] Names-en
- ☑ [EN-4] General-1-en
- ☑ [EN-4] General-2-en
- ☑ [en] Nick-en
- □ [ES-1] General-es

Rules

- ☑ (BAS-1-01) One digit search
- ☑ (BAS-1-02) One letter, language specific search
- ☑ (BAS-1-03) Two digit search
- ☑ (BAS-1-04) Two letter, language specific search
- ☑ (BAS-1-05) Three digit search
- ☑ (BAS-1-06) Three letter, language specific search
- ☑ (BAS-1-07) Four digit search
- ☑ (BAS-1-08) Five digit search
- ☑ (BAS-1-09) Five Markov characters within a threshold of one hundred with
- ☑ (BAS-1-10) Six digit search
- ☑ (BAS-1-11) Four Markov characters with a threshold of one primary search
- ☑ (BAS-2-01) Four letter, language specific search
- ☑ (BAS-2-02) Five letter, language specific search
- ☑ (BAS-2-03) Five Markov characters with a threshold of one primary search
- ☑ (BAS-2-04) Five Markov characters with a threshold of one primary reverse

- Rules are ordered smallest to largest
- All English dictionaries selected by default

# The Default Profile (English)



Profile: English

Description

Name: English

Comments: The English profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default English dictionaries and character sets are used

Languages

- □ Arabic
- ☑ English
- □ French
- □ German
- □ Italian
- □ Russian
- □ Spanish

Character Groups

- □ 7 Bit
- □ 8 Bit
- ☑ Digits
- ☑ Lowercase Letters
- ☑ Uppercase Letters
- ☑ Diacritics
- ☑ Symbols (Standard)
- □ Symbols (Extended)

Dictionaries

- □ [AR-1] Names-ar
- □ [AR-2] Quran-ar
- □ [AR-3] General-ar
- □ [DE-1] General-1-de
- □ [DE-1] General-2-de
- □ [DE-1] General-3-de
- □ [DE-1] General-4-de
- ☑ [EN-1] Common-en
- ☑ [EN-2] Miscellaneous-en
- ☑ [EN-3] Names-en
- ☑ [EN-4] General-1-en
- ☑ [EN-4] General-2-en
- □ [en] ace_wl-en
- □ [en] wl-en

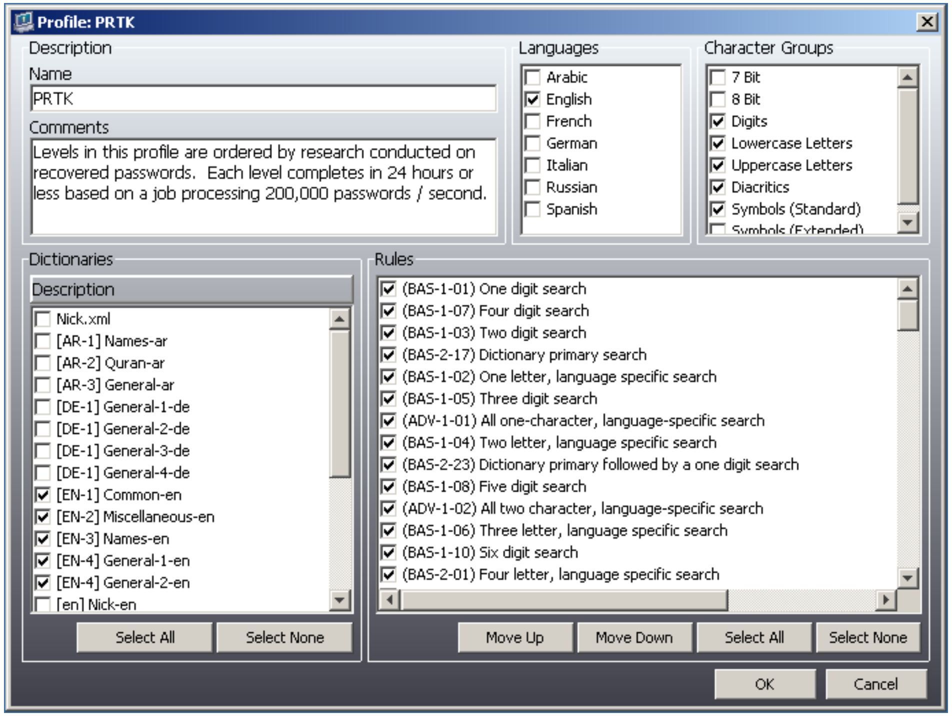
Rules

- ☑ (BAS-3-08) Lowercases words from selected dictionaries
- ☑ (BAS-3-09) Lowercases words from selected dictionaries followed by a '
- ☑ (BAS-1-01) One digit search
- ☑ (BAS-1-03) Two digit search
- ☑ (BAS-1-05) Three digit search
- ☑ (BAS-1-07) Four digit search
- ☑ (BAS-1-08) Five digit search
- ☑ (BAS-1-02) One letter, language specific search
- ☑ (BAS-1-04) Two letter, language specific search
- ☑ (BAS-1-06) Three letter, language specific search
- ☑ (ADV-1-01) All one-character, language-specific search
- ☑ (ADV-1-02) All two character, language-specific search
- ☑ (BAS-1-11) Four Markov characters with a threshold of one primary sea
- ☑ (BAS-2-03) Five Markov characters with a threshold of one primary sea

- No custom dictionaries
- Not efficient!

This was designed for the *untrained* user!

# The PRTK profile



Description

Name: PRTK

Comments: Levels in this profile are ordered by research conducted on recovered passwords. Each level completes in 24 hours or less based on a job processing 200,000 passwords / second.

Languages
- □ Arabic
- ☑ English
- □ French
- □ German
- □ Italian
- □ Russian
- □ Spanish

Character Groups
- □ 7 Bit
- □ 8 Bit
- ☑ Digits
- ☑ Lowercase Letters
- ☑ Uppercase Letters
- ☑ Diacritics
- ☑ Symbols (Standard)
- □ Symbols (Extended)

Dictionaries

Description
- □ Nick.xml
- □ [AR-1] Names-ar
- □ [AR-2] Quran-ar
- □ [AR-3] General-ar
- □ [DE-1] General-1-de
- □ [DE-1] General-2-de
- □ [DE-1] General-3-de
- □ [DE-1] General-4-de
- ☑ [EN-1] Common-en
- ☑ [EN-2] Miscellaneous-en
- ☑ [EN-3] Names-en
- ☑ [EN-4] General-1-en
- ☑ [EN-4] General-2-en
- □ [en] Nick-en

Rules
- ☑ (BAS-1-01) One digit search
- ☑ (BAS-1-07) Four digit search
- ☑ (BAS-1-03) Two digit search
- ☑ (BAS-2-17) Dictionary primary search
- ☑ (BAS-1-02) One letter, language specific search
- ☑ (BAS-1-05) Three digit search
- ☑ (ADV-1-01) All one-character, language-specific search
- ☑ (BAS-1-04) Two letter, language specific search
- ☑ (BAS-2-23) Dictionary primary followed by a one digit search
- ☑ (BAS-1-08) Five digit search
- ☑ (ADV-1-02) All two character, language-specific search
- ☑ (BAS-1-06) Three letter, language specific search
- ☑ (BAS-1-10) Six digit search
- ☑ (BAS-2-01) Four letter, language specific search

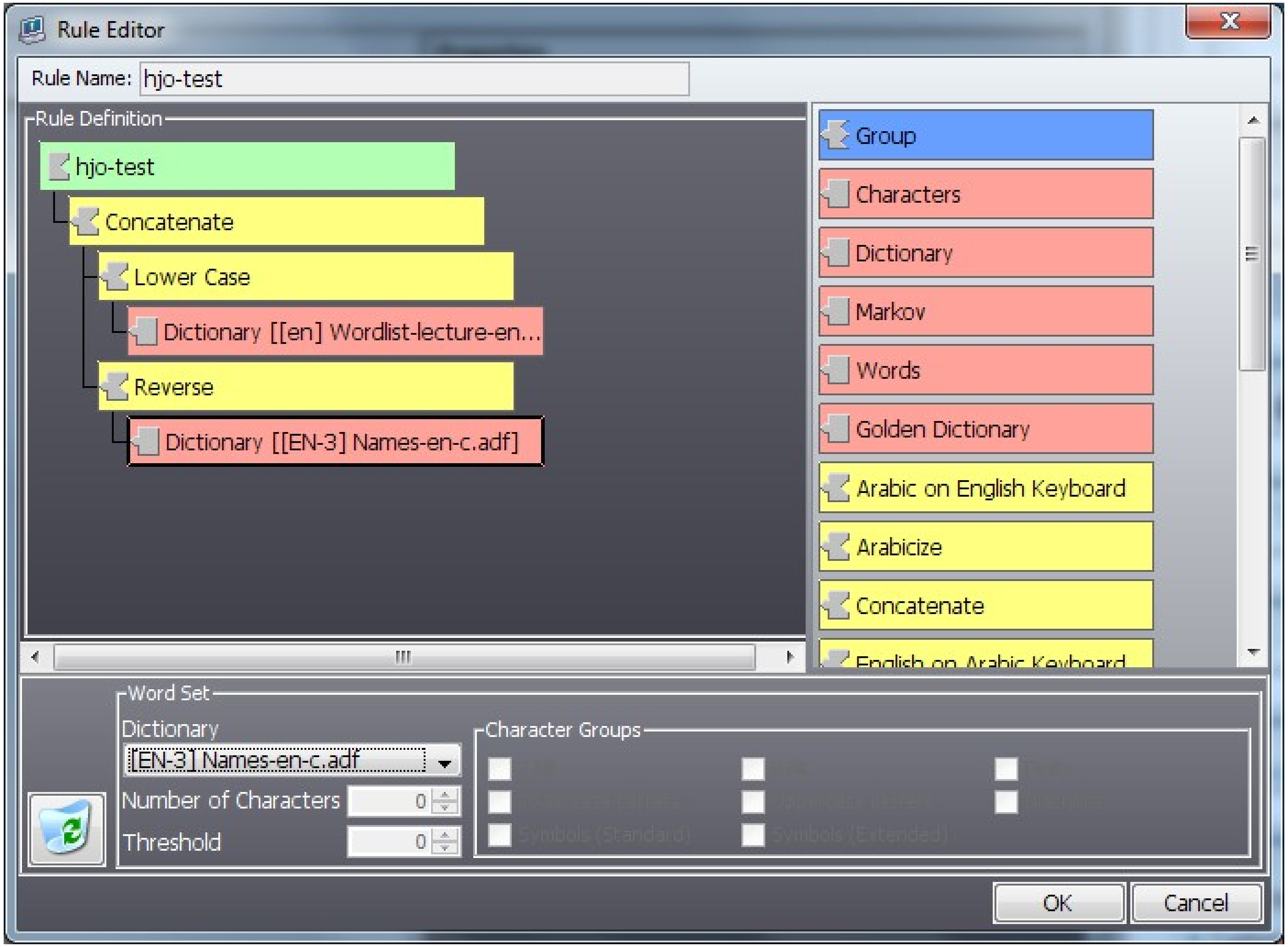
- Based on 1,000,000-password study
- Rules are ordered for efficiency
- Designed to complete in 1 week on average
- If unsuccessful, consider DNA
- Use it as a template
- Rename, update dictionary selections, and save for each new profile

This was designed for the *trained* user

Make it your default!

# User defined rules

Edit > Rules... Create and edit user defined rules



Rule Editor

Rule Name: hjo-test

Rule Definition

- hjo-test
  - Concatenate
    - Lower Case
      - Dictionary [[en] Wordlist-lecture-en...
    - Reverse
      - Dictionary [[EN-3] Names-en-c.adf]

Word Set

Dictionary: [EN-3] Names-en-c.adf

Number of Characters: 0

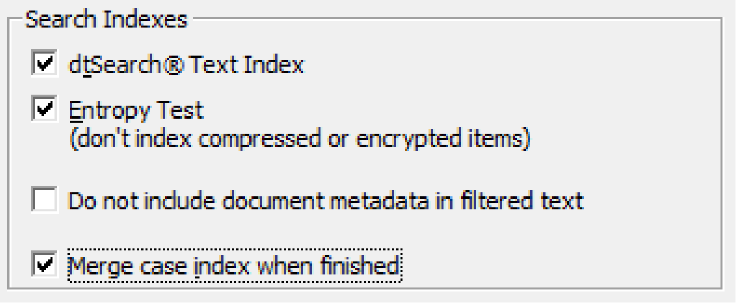
Threshold: 0

Character Groups

□ Symbols (Standard)
□ Symbols (Extended)

# FTK Export Word List...

- File > Export Word List...
- Exporterar indexerade sök registret till en fil, alltså alla textsträngar funna i caset (kom ihåg strängar från registry filer!)
- Notera var du spar din word list!
- Om man lyckats dekryptera något dokument etc.
  - I FTK kör Evidence > Additional Analysis..., markera följande boxar i ”Search Indexes” så de nya textsträngarna kommer med och merga indexet. Generera en ny word list, uppdatera sedan dictionary i PRTK.



Search Indexes

☑ dtSearch® Text Index

☑ Entropy Test
(don't index compressed or encrypted items)

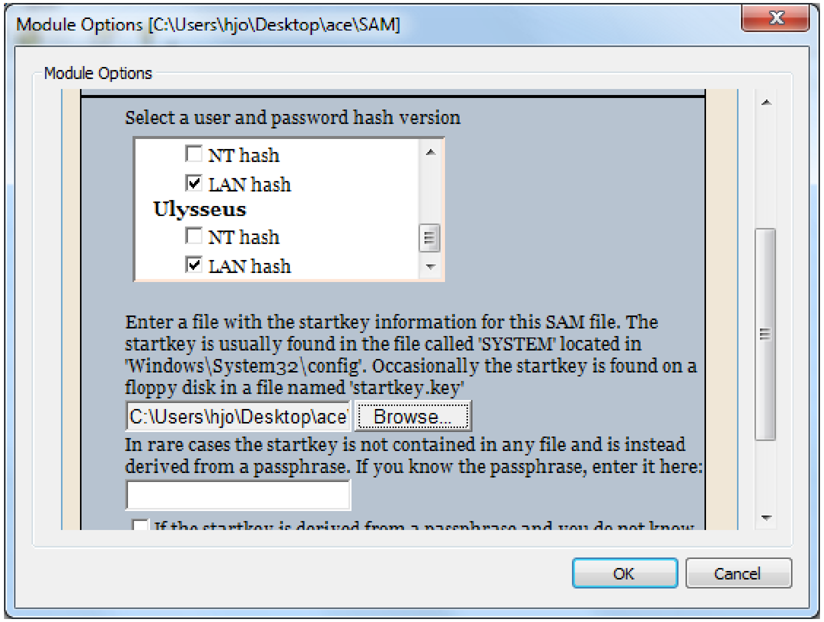
□ Do not include document metadata in filtered text

☑ Merge case index when finished

- Snabb word list attack
  - Utgå från FTK Wordlist Import mallen i Manage Profiles med ”(BAS-3-10) Uses entries 'AS-IS' from selected dictionaries”. Välj **din** word list som dictionary.

# Användarkonto exempel

- Enbart word list dictionary används, skall inte ta mer än några minuter maximalt!
- Enbart LAN hash markerad > vad innebär det?
  - LAN hash går snabbt att knäcka med Brute Force!



Module Options [C:\Users\hjo\Desktop\ace\SAM]

Module Options

Select a user and password hash version

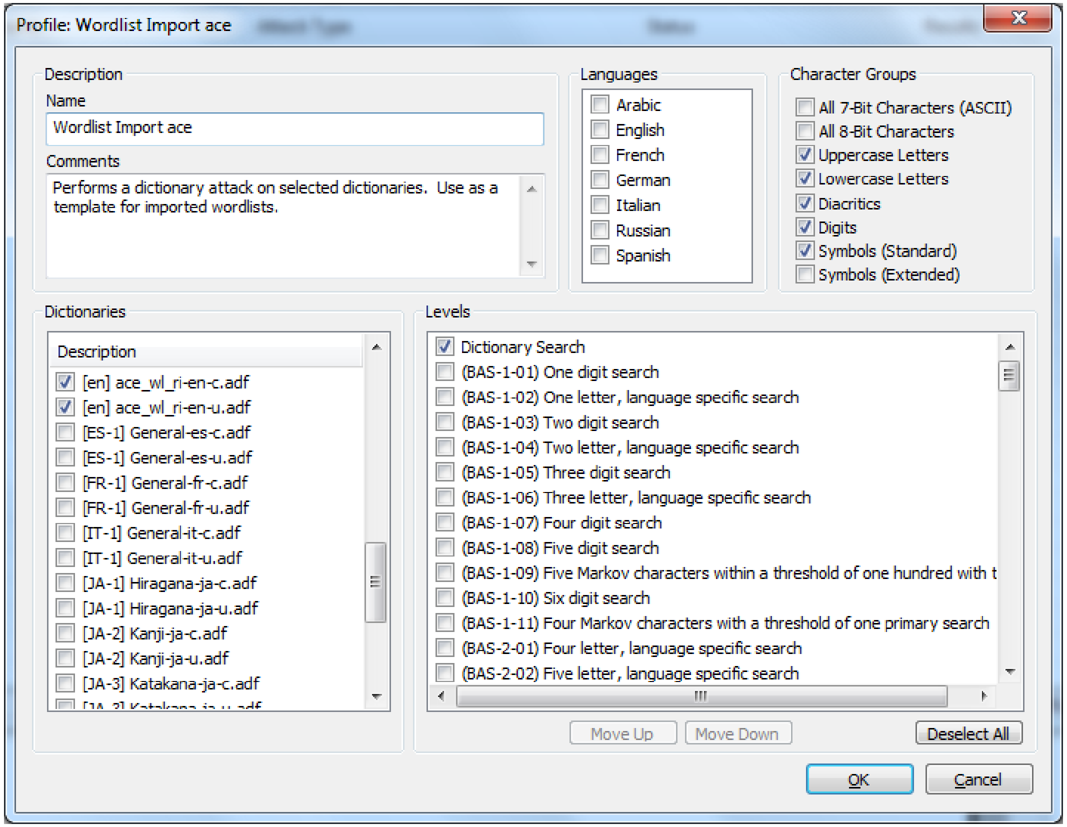
□ NT hash
☑ LAN hash
**Ulysseus**
□ NT hash
☑ LAN hash

Enter a file with the startkey information for this SAM file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'

C:\Users\hjo\Desktop\ace' [Browse...]

In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:

□ If the startkey is derived from a passphrase and you do not know



Profile: Wordlist Import ace

Description

Name: Wordlist Import ace

Comments: Performs a dictionary attack on selected dictionaries. Use as a template for imported wordlists.

Languages

□ Arabic
□ English
□ French
□ German
□ Italian
□ Russian
□ Spanish

Character Groups

□ All 7-Bit Characters (ASCII)
□ All 8-Bit Characters
☑ Uppercase Letters
☑ Lowercase Letters
☑ Diacritics
☑ Digits
☑ Symbols (Standard)
□ Symbols (Extended)

Dictionaries

Description
☑ [en] ace_wl_ri-en-c.adf
☑ [en] ace_wl_ri-en-u.adf
□ [ES-1] General-es-c.adf
□ [ES-1] General-es-u.adf
□ [FR-1] General-fr-c.adf
□ [FR-1] General-fr-u.adf
□ [IT-1] General-it-c.adf
□ [IT-1] General-it-u.adf
□ [JA-1] Hiragana-ja-c.adf
□ [JA-1] Hiragana-ja-u.adf
□ [JA-2] Kanji-ja-c.adf
□ [JA-2] Kanji-ja-u.adf
□ [JA-3] Katakana-ja-c.adf
□ [JA-3] Katakana-ja-u.adf

Levels

☑ Dictionary Search
□ (BAS-1-01) One digit search
□ (BAS-1-02) One letter, language specific search
□ (BAS-1-03) Two digit search
□ (BAS-1-04) Two letter, language specific search
□ (BAS-1-05) Three digit search
□ (BAS-1-06) Three letter, language specific search
□ (BAS-1-07) Four digit search
□ (BAS-1-08) Five digit search
□ (BAS-1-09) Five Markov characters within a threshold of one hundred with t
□ (BAS-1-10) Six digit search
□ (BAS-1-11) Four Markov characters with a threshold of one primary search
□ (BAS-2-01) Four letter, language specific search
□ (BAS-2-02) Five letter, language specific search

# Possible PRTK attacks

- Decryption Attack
  - Decrypts the password that locks the file
- Dictionary Attack
  - Uses the words in a dictionary, applies rules to the words, and applies the password to the files or converts the possible words into keys
- Keyspace Attack
  - Tries every possible key because there is a finite number of keys for the file
  - The possible number of keys can be very large, therfore used on applications that use 40-bit encryption or less
- Reset Attack
  - Rewrites the key that opens the file to a key that comes from a password that you specify. Few applications are susceptible to it.
- Multiple Attacks
  - Some applications are susceptible to more than one attack type which can decrease the time necessary to decrypt a file. PRTK starts with the least time-consuming attack type.

# Bit Strength Classification

Key: **Any One of a Larger Number of Values**

Keyspace: **Range of Possible Values (this can get big!)**

Easy

Moderate

Difficult

DNA !!

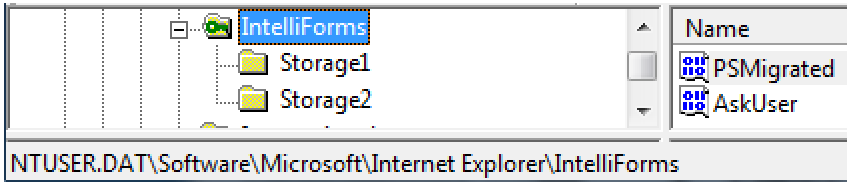
&%@# !!!

| | |
|---|---|
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 16 |
| 5 | 32 |
| 6 | 64 |
| 7 | 128 |
| 8 | 256 |
| 9 | 512 |
| 10 | 1 024 |
| 20 | 1 048 576 |
| 30 | 1 073 741 824 |
| 32 | 4 294 967 296 |
| 33 | 8 589 934 592 |
| 40 | 1 099 511 627 776 |
| 50 | 1 125 899 906 842 620 |

Check out the **keyspace_password.xls** file

# Break MS DPAPI (Data Protection Application Programming Interface)

- DPAPI is built in Windows since Win2K
  - http://en.wikipedia.org/wiki/Data_Protection_API
- DPAPI (Vista/IE7 and up) is the successor of the legacy PSSP (Protected Storage System Provider) which store (below) and moved to IntelliForms key
  - Form data, Web search queries, Web passwords and Outlook/Express passwords (PSSP are on the fly decrypted by RV)
  - Storage1 - queries and form data
  - Storage2 - login password info

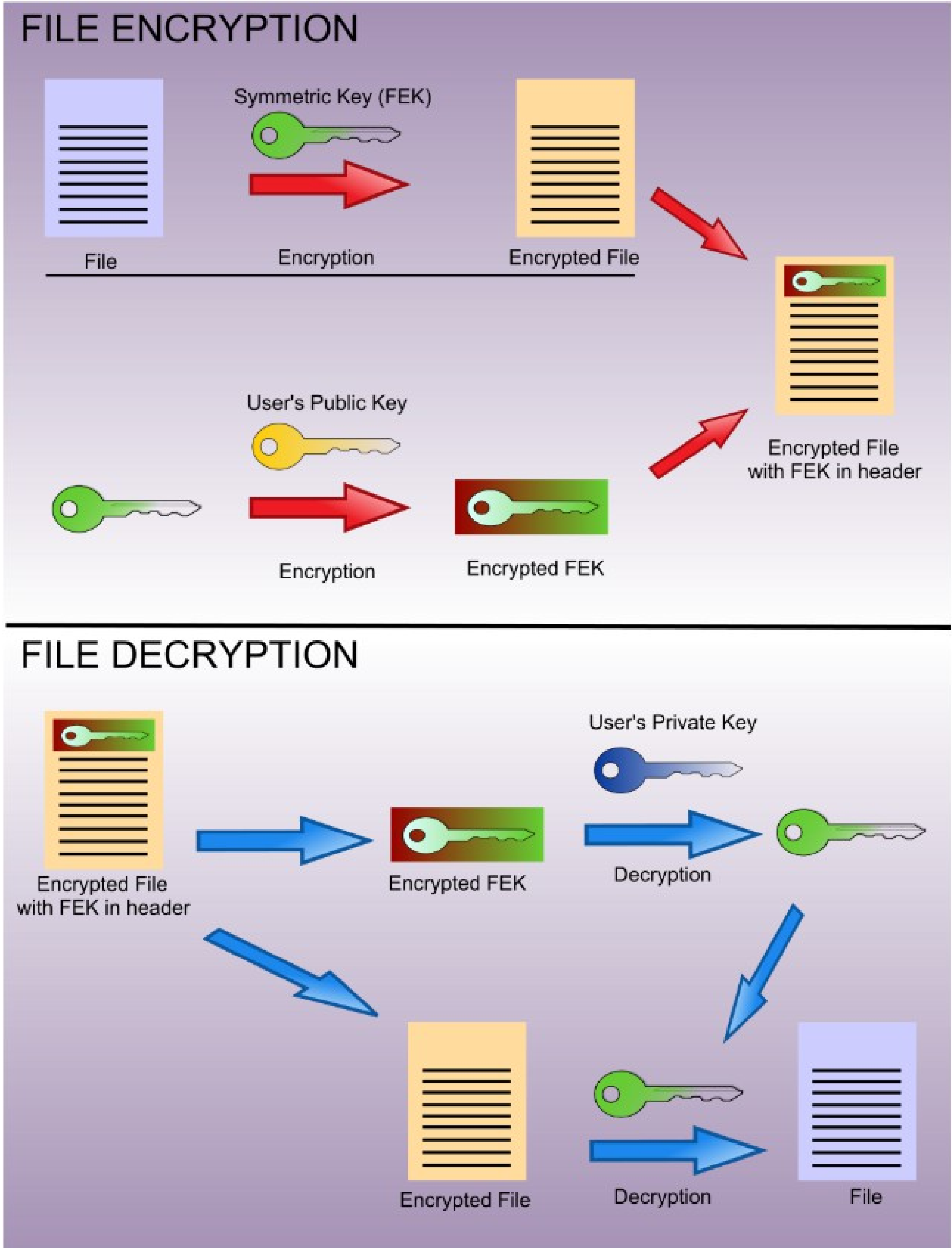


NTUSER.DAT\Software\Microsoft\Internet Explorer\IntelliForms

- To break DPAPI protected data we need: user logon password, users protect folder and information specific below
  - For URL logon pages: the address of the page accessed
  - For search terms: the query engine header
  - For form data: the field name of the form field used
  - The AccessData PDF “Decrypting IntelliForms” have instructions performing the DPAPI information decryption with PRTK at their support web
- DPAPI programming example with a C++ wrapper class
  - http://www.codeproject.com/KB/system/protected_data.aspx

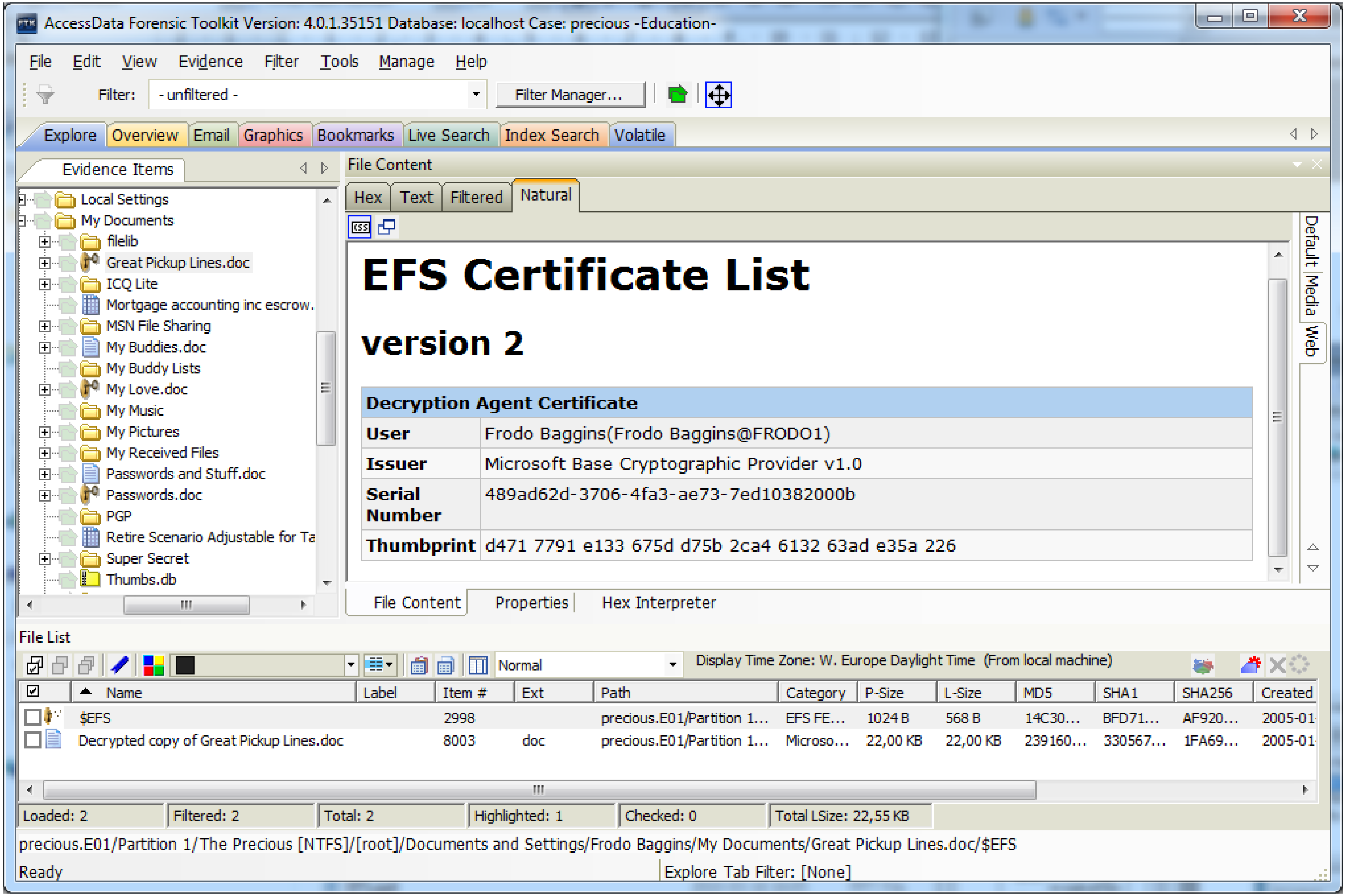
# Windows EFS (Encrypting File System) operation in short

- FEK
  - File Encryption Key - new random one for every file
  - Stored in an ADS, the $Logged Utility Stream attribute in MFT
  - Marked as $EFS in FTK
- Transparent for apps (Windows API)
- Decrypted if copied/moved outside NTFS or over the network
- Vista/7 supports storage of private key on smart card



# EFS and FTK

When PRTK has obtained the login password, use Tools > Decrypt Files...



## EFS Certificate List

## version 2

| Decryption Agent Certificate | |
|---|---|
| User | Frodo Baggins(Frodo Baggins@FRODO1) |
| Issuer | Microsoft Base Cryptographic Provider v1.0 |
| Serial Number | 489ad62d-3706-4fa3-ae73-7ed10382000b |
| Thumbprint | d471 7791 e133 675d d75b 2ca4 6132 63ad e35a 226 |

| ☑ | Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MD5 | SHA1 | SHA256 | Created |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | $EFS | | 2998 | | precious.E01/Partition 1... | EFS FE... | 1024 B | 568 B | 14C30... | BFD71... | AF920... | 2005-01 |
| □ | Decrypted copy of Great Pickup Lines.doc | | 8003 | doc | precious.E01/Partition 1... | Microso... | 22,00 KB | 22,00 KB | 239160... | 330567... | 1FA69... | 2005-01 |

Loaded: 2 | Filtered: 2 | Total: 2 | Highlighted: 1 | Checked: 0 | Total LSize: 22,55 KB

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/Great Pickup Lines.doc/$EFS

Ready | Explore Tab Filter: [None]

# PRTK new functions

- Accelerating Password Recovery using GPU Hardware
  - PRTK will automatically detect if GPU acceleration is possible and will utilize the hardware as necessary. No additional steps are required.
  - Using GPU acceleration is transparent on the computer. DNA and PRTK utilize the supported hardware if it is available. In the absence of such hardware, CPUs will continue to be utilized to their greatest capacity.
- Supports
  - List of jobs that can be run with GPU – see the manual
  - Nvidia CUDA GPUs