Foundstone®
STRATEGIC SECURITY

WHITE PAPER

FSCrack User Guide

Author: Juan Bocanegra, Foundstone, a division of McAfee, Inc®.

April 2006

Introduction

FSCrack is a front end for John the Ripper (JtR). FSCrack provides a graphical user interface (GUI) for access to most of JtR's functions.

JtR is described as follows (from http://www.openwall.com/john/):
"John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt (3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches."

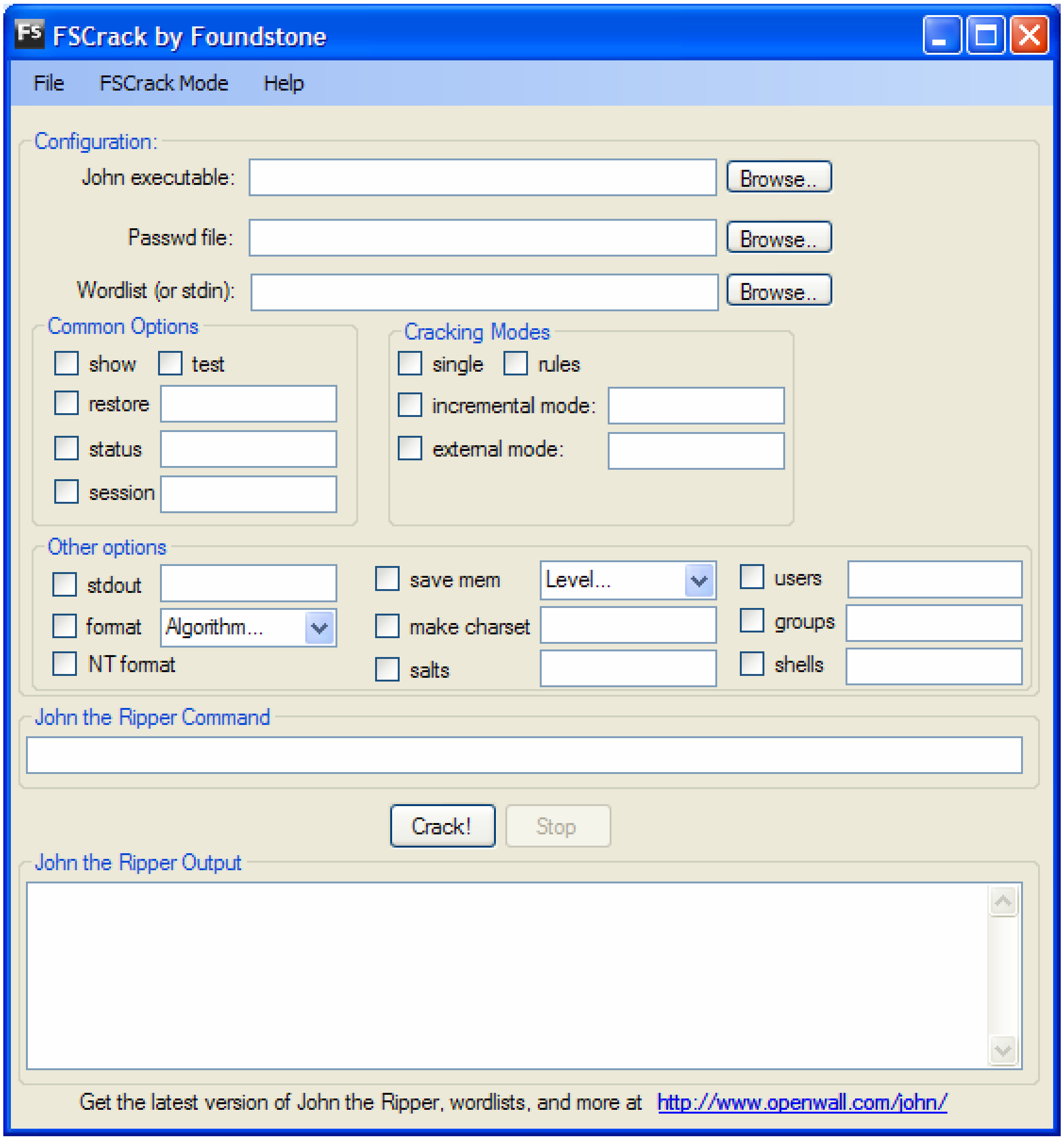
System Requirements

- John the Ripper binary (win32) written by Solar Designer. Available at http://www.openwall.com/john/
- .Net framework 2.0. Available at: http://msdn.microsoft.com/netframework/downloads/updates/default.aspx
- (Optional) NTLM (MD4) hash support patch written by Olle Segerdahl. Available at: http://olle.nxs.se/software/john-ntlm/

Foundstone

User’s Guide for FSCrack

Below is a screenshot of FSCrack:



Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

FSCrack has the following main functions:

- Configuration options for JtR
- JtR command builder
- JtR output viewer

Configuration options for John the Ripper

FSCrack provides a mechanism to configure the following JtR options:

- Configuration options
  - Required:
    - Path to the john executable (path to john*.exe)
  - Optional:
    - Path to passwd file (path to password file)
    - Path to wordlist (path to wordlist file)
    - –show (shows previously cracked passwords)
    - –test (performs a benchmark test)
    - –restore (restores a previous password cracking session)
    - –status (displays the status of an active password cracking session)
    - –session (give a new session the specified name)
    - –single (single-crack mode)
    - –rules (enable word mangling rules for wordlist mode)
    - –incremental mode (incremental mode using specified section mode)
    - –external mode (external mode or word filter)
    - –stdout (display candidate passwords)
    - –format (force-specified ciphertext format)
    - –save mem (enable memory saving at specified level)
    - –make charset (creates a charset and saves in specified file)
    - –salts (load salts with[out] specified passwords)
    - –users ([do not] load specified users)
    - –groups ([do not] load specified groups)
    - –shells (load users with[out] specified shells)
    - –NT format (displays the NTLM/MD4 values of cracked passwords)

- John the Ripper command builder:
  - FSCrack has a text area where you can view the command that is passed to the JtR executable. This command is displayed when selecting the **Crack!** button.

- John the Ripper output viewer:
  - FSCrack provides a text area where you can view the output of the JtR executable. Any standard error or output from JtR will display in this text area.

See Appendix A for more information on FSCrack's options.
See Appendix B for more information on JtR's options, from JtR's website.

Using FSCrack:
To run FSCrack, select the path of the JtR executable, select desired options, and click on the **Crack!** button.

Common FSCrack uses

- Cracking passwords using JtR's default settings:

  FSCrack's most common function is to use JtR's default setting to crack passwords. To configure FSCrack to use this default setting, only two items are required:
  1. The path to the JtR executable
  2. The path to a passwd file.

Once these two paths are selected, the user can click on the **Crack!** button, and FSCrack will run JtR using the default cracking mode, which consists of up to three different modes in the following sequence:

1. "single mode" cracking – which uses the default "single mode" cracking rules defined in the john.ini configuration file;
2. "wordlist mode" cracking – which uses the default wordlist file, passwords.lst;
3. "incremental mode" – which uses default word mangling rules also defined in the john.ini configuration file.

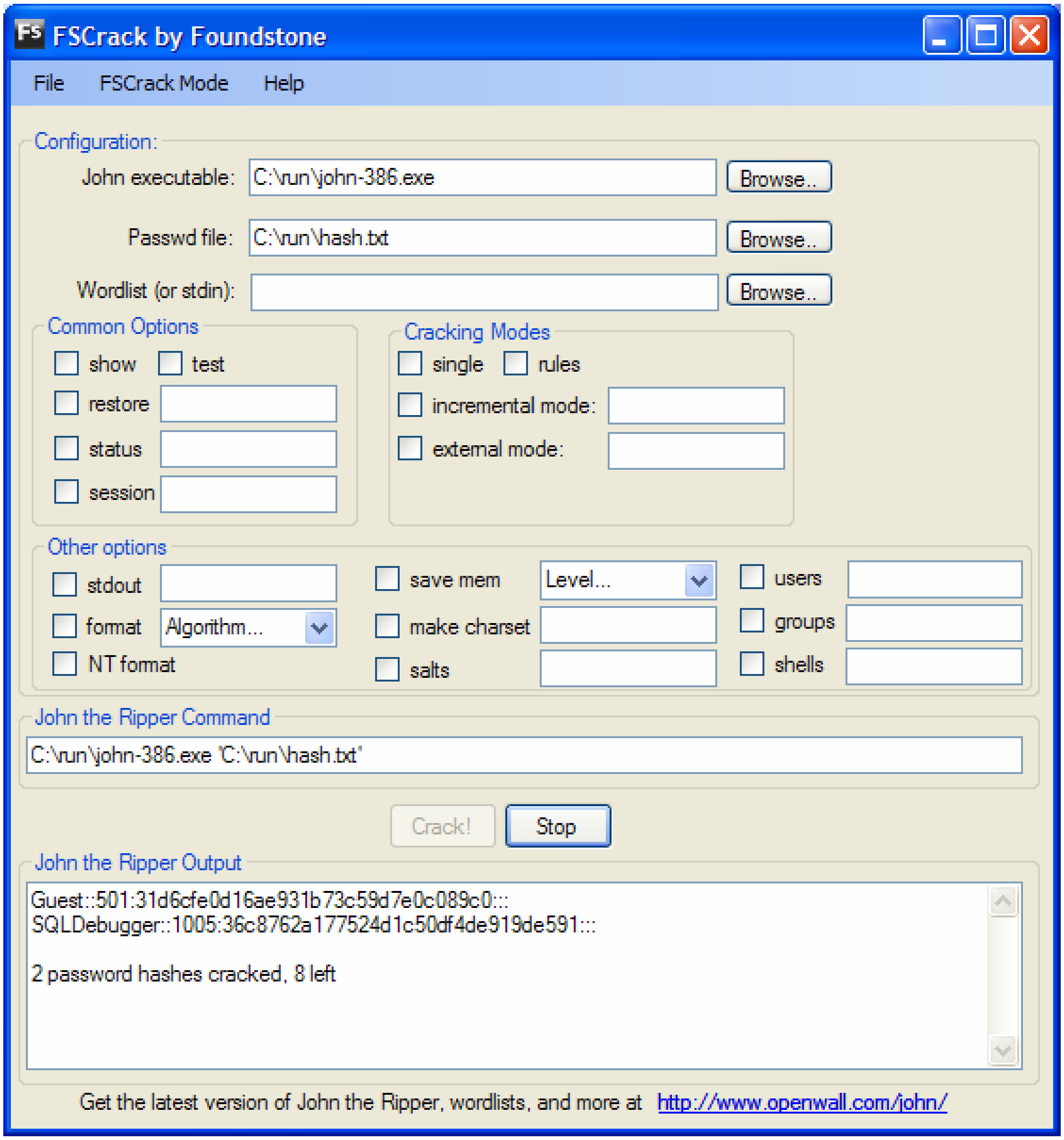
You can view these three modes as:

1. a quick check using very basic rules
2. another quick check using a basic password list
3. a brute force/hybrid attack.

For any casual user, this mode is the most effective and convenient method of running FSCrack.

This is the recommended approach for users when cracking passwords using JtR. The "single mode" and "incremental mode" are very time efficient. Casual users should not attempt to write their own rules for these two modes. The only cracking mode that a casual user might want to customize is the "wordlist mode". The "wordlist mode" takes any specified wordlist as input (selected using the **Browse…** button to the right of the **wordlist file** label). If no wordlist is specified, JtR will use the default password.lst file. There are many free wordlists available on the internet. The JtR website (http://openwall.org/john) also contains many different wordlists, available at a nominal fee.

The following is a screenshot of FSCrack actively cracking a password using the default configuration:



John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt'
```

John the Ripper Output

```
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
SQLDebugger::1005:36c8762a177524d1c50df4de919de591:::

2 password hashes cracked, 8 left
```

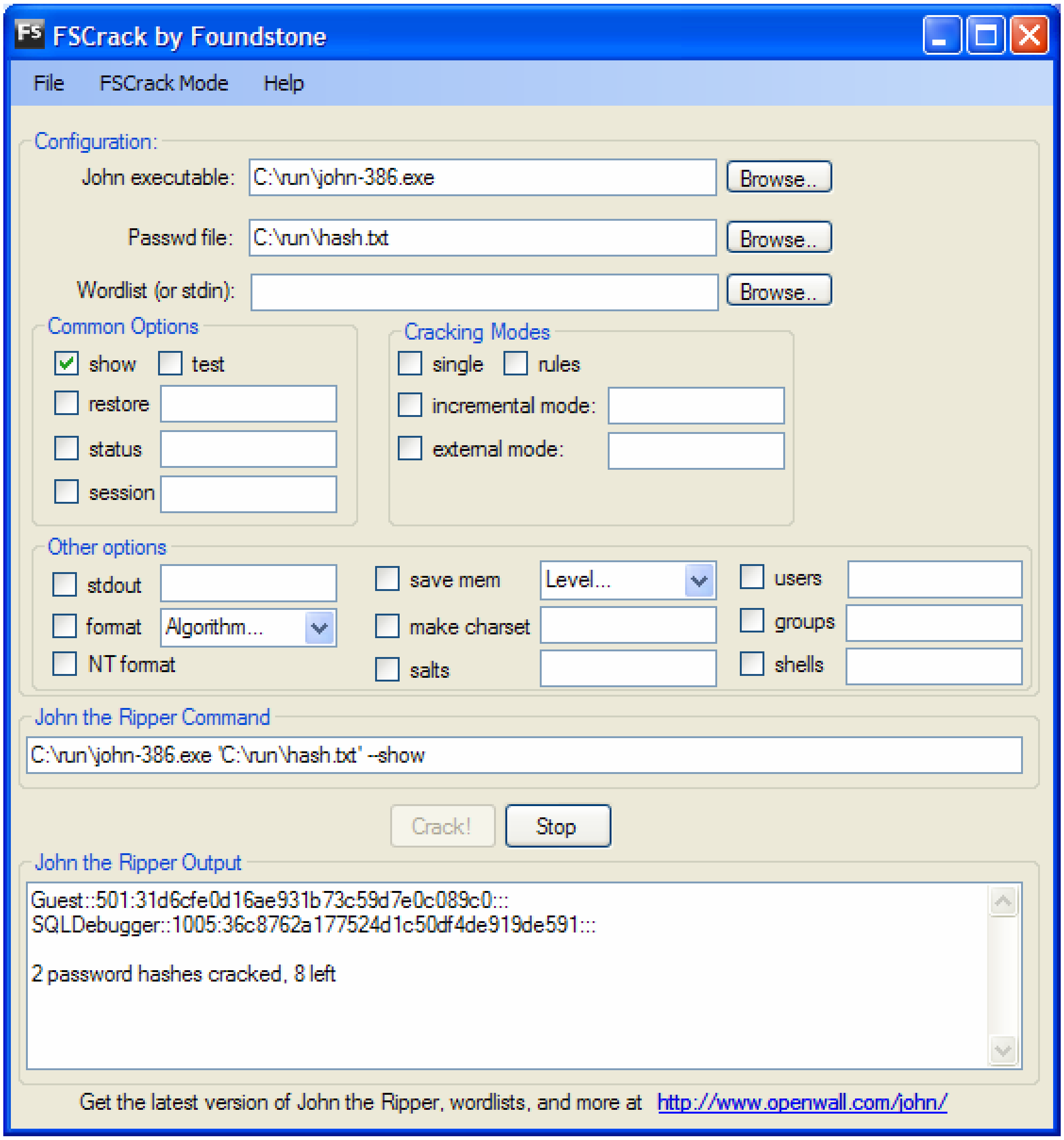
Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- Showing previously cracked passwords:

  The following most common use of FSCrack would be to display previously cracked passwords. Using the default method of cracking or any other method as detailed in Appendix A, cracked passwords can be displayed in the **John the Ripper output** text area using the **show** option.

The **show** option requires a passwd file. Once the **John executable**, **Passwd file**, and **show** option have been selected, clicking on the **Crack!** button will displayed cracked passwords for the specified passwd file.

Below is a screenshot of an end user running FSCrack with the **show** option selected to display previously cracked passwords from the file “c:\run\hash.txt.”



John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

☑ show ☐ test

☐ restore

☐ status

☐ session

☐ single ☐ rules

☐ incremental mode:

☐ external mode:

☐ stdout

☐ format Algorithm...

☐ NT format

☐ save mem Level...

☐ make charset

☐ salts

☐ users

☐ groups

☐ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt' --show
```

John the Ripper Output

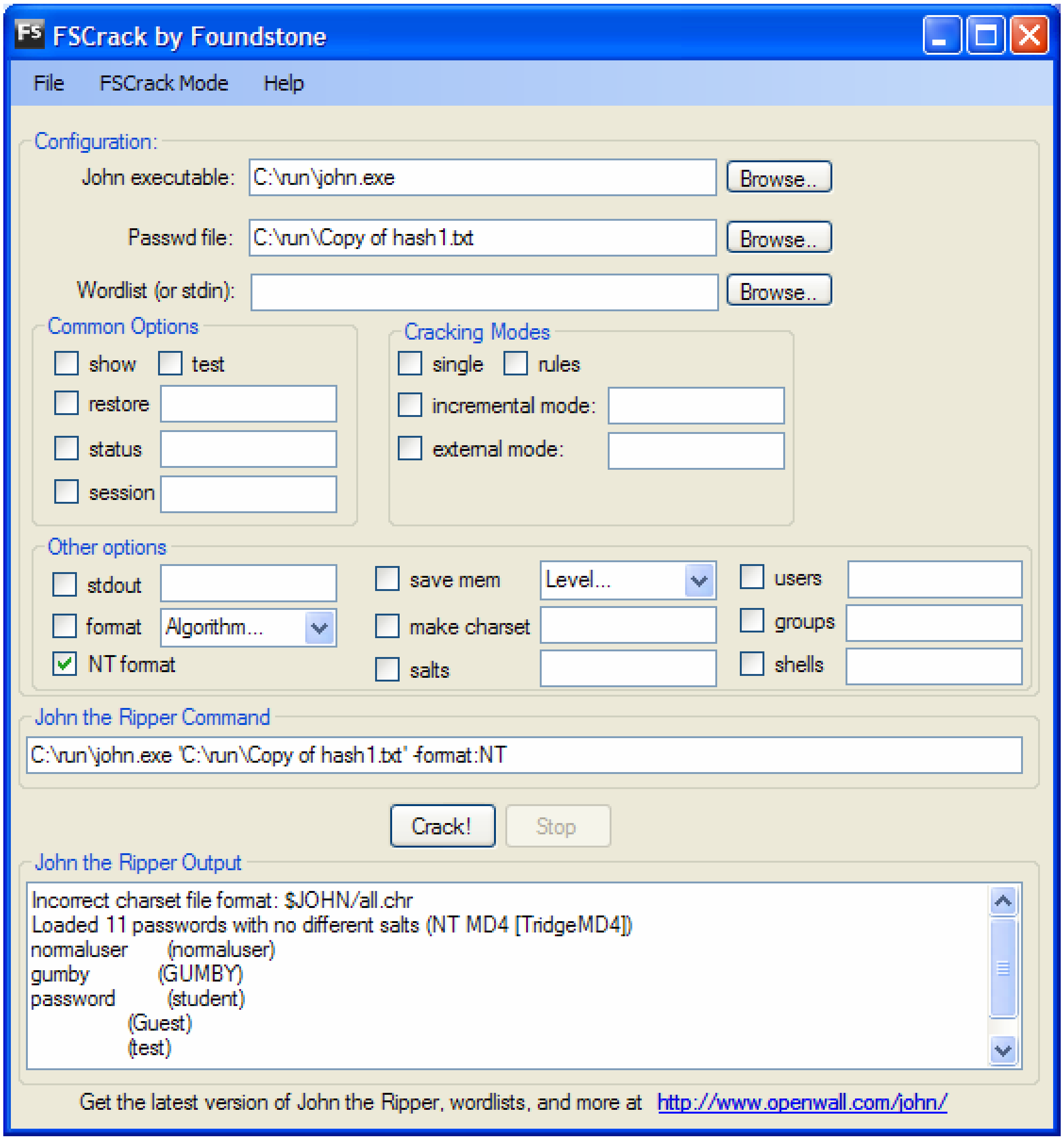
```
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
SQLDebugger::1005:36c8762a177524d1c50df4de919de591:::

2 password hashes cracked, 8 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- Displaying NTLM (MD4) passwords:

  Once you have cracked Windows passwords, you might want to figure out the case sensitivity of the cracked passwords. You can do this using the patch provided by Olle Segerdahl, available at: http://olle.nxs.se/software/john-ntlm/. Once this patched version of JtR is downloaded, select this patched version as the **John executable**, select the **passwd file** to view the NTLM values for, select the **NT format** option, and click on the **Crack!** button. FSCrack will output any NTLM formatted passwords to the **John the Ripper** output text area.

  The following is a screenshot of an end user running FSCrack with the **NT format** option to display the NTLM (MD4) value of the previously cracked passwords.



Configuration:

John executable: C:\run\john.exe

Passwd file: C:\run\Copy of hash1.txt

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format Algorithm...

☑ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

```
C:\run\john.exe 'C:\run\Copy of hash1.txt' -format:NT
```

John the Ripper Output

```
Incorrect charset file format: $JOHN/all.chr
Loaded 11 passwords with no different salts (NT MD4 [TridgeMD4])
normaluser      (normaluser)
gumby          (GUMBY)
password        (student)
                (Guest)
                (test)
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

Known Issues

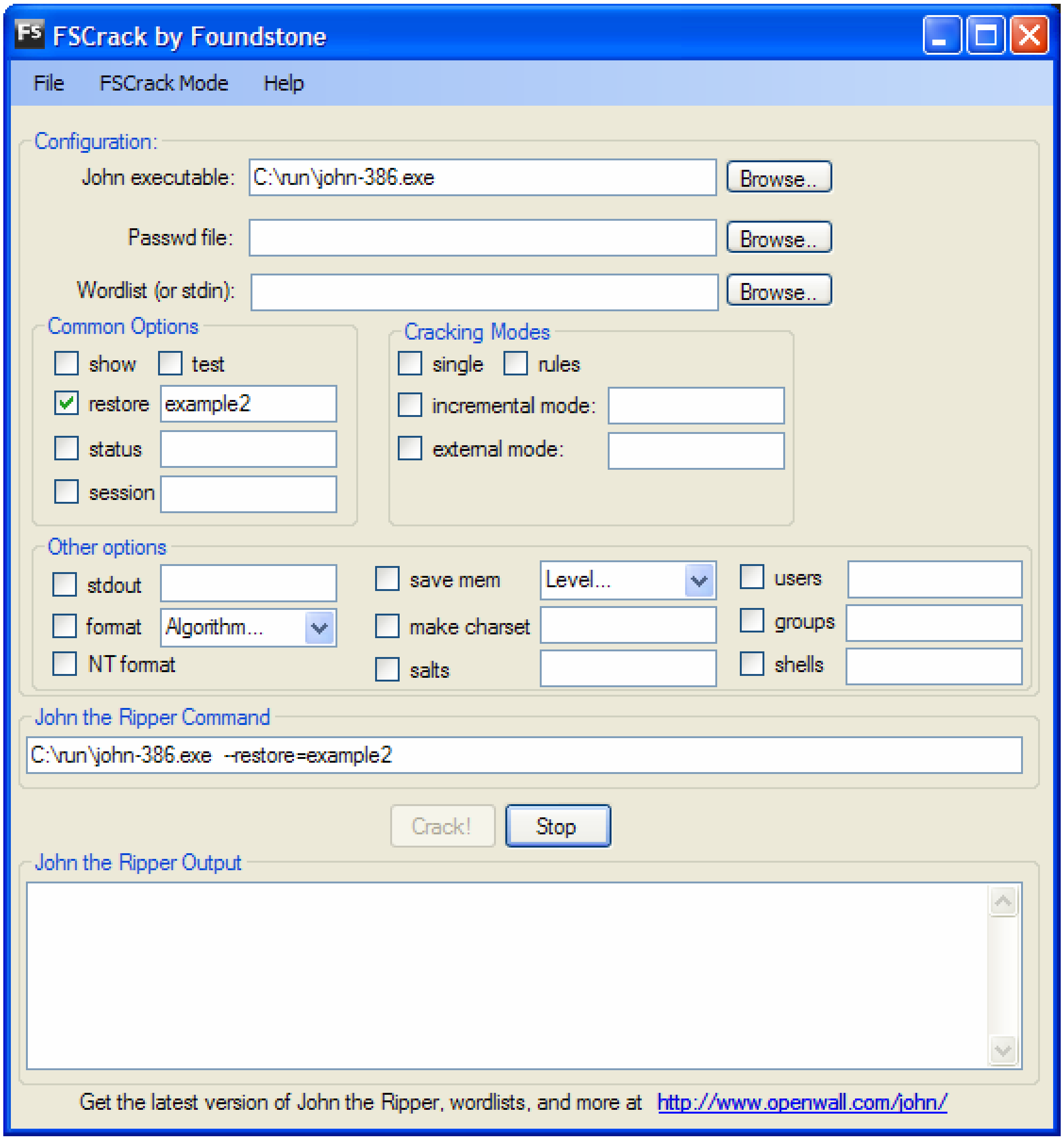
There are no known issues at this time.

Acknowledgements

A special thanks to Solar Designer (et al.) for creating a great password cracker. Also, special thanks to all who contributed patches to JtR.

Appendix A: Summary of common FSCrack options

FSCrack builds commands and options that are passed to the JtR executable when the **Crack!** button is clicked. The only required field for running FSCrack is the path to the John executable. JtR (and FSCrack) also accept a number of options and parameters. Some options take additional arguments, which you can type in the text areas immediately to the right of the desired option or select using the **Browse…** button. For example, if you would like to restore a session, select the restore checkbox and specify the name of the session to be restored; otherwise, the session you last ran is restored. Below is a screenshot of this example, assuming a named session already exists:



John executable: C:\run\john-386.exe

Passwd file:

Wordlist (or stdin):

□ show □ test

☑ restore example2

□ status

□ session

□ single □ rules

□ incremental mode:

□ external mode:

□ stdout

□ format Algorithm...

□ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

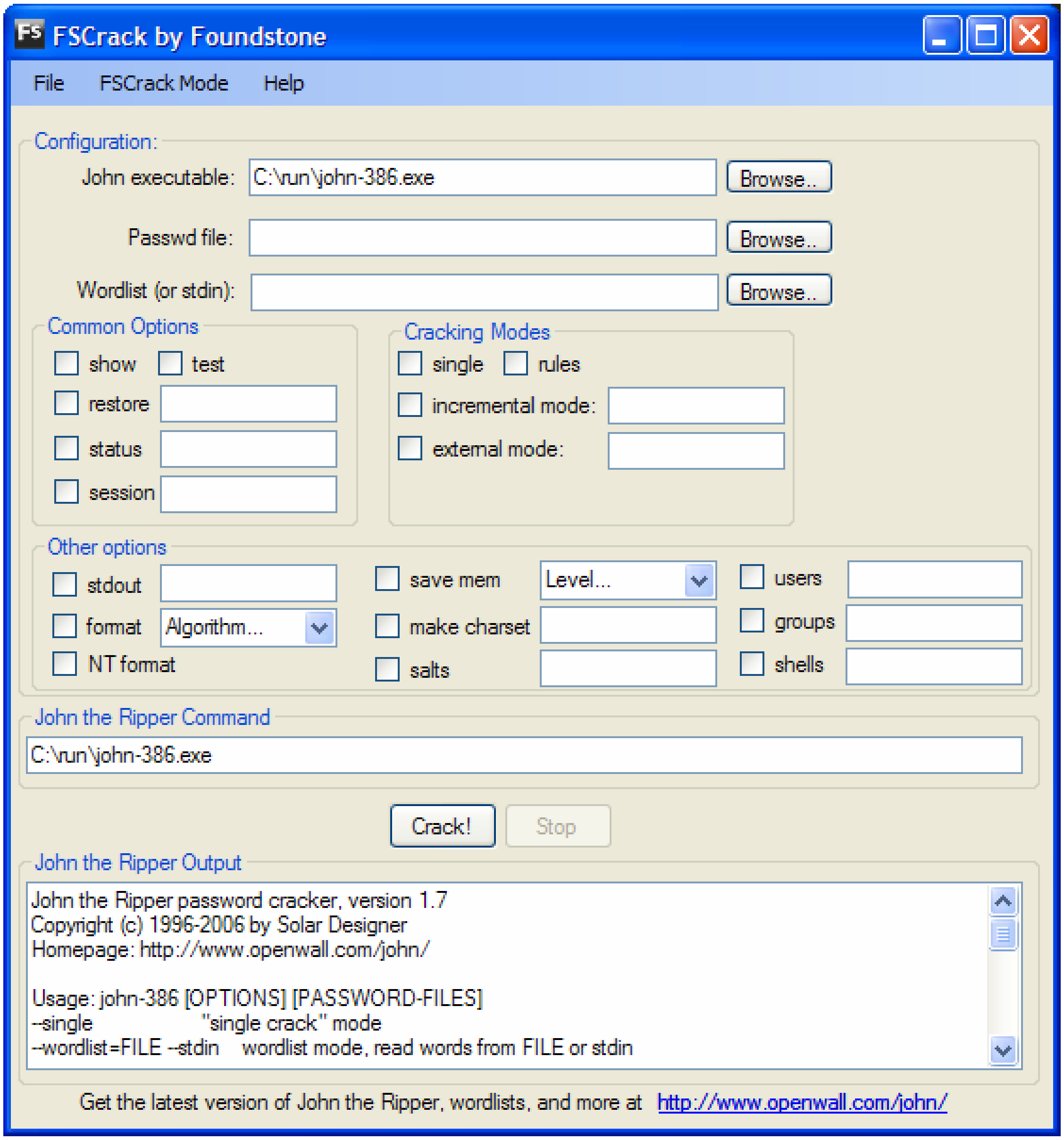
```
C:\run\john-386.exe  --restore=example2
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

FSCrack has implemented a mechanism to call the most common functions. The following is a list of all functions in the following format: name of the option, a brief description, how to use the option in FSCrack, and a screenshot of FSCrack using the specified option.

Common Options

- **Print out John's usage**
    - Description: this command prints out the usage for John the Ripper. This is the most basic function of John and a path to the JtR executable is always required when using FSCrack.
    - How to print John's usage from FSCrack: Select path to John using the **Browse…** button to the left of the **John executable** label and hit the **Crack!** button.
    - Screenshot below:

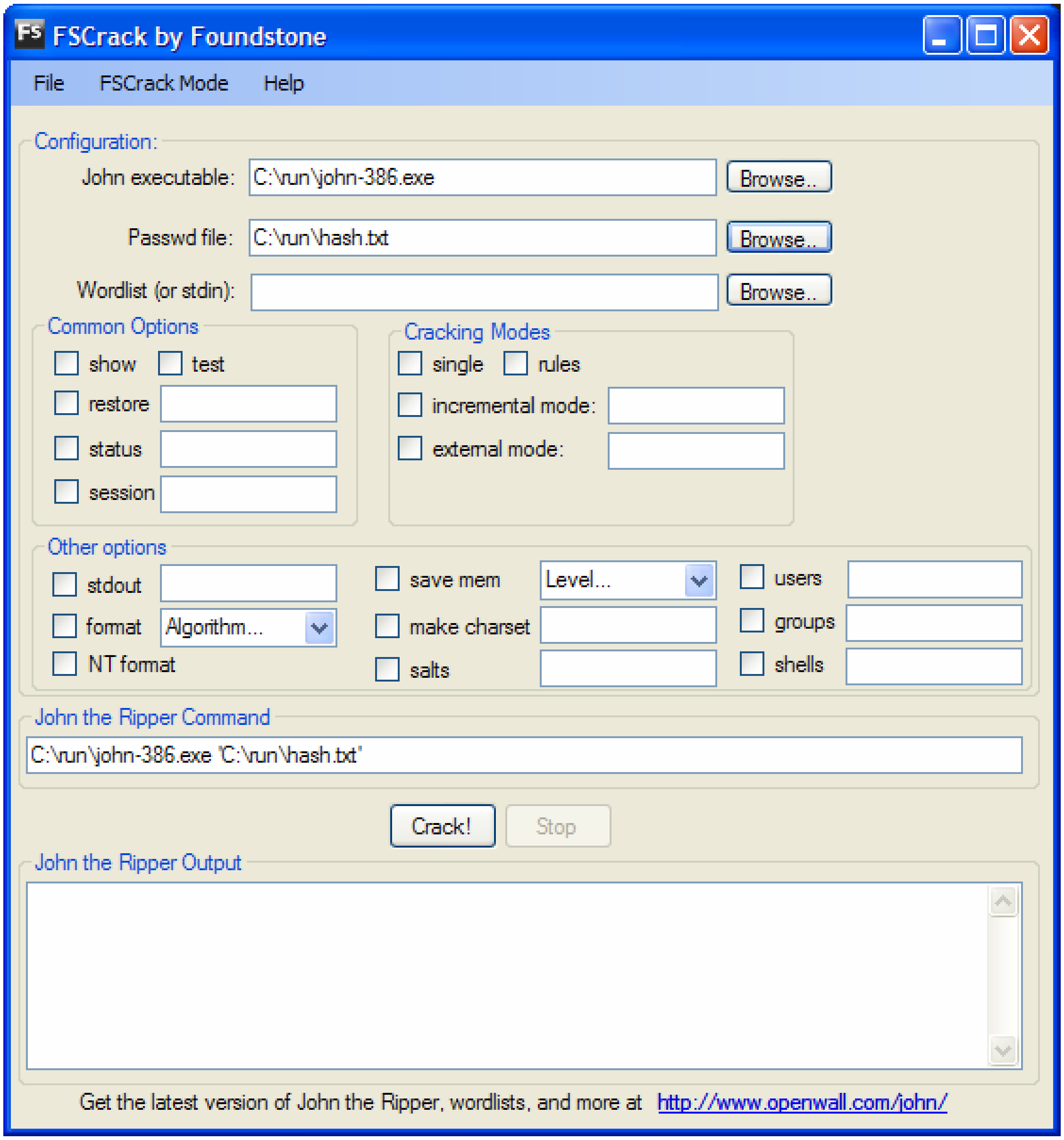


John executable: C:\run\john-386.exe

John the Ripper Command: C:\run\john-386.exe

```
John the Ripper password cracker, version 1.7
Copyright (c) 1996-2006 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john-386 [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin    wordlist mode, read words from FILE or stdin
```

- **Select a passwd file**
  - Description: This is the passwd file that JtR will crack. FSCrack uses a file dialog to select the desired passwd file to crack.
  - How to select a passwd file in FSCrack: Click on the **Browse…** button to the right of the **Passwd file** label to populate the **Passwd file** text area. If you click on the **Crack!** button, FSCrack will call JtR using John's default settings, which are specified in the john.ini configuration file.
  - Screenshot below:



John executable: C:\run\john-386.exe

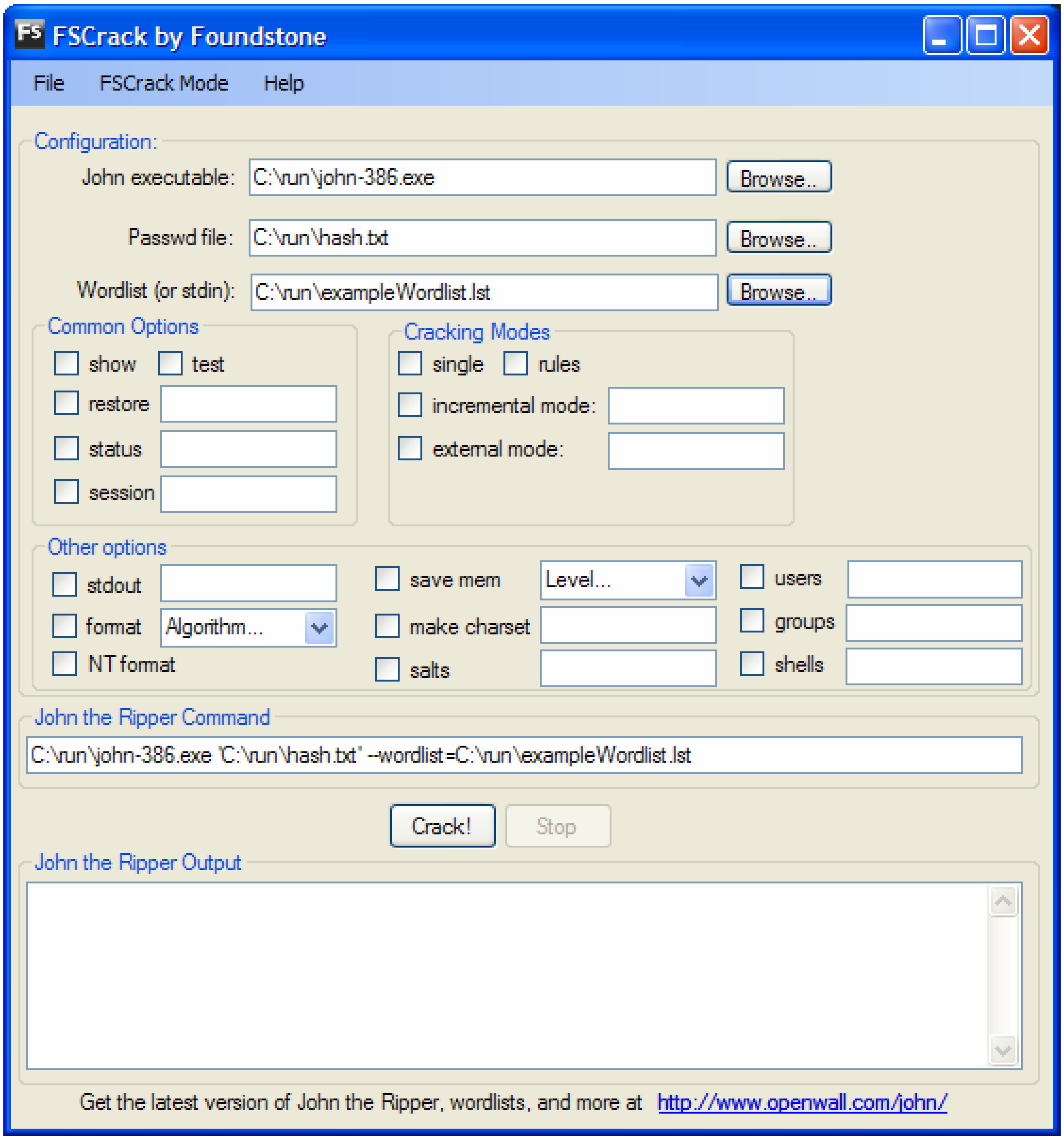
Passwd file: C:\run\hash.txt

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt'
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Select a Wordlist file**
  - Description: The wordlist file specifies a wordlist to use when cracking passwords. If a wordlist file is used, JtR will use the specified wordlist, instead of the default password.lst file. FSCrack uses a file dialog to select the desired wordlist file to use when cracking passwords.
  - Selecting a wordlist in FSCrack: Click on the **Browse…** button to the right of the **Wordlist file** label to populate the **Wordlist** text area.
  - Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

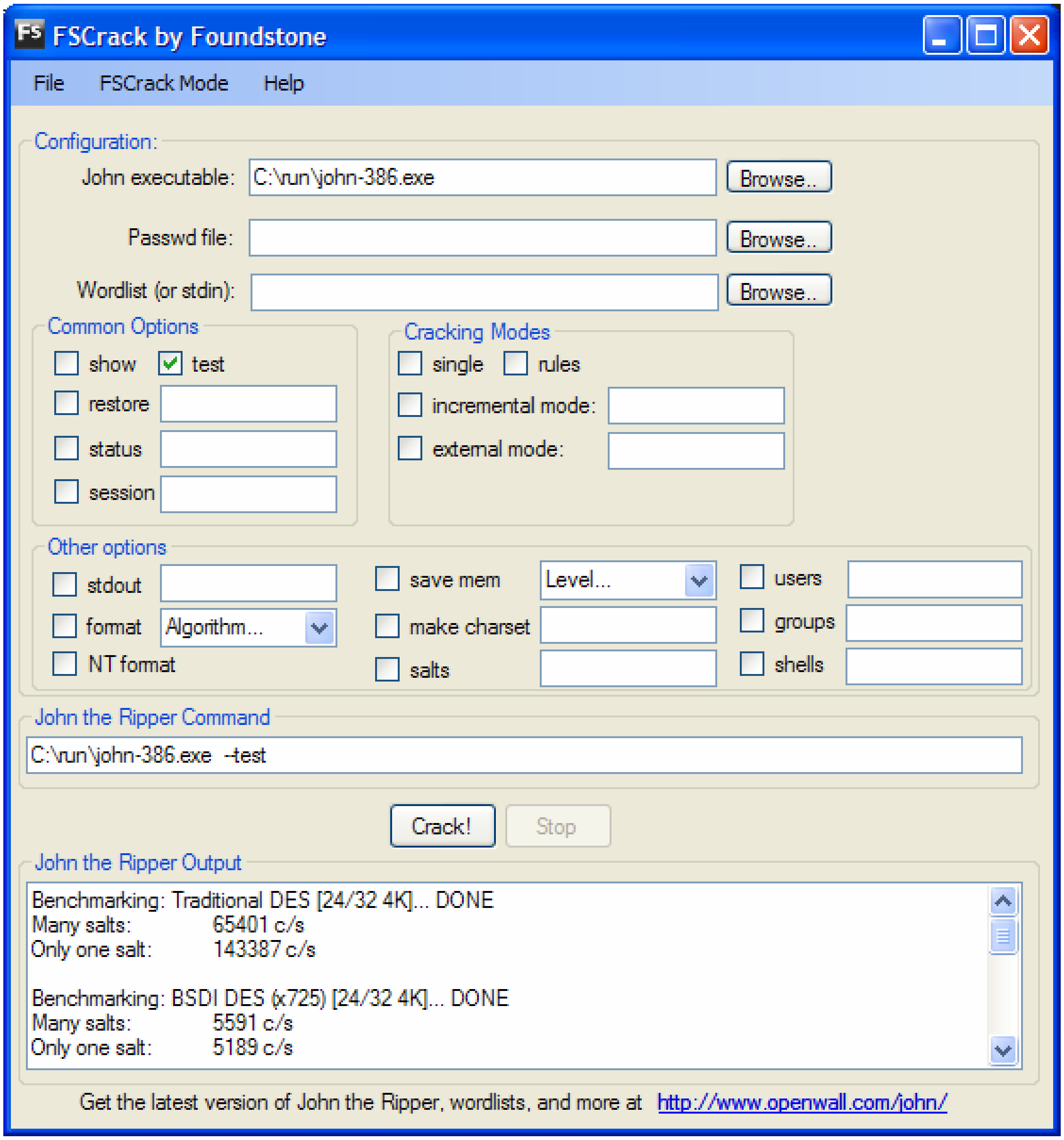
Wordlist (or stdin): C:\run\exampleWordlist.lst

John the Ripper Command:

```
C:\run\john-386.exe 'C:\run\hash.txt' --wordlist=C:\run\exampleWordlist.lst
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- Test
  - Description: The test option performs a benchmark test for JtR.
  - Running the **test** option in FSCrack: Select the **test** option and click on the **Crack!** button. FSCrack will output the benchmark results in the **John the Ripper output** text area.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file:

Wordlist (or stdin):

Common Options

□ show ☑ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format Algorithm...

□ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

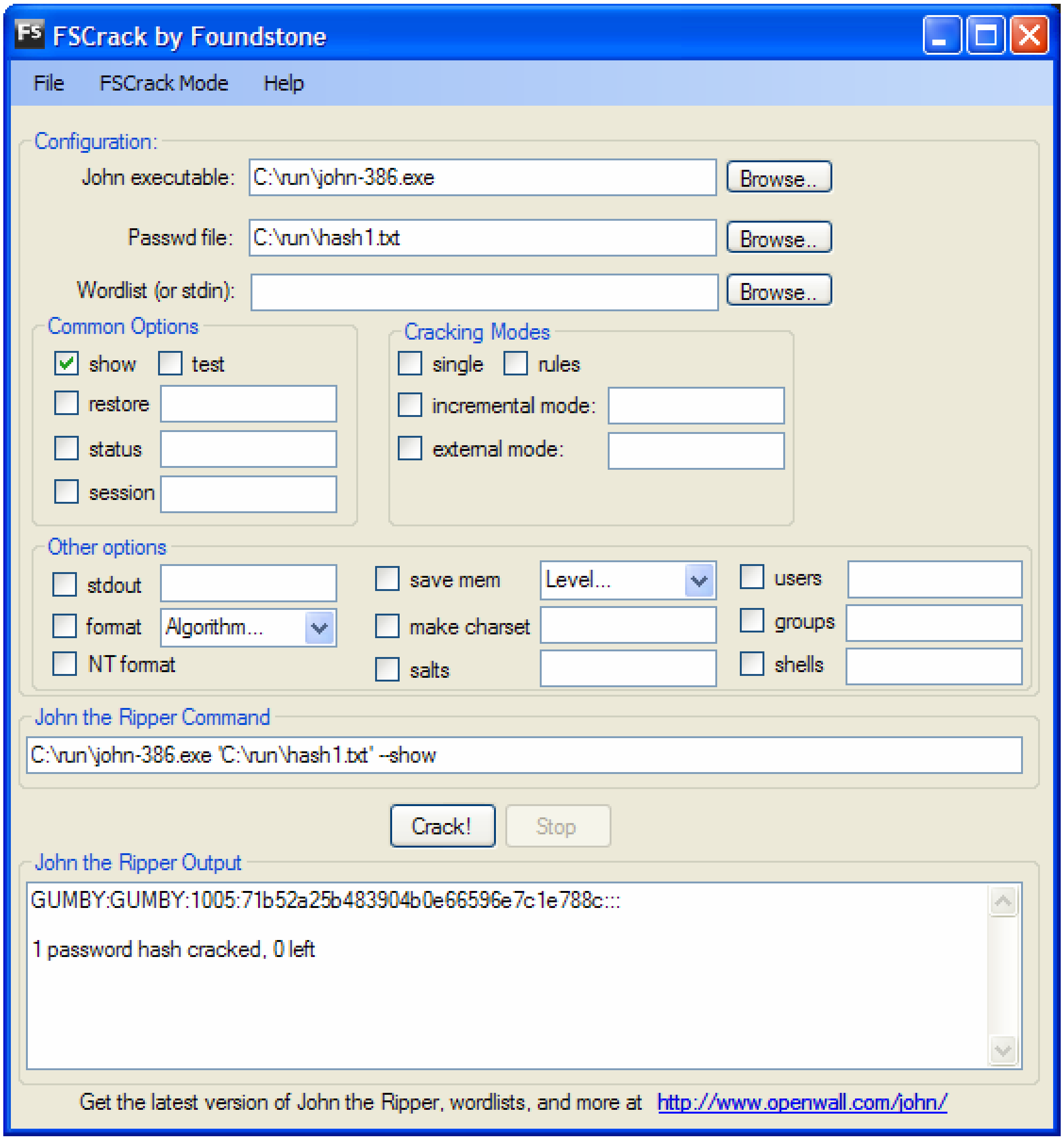
```
C:\run\john-386.exe  --test
```

John the Ripper Output

```
Benchmarking: Traditional DES [24/32 4K]... DONE
Many salts:        65401 c/s
Only one salt:     143387 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:        5591 c/s
Only one salt:     5189 c/s
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Show**
  - Description: The **show** option displays any previously cracked passwords.
  - Running the **show** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **show** option and click on the **Crack!** button. FSCrack will output the already cracked passwords from the specified passwd file in the **John the Ripper output** text area.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\hash1.txt

Wordlist (or stdin):

Common Options

☑ show ☐ test

☐ restore

☐ status

☐ session

Cracking Modes

☐ single ☐ rules

☐ incremental mode:

☐ external mode:

Other options

☐ stdout

☐ format Algorithm...

☐ NT format

☐ save mem Level...

☐ make charset

☐ salts

☐ users

☐ groups

☐ shells

John the Ripper Command

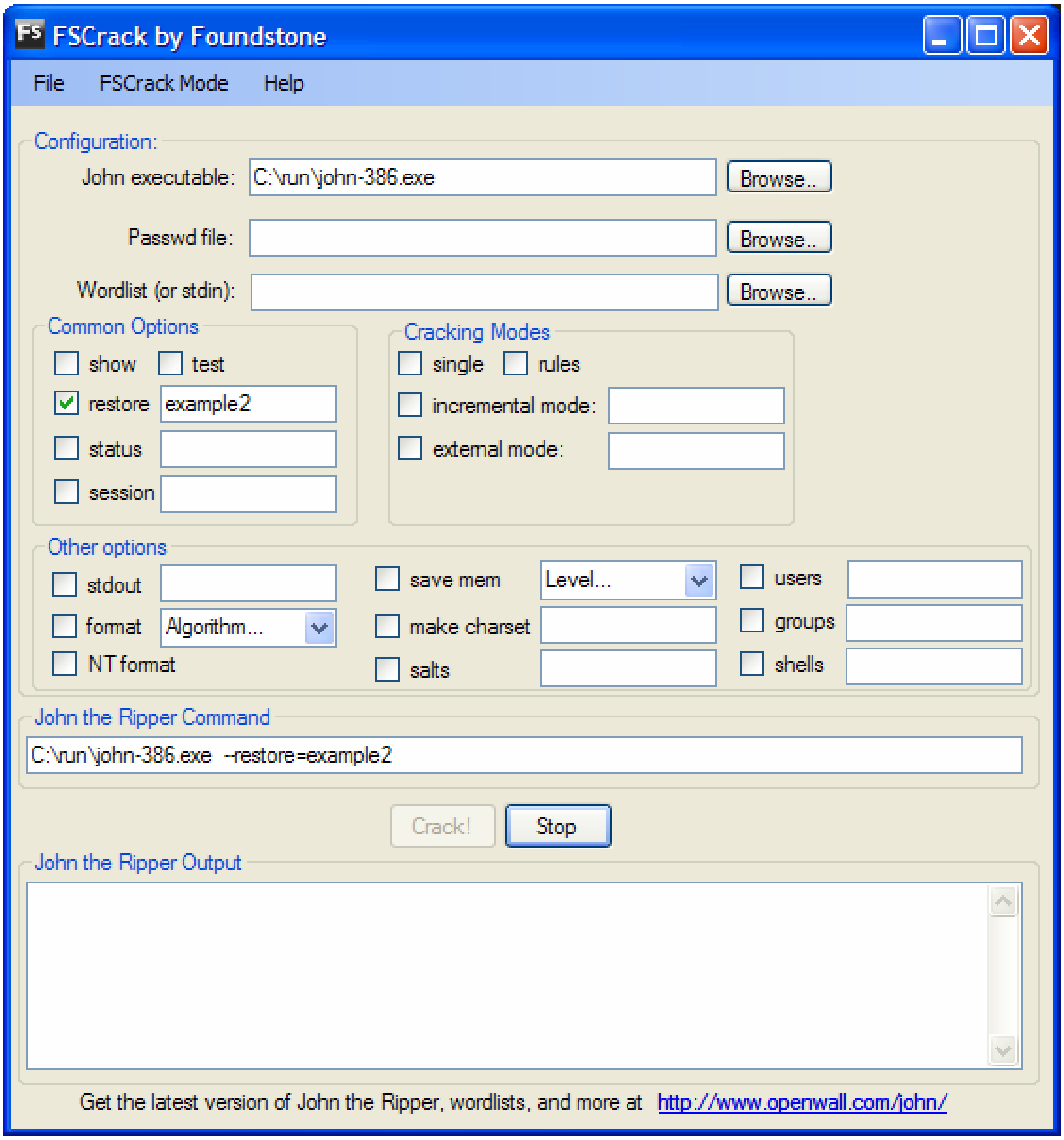
```
C:\run\john-386.exe 'C:\run\hash1.txt' --show
```

John the Ripper Output

```
GUMBY:GUMBY:1005:71b52a25b483904b0e66596e7c1e788c:::

1 password hash cracked, 0 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Restore**
  - Description: The **restore** option restores any previous JtR cracking session.
  - Running the **restore** option in FSCrack: Select the **restore** option (and select the name of a session to restore; otherwise, JtR will attempt to restore the last session you ran) and click on the **Crack!** button. FSCrack will resume cracking the specified session.
  - Screenshot below:



John executable: C:\run\john-386.exe

Passwd file:

Wordlist (or stdin):

Common Options: □ show □ test ☑ restore example2 □ status □ session

Cracking Modes: □ single □ rules □ incremental mode: □ external mode:

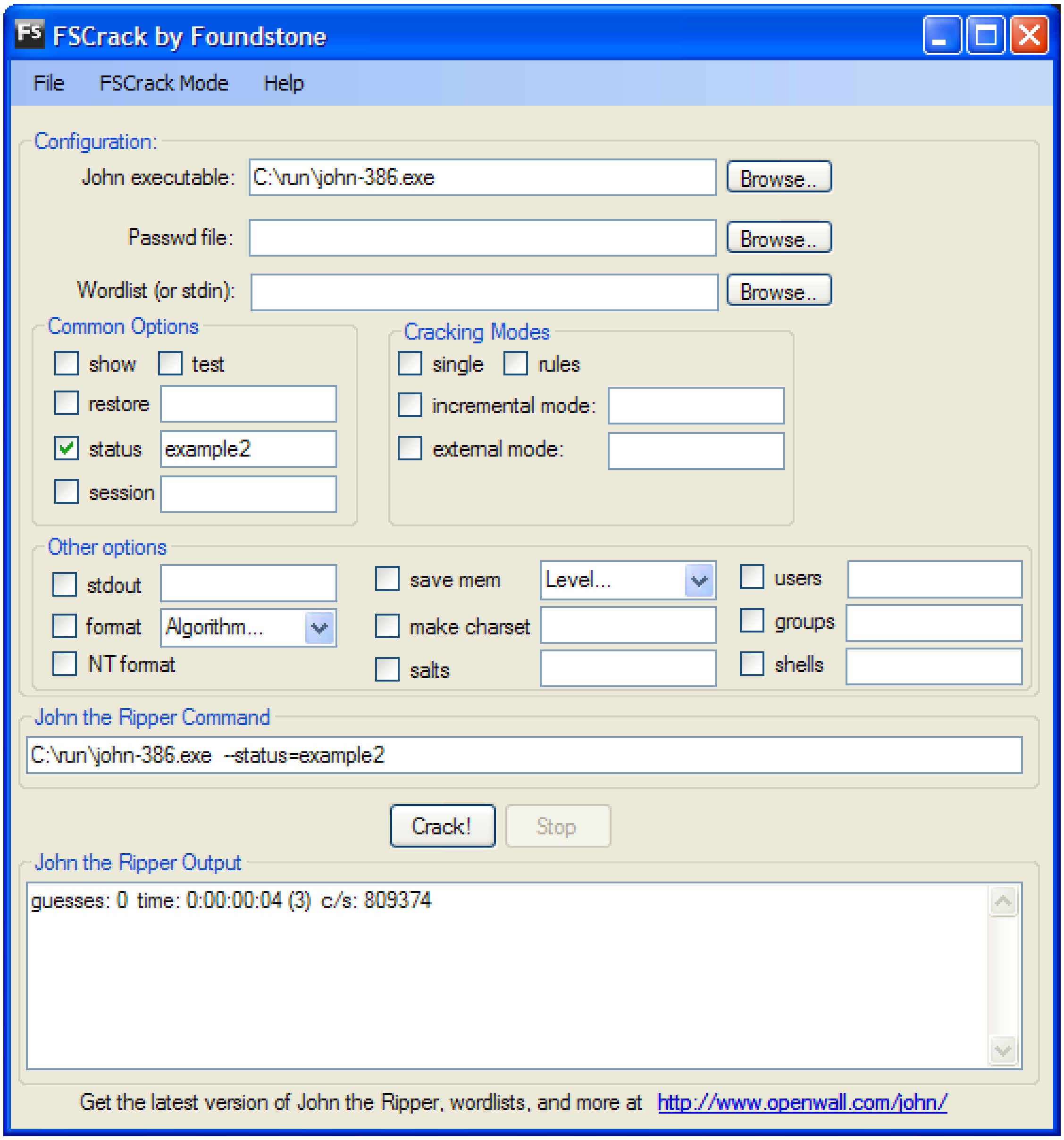
Other options: □ stdout □ format Algorithm... □ NT format □ save mem Level... □ make charset □ salts □ users □ groups □ shells

John the Ripper Command

```
C:\run\john-386.exe  --restore=example2
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Status**
  - Description: The **status** option outputs the status of a password cracking session.
  - Running the **status** option in FSCrack: Select the **status** option (and optionally specify the name of the session for which you wish to get status) and click on the **Crack!** button. FSCrack will output the status to the **John the Ripper output** text area.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file:

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

☑ status example2

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format Algorithm...

□ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

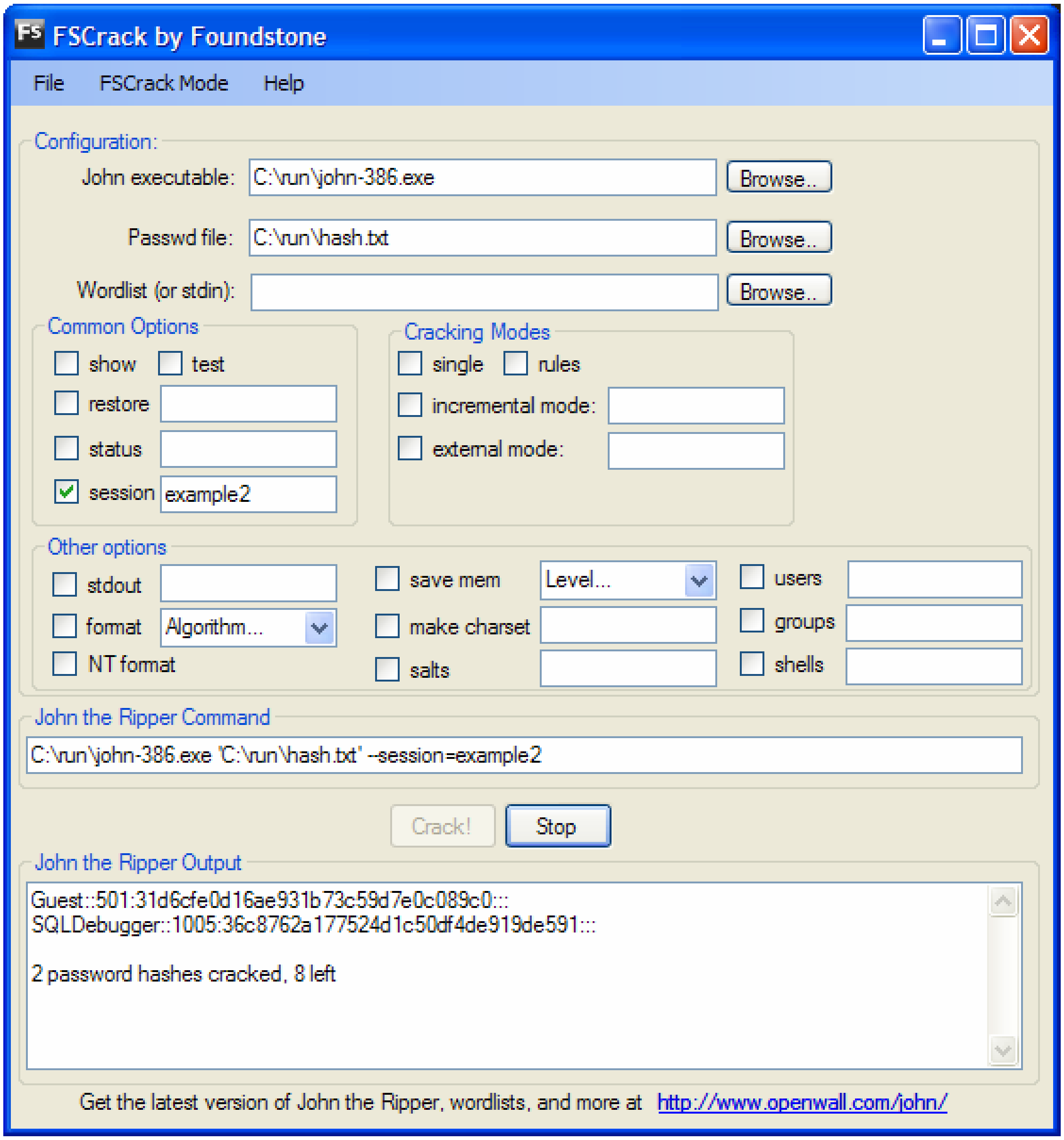
```
C:\run\john-386.exe  --status=example2
```

John the Ripper Output

```
guesses: 0  time: 0:00:00:04 (3)  c/s: 809374
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Session**
  - Description: The **session** option creates a new session with the specified name.
  - Running the **session** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **session** option and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file under the specified session name. This is helpful if one would like to later abort a session and later resume it with the given name.
  - Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

Common Options: □ show □ test □ restore □ status ☑ session example2

Cracking Modes: □ single □ rules □ incremental mode: □ external mode:

Other options: □ stdout □ format Algorithm... □ NT format □ save mem Level... □ make charset □ salts □ users □ groups □ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt' --session=example2
```

John the Ripper Output

```
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
SQLDebugger::1005:36c8762a177524d1c50df4de919de591:::

2 password hashes cracked, 8 left
```

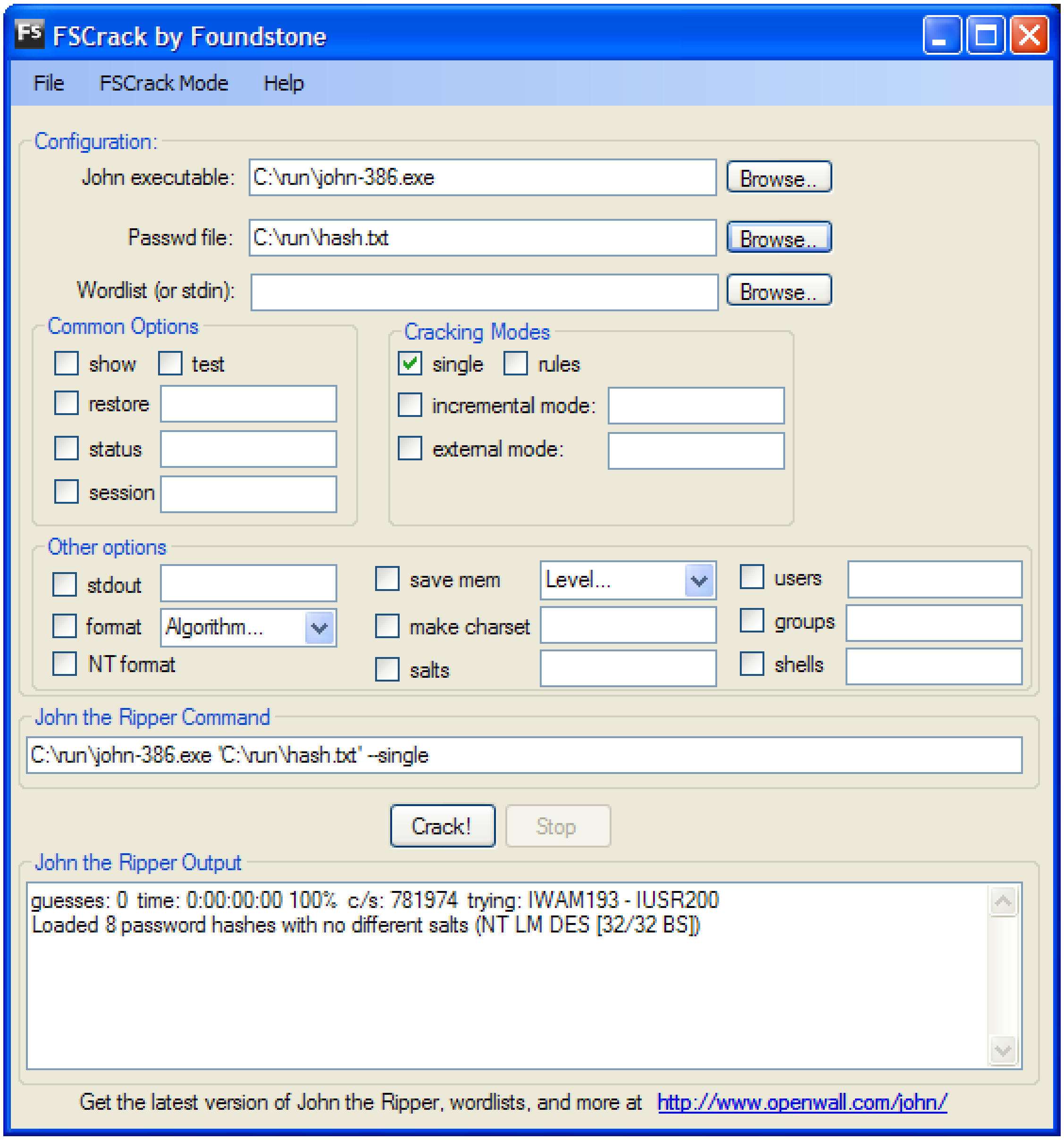
Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

Cracking Modes

- **Single**
  - Description: The **single** option specifies that the rules from the john.ini configuration file's single mode should be used exclusively. The single mode is a first pass that JtR makes by default when cracking passwords. It attempts to crack the passwords

based on the username, GECOS, user home directory names, and some basic word mangling rules based on these fields.

- Running the **single** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **single** option and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file using the single mode exclusively.
- Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

Common Options: ☐ show ☐ test ☐ restore ☐ status ☐ session

Cracking Modes: ☑ single ☐ rules ☐ incremental mode: ☐ external mode:

Other options: ☐ stdout ☐ format Algorithm... ☐ NT format ☐ save mem Level... ☐ make charset ☐ salts ☐ users ☐ groups ☐ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt' --single
```

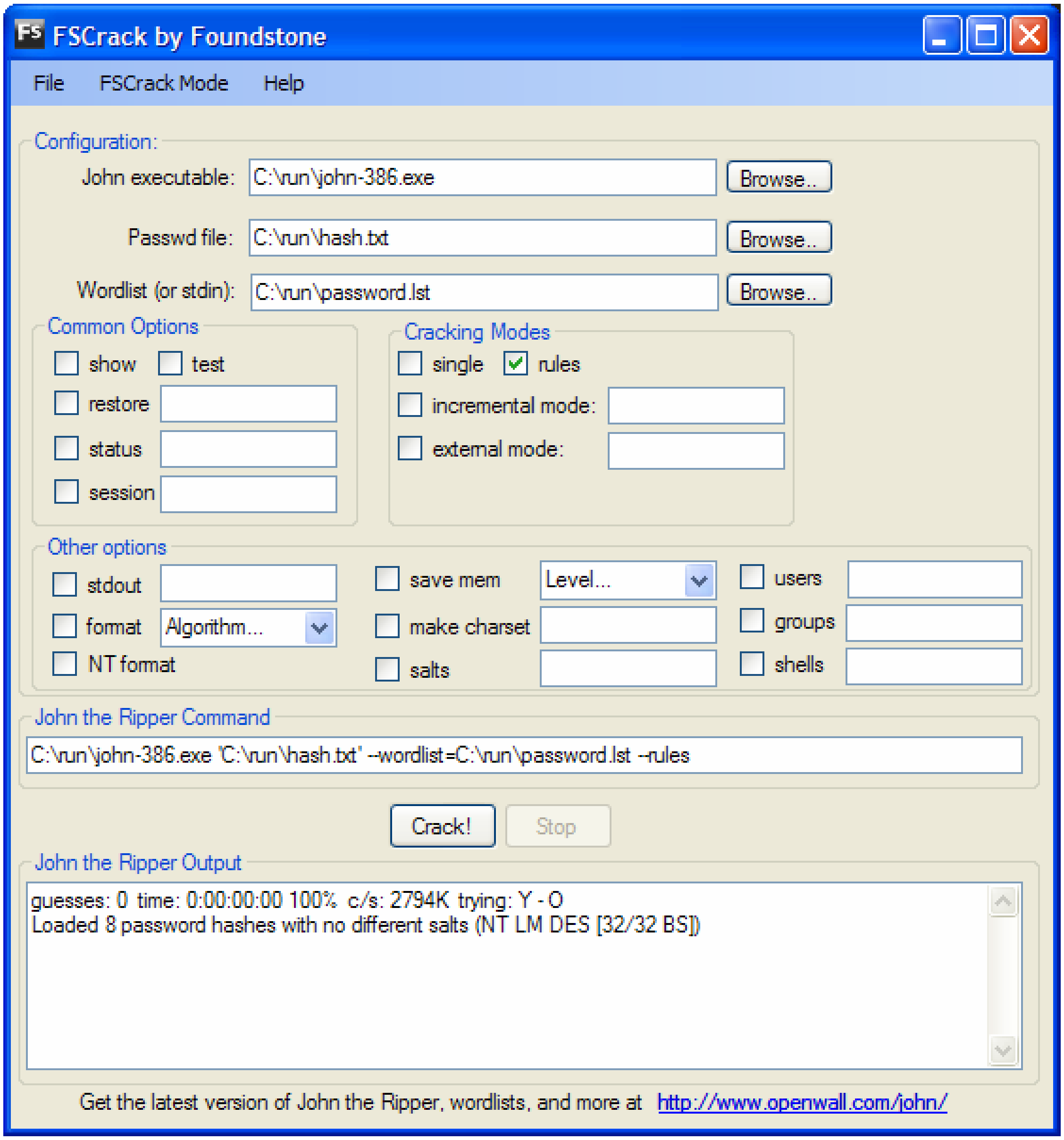
John the Ripper Output

```
guesses: 0  time: 0:00:00:00 100%  c/s: 781974  trying: IWAM193 - IUSR200
Loaded 8 password hashes with no different salts (NT LM DES [32/32 BS])
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Rules**

- Description: The **rules** option enables word mangling rules for a wordlist file when running a cracking session.
- Running the **rules** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select a wordlist file using the **Browse…** button to the right of the **Wordlist file** label. Select the **rules** option and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file and use word mangling rules on the wordlist file.
- Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin): C:\run\password.lst

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single ☑ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format Algorithm...

□ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

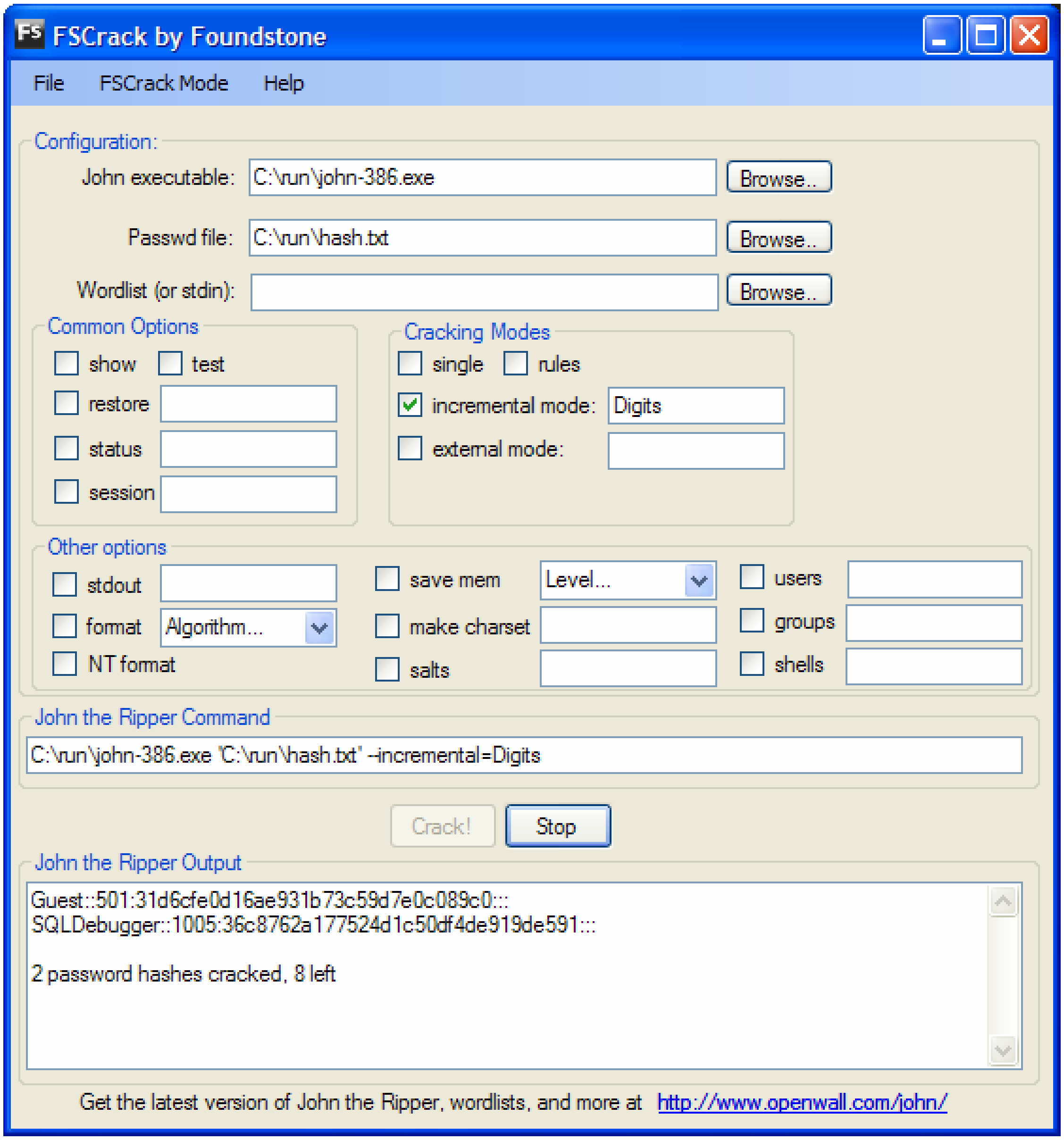
```
C:\run\john-386.exe 'C:\run\hash.txt' --wordlist=C:\run\password.lst --rules
```

John the Ripper Output

```
guesses: 0  time: 0:00:00:00 100%  c/s: 2794K  trying: Y - O
Loaded 8 password hashes with no different salts (NT LM DES [32/32 BS])
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Incremental mode**
  - Description: The **incremental mode** option specifies that JtR should try all possible combinations of characters as passwords. This is the most powerful and time-consuming cracking mode. The **incremental mode** option requires a specified mode, which is defined in the john.ini configuration file. The following modes are acceptable parameters: “All”, “Alpha”, “Alnum” (alpha/numeric), “Digits”, “LanMan”, or a custom-defined mode.
  - Running the **incremental** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **incremental** option, specify a mode name and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file using the incremental mode with the given name.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

Common Options

☐ show ☐ test

☐ restore

☐ status

☐ session

Cracking Modes

☐ single ☐ rules

☑ incremental mode: Digits

☐ external mode:

Other options

☐ stdout

☐ format Algorithm...

☐ NT format

☐ save mem Level...

☐ make charset

☐ salts

☐ users

☐ groups

☐ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt' --incremental=Digits
```

John the Ripper Output

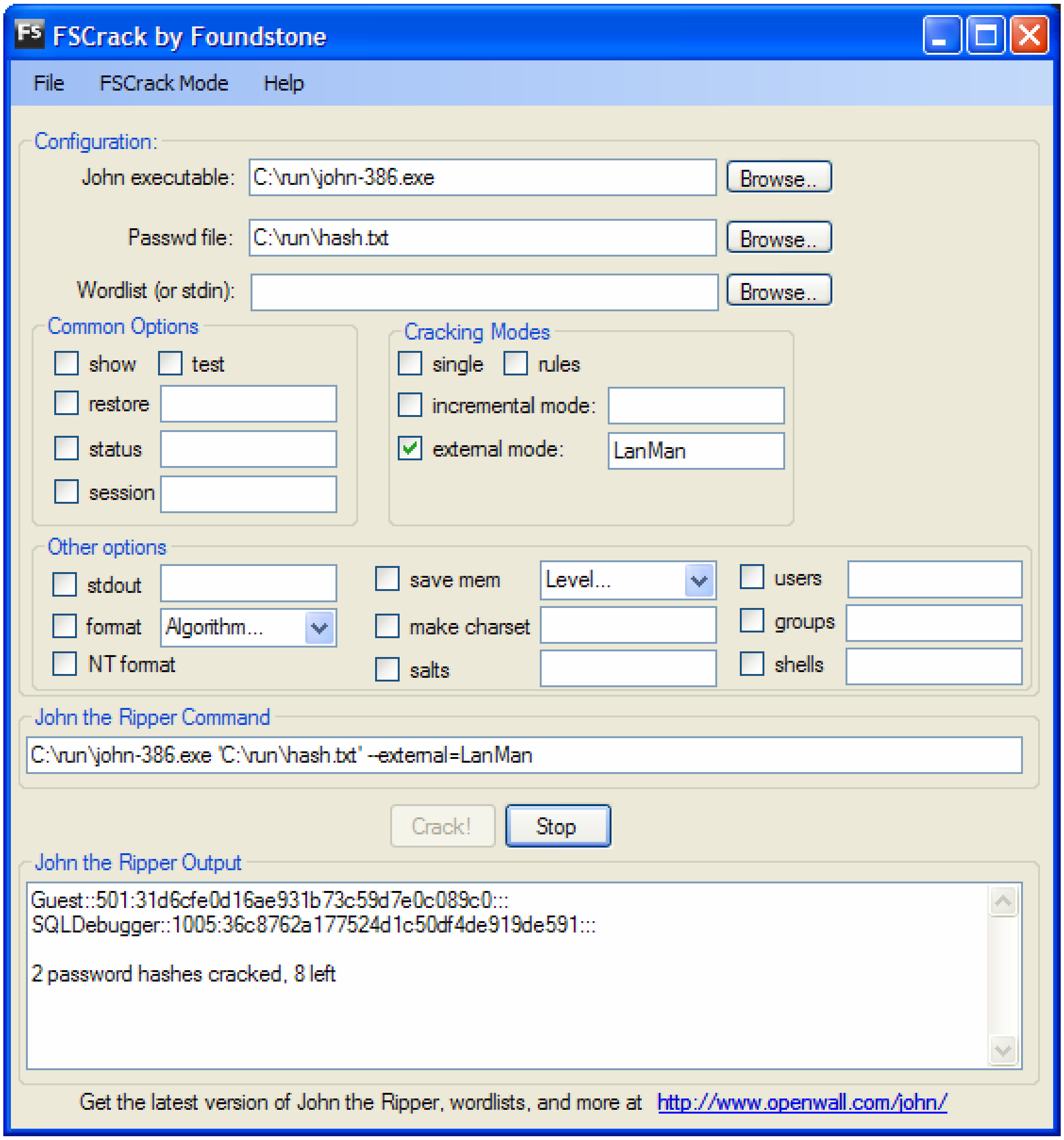
```
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
SQLDebugger::1005:36c8762a177524d1c50df4de919de591:::

2 password hashes cracked, 8 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **External mode**
  - o Description: The **external mode** option specifies that JtR should execute using a custom-defined mode. From the JtR website (http://openwall.org/john/doc/Modes.shtml): "You can define an external cracking mode for use with John. This is done with the configuration file sections called [List.External:MODE], where MODE is any name that you assign to the mode. The section should contain program code of some functions that John will use to generate the candidate passwords it tries. The functions are coded in a subset of C

and are compiled by John at startup when you request the particular external mode…"

- Running the **external mode** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **external mode** option, specify the name of the external mode, and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file using the given external mode.
- Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\hash.txt

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

☑ external mode: LanMan

Other options

□ stdout

□ format Algorithm...

□ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\hash.txt' --external=LanMan
```

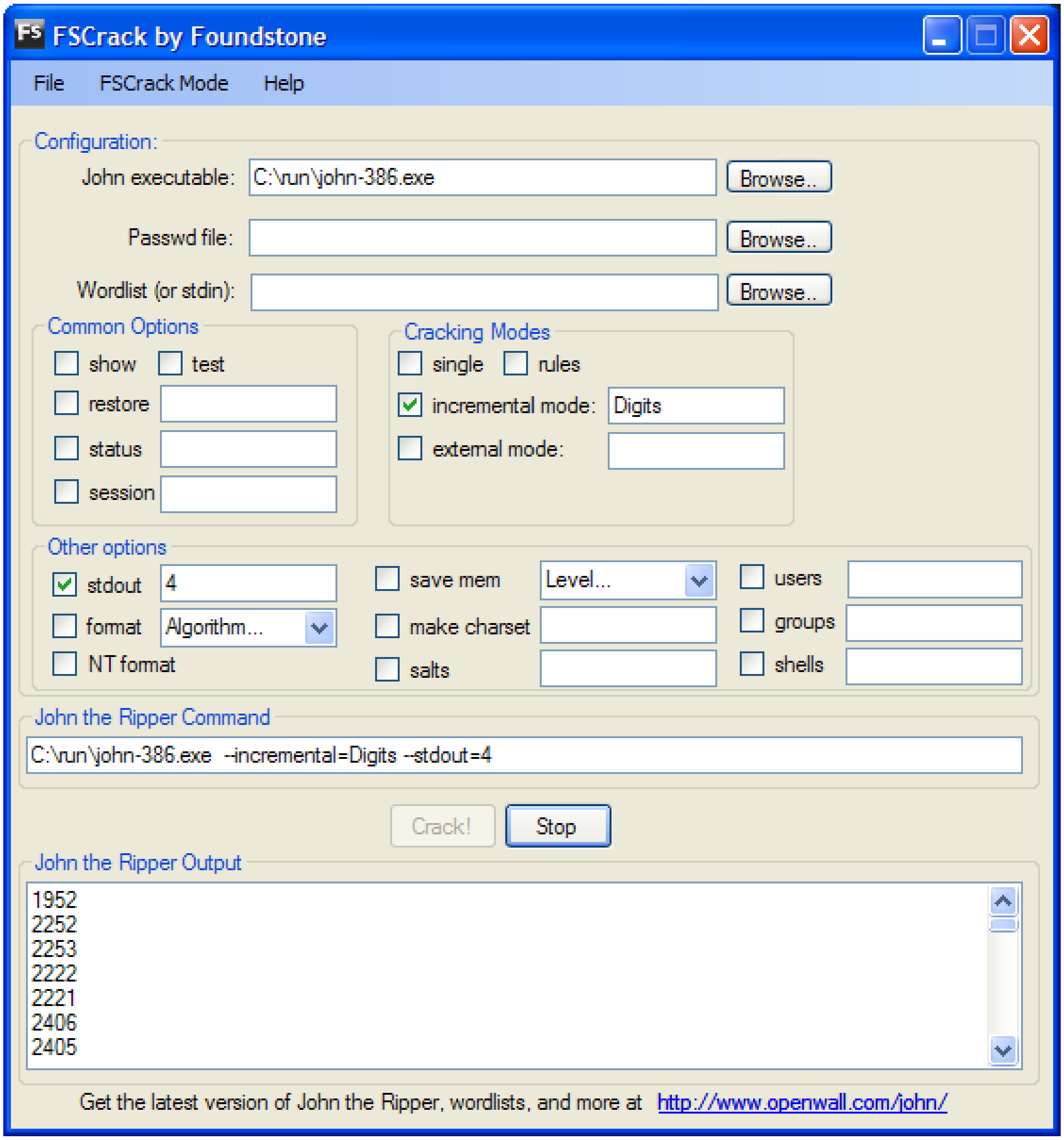
John the Ripper Output

```
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
SQLDebugger::1005:36c8762a177524d1c50df4de919de591:::

2 password hashes cracked, 8 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

Other options

- **Stdout**
  - Description: The **stdout** option, when used with a cracking mode (other than **single**) will output candidate passwords to the **John the Ripper Output** text area, instead of actually trying to crack the passwods. **Stdout** can optionally be passed a length parameter, which JtR will assume is the password length and, therefore, will not output any passwords with lengths greater specified.
  - Running the **stdout** option in FSCrack: Select a cracking mode using either the incremental, external or wordlist modes. Select the **stdout** option and optionally input a password length; and click on the **Crack!** button. FSCrack will output candidate passwords to the **John the Ripper Output** text area.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file:

Wordlist (or stdin):

Common Options

☐ show ☐ test

☐ restore

☐ status

☐ session

Cracking Modes

☐ single ☐ rules

☑ incremental mode: Digits

☐ external mode:

Other options

☑ stdout 4

☐ format Algorithm...

☐ NT format

☐ save mem Level...

☐ make charset

☐ salts

☐ users

☐ groups

☐ shells

John the Ripper Command

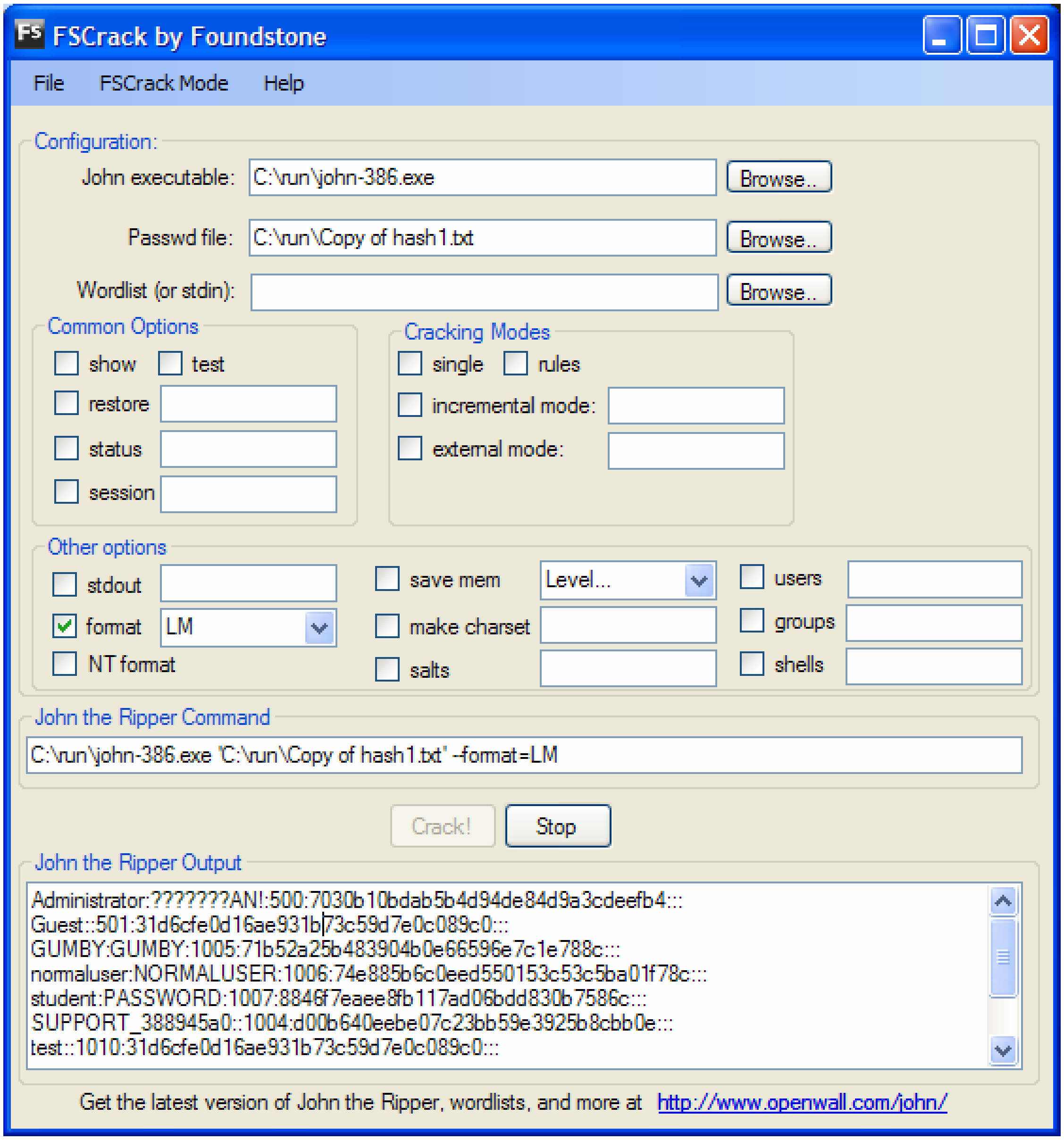
```
C:\run\john-386.exe  --incremental=Digits --stdout=4
```

John the Ripper Output

```
1952
2252
2253
2222
2221
2406
2405
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Format**
  - Description: The **format** option forces JtR to use a specified ciphertext format, such as DES, BSDI, MD5, BF, AFS, and LM.
  - Running the **format** option in FSCrack: Select a passwd file using the **Browse...** button to the right of the **Passwd file** label. Select the **format** option and click on the **Crack!** button. FSCrack will start cracking passwords using the specified format.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe [Browse..]

Passwd file: C:\run\Copy of hash1.txt [Browse..]

Wordlist (or stdin): [Browse..]

Common Options

☐ show ☐ test

☐ restore

☐ status

☐ session

Cracking Modes

☐ single ☐ rules

☐ incremental mode:

☐ external mode:

Other options

☐ stdout

☑ format LM

☐ NT format

☐ save mem Level...

☐ make charset

☐ salts

☐ users

☐ groups

☐ shells

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\Copy of hash1.txt' -format=LM
```

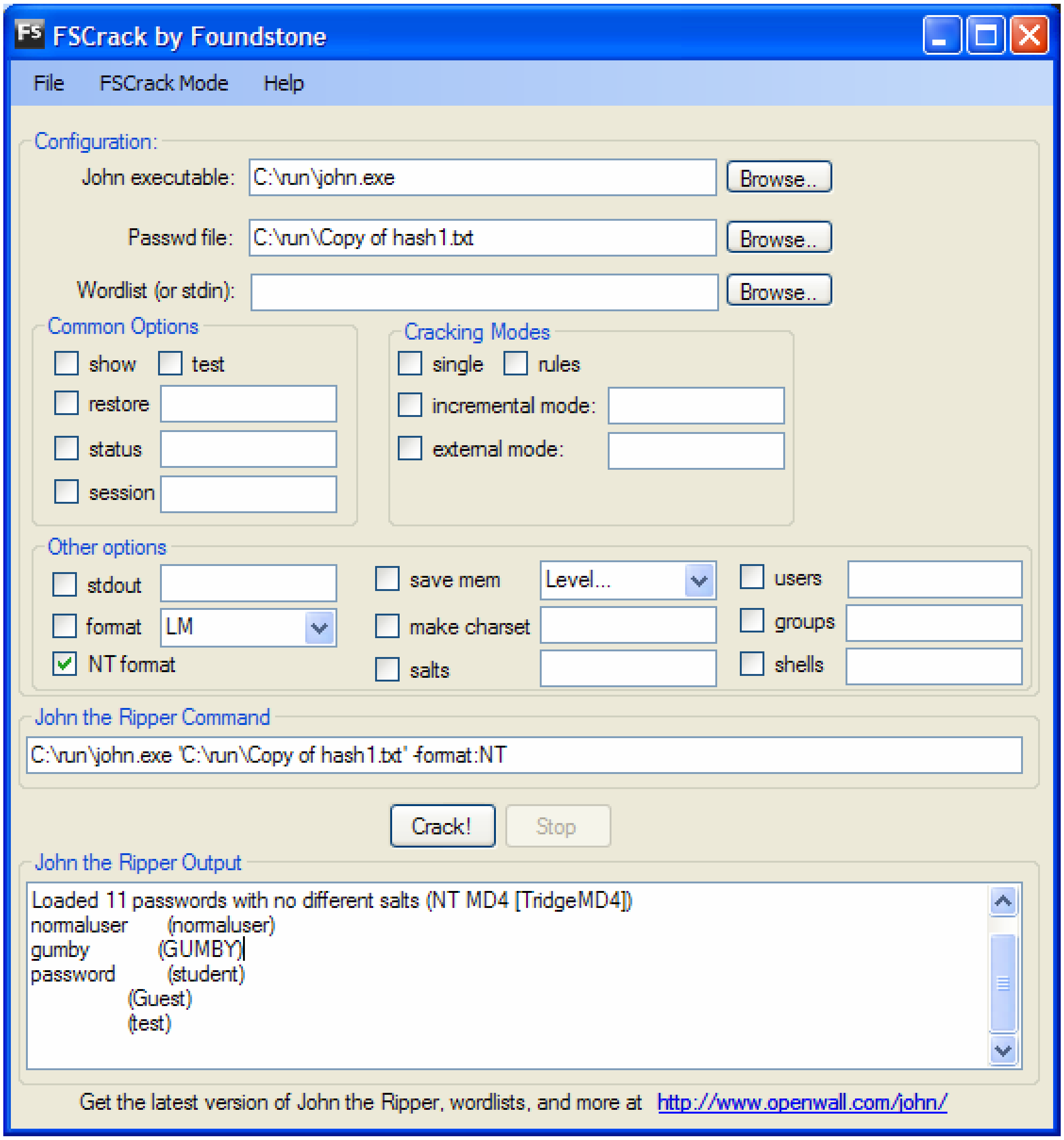
John the Ripper Output

```
Administrator:???????AN!:500:7030b10bdab5b4d94de84d9a3cdeefb4:::
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
GUMBY:GUMBY:1005:71b52a25b483904b0e66596e7c1e788c:::
normaluser:NORMALUSER:1006:74e885b6c0eed550153c53c5ba01f78c:::
student:PASSWORD:1007:8846f7eaee8fb117ad06bdd830b7586c:::
SUPPORT_388945a0::1004:d00b640eebe07c23bb59e3925b8cbb0e:::
test::1010:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **NT format**
  - Description: The **NT format** option allows for JtR to output cracked passwords in NTLM format, using the patch for NTLM (MD4) hash by Olle Segerdahl.
  - Running the **NT format** option in FSCrack: Select the JtR (Olle Segerdahl-patched) executable using the **Browse...** button to the right of the **John executable** label. Select a passwd file using the **Browse...** button to the right of the **Passwd file** label for a password file that includes at least one password that has been cracked. Select the **NT format** option, and click on the **Crack!** button. FSCrack will output the passwords in correct NTLM formatted passwords.

- o Screenshot below:



Configuration:

John executable: C:\run\john.exe

Passwd file: C:\run\Copy of hash1.txt

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format LM

☑ NT format

□ save mem Level...

□ make charset

□ salts

□ users

□ groups

□ shells

John the Ripper Command

```
C:\run\john.exe 'C:\run\Copy of hash1.txt' -format:NT
```

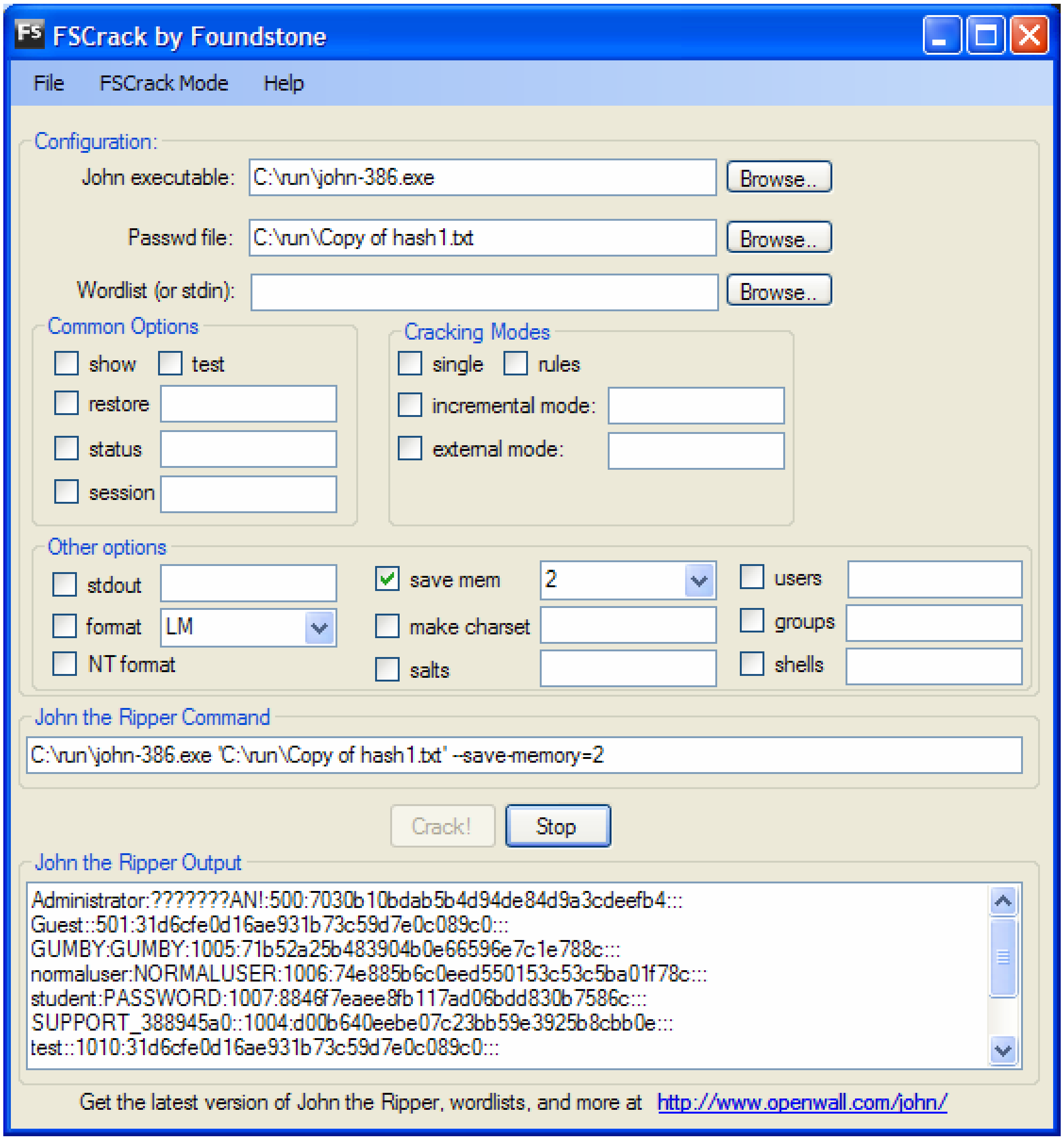
John the Ripper Output

```
Loaded 11 passwords with no different salts (NT MD4 [TridgeMD4])
normaluser      (normaluser)
gumby          (GUMBY)
password        (student)
               (Guest)
               (test)
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Save mem**
  - o Description: The **save mem** option should be used if the end user doesn't have a lot of memory or if JtR is interfering with other programs. This option only works when a mode other than single mode is selected and allows for three different levels of memory saving, "1", "2", "3". JtR will take a performance hit when using less memory.

- o Running the **save mem** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **save mem** option, select a level (1-3), and click on the **Crack!** button. FSCrack will start cracking passwords with memory restrictions.
- o Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\Copy of hash1.txt

Wordlist (or stdin):

□ show □ test
□ restore
□ status
□ session

□ single □ rules
□ incremental mode:
□ external mode:

□ stdout
□ format LM
□ NT format
☑ save mem 2
□ make charset
□ salts
□ users
□ groups
□ shells

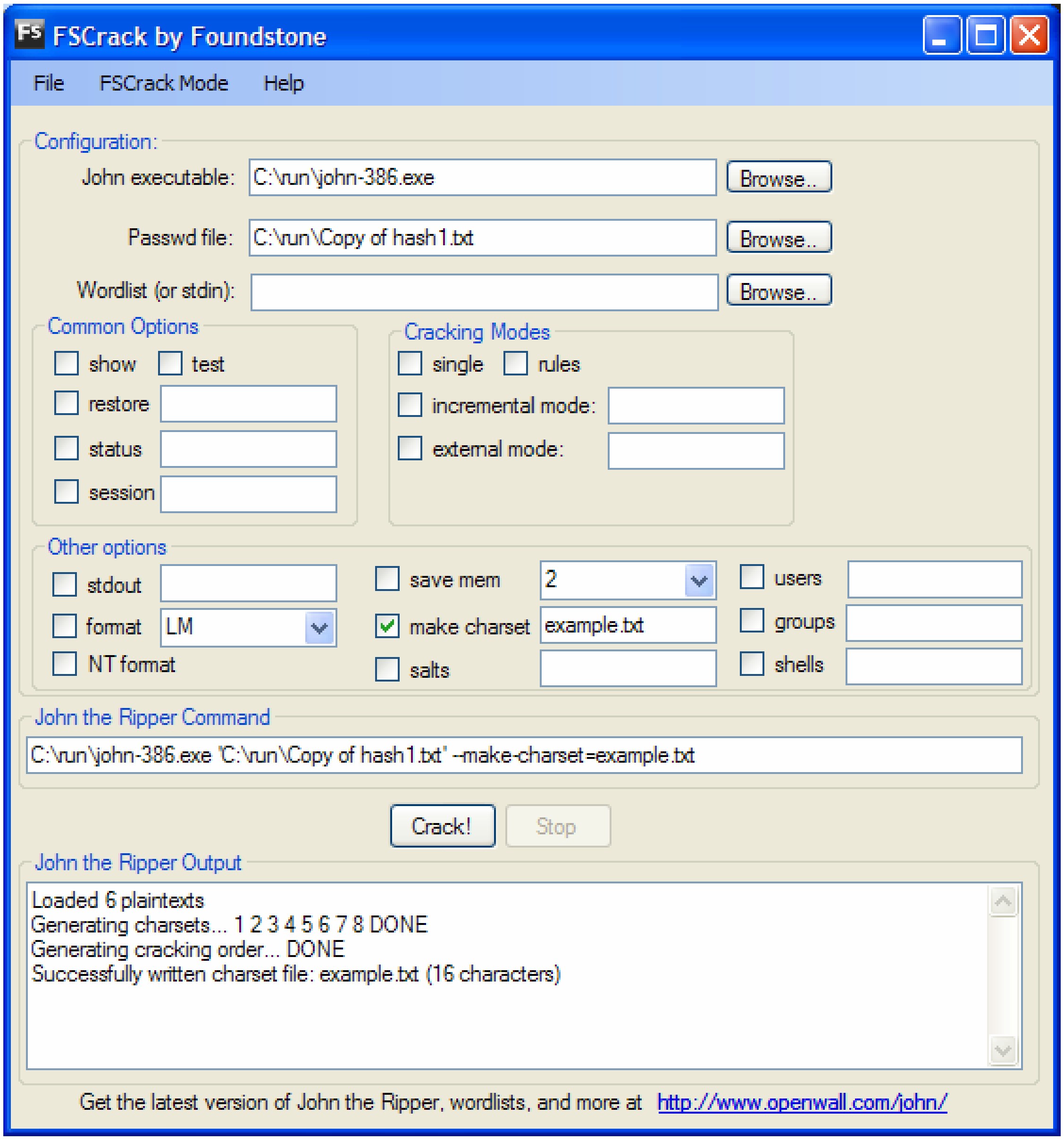
```
C:\run\john-386.exe 'C:\run\Copy of hash1.txt' --save-memory=2
```

```
Administrator:???????AN!:500:7030b10bdab5b4d94de84d9a3cdeefb4:::
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
GUMBY:GUMBY:1005:71b52a25b483904b0e66596e7c1e788c:::
normaluser:NORMALUSER:1006:74e885b6c0eed550153c53c5ba01f78c:::
student:PASSWORD:1007:8846f7eaee8fb117ad06bdd830b7586c:::
SUPPORT_388945a0::1004:d00b640eebe07c23bb59e3925b8cbb0e:::
test::1010:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Make charset**

- Description: The **make charset** option creates a new character set based on the frequency of chars found in the cracked john.pot file and can only be used with the incremental mode.
- Running the **session** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **make char** option, specify a file name for the charset file, and click on the **Crack!** button. FSCrack will generate a new file with the given name containing a charset of the cracked passwords from the passwd file.
- Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\Copy of hash1.txt

Wordlist (or stdin):

☐ format: LM

☐ save mem: 2

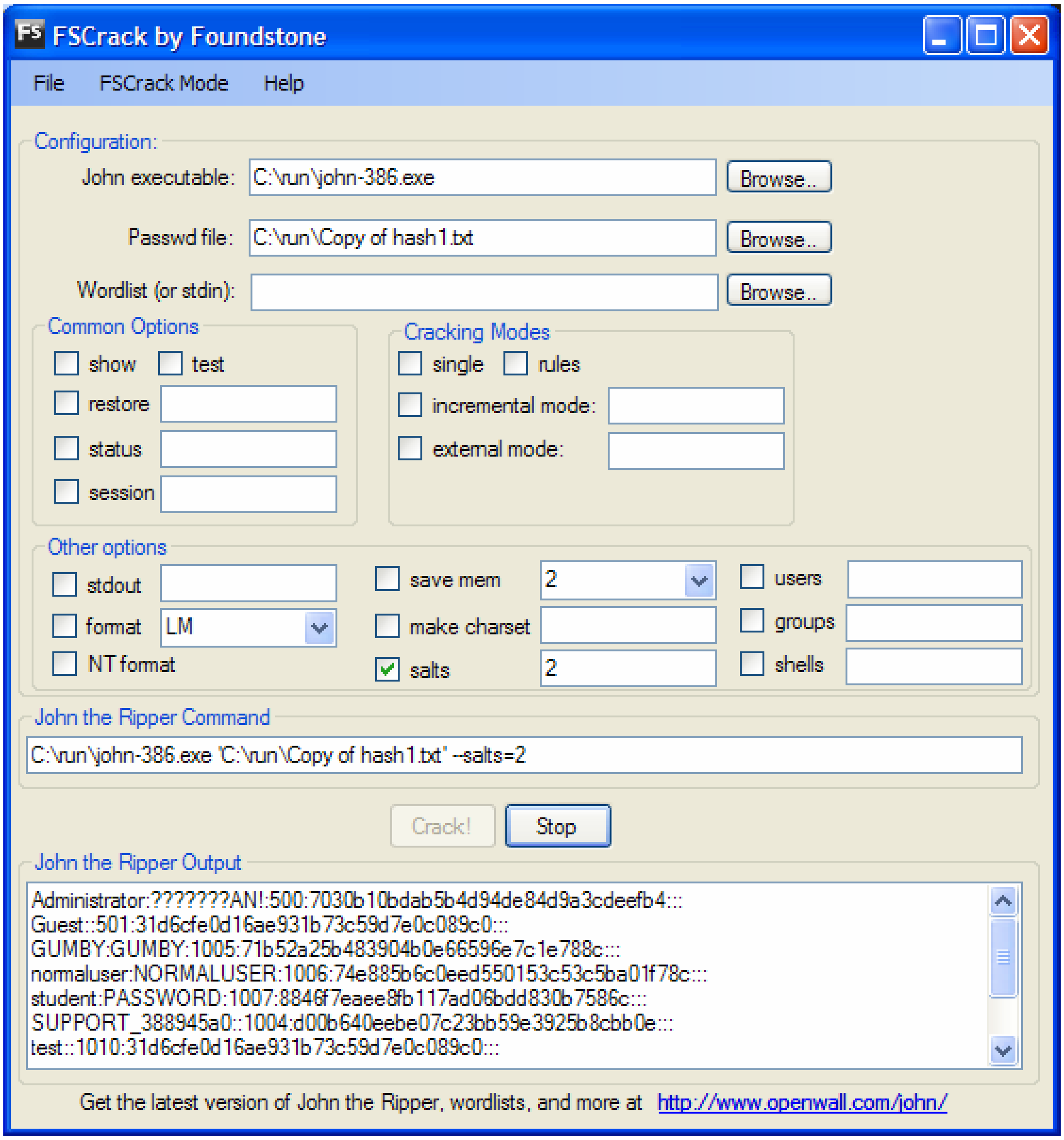
☑ make charset: example.txt

```
C:\run\john-386.exe 'C:\run\Copy of hash1.txt' --make-charset=example.txt
```

```
Loaded 6 plaintexts
Generating charsets... 1 2 3 4 5 6 7 8 DONE
Generating cracking order... DONE
Successfully written charset file: example.txt (16 characters)
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Salts**
  - Description: The **salts** option loads salts with (or without, if preceeded by a “-“) at least the specified number of passwords. This feature can be used to speed up JtR’s execution time in certain situations.
  - Running the **salts** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **salts** option, specify a parameter for the **salts** option, and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file that match the filter set in the **salts** option.
  - Screenshot below:



John executable: C:\run\john-386.exe

Passwd file: C:\run\Copy of hash1.txt

Wordlist (or stdin):

Common Options: □ show □ test □ restore □ status □ session

Cracking Modes: □ single □ rules □ incremental mode: □ external mode:

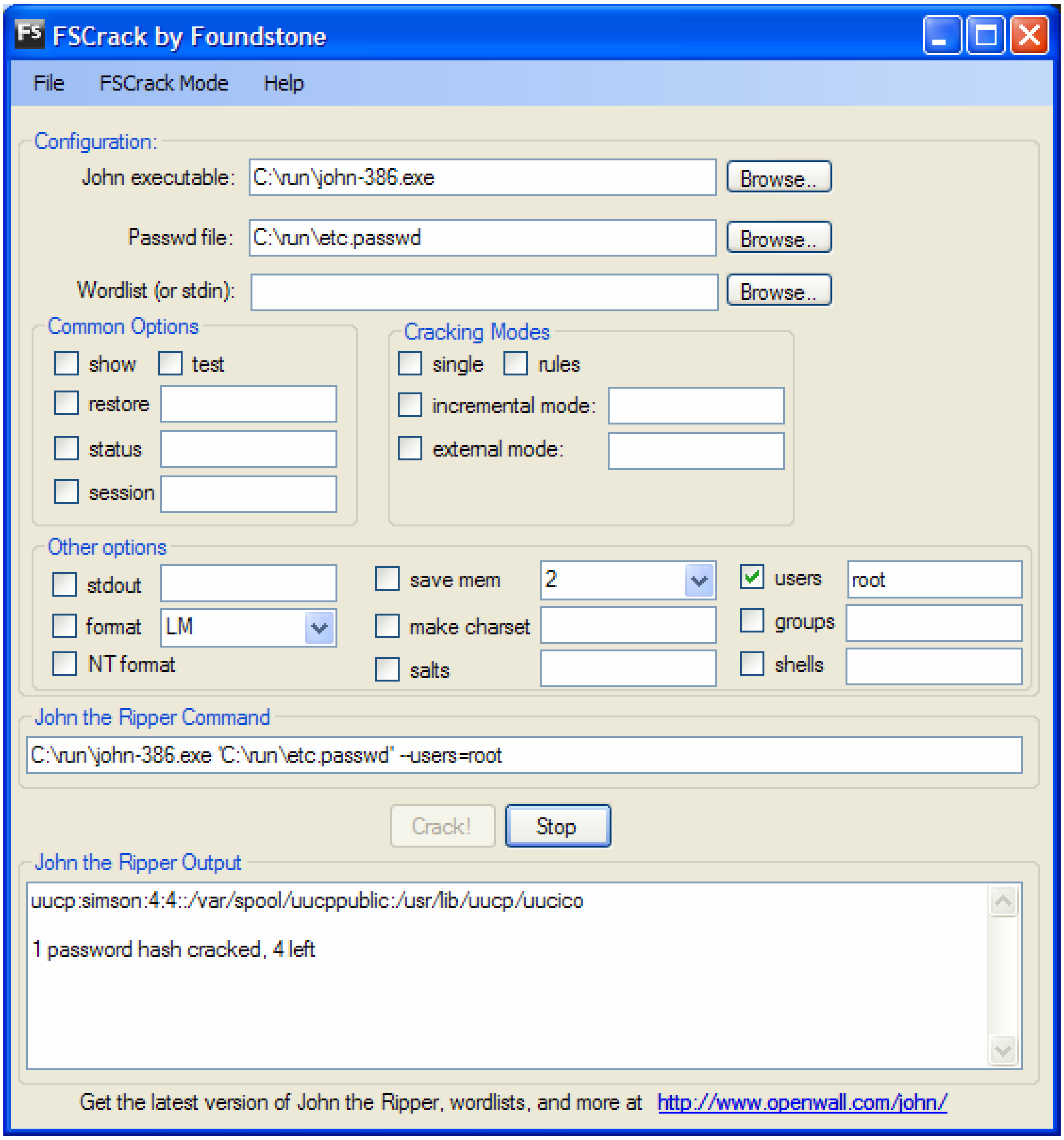
Other options: □ stdout □ format LM □ NT format □ save mem 2 □ make charset ☑ salts 2 □ users □ groups □ shells

```
C:\run\john-386.exe 'C:\run\Copy of hash1.txt' --salts=2
```

```
Administrator:???????AN!:500:7030b10bdab5b4d94de84d9a3cdeefb4:::
Guest::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
GUMBY:GUMBY:1005:71b52a25b483904b0e66596e7c1e788c:::
normaluser:NORMALUSER:1006:74e885b6c0eed550153c53c5ba01f78c:::
student:PASSWORD:1007:8846f7eaee8fb117ad06bdd830b7586c:::
SUPPORT_388945a0::1004:d00b640eebe07c23bb59e3925b8cbb0e:::
test::1010:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Users**
  - Description: The **users** option loads the users with (or without, if preceeded by a "-") with matching logins or UIDs. This feature can be used to speed up JtR's execution time, if only certain user passwords should be cracked.
  - Running the **users** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **users** option, enter user logins or UIDs, and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file that match the filter set in the **users** option.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\etc.passwd

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format LM

□ NT format

□ save mem 2

□ make charset

□ salts

☑ users root

□ groups

□ shells

John the Ripper Command

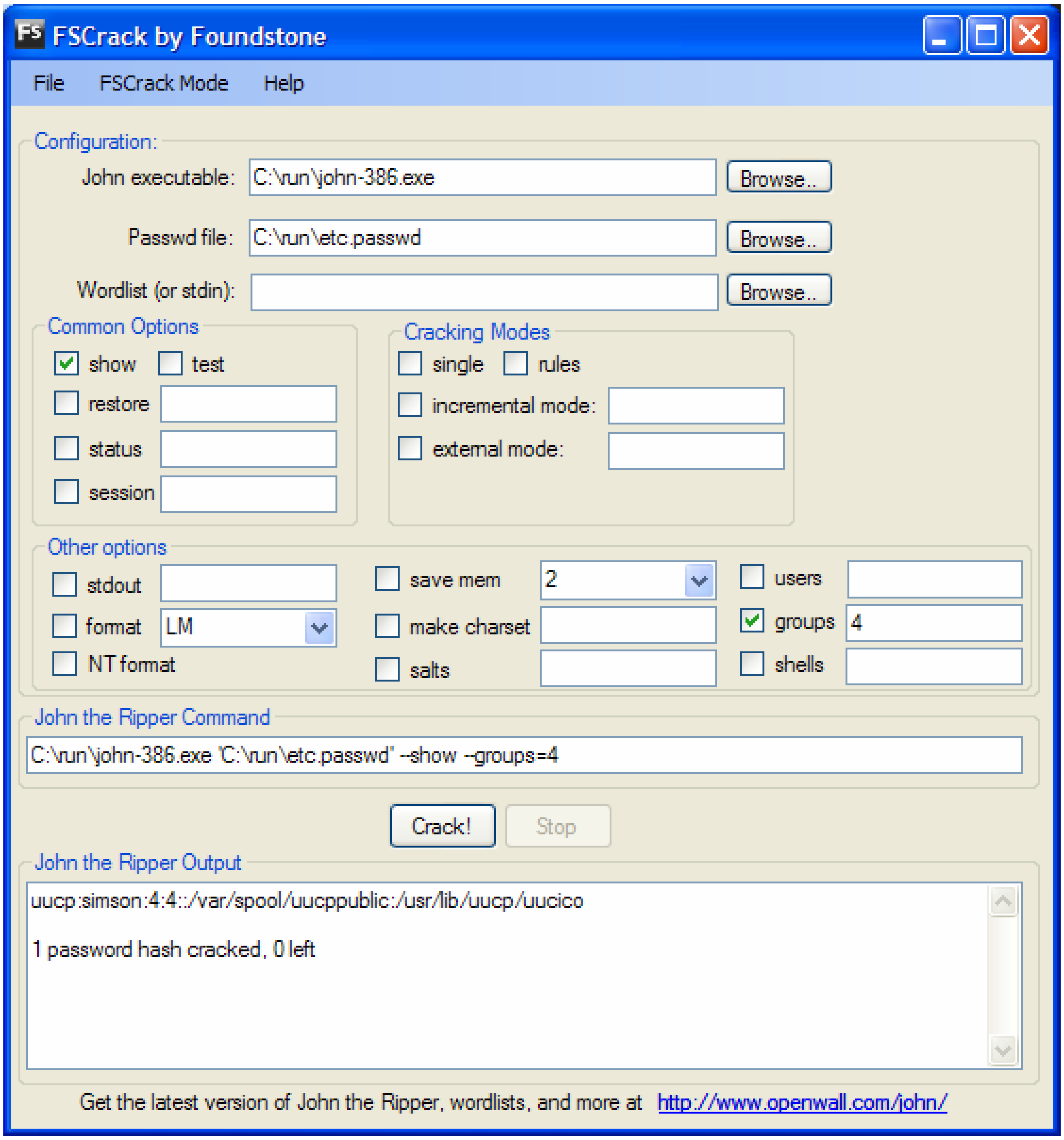
```
C:\run\john-386.exe 'C:\run\etc.passwd' –users=root
```

John the Ripper Output

```
uucp:simson:4:4::/var/spool/uucppublic:/usr/lib/uucp/uucico

1 password hash cracked, 4 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Groups**
  - Description: The **groups** option loads the users with (or without, if preceeded by a "-") with matching GIDs. This feature can be used to speed up JtR's execution time if only certain group members' passwords should be cracked.
  - Running the **groups** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **group** option, enter GIDs, and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file that match the filter set in the **groups** option.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\etc.passwd

Wordlist (or stdin):

Common Options

☑ show ☐ test

☐ restore

☐ status

☐ session

Cracking Modes

☐ single ☐ rules

☐ incremental mode:

☐ external mode:

Other options

☐ stdout

☐ format LM

☐ NT format

☐ save mem 2

☐ make charset

☐ salts

☐ users

☑ groups 4

☐ shells

John the Ripper Command

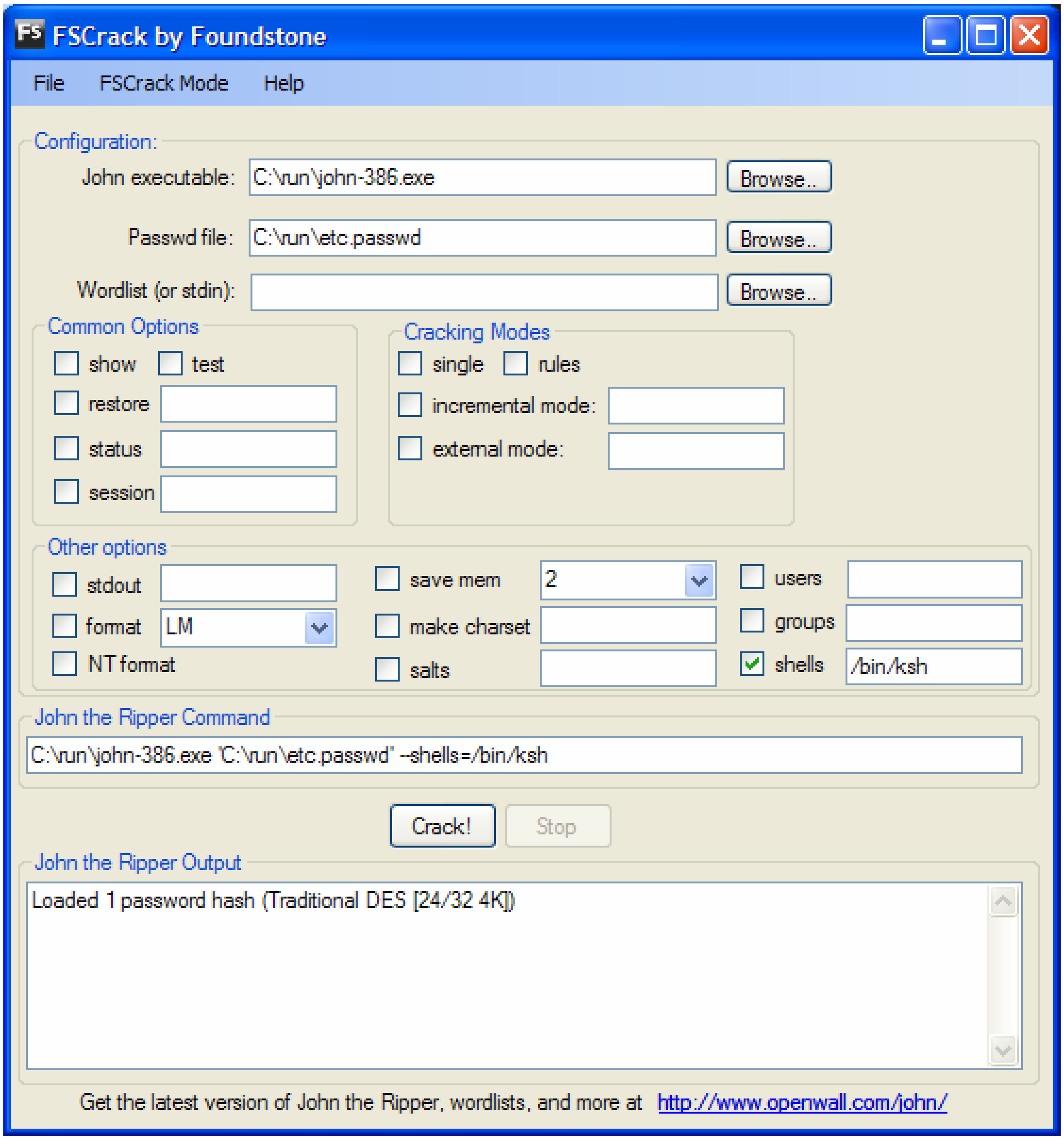
```
C:\run\john-386.exe 'C:\run\etc.passwd' --show --groups=4
```

John the Ripper Output

```
uucp:simson:4:4::/var/spool/uucppublic:/usr/lib/uucp/uucico

1 password hash cracked, 0 left
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

- **Shells**
  - Description: The **shells** option loads the users with (or without, if preceeded by a "-") with matching shells. This feature can be used to speed up JtR's execution time, if only certain users' passwords, with particular shells should be cracked.
  - Running the **shells** option in FSCrack: Select a passwd file using the **Browse…** button to the right of the **Passwd file** label. Select the **shells** option, enter a shell name, and click on the **Crack!** button. FSCrack will start cracking passwords from the specified passwd file that match the filter set in the **shells** option.
  - Screenshot below:



Configuration:

John executable: C:\run\john-386.exe

Passwd file: C:\run\etc.passwd

Wordlist (or stdin):

Common Options

□ show □ test

□ restore

□ status

□ session

Cracking Modes

□ single □ rules

□ incremental mode:

□ external mode:

Other options

□ stdout

□ format LM

□ NT format

□ save mem 2

□ make charset

□ salts

□ users

□ groups

☑ shells /bin/ksh

John the Ripper Command

```
C:\run\john-386.exe 'C:\run\etc.passwd' --shells=/bin/ksh
```

John the Ripper Output

```
Loaded 1 password hash (Traditional DES [24/32 4K])
```

Get the latest version of John the Ripper, wordlists, and more at http://www.openwall.com/john/

Appendix B: JtR Options

The following is an explanation of the common options found in JtR, taken from http://www.openwall.com/john/doc /OPTIONS/shtml:

When invoked with no command-line arguments, "john" prints its usage summary.

The supported command-line arguments are password file names and options. Many of the supported options accept additional arguments.

You can list any number of password files right on the command line of "john". You do not have to specify any options. If valid password files are specified but no options are given, John will go through the default selection of cracking modes with their default settings.

Options may be specified along with password files or on their own, although some require that password files be specified and some do not support operation on password files.

All options are case sensitive, can be abbreviated as long as the abbreviations are unambiguous, can be prefixed with two dashes (GNU-style) or with one dash, and can use "=" or ":" to indicate an argument (if supported for a given option).

The supported options are as below. Square brackets denote optional arguments.

--single "single crack" mode

Enables the "single crack" mode, using rules from the configuration file section [List.Rules:Single].

--wordlist=FILE wordlist mode, read words from FILE,
--stdin or from stdin

These are used to enable the wordlist mode.

--rules enable word mangling rules for wordlist mode

Enables word mangling rules that are read from [List.Rules:Wordlist].

--incremental[=MODE] "incremental" mode [using section MODE]

Enables the "incremental" mode, using the specified configuration file definition (section [Incremental:MODE], or [Incremental:All] by default except for LM hashes for which the default is [Incremental:LanMan]).

--external=MODE external mode or word filter

Enables an external mode, using external functions defined in section [List.External:MODE].

--stdout[=LENGTH] just output candidate passwords

When used with a cracking mode, except for “single crack”, makes John output the candidate passwords it generates to stdout instead of actually trying them against password hashes; no password files may be specified when this option is used. If a LENGTH is given, John assumes that to be the significant password length and only produces passwords up to that length.

--restore[=NAME] restore an interrupted session

Continues an interrupted cracking session, reading state information from the specified session file or from $JOHN/john.rec by default.

--session=NAME give a new session the NAME

This option can only be used when starting a new cracking session and its purpose is to give the new session a name (to which John will append the “.rec” suffix to form the session file name). This is useful for running multiple instances of John in parallel or to be able to later recover a session other than the last one you interrupt.

--status[=NAME] print status of a session [called NAME]

Prints status of an interrupted or running session. Note that on a Unix-like system, you can get a detached running session to update its session file by sending a SIGHUP to the appropriate “john” process; then use this option to read in and display the status.

--make-charset=FILE make a charset, overwriting FILE

Generates a charset file based on character frequencies from $JOHN/john.pot, for use with “incremental” mode. The entire $JOHN/john.pot will be used for the charset generation unless you specify some password files. In that case, only the cracked passwords which correspond to those password files will be used. You can also use an external filter() routine with this option.

--show show cracked passwords

Shows the cracked passwords for given password files (which you must specify). You can use this option while another instance of John is cracking to see what John did so far. To get the most up-to-date information, first send a SIGHUP to the appropriate “john” process.

--test perform a benchmark

This option benchmarks all of the compiled in hashing algorithms and tests them for proper operation.

--users=[-]LOGIN|UID[,..]   [do not] load this (these) user(s)

This option allows you to select just a few accounts for cracking or for other operations. A dash before the list can be used to invert the check. (That is, load information for all the accounts that are not listed.)

--groups=[-]GID[,..]   load users [not] of this (these) group(s)

This option tells John to load (or to not load) information for accounts in the specified group(s) only.

--shells=[-]SHELL[,..]   load users with[out] this (these) shell(s)

This option is useful for loading accounts with a valid shell only or to not load accounts with a bad shell. You can omit the path before a shell name, so "--shells=csh" will match both "/bin/csh" and "/usr/bin/csh", while "--shells=/bin/csh" will only match "/bin/csh".

--salts=[-]COUNT   load salts with[out] at least COUNT passwords

This is a feature which allows you to get better performance in some special cases. For example, you can crack only some salts using "--salts=2" faster and then crack the rest using "--salts=-2". Total cracking time will be about the same, but you will likely get some passwords cracked sooner.

--format=NAME   force ciphertext format NAME

This option allows you to override the hash-type detection. Currently, valid "format names" are DES, BSDI, MD5, BF, AFS, and LM. You can use this option when cracking or with "—test". Note that John can't crack hashes of different types at the same time. If you happen to get a password file which uses more than one hash type (for different accounts), then you have to invoke John once for each hash type, and you need to use this option to make John crack hashes of types other than the one it would autodetect by default.

--save-memory=LEVEL   enable memory saving, at LEVEL 1..3

You might need this option if you don't have enough memory or don't want John to affect other processes too much. Level 1 tells John to not waste memory on login names. It is only supported when a cracking mode other than "single crack" is explicitly requested. The only impact of this is that you won't see the login names while cracking. Higher memory-saving levels have a performance impact. You should probably avoid using them unless John doesn't work or gets into swap.

* For more information on these options, please consult the online documentation for John the Ripper. http://www.openwall.com/john/doc/