

# Pico Computing Inc.



## **Chipper: Password Recovery Program**

**Version 5.0.0.3. Apr 16th, 2010.**

Pico Computing, Inc.  
150 Nickerson, Suite 311  
Seattle, WA, 98109-1634  
(206) 283-2178  
[www.picocomputing.com](http://www.picocomputing.com)

## 1 Overview

This document describes the Pico Chipper application program. This program uses one or more Pico Cards to recover usernames and/or passwords from several different forms of encrypted information. It is also possible to use the PC's core computing power to recover information. The current version handles Bluetooth encryption, WPA encryption, Filevault encryption, WinZip encryption, and WEP encryption.

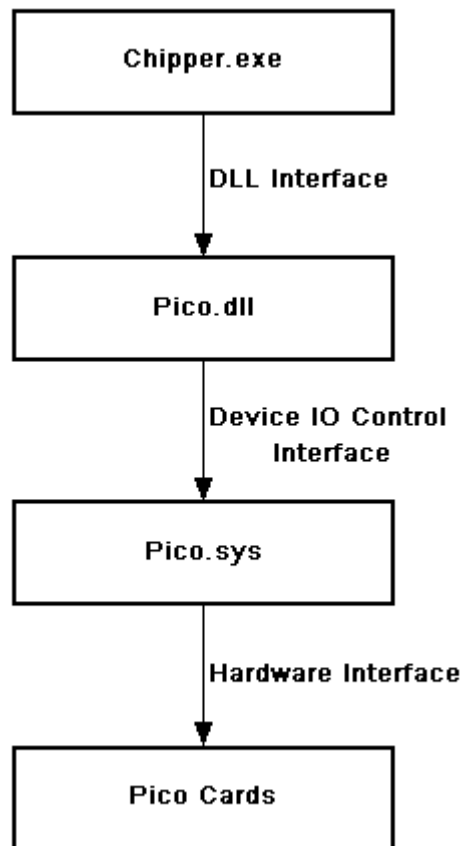
The recovery process works by loading one or more pieces of encrypted information onto the Pico card and then, using specialized firmware in the FPGA on the Pico Card, exhaustively test the possible decrypted values.

Other manuals in this help library are located at [GuideToDocumentation.pdf](#)

NOTE: This link will access the pdf from the PicoComputing.com Website .

## 2 Operation of Chipper

Chipper.exe is a GUI that provides an interface for Pico Computing's supported cryptology algorithms: Bluetooth crack, WPA crack, WEP cracks, FileVault cracks, and WinZip cracks. The cracks can be performed on either the native CPU or on one to multiple Pico Cards.

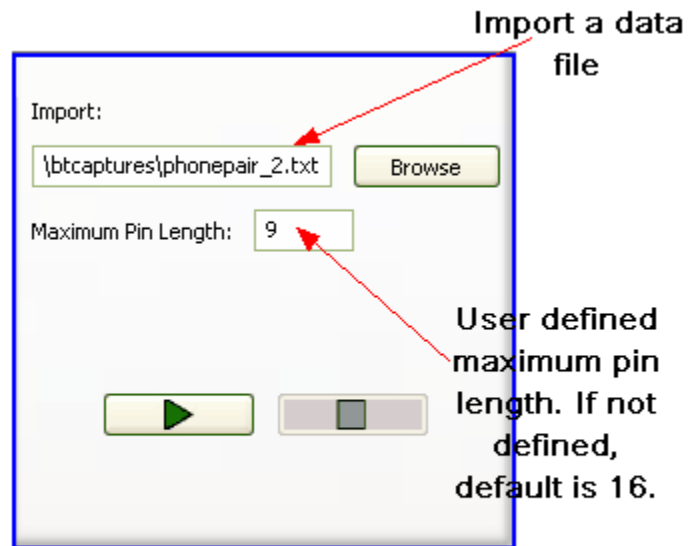


PC Software Flow

## 2.1 Bluetooth Crack

In order to perform a Bluetooth crack, you must first provide the needed information. This can be done two ways:

- 1) Import a data file:



2) Or manually enter required fields:

Status	Data
m_bd_addr:	0002EE6AFF2A
s_bd_addr:	0002EE790B5D
in_addr:	74:ad:c1:8a:e0:a8:b5:7b:5c:23:d2:f0:b5:62:ce:c7
m_comb_key:	15:eb:50:28:5a:9d:f9:3e:27:3d:d9:e5:6b:eb:06:cd
s_comb_key:	5b:b8:84:5b:9b:ff:b9:e1:fe:26:f4:6d:5a:b6:e2:90
m_au_rand:	8f:cb:df:04:39:7b:74:70:b4:d6:7c:0a:ad:c4:3e:2d
s_au_rand:	b0:d2:73:72:83:05:af:5d:77:db:92:0d:a2:61:86:24
m_sres:	a2:ec:89:16
s_sres:	f7:93:d2:88
kab:	
pin:	

**Always manually inserted**

**Results**

**Either imported file information or user defined.**

After providing the desired information, you may also define a maximum pin length. If no pin length is defined, the default length is 16 digits. Then, press "play". The Bluetooth crack will end once it has either found the pin or has reached the maximum pin length. If it is desired to end the crack early, either press "stop" or "pause." If "pause" is pressed, you will be able to restart the crack at a later time. The results will be displayed in the Bluetooth log window as well as in the designated fields in the Bluetooth data tab.

## 2.1.1 Performance

### SAFER+ Core

This core is an implementation of the SAFER+ algorithm that's slightly modified to be compatible with the Bluetooth standard. It includes many optimizations such as using blockrams for the S-Boxes and utilizes the algebraic manipulation described in [Cracking the Bluetooth PIN](#).

### Bluetooth Pin Cracking Core

The Bluetooth pin cracking core implements the basic bluetooth pin cracking attack by generating possible PINs and running them through SAFER+ to verify if they are correct or not. This uses the pipelined implementation of SAFER+ and loops the output of the pipeline back into itself 7 times to perform all of the E21/E22/E1 functions. The max clock speed we've been able to run it at on an E-12 is 75MHz which results in ~10 million PINs per second compared to roughly 40k on a modern CPU.

### btpincrack

Currently btpinckrack has support for cracking PINs on your CPU or by offloading it to a Pico E-12, Pico E-16, or Pico E-101 card. It supports importing Merlin capture files and will soon support importing CSV exports from the Frontline Test Equipment hardware.

Processor	Speed	FPGA	Speed
3300 Sempron	~40,000/sec	Pico E-12 (Virtex-4 LX25)	~10,000,000/sec
2.16GHz Intel Duo	~48,000/sec		

Copyright © 2006 - The OpenCiphers Project <[dhulton@picocomputing.com](mailto:dhulton@picocomputing.com)>

## 2.1.2 Example

Instructions for a sample Bluetooth crack:

1) Import one of the following files:

```
%picobase%\chipper\btcaptures\phonepair_1.txt
%picobase%\chipper\btcaptures\phonepair_2.txt
%picobase%\chipper\btcaptures\phonepair_3.txt
%picobase%\chipper\btcaptures\ppcpair_4.txt
%picobase%\chipper\btcaptures\ppcpair_5.txt
%picobase%\chipper\btcaptures\phonepair_8.txt
```

2) Manually enter the corresponding m\_bd\_addr and s\_bd\_addr found in %picobase%\chipper\btcaptures\CaptureReadme.txt

```

CaptureReadme.txt - Notepad
File Edit Format View Help
Cellphone pair with Cellphone
phonepair_1.txt M: 0002EE6AFF2A S: 0002EE790B5D PIN: 712983
phonepair_2.txt M: 0002EE6AFF2A S: 0002EE790B5D PIN: 61748293
phonepair_3.txt M: 0002EE6AFF2A S: 0002EE790B5D PIN: 218699
phonepair_8.txt M: 0002EE6AFF2A S: 0002EE790B5D PIN: 2860

Cellphone pair with PocketPC
ppcpair_4.txt M: 0002EE6AFF2A S: 0800171CCE21 PIN: 621849
ppcpair_5.txt M: 0002EE6AFF2A S: 0800171CCE21 PIN: 33942810

m_bd_addr
s_bd_addr
correct pin

```

3) If desired, enter a maximum pin length. You can use the known pin solutions in %picobase%\chipper\btcaptures\CaptureReadme.txt as a guide for the maximum pin length to enter.

4) Once cracked, the pin and kab will be displayed both in the log window and in the Bluetooth data tab.

Note: The default crack is an FPGA crack. If a PC crack is desired, see help section "Menu Options."

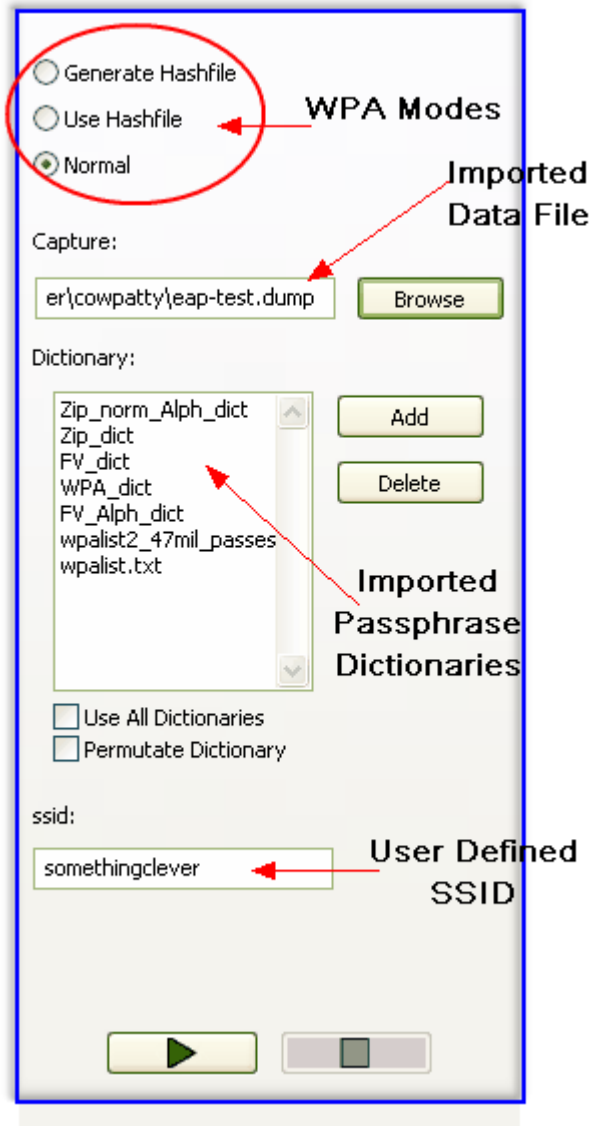
## 2.2 WPA Crack

There are three different modes of operation for the WPA tab:

### Normal Mode:

This mode performs a CoWPAtty crack using user defined capture file dictionary file. This information can be defined in two ways:

1) Import a data file:





**Use Hashfile Mode:**

This mode performs a CoWPAtty crack using a user defined capture file and a hashfile. The required information can be defined in the two ways detailed above. The default mode is FPGA, although the PC is plenty efficient enough to perform this crack. See help section "Menu Options" in order to use the PC.

Generate Hashfile  
 Use Hashfile  
 Normal

**Imported Capture File**

Capture:  
er\cowpatty\jeap-test.dump

Hash File:

hashfile

**Imported Hash File**

Use All Dictionaries  
 Permutate Dictionary

ssid:  
somethingclever

**Generate Hashfile mode:**

This mode allows you to create a hashfile using an input dictionary file and a user defined ssid. It is possible to generate a hashfile using either the FPGA or the PC. See help section "PC Crack" in order to see how to use the PC to generate a hash file.

Generate Hashfile  
 Use Hashfile  
 Normal

**User defined hash file name**

Hash File:

Dictionary:

- Zip\_norm\_Alph\_dict
- Zip\_dict
- FV\_dict
- WPA\_dict
- FV\_Alph\_dict
- wpalist2\_47mil\_passes
- wpalist.txt

**Imported dictionary files**

Use All Dictionaries  
 Permutate Dictionary

ssid:

**User defined SSID**

## 2.2.1 Performance

### SHA-1 Core

This core is a tiny implementation of SHA-1 that is optimized more for size than speed. It requires less than 500 Slices and 4 BlockRAMs and can be clocked up to 120MHz on the Virtex-4 (80 clock cycles are required for valid data). It uses a simple bus interface to write values to it and pull out results. The end goal of this project is to create a full core that is able to accelerate WPA-PSK cracking through hooks into coWPAtty and/or aircrack. The small size should allow us to parallelize multiple instances of the SHA-1 core on an FPGA to multiply the performance.

### WPA-PSK PBKDF2 Core

This is the SHA1 core adapted for doing WPA-PSK cracking. It uses BlockRAMs to buffer the SHA1 input and output values to streamline throughput. It's setup to accomodate larger FPGA designs that can use more SHA1 cores to increase performance.

### coWPAtty

Currently coWPAtty has full support for cracking WPA-PSK on the Pico E-12 and Pico E-16 cards. This project contains the modifications made to coWPAtty and the proper Pico E-12 or Pico E-16 bit file to use FPGA acceleration under Linux 2.4 using the pcmcia-cs memory\_cs driver. The FPGA acceleration provides roughly a 6x speed improvement over a top of the line Intel/AMD processor as shown below:

Processor	Speed	FPGA	Speed
800MHz P3	~25/sec	Pico E-12 (Virtex-4 LX25)	~430/sec
3.6GHz+ P4	~60/sec	Pico E-14 (Virtex-4 FX20)	~380/sec
2.16GHz Intel Duo	~70/sec	Pico E-14 (Virtex-4 FX60)	~1,000/sec

### Precomputed Hashtables

The Shmoo Group has been nice enough to host our WPA tables on their bittorrent tracker located [here](#). If you want to help out, please download and seed the tables to help speed up the download for others.

Copyright © 2006 - The OpenCiphers Project <[dhulton@picocomputing.com](mailto:dhulton@picocomputing.com)>

### 2.2.2 Example

Instructions for sample WPA cracks:

#### Normal

- 1) Select the "normal" radio button.
- 2) Import %picobase%\Chipper\coWPAtty\leap-test.dump as the capture file.
- 3) Add %picobase%\Chipper\coWPAtty\dict to the dictionary list.  
Hint: It may help to rename "%picobase%\Chipper\coWPAtty\dict" to "WPA dictionary" or something similar. All example dictionary files are named "dict."
- 4) Enter "somethingclever" as the ssid.
- 5) Select the dictionary file and hit "play."
- 6) The psk will display in the WPA log window and data tab. **The correct psk is "family movie night."**

#### Use Hashfile

- 1) Select the "Use Hashfile" radio button.
- 2) Import %picobase%\Chipper\coWPAtty\leap-test.dump as the capture file.
- 3) Add %picobase%\Chipper\coWPAtty\hashfile to the hashfile list.
- 4) Enter "somethingclever" as the ssid.
- 5) Select the hashfile and hit "play."
- 6) The psk will display in the WPA log window and data tab. **The correct psk is "family movie night."**

#### Generate Hashfile

- 1) Select the "Generate Hashfile" radio button.
- 2) Enter a hashfile name.  
ex. "MyHashfile"
- 3) If there are no dictionaries imported, import a dictionary. Sample dictionaries included with Chipper are:
  - %picobase%\Chipper\coWPAtty\dict
  - %picobase%\Chipper\vileFault\dict
  - %picobase%\Chipper\winzipcrack\dict
- 4) Select a dictionary.
- 5) Enter an ssid.

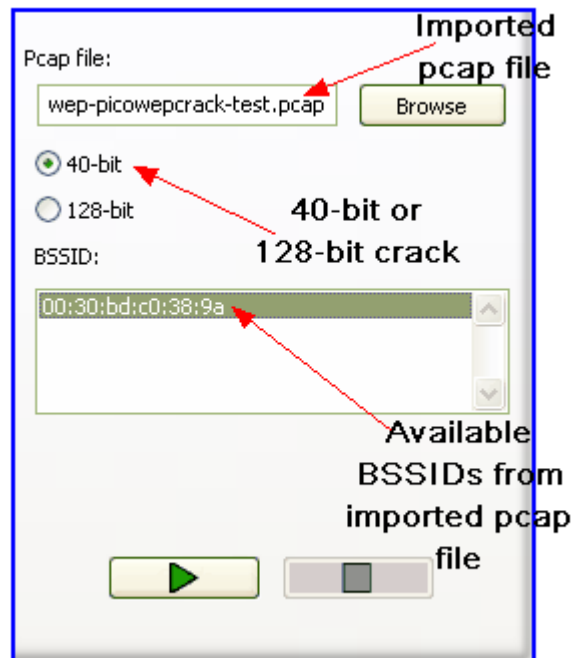
ex. "somethingclever"

6) Click "play." The status tab window will display the words in the dictionary that are being used to generate the hashfile.

7) When complete, the new hashfile will be located in the current directory under the user-defined hashfile name.

## 2.3 WEP Crack

In order to perform a WEP crack, import a pcap file by clicking browse and selecting the desired file. Then, select whether to perform a 40 or 128 bit crack and select the BSSID from the imported pcap file. Finally, press the "play" button. There is no relevant data to be displayed. Therefore, there is only a Status Tab in the WEP tab. The results of the crack will be displayed in the WEP log window.



## 2.3.1 Performance

### Pico-Wepcrack Core

This rc4 core is specifically made to be small and to only compute the first 6 bytes of PRGA. The idea for this core is to have a higher level core that feeds it possible WEP keys and then verifies if the key is correct by seeing if the PRGA ^ packet0 == [the first 6 bytes of the snap header]. The main difference between this core and the previous is that it uses a 16-bit BlockRAM for the S-Box and swaps between using the top 8 bits and the bottom 8 bits for KSA/PRGA and for Initialization, which allows you to skip the Initialization step when running rc4 continuously back-to-back (this is explained a bit better in my LayerOne and RECON presentations). Airbase (jc-wepcrack) currently has basic Pico E-12 and Pico E-16 acceleration support, for more information on Airbase, check out the link below.

- [Airbase](#)

Copyright © 2006 - The OpenCiphers Project <[dhulton@picocomputing.com](mailto:dhulton@picocomputing.com)>

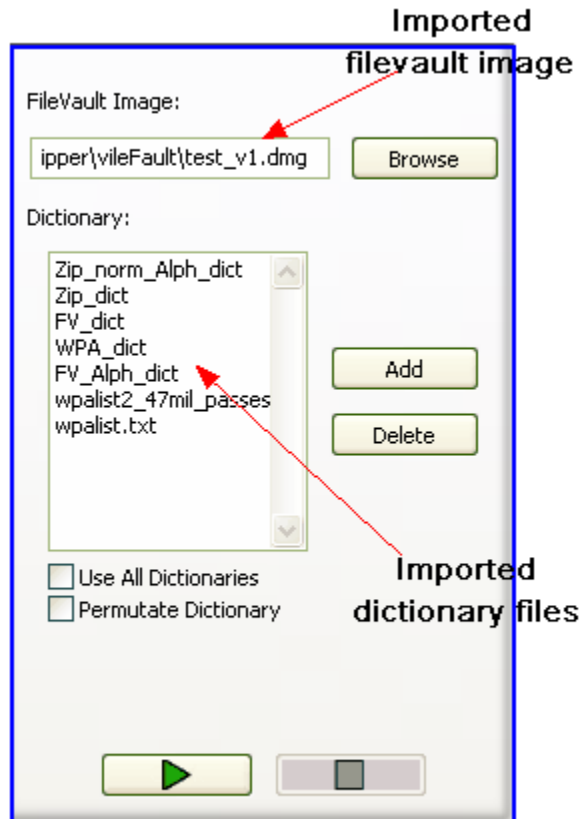
### 2.3.2 Example

Instructions for a sample WEP crack:

- 1) Import %picobase%\chipper\WEP\scripts\40bitwep-picowepcrack-test.pcap
- 2) Select 40-bit crack.
- 3) Select the BSSID "00:30:bd:c0:38:9a"
- 4) Hit "play."
- 5) The key will be displayed in the WEP log window. **The correct key is "00:11:22:33:44"**

## 2.4 FileVault Crack

In order to perform a FileVault crack, import a FileVault image, import and select a dictionary file, and click "play". There is no relevant data to be displayed. Therefore, there is only a Status Tab in the FileVault tab. The results of the crack will be displayed in the FileVault log window.



## 2.4.1 Performance

### FileVault Cracking Core

This core is actually just a modification of the WPA-PSK cracking core since filevault uses PBKDF2 to do its password hashing. All that we did was change the iteration count from 4096 to 1000. Because of the lower iteration count, vfcrack will crack hashes roughly 4x faster than cowpatty and have roughly the same speed improvement over cracking on a CPU.

### vfcrack

Currently vfcrack has support for cracking on your CPU or using a Pico E-12 card or Pico E-16 card. All you need to use vfcrack is the dmg file and a list of passwords you want to try. Typically a laptop will get around 320 passphrases per second and an E-12 or E-16 will get around 1800 per second.

Processor	Speed	FPGA	Speed
3300 Sempron	~320/sec	Pico E-12 (Virtex-4 LX25)	~1,800/sec
2.16GHz Intel Duo	~350/sec		

Copyright © 2006 - The OpenCiphers Project <[dhulton@picocomputing.com](mailto:dhulton@picocomputing.com)>

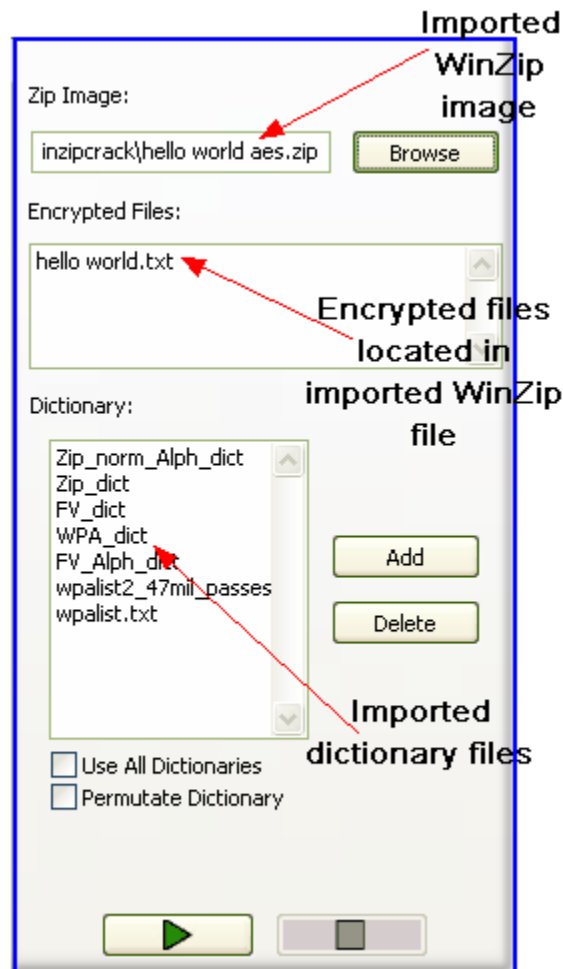
## 2.4.2 Example

Instructions for a sample FileVault crack:

- 1) Import %picobase%\Chipper\vileFault\test\_v1.dmg.
- 2) Add %picobase%\Chipper\vileFault\dict to the dictionary list.  
Hint: It may help to rename "%picobase%\Chipper\vileFault\dict" to "FV dictionary" or something similar. All example dictionary files are named "dict."
- 3) Select the dictionary and hit "play."
- 4) The passphrase will be displayed in the FileVault log window. **The correct passphrase is "123456."**

## 2.5 WinZip Crack

In order to perform a WinZip crack, first import a WinZip image. If there are encrypted files in this image, the file names will appear in the box entitled "Encrypted Files." Select an encrypted file to crack, import and select a dictionary file, and click "play". There is no relevant data to be displayed. Therefore, there is only a Status Tab in the WinZip tab. The results of the crack will be displayed in the WinZip log window.



## 2.5.1 Performance

### WinZip AES Cracking Core

This core is actually just a modification of the WPA-PSK cracking core since WinZip uses PBKDF2 to do its password hashing. All that we did was change the iteration count from 4096 to 1000. Because of the lower iteration count, winzipcrack will crack hashes roughly 4x faster than cowpatty and have roughly the same speed improvement over cracking on a CPU.

### winzipcrack

Currently winzipcrack has support for cracking on your CPU or using a Pico E-12 or Pico E-16 card. All you need to use winzipcrack is the zip file, the name of the encrypted file in the zip file, and a list of passwords you want to try. Typically a laptop will get around 320 passphrases per second and a E-12 or E-16 will get around 1800 per second.

Processor	Speed	FPGA	Speed
3300 Sempron	~320/sec	Pico E-12 (Virtex-4 LX25)	~1,800/sec
2.16GHz Intel Duo	~350/sec		

Copyright © 2006 - The OpenCiphers Project <[dhulton@picocomputing.com](mailto:dhulton@picocomputing.com)>

## 2.5.2 Example

Instructions for a sample WinZip crack:

1) Import one of the following winzip files:

```
%picobase%\Chipper\winzipcrack\hello world aes256.zip
%picobase%\Chipper\winzipcrack\hello world aes.zip
%picobase%\Chipper\winzipcrack\hello world blah.zip
%picobase%\Chipper\winzipcrack\hello world bob aes.zip
%picobase%\Chipper\winzipcrack\hello world bob.zip
%picobase%\Chipper\winzipcrack\hello world.zip
```

2) Depending on the winzip file that is imported, the following encrypted files should appear:

```
hello world aes256.zip
    hello world.txt
hello world aes.zip
    hello world.txt
hello world blah.zip
    There are no encrypted files in this winzip file.
hello world bob aes.zip
    hello bob.txt
    hello world.txt
hello world bob.zip
    There are no encrypted files in this winzip file.
hello world.zip
    There are no encrypted files in this winzip file.
```

3) Add %picobase%\Chipper\winzipcrack\dict to the dictionary list.

Hint: It may help to rename "%picobase%\Chipper\winzipcrack\dict" to "Zip dictionary" or something similar. All example dictionary files are named "dict."

4) Select the dictionary and an encrypted file and hit "play."

5) The password will be displayed in the Zip log window. **The correct password for all encrypted files is "test."**

## 2.6 Status Window

The status window displays the information for all current cracks. The status window is accessible from any of the algorithm tabs.

**Multi-card FPGA**

	Start	Stop	Current	Algorithm
1	00:00:00:00:00	00:c0:00:00:00	00:04:72:24:b0	WEP
2	NULL	9999999999999999	04098150	Bluetooth

**PC Crack**

	Start	Stop	Current	Algorithm
PC	0	30202	12400: console	FileVault
PC	0	10204	600: affectation	WPA
PC				WinZip

Numerically where the crack starts
Numerically where the crack ends
Current passphrase attempt
Currently active algorithm

Single card support:

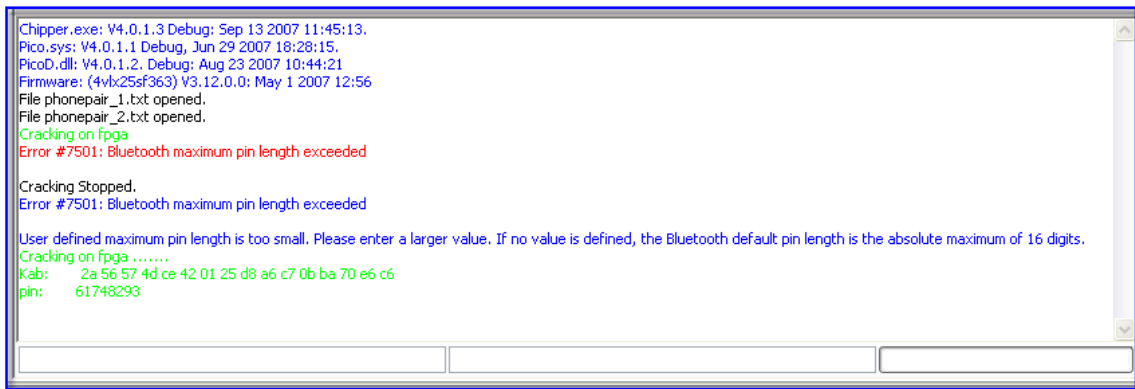
All frames in this window are predetermined by the software. While on a specific algorithm tab, it is only possible to start a crack using that algorithm. Although only one PC crack per algorithm is possible, there are a reasonably unlimited number of possible PC cracks available. See the "Menu Options" section for help on how to perform a PC crack. There is only one FPGA crack available due to the fact that there is only one FPGA available to perform a crack on. Without any cards in the system, it is only possible to perform PC cracks.

Multi-card support:

With multi-card support, it is possible to specify an algorithm for each card. It is also possible to use multiple cards to perform a single crack. With this function, Chipper automatically parallelizes the algorithm based on the number of cards allocated for the attack. This feature is available for our supercluster product line.

## 2.7 Log Window

The log window displays relevant Chipper text:



```

Chipper.exe: V4.0.1.3 Debug: Sep 13 2007 11:45:13.
Pico.sys: V4.0.1.1 Debug: Jun 29 2007 18:28:15.
Pico.dll: V4.0.1.2. Debug: Aug 23 2007 10:44:21
Firmware: (4vbx25sf363) V3.12.0.0: May 1 2007 12:56
File phonepair_1.txt opened.
File phonepair_2.txt opened.
Cracking on fpga
Error #7501: Bluetooth maximum pin length exceeded

Cracking Stopped.
Error #7501: Bluetooth maximum pin length exceeded

User defined maximum pin length is too small. Please enter a larger value. If no value is defined, the Bluetooth default pin length is the absolute maximum of 16 digits.
Cracking on fpga .....
Kab: 2a 56 57 4d ce 42 01 25 d8 a6 c7 0b ba 70 e6 c6
pin: 61748293
  
```

### Color Code:

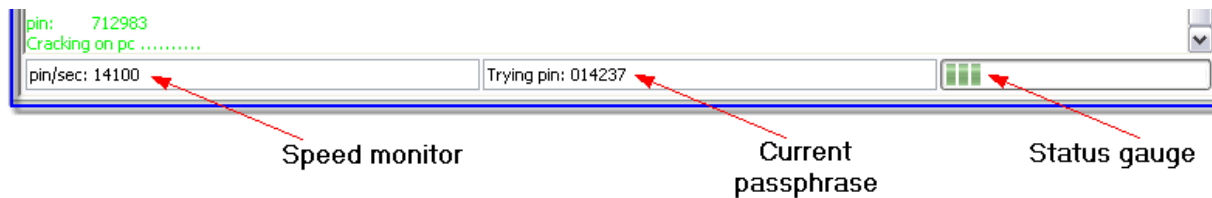
**Blue:** Globally relevant information. This text is displayed in all log windows.

**Black:** Specific algorithm information. This text generally pairs with user initiated actions. It is only displayed in the relevant algorithm log windows.

**Green:** Algorithm generated text. This text will display relevant information during a crack. It is only displayed in the relevant algorithm log windows.

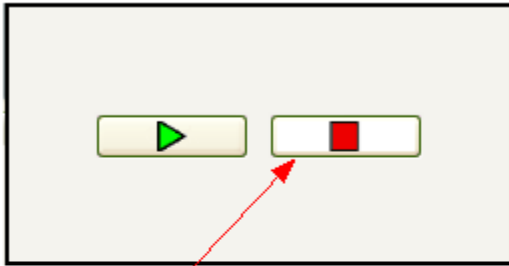
**Red:** Error information. This text displays any error code from Chipper. This text is displayed in any relevant algorithm log windows.

The status fields along the bottom of the log window also display relevant information. This information is only displayed in the relevant algorithm tabs:



## 2.8 Restarting a Crack

It is possible to restart a crack once it has been paused. The crack will pause if either 1) you select pause during a crack or 2) Chipper crashes during a crack. If a crack is paused, you will see the following things in the Chipper window:



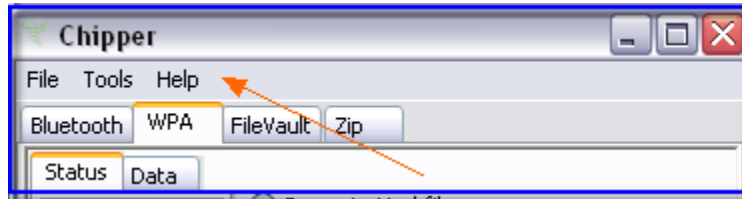
When paused,  
the stop button  
will be enabled.



In order to restart the crack, simply press "play." If you do not want to restart the crack and would rather delete the pause memory, simply press "stop."

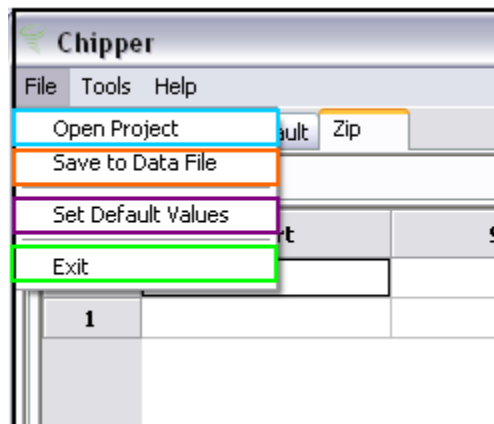
## 2.9 Menu Options

Details on each of the menu options.



### 2.9.1 File Menu

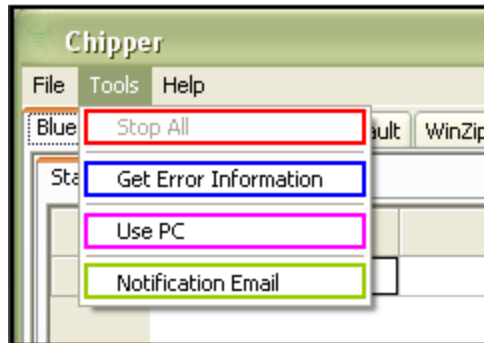
#### File Menu



- Open Project:** Opens a saved project file
- Save to Data File:** Save all relevant values from the current Chipper crack to a user-defined file.
- Set Default Values:** Sets all relevant filed values from the current Chipper frame to default values. These values will continue to be the default values for Chipper until manually changed to something new.
- Exit:** Exit Chipper

## 2.9.2 Tools Menu

### Tools Menu



**Stop All:**

Stop all the currently active cracks

**Get Error Information:**

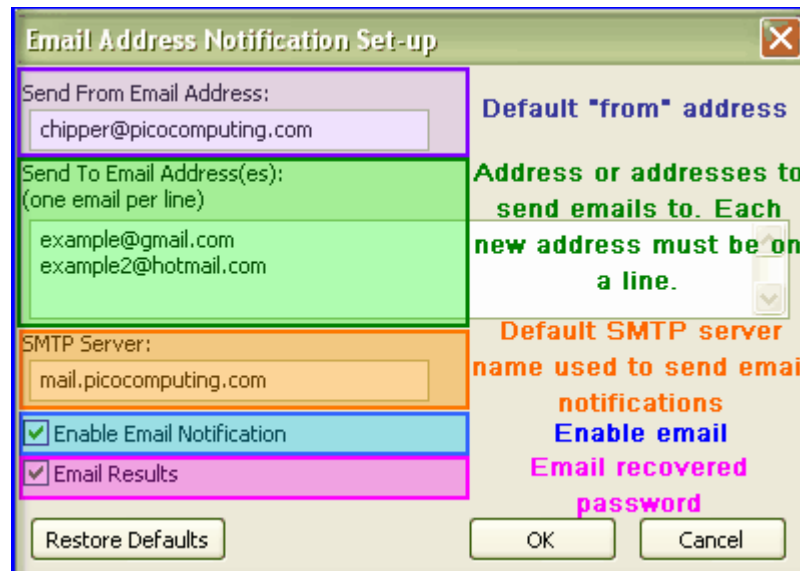
Get more detailed information on any error number

**Use PC:**

Use the PC processor(s) for cracks instead of the Pico FPGA. This mode is default if there are no FPGAs located in the system. When in this mode, all cracks, regardless of the tab, will be performed on the PC. Once the temporary mode of PC is selected, all cracks must be finished on the PC in order to return to FPGA mode. In order to return to FPGA mode, select "Use PC" again.

**Notification Email:**

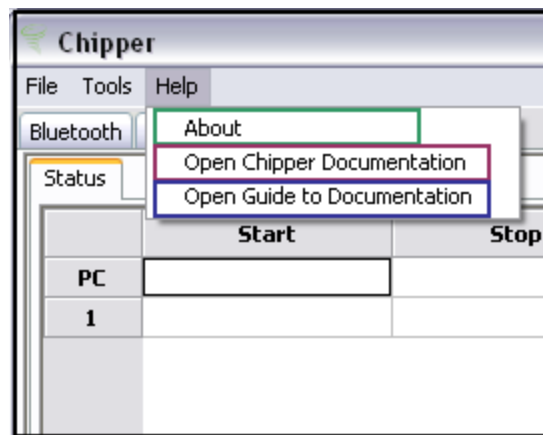
Displays the following menu:



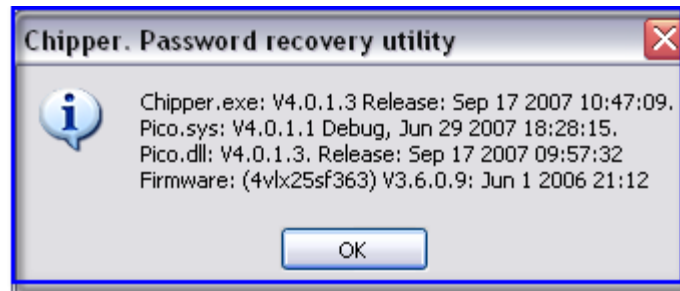
These values are saved as default once entered. Chipper will hold your defined values until redefined.

## 2.9.3 Help Menu

### Help Menu



**About:** Displays the screen below:



**Open Chipper Documentation:** Opens this documentation guide.

**Open Guide to Documentation:** Opens the guide for all Pico documentation.

### 3 Files required by Chipper

**Chipper.exe will be installed by the Pico Installer in the Pico\bin directory, as will the following files:**

• Pico.dll	The interface to the Pico Card(s) loaded by Chipper.exe
• E12LX25-BTPinCrack.bit	This file is used for the Bluetooth E12 crack
• E16LX50-BTPinCrack.bit	This file is used for the Bluetooth E16 crack
• E101-BTPinCrack.bit	This file is used for the Bluetooth E101 crack
• E12LX25-CoWPAtty.bit	This file is used for the WPA E12 crack
• E16LX50-CoWPAtty.bit	This file is used for the WPA E16 crack
• E12LX25-RC4.bit	This file is used for the WEP E12 crack
• E16LX50-RC4.bit	This file is used for the WEP E16 crack
• E12LX25-VileFault.bit	This file is used for the FileVault E12 crack
• E16LX50-VileFault.bit	This file is used for the FileVault E16 crack
• E12LX25-WinZip.bit	This file is used for the WinZip E12 crack
• E16LX50-WinZip.bit	This file is used for the WinZip E16 crack

NOTE: The bit files are normally shipped on the flash ROM of the FPGA and/or in Pico\bin. If the desired .bit image does not exist on the ROM of the FPGA, Chipper will write the file from Pico\bin to the flash ROM.

#### Data Files shipped with Chipper include:

• btcaptures\phonepair_1.txt	Bluetooth example file
• btcaptures\phonepair_2.txt	Bluetooth example file
• btcaptures\phonepair_3.txt	Bluetooth example file
• btcaptures\ppcpair_4.txt	Bluetooth example file
• btcaptures\ppcpair_5.txt	Bluetooth example file
• btcaptures\phonepair_8.txt	Bluetooth example file
• btcaptures\CaptureReadme.txt	Bluetooth example file
• cowpatty\dict	WPA example file
• cowpatty\hashfile	WPA example file
• cowpatty\leap-test.dump	WPA example file
• cowpatty\wpapsk-linksyp.dump	WPA example file
• WEP\scripts\40bitwep-picowepcrack-test.pcap	WEP example file
• vileFault\dict	FileVault example file
• vileFault\test_v1.dmg	FileVault example file
• winzipcrack\dict	WinZip example file
• winzipcrack\hello world aes256.zip	WinZip example file
• winzipcrack\hello world aes.zip	WinZip example file
• winzipcrack\hello world blah.zip	WinZip example file
• winzipcrack\hello world bob aes.zip	WinZip example file
• winzipcrack\hello world bob.zip	WinZip example file
• winzipcrack\hello world.zip	WinZip example file

NOTE: The data files are normally shipped in Pico\Chipper.

## 4 Further Information

Other information is available from the following Websites:

- [Pico Computing](#)
- [Openciphers Project](#) Link to most recent performance information
- [OpenWall Windows Password Recovery Tools](#)

For your convenience we have included the following PPT:

- [Slides delivered to Microsoft 8/19/2005](#)