

User's guide

KeyCarbon PCI Card



TRADEMARKS

Copyright © BitForensics, Inc., 2000-2007. All rights reserved.

Linux is a registered trademark of Linus Torvalds.

OS/2 is a registered trademark of IBM Corporation.

UNIX is a registered trademark of The Open Group.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

END-USER LICENSE AGREEMENT

The KeyCarbon PCI Card (the hardware) is Copyright © BitForensics, Inc., 1999-2007. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the hardware only, subject to the following restrictions and limitations.

1. The original purchaser may use the hardware on a single computer owned or leased by the original purchaser.
2. The original purchaser may not engage in, nor permit third parties to engage in, any of the following:
 - ▷ Making alterations of any kind in the hardware (except as specifically permitted above).
 - ▷ Attempting to un-assemble, de-compile or reverse engineer the hardware in any way.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE HARDWARE IS WITH YOU THE PURCHASER. BITFORENSICS DOES NOT WARRANT THAT THE HARDWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE HARDWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED. NO LIABILITY FOR CONSEQUENTIAL DAMAGES — IN NO EVENT SHALL BITFORENSICS OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF BITFORENSICS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Introduction

What is the KeyCarbon PCI card?

The KeyCarbon PCI device is a hardware device that can record all typing, and serial port data, on your computer.

The KeyCarbon PCI device fits inside the computer, and is plugged into the PCI slot of a computer motherboard.

The device can be installed in less than 10 seconds.

The device is safe from removal or tampering by a third party as the device can be locked inside the case of the computer.

Once fitted to the machine, every keystroke typed is recorded in onboard memory card, in an encrypted file.

The card is 100% passive, and 100% undetectable by software running on the machine. The card requires no drivers.

Capabilities of the KeyCarbon PCI card:

- ▷ Record typing from a PS/2 keyboard.
- ▷ Record typing from a USB keyboard.
- ▷ Record RS232 serial port data from the motherboard.
- ▷ Create an encrypted audit trail suitable for use in a court of law.
- ▷ The built-in SD card can be removed, and the keystrokes decoded on another computer.

Hardware Features of the KeyCarbon PCI card:

- ▷ 100% invisible to software running on the host PC.
- ▷ 100% passive.
- ▷ No drivers required - just plug and record.
- ▷ Device can be hot-plugged, while the PC is still running.
- ▷ Prevent tampering by locking the card inside the computer.

Why is it Necessary to Record Typing on a Computer?

The KeyCarbon PCI is a complete solution to create an audit trail on a standard computer.

The following capabilities of the KeyCarbon PCI device ensure the creation of a secure audit trail:

- ▷ Recording of all keystrokes and typing on a standard PC.
- ▷ Tamper resistant – device can be either locked inside the computer case or secured with tamper resistant tape.
- ▷ Compatible with all keyboards including PS/2 and USB keyboards.
- ▷ Recording of all RS232 serial data on a standard PC.
- ▷ Encryption of log contents in a virtual tamper resistant vault (requires firmware upgrade; available 2007Q2).
- ▷ Date/time stamping of recorded keystrokes.

System Requirements

The minimum system requirements for the KeyCarbon PCI device are:

- ▷ A computer with a Pentium CPU or equivalent.
- ▷ A free PCI slot on the computer motherboard.
- ▷ Any OS (operating system) including:
 - Windows™ (all versions).
 - Linux (all versions).
 - OS/2™ (all versions).
 - DOS (all versions).
 - BeOS (all versions).
 - Any other operating system that runs on a PC with a Pentium CPU or equivalent.

How to Install the KeyCarbon PCI Card

Installing the KeyCarbon PCI card is exactly the same as installing any standard PCI card such as a PCI modem, or a PCI Ethernet card.

There are two methods to install the card:

1. Cold-Plugging allows you to install the card while the computer is **switched off**.
2. Hot-Plugging allows you to install the card while the computer is **switched on**, and powered up.

Installing - Cold Plugging

To install the KeyCarbon PCI card with the computer powered off (the “cold-plugging” method):

1. Power down the computer.
2. Open the case of the computer.
3. Locate a spare PCI slot on the computer motherboard.
4. Remove the KeyCarbon PCI card from its static protection bag.
5. Ensure that there is an SD memory card installed in the SD slot on the KeyCarbon PCI card.
The SD memory card is needed for the KeyCarbon PCI card to store its captured data.
6. Plug the KeyCarbon PCI card into a spare PCI slot on the computer motherboard.
7. Power up the computer.

The KeyCarbon PCI card will immediately start to capture keystrokes and RS232 serial data.

You can remove the SD card and read the captured data at any time.

Installing - Hot plugging

To install the KeyCarbon PCI card with the computer powered on (the “hot-plugging” method):

1. Power up the computer.
2. Open the case of the computer.

3. Locate a spare PCI slot on the computer motherboard.
4. Remove the KeyCarbon PCI card from its static protection bag.
5. Ensure that there is an SD memory card installed in the SD slot on the KeyCarbon PCI card. The SD memory card is needed for the KeyCarbon PCI card to store its captured data.

Warning: Failure to follow the next step (“Power up the card”) may result in the computer experiencing an automatic reboot when the PCI card is inserted. This will not harm the PC.

6. Power up the card by either connecting the power supply connector to the KeyCarbon PCI card, or connecting a USB cable to the card.
7. Plug the KeyCarbon PCI card into a spare PCI slot on the computer motherboard.
8. The KeyCarbon PCI card will immediately start to capture keystrokes and RS232 serial data. You can remove the SD card, and read the captured data, at any time.

Difference Between PS/2 and USB Keyboards

There are two different types of keyboards - PS/2 keyboards (round plug) and USB keyboards (square plug). For the difference between these two types of keyboards, see:

http://www.keycarbon.com/wiki/keyboards_ps2_vs_usb/.

As PS/2 keyboards and USB keyboards communicate with the computer using different protocols, two separate methods of recording the keystrokes are required.

Capturing Keystrokes from a PS/2 Keyboard

The card records any keystrokes from a PS/2 keyboard automatically. It does this by looking at stray signals on the PCI bus.

All captured keystrokes are written to a file on the SD card.

You can tell if PS/2 keystrokes are being recorded if the LED labelled “D100” flashes each time you press a key on the PS/2 keyboard.

Capturing Keystrokes from a USB Keyboard

The card records keystrokes from a USB keyboard via a tap wire. This tap wire records signals from the USB plug on the computer motherboard.

Before USB keystrokes can be recorded with the unit, the signals from the USB keyboard must be run from the motherboard into the D+ and D- ports on the PCI card.

There are two USB recording channels available, up to two USB ports can be monitored simultaneously for keystrokes. These keystrokes are written to a file on the SD card.

To attach the tap wire, use the alligator clips to connect the D- signal on the PCI card to the D- signal of the USB plug on the motherboard. Similarly, connect the D+ signal on the PCI card to the D+ signal on the USB plug of the motherboard. The D+ and D- pins are paired, run one keyboard

into the left hand pair, and one keyboard into the right hand pair.

You can tell if USB keystrokes are being recorded if the LED labelled “D101” flashes as you press keys on the USB keyboard.

The USB recording is compatible with USB 2.0, low speed (1.1MBit/sec) and high speed (12Mbit/sec).

Viewing the Log

The file “datafile.klr” contains all data recorded by the KeyCarbon PCI card.

The file “datafile.klr” is located on the SD memory card which is inserted into a slot on the KeyCarbon PCI card.

The file “datafile.klr” can be decoded using the “KeyCarbon PCI Windows Utility” available from:

http://www.keycarbon.com/products/keycarbon_pci/software/.

To view the log:

1. Download the “KeyCarbon PCI Windows Utility” from.:
http://www.keycarbon.com/products/keycarbon_pci/software/.
2. Install this utility.
3. Copy the file “datafile.klr” from the SD card, in the KeyCarbon PCI card, to your desktop.
4. Select “File..Import” from the “KeyCarbon PCI Windows Utility”.
5. Select the file “datafile.klr” from the desktop.
6. The keystrokes will be displayed within the utility.

Configuring the Card

You may configure the card by altering the file “config.ini” on the SD card.

This file “config.ini” is automatically created by the KeyCarbon PCI device, if the file does not exist on the SD card.

There are four reasons to alter or delete the file “config.ini”:

1. Altering the date/time in the KeyCarbon PCI device, used to timestamp the log.
2. Altering the encryption key (available after 2007Q2 with a free firmware upgrade from www.keycarbon.com).
3. Altering the I/O port that the card records from.
4. Regenerating the “config.ini” file if it is corrupt.

Configuring the Card – Altering the Date/Time

The log of keystrokes is stamped with the date and time. The KeyCarbon PCI card contains a Real Time Clock (RTC) powered by an onboard battery. To alter the timestamp, follow the steps below:

1. Open the file “config.ini” on the SD card.

2. Edit the current date and time under the section “date”. The format is YYYYMMDD-HHMM format where YYYY is year, MM is month, DD is day, HH is hour (24 hour format) and MM is minute. The seconds cannot be specified.
3. Save the file “config.ini” to the SD card.
4. Remove, then reinsert the SD card on the KeyCarbon PCI device. The KeyCarbon PCI device will update its internal clock with the new date and time.
5. Open the file “applog.txt” on the SD card. This file contains a log of activity on the KeyCarbon PCI card. Check the last line in this file; the last line will indicate that the device has updated its internal Real Time Clock (RTC) with the new date and time. If the KeyCarbon PCI device could not recognize the time format, it will write an error into the log.

Configuring the Card – Altering Your Encryption Key

The configuration file can be altered to specify a password. This password is used to protect sensitive data written to the SD card.

This feature is available with a free firmware upgrade from <http://www.keycarbon.com/> in 2007Q2.

Altering the I/O Port that the Card Records From

The “config.ini” file can be altered so that the card records from an alternate I/O port on the computer.

Ring technical support if you wish to configure the card for a different I/O port.

Configuring the Card – Regenerating the “config.ini” File

You may force the card to regenerate the “config.ini” file, by deleting the “config.ini” file from the SD card, then removing/reinserting the SD card from the KeyCarbon PCI device.

This technique is useful, if the file “config.ini” is edited badly, so that “applog.txt” records “cannot read config.ini” errors.

Upgrading Your Firmware

From time to time, BitForensics will provide free firmware upgrades that are downloadable from our website.

These firmware upgrades allow you to take advantage of product improvements, and new features, that were introduced after you purchased your device.

From time to time it may be necessary to upgrade the “firmware” or operating system on the card.

Upgrading the firmware allows enhancements, new features, and bug fixes to be added to the card.

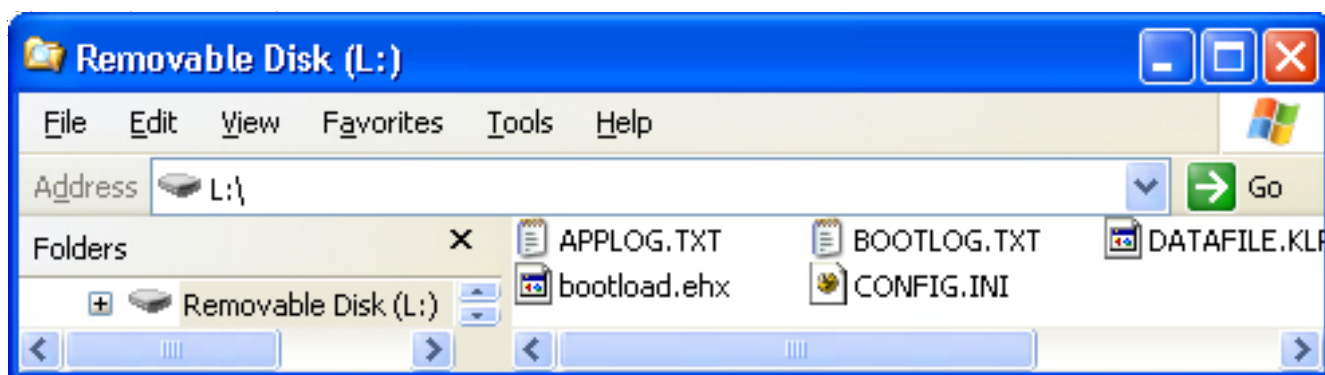
There are two methods to upgrade the firmware on the card:

1. The recommended method is to use the built-in SD card mass storage device on the KeyCarbon PCI card (see method 1).
2. Use a 3rd party SD card reader (see method 2). We recommend this method if you already own

an SD card reader.

Method 1 – Firmware Upgrade via Mass Storage

1. Download the latest firmware upgrade file from: http://www.keycarbon.com/products/keycarbon_pci/firmware/. This will be named “KeyCarbon PCI Firmware Upgrade vX.NN.zip” where vX.NN is the firmware version.
2. Use WinZip to extract the file “bootload.ehx” onto your desktop or another temporary directory on your hard drive.
3. Plug the small end of the supplied USB cable into the USB port on the KeyCarbon PCI card.
4. Plug the other end of the supplied USB cable into a free USB slot on your computer. If you are using Windows™ a dialog box similar to picture below will pop up allowing you to browse the

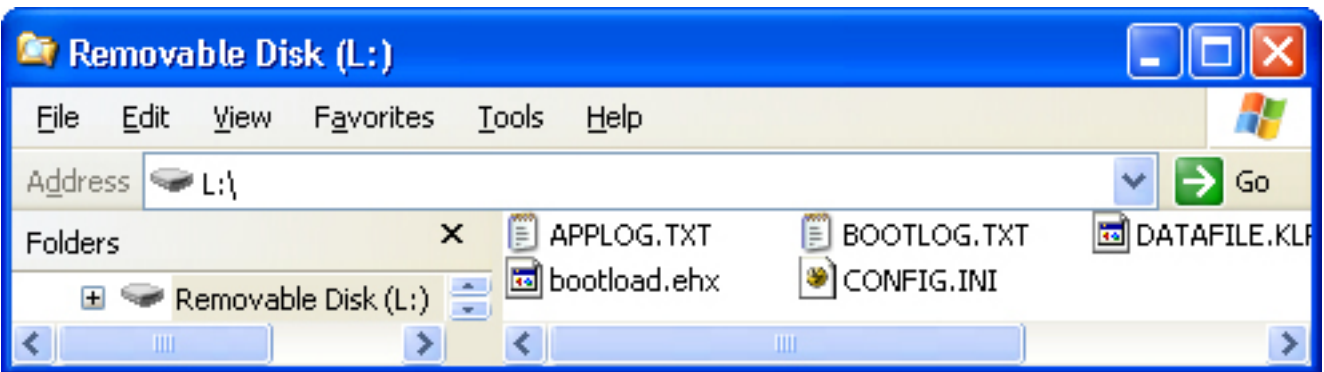


5. Copy the file “bootload.ehx” to the base directory of your SD card, as shown in the dialog box above.
6. Unplug the small end of the USB cable from the KeyCarbon PCI card. Wait 20 seconds then examine the file “bootlog.txt” in the base directory of the SD card. The file “bootlog.txt” contains a log of the bootload procedure. The last line in the file will read “[200x-xx:xx: Bootload: Info: Updated application to vX.NN]” where x-xx:xx is the date and time, and vX.NN is the firmware version. This firmware version must match the firmware version from step 1. This indicates that the firmware upgrade was successful.

Method 2 – Firmware Upgrade via a SD memory card reader:

To upgrade the firmware on the card:

1. Download the latest firmware upgrade file, from http://www.keycarbon.com/products/keycarbon_pci/firmware/. This will be named “KeyCarbon PCI Firmware Upgrade vX.NN.zip” where vX.NN is the firmware version.
2. Remove the SD card from the KeyCarbon PCI device.
3. Plug the SD card into a 3rd party SD card reader (not supplied).
4. If you are using Windows™ a dialog box similar to the picture below will appear. You can now browse the files on the SD card.



5. Copy the file “bootload.ehx” to the base directory of the SD card, as shown in the dialog box above.
6. Remove the SD card from the SD card reader, and insert it back into the KeyCarbon PCI device.
7. Apply power to the KeyCarbon PCI device. Plug the small end of the USB cable into the USB port on the KeyCarbon PCI card. Plug the other end into a free USB slot on the computer.
8. Wait 20 seconds.
9. The firmware upgrade is now complete.
10. Examine the file “bootlog.txt”, in the base directory of the SD card. The file “bootlog.txt” contains a log of the bootload procedure. The last line in the file should read “[200x-xx:xx: Bootload: Info: Updated application to vX.NN]”.

Appendix A - Definition of Terms

SD memory card – What is a Secure Digital (SD) memory card?

A Secure Digital (SD) memory card is a card used to store the captured data, on the KeyCarbon PCI card.

SD memory cards are used for storing data on many digital cameras, cellphones, and other devices that store data.

See <http://www.sdcard.org/>.

PCI slot – What is the PCI slot on a computer motherboard?

The PCI slot is used to add expansion cards to a computer.

KeyCarbon PCI – What is the KeyCarbon PCI card?

The KeyCarbon PCI card is a PCI card that captures keystrokes and RS232 serial data, from the motherboard of a standard IBM compatible computer.

The KeyCarbon PCI card fits inside the PC.

PCI Modem – What is a PCI Modem?

A PCI Modem is a device that plugs into a computer motherboard. The PCI modem allows one to dial up to a server to gain internet access.

USB Port – What is a USB port?

A USB port is the plug on the back of a computer that peripherals such as keyboards, SD card readers, and digital cameras are plugged into. See <http://www.usb.org/>.

PS/2 Keyboard – What is a PS/2 Keyboard?

A PS/2 keyboard is the older style of keyboard.

You can identify a USB keyboard, by looking at the plug on the end.

The plug is round.

USB Keyboard – What is a USB Keyboard?

A USB keyboard is the modern style of keyboard.

You can identify a USB keyboard, by looking at the plug on the end.

The plug is rectangular, see <http://www.usb.org/>.

USB Cable – What is a USB cable?

A USB cable is a cable used to transfer data between a computer and its peripheral.

See <http://www.usb.org/>.

5.25” Power Supply Connector – What is it?

This is the standard power supply connector used to power a 5.25” hard drive inside a computer.

PCI Card – What is a PCI Card?

A PCI card plugs into the motherboard of a computer, to add additional capabilities of the computer. For an example of a PCI card, see PCI Modem.

Firmware – What Exactly Is Firmware?

The word “firmware” means the same as the word “software”. Firmware is the computer program, or Operating System, that runs on an electronic device with a microcontroller.

For more information on firmware, see:

<http://en.wikipedia.org/wiki/Firmware/>

Firmware Upgrade – What Exactly Is A Firmware Upgrade?

The process of upgrading the firmware in a consumer device; for more information see:
http://en.wikipedia.org/wiki/Firmware_upgrade/

SD Card Reader – What is a Secure Digital (SD) Card Reader?

An external Secure Digital (SD) card reader can be used to read or write the files on a SD memory card.

An SD card reader plugs into the USB port of a computer.

Many laptop computers can read SD cards, via the built-in SD slot on the side.

An example of a SanDisk SD card reader is shown below.



Technical Support

Users who have purchased this product will receive free e-mail, fax, and phone technical support from BitForensics. If you have problems installing or using the system that you cannot resolve with the help of this guide and readme file please contact technical support.

Support URL: <http://www.keycarbon.com/support/>

E-mail: support@keycarbon.com.

Phone: see website.