User's Guide

KeyGrabber Forensic Keylogger

Check http://www.keelog.com/ for the latest version of this document.

Table of contents

Getting started

Already familiar with KeyGrabber keyloggers?

⇒ Start key-logging in 2 simple steps: section **Quick start**

New to KeyGrabber hardware keyloggers?

⇒ Learn about keystroke recording first: section **Recording keystrokes**
⇒ Then learn to retrieve the recorded data: section **Viewing recorded data**

Questions or problems?

⇒ Go through the **Troubleshooting** section.

Introduction

About the product

The *KeyGrabber Forensic Keylogger* is an advanced USB hardware keylogger with a huge internal flash disk, organized as a file system. Text data typed on the USB keyboard will be captured and stored on the internal flash drive in a special file. This data may be retrieved on any other computer with a USB port and keyboard, by switching to flash drive mode. The keylogger will pop up as a removable drive, giving instant access to all captured data. The *KeyGrabber Forensic Keylogger* is 100% transparent for computer operation and no software or drivers are required.

Features

- High-capacity internal flash memory, accessible as a USB removable drive
- Compatible with all USB keyboards (including Linux & Mac)
- Ultra fast memory contents retrieve via USB port
- Transparent to computer operation, undetectable for security scanners
- No software or drivers required, operating system independent
- Memory protected with strong 128-bit encryption
- Quick and easy national keyboard layout support
- Ultra-compact and discreet

Requirements

- Computer with standard USB 1.1, 2.0 or 3.0 port
- USB HID-compliant keyboard
- Operating system with USB Mass-Storage device support

Applications

Employers:

- Monitor acceptable internet usage
- Monitor employee productivity
- Detect unauthorized access attempts
- Backup typed text
- Collect computer usage statistics

Parents:

- Monitor your family's computer activity
- Protect your child from on-line hazards and predators
- Observe WWW, E-mail, and chat usage
- Save a copy of written documents

Investigators:

- Monitor remote computers
- Retrieve unknown passwords, operating system independent
- Collect computer-related evidence
- Detect unauthorized use of computer equipment

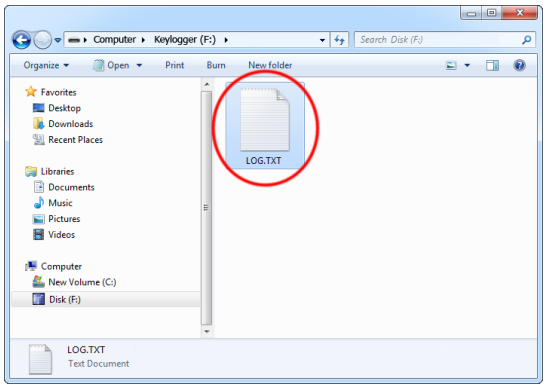
Quick start

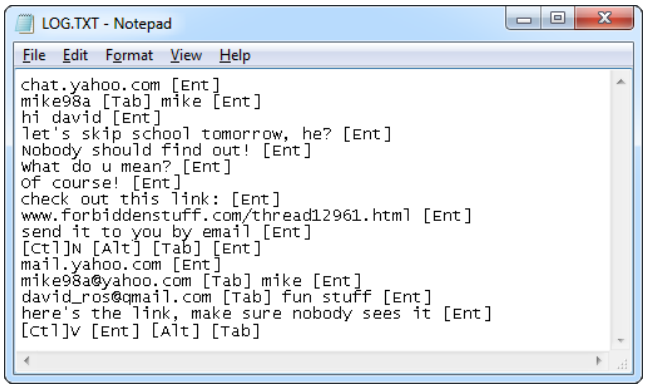
This section contains concise information on basic keylogger handling. If you need detailed instructions, please refer to sections **Recording keystrokes** and **Viewing recorded data**.

To record keystrokes, plug the device in-between the keyboard and USB port.

To view recorded data, plug the device in-between the keyboard and USB port, and press the 3-key combination **simultaneously** (by default K, B, S)

The keylogger will pop up as a removable drive, containing the file LOG.TXT. This file will contain all recorded keystroke data.





Recording keystrokes

Installation of the *KeyGrabber Forensic Keylogger* is quick and easy. Simply plug it in between the USB keyboard and the USB port. No software or drivers are required. The USB hardware keylogger will start recording all data typed on the keyboard to the internal flash disk. Once recording starts, new data will be appended to the end of the log file. The device is completely transparent for computer operation.

Step 1. Disconnect the USB keyboard from the USB port at the computer or hub. This can be done even with the computer up and running.

Step 2.Connect the hardware USB keylogger between the USB keyboard and the USB port. Keystroke logging will start automatically.

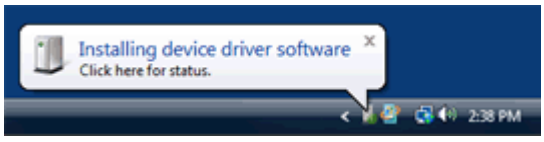
Note: If an external USB hub is being used, connect the keylogger between the hub and the USB keyboard.

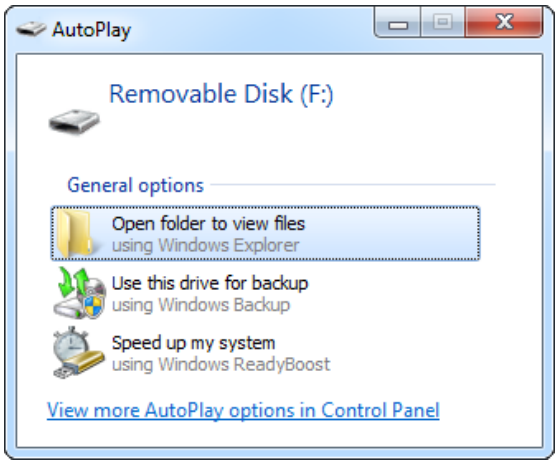
Viewing recorded data

Once keystroke data has been recorded, it may be retrieved on any computer with a USB port. This is done by switching to flash drive mode. The *KeyGrabber Forensic Keylogger* and keyboard should be connected in the same way, as during normal recording.

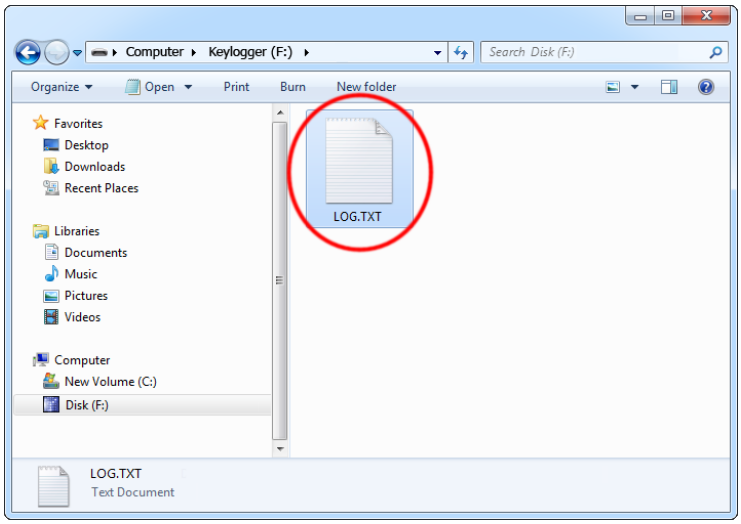
Each device has a built-in 3-key combination (by default K, B, S). Press these 3 magic keys **simultaneously** to trigger flash drive mode.

After a few seconds, the hardware keylogger will automatically get detected as a mass storage device. The operating system will use the standard built-in mass storage driver (*MS Windows 7* in the following examples).

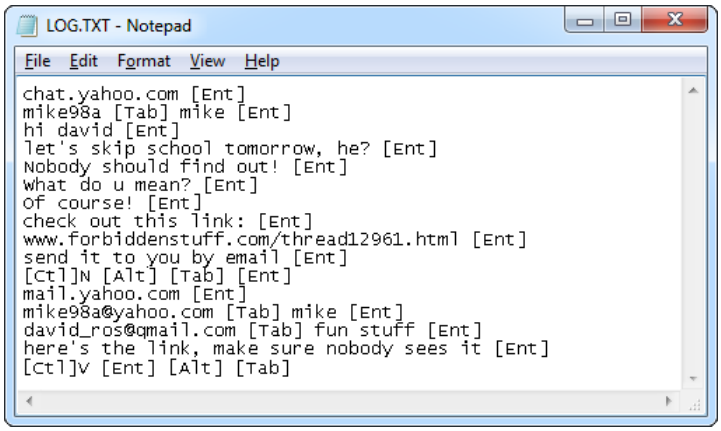




Depending on the drive letters available, the device will be visible as a new drive, for example F:. Use the systems file manager to browse this disk (for example *Explorer*). The keyboard will be disconnected and unavailable, so the mouse must be used to browse the disk.



The removable disk will contain the file LOG.TXT with a text log of all captured data. Keystroke data is formatted in the same as it would appear on the screen, with special keys in brackets ([Ent], [Esc], [Del] etc.). This file can be viewed and searched with any text editor, such as *Notepad* or *MS Word*.



During flash drive mode, the USB keyboard is inaccessible, and usually the mouse is the only operating device. Therefore it is a good idea to copy the file to the hard drive, and restore standard operation. Erasing and editing the file LOG.TXT is obsolete, because the flash disk has a huge memory worth of years of intensive typing.

Switching back to standard mode can be achieved by a safe software removal of the flash disk. Use the systems standard disk removal procedure. For *MS Windows*, left-click on the *Safe Removal* icon in the system tray and select the appropriate drive. Some systems will require to unplug the reconnect the keylogger.

Note: During the first switch to flash drive mode, the operating system can ask for drivers. In such case choose automatic driver installation (usually default option).

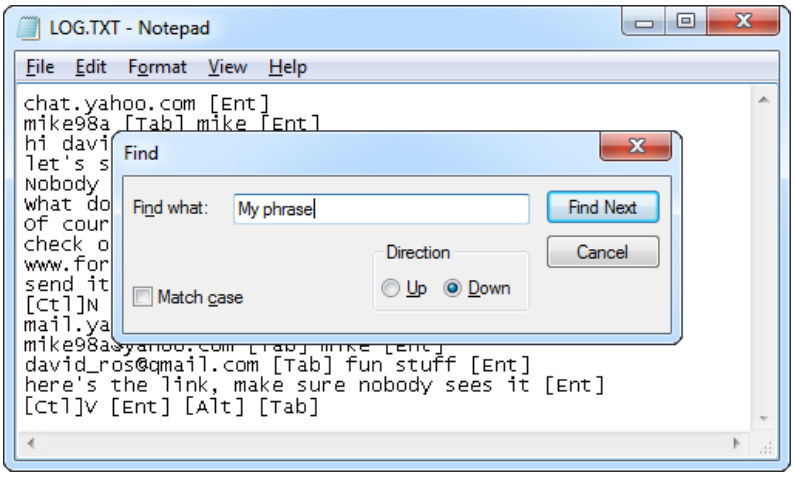
Note: While in flash drive mode, the USB keyboard is disabled. Use the mouse to operate the system. If mouse operation is dependent on the keyboard (i.e. wireless desktop or USB keyboard with mouse attached to it), connect the keyboard/mouse combo to a different USB port after switching to flash drive mode.

Flash drive options

Flash drive mode allows several standard examination and maintenance procedures to be performed through the operation system. The most common operations are described below with *MS Windows* as an example operating system.

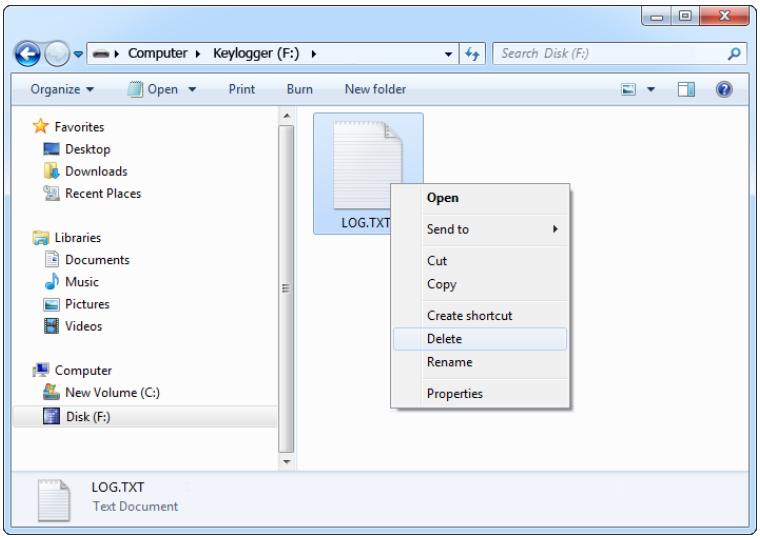
Phrase searching

Copy the log file LOG.TXT to the hard drive and restore standard mode, by disconnecting the flash disk. Open LOG.TXT in any text editor, such as *Notepad* or *MS Word*. The entire log file may be viewed, or searched using the text editor built-in *Find* option (CTRL-F). To locate WWW & E-mail addresses, define the search phrase as '*www'*, '*.com'*, '@' etc.



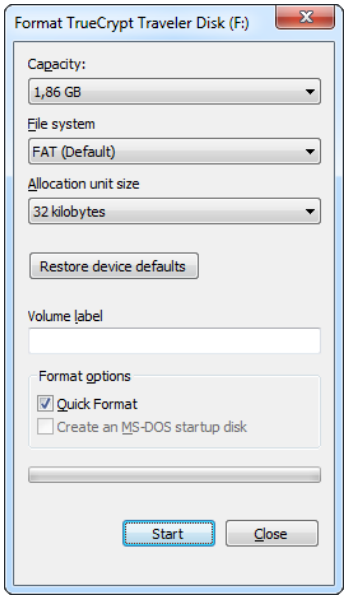
Memory erasing

A flash disk capacity of several megabytes makes memory erasing obsolete. This is equivalent to several years' worth of intensive typing. However, it is possible to keep the log file clean by erasing it occasionally. This can be achieved by the standard system file delete procedure while in flash drive mode. For *MS Windows* active the context menu for the log file and select *Delete*. A new log file will be created on the next power-up.



Memory formatting

Flash disk formatting will erase all data present, including the log, configuration, and layout files. For *MS Windows* activate the flash drive context menu and choose *Format*. Make sure the correct disk is selected and check the option *Quick Format*.



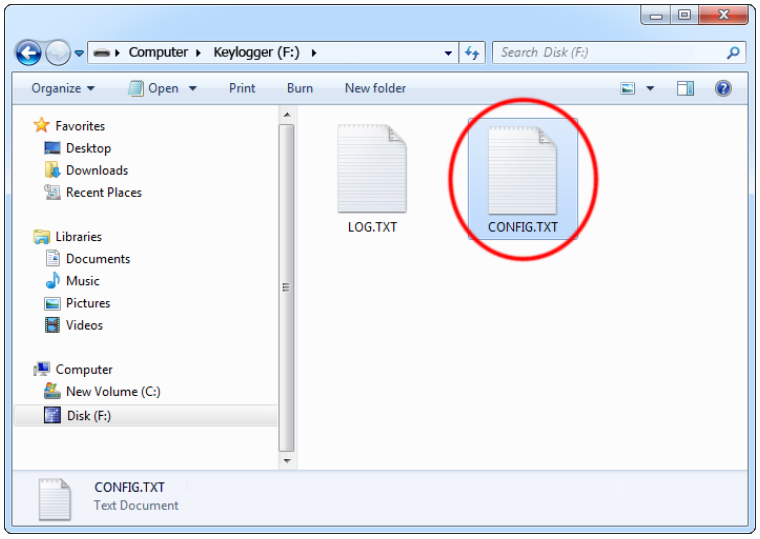
Disconnect and reconnect the keylogger from the USB port immediately after formatting has finished. Default settings will be restored and a new log file will be created.

Configuration options

The *KeyGrabber Forensic Keylogger* may be configured through the file CONFIG.TXT, placed in the flash drive root folder. Use any text editor to prepare such a configuration file, containing the following text:

```
Password=KBS
LogSpecialKeys=Some
DisableLogging=No
```

Copy this file to the root folder in flash drive mode. The new configuration will be loaded on next power-up.



The following list presents the most common configuration options. All variable and value strings are case insensitive.

Password sets the 3-key combination for triggering flash drive mode. Any three-letter key combination is allowed (sequence is irrelevant). The password setting is national-layout independent. Default value is *KBS*.

LogSpecialKeys sets the logging level for special keys, such as Enter, Escape, F1...F12 etc. Special keys are logged in brackets, i.e. [Ent]. Allowed values are *None* (only text is logged), *Some* (text with basic function keys are logged), and *All* (text with all special keys are logged). Default value is *Some*.

DisableLogging allows to disable keystroke logging, however does not affect mode switching. Allowed values are *Yes* (logging disabled) and *No* (logging enabled). Default value is *No*.

DisableLayout allows disabling the currently loaded layout, without having to delete the layout file. Allowed values are *Yes* (layout disabled) and *No* (layout enabled, if present). Default is *No*.

Encryption enables flash disk encrypting. Encryption will ensure full confidentiality of the stored data, even if the device is physically tampered with. Allowed values are *Yes* (encryption enabled) and *No* (encryption disabled). Default is *No*.

Important: toggling the encryption setting will format the entire flash disk. All data will be lost, including the configuration and layout files!

An example configuration file contents is shown below:

```
Password=SVL
LogSpecialKeys=Full
Encryption=Yes
```

A full list of available parameters with descriptions is available below.

Basic parameter list

Parameter	Values	Example	Description
Password	3-character password (default KBS)	Password=SVL	Three-character key combination for activating flash drive mode.
LogSpecialKeys	None Some (default) All	LogSpecialKeys=All	Special key logging level.
DisableLogging	Yes No (default)	DisableLogging=Yes	Keystroke logging disable flag.
DisableLayout	Yes No (default) Menu	DisableLayout=Yes	National layout disable flag (see section **National keyboard layouts**).

Advanced parameter list (use only when you know what you're doing!)

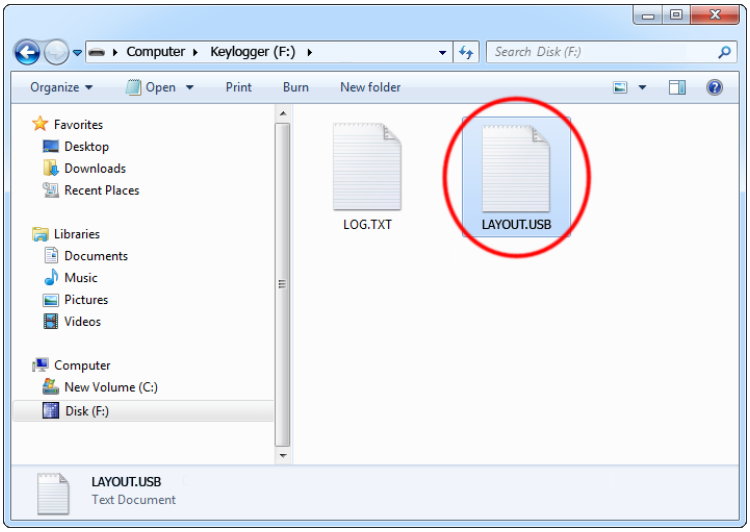
Parameter	Values	Example	Description
Encryption	Yes No (default)	Encryption=No	Flash drive encryption setting (caution: changing this value will re-format the flash drive).
CheckPid	Yes No (default)	CheckPid=Yes	Check the PID of each frame against known values.
LastChanceFitting	No Yes (default)	LastChanceFitting=No	Sets whether an additional software algorithm is used to fit captured frames.
FilterLevel	Filter level value (range 0…6, default 2)	FilterLevel=3	USB frame filter level value. A higher value corresponds to a more restrictive filter. A lower value corresponds to a more relaxed filter.
UsbDeviceSpeed	Auto (default) Full Low	KeyboardSpeed=Auto	Allows to manually sets the USB device standard between Low-speed and Full-speed.

National keyboard layouts

It is possible to enable a national layout for language-adapted keyboards, such as French, German etc. This will allow national characters to get logged properly (including those with Alt Gr), such as ö, æ, ß, ó etc. The following example demonstrates the advantages of applying the German national layout.

Text logged without layout	Text logged with layout
Kezlogger)PS-2 / USB=	*KeyLogger (PS/2 & USB)*

To enable a national layout, the appropriate layout file named LAYOUT.USB must be placed on the flash disks root folder. The file must be copied in flash drive mode. Layout files may be obtained from the CD-ROM attached with the device.



To enable the layout, safely remove the flash disk. On power-up, the layout file will be loaded automatically.

Specifications

Power supply	4.5 V – 5.5 V DC (drawn from the USB port)
Max. power consumption	65 mA (0.33 W)
Maximum burst log speed (approx.)	500 byte/s
Maximum continuous log speed (approx.)	100 byte/s
Data retention	100 years
Keyboard support	USB HID-compatible keyboard (Low-speed, Full-speed)
Maximum log read speed	500 kB/s
Dimensions excluding USB connectors (L x W x H)	10 mm x 16 mm x 11 mm (0.4" x 0.6" x 0.4")

Troubleshooting

The *KeyGrabber Forensic Keylogger* will **not** work with the following hardware configurations:

1. Internal laptop keyboards
2. Bluetooth keyboards
3. USB-PS/2 and PS/2-USB adapters
4. Non-conformant USB keyboards

The keyboard is not responding

The keyboard connector or the keylogger connector is not inserted firmly. Please check the connection with the USB keyboard and port.

The keylogger does not switch to flash drive mode

Please check the following:

1. Is the keylogger inserted between the keyboard and the keyboard port on the PC or hub?
2. Is your 3-key combination correct?
3. Are you pressing the 3 keys simultaneously? The 3-key combination will not be accepted if pressed sequentially.

Problems with logging national characters

Please check if you have downloaded the correct layout file and copied it to the flash disk root directory? If not, please check the **National keyboard layouts** section.

The keyboard doesn't work in flash drive mode

This is normal behavior. In flash drive mode, the keylogger will install the removable disk instead of the keyboard. Use the mouse to copy the log file to the hard drive, then restore normal operation. Alternatively, you may connect the keyboard to a different USB port after switching to flash drive mode.

The mouse and keyboard don't work in flash drive mode

This can happen on wireless keyboards and keyboard/mouse combos. In flash drive mode, the keylogger will install the removable disk instead of the keyboard/mouse combo. To get around this, connect the keyboard/mouse to a different USB port after switching to flash drive mode.

I've checked everything, nothing helps!

If you are still experiencing problems, please do the following:

1. Check if the problem appears on a different keyboard.
2. Check if the problem appears on a different computer.
3. Contact the dealer you have purchased the device from. Please supply all necessary information (keyboard model and manufacturer, OS type and version, and a short description of the problem).

List of special keys

[Esc]	-	Escape
[F1]	-	F1
[F2]	-	F2
[F3]	-	F3
[F4]	-	F4
[F5]	-	F5
[F6]	-	F6
[F7]	-	F7
[F8]	-	F8
[F9]	-	F9
[F10]	-	F10
[F11]	-	F11
[F12]	-	F12
[Ctl]	-	Control
[Alt]	-	Alt
[Ins]	-	Insert
[Hom]	-	Home
[PUp]	-	Page Up
[PDn]	-	Page Down
[Del]	-	Delete
[Win]	-	Win
[Aps]	-	Apps
[Cap]	-	Caps Lock
[Ent]	-	Enter
[Bck]	-	Backspace
[Tab]	-	Tab

[Prn]	-	Print Screen
[End]	-	End
[Scr]	-	Scroll Lock
[Up]	-	Up
[Dwn]	-	Down
[Lft]	-	Left
[Rgh]	-	Right
[Num]	-	Num Lock
[-N]	-	- (num)
[+N]	-	+ (num)
[.N]	-	. / Delete (num)
[/N]	-	/ (num)
[*N]	-	* (num)
[0N]	-	0 / Insert (num)
[1N]	-	1 / End (num)
[2N]	-	2 / Down (num)
[3N]	-	3 / Page Down (num)
[4N]	-	4 / Left(num)
[5N]	-	5 (num)
[6N]	-	6 / Right (num)
[7N]	-	7 / Home (num)
[8N]	-	8 / Up (num)
[9N]	-	9 / Page Up (num)
[Pwr]	-	Power
[Slp]	-	Sleep
[Wke]	-	Wake

Legal disclaimer

No responsibility is taken for any damage, harm or legal actions caused by misuse of this product. The user should follow the guidelines contained in this document, otherwise no liability will be assumed. It is the user's responsibility to obey all effective laws in his/her country, which may prohibit usage of this product.

In most countries the usage of a keylogger is fully legal as long as a clear notice is displayed, informing the user of the monitored equipment about the presence of a keystroke logger. We encourage the use of this equipment only for the purpose of monitoring your own computer, especially for protecting children against online hazards. It is NOT LEGAL to use a keylogger for the purpose of intercepting third party data, especially passwords, banking data, confidential correspondence, etc. If in doubt, please seek legal advice before using a keystroke logger. A good starting point is the U.S. Department of Justice Letter on Keystroke Monitoring and Login Banners, according to which a clear notice should be displayed, warning that user keystrokes may be logged.

For more information, visit the following websites:

http://www.keelog.com/

http://www.airdrivewifi.com/

You should not use this device to intercept data you are not authorized to possess, especially passwords, banking data, confidential correspondence etc.