

User's Guide

Keysnatchger™ Flash USB

4 MB, 1 GB, 2 GB



	Page
Introduction	2
Record Mode	4
Playback Mode (Flash Drive)	6
Flash Drive Options	10
Configuration Options	13
National Keyboard Options	15
Specifications	16
Troubleshooting	17
Special Key List	21
Legal Disclaimer	22

Check <http://www.keysnatch.com/> for the latest version of this document.

Introduction

Keysnatchger™ Flash USB

The Keysnatchger™ Flash USB is an advanced USB hardware keylogger with a huge 4 MB, 1 GB, or 2 GB internal flash disk, organized as a file system. All text data typed on the USB keyboard will be captured and stored on the internal Flash Drive in a special file. Text data may be retrieved on any other computer with a USB port and keyboard. Super fast data retrieve is achieved by switching into Flash Drive mode for keystroke data transmission. This hardware keylogger is 100% transparent for computer operation and no software or drivers are required.

Features

- Huge memory capacity (up to 2 GB), organized as a flash file system
- Compatible with all USB keyboards (including Linux & Mac)
- Super fast memory contents retrieve (125 kB/s) via USB port
- Transparent to computer operation, undetectable for security scanners
- No software or drivers required, operating system independent
- Quick and easy national keyboard layout support
- Ultra compact and discrete, only 1.5" (38 mm) long

Requirements

- USB 1.1 or 2.0 port
- USB HID-compliant keyboard (Low-Speed, Full-Speed, or High-Speed)
- 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

Record Mode

Installation of the Keysnatchger™ Flash USB in record mode is quick and easy. Simply plug it in between the USB keyboard and the USB port. No software or drivers are required to operate in record mode. 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 (see section Playback Mode). The device is completely transparent for operation of the computer.



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



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

If an external hub is being used, connect the keylogger between the hub and the USB keyboard. The picture below explains connection of the keylogger through an external USB hub.

Note: Keystroke logging will start approximately 5 seconds after power-up.

Note: If using a USB keyboard with a built-in USB hub with external devices attached, keystroke logging may start 5-10 seconds after power-up. This is due to the multiple device initialization process.

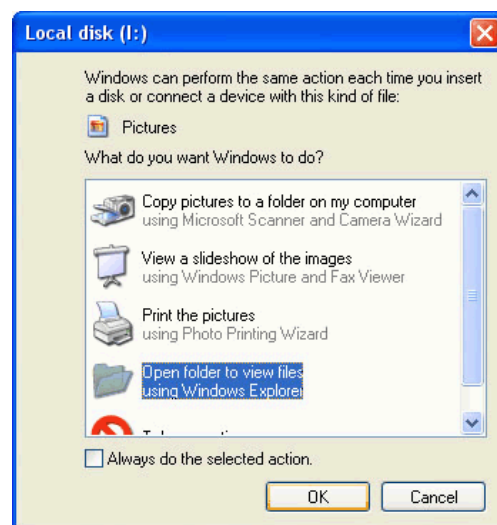
Playback Mode (Flash Drive)

Once data has been captured in record mode, it may be retrieved on any computer with a USB port. This is done by switching to Flash Drive mode. The Keysnatchger™ Flash USB and keyboard should be connected in the same way, as in record mode.

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. Initiating Flash Drive mode will automatically disconnect the USB keyboard.

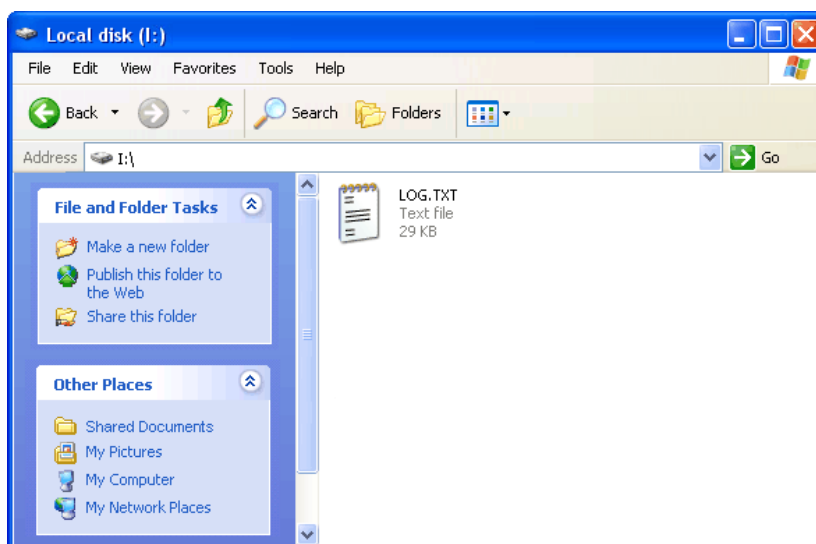


After a few seconds, the hardware keylogger will automatically get detected as a mass storage device. The operating system will use the standard built-in mass storage driver (*MS Windows XP* in the following examples).

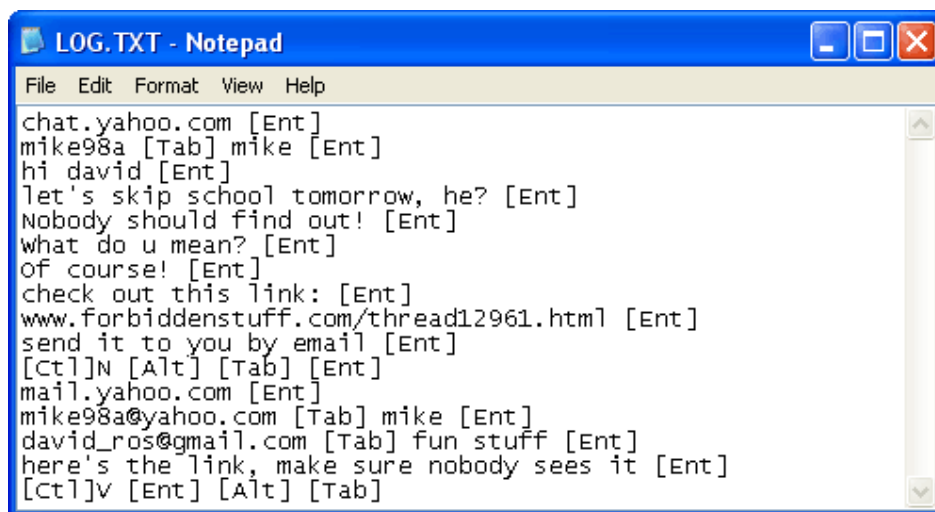


Depending on the drive letters available, the device will be visible as a new drive, for example I:. Use the systems file manager to browse this disk (for

example *Explorer*). The keyboard is disconnected and unavailable, so the mouse must be used to browse the disk.

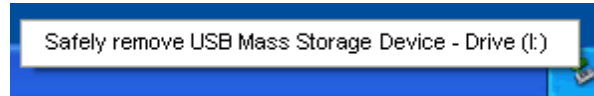


The Flash Drive will contain the file LOG.TXT with a text log of all captured data. Keystroke data is formatted in the same as it would appear on the screen, with special keys in brackets ([Ent], [Esc], [Del] etc.). This file can be viewed and searched with any text editor, such as *Notepad* or *MS Word*.

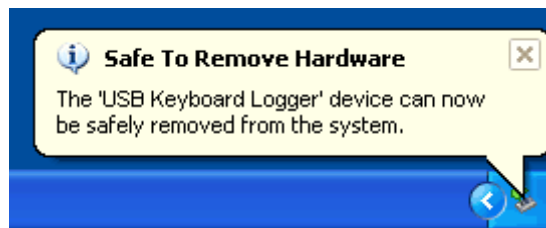


During Flash Drive mode, the USB keyboard is inaccessible, and usually the mouse is the only operating device. Therefore it is a good idea to copy the file to the hard drive, and restore record mode. Erasing and editing the file LOG.TXT is obsolete, because the flash disk has a huge memory worth of over one year of intensive typing. For typical keyboard usage, this is enough for several years of operation in record mode.

Switching back to record 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.



The system should respond with disconnecting the flash disk. Keyboard operation should be restored within a few seconds. Record mode will be initiated after another few seconds.



Note: To safely remove the flash disk, it cannot be simultaneously used by any other application.

Note: While in Flash Drive mode, the USB keyboard is disabled. Use the mouse to operate on the log file. If mouse operation is dependent on the keyboard (i.e. wireless desktop or USB keyboard with built-in hub with mouse attached), use a separate keyboard, mouse, or pointing device.

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).



On systems without built-in USB Mass Storage drivers, the driver has to be manually downloaded and installed:

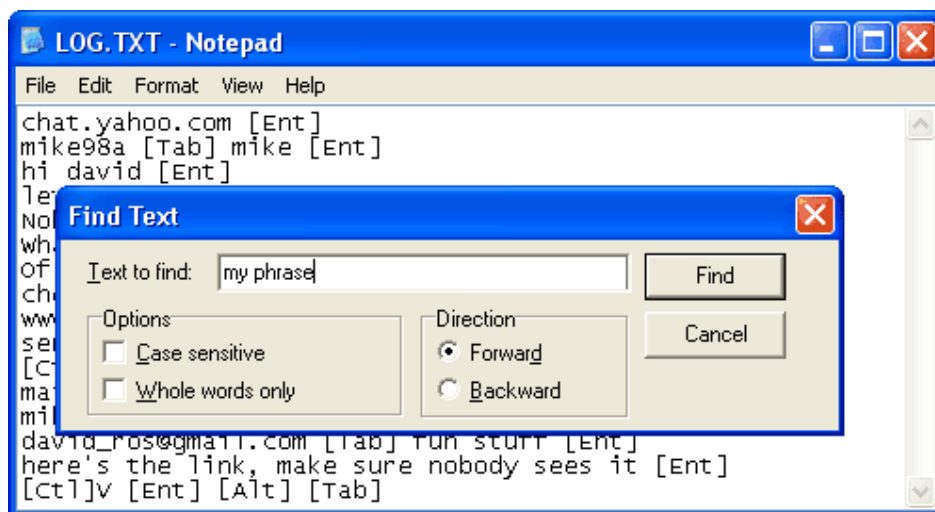
- MS DOS, MS Windows 95/98/NT and earlier do not feature USB Mass Storage drivers. Please try a third party generic mass storage driver, for example:
<http://www.technical-assistance.co.uk/kb/usbmsd98.php>
- Apple Computer's Mac OS supports USB Mass Storage by means of optional drivers from OS 8.5.1. OS 9 and OS X support USB mass storage natively.
- Linux support for USB Mass Storage has begun in kernel version 2.4, although 2.2 has been back-patched to support it.
- Solaris Operating Environment supports USB Mass Storage devices as well since the 2.8 release and up.
- NetBSD supports USB Mass Storage devices since the 1.5 release and up.

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

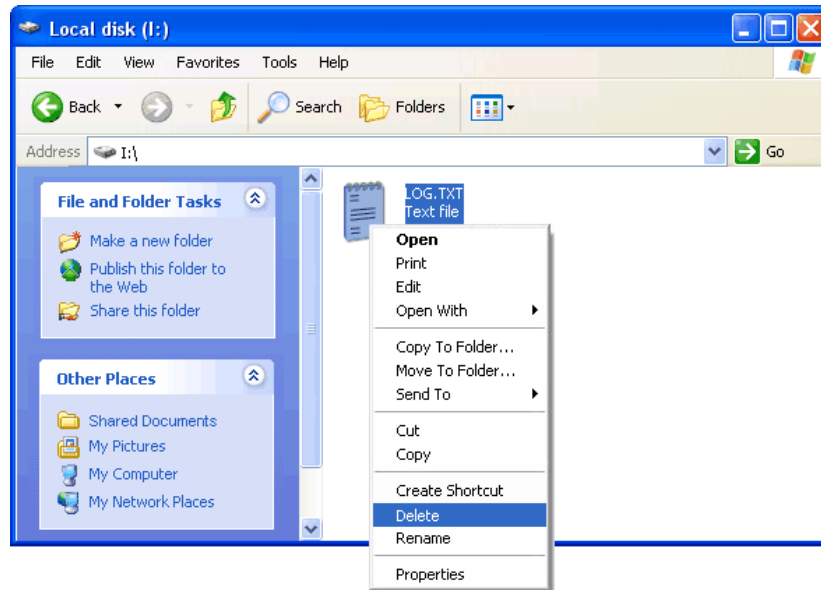
Copy the log file LOG.TXT to the hard drive and restore record mode, by disconnecting the flash disk. Open LOG.TXT in any text editor, such as *Notepad* or *MS Word*. The entire log file may be viewed, or searched using the text editor built-in *Find* option (CTRL-F). To locate WWW & E-mail addresses,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



Memory erasing

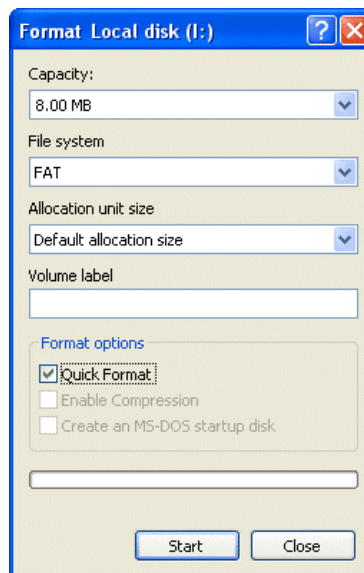
The flash disk capacity (2, 4, or 8 MB) makes memory erasing obsolete. This is an equivalent for several years worth of intensive typing. However it is possible to keep the log file clean by erasing it occasionally. This can be achieved by the standard system file removal procedure while in Flash Drive mode.

For *MS Windows* active the context menu for the log file and select *Delete*. A new log file will be created upon record mode initialization.



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

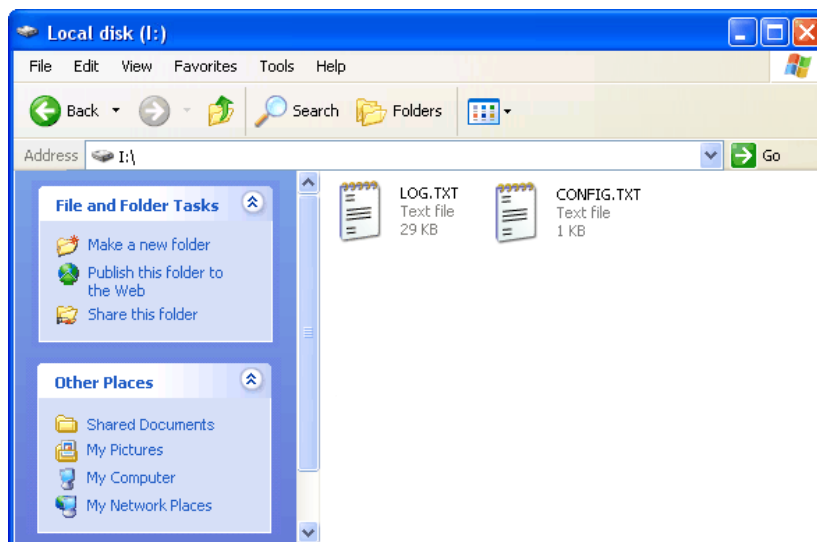
The USB hardware keylogger may be configured through the file CONFIG.TXT, placed in the Flash Drive root folder. Use any text editor to prepare such a configuration file, containing the following text:

Password=KBS

LogSpecialKeys=Medium

DisableLogging=No

Copy this file to the root folder in Flash Drive mode and switch to record mode. The configuration will be loaded on next record mode initialization.



The configuration file must be named CONFIG.TXT and must be placed in the root folder. Variable and value strings are case insensitive, however they must match the options listed below.

Password sets the 3-key combination for triggering Flash Drive mode. Any three-letter key combination is allowed (sequence is irrelevant). 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), *Medium* (text with basic function keys are logged), and *Full* (text with all special keys are logged). Default value is *Medium*.

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

ImeMode enables a special logging mode intended for use with systems with an IME editor, such as Japanese, Chinese, Korean, etc. If IME mode is enabled, the layout is discarded and every key pressed is logged using a normalized character sequence. Data logged in IME mode can be further processed with an external software text converter. Allowed values are *Yes* (IME mode enabled) and *No* (IME mode disabled). Default is *No*.

For more configuration options, see section Troubleshooting.

Example configuration file contents is shown below:

```
Password=SVL  
LogSpecialKeys=None  
DisableLogging=No
```

Note: Variable and value strings are case insensitive.

Note: Password characters are national layout independent.

Note: Logging all special keys (*LogSpecialKeys=Full*) may lead to increased memory usage.

National Keyboard Options

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.

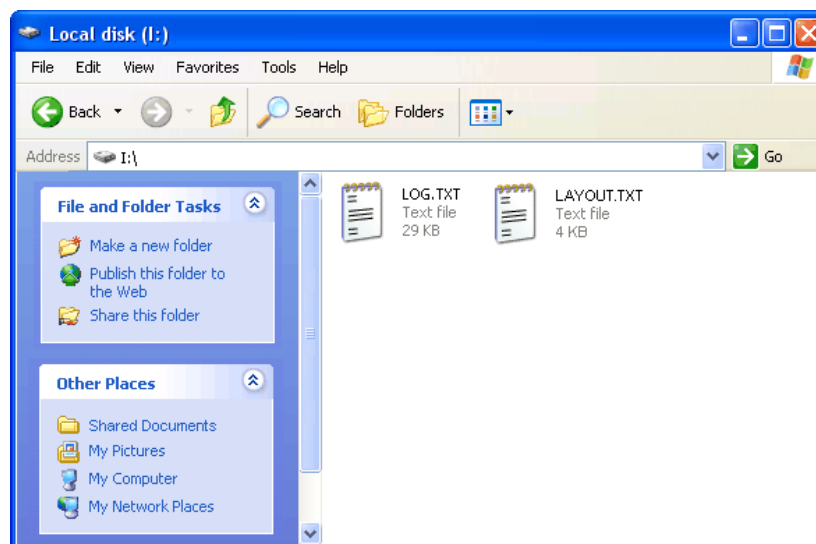
Text logged without layout

KeyLogger (PS/2 & USB)

Text logged with layout

Kezlogger)PS-2 / USB=

To enable a national layout, the appropriate layout file named LAYOUT.TXT must be placed on the flash disks root folder. The file must be copied in flash drive mode, because there is no access to the flash disk in record mode. Layout files may be obtained from the CD-ROM attached with the device or from the Keysnatch website <http://www.keysnatch.com/>. The flash disks main folder should contain the file LAYOUT.TXT and the standard log file LOG.TXT (and optionally a configuration file).



To enable the layout safely remove the flash disk. On record mode initiation, the layout file will be loaded automatically.

Specifications

Power supply – 4.5 V – 5.5 V DC (drawn from the USB port)

Power consumption – 65 mA (0.33 W)

Maximum burst log speed - 500 byte/s (approx.)

Maximum continuous log speed - 100 byte/s (approx.)

Memory capacity – 2 MB, 512 MB, 2 GB

Data retention - 100 years

Download speed – 125 kB/s

Body dimensions inc. USB connectors (L x W x H) -
53 mm x 20 mm x 12 mm (2.1" x 0.8" x 0.5")



All Keysnatch products come with 1 year warranty against manufacturer defects. Defect products must be shipped by the customer. All warranty repairs and delivery to the customer will be paid by Keysnatch.

Troubleshooting

The Keysnatchger™ Flash USB will not work for the following hardware configurations:

1. PS/2 keyboards (even with adapters)
2. Internal notebook keyboards
3. Keyboards with coded transmission (requiring drivers)
4. Some types of wireless keyboards (consult us first)

The keylogger does not switch to playback mode (flash drive)

Please check the following:

1. Is the keylogger inserted between the USB keyboard and the USB 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.
4. Do you have a compatible USB HID-compliant keyboard? Please use *USB View* (included with CD-ROM) to check your keyboard.
5. Does your operating system have built-in USB Mass Storage drivers? Older systems (for example Windows 95/98/NT) require installation of a universal mass storage driver. Please check the Playback Mode section.

The keylogger drops a few characters after power-up

The keylogger may drop a few characters directly after powering up, due to the internal startup sequence. Typically, this takes around 5 seconds. If using a USB keyboard with a built-in hub, the startup procedure may in some cases take additional time. This is due to the fact, that the keylogger must recognize all devices attached to the USB hub, including the keyboard itself, in order to filter USB traffic.

It is possible to speed-up this process, by supplying some additional information to the keylogger. This is done, by adding a configuration option to the CONFIG.TXT file (see section Configuration Options).

Important: incorrect configuration may lead to complete lock-up of the keylogger. Proceed only, if you are absolutely sure of your keyboard type. Use the *USB View* application or [consult us](#) first, if in doubt.

In most cases, both the hub and keyboard are USB Full-Speed devices. Typical examples include Apple A1048, Dell SK-8125, Dell SK-8135. In such case, add the following line to the CONFIG.TXT file:

```
KeyboardSpeed=Full
```

A few keyboards exist, which are composed of a Full-Speed USB hub and a Low-Speed keyboard. The most common examples are Apple A1243 and Apple M2452. In such case add the following line to the CONFIG.TXT file:

```
KeyboardSpeed=Low
```

Characters are missing in the log file

The keylogger may drop a few characters directly after powering up, due to the internal startup sequence. If characters are being skipped during normal operation, it is possible to remove some USB traffic filtering rules. This is done, by adding configuration options to the CONFIG.TXT file (see section Configuration Options). Add the following lines to the configuration file one-by-one, verifying device operation after adding each rule:

```
FrameFilter=34 (other possible values: 2, 0)
```

```
CheckModifierByte=No
```

```
CheckShortFrame=No
```


The keylogger does not switch back to record mode

Please check the following:

1. Are all applications connected to the flash disk (for example *Explorer*) closed?
2. Are you disabling the correct drive?

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 Options section.

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 us (keysnatch@keysnatch.com, <http://www.keysnatch.com/>). Please supply us all necessary information (keyboard model and manufacturer, OS type and version, and a short description of the problem).

Special Key List

[Esc]	-	Escape	[Prn]	-	Print Screen
[F1]	-	F1	[End]	-	End
[F2]	-	F2	[Scr]	-	Scroll Lock
[F3]	-	F3	[Up]	-	Up
[F4]	-	F4	[Dwn]	-	Down
[F5]	-	F5	[Lft]	-	Left
[F6]	-	F6	[Rgh]	-	Right
[F7]	-	F7	[Num]	-	Num Lock
[F8]	-	F8	[-N]	-	- (num)
[F9]	-	F9	[+N]	-	+ (num)
[F10]	-	F10	[.N]	-	. / Delete (num)
[F11]	-	F11	[/N]	-	/ (num)
[F12]	-	F12	[*N]	-	* (num)
[Ctl]	-	Control	[0N]	-	0 / Insert (num)
[Alt]	-	Alt	[1N]	-	1 / End (num)
[Ins]	-	Insert	[2N]	-	2 / Down (num)
[Hom]	-	Home	[3N]	-	3 / Page Down (num)
[PUp]	-	Page Up	[4N]	-	4 / Left(num)
[PDn]	-	Page Down	[5N]	-	5 (num)
[Del]	-	Delete	[6N]	-	6 / Right (num)
[Win]	-	Win	[7N]	-	7 / Home (num)
[Aps]	-	Apps	[8N]	-	8 / Up (num)
[Cap]	-	Caps Lock	[9N]	-	9 / Page Up (num)
[Ent]	-	Enter	[Pwr]	-	Power
[Bck]	-	Backspace	[Slp]	-	Sleep
[Tab]	-	Tab	[Wke]	-	Wake

Legal Disclaimer

Keysnatch does not take responsibility for any damage, harm or legal actions caused by misuse of its products. 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 Keysnatch products. Please also consider, that not knowing the law does not allow to not obey it. A good example 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. Please check with your legal representative for logging requirements in your country.

For more information on Keysnatch products, visit our website:

<http://www.keysnatch.com/>

You should not use this device to intercept data you are not authorized to possess, especially passwords, banking data, confidential correspondence etc. Most countries recognize this as a crime. Please consult a legal representative for logging requirements in your country.



KeySnatch

57 Flintridge Rd.
Toronto, Ontario
Canada, M1P 1C4

<http://www.keysnatch.com/>

Copyright © 2009. All rights reserved.