

Ultimate Forensic Write Protection Kit II

User's Guide

Forensic Computers, Inc.
110 Forensic Lane
Glen Lyn, VA 24093

www.forensic-computers.com

© 2009 Forensic Computers, Inc. All rights reserved.
© 2008-2009 Tableau, LLC. All rights reserved.
Tableau is a registered trademark of Tableau, LLC.

Table of Contents

1. Ultimate Forensic Write Protection Kit II	3
2. How to Use This Manual	3
3. Quick Start	3
3.1 Unpacking Your Ultimate Forensic Write Protection Kit II (UFWPK-II)	3
3.2 Using the Tableau T35e Forensic SATA/IDE Bridge (SATA)	7
3.3 Using the Tableau T35e Forensic SATA/IDE Bridge (IDE)	8
3.4 Using the Tableau T4 SCSI Bridge	10
3.5 Using the Tableau T8 USB Bridge	11
4. Useful Information	12
4.1 Configuration Switches	12
4.2 Removal Procedures	13
4.3 Daisy-Chaining Forensic Bridges	14
4.4 Hot-Swapping Drives	15
4.5 Other Tips & Information	15
5. Glossary	16

1. Ultimate Forensic Write Protection Kit II

The Ultimate Forensic Write Protection Kit II (UFWPK-II) does it ALL for the following media types: IDE, IDE Notebook, SATA, SCSI(50-pin, 68-pin, and SCA-80), PLUS seven varieties of flash media. The Ultimate Forensic Write Protection Kit comes packaged in either the Targus Laptop Bag (FAL VI MK III, FAL M-15 SR, or the FAL M-12) or in a Pelican 1450 (FAL IV MK II, or FAL V MK II) or in a Plano Tackle Box (OFT II, FT II, FT III, FT III DX, FSST, FSST DOPT).

2. How to Use This Manual

This manual has two main sections: Quick Start and Useful Information.




The Quick Start section of the manual will give the user enough information about the Ultimate Forensic Write Protection Kit II (UFWPK-II) and its accessories to get started. There is an overview of the additional components that come with the UFWPK-II and their use. The Useful Information section goes into more detail about specific components of the Ultimate Forensic Write Protection Kit II (UFWPK-II).








3. Quick Start

3.1 Unpacking Your Ultimate Forensic Write Protection Kit II (UFWPK-II)

In the Ultimate Forensic Write Protection Kit II (UFWPK-II), there are six categories of items: Forensic Bridges, Cables, Adapters, Power Assembly, Media Reader and Carrier Case.



When you first receive your UFWPK-II, please familiarize yourself with all of its contents. The following table lists each of the items found in the kit.

Photo	Description
	<p>The Tableau T35e can be used to connect to FireWire400, FireWire800, USB 1.1 and 2.0 devices to extract data from another computer. The T35e has a SATA, IDE and a power connection on its right side. (PN: T35e)</p>
	<p>The Tableau T35e-RW can be used to connect to FireWire400, FireWire800, USB 1.1 and 2.0 devices to extract data from another computer. The T35e-RW has a SATA, IDE and a power connection on its right side. (PN: T35e-RW)</p>
	<p>The Tableau T4 Forensic Bridge is a write-blocker for use with SCSI (Small Computer Systems Interface) hard disks. The T4 is identifiable from the T3u or the T35e by the SCSI port located on its right side. (PN: T4)</p>

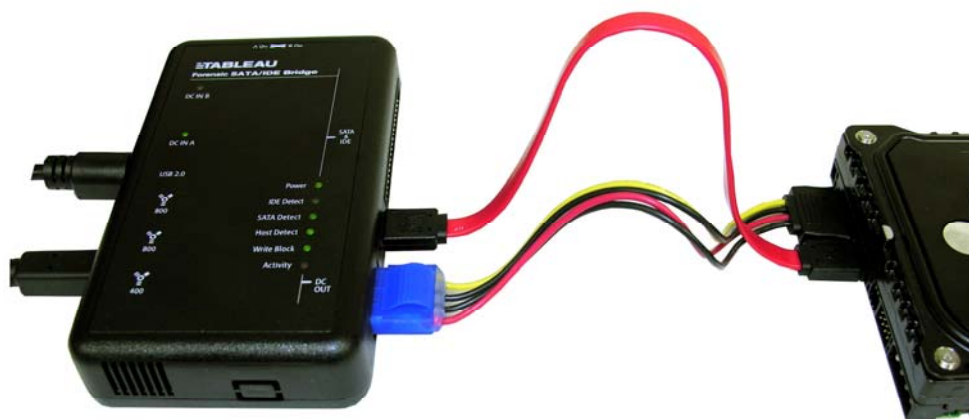
	<p>The Tableau T8 USB Forensic bridge works with mass storage devices like USB thumb drives, external USB hard drives, Apple iPod's that have USB interfaces, and even USB-based cameras with card-reader capability. (PN: T8)</p>
	<p>The TC10-8 SCSI ribbon cable is a high-quality, 68-conductor SCSI cable with standard high-density 68-pin SCSI connectors at each end. There are pull tabs at each end to make the cable more rugged. (PN: TC10-8)</p>
	<p>The TC6-8 IDE ribbon cable is a high-quality, 80-conductor IDE cable with standard high-density 40-pin IDE connectors at each end. There are pull tabs at each end to make the cable more rugged. (PN: TC6-8)</p>
	<p>50-pin SCSI cable</p>
	<p>The P9-P9 FireWire cable is a six feet in length. The P9 stands for the nine parallel wires inside of the cable. FireWire400 uses P4 or P6 connectors that have four or six parallel wires inside of the cable.</p>
	<p>The Mini Type B to USB cable has a type A connector on one end and a type B mini USB connector on the other end.</p>
	<p>TC3-8 SATA Signal Cable: SATA signal cable to connect ATA hard drives to the T35i.</p>

	<p>TC2-8 Power Cable: Molex power cable to connect IDE hard drives to the T35i.</p>
	<p>TC5-8 SATA Power Cable: SATA power cable to connect the 15-pin SATA power connector to the T35i.</p>
	<p>The 6" USB Extension Cable is a type A Male to Female USB extension cable, allowing one to extend an existing USB 2.0 connection.</p>
	<p>The 50-pin Male to 68-pin Female SCSI adapter converts a 50-pin SCSI cable to a 68-pin Female connection.</p>
	<p>The P6 Fire Wire adapters are used to convert FireWire800 P9 cables to a FireWire400 P6 connection. (PN: TCA7-6-9)</p>
	<p>The P4 FireWire adapters are used to convert FireWire800 P9 cables to a FireWire400 P4 connection. (PN: TCA7-4-9)</p>

	<p>The HP68 to SCA-80 Adapter converts a 68-pin SCSI connection to a SCA-80 SCSI connection.</p>
	<p>TDA5-25 2.5" IDE Notebook Adapter: Adapter for 1.8" notebook hard drives.</p>
	<p>TDA5-18 1.8" IDE Notebook Adapter: Adapter for 2.5" notebook hard drives.</p>
	<p>The Tableau TDA5-ZIF IDE Hard Disk adapter allows the user to connect to a Hitachi or Toshiba ZIF Notebook hard drive. The Tableau TDA5-ZIF IDE Hard Disk adapter comes with two FFC cables for the Hitachi drives, two FFC cables for the Toshiba drives and a handy pouch. (PN: TDA5-ZIF)</p>
	<p>The TDA3-1 can be used to adapt any Tableau SATA Forensic Product for use with a Micro SATA solid state drive. (PN: TDA3-1)</p>
	<p>The Tableau TDA8-M Media Card Reader combined with a Tableau T8 USB Bridge is capable of "write-blocked" access to twelve different popular digital media types including CF-I, CF-II, Smart Media™, Memory Stick™, Memory Stick PRO™, Memory Stick DUO™, Memory Stick PRO DUO™, Micro Drive™, Multimedia Card™, Secure Digital Card™, MINI Secure Digital Card™, and XD™ flash memory cards. When used independent of the Tableau T8, the TDA8-M functions as a non write blocked general purpose flash memory reader/writer. (PN: TDA8-M)</p>

	<p>The TP2 will connect to all Tableau products. The power cord connects to the TP2 via an IEC C7 "figure of eight" power connector. (PN: TP2)</p>
	<p>The PC Power cords are to power the TP2 power brick and the items that are connected to it.</p>

3.2 Using the Tableau T35e Forensic SATA/IDE Bridge (SATA)



Step by Step Instructions for connecting SATA hard drives to the T35e.

1. Ensure the T35e Forensic SATA/IDE Bridge's 'DC IN B' is in the 'B On' position.
2. Connect the TP2 power source to the left side of the T35e SATA Bridge via the 5-pin Mini-DIN connector.
3. Connect the power cable to the TP2 power source and also into an electrical socket.
4. Turn the power on to verify "write block" LED is ON. After verification, turn the power to the bridge OFF prior to connection to suspect hard drive.
5. Connect the female Molex connector of the TC5-8 SATA-Style Power Cable to the DC OUT located on the right side of the T35e SATA/IDE Bridge.
6. Connect the SATA power connector of the TC5-8 SATA-Style power cable to the suspect hard drive's SATA power connector.

Note

(DO NOT use both Molex and SATA power connections when connecting to a suspect hard drive, as this will overload the suspect hard drive.)

7. Connect the TC3-8 SATA Signal Cable to the T35e SATA/IDE Bridge.
8. Connect the other end of the TC3-8 SATA Signal Cable to the suspect hard drive.
9. The T35e has several means of communication between itself and the host computer: USB 2.0, two FireWire 800 connections and one 4-pin FireWire 400 connection. Plug one end of the chosen data cable to one of the ports on the left side of the T35e SATA/IDE Bridge.
10. Plug the other end of the chosen data cable to a port on the host computer.

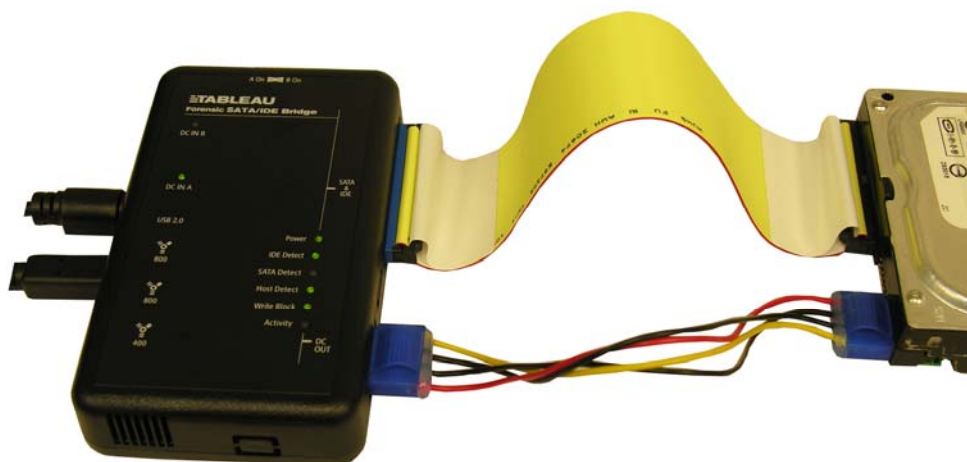
Note

(If using a FireWire connection to the HOST, the "HOST DETECT" LED will not come on until the bridge is communicating with the suspect hard drive. If using a USB 2.0 connection to the HOST, at power ON the "HOST DETECT" LED will immediately come ON.)

11. Flip the switch on the top of the T35e SATA/IDE Bridge to the 'A On' position. The host computer should now see the suspect hard drive.
12. The T35e SATA/IDE Bridge is configured to be a READ ONLY device, hence the black color of the device. To configure the T35e SATA/IDE Bridge to be a READ/WRITE device, please refer to the section titled "Configuration Switches".

3.3 Using the Tableau T35e Forensic SATA/IDE Bridge (IDE)

[Step by Step Instructions for connecting IDE hard drives to the T35e.](#)



1. Ensure the T35e Forensic SATA/IDE Bridge's 'DC IN B' is in the 'B On' position.
2. Connect the TP2 power source to the left side of the T35e SATA/IDE Bridge via the 5-pin Mini-DIN connector.
3. Connect the power cable to the TP2 power source and also into an electrical socket.
4. Turn the power on to verify "write block" LED is ON. After verification, turn the power to the bridge OFF prior to connection to suspect hard drive.
5. Connect one female Molex connector of the TC2-8 Molex-style Power cable to the DC OUT located on the right side of the T35e SATA/IDE Bridge.
6. Connect the other female Molex connector of the TC2-8 Molex-style Power cable to the suspect hard drive's Molex connector.
7. Connect the TC6-8 IDE Signal Cable to the T35e SATA/IDE Bridge.
8. Connect the other end of the TC6-8 IDE Signal Cable to the suspect hard drive.
9. The T35e has several means of communication between itself and the host computer: USB 2.0, two FireWire 800 connections and one 4-pin FireWire 400 connection. Plug one end of the chosen data cable to one of the ports on the left side of the T35e SATA Bridge.
10. Plug the other end of the chosen data cable to a port on the host computer.

Note

(If using a FireWire connection to the HOST, the "HOST DETECT" LED will not come on until the bridge is communicating with the suspect hard drive. Although, if using a USB 2.0 connection to the HOST, at power ON, the "HOST DETECT" LED will immediately come ON.)

11. Flip the switch on the top of the T35e SATA/IDE Bridge to the 'A On' position. The host computer should now see the suspect hard drive.
12. The T35e SATA/IDE Bridge is configured to be a READ ONLY device, hence the black color of the device. To configure the T35e SATA/IDE Bridge to be a READ/WRITE device, please refer to the section titled "Configuration Switches".

3.4 Using the Tableau T4 SCSI Bridge

Step by Step Instructions for connecting SCSI hard drives to the T4.



1. Ensure the T4 Forensic SCSI Bridge's 'DC IN B' is in the 'B On' position.
2. Connect the TP2 power source to the left side of the T4 SCSI Bridge via the 5-pin Mini-DIN connector.
3. Connect the power cable to the TP2 power source and also into an electrical socket.
4. Connect the female Molex connector of the TC2-8 Molex-style Power cable to the DC OUT located on the right side of the T4 SCSI Bridge.
5. Connect one Molex connector of the TC2-8 Molex-style Power cable to the suspect hard drive's Molex connector.
6. Connect the appropriate Signal Cable to the T4 SCSI Bridge. If the suspect hard drive has a 50-pin SCSI connector then use the 50-pin SCSI cable with the 50-pin to 68-pin SCSI adapter. If the suspect hard drive has a 68-pin SCSI connector, then use the TC10-8 SCSI Signal Cable. If the suspect hard drive has a SCA-80 connector, then use the TC10-8 SCSI Signal cable and the SCA-80 Adapter.
7. Connect the other end of the appropriate Signal Cable to the suspect hard drive using the appropriate adapter, if necessary.
8. The T4 has several means of communication between itself and the host computer: USB 2.0, two FireWire 800 connections and one 4-pin FireWire 400 connection. Plug one end of the chosen data cable to one of the ports on the left side of the T4 SCSI Bridge.
9. Plug the other end of the chosen data cable to a port on the host computer.
10. Flip the switch on the top of the T4 SCSI Bridge to the 'A On' position. The host computer should now see the suspect hard drive.
11. The T4 SCSI Bridge has two additional LED's mounted on the side of the unit between the "HD68 SCSI connector and the DC OUT Molex connector. These two LED's indicate which type of SCSI bus is in use: LVD or Low Voltage Differential (green LED), and the SE or Single Ended (yellow LED). IF neither LED is illuminated, you may be attempting to use an older HVD SCSI device; and the T4 is not compatible with HVD devices.
12. The T4 SCSI Bridge is configured to be a READ ONLY device, hence the black color of the device. To configure the T4 SCSI Bridge to be a READ/WRITE device, please refer to the section titled "Configuration Switches".

3.5 Using the Tableau T8 USB Bridge

[Step by Step Instructions for connecting USB drives to the T8.](#)



1. Ensure the T8 Forensic USB Bridge is in the 'Off' position as shown in Figure 4.1.
2. Connect the TP2 power source to the left side of the T8 USB Bridge via the 5-pin Mini-DIN connector.
3. Connect the power cable to the TP2 power source and also into an electrical socket.
4. Connect the suspect USB drive to the right side of the T8 USB Bridge.
5. Connect the other end of the appropriate Signal Cable to the suspect hard drive using the appropriate adapter, if necessary.
6. The T8 has several means of communication between itself and the host computer: USB 2.0, and one 6-pin FireWire 400 connection. Plug one end of the chosen data cable to one of the ports on the left side of the T8 USB Bridge.
7. Plug the other end of the chosen data cable to a port on the host computer.
8. Flip the switch on the right side of the T8 USB Bridge to the 'On' position. The host computer should now see the suspect hard drive.
9. The T8 USB Bridge has a LCD Display on the front face of the device, with two buttons to navigate. For more detailed information on navigating the LCD Display, please refer to the T8 LCD Users Guide on Tableau's website: [Tableau T8 LCD Document](#)
10. The T8 USB Bridge is configured to be a READ ONLY device, hence the black color of the device. Unlike the other forensic bridges created by Tableau, which can be "field-switched" between READ ONLY (write-block) and READ/WRITE modes of operation, the T8 is permanently configured for write-blocking operation only.

4. Useful Information

4.1 Configuration Switches

On each of the following Tableau Forensic Bridges, there is a 4-position DIP switch that can be used to set a variety of configurations: T3u, T35e, T4 and T5. The switches can be accessed by removing a small knockout panel on the bottom edge of the bridge's plastic enclosure.

The following table summarizes the function of the configuration switches on Tableau forensic bridges.

Switch	Operation	
	Switch OFF	Switch ON
1	Bridge operates in READ-ONLY mode and may be used to capture forensically sound images from subject hard disks.	Bridge operates in READ-WRITE mode.
2	Bridge reports errors if host computer attempts to write when bridge is in READ-ONLY mode.	Bridge does not report write errors when in READ-ONLY mode. (The bridge discards write data without returning an error.)
3	Bridge reports that it is WRITE-PROTECTED to the host computer when in READ-ONLY mode.	Bridge does not report that it is WRITE-PROTECTED when in READ-ONLY mode.
4	This switch is RESERVED as must remain in the OFF position for correct operation.	

The following table summarizes the recommended Tableau bridge configuration depending on the operating system you are using. These recommendations apply only when using the Tableau bridge in READ-ONLY mode to capture forensic images from subject hard drives (i.e., when switch 1 is OFF):

O/S	Switch 2	Switch 3	Comments
Windows XP	OFF	OFF	In most situations, Windows XP handles READ-ONLY bridges correctly and will work optimally when leaving switches 2 and 3 in the OFF (default) state. However, Tableau has seen cases where Windows XP will not allow a user to access a read-only partition. If you encounter a situation in which Windows XP reports that a volume is "write protected" and will not allow you to access the partition, then try the switch setting recommended for Windows 2000, below.
Windows 2000	ON	ON	Windows 2000 does not mount NTFS volumes correctly when the bridge declares that it is READ-ONLY. These settings make Windows 2000 believe the bridge is in READ-WRITE mode (even though it is not), and Windows 2000 will successfully mount NTFS volumes.

Windows ME/98se	ON	OFF	Windows ME/98se may not recognize that a bridge is READ-ONLY and may attempt to write to the bridge anyway. If this happens, Windows ME/98se will generate a "blue screen" error. The recommended settings to the left eliminate the "blue screen" error. NOTE: Some forensic users <i>prefer</i> to see the Windows "blue screen" error if a write is attempted. Users with this preference should use the recommended settings for Windows XP instead.
Other	OFF	OFF	Most other modern operating systems handle READ-ONLY forensic bridges correctly, so the default OFF settings is best for users of these operating systems.

IMPORTANT: As long as switch 1 is OFF (as confirmed by the Write Block LED being illuminated), the Tableau bridge will *never* permit writes or other modifications to the subject hard disk. Switches 2 and 3 only affect the way the bridge *appears to behave* from the perspective of the host computer.

NOTE: Switches 2 and 3 are ignored when the Tableau bridge is in READ-WRITE mode (i.e., when switch 1 is ON).

4.2 Removal Procedures

- Use the Safely Remove Hardware application (Windows XP see Figure B.1) by clicking on the Safely Remove Hardware icon in the notification area of the Taskbar. Clicking on the icon will produce a list of removable devices. Click on the hard disk drive you wish to remove. A message will appear indicating that the device has been safely removed.



FIGURE B.1 Windows XP Safely Remove Hardware Icon.

- On the forensic bridge (T3u, T35e, T4 or T8), move the power switch to the OFF position and wait for the hard disk drive to stop spinning. If using the TP2 5-pin DIN connector, move the switch to the 'B On' position. If using a Molex connector, move the switch to the 'A On' position.
- Shutdown the forensic workstation, carefully disconnect all cables and store them in a manner to prevent physical damage.
- According to the situation, properly secure the SUBJECT hard drive(s).

4.3 Daisy-Chaining Forensic Bridges

To accomplish a daisy-chain of forensic bridges, one must use only the FireWire 400 or 800 ports on the T3u, the T35e, the T4 or the T5 forensic bridges. One can NOT use the USB ports and cables to cascade devices.

For instance, if one had two differing types of suspect hard drives, one could connect each to their appropriate forensic bridge, daisy chain the forensic bridges together using FireWire cabling and then connect the set to the host computer.



FIGURE C.1 Daisy Chain Example without both TP2 Power Units.

Daisy Chain Example (SATA and SCSI)

Items Needed:

- Host computer
- SATA suspect hard drive
- SCSI suspect hard drive (68-pin)
- (2) T2 Drive Power Switches
- (2) TP2 Power Units
- (2) Power Cables
- (2) P9 FireWire cables
- TC3-8 SATA Signal Cable
- TC10-8 SCSI Signal Cable (68-pin)
- T3u SATA Bridge
- T4 SCSI Bridge
- (2) TC2-8 Molex-Style Power Cables

Or TC2-8 Molex-Style Power Cable and TC5-8 SATA-Style Power Cable
(if needed: FireWire Cable Adapters)

1. Use the T3u SATA Bridge Installation Procedure and the T4 SCSI Installation Procedure from Chapters 2 & 3 except for the “power on” of both procedures.
2. Connect the p9 FireWire cable to the left hand side of the T3u SATA Bridge.
3. Connect the other end of that same cable to the left hand side of the T4 SCSI Bridge.
4. Connect another p9 FireWire cable to the second port of the T4 SCSI Bridge.
5. Connect the other end of the second p9 FireWire cable to the host computer.
6. If using the TP2 power unit without the T2 Drive Power switch, turn the T3u on by placing the top switch to the ‘A On’ position. Do the same with the T4. If using the TP2 power unit with the T2 Drive Power Switch, turn both T2 Drive Power switches on, and turn both the T3u and the T4 switches to the ‘B On’ position.

4.4 Hot-Swapping Drives

1. Follow 1 and 2 of the Removal Procedures listed above.
2. Disconnect the power connection from the suspect hard drive.
3. Disconnect the data/signal cable from the suspect hard drive.
4. Connect the power connector to the new suspect hard drive.
5. Connect the data/signal cable to the new suspect hard drive.
6. Switch the forensic bridge to the ‘ON’ position: if using TP2 only, switch to the ‘A On’ position, if using TP2 and T2 Drive Power Switch, switch to the ‘B On’ position.

4.5 Other Tips & Information

- When removing the Berg/Floppy connector from the T14s or the T15, ALWAYS firmly grasp the plastic housing of the Berg/Floppy connector and gently pull or rock the plastic housing from side-to-side. Do NOT pull by the wiring, as this will disrupt the electrical connection.
- Do NOT remove a hard drive from a forensic bridge while the power is ON.
- Do NOT use USB cable extenders with any forensic bridge.
- As with all established Computer Forensics Best Practices it is the user’s responsibility to test the hardware on non-evidentiary media/data prior to using the hardware/software/procedures on live evidence.
- When a removable device such as a FireWire module/hard disk drive combination is improperly removed from a booted system it is referred to as a “surprise removal” and the FireWire device may or may not reinitialize correctly. In some situations the “surprise removal” can result in data loss or corruption. Using the T2 Drive Power Switch eliminates this problem.

5. Glossary

A

ATA – AT Attachment is a standard interface for connecting storage devices such as hard disks and CD-ROM drives inside of personal computers.

B

C

D

DIN- the abbreviated name of the German Institute for Standardization (Deutsches Institut für Normung) and is used in the names of its standards. There are a variety of DIN connectors in existence today. The one mentioned in this text is a 5-pin DIN connector.



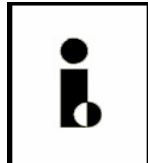
DIP – as in DIP Switch, is an electric switch that is packaged in a group of standard dual in-line package and is designed to be used on a printed circuit board along with other electronic components and is commonly used to customize the behavior of an electronic device for specific situations.

E

eSATA – external serial advanced technology attachment: an external interface for SATA technologies.

F

FireWire Symbols -



a.

b.

The above symbols represent the IEEE1394 standard. These symbols will help you identify products that are compatible with computers and cameras that use this standard. The

FireWire symbol on the left (a) is a trademark of the Apple Corporation. The i. Link symbol on the right (b) is a trademark of Sony Corporation.

G

H

Hot swapping or hot plugging is the ability to remove and replace components of a machine, usually a computer, while it is operating.

I

IDE – Integrated Drive Electronics, a synonym for an ATA storage device.

iPOD – a brand of portable media players designed and marketed by Apple Computer.

J

K

L

Forensic Computers

M

Molex[®] - A type of power connection used the computer industry, which has a plastic end attached to four wires: one yellow (12V), one red (5V) and two black (ground). There are female and male Molex[®] connectors.



N

O

P

Q

R

S

SAS – Serial Attached SCSI, a data transfer designed to move data to and from computer storage devices.

SATA – is a traditional dish from the Malaysian state of Terenngganu, consisting of spiced fish meat wrapped in banana leaves and cooked on a grill.

NO REALLY -Serial ATA, a computer bus technology primarily designed for the transfer of data from a hard disk.

SCSI – Small Computer System Interface is a standard interface and command set for transferring data between devices on both internal and external computer buses. (pronounced skuzzy)

T

U

USB – Universal Serial Bus is a serial bus standard to interface devices. It was designed for computers such as PCs and the Apple Macintosh, but its popularity has prompted it to also become commonplace on video game consoles, PDAs, cell phones and even devices such as televisions and home stereo equipment (mp3 players) and portable memory devices.

V

W

X

Y

Z