

Forensic Tower II

User's Guide

June 12, 2009

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. Forensic Tower II (FT II)	3
2. How to Use This Manual	3
3. Quick Start	3
3.1 Unpacking Your Forensic Tower II (FT II)	3
3.2 Using the Tableau T335 Drive Bay Controller	5
3.3 Imaging the OS Drive	6
4. Glossary	10

1. Forensic Tower II (FT II)

The Forensic Tower II is the latest addition to Forensic Computers' line of high quality powerful forensic workstations. There are five external 5.25" bays and six internal 3.5" bays in the Forensic Tower II's case that allow for easy upgrades and the flexibility to configure a forensic lab system to meet your needs.

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 Forensic Tower II and its accessories to get started. There is an overview of the additional components that come with the FT II and their use. The Useful Information section goes into more detail about specific components of the Forensic Tower II (FT II).

3. Quick Start

3.1 Unpacking Your Forensic Tower II (FT II)

The Forensic Tower II system has the following items: the Forensic Tower II, the monitor, the keyboard, the mouse, the PC power cord and the Forensic Write Protection Kit. The Forensic Tower II system utilizes CRU-DataPorts controlled by a Tableau T335 Forensic Drive Bay Controller, which allows the forensic investigator to extract a forensically sound image (or copy) of a subject hard drive.

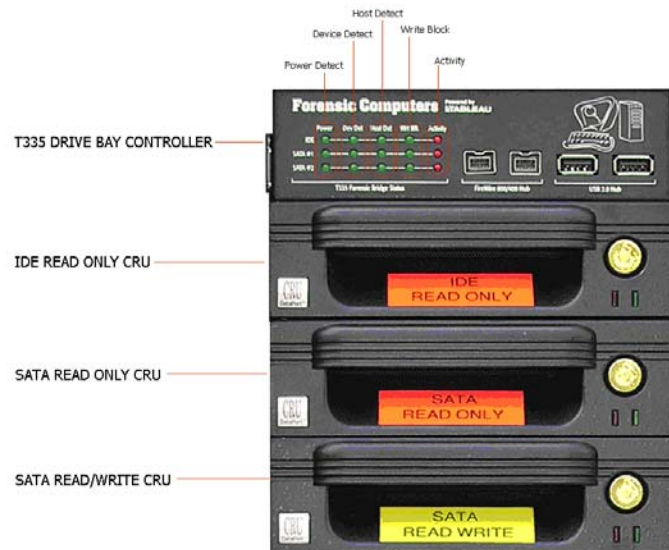
When you first receive your FT II, please familiarize yourself with all of its contents. The following table lists each of the items found in the kit.

Photo	Description
	Forensic Tower II
	Dell 22" LCD Widescreen Panel

	Keyboard & Mouse Combo
	Manual Bag
	CD Wallet
	Screwdrivers:
	Flashlight
	Surge Protector
	IDE to SATA tray for the SATA READ/WRITE bay.

3.2 Using the Tableau T335 Drive Bay Controller

The three CRU DataPort trays (IDE READ ONLY, SATA READ ONLY, and the SATA READ/WRITE) are removable from their prospective bays. With the addition of a T335 Drive Bay Controller, the CRU DataPort trays are then “hot swappable” (meaning one can insert or remove a hard drive from the trays while the computer is still powered ON). If the CRU DataPort lock is in the “locked/ON” position, and the computer is on, the T335 Drive Bay Controller’s “Power” LEDs will be consistently ON whether or not a hard drive is in the tray.



Step by Step Instructions for accessing hard drives via CRU.

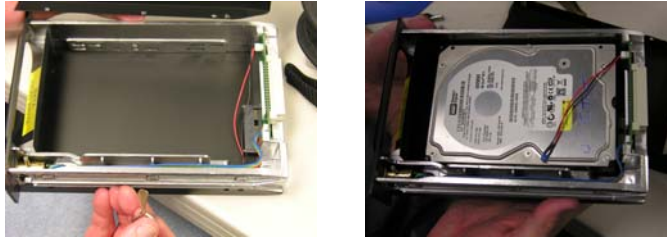
1. In order to insert a hard drive into one of the trays, one must unlock the CRU DataPort tray with a CRU Key and gently pull the tray from the computer.



2. Using a CRU Opener, place the flat end up under the lid of the CRU DataPort tray and gently pry loose the lid of the CRU DataPort tray.



3. Inside of the tray will be power and data connections for either a SATA or an IDE hard drive. Connect the corresponding hard drive to its power and data connectors and gently lay the hard drive in the CRU DataPort tray.



4. Replace the lid of the tray back on, and insert the entire tray in the computer bay from whence it came.
5. Once the tray has been re-inserted, use the CRU Key to turn the CRU DataPort back to the "ON/locked" position.



The operating system and the T335 should at this point see the suspect hard drive. If the hard drive is in the IDE READ ONLY tray, then (on the T335 Drive Bay Controller) the IDE Power, Dev Det, the Host Det, and the Wrt Blk LEDs will be lit. The Activity light will blink ON and OFF as "activity" occurs. The Microsoft Windows XP Professional will usually have a pop-up window on detection of the suspect drive. If a pop-up window does not occur, one can check Device Manager for the hard drive under "Disk Drives" or in "Disk Management", which is a part of Computer Management. One can also use their forensic software to determine whether the suspect hard drive has been detected.

3.3 Imaging the OS Drive

Over time, an investigator will need to image and re-image their OS hard drive. As of December 2007 three types of software have been used to create the initial OS hard drive images sent out with Forensic Computers' line of systems: Norton Ghost, Acronis TrueImage version 10 and Image for Windows.

3.3.1 Re-Installing the image for the OS Hard Drive (Image for Windows)

(Your username and SN for IMAGE FOR WINDOWS will be located in your CD wallet. If it is not, call us with the serial number of your system and we will locate your IMAGE FOR WINDOWS serial number.)

- Enter the BIOS and ensure that the DVD_RW is set to boot before the hard drive
- Insert the DVD into the DVDRW

- The program will automatically start up and ask you to "press <space> for menu or wait for the restore to start"
- Wait for the restore to start as it will select the first hard disk (HD0) which is your OS drive
- The program will then ask if you want to continue with the restore on HD0 (this will erase everything on the drive and restore it to factory defaults.)
- Once the restore has completed and has been rebooted, the machine will be ready for use.
- For more advance and detailed instructions please refer to the PDF included on your Image for Windows CD

3.3.2 Re-Imaging the OS Hard Drive (Image for Windows)

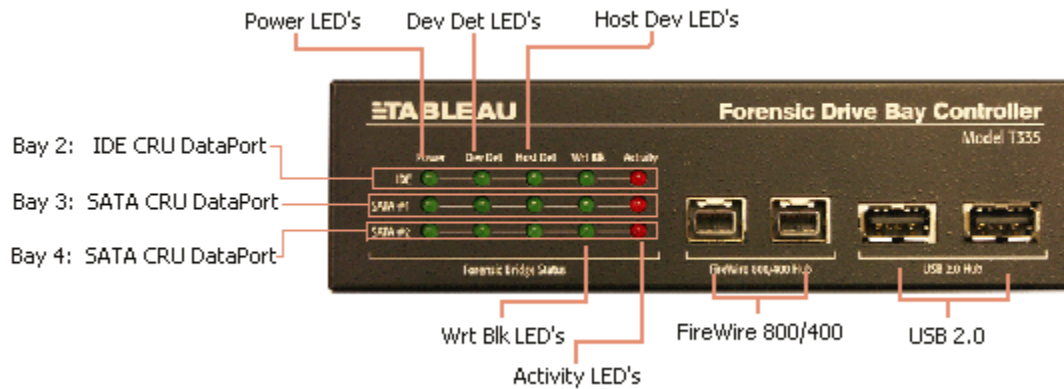
- Start Acronis True Image Home 10 from desktop shortcut/start menu
- Choose operation to perform: Backup (next)
- Select Partition: HD0 / specific hard drive (next)
- Select Destination: DVDRW (next)
- Backup Options (default settings) (Finish)

Image for Windows will burn an image of the drive to the disk and then proceed to automatically validate the disk. If errors occur during validation, one must start completely over with a fresh DVDRW.

4. Useful Information

4.1 Tableau T335 Drive Bay Controller

The Tableau T335 Forensic Drive Bay Controller is in the first bay of the Forensic Tower II. The Forensic Drive Bay Controller manages the following three CRU-DataPorts: the READ ONLY IDE CRU-DataPort, the READ ONLY SATA CRU-DataPort, and the READ/WRITE SATA CRU-DataPort. On the left hand side of the T335 Forensic Drive Bay Controller are the LED's. The five sets of LED's on the left hand side correspond to the three CRU-DataPorts: IDE CRU-DataPort (bay two), SATA READ ONLY CRU-DataPort (bay three), and SATA READ/WRITE CRU-DataPort (bay four). SATA #1 corresponds to the SATA READ ONLY CRU-DataPort and SATA #2 corresponds to the SATA READ/WRITE CRU-DataPort. The first row of LED's correspond to the IDE CRU-DataPort, the second row of LED's correspond to the SATA READ ONLY CRU-DataPort and the last row of LED's correspond to the SATA READ/WRITE CRU-DataPort. There are two FireWire 800/400 ports in the middle and two USB 2.0 ports on the right hand side. The last bay contains a DVD-RW. The OS hard drive and the DATA drive are in slots one and two of the internal bay configuration.



The following is a table of each of the items of the Tableau T335 and a description of its purpose:

Front Element	Description
Power LEDs	The Power LED for an individual CRU-DataPort unit indicates whether the power is ON or OFF for that unit. The Power LED will be on solidly when the corresponding CRU-DataPort or drive bay is ON. If the Power LED is blinking ON and OFF, then the drive bay is OFF and the T335 Forensic Drive Bay Controller is working normally.
Dev Det LEDs	The Dev Det LEDs (Device Detection) indicate that a hard drive has been recognized by the CRU-DataPort or drive bay unit in which the hard drive has been placed.
Host Det LEDs	The Host Det LEDs (Host Detection) indicate communication between the "Host" computer (in this case the Forensic Tower II), the T335 Forensic Drive Bay Controller and the subject hard drive which is in one of the CRU-DataPort units.

Wrt Blk LEDs	The Wrt Blk LEDs (Write Block) indicate the Tableau T335 Forensic Drive Bay Controller is in READ ONLY mode. If the individual LED is ON, then the corresponding drive bay may be used to capture a forensically sound image or copy of the hard drive that has been inserted into the drive bay CRU.
Activity LEDs	The Activity LED's indicate that host computer is communicating with the hard drive in the corresponding drive bay.
FireWire 800/400	The two FireWire 800/400 ports are NOT write-blocked, meaning that if one is using either one of the two FireWire ports to examine a hard drive, then the user can "write" to that hard drive and may corrupt evidence. The two FireWire 800/400 ports are used to attach other FireWire devices, such as the Tableau T4 Forensic SCSI Bridge.
USB 2.0	The two USB 2.0 ports on the front of the Tableau T335 are also NOT write-blocked. The USB ports are for connecting other external USB devices, such as a USB security dongle or any other device.

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.



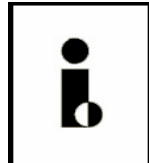
DIP – as in DIP Switch, is an electric switch that is packaged in a group of standard dual in-line package and is designed to be used on a printed circuit board along with other electronic components and is commonly used to customize the behavior of an electronic device for specific situations.

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 Terengganu, 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