Forensic Quest® User's Manual

Logicube, Inc.
Chatsworth, CA 91311
818 700 8488

P/N MAN-Quest-2
For Device P/N F-Quest-2
Version: 1.8
Date: 12/08/14

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER’S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

DISCLAIMER

IMPORTANT - PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. BY INSTALLING OR USING LOGICUBE PRODUCTS, YOU AGREE TO BE BOUND BY THIS AGREEMENT.

IN NO EVENT WILL LOGICUBE BE LIABLE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) FOR ANY AMOUNTS REPRESENTING LOSS OF PROFITS, LOSS OR INACCURACY OF DATA, LOSS OR DELAYS OF BUSINESS, LOSS OF TIME, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, PROPERTY DAMAGE, OR INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF A PURCHASER OR USER OF LOGICUBE PRODUCTS OR ANY THIRD PARTY. LOGICUBE’S AGGREGATE LIABILITY IN CONTRACT, TORT, OR OTHERWISE (WHETHER UNDER THIS

AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) TO A PURCHASER OR USER OF LOGICUBE PRODUCTS SHALL BE LIMITED TO THE AMOUNT PAID BY THE PURCHASER FOR THE LOGICUBE PRODUCT. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF LOGICUBE HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGES.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ITS PRODUCTS. HOWEVER, THE PURCHASER IS RESPONSIBLE FOR VERIFYING THAT THE OUTPUT OF A LOGICUBE PRODUCT MEETS THE PURCHASER'S REQUIREMENTS. THE PURCHASER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCTS CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DEFECTIVE DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY PURCHASER, EITHER UNDER THE WARRANTY SET FORTH BELOW OR ON A TIME AND MATERIALS BASIS.

LIMITED WARRANTY

FOR ONE YEAR FROM THE DATE OF SALE (THE “WARRANTY PERIOD”) LOGICUBE WARRANTS THAT THE PRODUCT (EXCLUDING CABLES, ADAPTERS, AND OTHER “CONSUMABLE” ITEMS) IS FREE FROM MANUFACTURING DEFECTS IN MATERIAL AND WORKMANSHIP. THIS LIMITED WARRANTY COVERS DEFECTS ENCOUNTERED IN THE NORMAL USE OF THE PRODUCT DURING THE WARRANTY PERIOD AND DOES NOT APPLY TO: PRODUCTS DAMAGED DUE TO PHYSICAL ABUSE, MISHANDLING, ACCIDENT, NEGLIGENCE, OR FAILURE TO FOLLOW ALL OPERATING INSTRUCTIONS CONTAINED IN THE OPERATING MANUAL; PRODUCTS WHICH ARE MODIFIED; PRODUCTS WHICH ARE USED IN ANY MANNER OTHER THAN THE MANNER FOR WHICH THEY WERE INTENDED, AS SET FORTH IN THE OPERATING MANUAL; PRODUCTS WHICH ARE DAMAGED OR DEFECTS CAUSED BY THE USE OF UNAUTHORIZED PARTS OR BY UNAUTHORIZED SERVICE; PRODUCTS DAMAGED DUE TO UNSUITABLE OPERATING OR PHYSICAL CONDITIONS DIFFERING FROM THOSE RECOMMENDED IN THE OPERATING MANUAL OR PRODUCT SPECIFICATIONS PROVIDED BY LOGICUBE; ANY PRODUCT WHICH HAS HAD ANY OF ITS SERIAL NUMBERS ALTERED OR REMOVED; OR ANY PRODUCT DAMAGED DUE TO IMPROPER PACKAGING OF THE WARRANTY RETURN TO LOGICUBE. AT LOGICUBE'S OPTION, ANY PRODUCT PROVEN TO BE DEFECTIVE WITHIN THE WARRANTY PERIOD WILL EITHER BE REPAIRED OR REPLACED USING NEW OR REFURBISHED COMPONENTS AT NO COST. THIS WARRANTY IS THE SOLE AND EXCLUSIVE REMEDY FOR DEFECTIVE PRODUCTS. IF A PRODUCT IS HAS BECOME OBSOLETE OR IS NO LONGER SUPPORTED BY LOGICUBE THE PRODUCT MAY BE REPLACED WITH AN EQUIVALENT OR SUCCESSOR PRODUCT AT LOGICUBE'S DISCRETION. THIS WARRANTY EXTENDS ONLY TO THE END PURCHASER OF LOGICUBE PRODUCTS. THIS WARRANTY DOES NOT APPLY TO, AND IS NOT FOR THE BENEFIT OF, RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS. UNLESS OTHERWISE AGREED IN WRITING BY LOGICUBE, NO WARRANTY IS PROVIDED TO RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS.

IN ORDER TO RECEIVE WARRANTY SERVICES CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA PHONE OR E-MAIL. PRODUCTS RETURNED TO LOGICUBE FOR REPAIR UNDER WARRANTY MUST REFERENCE A LOGICUBE RETURN MATERIAL AUTHORIZATION NUMBER (“RMA”). ANY PRODUCT RECEIVED BY LOGICUBE WITHOUT AN RMA# WILL BE REFUSED AND RETURNED TO PURCHASER. THE PURCHASER MUST CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA E-MAIL (SUPPORT@LOGICUBE.COM) OR VIA PHONE AT +1-818-700-8488

OPT. 3 TO OBTAIN A VALID RMA#. THE PURCHASER MAY BE REQUIRED TO PERFORM CERTAIN DIAGNOSTIC TESTS ON A PRODUCT PRIOR TO LOGICUBE ISSUING AN RMA#. THE PURCHASER MUST PROVIDE THE PRODUCT MODEL, SERIAL NUMBER, PURCHASER NAME AND ADDRESS, EMAIL ADDRESS AND A DESCRIPTION OF THE PROBLEM WITH AS MUCH DETAIL AS POSSIBLE. REASONABLE TELEPHONE AND EMAIL SUPPORT ARE ALSO AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS AGREEMENT, LOGICUBE PRODUCTS ARE PROVIDED AS-IS AND AS-AVAILABLE, AND LOGICUBE DISCLAIMS ANY AND ALL OTHER WARRANTIES (WHETHER EXPRESS, IMPLIED, OR STATUTORY) INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT OF THIRD PARTY RIGHTS.
SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Technical Support Contact Information

1. By website: www.logicube.com
2. By email: techsupport@logicube.com
3. By telephone: 1 - (818) 700 8488 ext. 3 between the hours of 7am –5pm PST, Monday through Friday, excluding U.S. legal holidays

Table of Contents

1. Introduction to the Forensic Quest

Introduction

Thank you for purchasing the Logicube Forensic Quest. With proper use, this unit will provide you with accurate HDD capturing for years to come.

The Logicube Forensic Quest is a drive-to-drive duplication device. Typically, a suspect (source) hard drive and an evidence (destination) drive will be connected to the unit. Within minutes of starting the process, the contents of the suspect drive are accurately copied over to the evidence drive for further examination. Handling of the suspect drive is held to a minimum with zero alteration of its contents.

Designed with the Forensics investigator in mind, the system ensures that proper evidence capture procedures are maintained, while speeding up the process significantly.

Specifications

The Forensic Quest is a feature-packed hand-held forensic data capture device designed specifically for the demanding requirements of law enforcement, military, government and corporate security organizations. Quest the latest computer forensic solution from Logicube® is designed to meet the complex challenges of digital forensic investigations. This high-speed solution allows users to quickly capture data from SATA and IDE hard drives. Optional support for capture from SCSI and SAS hard drives is available, and the Quest provides built-in USB connectivity. Quest allows investigators to quickly acquire potential evidence from suspect hard drives and is perfect for in-the-field or in-the-lab acquisition and verification.

Power Requirements	90 - 230 VAC 47 to 63Hz
Power Consumption	< 66 watts
Operating Temperature	5°-60°C
Relative Humidity	20%-80%
Net Weight	.03 lbs
Dimensions	5.2” W x 9” H x 2.6” D
Agency Approvals	RoHs compliant, FCC Part 15 Class A, CE

Features

- Capture data from one source hard drive to one destination drive at speeds approaching 6GB/min
- Built-in support for capture from SATA/IDE hard drives
- Optional support for capture from SCSI and SAS hard drives with the SCSI or SAS Cloning Adapter
- Ability to capture to two destination drives (with optional adapter)
- Ability to compute SHA-256 or MD5 Hash in real time (at full Capturing speed).
- DD image capture mode – Capture a suspect’s hard drive to multiple DD image files. User specified file size of: 650MB, 2GB, and 4GB for later archiving on to CD/DVD media and Flash Memory.

- Save configuration setting feature allows the operator to save frequently used capture settings.
- Destination drive fits inside Quest with a unique “clam shell” design that reduces footprint and gives added drive protection.
- Features Single Pass Wipe and DoD Wipe.
- Write-protected data transfer to prevent overwriting
- Captures from DCO and HPA areas of the hard drive
- Audit trail reporting. Generate and Write to Compact Flash™ for review and printing
- Externally accessible Flash memory – Stores software updates and reports etc. (Accessible via USB).
- Capture from an unopened desktop/laptop PC or MAC (except MacBook Air) with the Forensic USB Cloning Software (included on a CD-ROM with the Quest)
- High-speed acquisition of USB enclosures, USB Thumb/flash drives is available with an optional software key code and either the SCSI or SAS adapter
- Integrated LCD Touch Screen – For easy entry of file names, user passwords and keyword lists, etc.

Using this guide

This user guide is made up of 10 sections:

- Introduction
- Getting Started (Fast Start)
- Drive Capture Modes and Settings
- Other Modes
- USB Connection
- Printing Instructions
- Optional Peripherals
- Compact Flash™ Memory
- Software and Firmware Loading Instructions
- Reference / FAQ’s / Index

Please read **Section 1: Introduction & Section 2: Getting Started** before attempting a drive capture. It is recommended that you practice with a test or scratch drive to fully appreciate the unit’s features.

System description

The Forensic Quest solution is packed in a rugged carrying case. Inside, you will find the following components:

- The Logicube Forensic Quest with power adapter.
- 2 drive power cables, 1 short and 1 long (used to connect PATA suspect and destination drives to the unit).
- 2 HDD (Hard Disk Drive) data cables, 1 short and 1 long (used to connect PATA drives to the unit).
- 2 Serial ATA data/power cables for attaching Serial ATA (SATA) suspect and destination drives to the unit.
- A “Mini-B” USB cable that allows the unit to be connected to the USB port of a PC.
- A flashlight and screwdriver.
- A CD-ROM that contains the Forensic USB/Firewire Cloning Software
- A CD-ROM that contains the user’s manual
- A carrying case.

NOTE: It is recommended that you always use the carrying case to store and carry the unit.

The Forensic Quest menu and this User’s Guide occasionally refer to the drive locations as S1 and D1. The S1 designation corresponds with the Source drive while the D1 designation corresponds to the Destination drive.

Caution: Incorrectly connecting the suspect drive to the system can result in data on the suspect drive to be lost forever.

Caution: Never place a suspect drive INSIDE the Forensic Quest as data erasure can result.

Caution: Never place a suspect drive into any other Logicube products (e.g. Sonix®) that are used for Operating System cloning.

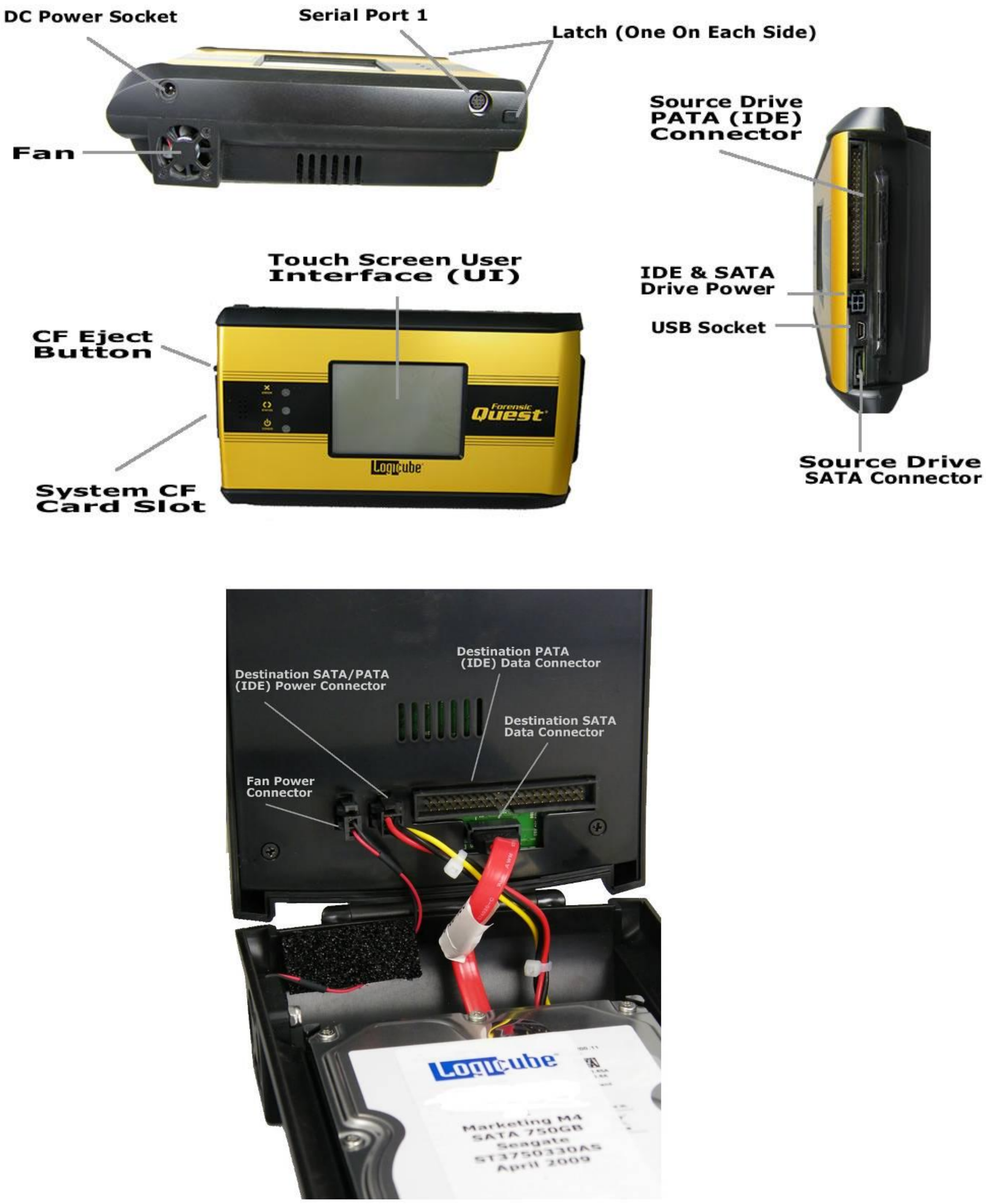


Figure 1, Forensic Quest

2. Getting Started (Fast Start)

Drive Names and Locations

The following naming conventions will be used throughout this manual:

The internal drive is always referred to as **Destination** (or **Evidence**) drive and the outside drive is always referred to as the **Source** (or **Suspect**) drives.

Please see Fig. 2 below:

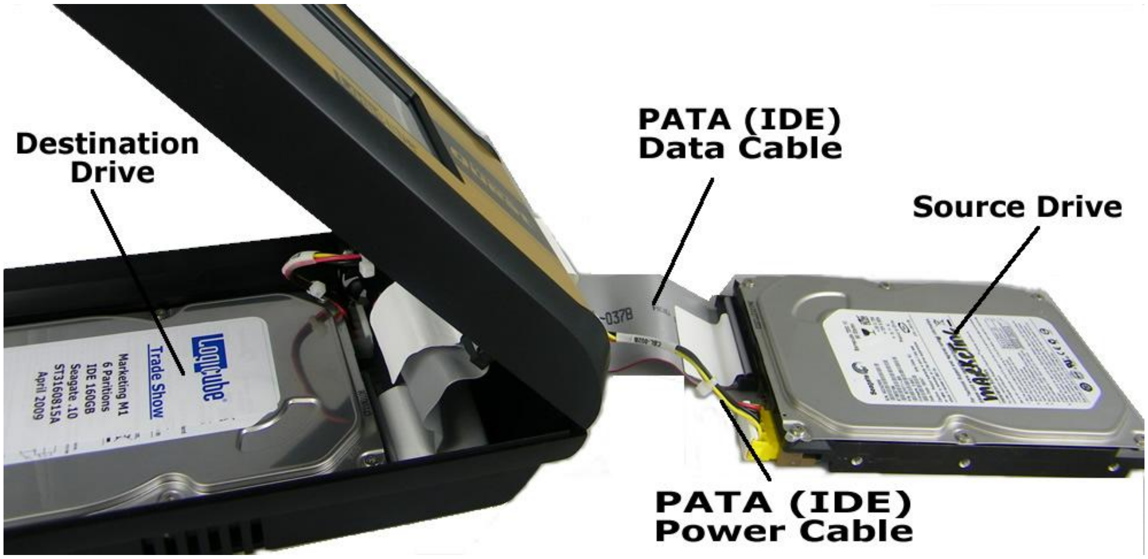


Figure 2, Drive Locations

Setting Up the Logicube Quest

The Logicube Quest is able to detect whether parallel (IDE or PATA) or Serial ATA (SATA) drives are attached to the Source or Destination position. The unit is capable of cloning to a SATA drive from an IDE drive and vice versa (as well as IDE to IDE and SATA to SATA).

NOTE: Never attach both an IDE and SATA drive to a single Source or Destination position. The unit can only handle one drive on each position.

Before applying power perform the steps listed below:

Opening the Logicube Quest

A Destination drive is attached to the inside of the Logicube Quest. Follow these steps to open the unit:

1. Push the two latch buttons on the left side of Quest. See Fig. 3 below.

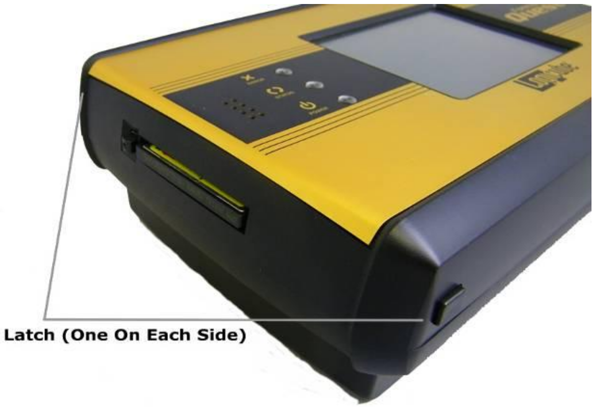


Figure 3, Opening Tabs CF Side.

2. Open the Quest unit as show in Fig. 4 below.

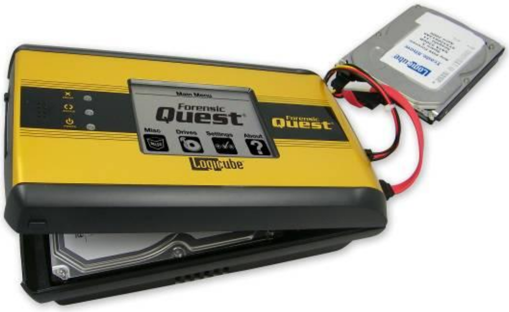


Figure 4, Opening Quest.

Connecting a Parallel (IDE) Drive

1. Open the Logicube Quest by pressing the tabs on the two left corners when facing the unit. You will notice three available connections at the Destination drive position: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the SATA connection.

NOTE: When connecting the data & power cables, ensure that the flat data ribbon loops on the upper side of the destination drive by carefully sliding the drive under both cables. See Figure 5, “Connecting Destination drives to the Logicube Quest through 5” Data/Power cables”.

2. Connect a Destination hard drive and close the Quest
3. Plug in the set of 9” cables, to the connections found on the back of the Logicube Quest.

NOTE: See Figure 6, “Connecting Source drives to the Logicube Quest through 9” data/power cables”.

4. Connect a Suspect drives to these cables.

   NOTE: The Internal drive is always referred to as the **Destination** (or **Evidence**) drive and an outside drive is always referred to as the **Source** (or **Suspect**) drive.

5. Connect the external power supply to the Logicube Quest and power-up the unit. In 6 – 7 seconds, the main menu screen appears.

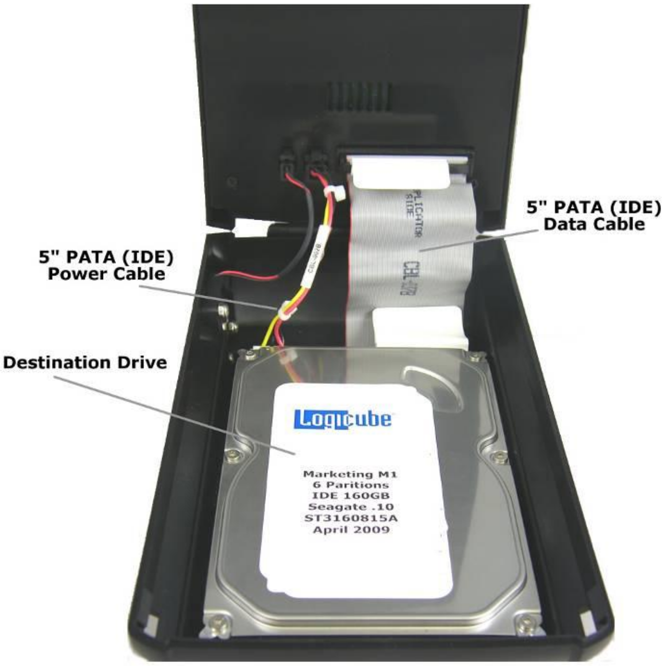


Figure 5, Connecting a Destination drive to the Logicube Quest through 5” Data/Power cables.

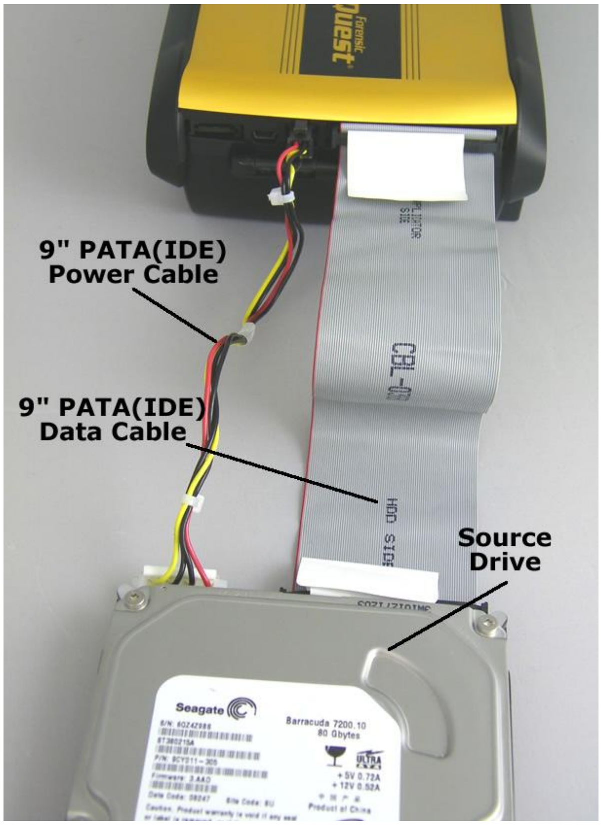


Figure 6, Connecting a Source drive to the Logicube Quest through 9" data/power cables.

NOTE: In order for a capture to work, most PATA drives must be configured as a master drive. If you are going to capture a drive that is used as a slave, move the jumper to the master position. Before moving a jumper note its position so you can return the suspect drive to its original state when the capture operation has been completed.

NOTE: There are several drives that do not follow the requirement stated above. Those drives are:

- **Western Digital** – Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this requirement is for the Western Digital "Xpert" series hard drives (an older manufactured version) where the jumper is set to the master position.
- **Quantum** - The jumper must be placed in the "DS" position. The "DS" position is adjacent to the IDE plug, see figure 7.

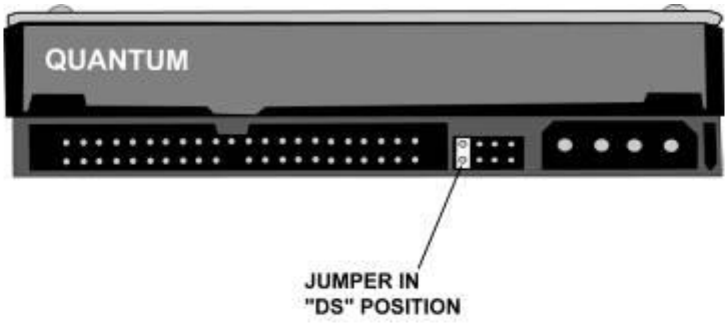


Figure 7, DS Position

Connecting a Serial ATA (SATA) Drive

1. Open the Logicube Quest by pressing the tabs on the two left corners when facing the unit. You will notice three connections for the Destination drive position: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the SATA connection.

   NOTE: The UDMA drive data and power cables must be removed from the Quest when a SATA drive is connected.

   NOTE: See Figure 8, “Connecting SATA Destination drives to the Logicube Quest”.

2. Connect a Destination hard drive and close the Logicube Quest.
3. Plug in the long SATA cable to the connections found on the back of the Logicube Quest.

   NOTE: See Figure 9, “Connecting SATA Source drives to the Logicube Quest through a 9” SATA cable”.

4. Connect the Source drive to this cable.

   NOTE: The internal drive is always referred to as the **Destination** (or **Evidence**) drive and the outside drive is always referred to as the **Source** (or **Suspect**) drive.

5. Connect the power supply to the Logicube Quest and power-up the unit. In 8-9 seconds, the main display appears.

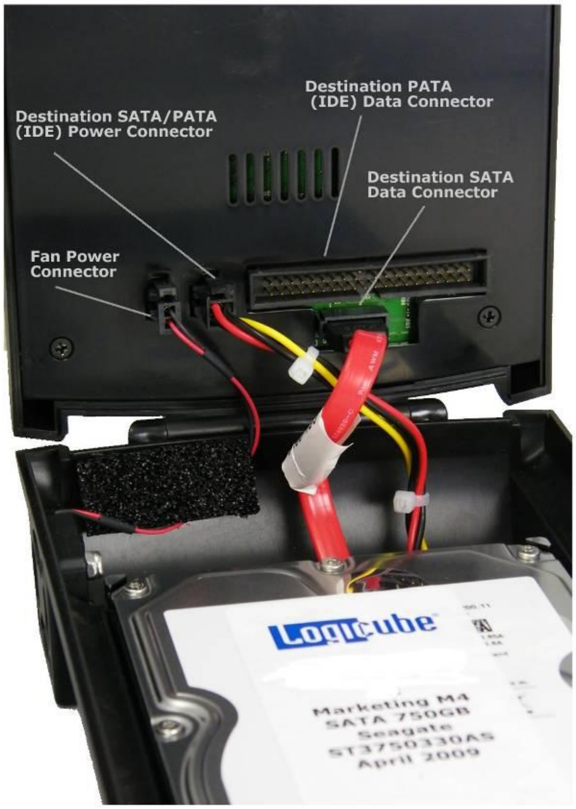


Figure 8, "Connecting SATA Destination drives to the Logicube Quest".

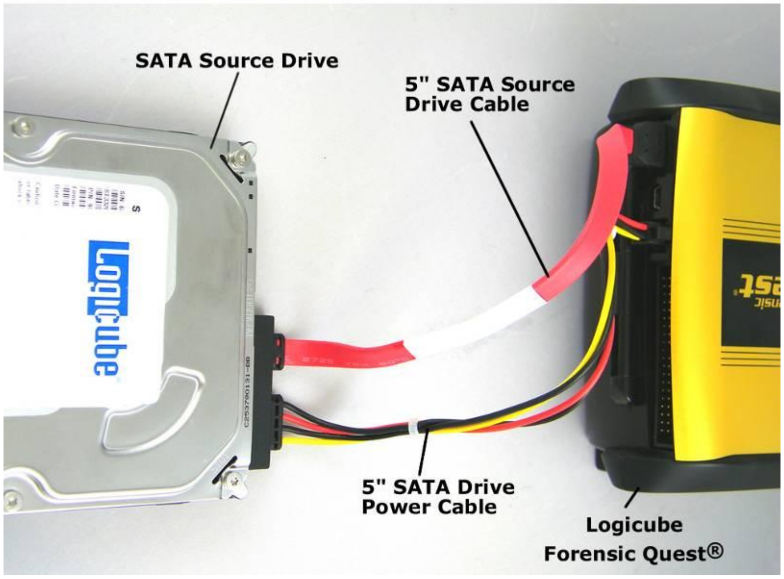


Figure 9, Connecting a SATA Source drive to the Logicube Quest through a 9" SATA cable.

Connecting other types of drives

Logicube sells specialized adapters that allow other types of drives to be connected to the Logicube Quest. Such drives include 2.5” laptop drives, 1.8” laptop drives (e.g. Toshiba “iPod®” drives, and USB drives.

Other specialized adapters are also available. If you are unsure about the type of drive that you have, please contact Logicube Technical Support for assistance.

NOTE: SCSI and SAS drives cannot be connected directly to the Logicube Quest.

The User Interface

The user interface (UI) has been re-designed with the professional in mind. It is fast, responsive, and to the point; which means it requires very few keystrokes to achieve a desired action.

NOTE: Please refer to Fig. 10 as you read the information below.

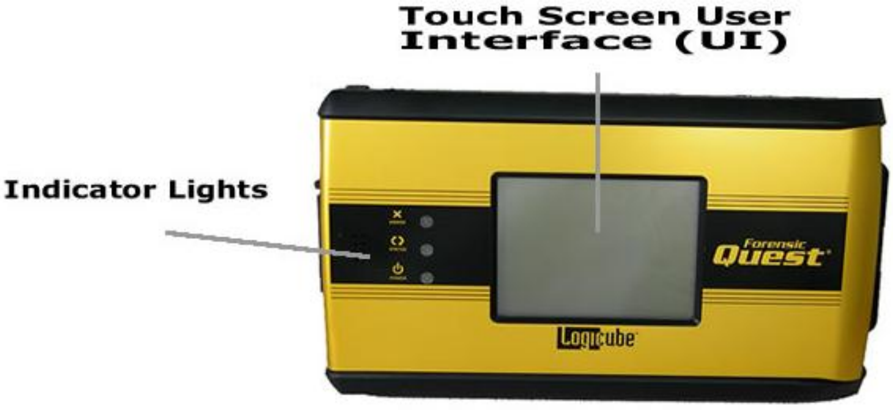


Figure 10, Interface and Indicator Lights

Touch Screen

The Quest features an LCD Touch Screen that allows the user to quickly input commands. This screen replaces all of the buttons that were present on older Logicube forensic products. The screen is bright and easy to read.

Calibrating the Touch Screen

There may be times when the user wants to recalibrate the Touch Screen. The procedure for this is very simple as outlined in the procedure below:

1. Unplug the Quest to turn it off.

2. Press and hold one finger on the screen then plug the Quest back in.
3. After approximately 6 seconds release your finger from the screen and the unit will boot to a screen that reads “Touchpad Calibration. Please touch square with finger (1/5)”.

   NOTE: You can also calibrate the touch screen with a stylus or the dull plastic tip of a writing instrument. Do not use any writing instrument that will leave marks on the unit.
4. Look for a square at the top of the screen. Touch the square when it is located.
5. Repeat the previous step four more times. The unit will count each time the square is pressed correctly. It will count (1/5), (2/5), etc.
6. Once the screen has been calibrated, it will reboot to the Main Menu Screen.

Key Icons on the Touch Screen

The Quest features two icons that are located on the right side of the touch screen display. These icons are available whenever who want to Start an operation or Back out of screen.

Start– Press it to begin a cloning operation using the current settings; press the Abort icon in mid process to abort the process.

Back - This button is used to go “up” in the menu system or to cancel out of a given operation.

Abort – press the Abort icon in mid process to force the process to abort.

Indicator Lights

The indicator lights are located to the left of the touch screen.

The **POWER** indicator light remains on while the Logicube Quest is receiving power.

The **STATUS** indicator is lit during cloning operations and any operation that accesses the Source or Destination drives. They will flash as data is transferred from Source to Destination.

The **ERROR** light will come on if a problem is encountered during cloning or any other operation. If this occurs, check the screen for an error message and instructions on what to do next.

3. Drive Capture Modes and Settings

Main Screen

The main menu screen appears when the Logicube Quest is first powered up. It displays the Title Screen and four menu options: **About**, **Drives, Settings** and **Misc**.

About

Tap the About Icon to display the serial number of your unit along with the software and firmware versions that are loaded. In addition, the About screen provides contact information for Logicube Technical Support.

To return to the main menu, simply press the Back Icon at any time.

Drives

Tap the Drives Icon. Another screen will come up asking you to select Either S1or D1. Make your choice by tapping the desired drive's Icon. The unit will then access the drive selected and report back the drive's model number, capacity, geometry and other information.

To return to the main menu, simply press the Back Icon at any time.

Settings

About – Tap the Settings Icon to access the settings screen.

NOTE: All of the features available in the Settings menu are explained starting with the next section.

Misc

Tap the “Misc” Icon to access the following functions:

- Manage Settings
- Manage Destination
- Authenticate Trail
- Debug
- SCSI/SAS Adapter
- Install Options
- Language

These options are explained in more detail under **Section 4: Other Modes**.

Modes of Operation

The Logicube Quest supports two different operations to clone data from a suspect drive. They are **Mirror Capture** and **DD Image Capture**. These modes are found in the Mode Setting Menu along with several other operations. The different modes of operation are briefly described below.

NOTE: Each time the Logicube Quest is powered on, the cloning mode and preference settings are returned to the last saved settings.

The following Modes of Operation are found in the Mode Setting Menu:

- **Capture** – This process captures all data from the source drive to the destination drive. This mode is also called a “Native Capture” or “Mirror Capture since data is captured at the sector level to the destination drive.
- **DD Image** – This mode of Capturing creates a sub-directory per drive captured, with DD style files of size 650 MB, 2GB or 4GB each. These files are directly accessible by popular Forensic analysis software tools, such as, Encase, FTK, and iLook.
- **Drive Defect Scan** – This operation performs a surface scan of **th**e drive media using the drive controller to verify the media, and detect bad or “weak” sectors. This mode is described in **Section 4. Other Modes**.
- **Wipe Destination**– This is used to erase all data on the destination drive prior to a Native

Capture. This mode is described in **Section 4: Other Modes**.

- **Calculate HASH** – This is used to compute SHA-256 or MD5 values of the source, destination or File on the Destination drive at extreme speeds, and is useful for an "after the fact" verification of a drive. This mode is described in **Section 4: Other Modes**.
- **USB –** This mode is used to connect the Quest to a PC through the USB port. This mode also needs to be engaged when attempting a capture through the USB port. This mode is described in **Section 6: USB Connection**.

Capturing a Drive

Connect the drives as previously described. Make sure the destination drive is larger in capacity than the suspect drive (source drive).

NOTE: For Mirror Capture, the Source and Destination drives can be the same size.

To perform a Mirror Capture

1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From the Main Screen, tap the Settings Icon to enter the Settings menu.
3. Tap the Capture Icon.
4. Tap the Mode Icon and choose the configuration that is best suited for your cloning session.
5. Scroll through the other optional preferences – Verify, On Error and Speed. Modify them as needed by tapping the different settings for each.

   NOTE: See Optional Preference Settings in this section for additional information on these preference settings.

6. Press the <Start> icon.

   NOTE: At this point you may see a message indicating…User attention required: Continuing will overwrite a portion of your destination drive. Are you sure? The normal answer to this question is YES provided you are confident that the

Destination drive does not contain any suspect data.

7. Quest will access the CF Drive, then the following message will appear: "Enter Log file name and Press OK:"
8. Select alphanumeric characters on the touch screen and enter a Log file name of 8 characters or less. Scroll through Upper Case, Lower Case, Numbers & available characters using Alt in the top left corner.
9. Press the OK icon in the top right corner when finished.
10. If the Destination drive has not been erased with the Wipe Destination Mode, the unit will ask if you wish to erase the Destination drive. Choose <Yes> or <No>. If <Yes> is chosen, the unit will completely wipe the destination drive before it begins to capture data. This process adds significantly to the duration of the capture session.

    NOTE: The final capture report will state whether or not the Destination drive has been properly erased.
11. After all sectors have been captured, if the destination drive was not erased, the unit will ask if you wish to erase the remainder of the Destination drive. Choose <Yes> or <No>. If <Yes> is chosen, the unit will completely wipe the rest of the destination drive.
12. The unit will "Mirror" Clone every readable sector from the Suspect drive to the Destination drive, whether or not it contains data.

    NOTE: The final capture report will state whether or not the Destination drive has been properly erased.
13. A copy of the Final Capture Report is written to the CF Drive. It is titled <Log file name>.LOG. The report can be accessed and printed from Windows, if the Quest unit is connected to a PC via USB.

    NOTE: Refer to **Section 7 *Printing Options*** for printing instructions.
14. The capture ends with a "Capture Successful!" message. When Mirror Capture is set to hash SHA-256 or MD5 the overall hash value for the Source drive will also be displayed on the screen.

Special Settings for Mirror Capture Mode

The settings below are used in Mirror Capture mode:

Verify Disk or File

For Mirror Capture Mode, the Verify Setting has some optional settings. Available selections are:

NONE

MD5 This verification setting uses special hardware to compute 128 bit MD5 hash values.

MD5 + V - This setting uses special hardware to compute the MD5 hash values at an extremely fast rate. It also performs read-back and comparison of each block of data as it is captured.

SHA256 - This verification setting uses special hardware to compute the SHA-256 hash values.

SHA256 +V - This setting uses special hardware to compute the SHA-256 hash values at an extremely fast rate. It also performs read-back and comparison of each block of data as it is captured

File Size

This setting allows the user to choose the size of captured DD Image files. The choices are:

650MB – Image files of this size can be archived on a CD-ROM.

2GB – Image files of this size can be archived on Flash Memory cards or Thumb Drives.

4GB – Image files of this size can be archived on larger Flash memory / USB drives or a DVD-ROM.

To Perform a DD Capture

Connect the drives as previously described. Make sure the destination drive is larger than the suspect (Source) drive.

1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From the Main Screen, tap the Settings Icon to enter the Settings menu.

3. Tap the DD Capture Icon.
4. Tap the Mode Icon and choose the configuration that is best suited for your cloning session.
5. Scroll through the other optional preferences – Verify, File Size, On Error and Speed. Modify them as needed by tapping the different settings for each.

   NOTE: See Optional Preference Settings in this section for additional information on these preference settings.

   NOTE: For DD Image Capture the total number of DD files that can be saved to the Compact Flash™ drive is limited to a maximum of 512. As soon as a DD Image Capture is initiated Quest checks the size of the source drive and determines if the total number of DD image files will be less then 513 based on the DD image File Size selected.

   If you see this message **"DD [650MB] will result in incomplete capture. Please increase DD file size."** Quest has determined that the maximum number of files has been exceeded. If this occurs adjust the File Size in the DD Image Capture Menu to either 2 GB or 4 GB chunks and restart the DD Image Capture.
6. Press the **<Start>** icon.

   NOTE: At this point you may see a message indicating…User attention required: Continuing will overwrite a portion of your destination drive. Are you sure? The normal answer to this question is YES provided you are confident that D1 does not contain any suspect data.
7. The Destination Drive needs to be formatted before data capture is possible. If it hasn't been formatted yet, a prompt will come up. Choose <Yes> to format the drive.

   NOTE: See **Section 4: Other Modes** for more information on managing the Destination drive.
8. The next screen prompts you to select alphanumeric characters on the touch screen to enter a Case file name. File names of up to 8 characters are allowed following traditional DOS naming conventions.

   NOTE: If a Case file already exists on the destination drive (i.e. from a previous DD

Image capture) the unit will not allow you to enter the same file name again.

9. A sub-directory (by the same name) will be created under the root directory on the destination drive.
10. The capturing process will create as many files as necessary within this sub-directory, with increasing extension numbers (e.g. my_disk.001, my_disk.002, etc.)
11. At the end of the process, a file with the **.log** extension is created and placed in the same sub-directory. The file is also written to the Compact Flash™ memory. It includes (among other things), the SHA-256 or MD5 Hash values of all captured DD files or the entire Source Drive. Refer to the **Special Settings** section below.
12. The capture ends with a “Capture Successful!” message.

NOTE: Refer to **Section 7 *Printing Instructions*** for information regarding report printing.

Special Settings for DD Image Mode

The settings below are used in DD Capture mode:

Verify Disk or File

For DD Image Capture Mode, the Verify Setting has some optional settings which are not available in any other mode. Available selections are:

NONE

MD5-FILE - This verification setting uses special hardware to compute the MD5 values for each individual DD Image file.

MD5-FILE + V - This setting behaves like File, except that it also reads back captured data and compares it to the Source drive.

MD5-DISK - This setting uses special hardware to compute the MD5 values for the entire Source drive.

MD5-DISK + V- This setting behaves like Disk, except that it also reads back captured data and compares it to the Source drive.

SHA256-FILE - This verification setting uses special hardware to compute the SHA-256 values for each individual DD Image file.

SHA256-FILE + V - This setting behaves like File, except that it also reads back captured data and compares it to the Source drive.

SHA256-DISK - This setting uses special hardware to compute the SHA-256 values for the entire Source drive.

SHA256-DISK + V- This setting behaves like Disk, except that it also reads back captured data and compares it to the Source drive.

File Size

This setting allows the user to choose the size of captured DD Image files. The choices are:

650MB – Image files of this size can be archived on a CD-ROM.

2GB – Image files of this size can be archived on Flash Memory cards or Thumb Drives.

4GB – Image files of this size can be archived on larger Flash memory / USB drives or a DVD-ROM.

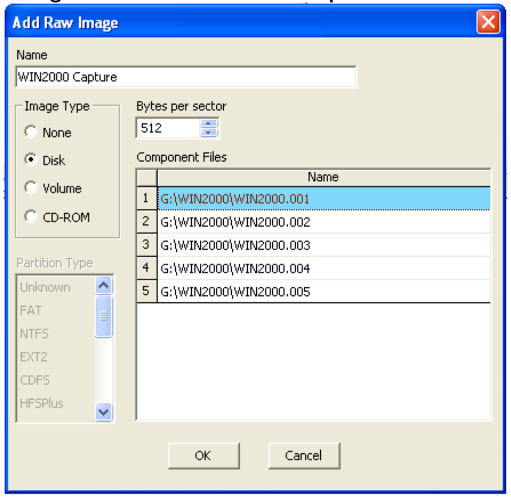
Loading DD Image files into Encase™

Once the DD Image files are captured to a Destination drive, they can be easily loaded into a Forensic Investigative tool like Encase™.

NOTE: These instructions are for Encase™, by Guidance Software. Other Investigative software products may follow a similar procedure. Consult your software's manual for more information.

1. Attach the Quest to the PC via the USB Port, (please refer to the procedure for "Destination Drive Management" on page 45.
2. Open Encase™ and start a new case.

3. Go to **File** – **Add Raw Image**. The "Add Raw Image" Window will come up.



Name: WIN2000 Capture

Image Type:
- ○ None
- ● Disk
- ○ Volume
- ○ CD-ROM

Bytes per sector: 512

Partition Type: Unknown, FAT, NTFS, EXT2, CDFS, HFSPlus

Component Files

	Name
1	G:\WIN2000\WIN2000.001
2	G:\WIN2000\WIN2000.002
3	G:\WIN2000\WIN2000.003
4	G:\WIN2000\WIN2000.004
5	G:\WIN2000\WIN2000.005

4. Set **Image Type** to **Disk** and leave **Bytes per Sector** at **512**.

5. Right-click in the **Component Files** box. Choose "**New - Insert**".

6. Browse to the location of your DD Image files, they should be in the drive labeled "Logicube_dd" and located in a folder with the case name that you entered during the capture session.

7. Select all DD Image files this way: Select the last file and then hold down the SHIFT key while clicking the first file.

8. Click "Open" to add the files to the "Add Raw Image" box.

9. You may need to click and drag the files up and down in order to put them in descending order (i.e. *.001, *.002, *.003, etc.).

10. Click **OK**. Encase will then put the files back together into a complete image of the entire disk.

Optional Preference Settings

All of the preference settings below are available for Mirror and DD Image Capture modes:

Mode

The Mode option allows the Quest to be configured to clone from 1 Source to 1 or 2 Destination drives. Two different cloning configurations are possible:

S1 (Source) to D1 (Destination) – This mode allows one Source drive to be captured to one Destination drive. It is the default mode setting.

S1 to D1 & D2 – This mode requires an Optional 1 to 2 Forensic Adapter that will allow the Quest to clone the contents of one Source drive to two Destination drives. This is ideal for making a copy to keep in evidence and an extra copy for the investigation.

NOTE: Section 8 - Optional Peripherals contains additional information regarding use of the 1 to 2 Forensic Adapter.

Verify

The Verify option is provided to add an increased level of confidence in the capture process. The choices are: **HASH**, **HASH + V** and **NONE**.

NOTE: When using S1 to D1 & D2 mode, Verify will only be performed on D1.

HASH - This setting uses special hardware to compute 256-bit SHA-256 or 128-bit MD5 values at an extremely fast and accurate rate.

HASH + V- This setting behaves like **HASH**, except that it also reads back captured data and compares it to the Source drive. This setting is recommended to ensure the accuracy of the hash values.

> **NOTE:** The "+ V" settings will increase the cloning time of a capture session.

NONE - No verification. This setting is only recommended for non-Forensic cloning operations.

> **NOTE:** Without verification, bad or weak sectors on the Destination drive will not be detected. This could cause the copy to be invalid.

Speed

The speed setting provides the option to set the speed at which an operation will be performed at.

UDMA-5 - With UDMA-5 selected, the software performs a test to determine the fastest speed setting that the drives will tolerate while streaming data from one drive to another.

When errors are encountered using UDMA-5, all lower speed grades will be tested (i.e. UDMA 0-4, PIO-AUTO PIO-PIO Medium and PIO-SLOW) in an effort to complete the capture.

UDMA-4 - Force the unit to use at most this speed. Set the unit to this mode in some rare situations where one or both drives do not support the higher speeds, and “misbehave” during our automatic speed benchmarking

UDMA-3 - Same as **UDMA-4.**

UDMA-2 - Same as **UDMA-4.**

UDMA-1 - Same as **UDMA-4.**

UDMA-0 - Same as **UDMA-4.**

PIO-Auto (PIO-4) – Force the unit to use this as the highest speed (PIO-4). Set the unit to this mode in some rare situations where one or both drives do not support higher speeds, and “misbehave” during our automatic speed benchmarking.

PIO-Medium – This is a fixed value that almost all drives will tolerate. It will result in copying speeds from about 200 to over 500 MB per minute depending upon the characteristics of the drives.

PIO-Slow – This is a speed value that all drives will be able to tolerate. It supports copying speeds from 100 to over 300 MB per minute depending on the characteristics of the drives.

NOTE: Use the MEDIUM or SLOW modes if you encounter drive “time-outs” or if you are capturing older drives. Many older 2.5” notebook drives require the PIO-SLOW setting.

On Error

The On Error setting determines the behavior of the unit in the case where bad spots are detected on the source (suspect) drive. This setting has four options, which include:

Skip - This is the default setting. Skip will allow the Quest to continue by stepping over the bad sector.

Retry - Retry will instruct the Quest to make several attempts to read data from the damaged area of the drive. The number of retry attempts is set to 50 by default.

Recover - Recover will attempt to recover as many bytes of data as possible from each bad sector that is encountered

Abort - This mode will cause the Quest to halt if an error such as a bad suspect drive sector is encountered.

NOTE: Data in any skipped sectors will NOT be copied to the destination drive. The corresponding sector of the Destination drive will instead be “padded” with zeroes. The padded sector will then be included in the final SHA-256 or MD5 values.

ADDITIONAL NOTE: The absolute location of each skipped sector will also be listed on the final Capture Report. The first 200 bad sectors will be recorded, after which the unit will continue to skip bad sectors but it will not record their absolute locations. The final capture report will show the total number of sectors skipped.

Option	Action	Time to complete
Abort	A bad sector aborts the cloning operation	Immediate
Skip (default)	Skips the bad sector	Fast
Retry	Attempts several retries to recover data of sector, then skips	Slower
Recover	Attempts a full-blown recovery algorithm, then skips	Very slow

Table 1, Error settings

NOTE: When capturing a Source drive that is known to have many bad sectors, the speed should be set to PIO-AUTO. Also, if the drive is captured or scanned multiple times, the SHA-256 or MD5 Hash value of each session could differ. This is because some bad sectors will read intermittently.

Capturing Data from HPA and DCO Configurations

Some PC manufacturers will employ a utility that creates a HPA or DCO configuration on a hard drive. These configurations are designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the PC BIOS.

HPA – Or Host Protected Area can limit the size of a hard drive, but it can also change many other settings such as speed and S.M.A.R.T. status.

DCO – Or Device Configuration Overlay limits the size of a drive only. For example, a 60GB drive can be made to look like a 30GB drive to a PC.

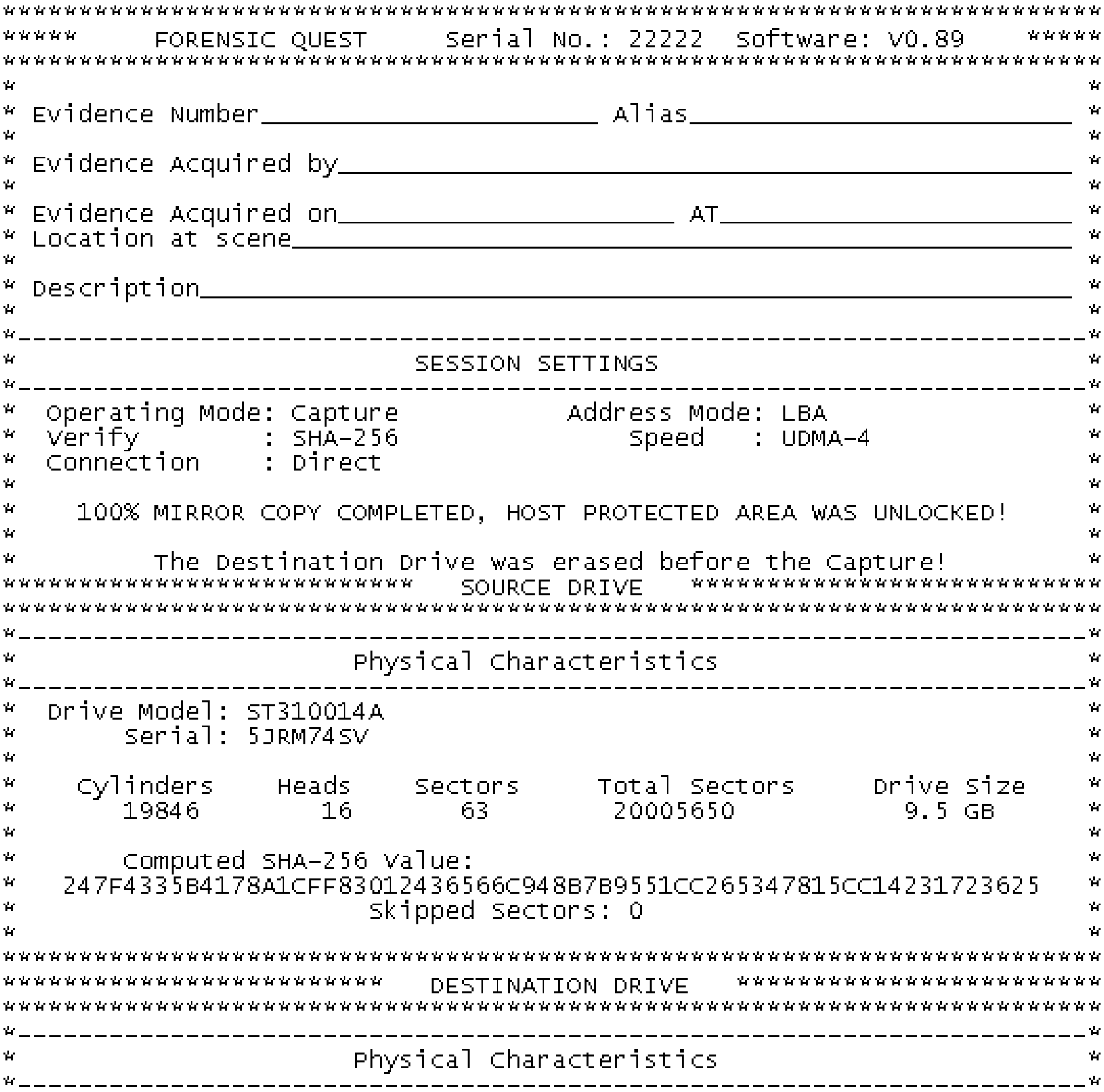
The Quest is able to unlock and capture data from both HPA and DCO configurations. The Quest will then re-lock the DCO. HPA's are relocked when the Source drive is hard-booted after capture.

The Final capture report is also able to report any HPA and/or DCO that is found.

The report only shows the existence of an HPA and if it was unlocked.

The report also shows the existence of a DCO and if it was unlocked and captured. It also lists the maximum LBA, size and speed setting of the DCO

NOTE: HPA and DCO can only be performed in Native Capture mode. If hash is selected the MD5 or SHA-256 digest will show up on the display upon completion of the Capture. HPA and DCO reports look similar to the examples provide below:



```
************************************************************************
*****     FORENSIC QUEST     Serial No.: 22222  Software: V0.89    *****
************************************************************************
*                                                                      *
* Evidence Number______________________ Alias_________________________ *
*                                                                      *
* Evidence Acquired by________________________________________________ *
*                                                                      *
* Evidence Acquired on______________________ AT_______________________ *
* Location at scene___________________________________________________ *
*                                                                      *
* Description_________________________________________________________ *
*                                                                      *
*______________________________________________________________________*
*                          SESSION SETTINGS                            *
*______________________________________________________________________*
*  Operating Mode: Capture           Address Mode: LBA                 *
*  Verify        : SHA-256               Speed   : UDMA-4              *
*  Connection    : Direct                                              *
*                                                                      *
*    100% MIRROR COPY COMPLETED, HOST PROTECTED AREA WAS UNLOCKED!     *
*                                                                      *
*         The Destination Drive was erased before the Capture!         *
***************************   SOURCE DRIVE   ***************************
************************************************************************
*______________________________________________________________________*
*                      Physical Characteristics                        *
*______________________________________________________________________*
*  Drive Model: ST310014A                                              *
*       Serial: 5JRM74SV                                               *
*                                                                      *
*    Cylinders    Heads    Sectors     Total Sectors     Drive Size    *
*       19846       16       63       20005650           9.5 GB        *
*                                                                      *
*       Computed SHA-256 Value:                                        *
*   247F4335B4178A1CFF83012436566C948B7B9551CC265347815CC14231723625   *
*                        Skipped Sectors: 0                            *
*                                                                      *
************************************************************************
*************************   DESTINATION DRIVE   ************************
************************************************************************
*______________________________________________________________________*
*                      Physical Characteristics                        *
*______________________________________________________________________*
```

Figure 11, HPA Sample Report

HPA and DCO configurations can only be detected on the Source drive. They cannot be seen on the Destination drive. The following Modes are able to detect, unlock and work with data inside HPA and DCO configurations when the drive is in the Source position:

- Drive Info
- Capture
- DD Image Capture
- Drive Defect Scan

4. Other Modes

Introduction

This section discusses other options that are found in the Settings menu. They are **Drive Defect Scan**, **Wipeclean,™ Destination** and **HASH Scan**. This section also discusses the options in the **Misc Menu** accessible from the Main Screen.

NOTE: **USB Mode** is discussed in **Section 6**.

Settings Menu Options

Drive Defect Scan

This function performs a surface scan of the drive media using the drive controller to verify the media. It is designed to look for bad sectors, weak sectors or weak spots, which it reports at the end of the scan.

Procedure

1. From the Main Screen, tap the Settings Icon.
2. Tap the Drive Defect Scan Icon.
3. Tap the "Drives" Icon. Choose one of the following drives: S1 or D1.
4. Tap the "Speed" Icon. Here you have two choices:
   - **FAST** (default): This mode does a single surface scan of the drive.
   - **SLOW**: This mode performs three surface scans in a row to better check for bad or weak sectors.
5. Press the **Start icon** to start the scan.
6. Quest will access Compact Flash™ memory, then the following message will appear: "Enter Log file name and Press OK:"

7. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the OK icon when finished.
8. When finished scanning, the Quest will display the number of bad or weak sectors found on the drive. A copy of the session report will also be copied to the internal flash memory as <Log file name>.LOG.

   NOTE: Refer to **Section 7 *Printing Instructions*** for information regarding report printing.

Wipe Destination

This function is the process that erases or wipes all existing information from the surface of the Destination drive. It is a good idea to erase the drive prior to performing Mirror captures. It ensures that no old data remains on the drive, to be later confused as evidence. Information regarding performing a wipe to DoD specifications can be found in the Other Settings section under Manage Destination.

Many newer drives will also support **Security Erase Mode**, which is a much more automated process for wiping data. This mode sends “Security AT” commands to the Destination drive, which allows it to wipe at a very high rate of speed. The unit will automatically switch to Security Erase if it is supported by the attached drives.

NOTE: If Security Erase is not supported by the destination drive we recommend the use of a scratch drive in conjunction with Wipeclean™. Instructions for creating and using a scratch HDD are located on page 41.

NOTE: Security Erase will not run as part of a Mirror Capture session. Ordinary Wipeclean™ mode is used instead.

Procedure

1. From the Main Screen, tap the Settings Icon to enter the Settings menu.
2. Tap the Wipe Destination Icon.
3. Tap the “Drives” Icon. Choose D1.
4. Tap the “Speed” Icon to set the desired UDMA or PIO speed.
5. Set the Signature setting to the desired position, there are two choices:

  - **YES**: Writes a small signature to the drive every logical cylinder. During a later capture session, this signature tells the Quest that the drive(s) have been correctly erased.
  - **NO** (Default): Leaves the signature off the drive. The Quest will not detect that the drive has been erased.

6. Press the <Start> icon to begin wiping.
7. The Quest will access Compact Flash™ memory, then the following message will appear: "Enter Log file name and Press OK:"
8. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the OK icon when finished.
9. Quest will automatically detect whether or not the Destination drive will support a Security Erase. If not, then the Quest will perform an ordinary Wipeclean™ operation based on the settings chosen by the user.

   NOTE: Just before the wipe starts you will see a message on the UI that says "Set Dest PW to Spaces" This means that a Password key command has been sent to retrieve the security erase support status of the destination drive. No user action is required. If the Quest performs a Security Erase, it will do a rough estimate of the Time Remaining. This estimate will appear above the progress bar while an "Elapsed Time" counter will count up the actual erase time.

   NOTE: The Progress bar will appear to "hang" at 99% if the actual erase time is longer than the estimated time. The elapsed time counter will continue to run and the Status light will keep blinking until the wipe is finished.
10. When finished, the Quest will display the following message "Erase Successful! Drive successfully erased!" A copy of the session report will also be copied to the Compact Flash™ memory as <Log file name>.LOG.

NOTE: The operation will abort with an error message if bad sectors are encountered on the Destination drive.

NOTE: Refer to **Section 7 *Printing Options*** for information regarding report printing.

HASH

This mode computes the SHA-256 or MD5 Hash values for a given drive (S1 or D1). It can also scan individual files (on the Destination Drive).

When using this mode, hard drives attached to the Source position (outside) will hash at PIO-AUTO speeds. Hard drives attached to the Destination position (inside) will hash at UDMA-4 speeds.

Procedure

1. From the Main Screen, tap the Settings Icon to enter the Settings menu.
2. Tap the Hash Scan Icon.
3. Tap the “Drives” Icon. Choose one of the following drives: S1, D1 or, File on D1.
4. Tap the Hash verification icon and choose either SHA256 or MD5.
5. Tap the “Speed” Icon to set the desired UDMA or PIO speed.
6. If a certain number of sectors need to be scanned, press the “Size” setting icon. Use the keypad to enter a size in number of sectors. Press the OK icon to confirm.
7. Press the <Start> icon to begin the scan.
8. The Quest will access the CF Drive, then the following message will appear: “Enter Log file name and Press OK:” Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Scroll through Upper Case, Lower Case, Numbers & available characters using Alt in the top left corner.
9. Press the OK icon in the top right corner when finished.

   NOTE: The operation will abort with an error if bad sectors are found on the drive.
10. When finished, the Quest will display the SHA-256 or MD5 Hash values. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.

    NOTE: Refer to **Section 7 *Printing Options*** for information regarding report printing.

USB

Please refer to Section 6 (USB Connection) for instructions on USB functionality.

Misc Menu Settings

This section describes the settings that are available under the **Misc Menu** that can be accessed from the Main Screen.

Manage Settings

This Icon brings up a series of Icons that allow you to adjust, save and reset various default settings.

Contrast – Use this setting along with the two Up Down arrow keys to increase or decrease the Touch Screen’s Contrast setting to your desired preference. The contrast setting will be retained in memory by pressing the OK Icon.

Save Settings – Use this Icon to save current configuration settings. Settings that can be saved through power recycle are: Mode, Speed, Verify, On Error, Contrast, Wipe Signature ON/OFF& Defect Scan Speed Fast or Slow.

Factory Settings – Reverts all adjustable settings to the default factory settings.

Logicube Admin – This Icon is used by Logicube and is intended for internal use only.

Manage Destination

This menu is used to prep the Destination drive prior to running a DD Image capture. The available settings are:

Format Dest. – This function formats the destination drive with a single FAT32 partition. This is necessary before DD Image files can be copied to the drive. When Format D1 is activated, the following prompt appears:

“Reformatting the Drive! All data on your internal drive will be lost! Continue?”

Choose <Yes>, the display will say “Zeroing first FAT” and “Zeroing second FAT” as it formats the drive. After a few minutes the drive will be formatted, (the time varies by drive size). Upon completion the display will read “Destination format completed”.

Choose <No>, the display will then go back to the Format Dest. menu.

Scan Disk – This function checks the Destination Drive for proper formatting. It also makes sure that the FAT32 partition is not corrupt. It functions much like Microsoft Windows Scandisk or Chkdsk.

Choose <Scan D1> to run Scan Disk. Upon completion, Quest will display a list of any errors found.

Browse Dest. – If the Destination drive is formatted with a FAT32 partition, Browse Destination will allow the user to navigate directories on the drive. It will also show the size of files on the drive. Use the Arrow and Select Icons to navigate the directory.

DoD Wipe D1 – In compliance with DoD M-5220 Quest will wipe a destination as follows: The drive will be wiped with all 0’s followed by all 1’s THREE consecutive times; after this the final value of 0xF6 will be written to all locations on the drive. To summarize, Quest will write the following 7 patterns to all the locations on the destination drive: all 0’s, all 1’s, all 0’s, all 1’s, all 0’s, all 1’s, 0xF6

The Icon for DoD Wipe D1 is located under Misc. and the Manage Destination Icon. Once pressed, Quest will determine if the patterns necessary to complete a DoD Wipe of the destination drive already exist on the current source drive. If the patterns are present Quest will request a log file name before it performs a DoD Wipe of the destination drive.

If the necessary data patterns are not present on the current source drive you will be asked to install a temporary scratch drive in destination location D1 so that Quest can write the required data to the scratch drive. If you receive the message “Unable to use a Source drive for erasing the Destination”. “Please build a scratch drive using the provided utility". To do this, perform the following:

1. Install an unimportant scratch drive in position D1.
2. Press the Build Scratch Drive Icon.

Once this step is complete the user is prompted to do the following:

1. Install the newly created scratch drive in position S1.
2. Reinstall the drive that is to be DoD Wiped in position D1.
3. Press the DoD Wipe D1 Icon again and the DoD Wipe process should begin immediately.

Authenticate Trail

This mode is used to verify the authenticity of a session report that has been written to the internal flash memory. It is designed to check the report for alteration. It verifies a proprietary Hash value that is written to the end of each report at the time of creation.

Procedure

1. From the Main Screen, tap the Misc Icon.
2. Tap the Authenticate Trail Icon.
3. The Quest will display a list of the Log files that are on the Compact Flash™ drive.
4. Using the arrow keys on the display scroll to the file name and press the OK icon
5. If the report has not been altered, the message will read "Log file authenticated. Press any key to return".
6. If the report has been altered in any way, the message will read "Log File not authenticated. Press any key to return".
7. Press the Back Icon to return to the Main Screen.

Debug

Use this setting to turn the Debug reporting tool on and off. This setting is used in conjunction with the Serial Port and a terminal link program or the Compact Flash Drive. The default setting for Debug is OFF. Debug should only be turned on when the user is directed to do so by Logicube Technical Support.

Press this Icon to select Serial Debug.

Press this Icon to store the Debug log to Compact Flash.

Install Options

As optional features become available use the install options Icon to activate purchased options by pressing Misc. and the Install Options Icons on Quest.

Enter the alphanumeric option code provided at time of optional purchase using the touch screen display. The option will automatically become available.

NOTE: New and improved Quest software will appear from time to time on our web site located at www.logicube.com. Verify your software is up to date by comparing the software revision on the Logicube website with the software revision listed under About on the main menu.

SCSI/SAS Adapter

The SCSI and SAS Adapters are designed to attach directly to the Logicube Forensic Quest.

Functionally each adapter acts like a pass through device and allows for external connection and capture (one adapter at a time) of SCSI or SAS source drives through the IDE port of Quest.

Info is used to display the Serial Number and current Firmware, BIOS, Kernel and Software revisions for the SCSI or SAS adapter you have connected to the source position of Quest.

BIOS Upgrade is used to upgrade the BIOS of the adapters PCB assembly.

Kernel Upgrade is used to upgrade the OS of the adapter.

FPGA Upgrade is used to upgrade the Firmware of the adapters PCB assembly.

The Application Upgrade Icon is used to upgrade the Capture Application for both the SCSI and SAS adapters. This update will most likely to be performed more frequently than those listed above.

NOTE: Please refer to **Section 8: Optional Peripherals** for information regarding use of the optional SCSI/SAS adapters.

Language

This function allows either English or Chinese (simplified or Traditional) characters on the Talon Enhanced display. Each selection has an option for YES or NO.

From the Quest Main menu, tap the ***Misc*** icon, then tap the ***More*** icon, and finally tap the ***Language*** icon. The following choices will appear:

Simplified Chinese (YES/NO)

Traditional Chinese (YES/NO)

English (YES/NO)

Tap the desired language to toggle between ‘Yes’ and ‘No’. When finished, tap the ***Back*** icon twice to return to the main menu.

6. USB Connection

Introduction

The integral USB port on your Logicube Quest provides connectivity between the unit and its connected drives to any PC with an active USB port. It also ensures zero alteration to Source and Destination drives under any operating system. USB 1.x and 2.0 are supported.

Additionally, drive capturing through the USB port is possible with the USB/Firewire Cloning Software included on a separate CD-ROM with your Quest.

IMPORTANT NOTE: The System CF, card is not write protected. Exercise caution when connecting to the System CF card so that log reports are not deleted.

Minimum Requirements

- A Logicube Quest unit with integral USB port.
- A 586 or better PC compatible computer with CD-ROM drive.
- An active USB port.
- Microsoft Windows 98SE/ME/2000/XP/Vista operating system (for drive access under Windows).
- A bootable CD for USB capture mode entitled Logicube Forensic USB/Firewire Cloning Software.

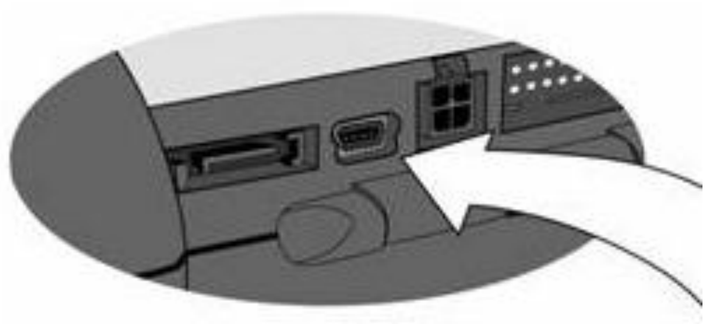


Figure 12, USB Port on Logicube Quest

USB Connection to Windows (for Drive Management)

Please refer to Figure 12 above:

1. Make sure that the desired drive(s) are attached to the Quest
2. Make sure your PC is running Win98 or above.
3. With power applied to Quest connect the USB cable (provided) to a PC USB slot on one end. Do not attach the other end to the Quest yet.
4. From the Main Screen of the Quest, tap the Settings Icon
5. Press the USB Icon
6. Tap the USB Icon and the current drive will appear.
   - **Drive:** Choose one of the following drives to connect: D1 or System CF (Quest's Compact Flash™ memory card).
7. Press Start and Quest will power up the chosen drive. A prompt will appear saying "USB Link Up…"
8. It is now safe to attach the USB cable to the Quest. You should now see some activity on your PC screen, which depends on the operating system.
9. If running XP/VISTA/Windows 7 your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
10. If running 98/98SE you will be prompted to install drivers. At the "have disk…" prompt please point the PC to the drivers CD (provided), and the installation should complete smoothly.
11. The chosen drive is now visible on Windows as an external drive. Any partitions that can be

accessed by your Operating System will be assigned a Drive Letter.

At this point the drive is fully visible to any Forensic analysis tool, such as EnCase, iLook, and FTK. The drive contents, however, cannot be altered in any way. Note that since Windows keeps caching information for every drive, some operations (such as file read), may appear to show changes in file access time etc. but these are purely virtual, and do not change anything on the drive itself.

Removing USB devices

Before physically disconnecting the USB cable and/or shutting down power to the Quest, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB Icon in the system tray (typically at the bottom right of screen).

2. Click the Icon once.

3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently).

4. Press the BACK Icon on the Quest to disengage the USB connection.

Cloning through the USB port

This mode allows the user to clone drives through the USB ports of a PC. The PC drive can only be the Source drive. Both USB 1.x and 2.0 are supported. Typically, the user will boot the computer from the provided boot CD. The CD is equipped with USB drivers and our drive capturing application.

USB Cloning only works with one Source drive cloning to one Destination Drive.

How to set up and use the USB/FireWire cloning software:

1. Follow these instructions to maintain the forensic integrity of the capture. With computer power off, insert the boot CD into the CD-ROM drive or depending on the computers CD-ROM drive you may need to insert the CD as far as it will go so it can be pulled in during power up. Start the computer and immediately enter the BIOS setup menu. This varies by computer but usually requires you to press (F12, F1 for IBM or the Delete key for most generic PC’s) just after startup. Make sure that the PC is set to boot

from the CD-ROM as the first bootable device. Allow the PC to continue booting off of the boot CD in the CD-ROM drive.

2. The Forensic USB Cloning CD-ROM is configured to automatically load the necessary drivers and run the client application. The user will be presented with a User Interface and a menu to select among the various capture options and settings.

   NOTE: A USB or FireWire (FireWire is supported only with the Forensic Dossier) connection must be made between the computer and the Logicube forensic capture device either before or after the Boot CD application starts. The following message will be displayed if the application starts without detecting connection to a Logicube forensic capture device: *Searching for Logicube Forensic Device. Make sure it is connected.*

3. On the Logicube device (Talon Enhanced, Forensic Dossier, Quest or Talon), attach a hard drive to the Destination (D1) position that is larger than the suspect drive you intend to capture.

4. Locate your Logicube device model from the 4 selections below and follow the instructions to set your Logicube device to USB mode:

   - **Talon Enhanced** – From the main menu, tap ***Settings > More > USB/ESATA > USB >*** make sure the ***Drive*** is set to D1 then press the ***START/STOP*** button twice.
   - **Forensic Dossier** – From the main menu, tap ***Settings > More > USB/1394 > USB >*** make sure the ***Drive*** is set to D1 then press the ***START/STOP*** button twice.
   - **Forensic Quest (F-QUEST-2)** – From the main menu, tap ***Settings > USB >*** make sure the ***Drive*** is set to D1 then tap the ***Back*** icon, then tap the ***Start*** icon.
   - **Forensic Talon** – Press the ***SET*** button. Next to Mode press ***SELECT***. Scroll down to ***USB Drive Mode*** and press ***SELECT***. Press the button under **<ATA>** then press the button under **<NO>**. Wait for the unit to prompt you to “attach the USB cable”.

5. Attach a mini USB cable (included with your Logicube device or any mini USB cable) between the Logicube device and PC. The Capture Utility will detect the connection.
6. The PC client software should now detect the presence of the Logicube device you are using. The Cloning software interface will then come up and all available functions will now be controlled from the PC client software application.

NOTE: For DD Captures only, if the destination drive is not formatted with a FAT32 partition, the application will prompt the user and will format the drive accordingly. If there is not enough room in the destination drive for a DD file capture, the application will exit with an error, notifying the user.

7. When either device is connected the application will display a menu containing three columns *PC Source Drives, Partitions and Modes*.

Selectable Capture Modes & Options

- **Native:** This is analogous to a mirror copy of the internal drive of the PC to the Destination. This mode calculates and displays an MD5 Hash value.
- **Native +V:** Capture suspect drive and compute MD5 on the master drive. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. The Capture Utility will display the Total MD5 Hash value on the screen at the end of the capture session.
- **DD-Image-650M:** The Master drive is broken up into (650 MB files) and a MD5 hash is computed on every file (MD5 Hash values are calculated for each DD image). This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-650M+V:** The Master drive is broken up into (650 MB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.

- **DD-Image-2G:** The Master drive is broken up into (2 GB files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-2G+V:** The Master drive is broken up into (2 GB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **DD-Image-4G:** The Master drive is broken up into (4 GB files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-4G+V**: The Master drive is broken up into (4 GB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **Compute Source MD5:** An MD5 hash is computed on the entire internal PC drive. The resulting value is displayed on the screen.
- **Compute Destination MD5:** An MD5 hash is computed on the entire destination drive. The resulting value is displayed on the screen.
- **Erase Destination:** A single pass wipe is performed on the destination drive. For erase destination the Capture Utility reports Total Drive Sectors, Erased Sectors, Erase speed in MB/Minute, Time to Completion and % Complete.

8. Use the arrow keys on your PC's keyboard to navigate through the various settings of the capture utility. Use the ***Enter*** key to make selections and the ***S*** key to start a process.

9. On the left side of the screen you will see a list of up to four available drives. Choose the “Source” drive you wish to capture by scrolling through the selections using the up/down arrow keys on your PC’s keyboard. When your selection is highlighted a brief description of the drive will appear in the middle of the screen. Press ***Enter*** to select a source drive.

10. On the right side of the screen you will see a list of capture modes. You can scroll through the selections using the up/down arrow keys on your PC’s keyboard. Press ***Enter*** to make your selection.

11. Once you have selected the “source” drive to be captured and selected the method of capture press ***S*** to start the data capture. A progress bar will appear on the screen.

NOTE: You may cancel or abort the capture at any time by pressing the *Esc* key. Press any key and by answering *[Y]es* to return to the main menu.

12. Once the capture has been completed a message will pop-up indicating the capture session has completed successfully.

13. If you have selected a capture method with an MD5 Hash the hash values will appear at the bottom of the screen.

NOTE: Except for DD captures, the hash values generated will not be saved if you exit this screen. You must record the hash values before exiting!

14. Upon completion of the data capture press any key and answer ***[Y]es*** to go back to the main screen. To perform a data capture from another source drive, install a new destination drive only if the current destination drive is full or your next capture will be performed as Native. Repeat steps 8 through 14 to perform a subsequent data capture.

15. To exit the Forensic Cloning Software, press the ***Esc*** key and answer ***[Y]es***. A message will display that indicates “You can now remove the CD-ROM”. Some computers will automatically eject the CD at this point. Power down the PC as soon as the CD has been removed from the CD-ROM drive to maintain the forensic integrity of the capture. ***Do not reboot!***

Cloning a Mac using FireWire and the Cloning Software

Follow these instructions to maintain the forensic integrity of a HDD capture from a Mac computer.

You will need a host PC (Non Apple/Mac) with FireWire support to run the USB/FireWire cloning software. Ensure that the Mac is turned OFF.

NOTE: The MacBook Air is not supported at this time.

1. Install a FireWire cable between the host PC running the cloning software and the Apple computer to be cloned.
2. Power up the Mac and wait for the Apple chime and immediately press and hold ***T*** to enter FireWire Target Disk Mode.
3. Load the cloning software CD onto the non-Apple/Mac PC by following instructions 1 through 8 on pages 2 - 4.
4. With FireWire Target Disk Mode already established, the User Interface on the host PC will display the Mac's hard drive in the list of available drives.
5. Continue following steps 9 through 15 on pages 3 and 4.

Additional Notes

- Capture speed depends wholly on the USB and FireWire hardware and the processor speed of the PC. Expected capture speeds are up to 1.4GB/min with verify and up to 1.8GB/min without verify. Your capture speeds may vary.
- 400/200/100 speed FireWire ports are supported. 800 Mbps FireWire is not supported.
- Upon detection of an error the capture will skip the bad sector(s) and write zeroes to the corresponding sector(s) on the destination drive.
- During most operations the capture utility reports Total Drive Sectors Cloned, Speed in MB/Minute, Time to Completion and % Complete.

7. Printing Instructions

Introduction

Printing Reports

Every Capture, DD Imaging, Scan or Wipe operation performed with Quest writes a copy of the session report to the Compact Flash™ Drive. This report can be easily accessed in Windows and printed from a text editor like Notepad.

Print Report Instructions

Hardcopy printouts of the report can be obtained in one of two ways. To manually print a report after the capture session, perform one of the following methods.

Method 1

1. Eject and remove the Compact Flash™ drive from Quest and install the drive into a CF media card reader connected to a PC.
2. Reports are written to the root of the CF Drive. They are titled <Log file name>.LOG.
3. Accessed the log file name in Windows, open and print the report from a text editor like Notepad.

Method 2

1. From the main menu tap Settings, USB and change the drive to System CF.
2. Tap the Back Icon and press Start. Once you see the message USB Link Up… connect a USB cable between Quest and

an available USB port on your Windows based computer.

3. The Compact Flash™ drive will become visible under My Computer.

4. All Reports are written to the root of the CF Drive. They are titled <Log file name>.LOG.

5. Accessed the log file report name in Windows, open and print the report from a text editor like Notepad.

8. Optional Peripherals

Introduction

Logicube has many different adapters and other peripherals that allow you to tackle almost any drive capturing job. This section focuses on five particular devices – the Clone Card Pro™, the Portable Battery Pack, 1 to 2 Forensic Adapter and the SCSI and SAS Adapters.

Logicube Clone Card Pro™

The optional CloneCard Pro™ is an intelligent PCMCIA adapter designed to provide fast cloning to and from laptop PC's. When used properly, it will support up to 115 MB/min transfer speed.

The CloneCard Pro™ is a real time-saver when a laptop drive needs to be captured, and it is undesirable to remove the internal hard drive from the PC. It is designed to work in both PCMCIA (16-bit) and CARDBUS (32-bit) systems.

In general, the user would boot the laptop from the supplied CD-ROM and run a client program. This client program detects the PCMCIA chip-set inside the laptop and will enable communication to the CloneCard Pro™. Now the Quest can be connected to the external cable of the card, and operation commences as if the Quest is connected directly to the suspect drive. All Quest modes and options are operational as though an actual drive is connected, with the exception of the speed of transfer.

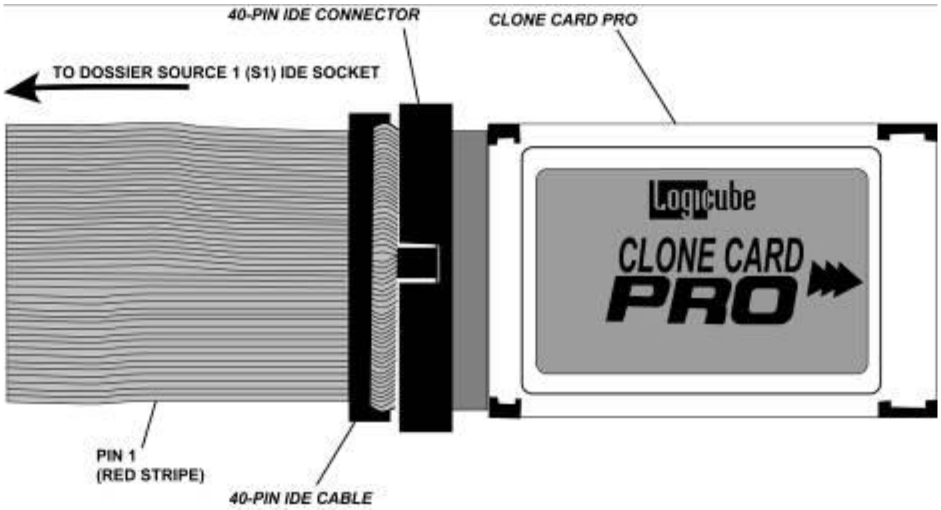


Figure 13, Clone Card Pro™

Before Capturing

Logicube provides a bootable CD-ROM which runs off the FREEDOS operating system. Follow the loading directions that come with your Clone Card Pro™.

Using the Logicube CloneCard™ Pro to Capture a Drive

Cloning with the CloneCard™ takes just a few steps.

1. Insert the CloneCard Pro™ into one of the PCMCIA slots on the laptop you are about to clone (make sure to remove all other PCMCIA cards.
2. Insert the CD-ROM into the laptop CD drive
3. Turn laptop on. Ensure that the laptop is set to boot from a CD-ROM. This is done through the setup screens that can be accessed by pressing F2 or <DEL> key during initial boot (consult your laptop manual regarding how to set the boot order).
4. The CD-ROM is configured to run the client application (CCclient.exe or pcmcia.exe) automatically.
5. Connect the S1 position of the Quest to the flat cable provided with the CloneCard Pro™.

Warning! Do not use one of Quest's included PATA drive cables. They are incompatible with the CloneCard Pro™.

6. Make all the necessary settings on your Quest.
7. Set the Speed setting to PIO-Slow**.** No settings are available on the client program.
8. Press the **START/STOP** button and wait for the process to complete.

Improving Speed of Transfer

Several settings in the CMOS setup screens can potentially improve the speed of transfer.

1. **PCI latency timer** - Try to reduce the value of this number as much as possible.
2. **PCI write buffer** - Set to enable to improve writing speed to the local drive.
3. **PCI zero-wait states** - Enable to decrease PCI cycle time.
4. **PCI delay transaction -** Disable to decrease PCI cycle time.
5. **PCI dynamic bursting** - Set to yes.

6. **Enable 32-bit access to hard drive -** We test for that, and if available, we use it to improve transfer speed, so no action is required on behalf of the user.

NOTE: Some of these settings may not be present on your machine. Also, some of these settings may cause other peripherals to not function properly, so use with caution, and always change one setting at a time.

Logicube Portable Battery Pack

The optional rechargeable battery pack (Logicube P/N F-BATTERY-EXTND) is used to power the Forensic Quest whenever connection to a standard AC outlet is either undesirable or not possible. This guide is intended to provide users with connectivity instructions unique to this rechargeable battery pack and the device it is designed to support.

Precautions

- Do not charge the battery pack in a gas tight container. Charge only in well ventilated areas
- Do not short the battery terminals or battery pack connector pins with metal objects
- Do not incinerate the battery
- Immediately flush with water for at least 15 minutes after physical contact with electrolyte (Acid)
- Always store the Portable Battery Pack in a cool dry ventilated area away from combustibles
- Use caution when lifting or carrying the battery to prevent injury

What's Included

- QTY 1 Battery Pack **P/N F-BATTERY_EXTND**
- QTY 1 Power Supply to charge the Battery
- QTY 1 Power Out Cable for connection between the Portable Battery Pack and the Forensic Quest
- QTY 1 CBL-088A cable used to daisy chain an additional battery pack.

Charging the Battery – Do's & Don'ts

1. A protection circuit prevents the battery from being over charged if the pack is left connected to the charger.

2. The *Power Out* & *Charge* female mating connectors on the battery each have three and four pins respectively and are keyed to simplify cable connection. Special care should be taken when inserting cables into the battery pack in order to prevent damage to the connectors.

Connecting Battery to Charger

Use only the supplied power supply to charge the portable battery pack.

1. Plug the A.C. power cord that came with the battery pack between the A.C input of the power supply and a grounded A.C. outlet.

2. Locate the four pin cable opposite the A.C. input of the power supply and plug the cable into the battery pack connector labeled CHARGE.

3. At this point an Amber colored LED will illuminate next to the word CHARGING irrespective of the position of the on/off switch. This amber LED indicates the battery is charging. A row of five LED's grouped together indicate the batteries current charge status and become visible during charging or anytime the power switch is in the ON position. See Figure 14 for details.

4. In order to achieve full charge capability the battery pack needs to be charged for approximately 9 hours.

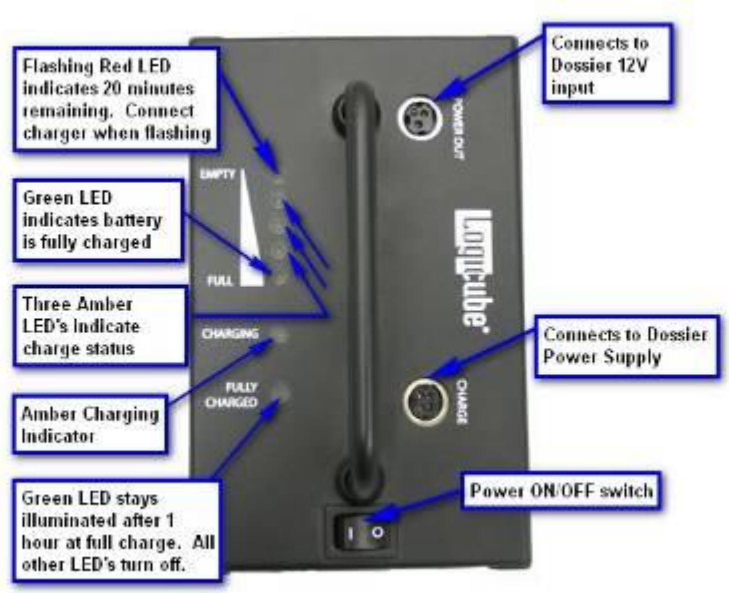

Flashing Red LED indicates 20 minutes remaining. Connect charger when flashing
Green LED indicates battery is fully charged
Three Amber LED's indicate charge status
Amber Charging Indicator
Green LED stays illuminated after 1 hour at full charge. All other LED's turn off.
Connects to Dossier 12V input
Connects to Dossier Power Supply
Power ON/OFF switch
EMPTY
FULL
CHARGING
FULLY CHARGED
POWER OUT
CHARGE
Logicube

Figure 14, Clone Card Pro

Connecting Battery & Device

- Use the supplied POWER OUT cable to connect the Portable Battery Pack POWER OUT connector to the Forensic Quest power input connector labeled **12V**.
- Use the ON/OFF switch on the Battery Pack to power up the Forensic Quest

Connecting Multiple Batteries

- Users can increase usable capture time by purchasing additional Battery Packs from Logicube Inc. and daisy chaining batteries together.
- At any time during capture mode or whenever the solid red LED status light is on, users can physically attach the supplied “POWER OUT” cable from an additional battery (Fully Charged) to the “CHARGE” connector of the battery pack currently powering the Forensic Quest.

Additional Considerations

- A fully charged F-BATTERY-EXTND battery pack has been shown to provide power to the Forensic Quest hard drive capture device for periods of up to 5hrs of use.
- It is safe to charge the Portable Battery Pack at any time during a Forensic capture.

Waste Disposal Method

- Federal and State laws prohibit the improper disposal of all lead acid batteries. The battery pack end users (owners) are responsible for their batteries from the date of purchase through their ultimate disposal. The only legally acceptable method of disposal of lead acid batteries is to recycle them at a Resource Conservation and Recovery Act (RCRA) approved secondary lead smelter.

NOTES: When storing the battery pack, turn the switch to the OFF position and charge the battery at least once every month to prevent possible damage to the battery.

A flashing RED status LED indicates the battery can supply power for approximately 20 minutes of continued operation. The charger should be plugged into the battery immediately if you are in the middle of a drive capture.

Only the FULLY CHARGED LED will remain illuminated after the battery has been in the fully charged state for approximately one hour.

Logicube SCSI Adapter

The Logicube SCSI adapter is designed to attach directly to specific Logicube HDD duplication devices. Functionally the adapter acts like a pass through device and allows for external connection and native cloning/capture of SCSI drives through the IDE port of select Logicube cloning devices. Optionally, USB and USB Thumb/Flash drives can also be captured through the adapter.

The SCSI adapter is designed to clone/capture from SAS to SATA/IDE not from SAS to SAS type drives.

NOTE: The Optional SCSI Adapter is compatible with the new Forensic Quest not the previous Quest.

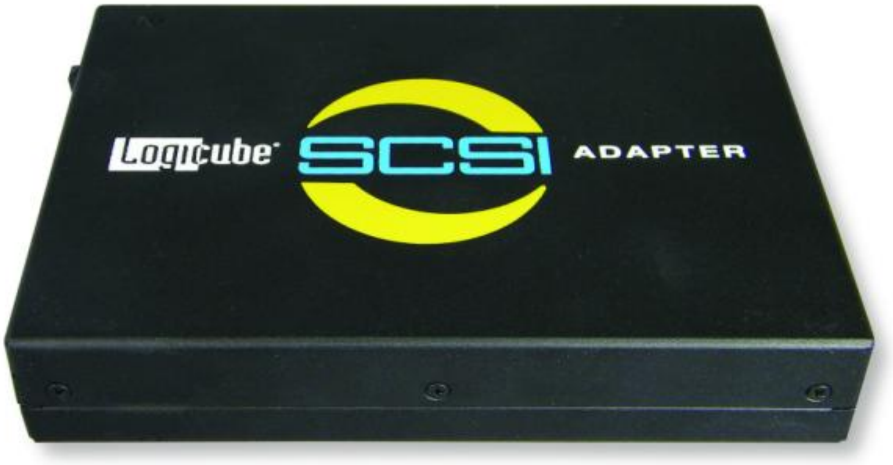


Figure 15 SCSI Adapter

What's Included

- Qty. (1) F-ADP-SCSI Adapter
- Qty. (1) CBL-037B IDE Ribbon Cable
- Qty. (2) CBL-002B Power Cable
- Qty. (1) CBL-031A SCSI Ribbon Cable

Installation Setup

1. Disconnect the power supply cord from the Logicube Hard Disk Drive Duplication device.

2. Locate the IDE ribbon cable P/N CBL-037B and plug the end labeled HDD SIDE into the SCSI adapter port marked IDE CONNECTOR IN.

3. Connect the other side of the ribbon cable labeled DUPLICATOR SIDE to an external IDE port on the Logicube cloning device you are using.

4. Locate the cable labeled CBL-002B and connect the end with the large white plug to the mating receptacle next to the IDE ribbon cable on the SCSI adapter.

5. Connect the other side of the CBL-002B to the external power port of the Logicube cloning device. Use the power port closest to the ribbon cable.

How to use the SCSI Adapter

Duplicating using Forensic Quest

- To capture a SCSI drive connect one side of cable CBL-031A to the SCSI HDD and plug the other side into the connector on the SCSI adapter located below the label SCSI CONNECTOR.
- Connect one end of CBL-002B (power cable #2) between the adapter connector labeled SCSI POWER and the mating receptacle on the SCSI HDD.
- Proceed to step 1.

1. Install a destination hard drive inside the Logicube Forensic Quest.

NOTE: For forensic captures the destination drive should be at least as large as the drive to be captured.

2. Reinsert the power supply cord to turn on the Logicube Quest. The LED located on top of the SCSI adapter near the RESET button will illuminate solid green indicating that the adapter is receiving power correctly.

3. At this point you can perform a standard drive info check to verify that the Logicube Forensic Quest recognizes the drive connected through the SCSI adapter.

4. Adjust the Forensic Quest capture settings as desired.

5. Start the capture process according to the instructions outlined in the Quest User's Manual.

Optional USB cloning with the SCSI Adapter

In order to use the USB port located on the Logicube SCSI Adapter, the USB cloning option must have been purchased and the feature enabled on the cloning device to which the adapter is connected. To verify if the USB cloning feature has been enabled, turn on the Logicube cloning device and press the About icon on the main menu. If *SCSI Adapter USB Option* is visible under Options installed; you can tap the BACK icon and continue to the next step. If *SCSI Adapter USB Option* is not in the list the feature has not been enabled. To verify if the option has been purchased contact Logicube Technical Support and provide the S/N of the cloning device listed at the top of the About screen. Once you have obtained an activation code follow the activation instructions listed below to enable the USB cloning feature.

Press Misc., More, Install Options, [Enter the code] and press OK. Once complete the About screen will read: *Options installed: SCSI Adapter USB Option* along with any other options that may be installed.

- To clone or capture a USB powered HDD connect a USB cable between the USB Drive and the SCSI adapter connector labeled USB PORT and proceed to step 1 of the appropriate Duplicate Using section for your device.

- To clone or capture a USB thumb drive connect the USB thumb drive directly into the SCSI connector labeled USB PORT and proceed to step of the appropriate Duplicate Using section for your device.

NOTE: A second LED located on top of the SCSI adapter will flash green during adapter control and whenever data transfer occurs.

The RESET button on the side of the SCSI adapter located next to the USB PORT is not active at this time and is reserved for future enhancements.

USB functionality via the SCSI adapter is tied to the S/N of the cloning device that receives the activation code. Once the USB option is activated, the USB cloning feature can only be used in conjunction with that specific cloning device.

SCSI/USB enabled Quest and SuperSonix® cloning devices may be able to clone flash media cards by using a USB multi card reader in conjunction with the SCSI adapter.

Logicube SAS Adapter

The Logicube SAS adapter is designed to attach directly to specific Logicube HDD duplication devices. Functionally the adapter acts like a pass through device and allows for external connection and native cloning/capture of SAS drives through the IDE port of select Logicube cloning devices. Optionally, USB and USB Thumb/Flash drives can also be captured through the adapter.

The SAS adapter is designed to clone/capture from SAS to SATA/IDE not from SAS to SAS type drives.

NOTE: The Optional SAS Adapter is compatible with the new Forensic Quest not the previous Quest.

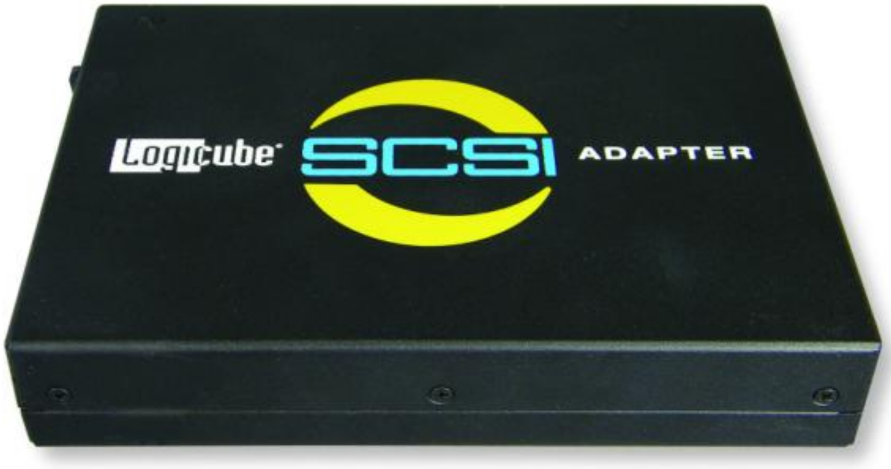


Figure 16 SAS Adapter

What's Included

- Qty. (1) F-ADP-SAS Adapter
- Qty. (1) CBL-037B IDE Ribbon Cable
- Qty. (1) CBL-002B Power Cable

- Qty. (1) CBL-SAS-001-A SAS Data/Power Cable

Installation Setup

1. Disconnect the power supply cord from the Logicube Hard Disk Drive Duplication device.

2. Locate the IDE ribbon cable P/N CBL-037B and plug the end labeled HDD SIDE into the SAS adapter port marked IDE CONNECTOR IN.

3. Connect the other side of the ribbon cable labeled DUPLICATOR SIDE to an external IDE port on the Logicube cloning device you are using.

4. Locate the cable labeled CBL-002B and connect the end with the large white plug to the mating receptacle next to the IDE ribbon cable on the SAS adapter.

5. Connect the other side of the CBL-002B to the external power port of the Logicube cloning device. Use the power port closest to the ribbon cable.

Cloning with the SAS Adapter

Duplicating using Forensic Quest

- To clone a SAS drive connect one side of cable CBL-SAS-001-A to the SAS HDD and plug the other side (which splits and forms the shape of a ‘Y’) into the SAS data and power ports located on the SAS adapter above the label MASTER and proceed to step 1.

1. Install a destination hard drive inside the Logicube Forensic Quest.

NOTE: For forensic captures the destination drive should be at least as large as the drive to be captured.

2. Reinsert the power supply cord to turn on the Logicube cloning devise. The LED located on top of the SAS adapter near the RESET button will illuminate solid green indicating that the adapter is receiving power correctly.

3. At this point you can perform a standard drive info check to verify that the Forensic Quest recognizes the drive connected through the SAS adapter.

4. Adjust the Forensic Quest capture settings as desired. When ready, start the capture process according to the instructions outlined in the Quest User's Manual.

Optional USB cloning with the SAS Adapter

In order to use the USB port located on the Logicube SAS Adapter, the USB cloning option must have been purchased and the feature enabled on the cloning device to which the adapter is connected. To verify the USB cloning feature has been enabled, turn on the Logicube cloning device and press the About icon on the main menu. If *SAS Adapter USB Option* is visible under Options installed; you can tap the BACK icon and continue to the next step. If *SAS Adapter USB Option* is not in the list the feature has not been enabled. To verify if the option has been purchased contact Logicube Technical Support and provide the S/N of the cloning device listed at the top of the About screen. Once you have obtained an activation code follow the activation instructions listed below to enable the USB cloning feature.

Press Misc., More, Install Options, [Enter the code] and press OK. Once complete the About screen will read: *Options installed: SAS Adapter USB Option* along with any other options that may be installed.

- To clone a USB powered HDD connect a USB cable between the USB Drive and the SAS adapter connector labeled USB PORT and proceed to step 1of the appropriate Duplicate Using section for your device.

- To clone a USB thumb drive connect the USB thumb drive directly into the SAS connector labeled USB PORT and proceed to step 1 of the appropriate Duplicate Using section for your device.

NOTES: A second LED located on top of the SAS adapter will flash green during adapter control and whenever data transfer occurs.

The RESET button on the side of the SAS adapter located next to the USB PORT is not active at this time and is reserved for future enhancements.

USB functionality via the SAS adapter is tied to the S/N of the cloning device that receives the activation code. Once the USB option is activated, the USB cloning feature can only be used in conjunction with that specific cloning device.

A SAS/USB enabled Quest and may be able to clone flash media cards by using a USB multi card reader in conjunction with the SAS adapter. Note that this functionality has not been fully verified and is not guaranteed.

Logicube 1 to 2 Forensic Adapter

The (Optional) Logicube 1 to 2 Forensic Adapter is designed to work exclusively with the Quest. It is an adapter that allows two hard drives to be connected to the Destination position simultaneously. The 1 to 2 Forensic Adapter allows two Destination drives to be cloned at the same time. This is important if the investigator needs to have one drive for evidence and a second drive for investigation. Attaching the 1 to 2 Forensic Adapter to the Quest is very similar to attaching an IDE (PATA) drive.

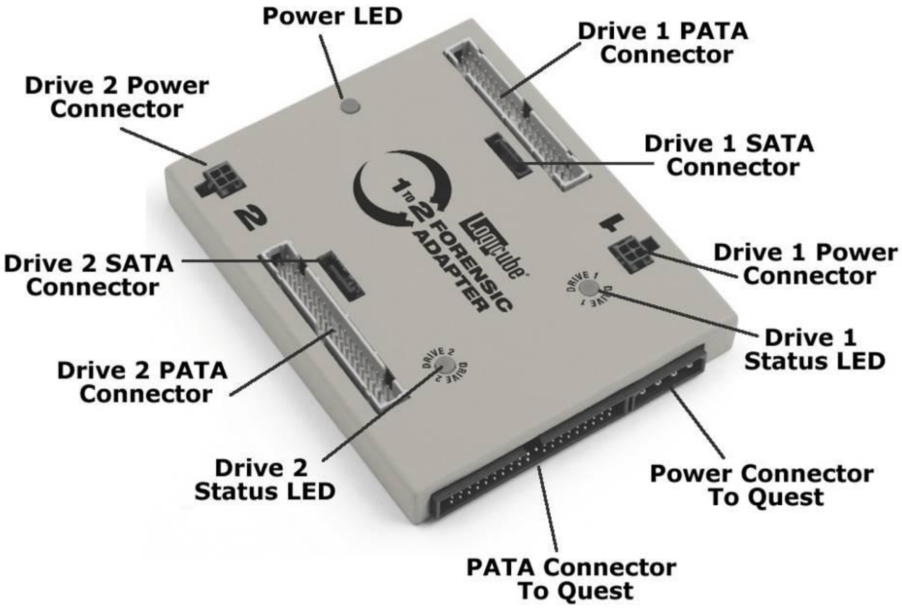


Figure 17, 1 to 2 Forensic Adapter

Connecting the 1 to 2 Forensic Adapter

1. Open the Logicube Quest by pressing on the two latches at the base of the unit and lifting the top. You will notice three connections: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the third connector for the Serial ATA cable.

NOTE: Please refer to **Section 2 – Getting Started** for more information on connecting hard drives.

2. Connect the 1 to 2 Forensic Adapter to the UDMA (PATA) drive power and data connectors on Quest. Leave the Logicube Quest lid open.

3. Connect Destination Drive 1 and 2 to the appropriate connectors on either side of the 1 to 2 Forensic Adapter.

NOTE: A Destination drive can be connected to either position on the 1 to 2 Forensic Adapter, if only one Destination drive is to be used.

4. Connect the Source drive to the outside of Quest.

5. Power the Quest by connecting it to an external power supply. In a few seconds, the main menu will appear.

Wiping with the 1 to 2 Forensic Adapter

When performing a single pass wipe on two destination drives using the 1 to 2 Forensic Adapter Quest will perform a Security Erase on Security Erase enabled drives or wipe both drives using DMA (Direct Memory Access). The DMA process is managed based on the size of the destination drive in position 1 of the 1 to 2 Forensic Adapter.

When performing a DoD wipe on two destination drives with the 1 to 2 Forensic Adapter Quest wipes the drives using DMA (Direct Memory Access). The DMA process is managed based on the size of the destination drive in position 1 of the 1 to 2 Forensic Adapter.

NOTE: Always place the larger of the two drives to be wiped in position 1. This will ensure that both destination drives are completely wiped by the DMA (Direct Memory Access) method of wiping.

Capturing with the 1 to 2 Forensic Adapter

Both Native Capture and DD Image Capture modes work in conjunction with either one or two Destination drives connected to the 1 to 2 Forensic Apapter. The procedure for cloning is exactly the same as cloning to a single Destination drive without the Forensic 1 to 2 Adapter. Both drives will appear in the final capture report.

Verification Modes, Drive Defect Scan Mode, and Calc. MD5/SHA-256 can only work with one Destination drive attached to the Forensic 1 to 2 Adapter. The drive can be in either position. If two destination drives are attached, the selected operation will be performed only to the drive attached to position 1.

USB Mode is not compatible with the Forensic 1 to 2 Adapter at this time. This incompatibility also extends to USB cloning.

NOTE: When wiping (Wipe and or DoD Wipe) two destination drives with the Forensic 1 to 2 adapter, the larger of the two destination drives should be attached to position 1.

9. Compact Flash™ Memory

Introduction

The Logicube Quest comes with a removable Compact Flash™ (CF) Drive that is located on the left side of the device when facing the unit. This drive is used to hold the Quest,software application, debug logs and for storing session reports.

NOTE: Please check our website periodically at www.logicube.com, any new CF functions will be posted there.

To load new software from the CF Drive, please refer to the procedure "**Loading Software Using the Compact Flash**" which is found in **Section 10: Software and Firmware Loading Instructions.**

Connecting the CF Drive to Windows via USB

This procedure is necessary to load new software files to the CF Drive. It is also necessary to pull session reports off the Quest.

Connecting Through USB Mode

1. Make sure your PC is running Win98 or above.
2. Connect the USB cable (provided) to a PC USB port on one end. Do not attach the other end to the Quest yet.
3. From the Main Screen of the Quest, tap the Settings Icon.
4. Press the USB Icon.

5. Tap the drive Icon displayed and 2 settings will appear:
   - Under the heading **Drive:** Choose System CF (Quest's flash memory card).
6. Press the Back Icon followed by the Start Icon.
7. The Quest will power up the chosen drive. A prompt will appear that reads "USB Link Up".
8. Press the Start Icon.
9. Attach the USB cable to the Quest. You should now see some activity on your PC screen, which depends on the operating system.
10. If running 2000/XP/VISTA/Windoews 7 your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
11. The System CF is now visible on Windows as an external drive. The System CF drive is not write-protected, so files can be modified on the card itself.

Removing USB devices

Before physically disconnecting the USB cable and/or shutting down power to the Logicube Forensic Quest, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB Icon in the system tray (typically at the bottom right of screen).

2. Click the Icon once.

3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently).

4. Press the Back Icon on Quest to disengage the USB Link.

Installation and Removal of the CF Drive

In rare occasions, it may become necessary to replace the CF drive that is located on the left side of the Quest when facing the unit.

Compact Flash™ Memory Removal and Installation

1. Unplug the Quest from the power supply.
2. Locate the Push button next to the CF card on the left side of the Quest.
3. Press the button once to extend the release button.
4. Push the button in a second time and the CF card ejection mechanism will partially eject the card.
5. Remove the Compact Flash™ drive from the slot.
6. To install the Compact Flash™ drive perform the following: With the release button flush with the Quest), gently sliding the Compact Flash™ drive label side up along the rails inside the CF mechanism until the drive stops.

10. Software and Firmware Loading Instructions

Introduction

New and improved software will appear from time to time on our web site at www.logicube.com. It is possible to update both the operating software and the firmware in the field by a user.

NOTE: Logicube provides a CD-ROM that contains a backup copy of the Quest software. This software is already loaded on your unit.

Loading New Software

The new software (a single file always called quest2.bin) has to be placed on the root directory of the Compact Flash™ memory (System CF).

1. Connect the Quest to a PC via USB connection as described elsewhere in this manual. (Alternatively, eject and remove the Compact Flash™ drive from Quest and install the drive into a CF media card reader connected to a PC).

2. Once the System CF is mounted on the PC, overwrite the existing **quest2.bin** file with a new version.

3. Disconnect the Quest from the PC as described elsewhere in this manual.

4. Reboot the Quest, and the new software will automatically load! (At this point you will be prompted to calibrate the touch screen)

5. Check the version and date of this software by pressing the “About” Icon at the Main Screen.

Loading New Firmware

In order to upgrade Quest FPGA a separate Compact Flash™ dives is temporarily required.

The upgrade instructions are as follows:

1. Download the Quest FPGA application from the Logicube website.

2. Insert a non system Compact Flash™ drive into a CF media card reader connected to a PC.

3. Once the non system Compact Flash™ drive is mounted on the PC, copy the FPGA application file to the root of the Compact Flash drive.

4. Remove the non system Compact Flash™ drive from the CF reader and insert it into the Forensic Quest.

5. Power up the Forensic Quest. and a menu screen will display with a single button

   Press this button to start the upgrade process and a confirmation message will be displayed warning the user that the upgrade process will take more than 30 minutes.

   WARNING! The unit MUST not be powered off during the FPGA upgrade process or the unit will become unusable.

   When the upgrade process ends a final message is displayed. “Remove the CF containing the FPGA application”.

6. Re-insert the CF containing the Quest Application.

7. Power up system up. The Quest application should now come up as it did before the upgrade.

11. Reference

Further Notes on Modes Available for the Quest

Capture – Native or DD image

This process captures all data from the source drive to the destination drive. See the "**Anatomy of a Drive Capture**" section below for more information.

Drive Defect Scan

The Drive Defect Scan operation performs a surface scan of the drive media using the drive controller to verify the media. This is done without transferring any data from the drive and results in extremely fast operation at the maximum media speed of the drive. This is typically faster than the maximum sustained transfer speed of the drive. The media is scanned in blocks of 256 sectors. If a block fails to verify, it is retried once at the block level. If it fails again, each of the 256 sectors is scanned individually. Each sector is scanned up to ten times. If a sector fails immediately, it is classified as bad. If the sector fails to verify after a good read any time up to the tenth read it is classified as weak. If the sector is verified good for ten reads it is classified as good. If, after the individual sectors are all scanned and there are no bad sectors found, the block is classified as a weak Spot.

Options

Drive – Choices are S1& D1

Speed – Choices are, Fast or Slow

Wipe Destination

The Wipe Destination function is the process that erases or wipes all existing information from the surface of destination disk drive.

Options

These are the user configurable options for the Quest erase process.

Speed - The speed setting provides the option to set the speed at which an operation will be performed.

The choices are UDMA-5 to UDMA-0, PIO-AUTO, PIO-MED and PIO-SLOW.

Signature - A unique digital signature is written to the destination drive on the first sector of each logical cylinder boundary across the entire drive.

Choices are Yes or No

Erase process with Security Erase.

The software sends an ATA command to the drive to erase itself with a pattern of 0's.

Erase process using non Security Erase drives

The software will do a CPU-erase. This is a process where the Quest's CPU writes a pattern of 0's to the drive.

Additional Commands

Verify

The Verify option adds an increased level of confidence in the capture process. The choices are: HASH, HASH + V and None.

HASH

This mode uses special hardware to compute SHA-256 or MD5 Hash values at an extremely fast and accurate rate.

NOTE: If the Destination drive has bad or weak sectors, this mode may not guarantee the accuracy of the Hash values. If the destination drive's health is unknown, use the "+V" setting.

HASH + V

This mode uses special hardware to compute SHA-256 or MD5 Hash values at an extremely fast and accurate rate. It also performs a read-back and comparison of each block of data as it is captured. It is highly recommended that this mode be selected to ensure the accuracy of the Hash values.

None

(Default setting). This method performs no special verification and is used only for non-forensic cloning purposes.

On Error

The On Error option controls what actions are taken when the software runs into problem areas on the source drive. The choices are:

ABORT - The Abort option causes the software to stop the copying process and display an error message when an unreadable area is encountered on the source drive.

SKIP - The Skip option causes the software to ignore a bad sector and not copy it to the destination drive. All prior and subsequent sectors are copied while only the unreadable sector is skipped. This Sector is filled with zeros on the destination drive.

RETRY - The Retry option attempts to reread an offending sector. The number of retry attempts is set to 50 by default. The Quest uses the following sequence for retry:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.
3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.

If the sector is still unreadable after the maximum number of retries, then it is skipped and the copying process continues with the following sectors. As with the skip option, if the sector is skipped, it is filled with zeros on the destination drive.

RECOVER - At least one reinitialize and retry is performed for all choices before recovery is attempted. This prevents recoverable errors from halting the completion of the copying process. For all modes, except ABORT, the hardcopy printout will provide a list of sector numbers that failed.

The Recover option makes up to 50 attempts to reread an offending sector using the following sequence:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.

3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.
4. If the read failed, the low level code transfers the drive's buffer contents anyway. The buffer is examined and information is collected for a majority vote algorithm.
5. If the sector is still unreadable after the maximum number of retries, the software will then attempt to reconstruct the sector by applying a majority vote algorithm to the data collected while performing the retries. The sector is then written to the destination drive and the copying process continues with the following sectors.

Anatomy of a Drive Capture

The drive capture process implemented in the Quest is a specific and detailed process designed to ensure maximum integrity and certifiable performance. It consists of a number of checks and procedures that are detailed in the following section.

Power-up and Initialization

Power and reset are applied to both source and destination drives, then the software waits for up to 30 seconds for the source drive to become ready.

When the source drive is ready, the software identifies the drive configuration and initializes drive parameters.

The software then checks the destination drive for ready status and waits, if necessary. When the destination drive becomes ready, the software identifies the drive configuration and initializes drive parameters.

If the initialization of either drive fails, the software aborts the process with an error message.

The software verifies that the destination drive capacity is equal to or greater than the source drive. If the destination capacity is insufficient, then the user is informed and the software will abort the capture process.

Log file name entry

The unit initializes the CF Drive, and then asks the user to enter a case name. Case name(s) must be 8 characters or less and use DOS naming conventions.

The Log file name is assigned to the report that is created at the end of the capturing session and written to the System CF. The report can be opened and printed from any text editor in Windows (like Notepad). Refer to **Section 7 *Printing Options*** for more printing options.

Calibrate Transfer Speed

If the Speed option described previously is set to any UDMA speed, then the calibration procedure is performed as follows:

1. In the drive identification process, the maximum speed of each drive is identified and stored.
2. The UDMA calibration process, simply takes the lowest common denominator of all drives involved in the process.

If none of the involved drives are UDMA capable, OR, if the Speed option described previously is set to any of the PIO speeds, then the following PIO calibration procedure is performed:

1. The transfer speed is set to a conservative initial value.
2. A chunk of the source drive is copied to the destination drive.
3. If there are no errors, then the elapsed time is stored. If there is an error, then the software will set the transfer speed to a lower value and exit the routine.
4. The transfer speed is set to the next higher value and the process is repeated until the highest speed is reached that does not result in any errors.

Check Capture Integrity

This procedure tests the integrity of the data path including the following items.

- Drive interface
- Data cables
- Unit integrity
- Loose connectors.

The method used is as follows:

1. For drives that are running at PIO speeds: All bits of the data lines of the source drive are checked for toggling between one and zero while reading data from the drive. This is necessary because

the data lines can be broken or unreliable and we can still communicate with and control the drive without transferring data.

> **NOTE**: For this test, the unit checks an 8 MB portion of the drive that starts 50MB from the start of the drive. If the drive is wiped, or there is no data in that area, then the unit will pause with an error: "**Source drive data lines can not be verified. Do you wish to continue?**" Choose <Yes> to continue with the Capture or choose <No> to abort. If the capture is continued, then the error message will not show up on the final capture report.

2. A chunk of the source drive is then copied to the destination drive at the speed previously set in the calibration procedure.
3. <u>Every</u> byte of <u>every</u> sector copied is then compared on the source and destination drives.
4. If the data on both drives match, then the software will exit the Integrity check and continue the capture process. If the data does not match, the transfer speed is lowered to the next available setting. The process is then repeated until the data is identical on each drive.

> **NOTE**: If a match does not occur, the unit will fail with an error.

Verify Destination Drive is Erased

Verify Erasure

The destination drive is checked to be sure it has been erased before copying the data from the source to the destination drive. Verifying the existence of a unique digital signature that is written to the drive during the Wipe-clean or erase function performs this check. The signature is written periodically across the entire drive when the Quest erases it. If the drive is verified as erased, then the Capture process will proceed without any user intervention. If the erase is not verified, the user is asked if the drive should be erased now. If the user says yes, then the drive is erased and the Capture process will proceed. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed.

Wipe Destination

The next section only applies if Wipe Destination is chosen during a capture session:

Erase Process

The software will write zero-filled sectors directly to the entire destination drive using programmed I/O.

If the words Security Erasing show in the UI during the wipe the drive is Security Erase enabled.

If the word Erasing shows in the UI during the wipe the drive is not Security Erase enabled.

Write a unique signature to the destination drive.

By default, the software writes a unique digital signature to the destination drive on the first sector of each logical cylinder boundary across the entire drive. This enables the Capture process to quickly verify that the destination drive has been erased prior to the Capture process. The unique signature is written to the last 12 bytes of the sector. The data pattern is

0xAAAA, 0x5555, followed by the character string “Logicube”.

If needed, the user can disable the signature by selecting “NO” on the “Signature” menu located in the settings menu.

Capture Source Drive Data To Destination Drive

All Data on the source drive is copied sector-by-sector to the destination drive.

Check for Erasure of Unused Portion of Destination Drive

If the destination drive has not been previously verified as erased and the source drive has less capacity than the destination drive, then the software will ask the user whether or not to erase the unused remaining portion of the destination drive. If the user accepts, then the remainder of the destination drive will be erased and the Capture process will continue. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed. This is to ensure that there is no leftover data from any previous usage on the extra portion of the drive.

NOTE: In the DD imaging modes, erasure of remainder of drive is not an option.

A copy of the report is also written to the CF drive. It is named <Log file name>.LOG and can be accessed via the USB port by following the print instructions found in **Section 7 *Printing Options.***

Final Capture Report (Hardcopy Printout)

The hardcopy printout available on the Quest was designed to provide sufficient information for use as an evidence identification tag. It contains information on the unit used to acquire the evidence, the personnel acquiring the evidence, and the important information for the actual capture session.

Information Format

This section describes the information format that appears on the Forensic Quest hardcopy printouts. For an example, see the included page at the end of this section.

Unit Information - The unit Information section identifies the model name of the acquiring unit, the unit serial number, and the software version installed.

Forensic Information - The Forensic Information section contains several lines for the user to enter the necessary information relevant to each investigation.

There are spaces for the following information:

- Evidence number and/or any alias identifier.
- The name of the person(s) acquiring the evidence.
- The date and time that the evidence was acquired.
- The location at the scene of the investigation where the evidence was acquired.
- A description of the acquired evidence.

Session Information - This section of the printout contains information specific to the actual Capture session.

Session Settings Information – This section contains information pertaining to the actual Session that is not specific to either drive. It contains the following:

- Operating Mode. This can be Capture, DD Capture, Scan or Wipe clean.
- Verify. This reflects the Verify option setting for each operating mode as explained in previous sections of this text.
- Speed. This reflects the Speed option setting for each operating mode as explained previously.
- Connection. This is the connection method for the operating mode. This is meant to indicate whether a direct IDE, SATA or USB connection was used for the operating mode.

- Results. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines.
  - "MIRROR COPY OF THE DRIVE HAS BEEN SUCCESSFULLY EXECUTED!"
  - "SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS ABORTED!"
  - "SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS IN ERROR!"
- Extra information. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines:

– The destination drive was verified as erased before Capture!

– The destination drive was erased during the Capture!

– Operator declined FULL destination drive erase and erased remainder.

– Operator declined FULL and remainder destination drive erase!

Source drive Information - This section of the printout contains information specific to the Source or Suspect drive. This will only appear if the operating mode was (Native) Capture or DD Image Capture with Verify set to **HASH** or **HASH-Disk**. It contains the following:

- Drive Identification. These lines print the model and serial number as reported by the source drive.
- Physical Geometry. These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- HASH Value. This line prints the computed SHA-256 or MD5 values for the source drive.
- Error recovery information. These lines will only appear if the On Error setting for the Capture operation was set to something other than abort.
  If the setting was set to "skip", then a single line containing the total number of skipped sectors will be printed.
  If the setting was "retry" or "recover", two lines will be printed: One containing the total number of recovered sectors; one containing the total number of non-recovered or skipped sectors.

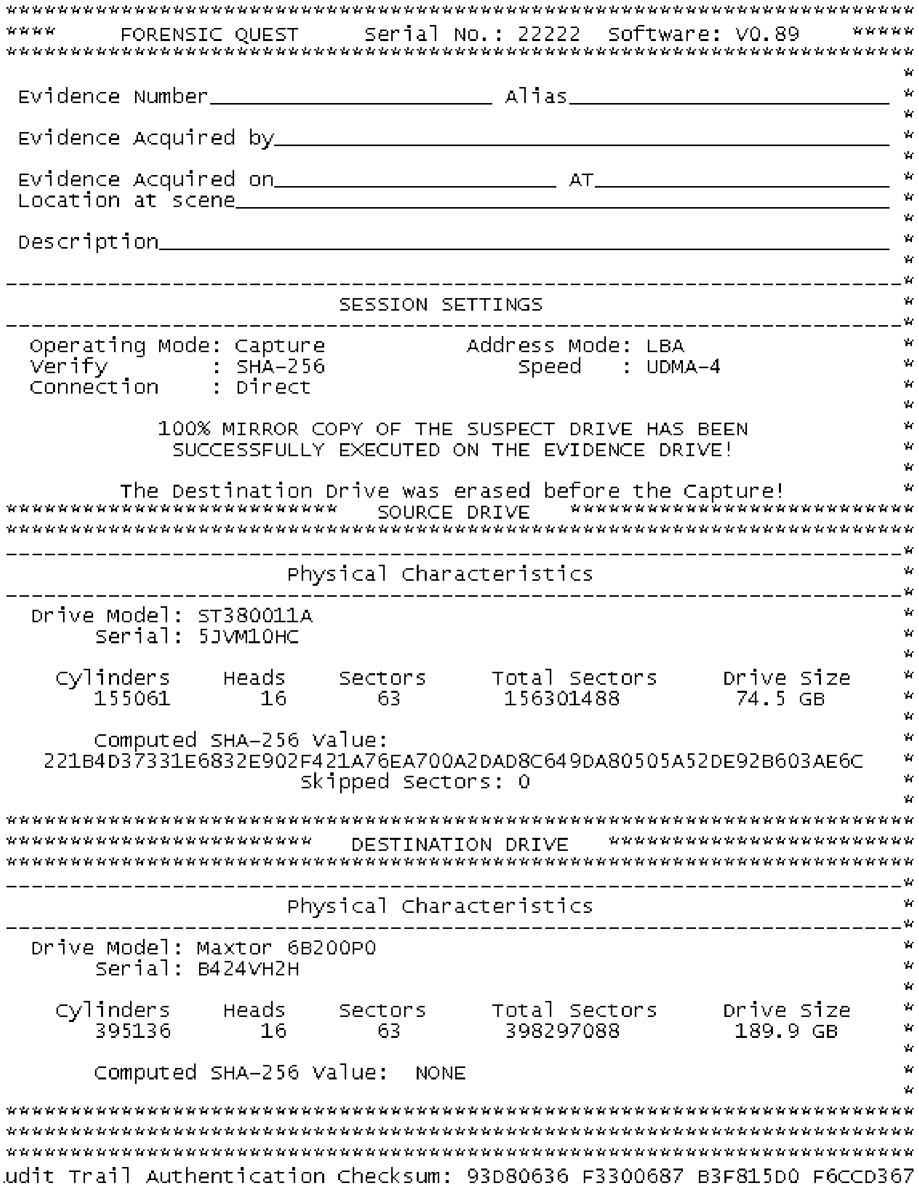
Destination drive Information - This section of the printout contains information specific to the destination drive. It contains the following.

- Drive Identification. These lines print the model and serial number as reported by the destination drive.
- Physical Geometry. These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- HASH Value. This line prints the computed SHA-256 or MD5 value for the destination drive. This will only appear if the operating mode was (Native) Capture with Verify set to **HASH**.
- Media Verify information. These lines will only appear if the operating mode was set to Scan. If after a Scan operation, any bad sectors, weak sectors, or weak spots are detected, then the addresses of those sectors are printed followed by the grand totals for each type.
- If one of the DD imaging modes was used with verify set to **HASH-File**, a list of file names with their respective SHA-256 or MD5 values will be printed at the bottom of the page.

Audit Trail Authentication Checksum – This number is used to verify if the report which resides on the system CF Drive has not been altered in any way. The Checksum is a proprietary Hash value.

NOTE: The Audit Trail Authentication Checksum value is not a standard MD5 Hash value and it will not match the value calculated by third-party software or other means.

Example of Hardcopy Printout



```
***********************************************************************
****     FORENSIC QUEST     Serial No.: 22222  Software: V0.89    *****
***********************************************************************
                                                                      *
 Evidence Number______________________ Alias__________________________*
                                                                      *
 Evidence Acquired by_________________________________________________*
                                                                      *
 Evidence Acquired on______________________ AT________________________*
 Location at scene____________________________________________________*
                                                                      *
 Description__________________________________________________________*
                                                                      *
----------------------------------------------------------------------*
                          SESSION SETTINGS                            *
----------------------------------------------------------------------*
  Operating Mode: Capture           Address Mode: LBA                 *
  Verify        : SHA-256               Speed   : UDMA-4              *
  Connection    : Direct                                              *
                                                                      *
            100% MIRROR COPY OF THE SUSPECT DRIVE HAS BEEN            *
             SUCCESSFULLY EXECUTED ON THE EVIDENCE DRIVE!             *
                                                                      *
         The Destination Drive was erased before the Capture!         *
**************************   SOURCE DRIVE   ***************************
***********************************************************************
----------------------------------------------------------------------*
                      Physical Characteristics                        *
----------------------------------------------------------------------*
  Drive Model: ST380011A                                              *
       Serial: 5JVM10HC                                               *
                                                                      *
    Cylinders    Heads    Sectors     Total Sectors     Drive Size    *
       155061       16       63        156301488         74.5 GB      *
                                                                      *
       Computed SHA-256 Value:                                        *
   221B4D37331E6832E902F421A76EA700A2DAD8C649DA80505A52DE92B603AE6C   *
                       Skipped Sectors: 0                             *
                                                                      *
***********************************************************************
************************   DESTINATION DRIVE   ************************
***********************************************************************
----------------------------------------------------------------------*
                      Physical Characteristics                        *
----------------------------------------------------------------------*
  Drive Model: Maxtor 6B200P0                                         *
       Serial: B424VH2H                                               *
                                                                      *
    Cylinders    Heads    Sectors     Total Sectors     Drive Size    *
       395136       16       63        398297088         189.9 GB     *
                                                                      *
       Computed SHA-256 Value:  NONE                                  *
                                                                      *
***********************************************************************
***********************************************************************
***********************************************************************
udit Trail Authentication Checksum: 93D80636 F3300687 B3F815D0 F6CCD367
```

12. Frequently Asked Questions and Answers

Q. What is the maximum drive capacity the Quest supports?

A. The Quest currently supports drives up to 1.5 TB in capacity.

Q. By comparison my Quest appears to be operating slower than other units.

A. Make sure that your unit is using the latest software. Visit **http://www.logicube.com** and go to the support page to view the latest software level and if necessary download the software for your system.

Q. My Quest continues to ask if I want to wipe a brand new capture HDD.

A. This is a normal question that will be asked unless the new HDD is wiped by the Quest. Using the Quest to prepare (pre-wipe) a new Destination HDD will eliminate this screen from displaying while on site thus speeding up the capture process.

Q. After installing a brand new destination HDD in my Quest and starting a capture, I received a message that the drive was not erased, is this normal?

A. Even though new drives are usually blank, they still need to be wiped to guarantee that they do not contain any data.

The Quest has the ability to write a signature to the destination drive during the wipe session. It is this signature that tells the Quest that the destination or capture drive was previously wiped. Destination drives can be prepared ahead of time by wiping them with signature set to "YES".

Q. Can I make bootable "Clone" with the Quest?

A. While the Quest was not designed to produce a bootable “clone”, it will create a copy of the source drive with bit-for-bit accuracy. Whether or not the destination drive will boot depends upon many factors that include drive geometry, operating systems, and PC BIOS issues.

Q. On my capture drive the information displayed on the Quest does not agree with the label fixed to the target HDD. Example: The number of cylinders displayed is different than the label

A. This issue has come up on Seagate HDDs. Although the information displayed may not agree, the correct information will be on the printed report generated at the end of the capture session.

Q. Drive information as displayed on the Quest does not agree with the label fixed to the target HDD. Example: The number of cylinders displayed is different than the label

A. Drive labels will only show Cylinders, Heads, and Sectors for a maximum of 8.5GB (example: 16383, 16, 63.) The actual drive parameters will be displayed both in drive information, and in the printed session report. Most of the newer drives only have an LBA (Logical Block Addressing) value printed on the label showing the drive's capacity in sectors

Q. Capturing data from a Western Digital HDD is not working.

A. Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this statement is for the Western Digital "Xpert" series Hard Drives (an older manufactured version), where the jumper is set to the master position.

Q. I'm trying to update my Quest with the latest software but I cannot get my PC to communicate with the unit.

A. Make sure that the PC is connected through the USB port or connect the units CF card directly to your PC using a flash media card adapter.

Q. Will DD Image capture files have the same "odd sector" problem of the Linux operating system?

A. Although DD Image capture files are formatted as "DD Linux" files, they do not utilize the Linux kernel. The Linux OS is unable to see the last sector of a drive that has an odd number of sectors. Some users have asked if this problem will prevent the last sector of an odd sector drive from being captured. The answer is no.

Q. What happens if a HASH mismatch occurs during a Mirror or DD capture with verification on?

A. The capture session will immediately abort and this message will be displayed on the Quest:

Error

Error Capturing Drive! Drive error.

Either the speed setting is too high

Or a bad sector was found!

Q. What will happen if a drive cable makes intermittent contact during a capture?

A. The capture session will immediately abort and an error message will be displayed on the Quest display.

Q. If a verification mismatch occurs during a capture will the clone complete?

A. No. The capture session will immediately abort and display an error message on the Quest indicating that an error has occurred. A Log file is not generated when a mismatch occurs.

13. Index

Technical Support Information

For further assistance please contact
Logicube Technical Support at: (**001) 818 700 8488 7am-5pm PST, M-F**
(excluding US legal holidays)
or by email to **techsupport@logicube.com**.