Logicube Portable Forensic Laboratory™ User's Manual

Logicube, Inc.
Chatsworth, CA 91311
818 700 8488

Version: 1.3

Date: 02/03/05

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

LOGICUBE PROVIDES A BASIC ONE-YEAR PARTS AND LABOR WARRANTY FOR ALL OF ITS PRODUCTS (EXCLUDING CABLES, ADAPTERS AND OTHER "CONSUMABLE" ITEMS). A TWO-YEAR EXTENDED WARRANTY IS ALSO AVAILABLE FOR AN ADDED COST. TELEPHONE AND EMAIL SUPPORT IS AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

Table of Contents

1. Introduction to the Portable Forensic Laboratory™

Introduction

Thank you for purchasing the Logicube Portable Forensic Laboratory™. With proper use, this powerful suite of tools will provide you with accurate HDD capturing for years to come.

The Logicube Portable Forensic Laboratory™ or PFL is designed to connect to a variety of storage media and capture the data to a secure destination. It also connects directly to the user's Examination PC to investigate the data right away.

Designed with the Forensics investigator in mind, the system ensures that proper evidence capture procedures are maintained, speeding up the process significantly with little room for error. It also "Write-Protects" the data and prevents contamination of the evidence.

The Logicube PFL is also capable of connecting to a Suspect PC through the USB port. The investigator can then copy data from the PC to a secure destination.

NOTE: Although the Portable Forensic Laboratory™ may come bundled with FTK™ by AccessData, it can also be used with other forensic examination tools like Encase™ (by Guidance Software) and similar products. Please see Chapter 6 – Standalone Logicube Utilities for more information.

Features

- (Optional) May come with a Panasonic Toughbook CF-73 PC. This ruggedized laptop is used for controlling the PFL and examining suspect data.
- IDE (PATA) and SATA capturing speeds nearing 3.3GB/min – Achieved through the use of the Logicube Talon™ or MD5™.
- Ability to capture SCSI drives[1]
- Ability to connect the destination drive to the Examiner's PC or a Suspect PC. The PFL can also quickly switch between both PC's.
- Write-Protected card reader for examining a wide variety of Flash media cards.
- Ability to control the Logicube Talon™ or MD5™ remotely from the Examiner's PC.
- (Optional) The PFL may come bundled with FTK™ and/or UTK™, by AccessData, which are extremely powerful forensic investigation utilities.
- (Optional) The PFL may include a Forensic Talon™ or MD5™, which are the latest high-speed forensic cloning devices from Logicube.

Using this guide

This user guide is made up of 8 sections:

- Introduction
- Getting Started (Fast Start)
- Examination PC
- Using the Portable Forensic Laboratory™
- Other Drive Capture Methods

[1] SCSI drives with 50-pin or 80-pin "SCA" connectors can only be attached to the PFL with special adapters. Please contact Logicube to procure these adapters.

- Logicube Standalone Utilities
- FAQ's

This manual covers the Portable Forensic Laboratory™ and how it works with the other included components. Please refer to the Logicube Talon™ manual, FTK™ manual and the Panasonic Toughbook™ manual for further instructions on these individual products.

System description

The Portable Forensic Laboratory™ system is packed in a rugged, watertight carrying case. Inside, you will find the following components:

- The Portable Forensic Laboratory™.
- (Optional) A Panasonic Toughbook™ CF-73 laptop which also comes with an AC power supply.
- (Optional) The Logicube Forensic Talon™ [2], which comes with the following items:
  - 5" drive power cable, UDMA data "ribbon" cable and a SATA cable.
  - A 64MB CF Card.
- A 5" power cable with black Molex connectors on either end – for connecting the Talon™ to the PFL.
- A 5" parallel Port cable – for connecting the Talon™ to the PFL.
- A 9" drive power cable and UDMA "ribbon" cable for connecting IDE (PATA) drives to the PFL.
- A 9" Serial ATA cable for attaching Serial ATA (SATA) drives to the PFL.
- A 5" SCSI cable for attaching SCSI drives to the PFL.
- Two USB cables that connect the PFL to the USB port of a PC.
- A padded case that can hold two 3.5"-sized hard drives.
- A flashlight and screwdriver.
- CD-ROM's that include:

[2] The PFL is also compatible with the Logicube Forensic MD5™, which is sold separately.

- (Optional) Logicube Talon™ software and utilities.
- (Optional) Talon™ USB Cloning software.
- (Optional) FTK™ Standalone by AccessData.
- (Optional) UTK™ by AccessData.
- A standalone PFL Button Bar utility to use outside of FTK™.
- (Optional)Drivers and backup software for the Panasonic Toughbook.
- Adaptec Drivers necessary for SCSI drive connections.
- USB drivers for Windows98.
- This manual, as well as (Optional) separate manuals for the Forensic Talon™, FTK™ and Panasonic Toughbook™.

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 into any other Logicube products (e.g. Sonix™) that are used for Operating System cloning).

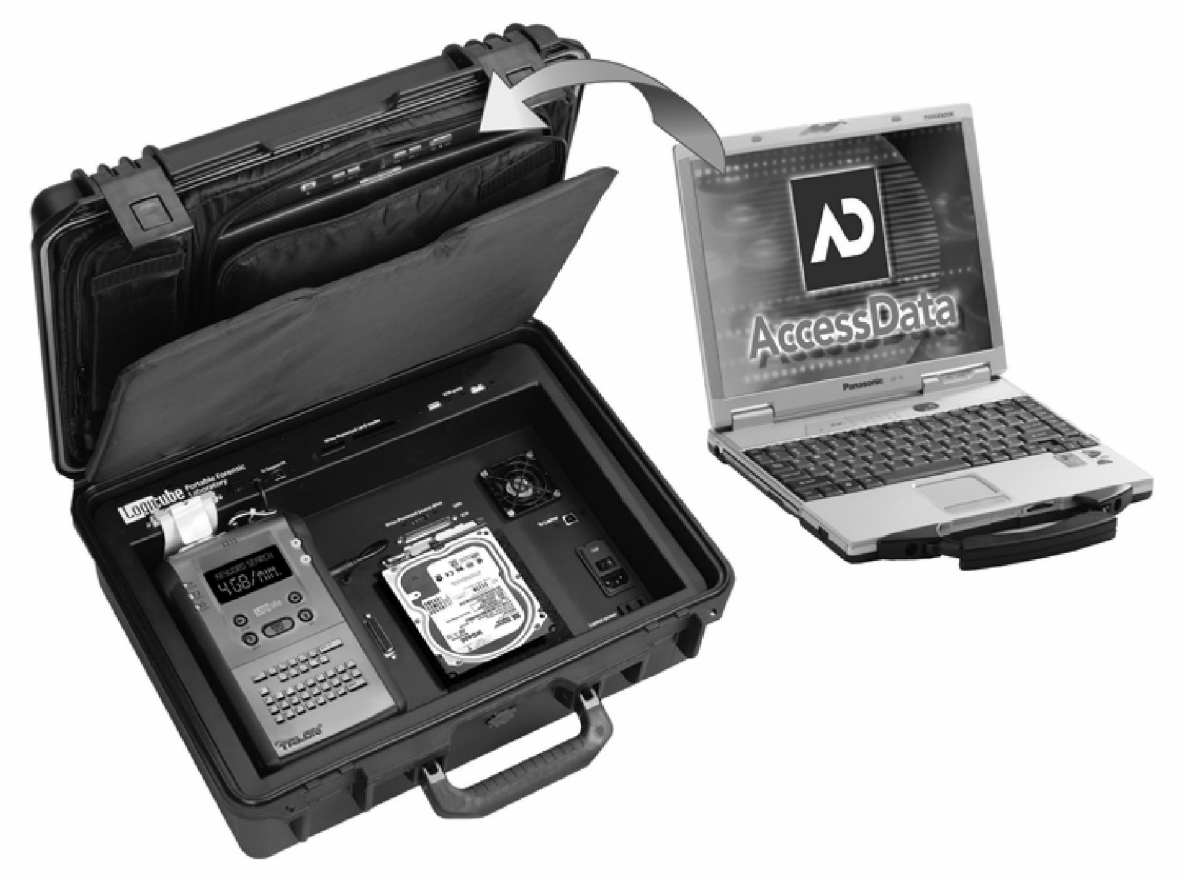


Figure 1. Portable Forensic Laboratory™

2. Getting Started (Fast Start)

Overview of the Portable Forensic Laboratory™

Please refer to Figure 2 below.

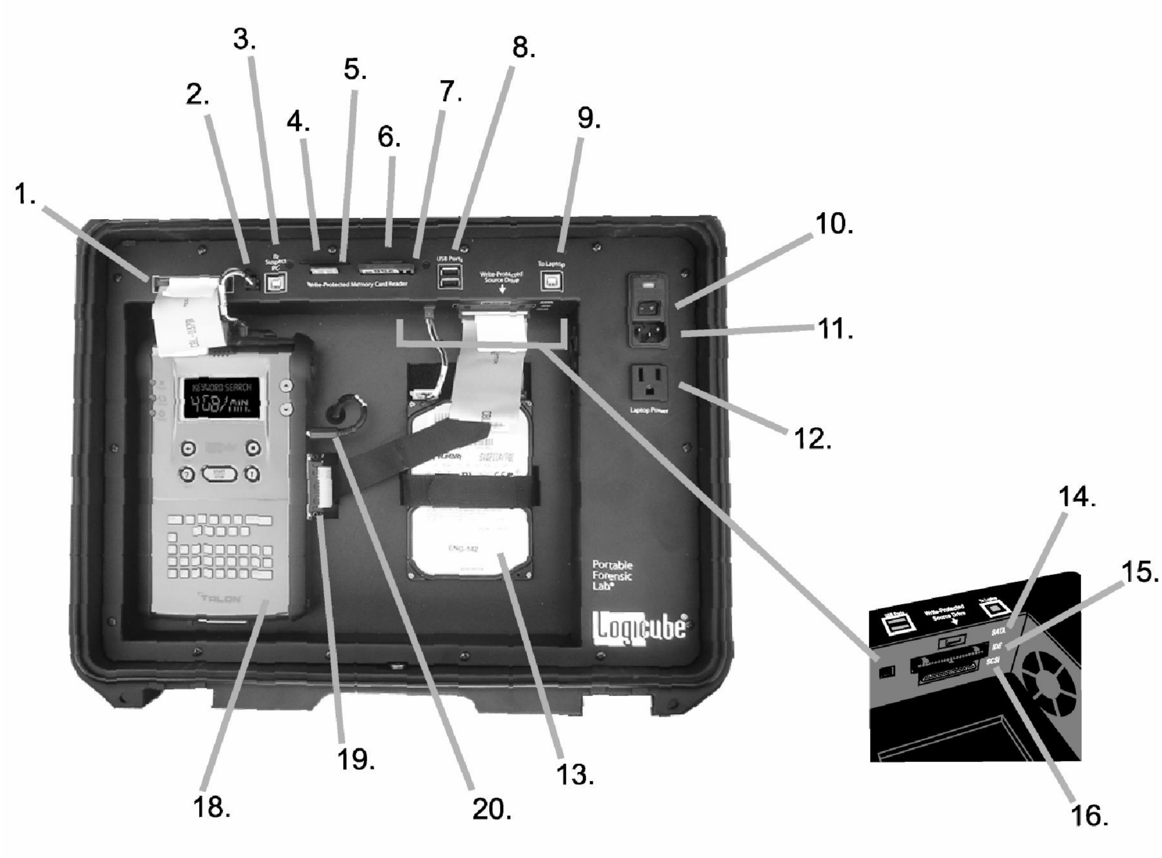


Figure 2 – PFL Overview

1. **Logicube Duplicator UDMA Cable Connector** - The Source UDMA cable from the Talon™ or MD5™ plugs in here.
2. **Logicube Duplicator Power Cable Connector** – The power cable with black "Molex" Connectors plugs in here. The other end plugs into the

Source Drive power socket of the Talon™ or MD5™.

3. **Suspect PC USB Port** – The USB Cable from the Suspect PC plugs in here.
4. **SM Card Reader** – This slot reads Smart Media (SM) Flash Cards on the Examiner's PC. The slot is write-protected.
5. **MS Card Reader** – This slot reads Memory Stick (MS) Flash Cards on the Examiner's PC. The slot is write-protected.
6. **SD Card Reader** – This slot reads Mini-SD Flash Cards on the Examiner's PC. The slot is write-protected.
7. **CF Card Reader** – This slot reads Compact Flash (CF) Flash Cards on the Examiner's PC. The slot is write-protected.

   NOTE: Other flash-based media cards (i.e. xD cards) can be read in an adapter that connects to one of the existing card reader slots. Such adapters are available in any electronic store.

8. **USB Ports** – These USB ports are used for connecting additional USB devices to the Examiner's PC.
9. **Examiner's PC USB Port** – The USB Cable from the Examiner's PC plugs in here.
10. **PFL Power Switch** – This is the main power switch for the Portable Forensic Laboratory™.
11. **PFL AC Socket** – This is where the PFL's main AC cable attaches. The power supply is variable to allow connectivity on 110V or 220V power.
12. **Laptop Power Socket -** This is an extra AC outlet for the Examiner's PC or other AC-powered device.
13. **Source Drive Position** – This is where the Source (or Suspect) drive is attached to the PFL. Tie-down straps are provided to hold the drive for travel.
14. **Source SATA Drive Connector** – This is where the Source drive is connected if it is a Serial-ATA (SATA) drive.
15. **Source Parallel Drive Connector** - This is where the Source drive is connected if it is a Parallel (PATA) drive.
16. **Source SCSI Drive Connector** – This is where the Source drive is connected if it is a SCSI drive.
17. **Source Drive Power Connector** – This is where the power cable for PATA or SCSI drives are

connected. Part of the SATA cable plugs in here as well.

18. **Logicube Duplicator Position** – This is where the Logicube Forensic Talon™ or MD5™ is attached to the PFL. The Destination (or Evidence) Drive is attached to the inside of the Duplicator. Tie-down straps are provided to hold the unit for travel.
19. **Parallel Port Connector –** This is where the parallel port cable connects the Talon™ or MD5™ to the PFL. This connection is necessary to control the Duplicator from the Examiner's PC.
20. **Duplicator AC Cable –** This is where the Logicube Forensic Talon™ or MD5™ gets power. The cable plugs into the unit's AC socket.

Setting Up the Portable Forensic Laboratory™

Connecting the Logicube Forensic Talon™ or MD5™

The Source and Destination Drives should be connected to the Portable Forensic Laboratory™ before it is powered up. The Destination drive is connected to the inside of the Forensic Talon™ or MD5™, and then the duplicator itself is connected to the PFL.

NOTE: The Forensic Talon or MD5 needs to have the Remote Control Option installed so that it can communicate with the PFL and Remote Control Interface properly. Please refer to the unit's User Manual for directions on loading optional features.

1. Attach the destination drive to the inside of the Forensic Talon™ or MD5™.

NOTE: Please refer to the Logicube Forensic Talon™ or MD5™ User Manual for directions on connecting the Destination drive.

2. Place the duplicator in the Logicube Duplicator Position on the PFL. Attach the tie-down straps.

3. Attach the 5” parallel cable to the connector on the side of the Forensic Talon™. Attach the other end to the Parallel Port Connector on the PFL.

NOTE: A longer parallel cable may be necessary if the Forensic MD5™ is attached to the PFL.

4. Attach the 5” UDMA cable to the Source Drive UDMA socket on the duplicator. Attach the other end to the Logicube Duplicator UDMA Cable Connector on the PFL.
5. Attach the power cable with two black connectors to the Source drive power socket of the duplicator. Attach the other end to the Logicube Duplicator Power Cable Connector on the PFL.
6. Attach the Duplicator AC Cable on the PFL to the power jack of the duplicator.

Attaching a Parallel (PATA) Source Drive

NOTE: Never attach more than one drive at a time (i.e. both a PATA and SATA drive) to the Source position. The unit can only handle one drive in the Source position.

Before applying power perform the steps listed below.

1. Plug in the set of 9” UDMA and power cables to the appropriate connections in the Source position of the Portable Forensic Laboratory™.

   Note: See Figure 3, Connecting an IDE (parallel) Source drive.

2. Connect the Source drive to these cables and attach the tie-down straps.

   Note: This drive is always referred to as the **Source** (or **Suspect**) drive.

3. Plug in the PFL and power it on. In 2 – 3 seconds, the main “Splash” screen appears on the Forensic Talon™ or MD5™.

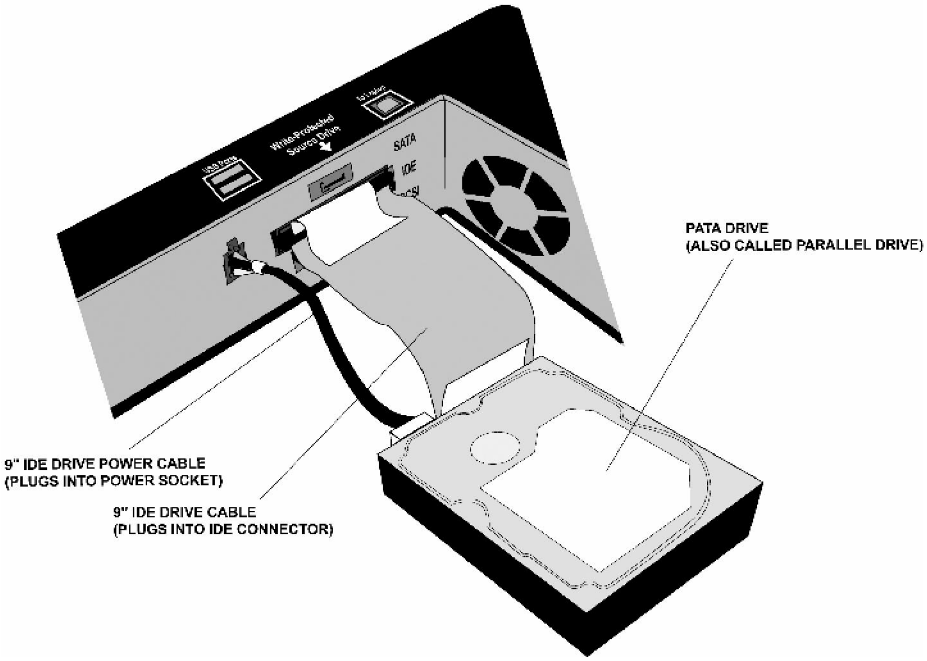

USB Ports
Write-Protected Source Drive
SATA
IDE
SCSI
PATA DRIVE (ALSO CALLED PARALLEL DRIVE)
9" IDE DRIVE POWER CABLE (PLUGS INTO POWER SOCKET)
9" IDE DRIVE CABLE (PLUGS INTO IDE CONNECTOR)

Figure 3. Connecting an IDE (parallel) Source Drive

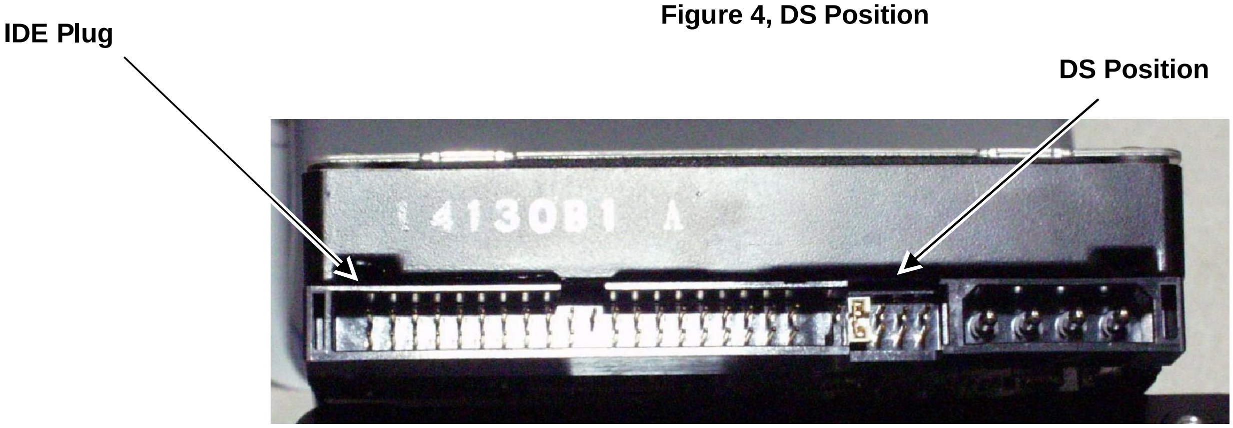
Parallel (PATA) Drive Jumper Settings

When PATA drives are used as a Source or Destination, they must be jumpered for Single Master Mode. For example, 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 Single Master Mode. 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 4.
- **2.5”, 1.8” and CF Drives** – These drives do not have external jumper settings. Logicube adapters will automatically set them to Single Master Mode.

Figure 4, DS Position



Connecting a Serial ATA (SATA) Drive

NOTE: Never attach more than one drive at a time (i.e. both a SATA and PATA drive) to the Source position. The unit can only handle one drive in the Source position.

Before applying power perform the steps listed below.

1. Plug in the 9” SATA cable to the SATA and Power connections in the Source position of the Portable Forensic Laboratory™.

   Note: See Figure 4, Connecting a Serial-ATA (SATA) Source drive.

2. Connect the Source drive to this cable and attach the tie-down straps.

   Note: This drive is always referred to as the **Source** (or **Suspect**) drive.

3. Plug in the PFL and power it on. In 2 – 3 seconds, the main “Splash” screen appears on the Forensic Talon™ or MD5™.

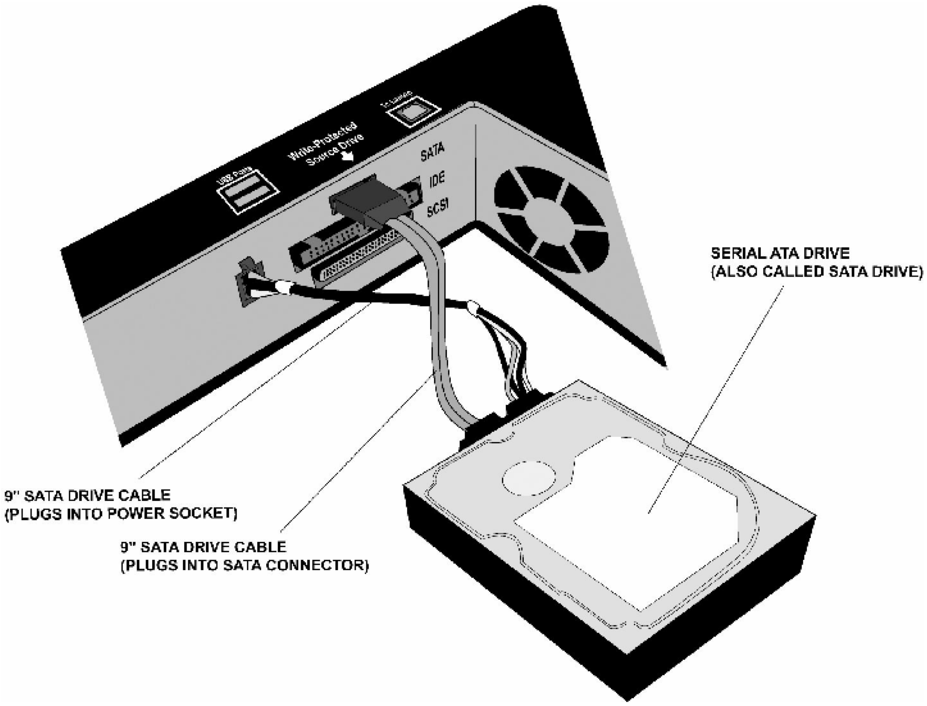

USB Ports
Write-Protected Source Drive
SATA
IDE
SCSI
SERIAL ATA DRIVE (ALSO CALLED SATA DRIVE)
9" SATA DRIVE CABLE (PLUGS INTO POWER SOCKET)
9" SATA DRIVE CABLE (PLUGS INTO SATA CONNECTOR)

Figure 5. Connecting a Serial ATA (SATA) Source Drive.

Connecting a SCSI Drive

NOTE: Never attach more than one drive at a time (i.e. both a SCSI and SATA drive) to the Source position. The unit can only handle one drive in the Source position.

NOTE: The PFL uses a 68-pin SCSI cable and connector. Special adapters for 50-pin and 80-pin (SCA) SCSI drives are available. Please contact Logicube if you need these adapters. Third-party adapters will NOT work with the PFL.

Before applying power perform the steps listed below.

1. Attach the 9" drive power cable to the Power connector and the 5" SCSI cable to the SCSI connector in the Source position of the Portable Forensic Laboratory™.

   Note: See Figure 5, Connecting a SCSI Source drive.

2. Connect the Source drive to these cables and attach the tie-down straps.

   Note: This drive is always referred to as the **Source** (or **Suspect**) drive.

3. Plug in the PFL and power it on. In 2 – 3 seconds, the main “Splash” screen appears on the Forensic Talon™ or MD5™.

4. If the “Add New Hardware” wizard appears on the PC, refer to **Chapter 3 – Examiner’s PC** and the “Loading Adaptec USB Drivers” section.

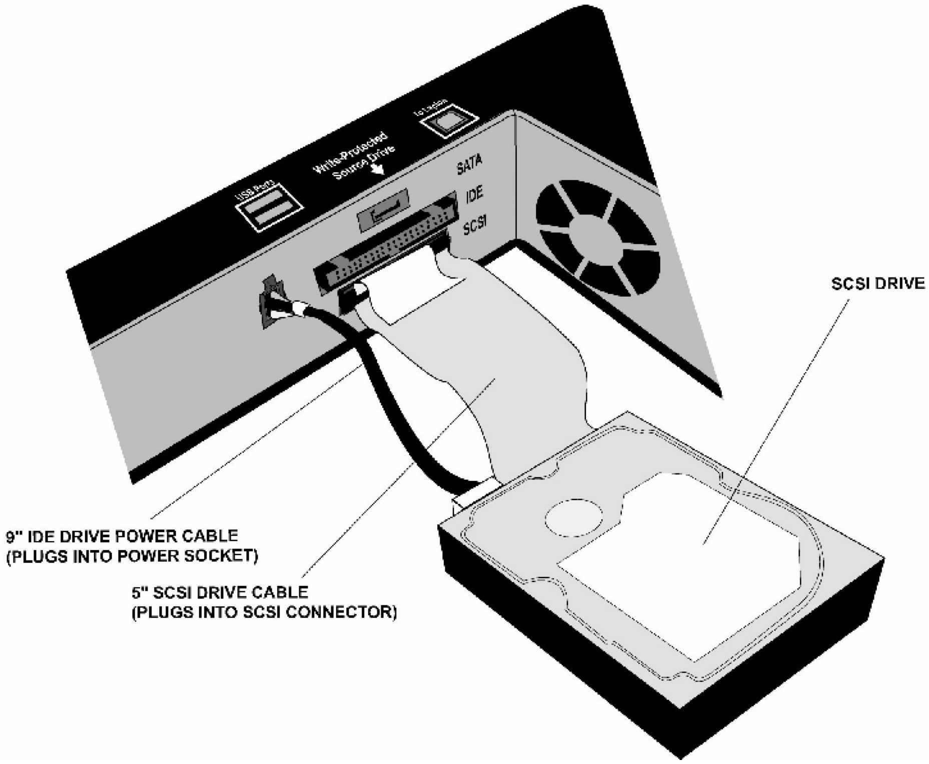


Figure 6. Connecting a SCSI Source Drive.

Connecting other types of drives

Logicube sells specialized adapters that allow other types of drives to be connected to the Portable Forensic Laboratory™. Such drives include 2.5” laptop drives, 1.8” laptop drives (e.g. Toshiba “iPod™” drives and compact Flash (CF) 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.

Connecting Flash-Based Media

The Portable Forensic Laboratory™ includes four flash media card slots for examining flash-based media (i.e. digital cameras, music players, PDA's, etc.) These card slots allow the media to be detected immediately by the Examiner's PC as a removable Media device.

Each card slot is also write-protected, which means that no data can be written to the media. This is necessary for forensic integrity.

Please follow this procedure to attach flash-based media cards:

1. Power up the PFL and wait 2 – 3 seconds.
2. Insert the flash-based media card into the appropriate card slot (i.e., CF, SD, etc.). Make sure that it is facing the correct way. Please refer to Figure 7 below.
3. When the Examiner's PC is powered up and attached to the PFL, all attached flash-based media cards will appear as an external USB Storage device.

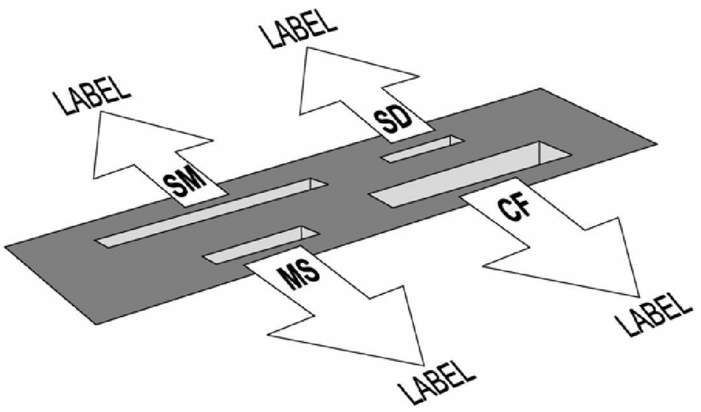


Figure 7 – Card Reader

Connecting Additional USB Devices

The Portable Forensic Laboratory™ includes two USB ports that are located to the right of the Card Reader slots. These ports connect to the Examiner's PC and allow the connection of additional USB devices (i.e. Portable Flash Drives, USB floppy drive, etc.) The ports are NOT Write Protected, so they should not be used for Suspect drives and media.

Please follow this procedure to attach additional USB devices:

1. Power up the PFL and wait 2 – 3 seconds.
2. Insert the USB device into one of the USB ports.
3. When the Examiner's PC is powered up and attached to the PFL, all attached USB Devices will be detected by the PC.

Connecting the Examiner's PC

The Examiner's PC refers to the Panasonic Toughbook™ that is included with the Portable Forensic Laboratory™. However, the user can substitute his or her own PC instead.

NOTE: The Examiner's PC needs to have USB ports enabled. It also needs to be running Windows 2000 or later as the Operating System.

Please follow this procedure to connect the Examiner's PC to the PFL:

1. Power up the Portable Forensic Laboratory™.
2. Wait 2 – 3 seconds, and then connect a USB cable to the Examiner's PC USB Port. This port is labeled "To Laptop" on the PFL.
3. Connect the other end of the USB cable to the Examiner's PC.
4. Any Flash-based media cards in the Card Reader slots will be immediately detected as USB drives.
5. Launch the PFL Button Bar and FTK™ to begin working with the Source and Destination drives.

   NOTE: Please refer to Chapter 3: Examiner's PC for more details on using these utilities.

Connecting the Suspect PC

The Suspect PC refers to any PC that is connected to the second USB port on the PFL. This port is labeled "To Suspect PC".

NOTE: The PC needs to have USB ports enabled and running Windows98 SE or later for the Operating System.

Please follow this procedure to connect the Suspect PC:

1. Power up the Portable Forensic Laboratory™.

2. Wait 2 – 3 seconds, and then connect a USB cable to the Suspect PC USB Port on the PFL. This port is labeled “To Suspect PC”.
3. Connect the other end of the USB cable to the Suspect PC.

NOTE: Please refer to Chapter 3: Examiner’s PC for more details on accessing the Suspect PC through the USB connection.

3. Examination PC

Introduction

The Portable Forensic Laboratory™ may come with an Examination laptop PC. As of this writing, the laptop is a Panasonic Toughbook™ CF-73. The Examination PC needs to be loaded with specific utilities that are needed for interfacing with the PFL. These utilities include the PFL Button Bar and may also include FTK™ by AccessData (or another forensic analysis tool of the user's choice).

NOTE: This manual discusses the Examination PC as it is used with the PFL. Please refer to the Panasonic Toughbook™ User Manual for more information on the PC itself.

Software Installation

This section describes the steps necessary to load FTK™ and other software on the Examiner's PC. Please refer to these instructions if the software needs to be reinstalled on the Panasonic Toughbook™ or if the user wishes to substitute his or her own PC.

NOTE: FTK™ by Access Data is optional for the PFL. If it is not available, please refer to **Chapter 6 – Logicube Standalone Utilities**.

Loading FTK™ by AccessData

1. The Portable Forensic Laboratory™ comes with an installation CD-ROM for FTK™. Place this disk in the CD-ROM drive of your PC.
2. The CD-ROM should automatically bring up the installation wizard. If not, then go to Start –

Run and browse to the Setup.exe utility on the disk.

3. Follow the directions in the installation wizard and choose default locations for everything.
4. Once the software is loaded, be sure to install the Dongle Drivers which are included on the FTK™ CD-ROM.
5. Attach the green dongle to one of the active USB ports on your PC. This Dongle is necessary to launch FTK™.
6. Once the software is loaded, reboot the PC. When it comes back up, verify that FTK™ and the PFL Button Bar are installed on your PC.
7. If FTK™ does not boot or stops with an error message, you may need to reload the Dongle drivers separately. These drivers are located on the FTK™ CD-ROM in a separate location.

NOTE: The Portable Forensic Laboratory™ comes with a separate CD-ROM that contains a standalone version of the PFL Button Bar. This utility is offered for those who wish to use the PFL in situations where FTK™ is not available. Please refer to **Chapter 6 – Logicube Standalone Utilities** for more information.

Loading Adaptec USB drivers

The PFL utilizes a special SCSI to USB adapter that is made by Adaptec. Before SCSI drives can be accessed on the PFL, special drivers need to be installed on the Examiner's PC. These drivers are located on the Adaptec "USB2XCHANGE" CD-ROM that is included with the PFL.

1. The first time a SCSI drive is attached to the PFL, Windows on the Examiner's PC will request drivers.
2. Place the Adaptec Driver CD-ROM in the CD-ROM drive of your PC.
3. Point the "Add New Hardware" wizard to the CD-ROM drive. It will automatically detect and load the correct drivers.

NOTE: This procedure will need to be performed again if the PFL is plugged into a different USB port on the Examiner's PC.

Loading Windows98 USB Drivers

Sometimes it may become necessary to load USB drivers on an Examination or Suspect PC that is running Windows 98 or ME as the Operating System. These drivers can be found on the PFL CD-ROM in the WIN98 folder. Please follow these directions to load the software:

1. When the PFL is connected to the PC, the "Add New Hardware" wizard will appear.
2. You will be prompted to install drivers. At the "have disk…" prompt please point the PC to the drivers floppy (provided), and the installation should complete smoothly.
3. All connected drives are now visible in Windows as external drives. Any partitions that can be accessed by your Operating System will be assigned a Drive Letter.

The PFL Button Bar Overview

PFL ButtonBar.exe is the main switching utility for the Examiner's PC. It allows the user to switch between the Source Drive, Destination drive (inside the Duplicator), Suspect PC and Examiner's PC.

NOTE: Although the PFL Button Bar is installed along with FTK™, the user will need to launch the Button Bar and FTK™ separately.

This utility is made up of four major buttons. Please refer to Figure 8 below:

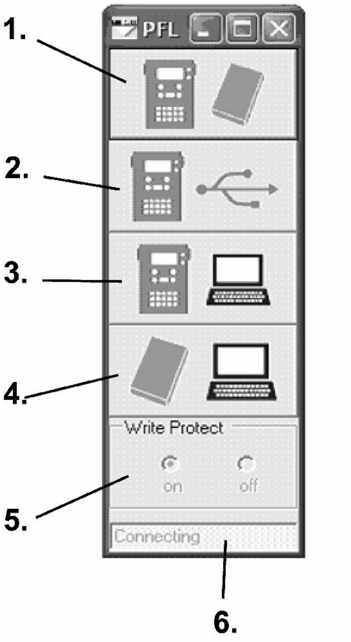


Figure 8 – PFL Button Bar

1. **Logicube Duplicator to Suspect Drive** – This mode connects the Source Drive to the Destination drive. It is used for DD Image Capturing. The Source Drive is Write Protected.
2. **Logicube Duplicator to USB Port for Examination** – This mode connects the Destination Drive to the Suspect PC USB port. A second Examination PC can also be connected to this port for investigating the drive. The Destination drive is not Write-Protected.
3. **Logicube Duplicator to Examiner's PC** – This mode connects the Destination Drive to the Examiner's PC. Write Protection can be turned on or off. This mode is used to examine the captured data as well as for SCSI drive capturing. (Please refer to **Chapter 5 – Other Capture Methods** for more information on SCSI capturing).

   NOTE: The Destination Drive needs to be in USB Mode for buttons 2 and 3. Please refer to the section "**Setting the Destination Drive to USB Mode**" in **Chapter 4 – Using the Portable Forensic Laboratory™**.

4. **Suspect Drive to Examiner's PC** – This mode connects the Source drive to the Examiner's PC. Write Protection is always on.
5. **Write Protection Switch** – This function allows the user to turn Write-Protection on or off.

Currently, only Mode 3 (Duplicator to Examiner's PC) is the only mode that allows optional Write-Protection.

6. **Connection Status** – This field shows whether or not the PFL Button Bar has a good connection to the PFL. It will constantly attempt a connection until successful, at which time it will read "connected".

FTK™ Overview

FTK™ by AccessData is a powerful forensic investigative tool. It is designed to examine captured data quickly and accurately. It also has a feature to control the PFL via remote control.

NOTE: This manual is concerned chiefly with FTK™ as it relates to the PFL. We highly recommend that you refer to the FTK™ User Manual for more information on this product.

NOTE: The PFL will also work with other forensic analysis tools, please refer to **Chapter 6 – Logicube Standalone Utilities** for more details.

Launching FTK™

1. From the Windows Desktop on the Examiner's PC, go to Start – Run – AccessData - FTK™.
2. When FTK™ comes up, it will immediately ask for a New Case, to Open an Existing Case or Exit. Please refer to Figure 9 below.

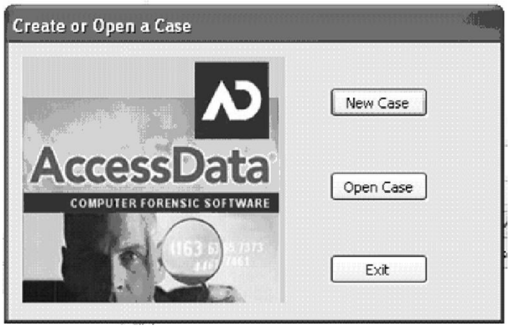


Figure 9 – FTK Welcome Screen

3. Choose New or Open Case and click "OK".
4. Once FTK™ is up and running, go to Tools – Logicube Forensic Dock.
5. If the PFL is powered up and connected properly, the Logicube Remote Control Interface will appear.

6. If the PFL is not connected correctly, an error message will pop up that reads “Error communicating with the Logicube Forensic Dock”. Check the USB connection between the Examiner’s PC and PFL.

   NOTE: Please contact Logicube Technical Support if you have any trouble connecting FTK™ to the PFL.

Remote Control Interface

Overview

The Remote Control Interface allows the user to connect the Destination drive to the Examination or Suspect PC, Capture the Source drive (with DD Image Capture Mode) and other similar functions.

Please refer to Figure 10 below:

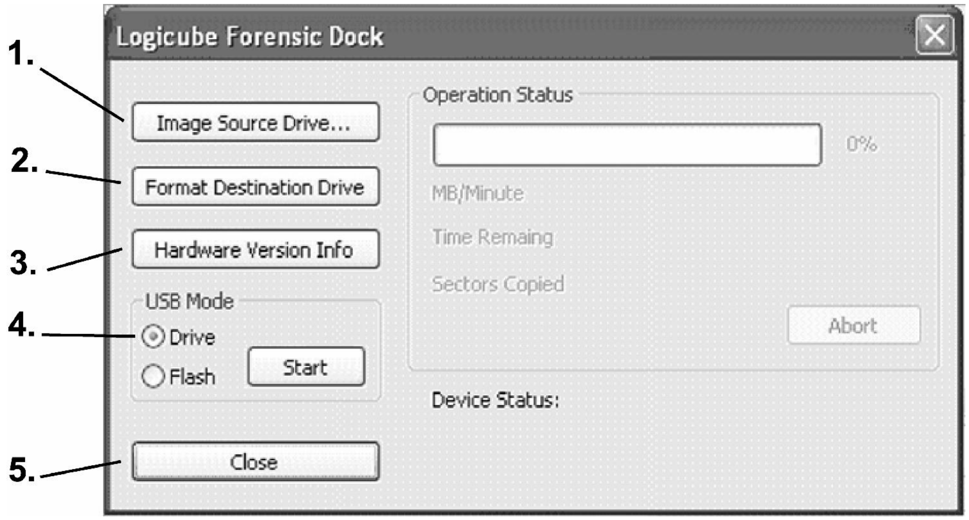


Figure 10 – FTK™ Remote Control Interface

The following descriptions are designed to introduce the reader to the different parts of the Remote Control Interface. Procedures for using this utility and the PFL Button Bar can be found in **Chapter 4 – Using the Portable Forensic Laboratory™**.

1. **Image Source Drive** – This function performs a DD Image Capture of the Source Drive to the Destination drive.
2. **Format Destination Drive** – This function formats the Destination Drive with a FAT32

partition. This step is necessary prior to running a DD Image Capture Session.

3. **Hardware Version Info** – This function queries the Logicube Duplicator and brings up information like serial number, Firmware version, etc.

4. **USB Mode** – This function sets the Destination Drive or Duplicator's Compact Flash drive into USB Mode. Once in USB Mode, either drive can be connected to the Examination or Suspect PC.

5. **Close** – This button exits the Remote Control Interface.

4. Using the Portable Forensic Laboratory™

Introduction

This chapter discusses the procedures for utilizing the PFL Button Bar and Remote Control Interface in FTK™, which are used for drive capturing and connecting drives to different PC's for examination.

The following instructions make use of the Remote Control Interface in FTK™. Instructions for using the PFL with other forensic tools are found in **Chapter 6 – Standalone Logicube Utilities**.

Starting the PFL

Please follow this step-by step procedure to set up the Portable Forensic Laboratory™ for use.

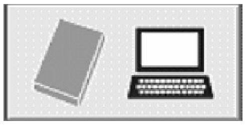
1. Attach the Source Drive and Logicube Duplicator to the PFL. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting drives.
2. Boot the Examiner's PC to Windows.
3. Attach the USB cable between the Examiner's PC and the PFL. Plug the cable into the USB port marked "To Laptop".
4. Attach any Flash-based media cards and USB Devices to the PFL. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting USB media.
5. Power up the PFL. Any devices in the card reader slots or extra USB ports should be immediately detected by the Examiner's PC.
6. If a second PC is to be connected to the PFL, go ahead and connect it now. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting the Suspect PC.

7. Launch the PFL Button Bar. Make sure that the Connection Status field reads “Connected”. If it remains on “Connecting”, then check the USB cable connection between the Examiner’s PC and PFL.
8. Launch FTK™ and open the Remote Control Interface by going to Tools – Logicube Forensic Dock. The Remote Control Interface should appear.

Connecting the Source Drive to Examiner’s PC

This procedure shows how to connect the Source (or Suspect) drive to the Examiner’s PC. This is useful for attaching the Source Drive to FTK™ for pre-capture analysis or comparison with the captured data.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.

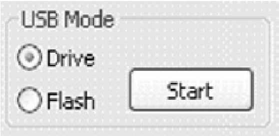


2. On the PFL Button Bar, click the fourth button down from the top. The Source Drive will power up.
3. After 5 – 7 seconds, the Source drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter. The Drive is always Write-Protected.
4. The drive can now be connected to FTK™ for analysis. Please refer to the FTK™ User Manual for more information.

Setting the Logicube Talon™ or MD5™ to USB Mode

Destination Drive

This procedure is necessary before the Destination drive can be connected to the Examiner’s or Suspect PC. It is performed through the Remote Control Interface in FTK™.



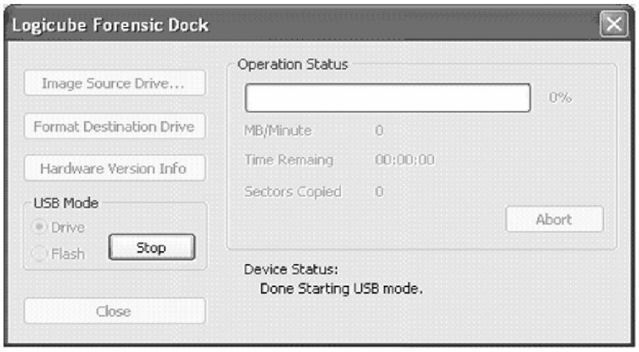
USB Mode

● Drive

○ Flash

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. In the Remote Control Interface, click the “Drive” radio button under “USB Mode”

3. Click the “Start” Button in the “USB Mode” box, a “Starting USB Mode” message will appear.
4. When the Duplicator is in USB Mode, a message will appear that reads: “Done Starting USB Mode”. See Figure 11 below.

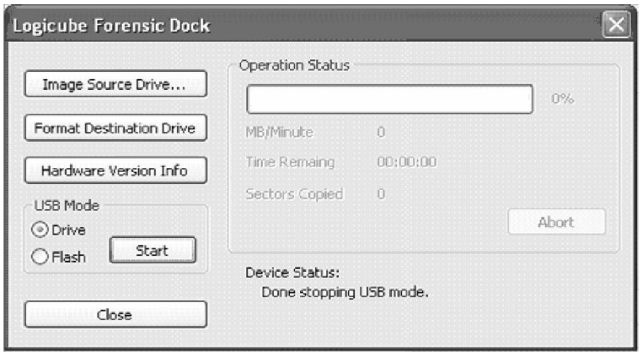


0%
MB/Minute 0
Time Remaing 00:00:00
Sectors Copied 0

Device Status:
Done Starting USB mode.

Figure 11 – USB Start Message.

5. To bring the Destination Drive out of USB Mode, click the “Stop” button. The Destination Drive will power off. When finished, a message will appear that reads: “Done Stopping USB Mode”. See Figure 12 below.

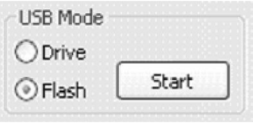


0%
MB/Minute 0
Time Remaing 00:00:00
Sectors Copied 0

Device Status:
Done stopping USB mode.

Figure 12 – USB Stop Message

Compact Flash



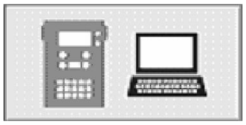
There may be instances where you need to connect the Forensic Talon or MD5’s Compact Flash (CF) Drive to the Examiner’s or Suspect PC. This is necessary if new Keywords or software updates need to be loaded on the unit.

NOTE: This procedure refers to the CF drive that is in the Logicube Talon™ or MD5™. It does not refer to the Flash-based media in the card reader slots.

The procedure for connecting the CF drive is very similar to the previous one:

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL.
2. In the Remote Control Interface, click the “Flash” radio button under “USB Mode”
3. Click the “Start” Button in the “USB Mode” box, a “Starting USB Mode” message will appear.
4. When the Duplicator is in USB Mode, a message will appear that reads: “Done Starting USB Mode”.
5. To bring the CF Drive out of USB Mode, click the “Stop” button. The Destination Drive will power off. When finished, a message will appear that reads: “Done Stopping USB Mode”.

Connecting the Destination Drive to Examiner’s PC

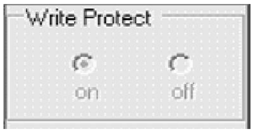


This procedure shows how to connect the Destination (or Evidence) drive to the Examiner’s PC. This is useful for attaching the captured data to FTK™ for post-capture analysis.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Set the Destination drive to USB Mode as described earlier in this chapter under “Setting the Logicube Talon™ or MD5™ to USB Mode”.
3. On the PFL Button Bar, click the third button down from the top.
4. After 5 – 7 seconds, the Destination drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter.
5. Write-Protection can be turned on or off. Please read the following section “Setting Write-Protect Status” for more information.
6. The drive can now be connected to FTK™ for analysis. Please refer to the FTK™ User Manual for more information.

Setting Write-Protect Status

When the Destination Drive is connected to the Examiner’s PC, Write Protection can be turned on



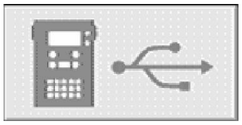
or off. Write Protection is necessary for captured data because it prevents new data being written to the drive (Windows is known to write data to the drive if it is connected via USB).

For instances where files need to be written to the Destination drive, write protection can be turned off.

Once the Destination drive is connected, set write-protect status with this procedure:

1. Go to the PFL Button Bar and click the "On" or "Off" radio buttons under the "Write Protect" field.
2. The Destination Drive will be briefly disconnected from the PC, then it will be reconnected with the new Write-Protection status.

Connecting the Destination Drive to Suspect PC



This procedure shows how to connect the Destination (or Evidence) drive to the Suspect PC. This is useful for copying files from the Suspect PC for later examination in FTK™. It is also necessary if the user wishes to clone data from the Suspect PC without removing the hard drive.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under "Starting the PFL".
2. Set the Destination drive to USB Mode as described earlier in this chapter under "Setting the Logicube Talon™ or MD5™ to USB Mode".
3. On the PFL Button Bar, click the second button down from the top.
4. After 5 – 7 seconds, the Destination drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter.
5. Write-Protection is always turned off.

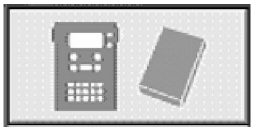
Connecting the CF Drive through USB Mode.

Since the Compact Flash (CF) Drive is connected to USB Mode the same way as the Destination drive, it can also be connected to the Examiner's or

Suspect PC. The same Write-Protection parameters apply.

Please follow the previous instructions for connecting the Destination drive. In the instructions, replace “Destination Drive” with “CF Drive”.

Connecting the Source Drive to Destination Drive



It is necessary to connect the Source Drive to the Destination drive prior to performing a DD Image capture. The Destination drive will also need to be brought out of USB Mode before the Source Drive can be captured.

The exception to this rule is when a SCSI drive is captured. This procedure is discussed later in this chapter under “Capturing SCSI Drives”.

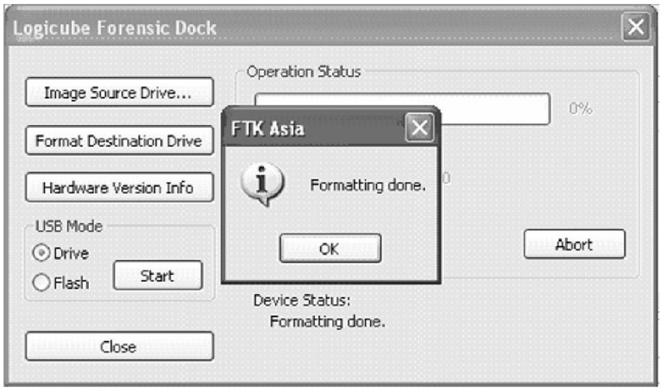
1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Make sure that the Destination Drive is out of USB Mode.
3. On the PFL Button Bar, click the top button. The Source Drive will power up.
4. Wait 3 – 5 seconds before performing any further actions on the Remote Control Interface.

Format Destination Drive

Formatting the Destination drive is a necessary step before a DD Image Capture session can be performed. This procedure is done from the Remote Control Interface of FTK™.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Make sure that the Source drive is connected to the Destination drive as described earlier in this chapter under “Connecting the Source drive to Destination drive”.
3. On the Remote Control Interface in FTK™, click the “Format Destination Drive” button.

4. FTK™ will Access the Destination drive and format it with a FAT32 partition. The Remote Control Interface will display the status of formatting.
5. When the format is done, a message box will prompt the user. See Figure 13 below:



Formatting done.

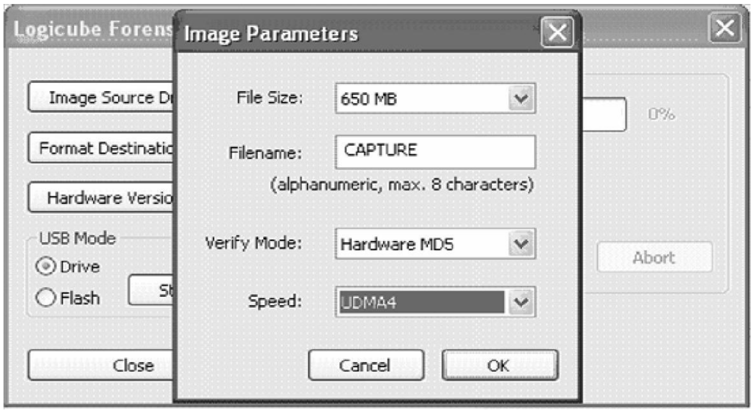
Device Status:
Formatting done.

Figure 13 – Destination Drive Format Completed.

Capturing PATA or SATA Source Drives

This procedure describes the steps necessary to capture data from the Source to the Destination drive. The data is captured in 650MB, 2GB or 4GB chunks and stored as “DDLinux” image files.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Make sure that the Source drive is connected to the Destination drive as described earlier in this chapter under “Connecting the Source drive to Destination drive”.
3. On the Remote Control Interface in FTK™, click the “Image Source Drive” button.
4. A Settings Window will appear where the Case name can be entered. The user can also set the size of Image Files, Speed and Verify settings. Please refer to Figure 14 below:



File Size: 650 MB

Filename: CAPTURE

(alphanumeric, max. 8 characters)

Verify Mode: Hardware MD5

Speed: UDMA4

Figure 14 – Image Parameters Screen

5. Set the "File Size" setting to 650MB, 2GB or 4GB. This determines the size of the Image files.

6. Enter a Case Name in the "Filename" setting. For best results, the name entered should be 8 characters or less.

7. Set the "Verify" setting to one of three choices:

   - **Hardware MD5** – This setting calculates the MD5 Hash for every sector that is captured. It increases the cloning time by 100%.

   - **Hardware CRC32** – This setting calculates the CRC32 Checksum value for every captured sector. It also increases the cloning time significantly.

   - **Software CRC32** – This setting only calculates the CRC32 Checksum for every 100,000th sector. It does not significantly increase cloning time.

8. Set the speed setting to the desired level. The different speeds are:

   - **UDMA-4** - The software performs a test procedure to determine the fastest setting that the drives will tolerate while streaming data from one to the other. When set to UDMA-4, all speeds grades below will be tested (i.e. UDMA0-4, PIO0-4)

   - **UDMA-3** - 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-2** - Same as **UDMA-4.**

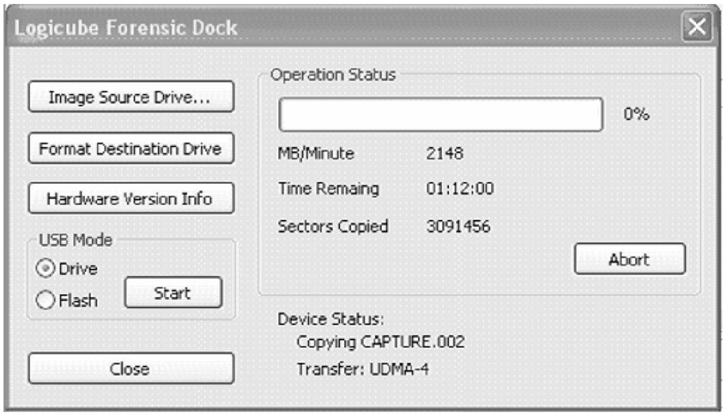
   - **UDMA-1** - Same as **UDMA-4.**

- **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.

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 MD5/CRC32 Hash value of each session could differ. This is because some bad sectors will read intermittently.

9. Once the Image Parameters are set properly, click the OK button.
10. 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.
11. A sub-directory (using the Case Name) will be created under the root directory on the destination drive.
12. 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.). The Remote Control Interface will show the Capturing speed, Time remaining, etc. It should look similar to Figure 15 below:



Operation Status

0%

MB/Minute 2148

Time Remaing 01:12:00

Sectors Copied 3091456

USB Mode

● Drive

○ Flash

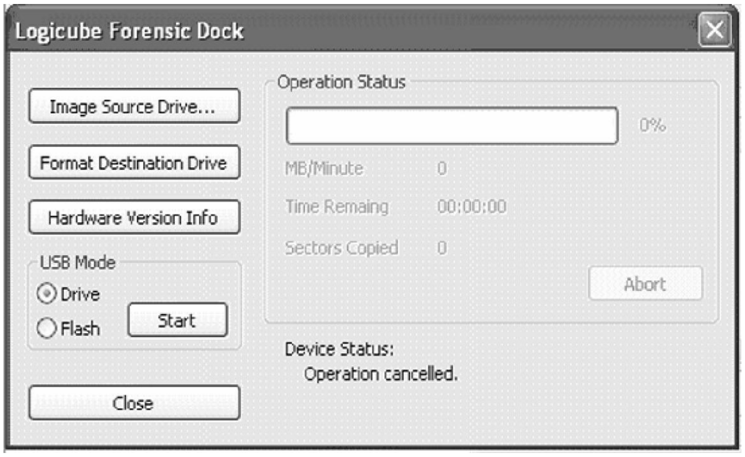
Device Status:
Copying CAPTURE.002
Transfer: UDMA-4

Figure 15 – Image Capture Progress Screen

13. 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 CF Drive. It includes (among other things), the SHA-256 Hash values of all captured DD files or the entire Source Drive. Refer to the **Special Settings** section below.
14. The capture ends with a “Capture Successful” message.

Aborting a Capture Session

The DD Image Capture Session can be aborted at any time simply by clicking the “Abort” button on the Remote Control Interface of FTK™. The screen will then look similar to Figure 16 below:



Operation Status

0%

MB/Minute 0

Time Remaing 00:00:00

Sectors Copied 0

USB Mode

● Drive

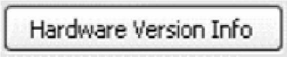
○ Flash

Device Status:
Operation cancelled.

Figure 16 – Image Capture Abort Screen

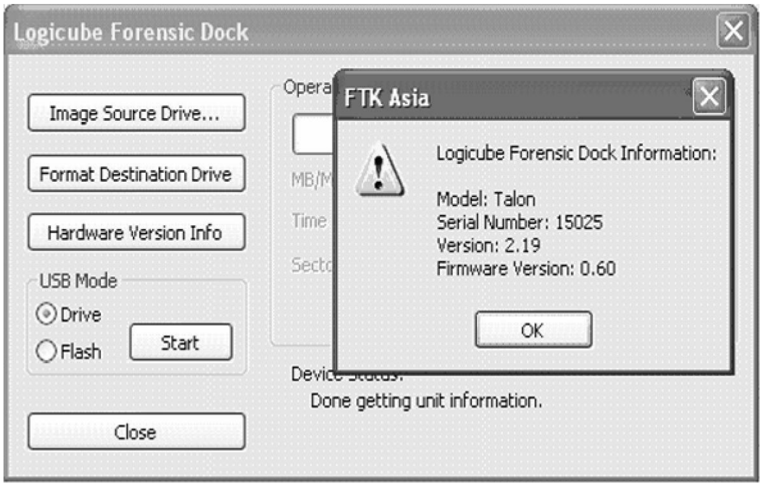
NOTE: The Abort command may take up to 2 – 3 minutes for the Image Capture session to end.

Hardware Version Info



The Remote Control Interface is also able to check the serial number, software and Firmware versions of the Forensic Talon or MD5.

Any time the Remote Control Interface is connected to the PFL, click the “Hardware Version Info” button. (See Figure 17 below).



Logicube Forensic Dock Information:

Model: Talon
Serial Number: 15025
Version: 2.19
Firmware Version: 0.60

Device Status:
Done getting unit information.

Figure 17 – Hardware Version Info

5. Other Drive Capture Methods

Introduction

This chapter deals with other procedures that can be performed with the Portable Forensic Laboratory™ in conjunction with FTK™. These procedures include Capturing SCSI, Flash or USB drives.

The main difference with cloning the aforementioned drives is that they cannot be connected directly to the Forensic Talon™ or MD5™. They need to actually be captured through FTK™ itself.

SCSI and USB Write Protection

As of this writing, SCSI drives are NOT write-protected when they are connected to the Examiner's PC. The same goes for any Flash and USB drives that are attached to the extra USB ports. It is possible for Windows to write data to the drives as they are connected.

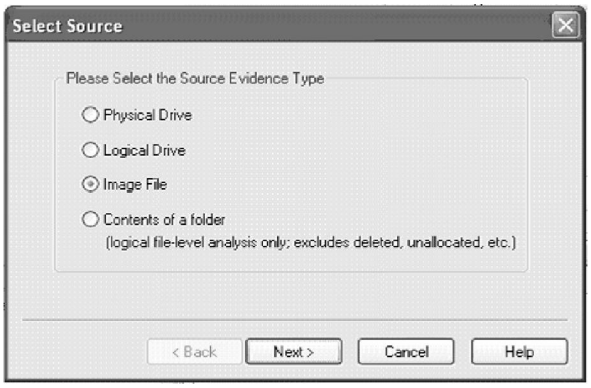
There are some alternate methods to enable write protection on SCSI and USB drives:

- Many SCSI drives have a write-protect jumper that can be enabled. Refer to your drive's documentation to determine if this jumper is available.
- Many USB drives have a small toggle switch that enables write-protection. Refer to your drive's documentation to determine if this feature is available.
- A third-party write blocking device can be employed. One example is the *SCSI Write Blocker* manufactured by Paralan Corporation.

Also, the use of FTK™ to capture data from SCSI and USB drives will minimize any risk of drive content change. Please refer to the procedures below for more details on capturing SCSI and USB drives.

Capturing SCSI drives

1. Make sure that the Portable Forensic Laboratory™ is set up as described in the last chapter under “Starting the PFL”.
2. Make sure that the Source drive is connected to the Destination drive as described in the last chapter under “Connecting the Source drive to Destination drive”.
3. Wait until the SCSI drive is fully connected to the Examiner’s PC. You may need to open the Device Manager to see the drive. To do this go to Start – Control Panel – System – Hardware – Device Manager, then expand the “Drives” tree.
4. In FTK™, go to Tools – Logicube Forensic Dock to open the Remote Control Interface.
5. If needed, format the Destination drive as described in the last chapter under “Format Destination Drive”.
6. Set the Destination Drive into USB Mode. Follow the instructions in the last chapter under “Setting the Logicube Talon™ or MD5™ into USB Mode”.
7. The Destination drive will eventually connect to the Examiner’s PC. It will appear under “My Computer” with a drive letter. The Volume Label is “DD_Logicube”.
8. Move the Remote Control Interface off to the side of the Desktop.
9. In FTK™, click on the “Create Disk Image” icon.
10. A prompt will come up asking for the type of Source Drive. Choose “Physical”. See Figure 18 below.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

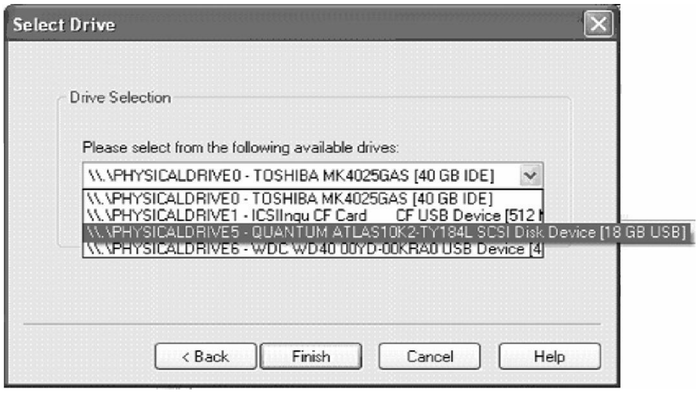
○ Logical Drive

● Image File

○ Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Figure 18 – Select Source Evidence Type

11. The next prompt will ask for the Source Drive. Choose the SCSI drive from the drop-down list. See Figure 19 below for an example.



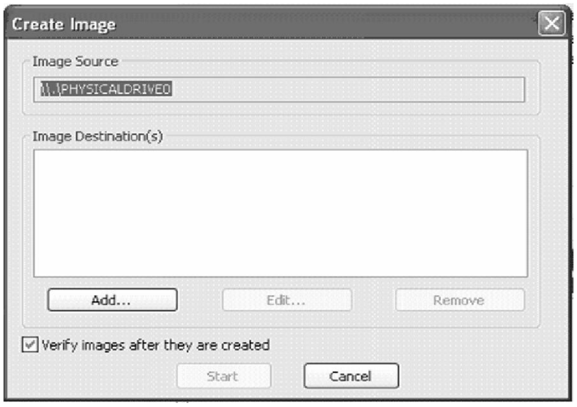
Please select from the following available drives:

\\.\PHYSICALDRIVE0 - TOSHIBA MK4025GAS [40 GB IDE]

\\.\PHYSICALDRIVE0 - TOSHIBA MK4025GAS [40 GB IDE]
\\.\PHYSICALDRIVE1 - ICSIInqu CF Card CF USB Device [512 I
\\.\PHYSICALDRIVE5 - QUANTUM ATLAS10K2-TY184L SCSI Disk Device [18 GB USB]
\\.\PHYSICALDRIVE6 - WDC WD40 00YD-00KRA0 USB Device [4

Figure 19 – Select Source Drive

12. The next prompt will show the chosen source drive in the “Source” field. Click on the Add button. See Figure 20 below.



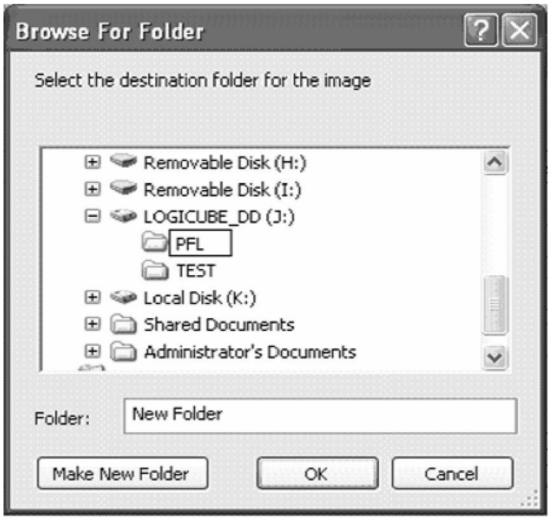
\\.\PHYSICALDRIVE0

☑ Verify images after they are created

Figure 20 – Source drive Selected

13. Browse through the Directory Tree until you come to the Destination Drive. Expand it and Click the “Add New Folder: button.

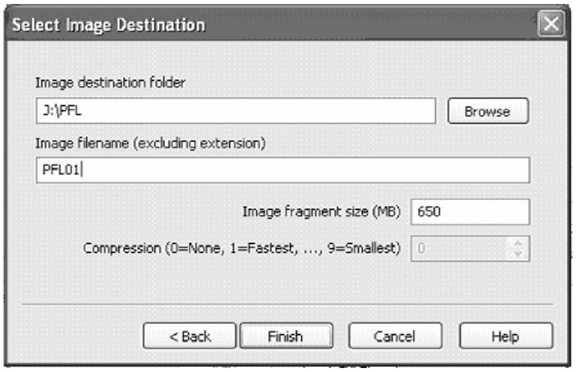
14. Name the folder with your case name. Keep the case name at 8 characters or less. Then click the OK button. See Figure 21 below.



Folder: New Folder

Figure 21 – Destination Folder

15. The next prompt will show the path to your Destination folder in the top field. Add your Case Name to the field below that. In the next field, choose the size of your DD Image Files (we recommend 650 MB, 2GB or 4GB in size). See Figure 22 below.



Select Image Destination

Image destination folder: J:\PFL

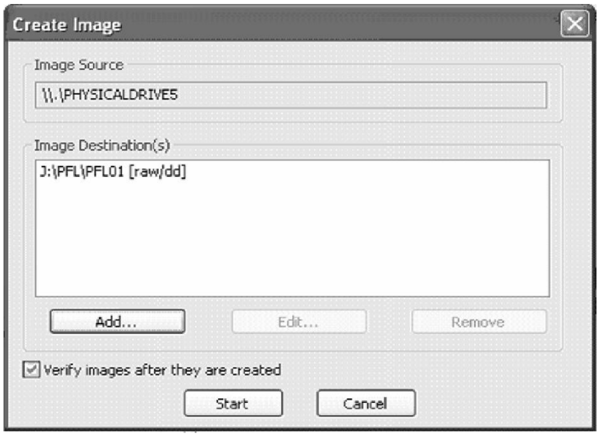
Image filename (excluding extension): PFL01

Image fragment size (MB): 650

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Figure 22 – Final Image Capture Settings

16. Once finished, click the “Finished” button. The next prompt will Show both the Source and Destination drives. Click on the “Verify Images After They are Created” checkbox if you wish to verify the data after capture. See Figure 23 below.



Create Image

Image Source: \\.\PHYSICALDRIVE5

Image Destination(s): J:\PFL\PFL01 [raw/dd]

☑ Verify images after they are created

Figure 23 – Image Capture Start Screen

17. Click the “Start” button to begin.

18. A Progress Window will come up that shows a Progress Bar as well as speed (in MB/sec), Time elapsed and Time Remaining. It also shows the current DD Image file. See Figure 24 below.

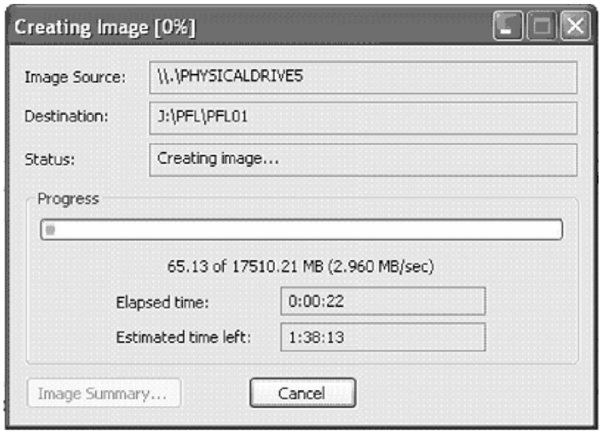


Image Source: \\.\PHYSICALDRIVE5

Destination: J:\PFL\PFL01

Status: Creating image...

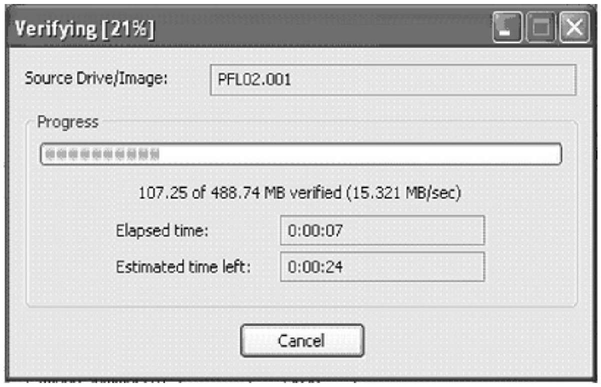
65.13 of 17510.21 MB (2.960 MB/sec)

Elapsed time: 0:00:22

Estimated time left: 1:38:13

Figure 24 – Image Capture Progress Screen

19. If the “Verify Data. . .” checkbox was checked before cloning, FTK™ will verify the data that was copied. This process takes significantly less time than capturing. See Figure 25 below.



Source Drive/Image: PFL02.001

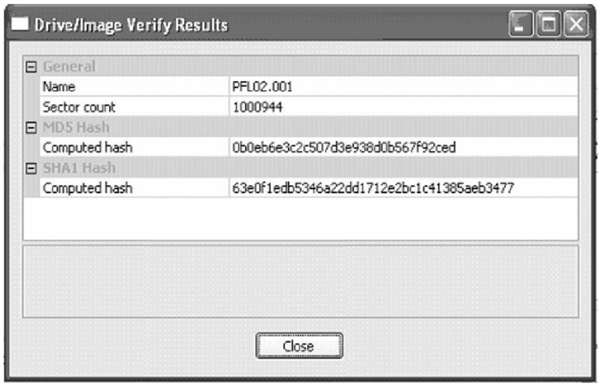
107.25 of 488.74 MB verified (15.321 MB/sec)

Elapsed time: 0:00:07

Estimated time left: 0:00:24

Figure 25 – Image Capture Verify Screen

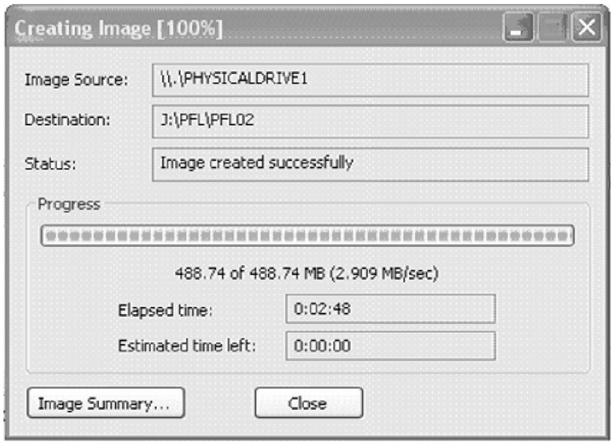
20. When the Verify process is finished, FTK™ will display the Image file names that were created as well as their MD5 and SHA-1 Hash Values. This data is also saved to a log file in the destination folder. See Figure 26 below.



⊟ General	
Name	PFL02.001
Sector count	1000944
⊟ MD5 Hash	
Computed hash	0b0eb6e3c2c507d3e938d0b567f92ced
⊟ SHA1 Hash	
Computed hash	63e0f1edb5346a22dd1712e2bc1c41385aeb3477

Figure 26 – Image Verify Results Screen

21. When the Drive/Image Verify Results window is closed, the Progress Screen shows that the Image was created successfully. The Summary Results can be displayed again by clicking the “Image Summary” button. See Figure 27 below.



Creating Image [100%]

Image Source: \\.\PHYSICALDRIVE1

Destination: J:\PFL\PFL02

Status: Image created successfully

Progress

488.74 of 488.74 MB (2.909 MB/sec)

Elapsed time: 0:02:48

Estimated time left: 0:00:00

Figure 27 – Image Completion Screen

Capturing Flash Media and USB Drives

Flash-based Media cards in the PFL’s card reader slots can be captured to the Destination drive just like SCSI drives. Likewise for USB drives that are attached to the PFL’s extra USB ports (not the Examiner’s PC or Suspect PC ports).

The Capturing process is essentially the same as it is for SCSI drives. The only difference is that there is no need to attach the Source drive through the PFL Button Bar.

Please follow this procedure:

1. Connect any Flash-based media cards to the PFL card reader slots as outlined in **Chapter 2 – Getting Started**.
2. Connect any write-protected USB devices to the PFL USB Ports as outlined in **Chapter 2 – Getting Started**.
3. Follow steps 4 – 21 in the previous procedure, “Capturing SCSI Drives”.

Capturing a Suspect PC via USB

This procedure describes the process for capturing a Suspect PC that is attached to the "Suspect PC" USB port of the Portable Forensic Laboratory. The data will be captured to the Destination drive inside the Logicube Talon™ or MD5™.

For this process to work, the user will need to have a copy of the Logicube Forensic USB Capturing Software. This software comes on a floppy disk that is provided with every Logicube Talon™ unit. It also comes with the Write PROtect Dongle™ for the Logicube MD5™.

1. Boot the Suspect PC with the bootable floppy. The floppy is configured to load the USB drivers, and run our client application. You might need to update your PC's CMOS settings to allow booting from a floppy drive.
2. Attach the USB cable to the "Suspect PC" USB port on the PFL. Do not attach the other end to the Suspect PC yet.
3. Attach a hard drive to the Destination position of your Logicube Talon™ or MD5™, and attach the unit to the PFL. Please refer to **Chapter 2 – Getting Started** for more details.
4. Set the Talon™ or MD5™ to USB Mode either through the Remote Control Interface in FTK™, or directly from the control buttons.
5. On the Examiner's PC, set the Button Bar to Mode 3 – Attach Duplicator to Suspect PC. Please refer to **Chapter 4 – Using the Portable Forensic Laboratory™** for more details.
6. On the Suspect PC, watch for a screen that prompts you to "attach the USB cable and hit any key when ready". Attach the USB cable to the PC™.
7. The PC client software should now detect the presence of the PFL, a link will be created and a white box will appear briefly on the screen. This screen shows the model number of the Destination drive. Press any key to continue.
8. You should now see on your PC screen a virtual control panel that resembles the overlay on the Logicube MD5™.
9. All functions will now be controlled from this virtual control panel in the exact same way they are used on the Logicube Talon™ or MD5™.

NOTE: Please refer to the Logicube MD5™ or Talon™ User Manual for proper cloning procedures.

10. After setting the cloning mode and any other settings desired on the virtual control panel, press the "START/STOP" button twice to start the operation.

NOTE: Instead of referring to drives as Source and Destination, the USB Cloning software refers to them as "PC" and "USB".

NOTE: In rare situations, the floppy will fail to fully boot due to lack of sufficient memory to load the drivers. We provide a flavor of DOS called CALDERA DR. DOS on the floppy. Installing WIN98 DOS over DR DOS can sometimes solve this problem. To do that, open a DOS window under Win98, change directories to c:\windows\command and type "sys a:" (assuming the floppy is in drive A). You would also need to copy himem.sys to the floppy.

6. Standalone Logicube Utilities

Introduction

The Portable Forensic Laboratory™ does not only work with FTK™ by Access Data. It can be used with other forensic analysis tools, or even by itself. Most of the same procedures can be performed to connect drives to USB, capture drives or analyze data.

This chapter looks at the procedures that were explored in the previous two chapters and suggests methods of performing the same function without FTK™.

Software Installation

This section describes how to load the PFL Button Bar utility that is located on the Portable Forensic Laboratory™ CD-ROM.

NOTE: This version of the PFL Button Bar is identical to the one that is installed with FTK™.

Loading the PFL Button Bar

1. Place the PFL CD-ROM in the CD_ROM drive of the Examiner’s PC.
2. Open the “PFL ButtonBar” folder that resides on the CD-ROM.
3. Copy the following files to a folder on the Examiner’s PC hard drive: *PFLButtonBar.exe, msvcr71.dll, MD5Remote.dll*.

NOTE: We recommend writing the files to a folder labeled “Logicube” on your C drive.

4. Make a shortcut to *PFLButtonBar.exe* and copy it to the Desktop.
5. Exit Windows Explorer and run the PFL Button Bar. If it fails to load or stops with an error

message, you may need to load DotNet by Microsoft.

NOTE: The DotNet framework is a shareware utility from Microsoft Corporation that is necessary to run DotNet – based applications like the PFL Button Bar.

6. Go back to the PFL CD-ROM and open the "MS DotNet" folder. Run *dotnetfx.exe*.
7. Follow the installation wizard and reboot the PC when necessary. Once DotNet is loaded, run the PFL Button Bar to make sure that it comes up.

Loading Adaptec USB drivers

The PFL utilizes a special SCSI to USB adapter that is made by Adaptec. Before SCSI drives can be accessed on the PFL, special drivers need to be installed on the Examiner's PC. These drivers are located on the Adaptec "USB2XCHANGE" CD-ROM that is included with the PFL.

1. The first time a SCSI drive is attached to the PFL, Windows on the Examiner's PC will request drivers.
2. Place the Adaptec Driver CD-ROM in the CD-ROM drive of your PC.
3. Point the "Add New Hardware" wizard to the CD-ROM drive. It will automatically detect and load the correct drivers.

NOTE: This procedure will need to be performed again if the PFL is plugged into a different USB port on the Examiner's PC.

Loading Windows98 USB Drivers

Sometimes it may become necessary to load USB drivers on an Examination or Suspect PC that is running Windows 98 or ME as the Operating System. These drivers can be found on the PFL CD-ROM in the WIN98 folder. Please follow these directions to load the software:

1. When the PFL is connected to the PC, the "Add New Hardware" wizard will appear.
2. You will be prompted to install drivers. At the "have disk…" prompt please point the PC to the drivers floppy (provided), and the installation should complete smoothly.
3. All connected drives are now visible in Windows as external drives. Any partitions that can be

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

The PFL Button Bar Overview

PFL ButtonBar.exe is the main switching utility for the Examiner's PC. It allows the user to switch between the Source Drive, Destination drive (inside the Duplicator), Suspect PC and Examiner's PC.

NOTE: Although the PFL Button Bar is installed along with FTK™, the user will need to launch the Button Bar and FTK™ separately.

This utility is made up of four major buttons. Please refer to Figure 8 below.

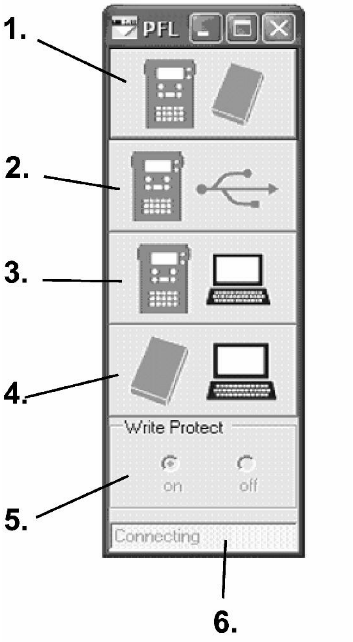


Figure 8 – PFL Button Bar

1. **Logicube Duplicator to Suspect Drive** – This mode connects the Source Drive to the Destination drive. It is used for DD Image Capturing. The Source Drive is Write Protected.
2. **Logicube Duplicator to USB Port for Examination** – This mode connects the Destination Drive to the Suspect PC USB port. A second Examination PC can also be connected to this port for investigating the drive. The Destination drive is not Write-Protected.

3. **Logicube Duplicator to Examiner's PC** – This mode connects the Destination Drive to the Examiner's PC. Write Protection can be turned on or off. This mode is used to examine the captured data as well as for SCSI drive capturing. (Please refer to **Chapter 5 – Other Capture Methods** for more information on SCSI capturing).

   NOTE: The Destination Drive needs to be in USB Mode for buttons 2 and 3. Please refer to the section "**Setting the Destination Drive to USB Mode**" in **Chapter 4 – Using the Portable Forensic Laboratory™**.

4. **Suspect Drive to Examiner's PC** – This mode connects the Source drive to the Examiner's PC. Write Protection is always on.
5. **Write Protection Switch** – This function allows the user to turn Write-Protection on or off. Currently, only Mode 3 (Duplicator to Examiner's PC) is the only mode that allows optional Write-Protection.
6. **Connection Status** – This field shows whether or not the PFL Button Bar has a good connection to the PFL. It will constantly attempt a connection until successful, at which time it will read "connected".

Starting the PFL

Please follow this step-by step procedure to set up the Portable Forensic Laboratory™ for use.

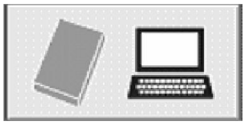
1. Attach the Source Drive and Logicube Duplicator to the PFL. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting drives.
2. Boot the Examiner's PC to Windows.
3. Attach the USB cable between the Examiner's PC and the PFL. Plug the cable into the USB port marked "To Laptop".
4. Attach any Flash-based media cards and USB Devices to the PFL. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting USB media.
5. Power up the PFL. Any devices in the card reader slots or extra USB ports should be immediately detected by the Examiner's PC.

6. If a second PC is to be connected to the PFL, go ahead and connect it now. Please refer to **Chapter 2 - Getting Started** for detailed instructions on connecting the Suspect PC.
7. Launch the PFL Button Bar. Make sure that the Connection Status field reads “Connected”. If it remains on “Connecting”, then check the USB cable connection between the Examiner’s PC and PFL.

Connecting the Source Drive to Examiner’s PC

This procedure shows how to connect the Source (or Suspect) drive to the Examiner’s PC. This is useful for attaching the Source Drive to FTK™ for pre-capture analysis or comparison with the captured data.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.



2. On the PFL Button Bar, click the fourth button down from the top. The Source Drive will power up.
3. After 5 – 7 seconds, the Source drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter. The Drive is always Write-Protected.
4. The drive can now be connected to forensic analysis software for examination. Please refer to your software’s User Manual for more information.

Setting the Logicube Talon™ or MD5™ to USB Mode

Destination Drive

This procedure is necessary before the Destination drive can be connected to the Examiner’s or Suspect PC. It is performed directly on the Forensic Talon™ or MD5™ itself.

Please refer to your Forensic Talon™ or MD5™ User Manual for the procedure on setting the unit to USB Mode.

Compact Flash

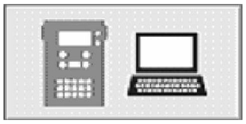
There may be instances where you need to connect the Forensic Talon or MD5’s Compact Flash (CF)

Drive to the Examiner’s or Suspect PC. This is necessary if new Keywords or software updates need to be loaded on the unit.

NOTE: This procedure refers to the CF drive that is in the Logicube Talon™ or MD5™. It does not refer to the Flash-based media in the card reader slots.

The procedure for connecting the CF drive is very similar to the previous one. Please consult your Talon™ or MD5™ User Manual for more information.

Connecting the Destination Drive to Examiner’s PC



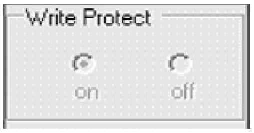
This procedure shows how to connect the Destination (or Evidence) drive to the Examiner’s PC. This is useful for attaching the captured data to FTK™ for post-capture analysis.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Set the Destination drive to USB Mode as described earlier in this chapter under “Setting the Logicube Talon™ or MD5™ to USB Mode”.
3. On the PFL Button Bar, click the third button down from the top.
4. After 5 – 7 seconds, the Destination drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter.
5. Write-Protection can be turned on or off. Please read the following section “Setting Write-Protect Status” for more information.
6. The drive can now be connected to forensic analysis software for examination. Please refer to your software’s User Manual for more information.

Setting Write-Protect Status

When the Destination Drive is connected to the Examiner’s PC, Write Protection can be turned on or off. Write Protection is necessary for captured data because it prevents new data from being written to the drive (Windows is known to write data to the drive if it is connected via USB).

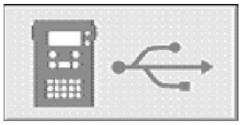
For instances where files need to be written to the Destination drive, write protection can be turned off.



Once the Destination drive is connected, set write-protect status with this procedure:

1. Go to the PFL Button Bar and click the “On” or “Off” radio buttons under the “Write Protect” field.
2. The Destination Drive will be briefly disconnected from the PC, then it will be reconnected with the new Write-Protection status.

Connecting the Destination Drive to Suspect PC



This procedure shows how to connect the Destination (or Evidence) drive to the Suspect PC. This is useful for copying files from the Suspect PC for later examination with forensic analysis software.

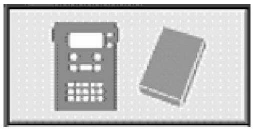
1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Set the Destination drive to USB Mode as described earlier in this chapter under “Setting the Logicube Talon™ or MD5™ to USB Mode”.
3. On the PFL Button Bar, click the second button down from the top.
4. After 5 – 7 seconds, the Destination drive will enumerate in the Windows Device Manager. If the partition on the hard drive is readable by your Operating System, it will be assigned a drive letter.
5. Write-Protection is always turned off.

Connecting the CF Drive through USB Mode.

Since the Compact Flash (CF) Drive is connected to USB Mode the same way as the Destination drive, it can also be connected to the Examiner’s or Suspect PC. The same Write-Protection parameters apply.

Please follow the previous instructions for connecting the Destination drive. In the instructions, replace “Destination Drive” with “CF Drive”.

Connecting the Source Drive to Destination Drive



It is necessary to connect the Source Drive to the Destination drive prior to performing a DD Image capture. The Destination drive will also need to be brought out of USB Mode before the Source Drive can be captured.

The exception to this rule is when a SCSI drive is captured. This procedure is discussed in a later section under “Capturing SCSI Drives”.

1. Make sure that the Portable Forensic Laboratory™ is set up as described earlier in this chapter under “Starting the PFL”.
2. Make sure that the Destination Drive is out of USB Mode.
3. On the PFL Button Bar, click the top button. The Source Drive will power up.
4. Wait 3 – 5 seconds before performing any further actions on the Talon™ or MD5™.

Format Destination Drive

Formatting the Destination drive is a necessary step before a DD Image Capture session can be performed. This procedure is done from the Forensic Talon™ or MD5™.

Please refer to your Forensic Talon™ or MD5™ User Manual for the procedure on formatting the Destination Drive.

Capturing PATA or SATA Source Drives

This procedure describes the steps necessary to capture data from the Source to the Destination drive. The data is captured in 650MB, 2GB or 4GB chunks and stored as “DDLinux” image files.

1. Make sure that the Portable Forensic Laboratory™ is set up as described in an earlier section under “Starting the PFL”.
2. Make sure that the Source drive is connected to the Destination drive as described in an earlier

section under “Connecting the Source drive to Destination drive”.

3. Please refer to your Forensic Talon™ or MD5™ User Manual for the procedure on running a DD Image Capture session.

Hardware Version Info

The serial number, software version and Firmware version of the Forensic Talon™ or MD5™ can be determined by going to the About Screen of the unit itself.

Please refer to your Forensic Talon™ or MD5™ User Manual for the procedure on accessing the About Screen.

Capturing SCSI drives

The main difference between cloning SCSI drives vs. PATA/SATA drives is that they cannot be connected directly to the Forensic Talon™ or MD5™. The only way to capture a SCSI drive is through the Examiner’s PC with forensic analysis software or another software-based capture method.

NOTE: Most forensic analysis software packages include a method for capturing data from one drive to another. Refer to your software’s User Manual for more information.

NOTE: As of this writing, SCSI drives are NOT write-protected when they are connected to the Examiner’s PC. Please refer to “*SCSI and USB Write Protection*” in **Chapter 5 – Other Capturing Methods** for alternate methods to write protect SCSI drives.

1. Make sure that the Portable Forensic Laboratory™ is set up as described in an earlier section under “Starting the PFL”.
2. Make sure that the Source drive is connected to the Destination drive as described in an earlier section under “Connecting the Source drive to Destination drive”.
3. Wait until the SCSI drive is fully connected to the Examiner’s PC. You may need to open the Device Manager to see the drive. To do this go to Start – Control Panel – System – Hardware – Device Manager, then expand the “Drives” tree.

4. If needed, format the Destination drive as described earlier in this chapter.
5. Set the Destination Drive into USB Mode. Follow the instructions earlier in this chapter under "Setting the Logicube Talon™ or MD5™ into USB Mode".
6. The Destination drive will eventually connect to the Examiner's PC. It will appear under "My Computer" with a drive letter. The Volume Label is "DD_Logicube".
7. Refer to your software's instructions for capturing data from one drive to another. Choose the SCSI drive as your Source drive and the Destination drive as the "Evidence" drive.

Capturing Flash Media and USB Drives

Flash-based Media cards in the PFL's card reader slots can be captured to the Destination drive just like SCSI drives. Likewise for USB drives that are attached to the PFL's extra USB ports (not the Examiner's PC or Suspect PC ports).

The Capturing process is essentially the same as it is for SCSI drives. The only difference is that there is no need to attach the Source drive through the PFL Button Bar.

NOTE: As of this writing, drives connected to the extra USB ports are NOT write-protected when they are connected to the Examiner's PC. Please refer to "*SCSI and USB Write Protection*" in **Chapter 5 – Other Capturing Methods** for alternate methods to write protect USB drives.

Please follow this procedure:

1. Connect any Flash-based media cards to the PFL card reader slots as outlined in **Chapter 2 – Getting Started**.
2. Connect any write-protected USB devices to the PFL USB Ports as outlined in **Chapter 2 – Getting Started**.
3. Follow steps 4 – 7 in the previous procedure,

7. Frequently Asked Questions and Answers

Q. I would like to use my Logicube Forensic Talon™ or MD5™ without the PFL. How do I do this?

A. The Forensic Talon™ and MD5™ are both designed to be self-contained forensic cloning devices. Please refer to your unit's User Manual for usage instructions.

Q. I switched Source or Destination drives and now the new drive won't come up.

A. This can sometimes happen if a drive is changed while the PFL is powered and the PFL Button Bar and/or FTK™ are running. Save your progress in FTK™, then shut down both FTK™ and the PFL Button Bar. Restart PFL Button Bar first, followed by FTK™.

Q. Will the Remote Control Interface come up if I am using Encase™ by Guidance Software, or another Forensic utility different than FTK?

A. No, the Remote Control Interface is a part of FTK™. The PFL Button Bar and PFL itself work fine with other forensic software packages. Please refer to **Chapter 6 – Logicube Standalone Utilities** for more information.

Q. Can I make bootable "Clone" with the Portable Forensic Laboratory™?

A. No, the Portable forensic Laboratory deals mainly with DD Image files when capturing a drive. These files are not bootable, however they contain a complete copy of the data for analysis.

Q. I know that the extra USB Ports on the PFL are not write-protected, but my USB Drive has a Write-Protect switch on it, will this protect my data for forensic capturing purposes.

A. Yes, although Logicube is not responsible for the Write-Protection ability of third-party vendors.

Q. I cannot detect a Western Digital HDD in the Source or Destination drive position of the PFL.

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. Drive information as displayed on the Forensic Talon™ 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. I am working in FTK™ after capturing a drive, but when I try to do anything I get a "Can't Find Dirent" error. What does this mean?

A. This error occurs if the Destination Drive is connected to the Examiner's PC with the PFL Button Bar and the Remote Control Interface. If the Button Bar mode is switched (Connect the Destination drive to the Suspect PC, for example), and then FTK is accessed, it will not be able to find the Destination drive and it will bring up this error. If you switch the Destination back to the Correct Mode (Connect Destination Drive to Examiner's PC) then the error message will not come up anymore.

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.

8. Index

19755 Nordhoff Pl., Chatsworth, CA 91311, Tel: 818 700 8488, Fax: 818 700 8466, www.logicube.com

For further assistance please contact Logicube Technical Support at: 818 700 8488 ext. 3, or by email to techsupport@logicube.com. Hours are 7:00am to 6:00pm PST M – F.