Massive Portable Forensic Storage (MPFS™)
User's Manual

Logicube, Inc.

Chatsworth, CA 91311

818 700 8488

Version: 1.0

MAN-MPFS

Date: 06/22/2010

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.

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 MPFS™

Introduction

Forensic investigators who need to capture large amounts of evidence data or need to transport sensitive data from the field to the lab will appreciate the convenience of the MPFS™.

The MPFS provides up to 8 TB of forensic data storage and connects seamlessly to the Forensic Dossier® data capture solution. Users can capture forensic data from suspect hard drives via the Dossier directly into evidence drives stored safely and securely within the MPFS. The MPFS eliminates the need to handle bulky sets of hard drives and reduces the risk of damaging sensitive hard drives during transport or compromising chain of custody.

A small footprint and convenient recessed “grip” areas on each side of the chassis make the MPFS easy to transport. The “always-on” cholesteric display allows users to identify contents at a glance making it convenient for archiving evidence data for future analysis.

Specifications

Power Requirements	90 to 240VAC 50 to 60Hz
Power Consumption	<170 watts
Operating Temperature	10°-35°C (50°-95°F)
Relative Humidity	10%-80%
Net Weight	3lbs 14oz (w/o drives)
Dimensions	10.5” X 8.3” X 2.5”
Agency Approvals	RoHs compliant

Features

- Provides up to 8 TB of write-protected data storage in a 4 drive tray configuration
- Supports 3.5” SATA drives, (each drive with a maximum capacity 2 TB), arranged in a 2 or 4 drive configuration
- The MPFS™ works seamlessly with the Forensic Dossier®. Simply connect the Dossier “head” to the MPFS base to immediately capture suspect drive data directly to the MPFS (will support both DD image and E01 file format capture modes, will not support Native capture mode)
- Stores multiple evidence capture sessions to hard disk drives in a JBOD configuration
- The MPFS features a compact footprint which makes it easy to transport from field to lab environments
- The Cholesteric “always on” battery-powered display requires no power and allows you to identify contents by file/case names at a glance.
- Available without hard disk drives or in 4 “drive-populated” versions; 1 TB, 4 TB, 6 TB and 8 TB
- Multiple cooling fans to protect your data

- The MPFS allows direct connection to a PC via FireWire 400, USB 2.0 or eSATA. Write-protected ports allow you to preview or transfer data from the MPFS to a PC. (***Note: When using the FireWire and USB ports for data transfer to a PC, MPFS will support a maximum capacity of 2 TB. eSATA port must be used for capacities greater than 2 TB. A 64-bit Operating System must be used for capacities greater than 2 TB)***

- The MPFS features a ruggedized chassis that provides superior protection to hard drives stored in MPFS

- Compatible with the NETConnect™ network module

Using this guide

This user guide is made up of 12 sections:

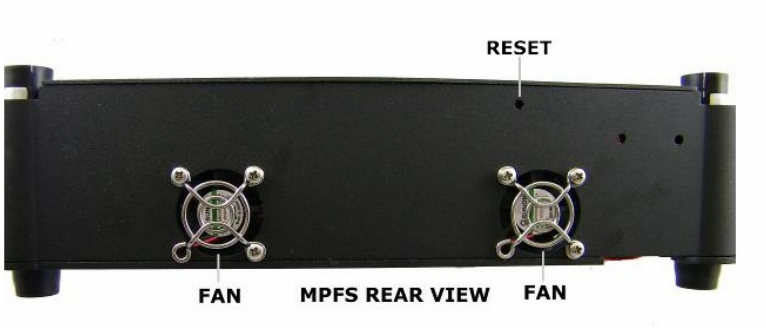
- Introduction
- Getting Started
- Using MPFS with the Forensic Dossier
- Drive Capture Modes & Settings
- Other Modes
- eSATA, USB and FireWire Connection
- Keyword Searching
- Using NETConnect™ with MPFS
- Software and Firmware Loading Instructions
- Reference
- FAQ's
- Index

System description

The MPFS™ includes the following:

- USB and eSATA cables
- Power supply
- Users' Guide on CD-ROM
- Magnetic screwdriver
- "0" drive configuration ships with drive mounting brackets and hardware to install hard disk drives
- Other configurations ship with hard drives pre-installed by Logicube

MPFS™


RESET
FAN
MPFS REAR VIEW
FAN


MPFS SIDE VIEW
RECESSED GRIP


MPFS™
INTERIOR VIEW

2. Getting Started

HARD DISK DRIVE INSTALLATION

Your MPFS was purchased in a “0” drive configuration or with hard disk drives pre-installed. If your MPFS already has drives installed proceed to the next section.

Either two or four hard disk drives can be installed into the MPFS**. (NOTE: MPFS will not support installation of 1 or 3 drives, you must install 2 or 4 drives)** These drives are set up with a JBOD configuration. JBOD is an acronym for "Just a Bunch of Drives". Hard drives in a JBOD configuration are seen by operating systems as a single disk. JBOD can be thought of as the opposite of partitioning. While partitioning sets up one single disk drive into smaller volumes, JBOD combines drives into larger logical volumes.

IMPORTANT!

JBOD Fault Tolerance
It is important to know that JBOD does not provide any fault tolerance. Data is written to any of the configured hard drives. If one hard drive fails, the data written to that drive is not written on any of the other drives in MPFS**. It is recommended you backup the data on the MPFS regularly**.

Drive Labeling
Logicube strongly recommends that you label each drive (your MPFS includes a blank set of drive labels and drives that are factory-installed are already labeled) to its corresponding position within MPFS (e.g. D1, D2, D3, D4) before installing the drives in MPFS**.**

IMPORTANT!
If drives that contain data are removed from MPFS and subsequently re-installed they must be installed in the exact same position prior to removal or data will be corrupted or lost.

The MPFS™ (Massive Portable Forensic Storage) solution is shipped with "0" hard disk drives or in various configurations with hard drives pre-installed at the factory. If you purchased your MPFS without hard disk drives factory-installed please read the following instructions carefully to properly install your own hard disk drives. Keep these instructions in a safe place for future reference.

Hard Disk Drive Specification

The MPFS supports a maximum of four 3.5" SATA hard disk drives (a maximum of 2 TB capacity each for a total maximum capacity of 8 TB). Do not attempt to install any other type of hard disk drive into the MPFS.

Important! The MPFS supports either a 2-drive or 4-drive configuration. MPFS does not support installation of only 1 drive or 3 drives. The drives do not need to be the same capacity, for example, you can install one 500GB drive and one 1 TB drive, or two 2 TB drives, or four 2 TB drives.

Please note that all drives installed in the MPFS must be set to 1.5 gigabits per second. Instructions on how to set hard disk drives to 1.5 Gb/s can be found on the label of the hard disk drive. If instructions are not found on the label, please check the hard disk drive manufacturer's website for more support.

The MPFS includes hardware to install a maximum of four hard drives. A description of what is included is listed below. If your MPFS did not include the following or if you are missing items, please contact Logicube Technical Support at 818-700-8488 x3 or support@logicube.com

List of Hardware

The following hardware is included with the MPFS™:

Name	Description	Quantity	Photo
HW1	Phillips 6-32 ¼" screw w/star washer	41	
HW2	Drive bracket	8	
HW3	Mounting bracket	3	
HW4	Magnetic screw driver	1	
HW5	Screws (Top Cover)	10	

Step-By-Step Installation

Step 1; Remove top cover plate from MPFS

Open top cover plate by removing the 10 screws as shown in figure 1. Verify hardware supplied with your MPFS as described above. If you are missing any hardware please contact Logicube Technical Support.

Figure 1

Step 2; Installing brackets on hard drives

You will need to install two drive brackets (HW2) on each drive installed in MPFS. Install a screw (HW1) and tighten in two places on each end of the drive bracket (HW4). Do the same for the other side of the same drives as illustrated in figure 2.

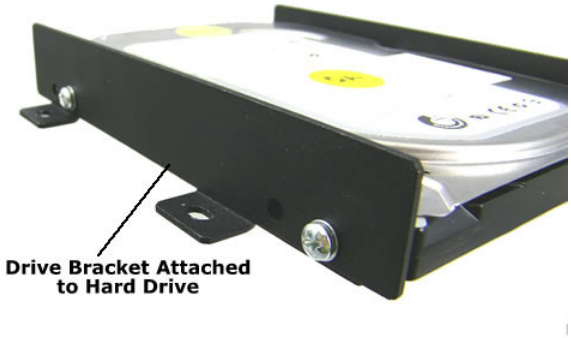


Figure 2

Step 3; Installing drives in MPFS

a) Gently insert the hard drive (with brackets installed) into the bottom of MPFS. SATA port on the drive should be facing the back wall of MPFS. Align the drive between the two guide pins on the back wall of MPFS.

b) Gently slide and push the drive forward firmly to engage the SATA connector.

c) Once the drive is engaged the mounting holes on the drive bracket and the bottom of the MPFS will align. Insert a screw (HW1) into each of the four mounting holes and tighten.

d) Repeat steps 1-3 for drive number two.

e) It is recommended that you test the MPFS at this point to ensure that the drives are properly engaged with the SATA connector. Attach the Forensic Dossier “head” and follow the instructions in section 4 of this manual and perform a “drive info” test by tapping the **“Drives”** icon from the main menu.

f) If you are only installing two drives in MPFS proceed to step 6.

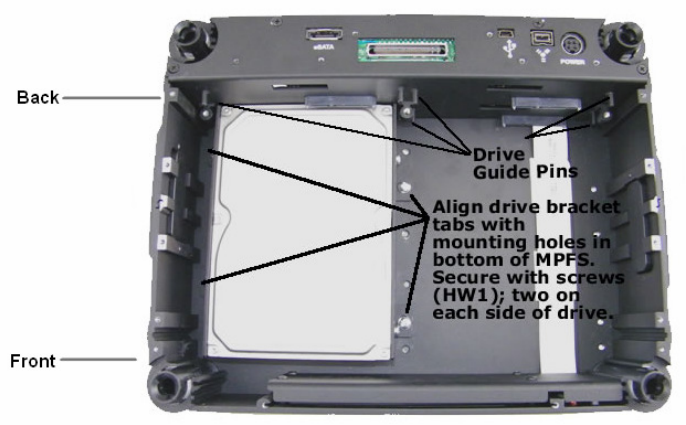


Figure 3

Step 4: Installing mounting brackets

a) You will insert three mounting brackets (HW3) in the bottom of MPFS; on the left side of drive #1, in between drive #1 and drive #2 and on the right side of drive #2. The mounting bracket should be aligned so that the longer notched end is against the back wall of MPFS.

b) Starting with the middle position in each bracket secure the mounting bracket secure the mounting bracket to the MPFS with a screw (HW1) in each of three mounting holes on the bracket as pictured in figure 4.

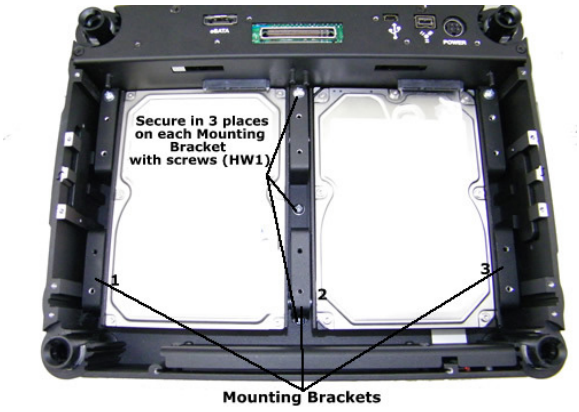


Figure 4

Step 5; Install 2nd layer of drives (drive 3 & 4)

a) Gently insert hard drive #3 into the left side of MPFS on top of mounting brackets (HW3). Align the drive between the two guide pins on the back wall of MPFS.

b) Gently and firmly push the drive forward to engage the drive with the SATA connector

c) Once the drive is securely engaged with the SATA connector the mounting holes on mounting bracket (HW3) will align with the drive bracket (HW2). Insert screws (HW1) into each of the four holes (two on each side of the drive) and tighten (see figures 5 and 6).

d) Repeat steps 1-3 for drive #4.

e) Prior to completing installation, it is recommended that you test the MPFS at this point to ensure that the drives are properly engaged with the SATA connector. Attach the Forensic Dossier "head" and follow the instructions in section 4 of this manual and perform a "drive info" test by tapping the **"Drives"** icon from the main menu.

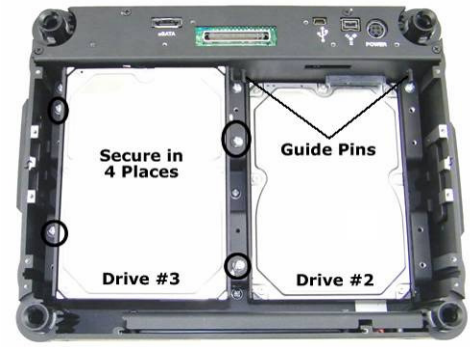


Figure 5

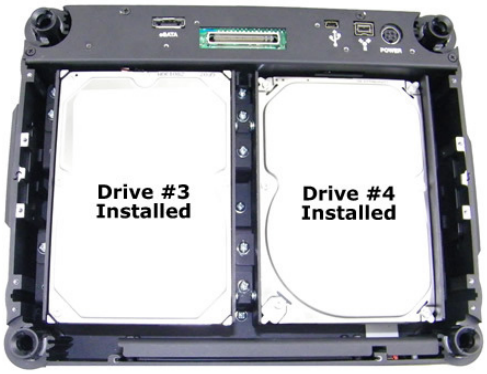


Figure 6

Step 6; Replace top cover

Complete the installation by placing the top cover plate on MPFS and securing in place with the 10 screws (HW5) removed at the beginning of the installation process.

CHOLESTERIC DISPLAY

The MPFS™ has an “always on” battery-powered cholesteric display with two buttons for scrolling up and down. The maximum number of files displayed on the cholesteric display is 21 files per page.

The cholesteric display can show the case/file names stored in the MPFS from previous extractions.

Figure 7, MPFS Display

Display Battery

The MPFS display uses a 9 volt lithium battery that can be replaced by the user.

Follow the instructions below to replace the battery:

1. Disconnect all cables from the MPFS™ (power, eSATA, USB, and FireWire).
2. Turn the MPFS™ upside down.
3. Locate the battery compartment on the bottom of the MPFS™.
4. Unscrew the two small screws to open the battery compartment cover.
5. Replace the battery.
6. Re-attach the battery compartment cover and secure the two screws tightly.

3. Using MPFS with the Forensic Dossier

Connecting the Forensic Dossier® to the MPFS™

The Dossier® head attaches to the MPFS™. Follow these steps to attach the two parts together:

WARNING: The Dossier® head is not hot swappable with the Dossier® tray and the MPFS™. Power must be unplugged from the Dossier® head before attaching it to the MPFS™ or the Dossier® tray.

1. If necessary, disconnect the Dossier® head from the Dossier® tray by turning the tabs on each corner of the unit as shown in Figure 8:

Figure 8, Opening corner latches.

2. Lift the top (or “head”) off the bottom of the unit as show in Fig. 9:

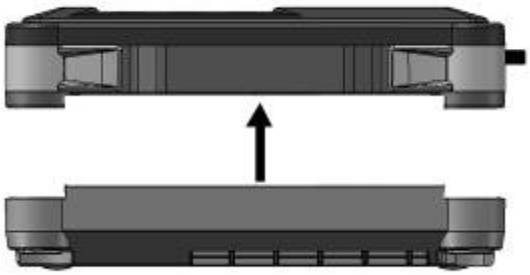


Figure 9, Lifting head off unit.

3. The bottom of the Dossier® head may have four foam pads. To connect the Dossier head to the MPFS these foam pads have to be removed.
4. Attach the Dossier® head to the top of the MPFS and turn the corner latches to lock the Dossier head in place.
5. Once the Dossier® head is attached to the MPFS, the power and connector ports on the MPFS™ are not accessible. Attach the power adapter to the Dossier® head to turn on the unit.

Connecting Suspect Drives to the Dossier

Connecting Source (or Suspect) drives

The Dossier® head has connections for up to two Source (or Suspect) drives labeled S1 (for Source 1) and S2 (for Source 2).

Connecting a Parallel ATA (IDE) Drive

To connect a Parallel ATA (IDE) drive, attach the drive to the Dossier® head using the UDMA cable (CBL-037B) and the power cable (CBL-002B).

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 10.

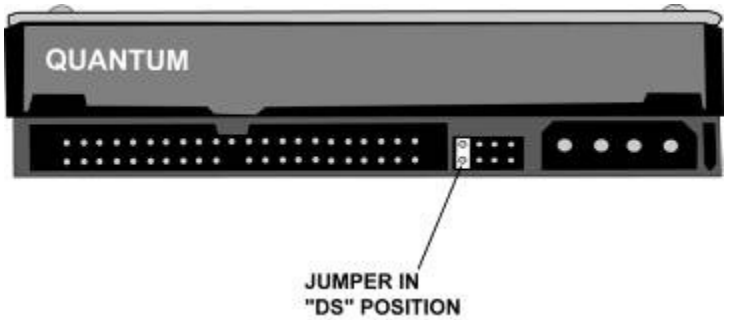


Figure 10, DS Position

Connecting a Serial ATA (SATA) Drive

To connect a Serial ATA (SATA) drive, attach the drive to the Dossier® head using the customized SATA cable (CBL-049A).

Connecting other types of drives

Logicube sells specialized adapters that allow other types of drives to be connected to the Logicube Dossier®. 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 Dossier® but can be connected via Logicube's optional SCSI and SAS adapters.

4. Drive Capture Modes and Settings

The main Dossier menu screen appears when the Logicube Dossier® head is attached to the MPFS™ and 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 button or tap the Back Icon at any time.

Drives

Tap the **"Drives"** icon to see drive information. Another screen will come up asking you to select S1, S2, Flash, or MPFS depending on what is connected to the unit. 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. If MPFS is chosen, it will display either two or four drives, depending on your configuration.

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

Settings

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:

- Backlight (on or off)

- Manage Settings
- Print Options
- Authenticate Trail
- Manage Destination
- Debug
- Beeper
- Install Options
- SCSI/SAS Adapter
- Audio Notice
- Upgrade MPFS FPGA
- Upgrade MPFS

These options are explained in more detail under **Chapter 5: Other Modes**.

Modes of Operation

The Logicube Dossier® with MPFS™ supports two different operations to clone data from a suspect drive. They are **DD Image Capture** and **E01 Image Capture**. These modes are found in the Settings Menu along with several other operations. The different modes of operation are briefly described below.

NOTE: Each time the Logicube Dossier® with MPFS™ is powered off, the cloning mode and preference settings are returned to their default settings. Certain settings can be set to default (Verify, Speed, etc.) For details on the **Save Settings** option, please see the **Misc Menu Settings** section in **Chapter 5. Other Modes**.

The following Modes of Operation are found in the Settings Menu:

- **DD Image** – This mode of Capturing creates a sub-directory per drive captured, with DD style files of size 650 MB, 2 GB or 4 GB each. These files are directly accessible by popular Forensic analysis software tools, such as, Encase, FTK, and iLook.

- **E01 Image** – The E01 option captures hard disk drives directly into the E01 file format. The evidence or destination drive can then be easily uploaded to the analysis software in a ready-to-analyze state. This eliminates the time-consuming conversion step that users typically must perform today.

- **Scan** – This operation performs a surface scan of the drive media using the drive controller to verify the media, and detect bad or "weak" sectors. This mode is described in **Chapter 5. Other Modes**.

- **Wipe** – This is used to erase all data on the MPFS™. This mode is described in **Chapter 5. Other Modes**.

- **HASH** – This is used to compute SHA-256 and MD5 values of the source, flash, or MPFS drives at extreme speeds, and is useful for an "after the fact" verification of a drive. This mode is described in **Chapter 5. Other Modes**.

- **USB** / **1394 –** This mode is used to connect the Dossier® attached to the MPFS™ to a PC through the USB or FireWire (1394) port. This mode also needs to be engaged when attempting a DD capture through the USB or FireWire port. For information on capturing via USB or FireWire (1394) please see **Chapter 6. USB and FireWire Ports** in the Forensic Dossier® User's Manual.

- **Search –** Used to perform a binary keyword search on a given drive. This mode is described in **Chapter 7. Keyword Search**.

Capturing a Drive

Connect the drives as previously described. Make sure the destination drives inside the MPFS™ are larger in total capacity than the suspect drive (source drive).

To Perform a DD Image Capture

1. Make sure that the Source drive is attached to the Dossier® head while it is attached to MPFS™ and power is applied to the Dossier® head.
2. From the Main Screen, tap the "**Settings**" Icon.
3. Tap the **"DD Image"** icon.
4. Tap the **"Mode"** icon and choose the configuration that is best suited for your capture session.
5. Scroll through the other optional preferences – **"Verify"**, **"File Size"**, **"On Error"**, **"Speed"**, **"Word List"**, **"Modify List"**, **and "GPS"**.

Modify them as needed by tapping the different settings for each.

> **NOTE**: See the **Special Settings for DD Capture Mode** section of this chapter for more information on these preference settings.

6. Press the **"START/STOP"** button twice.
7. The following message may appear: "MPFS appears to be corrupted! Would you like to reformat?" If this message appears, the hard drives inside the MPFS™ need to be formatted. To continue, tap the **"Yes"** icon. After a few moments, a confirmation screen will appear. Tap the **"Yes"** icon to continue. When the format is complete, a message will appear "MPFS format completed". Tap the **"OK"** icon.

NOTE: See **Chapter 4: Other Modes** for more information on managing the MPFS™.

8. The next screen prompts you to enter a Case file name using the keypad. Up to 8 characters are allowed following traditional DOS naming conventions.

   > **NOTE**: If a Case file already exists on the MPFS (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 of the MPFS™.
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 internal Flash memory. It includes (among other things), the SHA-256 and MD5 Hash values of all captured DD files or the entire Source Drive. Refer to the Special Settings for DD Capture Mode section below.
12. If Auto Print was set to "Yes" in the Misc. menu, you will be prompted to connect the printer and make sure that it is powered up and online. Press SET to print or BACK to skip printing.

    > **NOTE**: Please refer the section **"Printing a report"** in **Section 3. Drive Capture Modes and Settings** of the Forensic Dossier® User's Manual for more printing options.

13. The capture ends with a “DD Capture Successful” message.

Special Settings for DD Capture Mode

The settings below are unique to 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. The settings available are:

File - This is the default setting for verification and uses special hardware to compute SHA-256 and MD5 values for each individual DD Image file.

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

Disk - This setting uses special hardware to compute the SHA-256 and MD5 values for the entire Source drive.

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.

Speed

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

UDMA-6 - 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-6, all speed grades below will be tested (i.e. UDMA 0-6, PIO-AUTO PIO-PIO Medium and PIO-SLOW).

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 set to UDMA-5, all lower speed grades will be tested (i.e. UDMA 0-4, PIO-AUTO PIO-PIO Medium and PIO-SLOW)

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

NOTE: The unit will automatically choose this speed when capturing data from flash memory cards.

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 Dossier® to continue by stepping over the bad sector.

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

Retry - Retry will instruct the Dossier® to make several attempts to read data from the damaged area of the drive. The user can configure the number of retry attempts from 0 to 1,000 by tapping the Retries icon under Misc. to set the desired value.

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

NOTE: Data in any skipped sectors will NOT be copied to the MPFS™. The corresponding sector of the MPFS™ will instead be "padded" with zeroes. The padded sector will then be included in the final SHA-256 and 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/MD5 Hash value of each session could

differ. This is because some bad sectors will read intermittently.

Word List

The Word List Option is described in more detail in **Chapter 7: Keyword Searching of the Dossier Users Manual**.

Modify List

The Modify List Option is described in more detail in **Chapter 7: Keyword Searching in the Dossier Users Manual**.

GPS

The GPS setting can be turned on or off. Please refer to the Forensic Dossier® User's Manual, **Chapter 8: Peripherals** for more information on the GPStamp™.

E01 Image

The E01 option captures hard disk drives directly into the E01 format. The MPFS™ can then be easily uploaded to the analysis software in a ready-to-analyze state. This eliminates the time-consuming conversion step that users typically must perform.

NOTE: E01 is supported from SW release 1.17 and firmware release 8.15 forward. To use the Dossier® head with the MPFS™ you will need SW release 1.20 forward. If you need to update software and firmware to this revision in order to install the E01 option and your units S/N is below #77750 you must reset Dossier® to factory default settings by tapping Misc., Manage Settings and this icon.

NOTE: E01 does not currently support capture mode S1=>D1 & D2 or captures from RAID pairs.

NOTE: Currently E01 Flash media captures can only be performed with an external

flash media adapter used in conjunction with a USB enabled (Optional) SAS or SCSI adapter.

Procedure

1. Ensure the correct (UTC) offset value is entered into the Forensic Dossier® by tapping the E01 icon under settings followed by the More icon then the Time Zone icon.

2. Input a value (-12~12) with the keypad to set your time zone relative to (UTC) and press the SET button to enter the value. Example: The UTC for Los Angeles California is UTC-8.

   NOTE: To enter a negative (UTC) value press Shift '0' Shift and the number.

3. Tap the E01 icon under the Settings Menu and enter the desired E01 preference settings for Mode, Speed, Verify, On Error Retry and Setting. To enter any notes or to select the Info Show icon tap D1 or D2 respectively.

   The E01 selection choices for the settings Mode, Speed, Verify and On Error are explained below in the section *Optional Preference Settings.* The selection choices are as follows:

Mode 

S1=>MPFS
S1=>MPFS & S2=>MPFS

Speed 
Select UDMA-5 or UDMA-4

(Default is UDMA-5)

Verify 
Select DISK or DISK+V

On Error Retry 
Select Retry or Abort

The remaining icons are specific to E01 and are explained below.

Setting 

The Settings icon is used to add relevant case information using the keypad and must be entered for the capture to initiate:

Case Number

Examiner

Time information (yyyy/mm/dd hh:mm)

Notes

Tap the Notes icon to enter up to 64 characters of pertinent information using the keypad.

Press the <SET> button to save a note. Press the <BACK> button to leave the screen without saving a note.

Info Show

Tapping the Info Show icon will display the current case information that will be tied to the E01 capture report.

Sample E01 Info

Case No: GFK008

Examiner: R_SMITH

Notes: Any notes you wish to add.

Timestamp: 200910141439

TimeZone: UTC-8

Printing a report

Please refer to "*Printing a Report*" on page 33 of the Forensic Dossier® User's Manual for more printing options.

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 Dossier® is able to unlock and capture data from both HPA and DCO configurations. The Dossier® 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

HPA and DCO configurations can only be detected on the Source drive. They cannot be seen on the MPFS™. 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
- Calc. HASH
- Keyword Search

5. Other Modes

Introduction

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

NOTE: **Keyword Search** and related settings are discussed in **Chapter 7**, **USB/FireWire Mode** is discussed in **Chapter 6** and **GPS** is discussed in **Chapter 8** of the Forensic Dossier Users Manual.

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, S2, Flash, or MPFS.

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**/**STOP** button to start the scan.
6. The Dossier® with MPFS™ will access internal flash memory, then the following message will appear: "KEYPAD ENTRY: Enter Log file name. Press Set when done".
7. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Set button when finished.
8. When finished scanning, the Dossier® with MPFS™ 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.
9. If the Printer was set to "Auto Print", the user will be prompted to connect the printer and make sure that it is powered up and online. Choose YES to print or NO to skip printing.

   NOTE: Please refer to "*Printing a Report*" on page 33 of the Forensic Dossier® User's Manual for more printing options.

Wipe

This function is the process that erases or wipes all existing information from the surface of the MPFS™ drives. It ensures that no old data remains on the drive, to be later confused as evidence. Note; information regarding performing a wipe to DoD specifications can be found in the Other Settings section under Manage Destination.

Procedure

1. From the Main Screen, tap the Settings Icon to enter the Settings menu.

2. Tap the Wipe icon.
3. Tap the "MPFS" icon.

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** (Default): Writes a small signature to the drive every 16,065 sectors (or every logical cylinder). During a later capture session, this signature tells the Dossier® with MPFS™ that the drive(s) have been correctly erased.

- **NO**: Leaves the signature off the drive. The Dossier® will not detect that the drive has been erased.

1. Press the <Start/Stop> button to begin wiping.
2. The Dossier® will access internal flash memory, then the following message will appear: "KEYPAD ENTRY: Enter Log file name. Press Set when done".
3. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Set button when finished.
4. The Dossier® with MPFS™ will perform an Wipeclean™ operation based on the settings chosen by the user.

   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.
5. When finished, the Dossier® with MPFS™ will display the following message "drive successfully erased". A copy of the session report will also be copied to the internal flash memory as <Log file name>.LOG.

   NOTE: The operation will abort with an error message if bad sectors are encountered on the MPFS™.
6. If the Printer was set to "Auto Print", the user will be prompted to connect the printer and make sure that it is powered up and online. Choose YES to print or NO to skip printing.

   NOTE: Please refer to "*Printing a Report*" on page 33 of the Forensic Dossier® User's Manual for more printing options.

HASH Scan

This mode computes the SHA-256 and MD5 Hash values for a given drive (S1, S2, Flash, or File on MPFS™).

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, S2, Flash, or File on MPFS™.
4. Tap the “Speed” Icon to set the desired UDMA or PIO speed.
5. If a certain number of sectors need to be scanned, go to the “Size” setting. Use the keypad to enter a size in number of sectors. Press the Set button to confirm.
6. Press the <START/STOP> button to begin the scan.
7. The Dossier® with MPFS™ will access the CF Drive, then the following message will appear: “KEYPAD ENTRY: Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.

   NOTE: The operation will abort with an error if bad sectors are found on the drive.
8. When finished, the Dossier® with MPFS™ will display the SHA-256 and MD5 Hash values. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.
9. If the Printer was set to “Yes”, the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

   NOTE: Please refer to “*Printing a Report*” on page 33 of the Forensic Dossier® User’s Manual for more printing options.

Misc Menu Settings

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

Backlight

Use this setting to turn the Touch Screen's backlight on and off. This setting is useful for seeing the Touch Screen in low light conditions. The default setting is OFF.

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 icons to increase or decrease the Touch Screen's Contrast setting to your desired preference. The contrast setting will be retained in memory by tapping 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 and Defect Scan Speed Fast or Slow.

Factory Settings

Reverts all adjustable settings to the default factory settings.

Print Options

This mode is used to print reports directly from the Dossier® through the serial port. The settings available are:

Eject Page

This function sends a form feed signal to the printer. This function may be required to load paper in some printers.

Print Report

This function is used to manually print a report after a capture session. It also prints different reports associated with Keyword Search.

Print Last Session – This function prints the report from the last performed session (drive capture, defect scan, wipe, etc.). It is not able to print reports prior to the last session.

Print Search Detail – This function prints all of the found keywords from the last keyword search as well as their absolute locations on the Source drive.

NOTE: For more information, please refer to **Chapter 7: Keyword Searching**.

Print Search Text – This function prints a fragment of text before and after each found keyword. This allows each keyword to be viewed in context.

NOTE: For more information, please refer to **Chapter 7: Keyword Searching**.

Auto Print (After Capture)

This function tells the Dossier® with MPFS™ to print a report after the next capture session. It can be set to YES or NO (default).

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 Dossier® will display a list of the Log files that are on the internal flash memory.
4. Tap the desired Log file and tap OK.
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. Tap the Back Icon to return to the Main Screen.

Manage Destination

This menu is used to prep the MPFS™ drives prior to running a DD Image capture. The settings available are:

Format Dest. – This function formats the MPFS™ with a single FAT32 partition extremely quickly with the latest firmware release. This is necessary before DD Image or E01 Image files can be copied to the drive. When Format Dest. 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 30 – 60 seconds the drive(s) will be formatted, (the time varies by drive size).

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

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

Choose <Yes> to run Scandisk. After 30 seconds, it will display a list of errors, if any.

Debug

Use this setting to turn the Debug reporting tool on and off. This setting is used in conjunction with Serial Port 2 and a terminal link program. The default setting is OFF. Debug should only be turned on when the user is directed to do so by Logicube Technical Support.

Beeper

Use this setting to turn the beeper on and off. This setting is useful when in “stealth” mode or in an environment that requires no noise. The default setting is OFF. Any change to the setting is preserved after power off.

Install Options

As optional features become available, use the install options Icon to activate purchased options by tapping Misc. and the Install Options Icons on the Dossier®.

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 Dossier® 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 Dossier® head. These optional adapters can be purchased from Logicube. Contact the Logicube Sales Department for more information.

Functionally each adapter acts like a pass through device and allows for external connection and capture of SCSI and or SAS source drives through the IDE port of Dossier® head.

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 Dossier® head.

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.

Performing SAS and SCSI Adapter Updates

It's good practice to occasionally verify that your Adapter is running the current BIOS, Kernel, Firmware and Software Application. This is not something that will need to be updated frequently. Please refer to the SAS or SCSI Adapter Users Guides or the Forensic Dossier Users Guide for detailed instructions on how to update firmware and software.

Audio Notice for Error

Use this setting to provide an audible beep if the data capture has been completed successfully. A different audible beep will occur to alert the user that the capture has encountered an error. This beep will sound with a 50% duty cycle for approximately 2 minutes or until the user acknowledges the error via the user interface. The default setting for Audio Notice is OFF. Once enabled the Dossier® with MPFS™ will retain the setting last used prior to power recycle.

Upgrade MPS FPGA

This application setting is used to upgrade the MPFS™ firmware. Note: You must perform restart MPFS in for the firmware update to take effect.

Upgrade MPS

This application setting is used to upgrade the MPFS™ software.

NOTE: After performing a software upgrade to the MPFS™, the reset button must be pressed for proper operation. For more information, see **Chapter 9. Software and Firmware Loading Instructions**.

6. eSATA, USB and FireWire Ports

Introduction

The integral USB, FireWire (1394), and eSATA ports on your Logicube MPFS™ provide connectivity of the unit and its drives to any PC with an active USB, FireWire, or eSATA port.

When attaching the MPFS™ to a PC, one partition per hard disk drive will be seen. For example, if there are two hard disk drives inside the MPFS™, two partitions will be seen. If four hard disk drives are inside the MPFS™, four partitions will be seen.

Note regarding 2 TB limitation:

- The MPFS allows direct connection to a PC via FireWire 400, USB 2.0 or eSATA. Write-protected ports allow you to preview or transfer data from the MPFS to a PC. (***Note: When using the FireWire and USB ports for data transfer to a PC, MPFS will support a maximum capacity of 2TB. eSATA port must be used for capacities greater than 2TB. A 64-bit Operating System must be used for capacities greater than 2TB)***

Minimum requirements

- A Logicube MPFS™ unit with integral USB / FireWire / eSATA ports.
- A 586 or better PC compatible computer with CD-ROM drive.
- An active USB port and/or an active FireWire (1394) port and/or an active eSATA port.

- Microsoft Windows XP/Vista/7 operating system (for drive access under Windows).

eSATA Connection to Windows (for Drive Management)

1. Make sure your PC is running Windows XP/Vista/7
2. With power applied to the MPFS™ connect an eSATA cable to an eSATA port on a PC on one end and to the MPFS™ on the other end.
3. Windows will recognize the drives (this may take a few minutes).

USB Connection to Windows (for Drive Management)

1. Make sure your PC is running Windows XP/Vista/7.
2. With power applied to the MPFS™ connect a mini USB cable (provided with your Dossier®) to a PC USB slot on one end and the mini USB connector to the MPFS™.
3. Windows will recognize the drives (this may take a few minutes).

FireWire Connection to Windows (for Drive Management)

4. Make sure your PC is running Windows XP/vista/7.
5. With power applied to the MPFS™ connect a FireWire cable to a PC FireWire (IEEE1394) port on one end and the FireWire connector to the MPFS™.
6. Windows will recognize the drives (this may take a few minutes).

Removing USB devices

Before physically disconnecting the USB cable and/or shutting down power to the Dossier®, 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).

7. Keyword Searching

Introduction

The Dossier® head with MPFS™ can search for multiple keywords while capturing a suspect drive. This is a useful feature to provide early screening of a drive. For example, you could search for the names of all common drugs or the names of known offenders on a given drive. Presence of these keywords might indicate a connection between the suspect and the keywords.

In general, you select a pre-defined list of words which is loaded into the hardware based search engine. These words are automatically searched for during the next Capture session. At the end of the session, you can print one of several reports that indicate the number of occurrences, and absolute location on the drive of all matches found.

Searching During Capture

1. From the Main Screen of the Dossier® with MPFS™, tap the Settings Icon.
2. Choose DD Image Capture mode. (Keyword searching during capture is not currently available for E01 Capture mode. This feature will be available in a future software update)
3. Set all of the optional cloning settings as desired (verify, speed, etc.)

4. Tap the 'Word List' Icon.
5. The unit will read the list of available keyword lists from the Compact Flash, and display it on the screen.
6. Choose the desired list, and tap the OK icon.

NOTE: As of this writing, matches during capture are automatically logged in the capture

report. Other settings will be accessible in later versions of the software under the **On Match** Icon. Please contact Logicube for availability.

7. Form now on, the words in this list will be searched for as a by-product of any of the Capture modes.
8. At the end of a session, the Final Capture report will also list any keywords found. You can then print one or both Keyword Search reports:

- **Print Search Detail**: This report lists every keyword found and the sector where it resides.

- **Print Search Text**: This report lists every keyword and the surrounding line of text.

NOTE: The DD Image Capture Report or E01 Image Capture Report will not automatically list keywords. We suggest running the Search Detail report after the Capture Session to list any keywords found.

NOTE: Please refer to "*Printing a Report*" on page 33 for more printing options.

Keyword Lists

All keyword lists are stored on the Compact Flash in a file called keyword1.lst. The file is a simple text file which can be edited by any plain text editor, such as Notepad.

A sample file might look like this:

```
[Terrorism]
ABU NIDAL=case:yes,unicode:no,signature:no
ABU SAYYAF=case:yes,unicode:no,signature:no
AL-QAIDA=case:yes,unicode:no,signature:no
BLACK SEPTEMBER=case:yes,unicode:no,signature:no
DEMORALIZE=case:yes,unicode:no,signature:no
HAMAS=case:yes,unicode:no,signature:no
HIZBALLAH=case:yes,unicode:no,signature:no


[Computer crimes]
2600 =case:yes,unicode:no,signature:no
BACK ORIFICE=case:yes,unicode:no,signature:no
CRACK=case:yes,unicode:no,signature:no
```

DEFCON=case:yes,unicode:no,signature:no
ENCRYPTION=case:yes,unicode:no,signature:no
FLAME=case:yes,unicode:no,signature:no
HACK =case:yes,unicode:no,signature:no
IP SPOOFING=case:yes,unicode:no,signature:no

In the above example, two lists ([Terrorism] and [computer Crimes]), are listed. You can select only one for each search session. Many more lists with many more words can be defined.

Three options are available for each word:

1. **Case**: - yes/no. If Yes, the word is searched exactly as typed. No will search for all lower-case, all upper case, and First letter upper-case.
2. **Unicode**: yes/no. If No, the plain ASCII of the word will be searched for. Yes, the Unicode encoding of word is searched for.

   NOTE: The Unicode search utilizes the "little endian" code that is utilized by Microsoft operating systems. Other systems, like Linux, UNIX, Mac, etc. utilize the "big endian" code. A future version of the Dossier® software will also support big endian Unicode.
3. **Signature**: the word is only searched at the beginning of sector. This is useful to find all files of a certain type, e.g. all graphic files.

The unit allows some editing of the keyword lists. Please refer to the **Modify Lists** section below for more details.

NOTE: As of this writing, only the English alphabet is supported. Future software updates will include support for different languages. Please contact Logicube for further details.

Modify List Settings

Keyword Lists can also be created, modified and deleted from the Dossier® head with MPFS™ itself. The following settings are accessed from the Optional Preference Settings under Keyword Search or by using the More button to access the Optional Preferences under DD Capture and E01 Image Capture.

Modify Lists

Follow this procedure to directly access the Modify Lists menu:

9. From the Main Screen, tap the Settings Icon.
10. Tap the Search Icon.
11. Tap the Modify List Icon.
12. Three sub-menu functions appear:

- **Add New List**: This setting allows you to add a new Keyword Search List to the Compact Flash Card. When selected, you will see the words Enter new list name at the top of the screen. Enter the new list name and press Set and a screen will prompt you to add a Keyword to the list you just created. At this point you have an opportunity to assign whether or not Case Sensitivity, Unicode and Signature are to be factored into the search criteria. Enter YES or No for each of these setting and press the Set Icon when finished. You can continue to add more keywords to the list at this time by tapping the Add Icon. Once all of the Keywords have been added you must tap the Save Icon to add the new list.

  Tapping Abort at any time will take you back to the Modify List Menu

- **Edit List**: This setting allows Keywords in existing lists to be modified or removed. It also allows new Keywords to be added. When selected, the Dossier will ask which list needs to be modified. Use the arrow Icons on the screen to scroll through the list of file names. Once the list you wish to edit is located tap the OK Icon. The contents of the list and several selectable Icons will display along the bottom of the screen. The Icon choices within Edit List are:

  1. Add which allows you to add a new Keyword to the List.
  2. Edit which allows you to modify the Keywords Name, Case Sensitivity, Unicode and Signature search criteria.
  3. Delete which removes the Keyword from the list.
  4. Save which is a necessary step for the changes to be written to the CF

5. Abort which will take you back to the Modify List Menu

– **Remove List**: This setting removes a chosen list from the Compact Flash Card. When selected, the tool asks which list needs to be removed. Use the arrow Icons on the screen to scroll through the list of file names. Once the Search List is located tap the OK Icon.

WARNING: There is no “are you sure” screen either when a list is chosen or before hitting OK for removal.

Tapping Abort at any time will take you back to the Modify List Menu

Tap the Back Icon in the Modify List Menu will take you back to the Main Screen.

8. NETConnect™

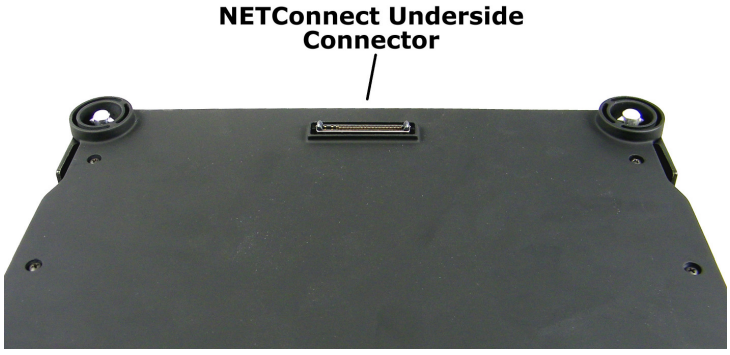
Using MPFS to NETConnect™

The MPFS works seamlessly with the optional NETConnect™ networking module. Please refer to the NETConnect Users Guide that was included with your NETConnect for complete information on all of NETConnect's features and how to use it with MPFS.

Connecting MPFS to NETConnect™

To connect the NETConnect to the MPFS™, follow the instructions below:

1. Ensure that power and all cables attached to the MPFS® have been disconnected.
2. Set the NETConnect on top of the MPFS™ and make sure the NetConnect underside connector aligns with the connector on top of the MPFS™.



3. Close the corner latches to lock the NetConnect in place.

NETConnect™

NETConnect Attached to MPFS

9. Software and Firmware Loading Instructions

Introduction

New and improved software and firmware 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.

The Dossier® head must be connected to the MPFS™ in order to update the software or firmware on the MPFS™.

Loading New Software

The new software (a single file always called mps.bin) has to be placed on the root directory of the internal flash memory (System CF) of the Dossier® head with MPFS™.

1. Connect the Dossier® head with MPFS™ to a PC via USB or FireWire connection:
    a. Attach a USB or FireWire cable to a PC. Do not attach the cable to the Dossier® with MPFS™ yet.
    b. With the Dossier® head with MPFS™ powered on, tap the **Settings** icon from the main menu.
    c. Tap the **USB** / **1394** icon.
    d. Select either **USB** or **IEEE1394** depending on the type of connection you will be using.
    e. On the USB or FireWire Mode menu, tap the **Drive** icon to change the drive. Select **System CF.**
    f. Press the **Start** button twice.
    g. Connect the USB or FireWire cable to the Dossier® with MPFS™. The System CF will appear on the PC as a removable disk and will be accessible via Windows Explorer or My Computer.

2. Once the System CF is accessible, overwrite the existing **mps.bin** file with a new version.
3. Disconnect the Dossier® head with MPFS™ from the PC as described in the Dossier® manual.
4. From the main menu of the Dossier® head with MPFS™, tap the **Misc** icon.
5. In the Preferences screen, tap the **More** icon to go to the second page of preferences.
6. Tap **Upgrade MPS**. A screen will appear stating:

   "This upgrade will take around 1 minute. Do you want to continue?"

7. Tap **Yes** to proceed with the upgrade.
8. After about 1 minute the screen should display the main screen.

Loading New Firmware

The new firmware (a single file called mpsfpga.rpd) also has to be placed on the root directory of the internal flash memory (System CF).

1. Connect the Dossier® to a PC via USB or FireWire connection as described in the Dossier® manual.
   a. Attach a USB or FireWire cable to a PC. Do not attach the cable to the Dossier® with MPFS™ yet.
   b. With the Dossier® head with MPFS™ powered on, tap the **Settings** icon from the main menu.
   c. Tap the **USB** / **1394** icon.
   d. Select either **USB** or **IEEE1394** depending on the type of connection you will be using.
   e. On the USB or FireWire Mode menu, tap the **Drive** icon to change the drive. Select **System CF.**
   f. Press the **Start** button twice.
   g. Connect the USB or FireWire cable to the Dossier® with MPFS™. The System CF will appear on the PC as a removable disk and will be accessible via Windows Explorer or My Computer.
2. Once the System CF is accessible, overwrite the existing **mps.bin** file with a new version.
3. Disconnect the Dossier® head with MPFS™ from the PC as described in the Dossier® manual.
4. From the main menu of the Dossier® head with MPFS™, tap the **Misc** icon.

5. In the Preferences screen, tap the **More** icon to go to the second page of preferences.
6. Tap **Upgrade MPS FPGA**. A screen will appear stating:

   "This upgrade will take around 20 minutes. Do you want to continue?"

7. Tap **Yes** to proceed with the upgrade.
8. After about 20 minutes the screen should display the main screen.
9. You must power off the MPFS and re-start the MPFS for the firmware upgrade to take effect.

10. Reference

Further Notes on Modes Available for the Dossier®

DD image

This process captures all data from the source drive to the MPFS™. 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, S2, D1, D2 or Flash

Speed – The choices are, Fast or Slow

Wipe

The Wipe function is the process that erases or wipes all existing information from the surface of the MPFS™.

Options

These are the user configurable options for the Dossier® erase process.

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

The choices are UDMA-6 to UDMA-0, PIO-AUTO, PIO-MED and PIO-SLOW.

Erase process

The software will do a CPU-erase. This is a process where the Dossier'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 and MD5 Hash values at an extremely fast and accurate rate.

NOTE: If the MPFS™ has bad or weak sectors, this mode may not guarantee the accuracy of the Hash values. If the health of the drives inside the MPFS™ are unknown, use the "+V" setting.

HASH + V

This mode uses special hardware to compute SHA-256 and 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 MPFS™. All prior and subsequent sectors are copied while only the unreadable sector is skipped. This Sector is filled with zeros on the MPFS™.

RETRY - The Retry option attempts to reread an offending sector. The user can set the number of retry attempts from zero to 1,000 attempts. The default setting is 50. The Dossier 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 MPFS™.

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:

4. Reinitialize the source drive.
5. Dump the drive's cache buffer.
6. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.
7. 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.

8. 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 MPFS™ and the copying process continues with the following sectors.

Printer

The printer option contains a submenu with various functions controlling the generation of hardcopy printouts of Capture, DD Imaging, Scan or Wipe Sessions.

AUTO PRINT - The print report option controls whether or not a hardcopy printout is automatically generated immediately following a Capture, Scan, or Wipe session. The choices are YES, or NO.

PRINT LAST SESSION - The Print Last Session option enables the user to get a hardcopy printout of the previous Capture, Scan or Wipe session even if the Print Report option above was not enabled. As long as power remains applied to the unit, the previous session's results are available.

PRINT SEARCH DETAIL – Prints a detailed report of all words matched during the last session, and their absolute location

PRINT SEARCH TEXT – Prints a snippet of text before and after the matched word, for every word matched during the last session

EJECT PAGE - The Eject Page option is a utility function that will send a page eject or form feed command to the printer. This may be necessary when using certain kinds of laser printers.

Anatomy of a Drive Capture

The drive capture process implemented in the Dossier® 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 MPFS™ 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 MPFS™ 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 MPFS™ capacity is equal to or greater than the source drive. If the MPFS™ 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. If you are capturing from two source drives to the MPFS™ the unit will ask for two separate case names. Case name(s) must be 8 characters or less and use DOS naming conventions. The Log file name is used for the report that is created at the end of the capturing session and written to the System CF Drive (if you are capturing from two source drives to the MPFS™ two reports will be generated). The report can be opened and printed from any text editor in Windows (like Notepad).

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 MPFS™.
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 identified. 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.

NOTE: This step does not apply to Flash Media Cards, even though they run at PIO-AUTO speeds.

2. A chunk of the source drive is then copied to the MPFS™ at the speed previously set in the calibration procedure.
3. Every byte of every sector copied is then compared on the source and MPFS™.
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.

Wipe

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

Erase Process

The software will write zero-filled sectors directly to the entire MPFS™ drives using programmed I/O.

Capture Source Drive Data To the MPFS™

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

Print Final Capture Report

If the Auto Print setting was set to YES prior to Capture, then the unit will prompt the user with a message: “Make sure that the printer is connected, powered up and online. Tap <OK> to print”. Press the Select button to initiate printing. A Final Capture Report will then be printed.

If the Printer setting was set to NO prior to capture, then a report can still be printed as long as the unit hasn’t been powered down, rebooted or used to clone more drives. Just go to the Misc Menu, tap the Print Options Icon, tap the “Additional Reports” Icon, find “Print Last Session”, tap it and press the Set button.

A copy of the report is also written to the CF drive. It is named <Log file name>.LOG.

Final Capture Report (Hardcopy Printout)

The hardcopy printout available on the Dossier® 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 Dossier® 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. When a DD capture is performed with Verify the Destination Hash

Value is reported in the verify section of the audit trail report.

- 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!"

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 and 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.

MPFS Drives Information - This section of the printout contains information specific to the MPFS™ drives. It contains the following.

- Drive Identification. These lines print the model and serial number as reported by the MPFS™ drives.
- 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 and MD5 value for the MPFS™ drives. 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 and 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 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.

Keyword List – If a keyword search was performed during the capture, a list of the found keywords will appear at the very end of the Final Capture report.

Example of Hardcopy Printout

```
** Forensic Dossier   --  Serial No.:77835 --  Software:V1.21RC11
*                                                                 *
* Acquired by_____________________ Location _____________________ *
*                                                                 *
* Acquired on_____________________________ AT_____________________ *
********************** SESSION SETTINGS ************************
* Operating Mode: 2GB DD:S1=>MPFS          Address Mode: LBA     *
* Verify        : Hash-Dsk+V               Speed    :    UDMA-6 *
* Connection    : Direct                                          *
*     AN EXACT DD IMAGE FILE COPY OF S1 HAS BEEN ACHIEVED.        *
*                                                                 *
******* SOURCE DRIVE(S) ************ DESTINATION DRIVE(S) ******
*            S1                    |            MPFS              *
* Model : Maxtor 2F040L0           | Model : WDC WD20EADS-00S2B0   *
* Serial: F1KJ78ZE                 | Serial: WD-WCAVY0640793       *
*                                  | Model : WDC WD20EADS-00S2B0   *
* C: 79656   H:  16    S: 63       | Serial: WD-WCAVY0673413       *
* Total Sectors   Drive Size       | Model : ST32000641AS          *
*    80293248      38.3 GB         | Serial: 9WM095KC              *
*                                  | Model : ST32000641AS          *
*                                  | Serial: 9WM094QC              *
*                                  |                               *
*                                  | Total Sectors   Drive Size    *
*                                  |    15628116672   7452.68GB    *
*                                  |                               *
*****************************************************************
*** S1 From: 0, To: 80293246, Size: 2218368
* SHA-256:
* ...63C5D6F3 32FF5B45 A2528A3C A522300A...
* ...F2DE20FB A7F6DCAE 99D13B98 5CA4C3BD...
* MD5:
* ...7D68B0C5 017CE939 400F8015 0CF19E50...
*****************************************************************
*                                                               *
*        Skipped Sectors[1]: 0  Recovered Sectors[1]: 0         *
*                                                               *
*---------------------------------------------------------------*
*        Skipped Sectors[2]: 0  Recovered Sectors[2]: 0         *
*                                                               *
*****************************************************************
Audit Trail Checksum: AA1F2F71 BEB32A59 5DC52AB7 7E89143F
```

11. Frequently Asked MPFS™ & Dossier Q & A

Q. How many drives can I install in MPFS?

A. MPFS will support installation of either 2 drives (minimum installation) or 4 drives. MPFS will not operate with only 1 drive installed, nor will it operate with only 3 drives installed. The maximum capacity of each drive installed in MPFS is 2TB for a total maximum capacity of 8TB.

Q. Why does the Cholesteric display show "Battery Mode" even after I plugged in the AC adapter?

A. This is typically seen when the AC adapter is disconnected then quickly reconnected to the Dossier(r) head. The cholesteric display needs to refresh completely, switching from "Power Mode" to "Battery Mode". After disconnecting the AC adapter, wait for the Cholesteric display to refresh completely before reconnecting the AC adapter.

Q. By comparison my Dossier® 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. I'm trying to update my Dossier® with the latest software but I cannot get my PC to communicate with the unit.

A. Make sure that the PC is either connected through the USB or FireWire port.

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 Dossier®:

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 Dossier® 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 Dossier indicating that an error has occurred. A Log file is not generated when a mismatch occurs.

Q. When two drives are created from one source drive as a DD image with Disk + Verification turned ON how do I know both copies have been verified by Dossier® to be exactly the same as the source?

A. If at any time during the capture either of the two copies encounters a hash mismatch as part of the verification process, Dossier® will terminate the capture before the log file can be created. If the capture completes successfully the SHA- 256 and MD5 digests for S1 will be displayed on Dossier® and in the log file along with the message AN EXACT DD IMAGE FILE COPY OF S1 HAS BEEN ACHIEVED.

12. Index

For further assistance please contact Logicube's tech support at: 818 700 8488 ext. 3, or by email to techsupport@logicube.com. Logicube tech support is available 7am –5pm PST, Monday through Friday, excluding U.S. legal holidays.

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