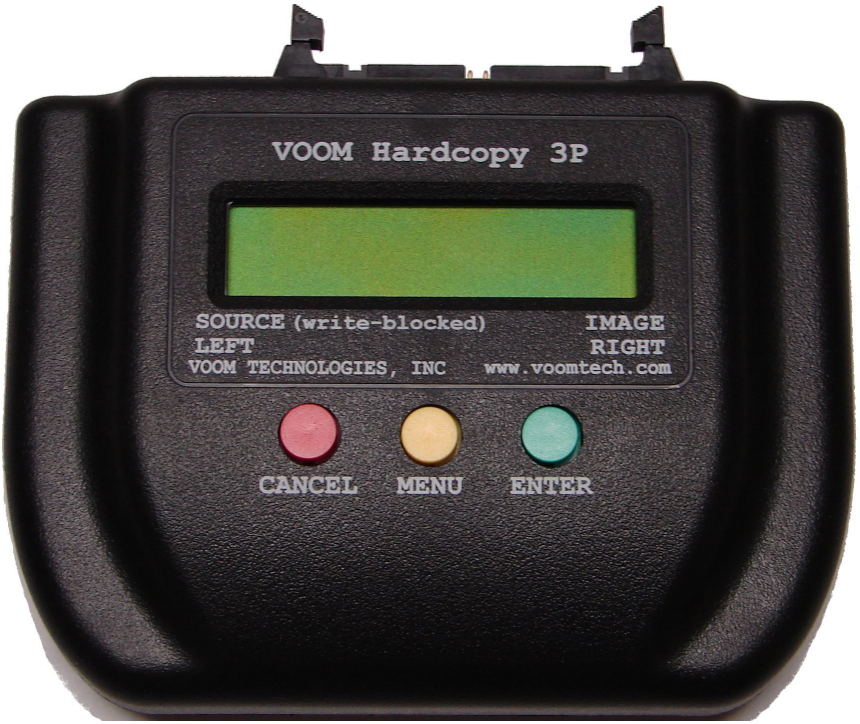
VOOM Technologies, Inc.

VOOM HardCopy 3P™ User Guide



HardCopy 3P

HardCopy 3P™ User Guide

Sixth Edition

22 January 2014

(Based on the HardCopy 3P v3-01 release)

HardCopy 3P is designed, developed, and manufactured in the USA.

VOOM Technologies, Inc.
110 St. Croix Trail South
Lakeland, Minnesota 55043
Telephone 651-998-1618
Fax 651-436-4030

Table of Contents

1 Information

1.1 Technical Documentation

Specifications and information contained in this manual are furnished by Voom Technologies, Inc. for informational use only and are subject to change at any time without notice and should not be construed as a commitment by Voom Technologies, Inc. Voom Technologies, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual; including the products, firmware and included accessories.

1.2 Data Protection Information

The user must be aware that an improper system configuration can lead to data corruption. Please read the System Configuration chapter of this manual carefully before attempting to capture any data. Voom Technologies, Inc. is not responsible for any loss of data resulting from the use, disuse or misuse of this product.

2 Technical Support

2.1 Support by Telephone

Technical support is available to registered owners of Voom Technologies, Inc. products by telephone Monday through Friday 8:00am to 4:00pm, Central Standard Time Zone at 651-998-1618.

2.2 Support by E-Mail

Voom Technologies, Inc. technical support is available by e-mail at support@voomtech.com.

2.3 Technical Support Tips

Call from a telephone where you have access to your HardCopy 3P. Please be prepared to provide the following information:

- Name, telephone number, e-mail address
- Model number and version of the product
- Make and model of your hard drives
- Symptoms of the problem

3 Preface

3.1 Product Contents

HardCopy 3P HardCopy 3P
0.5m SATA cables (three shipped)
18” PATA ribbon cable
Standard serial communication cable
AC adapter with power cord
Source DC power cord
Destination DC power cord with Y-adapter for dual destination
User Guide

3.2 Requirements

The HardCopy 3P supports PATA and SATA hard drives. The HardCopy 3P is capable of switching between the SHA-256 and MD5 hash calculators. This User Guide will use the term `hash` for either SHA-256 or MD5 depending on which hash calculator is in use.

3.3 Introduction

The HardCopy 3P is primarily designed to copy information from a Source Drive to one or two Destination Drives. It provides three distinct ATA buses, one for the Source Drive and one for each Destination Drive. This triple bus architecture allows the hardware to transfer data directly from the Source Drive to the Destination Drive(s), without the need for any type of software buffering. The PATA Source shares a bus with the SATA Source. HardCopy 3P always places all drives in “standby” mode after each operation has completed.
In addition, the source bus is write blocked.

HardCopy 3P currently supports the following operations:

- Perform a functional test of the current system configuration.
- Calculate a `hash` checksum and a 32-bit CRC (every 2GB) on the contents of the Source or Destination Drive.
- Perform a sector-by-sector copy of the Source Drive to the Destination Drive.
- Image the contents of the Source Drive to a file on the Destination Drive.
- Split the image into 2.3GB per file on a FAT32 formatted drive.
- Display the list of files (NTFS) or directories (FAT32) currently stored on the Destination Drive.

- Format the file system on the Destination Drive (NTFS or FAT32).
- Wipe all information from the Destination Drive.
- Initiate an ATA Security Erase Unit command.
- Unlocking of HPAs and DCOs.
- Show the last operation performed and report the `hash` checksum if one was generated.
- Set the time and date.
- Switch between SHA-256 and MD5.
- Update the firmware.

HardCopy 3P supports reading/writing drives greater than 2TB for Clone operations. Filesystem support is limited to 2TB for drives greater than 2TB. When formatting a destination drive larger than 2TB the filesystem written will use 2TB of the drive's available capacity.

The active hash calculator is displayed in the lower right of the LCD at the `Ready` prompt. Refer to the Switch to SHA/MD5 section for the procedure to activate the other hash calculator.

HardCopy 3P also supports error recovery for drives that operate intermittently. If the unit is unable to copy a sector from the Source Drive to the Destination Drive after 6 consecutive attempts it will fill the corresponding sector on the Destination Drive with an all zeros (0x00) data pattern, increment the appropriate drive access error counter, and continue with the capture operation. The total number of drive access errors (read or write), along with a list of the Logical Block Addresses associated with each of the errors (maximum of 16 for each access type), will be displayed to the user when the operation completes.

Note: When performing an ATA Security Erase Unit command, the hard drive is running stand alone and does not communicate with the HardCopy 3P unit until it has completed the erase. Any error recovery is up to the drive manufacturer.

The user interface for the HardCopy 3P supports a LCD (2 line x 16 character) managed through a button control panel. and a serial port that can be connected to any standard terminal. The user can execute commands by entering them from the button control panel or an attached terminal. The status information is always displayed to both the LCD and the attached terminal.

The HardCopy 3P also supports copying Source Drives that are configured with a Host Protected Area (HPA) and/or a Device Configuration Overlay (DCO). HPAs and DCOs are typically reserved areas for data storage outside the normal operating file system. This area is hidden from the operating system and the file system, and is typically used by specialized applications.

3.4 Definitions

This section describes much of the technical verbiage used throughout this document.

HardCopy: This term implies that the hardware is capable of copying large chunks of data from the Source Drive to the Destination Drive without software intervention, resulting in the fastest cloning possible.
Source Drive: The hard drive from which the data is read from during a cloning operation.
Destination Drive: The hard drive that the data is written to during a cloning operation.
Checksum: The process of calculating a `hash` checksum for every sector on the Source Drive.
Clone: The process of performing a sector-by-sector copy operation from the Source Drive to the Destination Drive. The number of sectors copied is determined by the size of the Source Drive.
Image: The process of performing a sector-by-sector copy operation from the Source Drive to a file on the Destination Drive. The size of the data file is determined by the size of the Source Drive.
Wipe: The process of writing zeros to every sector of the Destination Drive.
Erase: The Security Erase Unit command. Erases all sectors on the device and also clears the User password.
Security Feature Set: An optional feature set in the ATA Specification. When a User password is set, the ATA device is locked unless unlocked by the User password.
Format: The process of creating a file system on the Destination Drive. The Data Capture Unit can create either a NTFS or a FAT32 filesystem.
Partition: Partitions can be created on a hard drive so that each partition acts like a separate hard drive. In Microsoft Windows, partitions are commonly referred to as drive letters, such as C:\.
Host Protected Area (HPA): A reserved area for data storage outside the normal operating file system.
Device Configuration Overlay (DCO): A virtual device configuration for the hard drive which may change the drive size and/or other properties.
HD or HDD: Hard Drive, also called the Hard Disk Drive.
SSD: Solid State Device or Solid State Drive
SHA-256: A 256 bit value, or fingerprint, generated from each byte of data stored on a drive. In this instance, it is used to verify the data integrity of a drive.
MD5: A 128 bit value, or fingerprint, generated from each byte of data stored on a drive. In this instance, it is used to verify the data integrity of a drive.

GB:	Gigabyte:	1000000000	bytes.
MB:	Megabyte:	1000000	bytes.
KB:	Kilobyte.	1024	bytes.

4 System Configuration

This chapter describes how to connect the Source and Destination Drives to the HardCopy 3P using the component assemblies provided.

Note: Do not leave unconnected data cables plugged into the Data Capture Unit. A non-terminated cable may act as an antenna causing high data error rates. (Connecting a cable at both ends terminates it properly.)

4.1 Installing Source Drive

The Source Drive power and SATA data ports are on the left side of the Data Capture Unit. The Source Drive PATA data port is in the center of the back of the Data Capture Unit and is labeled PARALLEL SOURCE↑. Use the DC power cable with single connectors on both ends to power the Source Drive.

Please follow the steps described below to install a Source Drive:

1. **Power off the Data Capture Unit**.
2. Disconnect both the power and data cables from the Source Drive.
3. Attach the black connector on one end of the DC power cable to the port on the left side of the Data Capture Unit.
4. Attach the other end of the DC power cable to the power receptacle of the Source Drive. Remove the SATA power adapter for a PATA drive.
5. SATA only: Attach a SATA data cable between the Source Drive and the SATA data port on the left side of the Data Capture Unit.
6. PATA only: Attach the PATA ribbon cable between the Source Drive and the PARALLEL SOURCE↑ port on the back of the Data Capture Unit. Make sure the **blue** connector is attached to the Data Capture Unit. For jumper settings, refer to the PATA Jumper Settings section.

Note: Connect only one Source Drive to the Data Capture Unit at a time.

4.2 Installing Destination Drives

The Destination Drive power and SATA data IMAGE 1 ports are on the right side of the Data Capture Unit. The second SATA data port is on the back of the Data Capture Unit and is labeled `IMAGE 2`. Use the DC power cable with the dual SATA power connectors to power the Destination Drives.

Please follow the steps described below to install a Destination Drive:

1. **Power off the Data Capture Unit**.
2. Attach the single black connector on the end of the DC power cable to the port on right side of the Data Capture Unit.
3. Attach one power connector on the other end of the DC power cable to the power receptacle of each Destination Drive.
4. Attach a SATA data cable between each Destination Drive and the IMAGE SATA data ports on the right side and back of the Data Capture Unit.

5 Command Description

This chapter provides a detailed description of each of the commands supported by the HardCopy 3P. Refer to the Button Interface or Serial Interface chapters of this document for information on how to execute each of the commands. Please refer to the Troubleshooting chapter of this document for information relating to failure cases.

5.1 System Test Command

This feature is designed to verify that the drives are connected properly. The test is divided into two distinct steps. The first step reads a fixed number of sectors from the Source Drive and discards the data. The second step reads a fixed number of sectors from the Destination Drives and writes the same data back to the same location on the drives.

Note: No data is written to the Source drive. Both tests are non-destructive.

5.2 Checksum Drive Command

If an HPA and/or DCO exist on the Source Drive, the operator will be notified and the entire HPA will be included in the `hash` calculation. The entire DCO will be included in the `hash` calculation if the user chooses to include it.

Note: When a non-recoverable disk access error is encountered, the `hash` will include the sector of all zeroes that are written. Recovered disk access errors do not affect the `hash` checksum.

5.2.1 SHA-256

This feature calculates a SHA-256 checksum on the entire collection of data stored of either the Source or Destination Drive. Generally speaking, the SHA-256 checksum is a very reliable method of verifying data integrity. The SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. What it does, to quote the introduction of FIPS 180-2, is:

> "[The SHA-256 algorithm] is an iterative, one-way hash function that can process a message to produce a condensed representation called a *message digest*. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message

> authentication codes, and in the generation of random numbers (bits).”

5.2.2 MD5

This feature calculates a MD5 checksum on the entire collection of data stored of either the source or destination drive. Generally speaking, the MD5 checksum is a very reliable method of verifying data integrity. The MD5 algorithm was developed by Professor Ronald L. Rivest of MIT. What it does, to quote the executive summary of rfc1321, is:

> “[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.”

5.3 Clone Drive Command

This feature does a sector-by-sector copy from the Source Drive to the Destination Drive. If the size of the Destination Drive is less than the size of the Source Drive, a failure message will be displayed and the duplication process will terminate prematurely. If the size of the Destination Drive is greater than the size of the Source Drive, the unused sectors on the Destination Drive will automatically be wiped. However, the hardware used to generate the optional `hash` checksum will be disabled while erasing the data from the unused sectors of the Destination Drive.

To prevent accidentally copying over a previously formatted Destination Drive, the user is prompted with a message indicating that the file system will be overwritten, allowing the operator to cancel the current clone command.

If an HPA exists on the Source Drive, the operator will be notified and the entire HPA will be copied to the Destination Drive.

If a DCO exists on the Source Drive, the operator will be notified and the entire DCO will be copied to the Destination Drive if the user chooses to include it.

Whenever the `hash` checksum option is selected, the HardCopy 3P will default to automatically verify the information copied to the Destination Drive after the copy operation has successfully finished. To verify the data on the Destination Drive,

the unit first generates a `hash` checksum on the data copied from the Source Drive, then compares the `hash` checksum value with that previously generated for the Source Drive.

`Hash` option: A `hash` checksum of the Source Drive may be calculated by the hardware while the cloning operation is in process. The checksum is calculated by the hardware, with no software intervention required. However, it still impacts the throughput of the cloning process, throttling the operation at about 101 MB/s with SHA enabled or about 96 MB/s with MD5 enabled.

Wipe option: By default, any unused sectors on the Destination Drive will be wiped after the actual cloning operation has finished. Optionally, the auto-wipe of the Destination Drive may be disabled.

Note: When a non-recoverable disk access error is encountered, the `hash` will include the sector of all zeroes that are written. Recovered disk access errors do not affect the `hash` checksum.

5.4 Image Drive Command

This feature performs a sector-by-sector copy from the Source Drive to a single NTFS file, or multiple 2.3GB FAT32 files created on the Destination Drive. However, it requires the Destination Drive to be formatted prior to the operation. Refer to the Format Drive Command chapter for details.

When using NTFS two files are written to the Destination Drive with each Image Drive capture operation. The first file is a header file containing the summary information associated with the capture. The second file is the binary image file containing the actual data from the Source Drive. The file names associated with the initial capture are “data001.txt” and “data001.dd” respectively. Each successive capture to the same Destination Drive will create unique file names by incrementing the numeric field of the names, e.g. “data002.txt” and “data002.dd”.

When using FAT32 each Image Drive capture operation creates a header file plus multiple binary image files in a unique directory on the Destination Drive, e.g. “DATA001”. The header file will be named “DATA001.TXT” and the binary image files will be named “FILE.000, FILE.001…”.
With both file systems, the image files are linux dd compatible.

The header file contains the following information:

- Title: user entered information, e.g. where and when
- Drive Geometry: model, serial #, sectors, HPA, DCO, etc
- Capture Status: retries, amount captured, checksum, status, etc
- CRC Values: 2GB chunks NTFS, 2.3GB files FAT32

The header file is formatted similar to a Windows .ini file and is an ASCII text file. The Title section is optional while the other sections are automatically generated. An example header file follows:

```
[Title]
text=Captured from John Smith's PC - Voom 01-08-14

[Geometry]
ModelNumber=ST3160815AS
SerialNumber=             6RA8YMZX
BytesPerSector=512
MaximumLBA=312581808
TotalSectors=312581808
TotalCapacity=160041885696
DCOStartLBA=0
DCOSectors=0
DCOSize=0
HPAStartLBA=0
HPASectors=0
HPASize=0

[Capture]
Retries=0
Errors Successfully Recovered=0
ReadErrors=0
WriteErrors=0
MaximumLBA=312581808
TotalSectors=312581808
TotalBytes=160041885696
Source SHA=5130ce13da4543848837cf000269e9c206aea33
e363c192d92e8dbe39d479c74
Image1 SHA=5130ce13da4543848837cf000269e9c206aea33
e363c192d92e8dbe39d479c74
Image2 SHA=5130ce13da4543848837cf000269e9c206aea33
e363c192d92e8dbe39d479c74
Status=complete
Captured On Port IMAGE1
Started at  1/8/14  12:11:12
Finished at 1/8/14  13:32:41

[NTFS CRCs]
00000000-00406f3f=f2907e23
. . . (interim CRCs have been omitted)
12804740-12a19eaf=b24ea805

[Software]
HC3-P 3-01
```

Note: The Title may only be entered when initiating the Image command via the Serial interface.

If an HPA exists on the Source Drive, the operator will be notified and the HPA parameters will be written to the header file.

If a DCO exists on the Source Drive, the operator will be notified and the entire DCO will be copied to the Destination Drive if the user chooses to include it.

`Hash` option: A `hash` checksum of the Source Drive may be calculated while the imaging operation is in process. The checksum is calculated by the hardware with no software intervention required. However, it still impacts the throughput of the imaging process, throttling the operation at about 101 MB/s with SHA enabled or about 96 MB/s with MD5 enabled.

Note: When a non-recoverable disk access error is encountered, the `hash` will include the sector of all zeroes that are written. Recovered disk access errors do not affect the `hash` checksum.

5.4.1 Imaging a 2 Terabyte (2000 GB) Drive

The HardCopy 3P unit can image a 2 TB drive if a greater than 2TB drive is formatted with NTFS by the unit. The HardCopy 3P unit will format the > 2TB drive to (just shy of) 2048 GB, which is the maximum allowable by the MBR formatting scheme. Since commercial 2 TB drives are only 2000 GB in size, the drives formatted to 2048 GB will be able to hold the 2000 GB image.

5.5 File Directory Command

This feature displays the current status of the file system on the Destination Drive. With NTFS it displays the file name and file size, both actual and allocated, of each image capture file. With FAT32 it displays the directory name, allocated size, and number of files for each image capture.
After all files/directories have been displayed, the total size and the free space of the Destination Drives are displayed.

5.6 Format Drive Command

This feature formats a file system onto the Destination Drive. A Destination Drive must be formatted before an Image Drive operation may be attempted. The Data Capture Unit supports formatting a drive in FAT32 or NTFS, either of which can be read by many operating systems.

5.6.1 Formatting a Drive Larger than 2 Terabytes

The HardCopy 3P unit can format drives larger than 2 TB, but the size will be limited to 2048 GB.

Note: Any existing data on the Destination Drive will be lost as a result of a format operation!

5.7 Wipe Drive Command

This feature removes all of the information from the Destination Drive(s). It supports the DoD 5220.22-M specification for clearing information from a hard drive.

5.7.1 1 Pass Wipe Option

This option simply writes a fixed character of all ZEROs to the entire disk drive.

5.7.2 4 Pass Sanitize Option

This option writes for 3 passes and verifies with the fourth pass. First, it writes a fixed character of hex 35 to the entire disk drive. Next, it writes the compliment of the initial fixed character, hex CA, to the entire disk drive. Finally, it writes an arbitrary character, hex 97, to every byte of every sector on the disk drive and verifies that the arbitrary character was written correctly to the entire disk drive.

5.8 Unlock Drive Command

This feature will remove the HPA and DCO from the Destination Drives.

5.9 Show Last Command

This feature will show the last operation the unit performed along with the `hash` checksum if one was generated.

5.10 Set Date and Time Command

This feature allows the user to set the date and time of the Data Capture Unit's internal clock. The internal clock is used when placing a time stamp in the header file of disk images.

5.11 Switch to SHA/MD5 Command

This feature allows the user to switch between the SHA-256 and MD5 hash calculators. This setting is persistent.

5.12 Preserve/Remove DCO Command

This feature allows the user to set behavior to either preserve or remove DCO/HPA definitions from the Destination Drives for Clone operations. The default setting from the factory is to remove DCO/HPA definitions. Choosing this menu option toggles between the 2 behaviors. This persistent setting does not affect Image operations, only Clone operations.

5.13 Update System Command

This feature allows the user to update the system firmware. Specific instructions as to the procedure will be included with the firmware download. Persistent settings will revert to factory settings after a firmware update.

5.14 Security Erase Unit Command

This feature will initiate the ATA Security Erase Unit command. This command is only available via the Serial Interface. All LBAs on the drive will be erased and the User Security password will be cleared. A Security password must be set prior to executing this command. See Security Set Password for more information on the Security Feature Set.

Not all hard drives support the ATA Security Feature Set. The HardCopy 3P unit will let the user know if the Security Feature Set is not supported when the command is attempted.

5.15 Security Set Password Command

This feature will initiate the ATA Security Set Password command. This command is only available via the Serial Interface.

Not all hard drives support the ATA Security Feature Set. The HardCopy 3P unit will let the user know if the Security Feature Set is not supported when the command is attempted.

5.15.1 Security Feature Set Passwords

There are two passwords associated with the Security Feature Set, Master and User. The Master Security password does not activate Security. It exists to allow the drive to be re-purposed if the User Security password is forgotten. The User Security password when set will activate the Security Feature Set locking the drive unless the User password is known.

The HardCopy 3P unit will only allow the Master Security password to be set.

The Master Security password can be set and reset at will without knowing the

old Master password.

6 Button Interface

The button control panel and the LCD are the user interface. The button panel consists of the following three buttons:

Button	Function	Description
Yellow	Menu	This button is designed to step through each of the menu or parameter items. It always steps in a forward direction.
Green	Enter	This button is designed to either select a menu or parameter item, or acknowledge status information.
Red	Cancel	This button is designed to either abort the entering of a new command or the execution of the previous command.

The LCD is used to display each of the menu items, the progress of the current command, and to acknowledge the command status information.

Whenever commands are entered from the button control panel, all status information (e.g. `hash` checksum value, failure information, and completion status) must be acknowledged by the operator. A special arrow character [←] displayed in the lower right hand corner of the LCD indicates that the unit is waiting for acknowledgment of the data currently displayed in the LCD. Press the `<enter>` button each time the arrow character is displayed in order to continue executing the current command.

Note: The user may terminate an executing command by pressing the <cancel> button.

The button command menu is organized into a series of levels and parameter values. When displayed, the command information is displayed on the top line of the LCD and the parameter information on the bottom line. The level information is separated from the command information using a colon (e.g., [1:System Test] refers to level 1, and a command of "System Test"). Each of the parameters associated with a particular command (e.g., `hash` Enabled, `hash` Disabled) are displayed under the command once it has been selected. The prompting hierarchy used to organize the set of supported commands follows:

Level	Prompt	Description
1	System Test	Perform a system test.
2	Checksum Drive	Calculate a `hash` checksum of the entire drive.
	Source Drive	Operate on the Source Drive (default).
	Dest Drive	Operate on the Destination Drive.

Level	Prompt	Description
3	Clone Drive	Clone the entire drive.
	hash Re-Verify	Enable hash hardware while copying and verify the accuracy of the copy by re-calculating the hash checksum from the data written and comparing the results (default).
	hash Enabled	Enable hash hardware while copying.
	hash Disabled	Disable hash hardware while copying.
	Wipe Enabled	Enable wipe of unused area on Destination Drive (default).
	Wipe Disabled	Disable wipe of unused area on Destination Drive.
4	Image Drive	Copy the contents of a drive to a file.
	hash Re-Verify	Enable hash hardware while copying and verify the accuracy of the copy by re-calculating the hash checksum from the data written and comparing the results (default).
	hash Enabled	Enable hash hardware while copying.
	hash Disabled	Disable hash hardware while copying.
5	File Directory	Display the file names and free disk space on the Destination Drive.
6	Format Drive	Format a file system onto the Destination Drive.
	NTFS files	Use the NTFS filesystem.
	FAT32 files	Use the FAT32 filesystem.
7	Wipe Drive	Wipe all information from the Destination Drive.
	(1 Pass)	DoD 5220.22-M 1 pass wipe.
	(4 Pass)	DoD 5220.22-M 4 pass sanitize.
8	Unlock Drive	Remove an HPA and/or a DCO from the Destination Drive.
9	Show Last	Show the last operation.
10	Set Date/Time	Set the date and time.
11	Switch to SHA Switch to MD5	Switch between hash calculators.
12	Preserve DCO Remove DCO	Preserve or Remove DCO/HPA on Destination Drives for Clone operations.
13	System Update	Update the system firmware.

Step-by-step examples (SHA version) of the operations that the user can perform through the button interface are described in the following sections of this chapter:

6.1 System Test Procedure

The following table describes the normal sequence associated with performing a system test of the current configuration:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <enter> to execute the System Test command.
Source: 80GB Dest 1: 80GB Dest 2: 80GB	The status displayed after it discovers the current system configuration. (The LCD scrolls up.)
HPA Start79.3GB HPA Size: 512MB	The status displayed if the Source Drive has data hidden by an HPA.
DCO Start79.8GB DCO Size154.3MB	The status displayed if the Source Drive has data hidden by a DCO.
Testing Source ▒▒▒	Interim status of the system test of the Source Drive.
Testing Dest 1 ▒▒▒▒▒▒▒	Interim status of the system test of the Destination Drive.
Testing Dest 2 ▒▒▒▒▒▒▒▒▒▒	Interim status of the system test of the Destination Drive.
HPA Start LBA: 155000001 ←	If an HPA was detected, note the HPA start LBA, then press <enter> to continue.
HPA Sectors: 1000000 ←	If an HPA was detected, note the HPA size, then press <enter> to continue.
DCO Start LBA: 156000001 ←	If data hidden by DCO was detected, note the DCO start LBA, then press <enter> to continue.
DCO Sectors: 301487 ←	If data hidden by DCO was detected, note the DCO size, then press <enter> to continue.
Task Done 00:00 0B←	The status displayed after it completes the system test.

6.2 Checksum Drive Procedure

The following table describes the normal sequence associated with calculating a SHA checksum of the Source Drive:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <enter> to execute the Checksum Drive command.

LCD interface	Comments
2:Checksum Drive Source Drive	Press <enter> to calculate the SHA checksum on the Source Drive.
Source: 80GB	The status displayed after it discovers the Source Drive.
HPA Start79.3GB HPA Size: 512MB	The status displayed if the Source Drive has data hidden by an HPA.
DCO Start79.8GB DCO Size154.3MB	The status displayed if the Source Drive has data hidden by a DCO.
Summing Drive OK? (or cancel)	Press <enter> to proceed.
DCO hides 154.3MB ←	The status displayed if the Source Drive has data hidden by a DCO, press <enter> to continue.
Read from DCO? (cancel = NO)	Reading data hidden by a DCO is optional (see DCO special precautions). Press <enter> to include the data, <cancel> to exclude it.
DCO restoration after operation←	This information is displayed if you chose to read data hidden by a DCO, press <enter> to continue.
Do not power off until complete ←	This warning is displayed if you chose to read data hidden by a DCO, press <enter> to continue.
Summing 4.2GB/mi 00:06:11 Summing 4.2GB/mi 29/80GB	Interim status of the SHA checksum calculation of the Source Drive. Message will toggle bottom line every few seconds.
Hash for Source ←	Interim message, press <enter> to continue.
7dae7de2edc15a48 SHA words 0- 3←	After noting the SHA checksum value, press <enter> to view the next words.
e6343f7410f63cca SHA words 4- 7←	After noting the SHA checksum value, press <enter> to view the next words.
ab773942df1474d9 SHA words 8-11←	After noting the SHA checksum value, press <enter> to view the next words.
ce613f9608957074 SHA words 12-15←	After noting the SHA checksum value, press <enter> to view the completion status.
HPA Start LBA: 146443922 ←	If an HPA was detected, note the HPA start LBA, then press <enter> to continue.
HPA Sectors: 4551022 ←	If an HPA was detected, note the HPA size, then press <enter> to continue.
DCO Start LBA: 150994944 ←	If data hidden by DCO was detected, note the DCO start LBA, then press <enter> to continue.
DCO Sectors: 5306544 ←	If data hidden by DCO was detected, note the DCO size, then press <enter> to continue.
Task Done 00:23 80.0GB←	After viewing the completion status, press <enter> to return to the main window.

6.3 Clone Drive Procedure

The following table describes the normal sequence associated with cloning a Source Drive (SHA checksum and Wipe options both enabled):

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <enter> to execute the Clone Drive command.
3:Clone Drive SHA Re-Verify	Press <enter> to execute the clone drive command with the SHA checksum and verification feature enabled.
3:Clone Drive Wipe Enabled	Press <enter> to execute the clone drive command with the Wipe feature enabled.
Source: 40GB Dest 2: 80GB	The status displayed after it discovers the current system configuration.
HPA Start34.8GB HPA Size: 3.8GB	The status displayed if the Source Drive has data hidden by an HPA.
DCO Start38.7GB DCO Size: 1.3GB	The status displayed if the Source Drive has data hidden by a DCO.
Cloning Drive OK? (or cancel)	Press <enter> to proceed.
DCO hides 1.3GB ←	The status displayed if the Source Drive has data hidden by a DCO, press <enter> to continue.
Read from DCO? (cancel = NO)	Copying data hidden by a DCO is optional (see DCO special precautions). Press <enter> to include the data, <cancel> to exclude it.
DCO restoration after operation←	This information is displayed if you chose to copy data hidden by a DCO, press <enter> to continue.
Do not power off until complete ←	This warning is displayed if you chose to copy data hidden by a DCO, press <enter> to continue.
Cloning 3.5GB/mi 00:03:52 Cloning 3.5GB/mi 13/40GB	Interim status while copying data. Message will toggle bottom line every few seconds.
aeb716cc47784554 SHA words 0- 3←	Interim status (Source Drive SHA calculation).
c5bbd079cf4645f6 SHA words 4- 7←	Interim status (Source Drive SHA calculation).
f6d2ab2c0aa79d37 SHA words 8-11←	Interim status (Source Drive SHA calculation).

LCD interface	Comments
3e3a0af872c144be SHA words 12-15←	Interim status (Source Drive SHA calculation).
Clone Complete 00:04:01 Wiping to End 14/40GB	Interim status while erasing remaining space on Destination Drive (when Wipe feature enabled). Message will toggle every few seconds.
Wipe Complete 00:14 40.0GB	Interim status (when Wipe feature enabled).
Summing 3.5GB/m 00:07 24/40GB	Interim status (when SHA Re-Verify enabled).
Hash for Dest 2 ←	Interim message, press <enter> to continue.
aeb716cc47784554 SHA words 0- 3←	After noting the SHA checksum value, press <enter> to view the next words.
e6343f7410f63cca SHA words 4- 7←	After noting the SHA checksum value, press <enter> to view the next words.
f6d2ab2c0aa79d37 SHA words 8-11←	After noting the SHA checksum value, press <enter> to view the next words.
3e3a0af872c144be SHA words 12-15←	After noting the SHA checksum value, press <enter> to view the completion status.
HPA Start LBA: 68026393 ←	If an HPA was detected, note the HPA start LBA, then press <enter> to continue.
HPA Sectors: 7558487 ←	If an HPA was detected, note the HPA size, then press <enter> to continue.
DCO Start LBA: 75584880 ←	If data hidden by DCO was detected, note the DCO start LBA, then press <enter> to continue.
DCO Sectors: 2580480 ←	If data hidden by DCO was detected, note the DCO size, then press <enter> to continue.
Task Done 00:36 80.2GB←	After viewing the completion status, press <enter> to return to the main window.

6.4 Image Drive Procedure

The following table describes the normal sequence associated with imaging a Source Drive (SHA checksum option enabled):

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <enter> to execute the Image Drive command.
3:Image Drive SHA Re-Verify	Press <enter> to execute the image drive command with the SHA checksum and verification feature enabled.
Source: 40GB Dest 2: 80GB	The status displayed after it discovers the current system configuration.
HPA Start34.8GB HPA Size: 3.8GB	The status displayed if the Source Drive has data hidden by an HPA.
DCO Start38.7GB DCO Size: 1.3GB	The status displayed if the Source Drive has data hidden by a DCO.
Imaging Drive OK? (or cancel)	Press <enter> to proceed.
DCO hides 1.3GB ←	The status displayed if the Source Drive has data hidden by a DCO, press <enter> to continue.
Read from DCO? (cancel = NO)	Copying data hidden by a DCO is optional (see DCO special precautions). Press <enter> to include the data, <cancel> to exclude it.
DCO restoration after operation←	This information is displayed if you chose to copy data hidden by a DCO, press <enter> to continue.
Do not power off until complete ←	This warning is displayed if you chose to copy data hidden by a DCO, press <enter> to continue.
Allocating Space ▒▒▒▒▒▒▒▒▒▒▒▒	Interim status while preparing the destination file system.
Imaging 3.5GB/mi 00:03:52 Imaging 3.5GB/mi 13/40GB	Interim status while copying data. Message will toggle bottom line every few seconds.
Updating Files File:data001.dd	Interim status while updating the destination file system.
Summing 3.5GB/m 00:07 24/40GB	Interim status (when SHA Re-Verify enabled).
aeb716cc47784554 SHA words 0- 3←	After noting the SHA checksum value, press <enter> to view the next words.
e6343f7410f63cca SHA words 4- 7←	After noting the SHA checksum value, press <enter> to view the next words.

LCD interface	Comments
f6d2ab2c0aa79d37 SHA words 8-11←	After noting the SHA checksum value, press <enter> to view the next words.
3e3a0af872c144be SHA words 12-15←	After noting the SHA checksum value, press <enter> to view the completion status.
HPA Start LBA: 68026393 ←	If an HPA was detected, note the HPA start LBA, then press <enter> to continue.
HPA Sectors: 7558487 ←	If an HPA was detected, note the HPA size, then press <enter> to continue.
DCO Start LBA: 75584880 ←	If data hidden by DCO was detected, note the DCO start LBA, then press <enter> to continue.
DCO Sectors: 2580480 ←	If data hidden by DCO was detected, note the DCO size, then press <enter> to continue.
Task Done 00:36 80.0GB←	After viewing the completion status, press <enter> to return to the main window.

6.5 File Directory Procedure

The following table describes the normal sequence associated with displaying the file directory on the Destination Drive:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <enter> to execute the File Directory command.
data001.dd 80.0GB ←	Press <enter> to acknowledge the file entry information. Repeat until all files have been acknowledged or press <cancel> to return to the main window.
Total: 80.0GB Free: 0B ←	Press <enter> to acknowledge the file summary information.

6.6 Format Drive Procedure

The following table describes the normal sequence associated with formatting the file directory on the Destination Drive:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <enter> to execute the Format Drive command.
Formatting Dest OK? (or cancel)	Press <enter> to proceed.
Enter= FAT32 Cancel=NTFS	Press <enter> to choose FAT32, or press <cancel> to choose NTFS as the file system for the Destination Drives.
Erasing All Data OK? (or cancel)	Press <enter> to proceed.
Dest 1: 80GB Dest 2: 80GB	The status displayed after it discovers the Destination Drives.
Formatting ▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒	Interim status.
format complete ←	Press <enter> to return to the main window.

6.7 Wipe Drive Procedure

The following table describes the normal sequence associated with wiping the Destination Drive:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <menu> again to advance to the next menu item.
7:Wipe Drive	Press <enter> to proceed.
(1 Pass)	Press <menu> to advance to the next menu item.
(4 Pass)	Press <enter> to execute the 4 Pass wipe.
Dest 1: 74GB Dest 2: 74GB	The status displayed after it discovers the Destination Drives.
Sanitizing OK? (or cancel)	Press <enter> to proceed.
Wipe1 4.3GB/m 8.3/74GB Wipe1 4.3GB/m 00:01:51	Interim status. Message will toggle bottom line every few seconds.
Wipe2 4.3GB/m 14/74GB Wipe2 4.3GB/m 00:03:23	Interim status. Message will toggle bottom line every few seconds.
Wipe3 4.3GB/m 15/74GB Wipe3 4.3GB/m 00:03:44	Interim status. Message will toggle bottom line every few seconds.
Verify 4.3GB/m 16/74GB Verify 4.3GB/m 00:03:54	Interim status. Message will toggle bottom line every few seconds.

Task Done 01:17 74.3GB←	After viewing the completion status, press <enter> to return to the main window.

6.8 Unlock Drive Procedure

The following table describes the normal sequence associated with unlocking the Destination Drive:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <menu> again to advance to the next menu item.
7:Wipe Drive	Press <menu> again to advance to the next menu item.
8:Unlock Drive	Press <enter> to execute the Unlock Drive command.
Dest 2: 40GB Dest 1: 80GB	The status displayed after it discovers the Destination Drive.
Removing DCO/HPA OK? (or cancel)	Press <enter> to proceed.
Ds2 no HPA found Ds2 no DCO found	Interim status.
Ds1 HPA removed Ds1 DCO removed	Interim status.

6.9 Show Last Procedure

The following table describes the normal sequence associated with showing the last operation:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <menu> again to advance to the next menu item.
7:Wipe Drive	Press <menu> again to advance to the next menu item.
8:Unlock Drive	Press <menu> again to advance to the next menu item.
9:Show Last	Press <enter> to execute the show last command.
Last Operation: Checksum Drive ←	The last operation is shown.
Hash data for Source ←	Hash data for each drive will be shown, if it exists.
2903390d341b1637 SHA words 0- 3←	After noting the SHA checksum value, press <enter> to view the next words.
6f17b1524906b052 SHA words 4- 7←	After noting the SHA checksum value, press <enter> to view the next words.
a28da284f3cc3ae0 SHA words 8-11←	After noting the SHA checksum value, press <enter> to view the next words.
7aa60f2b910eda97 SHA words 12-15←	After noting the SHA checksum value, press <enter> to continue.

6.10 Set Date and Time Procedure

The following table describes the normal sequence associated with setting the date and time:

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <menu> again to advance to the next menu item.
7:Wipe Drive	Press <menu> again to advance to the next menu item.
8:Unlock Drive	Press <menu> again to advance to the next menu item.
9:Show Last	Press <menu> again to advance to the next menu item.
10:Set Date/Time	Press <enter> to execute the set date and time command.
Month 06/22/10 12:45	Allows incrementing the Month by pressing <enter>. Press <menu> to advance.
Day 06/22/10 12:46	Allows incrementing the Day by pressing <enter>. Press <menu> to advance.
Year 06/22/10 12:47	Allows incrementing the Year by pressing <enter>. Press <menu> to advance.
Hour 06/22/10 12:48	Allows incrementing the Hour by pressing <enter>. Press <menu> to advance.
Minute 06/22/10 12:49	Allows incrementing the Minute by pressing <enter>. Press <menu> to advance.

Note: Pressing <cancel> at any time will exit Set Date/Time.

6.11 Switch to SHA/MD5 Procedure

The following table describes the normal sequence associated with switching the hash calculator.

LCD interface	Comments
`HC3-P 3-01` `Ready  SHA-256`	From the main window, press <menu> to display the initial menu item.
`1:System Test`	Press <menu> again to advance to the next menu item.
`2:Checksum Drive`	Press <menu> again to advance to the next menu item.
`3:Clone Drive`	Press <menu> again to advance to the next menu item.
`4:Image Drive`	Press <menu> again to advance to the next menu item.
`5:File Directory`	Press <menu> again to advance to the next menu item.
`6:Format Drive`	Press <menu> again to advance to the next menu item.
`7:Wipe Drive`	Press <menu> again to advance to the next menu item.
`8:Unlock Drive`	Press <menu> again to advance to the next menu item.
`9:Show Last`	Press <menu> again to advance to the next menu item.
`10:Set Date/Time`	Press <menu> again to advance to the next menu item.

`11:Switch to SHA`
 	
`11:Switch to MD5`
	Press <enter> to execute the switch to SHA command.
	
	Press <enter> to execute the switch to MD5 command.

The Data Capture Unit will switch the active hash calculator and return to the `Ready` prompt.

6.12 Preserve/Remove DCO Procedure

The following table describes the normal sequence associated with toggling the Preserve/Remove DCO for Clone setting..

LCD interface	Comments
`HC3-P 3-01` `Ready  SHA-256`	From the main window, press <menu> to display the initial menu item.
`1:System Test`	Press <menu> again to advance to the next menu item.
`2:Checksum Drive`	Press <menu> again to advance to the next menu item.
`3:Clone Drive`	Press <menu> again to advance to the next menu item.
`4:Image Drive`	Press <menu> again to advance to the next menu item.
`5:File Directory`	Press <menu> again to advance to the next menu item.
`6:Format Drive`	Press <menu> again to advance to the next menu item.
`7:Wipe Drive`	Press <menu> again to advance to the next menu item.
`8:Unlock Drive`	Press <menu> again to advance to the next menu item.
`9:Show Last`	Press <menu> again to advance to the next menu item.
`10:Set Date/Time`	Press <menu> again to advance to the next menu item.
`11:Switch to MD5`	Press <menu> again to advance to the next menu item.

`12:Preserve DCO`
`  on Clone Dest`
 	
`12:Remove DCO`
`  on Clone Dest`
	Press <enter> to toggle behavior to Preserve DCO/HPA for Clone operations.
	
	Press <enter> to toggle behavior to Remove DCO/HPA for Clone operations.

`Clone will`
`Preserve DCO/HPA`
 	
`Clone will`
`Remove DCO/HPA`
	Press <enter> to return to the `Ready` prompt.

6.13 Update System Procedure

The following table describes the normal sequence associated with updating the system firmware.

LCD interface	Comments
HC3-P 3-01 Ready SHA-256	From the main window, press <menu> to display the initial menu item.
1:System Test	Press <menu> again to advance to the next menu item.
2:Checksum Drive	Press <menu> again to advance to the next menu item.
3:Clone Drive	Press <menu> again to advance to the next menu item.
4:Image Drive	Press <menu> again to advance to the next menu item.
5:File Directory	Press <menu> again to advance to the next menu item.
6:Format Drive	Press <menu> again to advance to the next menu item.
7:Wipe Drive	Press <menu> again to advance to the next menu item.
8:Unlock Drive	Press <menu> again to advance to the next menu item.
9:Show Last	Press <menu> again to advance to the next menu item.
10:Set Date/Time	Press <menu> again to advance to the next menu item.
11:Switch to MD5	Press <menu> again to advance to the next menu item.
12:Preserve DCO on Clone Dest	Press <menu> again to advance to the next menu item.
13:Update System	Press <enter> to execute the system update command.
Update Flash? (cancel = NO)	Press <enter> to begin updating the firmware.
Erasing Flash ...	Interim status.
Writing Flash ...	Interim status.
Switch Power Off	Switch the power off to complete the update. (It is now safe to power off the unit.)

Note: Do not switch the power off or disconnect the hard drive during the update process or the HardCopy 3P Unit will need to be returned to Voom for repair.

7 Serial Interface

With the HardCopy 3P unit turned off, connect the supplied serial cable between the HardCopy 3P and a computer. Using a terminal program capable of serial communications, such as HyperTerminal or Tera Term , configure the serial port (usually COM1) as described in the table below:

Parameter	Value
Baud Rate	115200
Data Bits	8
Parity	none
Stop Bits	1
Flow Control	none

Serial Port Settings

Once the serial cable is connected and the terminal program configured, the HardCopy 3P unit may be turned on. For more detail on setting up a terminal program please see the Other Documents on our website downloads page, www.voomtech.com/content/downloads.

The serial interface command list can be displayed anytime using the `Help` command. Command options are preceded with a "-" character and optional parameters are enclosed in brackets.

```
=> help
User Commands:
  Test                 Test the current system configuration
  Checksum <S|D> [bks] Calculate hash for Source or Dest   drives
  Clone    -[cvn] [bks] Clone Source drive to Dest   drive
  Image    -[cv]       Image Source drive to file on Dest   drive
  Directory            Show image files on Dest   drive
  Format               Format the Dest   drive
  Wipe     [4]         Wipe the Dest  drive(s), default is 1 pass
  Unlock               Remove DCO/HPA from the Dest   drive
  LastStatus           Show Last Command Status
  Date     [mm/dd/yy]  Set/Display date
  Time     [hh:mm]     Set/Display time
  SwitchHash           Switch to SHA Hash Calculator
  ToggleRemoveDCO      Toggle Whether to Remove DCO/HPA on Dest
                       drives for Clone Operations
  SecurityErase   -[u|m] [1|2]  Security Erase the Dest  drive(s)
           u or m (default) specifies user or master password
           default choice is ALL Dest  drives; or choose 1 or 2
  SecuritySetPass [1|2]         Set Master Security Password on
Dest  drive(s)
           default choice is ALL Dest  drives; or choose 1 or 2
```

All examples provided in this chapter are of typical operation.

7.1 System Test Procedure

When using the serial interface, the command syntax for testing the system is given below:

```
Test
```

The following example shows the output from a typical system test command.

```
=> Test
Initializing...
Source ST380815AS 80.0GB  (156301488 LBAs)
Dest 1 ST3250310AS 250.0GB  (488397168 LBAs)
Dest 2 ST3250410AS 250.0GB  (488397168 LBAs)
Spinning Drive Source
Spinning Drive Dest 1
Spinning Drive Dest 2
Reading 2048 sectors from Source drive
Reading/writing 2048 sectors from/to Dest 1 drive
Reading/writing 2048 sectors from/to Dest 2 drive
Task Done
```

7.2 Checksum Drive Procedure

When using the serial interface, the command syntax for calculating a `hash` checksum of either the source or destination disk drive is given below:

```
Checksum <S|D> [blks]
```

The required drive field (S = source, D = destination), is used to specify which drive to calculate the `hash` checksum on.

The optional “blks” parameter allows the user to enter a specific number of sectors to be processed. This option allows the user to checksum only the “sectors of interest” for re-verifying a clone on a destination drive which was larger than the source drive.

The following example shows the typical output from a MD5 checksum command.

```
=> Checksum S
Initializing...
Source ST380815AS 80.0GB  (156301488 LBAs)
Summing Drive
OK (y/n)? y
```

```
Spinning Drive Source
Calculating MD5 hash for 156301488 sectors on Source drive
00:00:10, 1516032 sectors, 78.1MB/s (4.5GB/m average)
00:00:20, 3064320 sectors, 78.0MB/s (4.6GB/m average)
00:00:30, 4612608 sectors, 78.0MB/s (4.6GB/m average)
. . .
00:22:23, 156301488 sectors, 42.6MB/s (3.6GB/m average)
Source Port:
MD5: 7a378d758a92b35e5fe43a63e5e395f6
Task Done (00:22:23, 80.0GB)
```

7.3 Clone Drive Procedure

When using the serial interface, the command syntax for duplicating a disk drive is given below:

```
Clone [-cnv] [blks]
       -c     (c)hecksum, enable the hash
calculation
       -n     (n)o-wipe, disable the auto-wipe
       -v     (v)erify, re-verify destination
       blks   only clone blks sectors to
destination
```

All parameters are optional. The default operation is to clone the source without performing a checksum and the auto-wipe enabled.

The optional “blks” parameter allows the user to enter a specific number of sectors to be processed. This option is useful for restoring a clone backup when the copy (now the source) is on a larger drive than the destination drive (originally the source).

The first example calculates a SHA-256 checksum of the source drive while cloning (wipe disabled). The second example calculates a SHA-256 checksum of the source drive while cloning, wipes any unused sectors on the destination drive, then calculates a SHA-256 checksum of the cloned sectors on the destination and verifies the two hash values match.

```
=> Clone -cn
Initializing...
Source ST380815AS 80.0GB  (156301488 LBAs)
Dest 1 ST3250410AS 250.0GB  (488397168 LBAs)
Dest 2 ST3250310AS 250.0GB  (488397168 LBAs)
Cloning Drive
OK (y/n)? y
```

```
Spinning Drive Source
Spinning Drive Dest 1
Spinning Drive Dest 2
Erasing Files
OK (y/n)? y

Copying 156301488 sectors from Source drive to Dest 2
drive and Dest 1 drive
00:00:10, 1354752 sectors, 78.0MB/s (4.1GB/m average)
00:00:20, 2903040 sectors, 78.0MB/s (4.3GB/m average)
00:00:30, 4451328 sectors, 78.1MB/s (4.4GB/m average)
. . .
00:21:57, 155054592 sectors, 37.6MB/s (3.6GB/m average)
00:22:08, 155828736 sectors, 37.7MB/s (3.6GB/m average)
00:22:14, 156301488 sectors, 60.0MB/s (3.6GB/m average)
Source Port:
SHA: 3d88be4d40e75d27767b1946d68f7552
     3c0c42d5aded5e29a09efdde206c36ee
Source Port:
SHA: 3d88be4d40e75d27767b1946d68f7552
     3c0c42d5aded5e29a09efdde206c36ee
Task Done (00:22:14, 80.0GB)


=> Clone -v
Initializing...
Source ST380815AS 80.0GB  (156301488 LBAs)
Dest 1 ST3250410AS 250.0GB  (488397168 LBAs)
Dest 2 ST3250310AS 250.0GB  (488397168 LBAs)
Source HPA Start66.5GB
Source HPA Size: 5.1GB
Source DCO Start71.6GB
Source DCO Size: 8.3GB
Data hidden by DCO: 8.3GB
Read from DCO?
OK (y/n)? y

Because DCO and HPA are both present,
HPA restore may fail if data hidden by DCO is read.
Read from DCO?
OK (y/n)? y

DCO will be restored after operation
Do not power off until Ready prompt
Cloning Drive
OK (y/n)? y
```

```
Spinning Drive Source
Spinning Drive Dest 2
Spinning Drive Dest 1
Erasing Files
OK (y/n)? y

Dest 1 HPA removed
Dest 1 DCO removed
Dest 2 HPA removed
Dest 2 DCO removed
Copying 156301488 sectors from Source drive to Dest 2
drive and Dest 1 drive
00:00:10, 1354752 sectors, 78.0MB/s (4.5GB/m average)
00:00:20, 2903040 sectors, 78.0MB/s (4.6GB/m average)
00:00:30, 4451328 sectors, 78.1MB/s (4.6GB/m average)
. . .
00:22:14, 156301488 sectors, 38.4MB/s (3.6GB/m average)
Source Port:
SHA: 3d88be4d40e75d27767b1946d68f7552
     3c0c42d5aded5e29a09efdde206c36ee
Clone Complete (00:22:14, 80.0GB)
Wiping 332095680 sectors on Dest 2 drive and 332095680
sectors on Dest 1 drive
00:00:10, 1838592 sectors, 94.0MB/s (5.5GB/m average)
00:00:20, 3709440 sectors, 95.4MB/s (5.6GB/m average)
00:00:30, 5580288 sectors, 95.4MB/s (5.6GB/m average)
. . .
00:34:37, 332095680 sectors, 61.2MB/s (4.9GB/m average)
Wipe Complete (00:34:37, 170.0GB)
Verifying 156301488 sectors on  Dest 2 drive and Dest 1
drive
00:00:10, 1741824 sectors, 92.4MB/s (5.3GB/m average)
00:00:20, 3580416 sectors, 92.6MB/s (5.4GB/m average)
00:00:30, 5419008 sectors, 92.6MB/s (5.4GB/m average)
. . .
00:13:59, 156301488 sectors, 103.5MB/s (5.7GB/m average)
Verify Complete (00:13:59, 80.0GB)
Image Ports (identical):
SHA: 3d88be4d40e75d27767b1946d68f7552
     3c0c42d5aded5e29a09efdde206c36ee
Source HPA Start: 130000001
Source HPA Size: 10000000
Source DCO Start: 140000001
Source DCO Size: 16301487
Task Done (01:10:50, 250.0GB)
```

7.4 Image Drive Procedure

When using the serial interface, the command syntax for imaging a disk drive is given below:

```
Image [-cv]
       -c     (c)hecksum, enable the hash
calculation
       -v     (v)erify, re-verify destination
```

The default operation is simply to create an image of the source drive without performing a checksum.

The example creates a drive image while `hashing` the Source Drive, then re-verifies the `hash` on the Destination Drives.

```
=> Image -v
Initializing...
Source ST31000340AS 1000.2GB  (1953525168 LBAs)
Dest 1 ST31500341AS 1500.3GB  (2930277168 LBAs)
Dest 2 ST31500341AS 1500.3GB  (2930277168 LBAs)
Imaging Drive
OK (y/n)? y

Title (255 characters):
> Captured from the PC of John Smith, Voom lab 07-06-2010

Spinning Drive Source
Spinning Drive Dest 1
Spinning Drive Dest 2
Allocating disk space
Copying 1953525168 sectors from Source drive to  Dest 2
drive and Dest 1 drive
00:00:10, 1932608 sectors, 100.9MB/s (5.8GB/m average)
00:00:20, 3932480 sectors, 101.3MB/s (5.9GB/m average)
00:00:30, 5932352 sectors, 101.1MB/s (5.9GB/m average)
. . .
03:18:50, 1953525168 sectors, 56.9MB/s (5.0GB/m average)
Source Port:
SHA: f494a272b7fbd55fd32ca176beb2d03b
     416127ef9ce78187479f43f11e78f365
Updating File System [file: data001.dd]
Verifying 1953525168 sectors on  Dest 2 drive and Dest 1
drive
00:00:10, 1964864 sectors, 100.7MB/s (5.9GB/m average)
00:00:20, 3964736 sectors, 101.1MB/s (5.9GB/m average)
00:00:30, 5964608 sectors, 101.1MB/s (6.0GB/m average)
```

```
. . .
02:46:11, 1953525168 sectors, 94.8MB/s (6.0GB/m average)
Image Ports (identical):
SHA: f494a272b7fbd55fd32ca176beb2d03b
     416127ef9ce78187479f43f11e78f365
Image Ports (identical):
SHA: f494a272b7fbd55fd32ca176beb2d03b
     416127ef9ce78187479f43f11e78f365
Verify Complete (02:46:11, 1000.2GB)
```

7.5 File Directory Procedure

When using the serial interface, the command syntax for displaying the current file directory is given below:

```
Directory
```

The examples below shows the output for each filesystem associated with displaying the current file directory of the destination drive. The comments in parentheses are informational only and are not to be typed.

```
=> Directory     (NTFS)
Initializing...
              Dest 2 missing
Dest 1 WDC WD3000GLFS-01F8U0 300.0GB  (586072368 LBAs)
Spinning Drive Dest 1
File Name    File Size  Allocated
-----------  ---------  ---------
 data001.dd     80.0GB     80.0GB
data001.txt      1.9KB      4.1KB
Total Bytes: 300.0GB
Free  Bytes: 220.0GB

=> Directory     (FAT32)
Initializing...
Dest 1 WDC WD3000GLFS-01F8U0 300.0GB  (586072368 LBAs)
Dest 2 WDC WD3000GLFS-01F8U0 300.0GB  (586072368 LBAs)
Spinning Drive Dest 1
Spinning Drive Dest 2
DIR  Name    Used Size  Files
-----------  ---------  ---------
    DATA001     80.0GB         36
Total Bytes: 300.0GB
Free  Bytes: 220.0GB
```

7.6 Format Drive Procedure

When using the serial interface, the command syntax for formatting the destination drive is given below:

```
Format
```

The following example shows the output associated with formatting the file system on the destination drive.

```
=> Format
USE FAT32?
OK (y/n)? n

Formatting Dest
OK (y/n)? y

Erasing Data
OK (y/n)? y

Initializing...
Dest 1 ST31500341AS 1500.3GB  (2930277168 LBAs)
Dest 2 ST31500341AS 1500.3GB  (2930277168 LBAs)
Spinning Drive Dest 1
Spinning Drive Dest 2
Formatting NTFS file system
format complete
```

7.7 Wipe Drive Procedure

When using the serial interface, the command syntax for wiping the destination drive is given below:

```
Wipe [4]
      4     Choose the 4 Pass Wipe, default is
            1 Pass
```

The following example shows the output associated with wiping the information from the destination drive.

```
=> wipe
Initializing...
              Dest 2 missing
Dest 1 WDC WD3000GLFS-01F8U0 300.0GB  (586072368 LBAs)
Wiping Dest
OK (y/n)? y

Spinning Drive Dest 1
Wiping 586072368 sectors on Dest 1 drive
00:00:10, 2354688 sectors, 119.8MB/s (7.0GB/m average)
00:00:20, 4741632 sectors, 119.8MB/s (7.1GB/m average)
00:00:30, 7128576 sectors, 119.8MB/s (7.1GB/m average)
. . .
00:46:55, 586072368 sectors, 91.2MB/s (6.3GB/m average)
Task Done (00:46:55, 300.0GB)
```

7.8 Unlock Drive Procedure

When using the serial interface, the command syntax for unlocking the destination drive is given below:

```
Unlock
```

The following example shows the output associated with removing the HPA and DCO from the destination drive.

```
=> Unlock
Initializing...
              Dest 2 missing
Dest 1 ST380815AS 80.0GB  (156301488 LBAs)
Removing DCO/HPA
OK (y/n)? y

Spinning Drive Dest 1
Dest 1 HPA removed
Dest 1 DCO removed
```

7.9 Show Last Status Procedure

When using the serial interface, the command syntax for showing the last command status is given below:

```
LastStatus
```

The following example shows the output associated with showing the status of the last command.

```
=> LastStatus

Last Operation: Checksum Drive
Hash data for Dest 1:
SHA: d2517c859944ed5654f68061f09c824e
     f1dfaff3f394b551013eab584236a7b7
```

7.10 Date Procedure

When using the serial interface, the command syntax for showing/setting the date is given below:

```
Date [dd:mm:yy]
```

The following example shows the output associated with showing the status of the last command.

```
=> date
5/21/08  15:51:30
=> date 07/08/10
7/8/10  15:51:39
```

7.11 Time Procedure

When using the serial interface, the command syntax for showing/setting the time is given below:

```
Time [hh:mm]
```

The following example shows the output associated with showing the status of the last command.

```
=> time
5/21/08   6:22:18
=> time 15:51
5/21/08  15:51:28
```

7.12 Switch Hash Procedure

When using the serial interface, the command syntax for switching the active hash algorithm is given below:

```
SwitchHash
```

The following example shows the output associated with switching the hash algorithm.

```
=> SwitchHash
MD5 Hash Calculator Enabled
=> SwitchHash
SHA Hash Calculator Enabled
```

7.13 Toggle Remove DCO Procedure

When using the serial interface, the command syntax for toggling the remove DCO persistent setting is given below:

```
ToggleRemoveDCO
```

The following example shows the output associated with toggling the remove DCO persistent setting.

```
=> toggleremovedco
Clone Command will preserve DCO/HPA.
=> toggleremovedco
Clone Command will remove DCO/HPA.
```

7.14 Security Erase Unit Procedure

The Security Erase Unit command is only available via the serial interface. The command syntax for initiating a Security Erase Unit command is given below:

```
SecurityErase -[u|m] [1|2|
        u       use the User password
        m       use the Master password (default)
        1       Erase only dest 1
        2       Erase only dest 2
                (default is all destination drives)
```

```
=> securityerase 2
Erasing Drive
OK (y/n)? y

Initializing...
             Dest 1 missing
Dest 2 WDC WD1600AAJS-00YZCA0 160.0GB  (312581808 LBAs)

Please enter the Master Password
> ****

Dest 2:  Beginning security erase.
Spinning Drive Dest 2
00:00:10 Time est  30 min from Manufacturer
00:00:20 Time est  30 min from Manufacturer
. . .
00:30:00 Time est  30 min from Manufacturer
00:30:10 Time est  30 min from Manufacturer
Dest 2:  security erase completed successfully
Task Done(00:30:12, 0B)
```

Note: A Security password must be set for Security Erase Unit to succeed.

Note: The maximum password length is 32 characters.

Important: Use Security Erase Unit instead of Wipe/Sanitize for SSDs to prevent unnecessary writes which will shorten the life of the SSD.

7.15 Security Set Password Procedure

The Security Set Password command is only available via the serial interface. The command syntax for initiating a Security Set Password command is given below:

```
SecuritySetPass [1|2|
       1      Set Master password only on dest 1
       2      Set Master password only on dest 2
              (default is all destination drives)
```

```
=> securitysetpass
Setting Security Password
OK (y/n)? y

Initializing...
             Dest 2 missing
Dest 1 ST3250312AS 250.0GB  (488397168 LBAs)

Please enter the Master Password
> ****


Please Re-enter the Password
> ****

Dest 1:  Setting Master password.
Task Done(00:00:01 0B)
```

Note: The maximum password length is 32 characters.

Due to the sensitive nature of security procedures VoomTech has chosen not to implement the feature of setting a User Security password, which activates the Security Feature Set on the device. We allow the setting of a Master Security password because an active password is necessary to initiate the Security Erase Unit command. Master Security passwords do not activate the Security Feature Set. The purpose of the Master Security password is for re-purposing the device if the User Security password has been forgotten.

8 File Management

8.1 NTFS

The Data Capture Unit is designed to manage a NTFS compatible file system on Destination Drives. An entire Source Drive can be captured to a single file on a Destination Drive. With the built in NTFS support multiple Source Drives may be captured to distinct files on a single Destination Drive. The process of capturing multiple Source Drives to a single Destination Drives is as follows:

1. Install a new Destination Drive on the Data Capture Unit.
2. Prepare the Destination Drive using the Format Drive command with the NTFS option.
3. Capture the first Source Drive using the Image Drive command.
4. View the remaining capacity on the Destination Drive using the File Directory command.
5. If sufficient free space remains on the Destination Drive, Image another Source Drive.
6. Remove the Destination Drive from the Data Capture Unit.
7. Install the Destination Drive on a computer to analyze the captured data.

However, because NTFS is a closed specification, it is important to note the limitations of the built-in NTFS compatible support listed below:

- After **mounting a hard drive read/write on MS Windows** to analyze an image the Data Capture Unit will require the hard drive to be reformatted. This feature is designed to protect existing file systems from being corrupted by HardCopy's incomplete directory support.
- The Destination Drive **must be formatted** with the Data Capture Unit's Format Drive command.
- Files may **only be added** to the Destination Drive. There is no support for deleting old files (with the exception of a new Format command).
- There is a 28 file limit. As each capture creates both a header and a binary file only **14 Source Drives may be captured** to a single Destination Drive.

8.2 FAT32

The FAT32 compatible file system support operates similarly to the NTFS compatible file system support. The differences are noted here:

- HardCopy stores images in separate directories in consecutively numbered chunked files. (Versus a single file with NTFS.)
- FAT32 does not have the 28 file limit.

9 Special Precautions

This chapter describes some scenarios that require special attention in order to prevent unexpected results when operating the Data Capture Unit. Each situation is described within this chapter.

9.1 Using the Buttons

The system automatically de-bounces each of the switch operations. In addition, to avoid unexpected results caused by “double-clicking” any of the buttons, all previous button status is cleared after each prompting message is displayed to the LCD. Therefore, each prompting message will be displayed for a minimum of 0.5 seconds before the unit will respond to any operator input from the buttons.

The user may experience up to a 30 second response delay if the hardware is waiting for a drive to respond (e.g. spinning up a drive).

9.2 Formatting Destination Drives

Powering off the Data Capture Unit while formatting a Destination Drive will result in a corrupt file system. To avoid a corrupt file system **do not power off the Data Capture Unit until after the Format Drive operation has completed**.

Note: The Format Drive command cannot be interrupted by the <cancel> button.

9.3 Powering Off the HardCopy 3P

Powering off the unit while the Data Capture Unit is operating is not recommended. Before powering off the unit, make sure that it is in the idle state by canceling any command that is currently executing. To cancel a command from the button interface, first press the <cancel> button - once only - and then respond to each of the prompts until the “Ready” status is indicated on the LCD. To cancel a command from the serial interface, first enter <Ctrl C>, then respond to each of the user prompts until the “=>” is displayed on the terminal.

Note: Powering off the Data Capture Unit while imaging a Source Drive will result in a corrupt file system on the Destination Drive. To avoid a corrupt file system do not power off the Data Capture Unit until after the Image Drive operation has completed or successfully canceled.

Note: The Image Drive command cannot be interrupted by the <cancel> button while it is either allocating or de-allocating space on the Destination Drive.

9.4 PATA Jumper Settings

Theoretically, any jumper setting should work provided the PATA Source Drive is connected to the end of the ribbon cable (black connector). In practice however, the jumper setting may matter.

- If the Source Drive has a “single” drive jumper setting, use it. This setting tells the drive it is the only drive on the cable and the initialization times will be faster. (This setting may be called “force 1 drive.”)
- If the Data Capture Unit does not see a PATA Source Drive using one jumper setting, try a different one. Some drives may respond in a way which is incompatible with the Data Capture Unit in one setting versus another. If such a drive is found, please let Voom know the drive model and which jumper setting did not work.

Known incompatible settings (incompatible setting marked with X):

Model	Master	Cable Select	Slave	Single
IBM Deskstar DTLA-305020		X	X	
Western Digital Caviar 84AA	X			

9.5 Device Configuration Overlays (DCOs)

The ATA Device Configuration Overlay (DCO) feature set provides yet another way to hide data on a disk drive. The HardCopy 3P will recognize the presence of data hidden by a DCO on the Source Drive, and allows you to include that data as part of a Clone or Image.

Because of the way that the DCO feature works and the way it interacts with the HPA feature set, a power interruption (including switching the HardCopy 3P unit off) while accessing data hidden by a DCO will cause the loss of the DCO definition (and HPA as well, if present). For this reason, the HardCopy 3P allows you to choose not to copy data hidden by a DCO. Also, if HardCopy 3P does not recognize the format of the DCO information reported by the Source Drive, it will not attempt to access the data hidden by a DCO.

Another possible loss of the HPA definition exists if both a DCO and HPA reside on the same drive and the DCO is read. Some hard drives may not permit an HPA to be restored after accessing data hidden by a DCO. No data is lost or changed on the Source drive if this issue occurs, but there would no longer be data hidden by an HPA. For this reason, the Data Capture Unit will warn the user of the possible loss of the HPA before allowing the user to proceed. The user should always write down the start LBA of the HPA before initiating an operation

which reads from the DCO if HPA restoration is desired. If HPA restoration fails, the user will need to manually restore the HPA with a program such as hdparm.

9.6 Security Erase Unit Behavior

We have noticed some hard drives will not succeed with the Security Erase Unit command. These drives are:

- Seagate Barracuda 7200.9 family
- Seagate Barracuda 7200.10 family
- Hitachi Deskstar HDS721680PLA380

Security Erase Unit did succeed with Seagate Barracuda 7200.7, 7200.11 and 7200.12 family drives.

9.7 Defective Hard Drives

In our Voom Technologies, Inc. lab we have noticed that a hard drive which has just begun to fail may not throw an error, but fail to correctly write the data. For this reason it is always recommended to choose the Re-Verify option for all Clone and Image operations. The Data Capture Unit will report a `hash` mismatch in this case when Re-Verify is enabled.

9.8 Incompatibility Issues

Our goal is to support every hard drive possible. Almost all read/write problems with hard drives are due to damaged hard drives, whether it is damaged media or damaged hard drive controllers.

Occasionally there are hard drives that violate the ATA bus standard, and we have included special support for these drives as we encounter them. If you have problems imaging a drive, other than errors reading sectors, please contact us via email, and we will respond promptly.

10 Troubleshooting

This chapter describes operation failures that may occur during the execution of the commands previously described.

10.1 Standard Commands

Since the same information is displayed to both the LCD and the serial interface, we will use the LCD format to describe each of these conditions. The following table provides a brief description of the most common events leading up to each failure condition and also describes some suggestions for resolving the problem:

LCD information	Detailed description
`Error Recovery`	HardCopy 3P supports error recovery for drives that operate intermittently. If the unit is unable to copy a sector from the Source Drive to the Destination Drive after 6 consecutive attempts it will fill the corresponding sector on the Destination Drive with an all zeros (0x00) data pattern, increment the appropriate drive access error counter, and continue with the capture operation. The total number of drive access errors (read or write), along with a list of the Logical Block Addresses associated with each of the errors (maximum of 16 for each access type), will be displayed to the user when the operation completes.
`Source Drive -no drive found`	This message is displayed whenever one of the following conditions occur: No power to the Source Drive. No SATA cable to the Source Drive. Unable to identify the Source Drive. Hint: Make sure that the SATA cable is installed correctly.
`Source Drive -read error`	This message is displayed whenever one of the following conditions occur: A read error was detected while testing the Source Drive. A read error was detected while calculating a checksum on the Source Drive. Hint: Check the cables and repeat the command, as the sectors on the Source Drive may be intermittent.

Destination Driv - no drive found	This message is displayed whenever one of the following conditions occur: No power to the Destination Drive. No SATA cable to the Destination Drive. Unable to identify the Destination Drive. Hint: Make sure that the SATA cable is installed correctly.
Destination Driv -read error	This message is displayed whenever the following condition occurs: A read error was detected while testing the Destination Drive. Hint: Check the cables and/or replace the Destination Drive.
Destination Driv -write error	This message is displayed whenever one of the following conditions occur: A write error was detected while testing the Destination Drive. A write error was detected while capturing a Source Drive. Hint: Replace the Destination Drive.
Destination Driv -data error	This message is displayed whenever the following condition occurs: A data error was detected while testing the Destination Drive. Hint: Replace the Destination Drive.
Destination Driv -not enough capa	This message is displayed whenever the following condition occurs: Attempting to clone a Source Drive that has a larger capacity than the current Destination Drive. Hint: Install a Destination Drive with adequate capacity to capture the Source Drive.
Destination Driv -directory is fu	This message is displayed whenever the following condition occurs: Attempting to image a source drive when the Destination Drive has too many files stored on it. Hint: Reformat the Destination Drive. The directory limit is 28 files for NTFS, which is enough to capture 14 source drives. Fat32 has no file limit.

Destination Driv -drive is full	This message is displayed whenever the following condition occurs: Attempting to image a source drive when the Destination Drive has too little free space on it. Hint: Reformat the Destination Drive. An image file for a 80 GB drive requires more than 80 GB of space on the Destination Drive due to the file system overhead.
Destination Driv -partition error	This message is displayed whenever the following condition occurs: Unable to partition the Destination Drive. Hint: Reformat the Destination Drive. If unable to do so, replace the Destination Drive.
Destination Driv -format error	This message is displayed whenever the following condition occurs: Unable to format the Destination Drive. Hint: Replace the Destination Drive.
Destination Driv -drive not forma	This message is displayed whenever the following conditions occur: The previous clone operation destroyed the file system on the Destination Drive. The file system on the Destination Drive was modified by a different operating system. Hint: Reformat the Destination Drive.
Destination Driv -no PIO mode (NT	This message is displayed whenever the following condition occurs: Attempting to format a Destination Drive that only supports PIO access. Hint: Replace the Destination Drive with one that supports UDMA access.
Insufficient Mem [Power Off Unit]	This message is displayed whenever the following condition occurs: The operating system has exhausted all of its memory resources. This should never happen under normal operating circumstances. Hint: Please report this problem to the customer service department so that can be corrected in the next software release.

`Write Protect Er [Power Off Unit]`	This message is displayed whenever the following condition occurs: The unit attempted to write information to the Source Drive. This should never happen under normal operating circumstances. Hint: Please report this problem to the customer service department so that can be corrected in the next software release.

10.2 Serial Interface Only Commands

`Drive x: Command Failed: Command aborted`

The most likely reason this error will be reported is if the security password supplied did not match or was not set on the device.

Try a power cycle to clear the device status and try again.

Any other reason is undocumented. The device being erased likely failed to complete the command.

11 Warranty

11.1 Limited Warranty

Voom Technologies, Inc. (VoomTech) warrants the HardCopy 3P hardware against defects in material and workmanship under normal use and service for one (1) year from the original date of purchase. Voom, at its option, shall repair or replace the defective unit covered by this warranty.

VoomTech does not warrant this product to be free of interruption or errors.

This warranty covers only defects that arise from normal usage of the product, as it is intended by Voom and indicated in this User Guide and does not cover other issues, including those arising from:

- Improper maintenance or handling,
- Use of parts or supplies not included with the product or approved for usage by VoomTech,
- Operations that deviate from those intended or indicated in this User Guide,
- Misuse or abuse of the product, modification of the product that is unauthorized by Voom, subjecting the product to abnormal working conditions (including, but not limited to, water or lightning damage) or tampering with the product.

Upon notification of defect in materials or workmanship and return of the product in accordance with the Warranty Return Instructions (below) and in concurrence with the warranty conditions as indicated above, VoomTech shall either repair or replace the product at its discretion. VoomTech reserves the right to replace the product with a new or like-new product that has functionality equal to or exceeding that of the originally purchased product.

Voom will be obligated to repair or replace the product only after the product has been returned according to the instructions below and has been received by VoomTech.

This warranty is valid only if the product is used in conjunction with devices indicated in this User Guide.

Repair or replacement as provided under this warranty is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose, and Voom Technologies, Inc., shall in no event be liable to purchaser for indirect or consequential damages of any kind or character.

Some states do not allow the exclusion or limitation of incidental or consequential damages or allow limitations on how long an implied warranty lasts, so the above limitations or exclusion may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

11.1.1 Wearable Parts

The data cables are subject to wear and should be replaced on a regular basis. The DC power cables and data cables are considered “wearable” parts and as such are not covered under the warranty except for initial manufacturer defects.

11.2 Warranty Return Instructions

For timely warranty repair and return of the Product please follow the procedure outlined below.

1. Contact a VoomTech representative (651-998-1618) to obtain a Return Material Authorization (RMA) number.
2. Please be prepared to provide the VoomTech representative with the product serial number, the invoice number and the date of purchase in order to facilitate this process.
3. Once you receive a RMA number, please pack the Product in its original packaging or any other secure box so that no damage may occur.
4. Deliver the Product **shipping prepaid** to:

   Voom Technologies, Inc.
   110 St. Croix Trail South
   Lakeland, MN 55043
   Attention: RMA _____

5. Shipping with proper insurance and a tracking number is highly advised.
6. Please be sure to include in the return package complete contact information including return shipping information. Please also include a brief description of the problem and a copy of the RMA number.
7. If you do not obtain an RMA, your return will not be able to be processed immediately and may be returned unprocessed.

NOTE: Voom Technologies, Inc. is not responsible for items lost or damaged in transit.

12 Specifications

This chapter describes the specifications for the Model No. VTHCPL-3PFD HardCopy 3P unit.

AC Electrical Requirements	
AC Adapter Voltage	Universal AC, 100 VAC/240 VAC
Frequency	50-60 Hz
Current	1.3 Amps
Output Voltage	12 VDC @ 7 A
Manufacturer	FSP Group Model: FSP084-DMAA1 or equivalent
Fusing	5 Amp slow blow (5X20 mm) internal

Operating Environment	
Temperature	50 to 95 Degrees F
Relative Humidity	20% to 80% (non condensing)
Altitude	0 to 8000 Feet

Physical Characteristics	
Height	1.5 inches
Width	5.625 inches
Depth	4 inches
Weight	I pound (excluding accessories)

Specifications are subject to change without notice.

12.1 CE

Users need to notify any information technology equipment users within a 60 meter radius that HardCopy 3P may interfere with other electronic equipment. Although the manufacturer has not observed electromagnetic interference from the HardCopy 3P with other electronic equipment in its development lab or offices, this is not an indication that the user will not experience electromagnetic interference from the HardCopy 3P with other electronic equipment within the 60 meter radius.

12.2 FCC Exemption

This device is exempt from FCC regulations under Part 15, Section 103 c.