

PUMA

Portable Universal Media Archive



User Manual V 2.8

Including PUMA^{BP} and Dual Drive

Jan 2022

Table of Contents

1	Description.....	4
2	Quick Start Guide.....	6
2.1	Making Master and Working Copies.....	6
2.2	Turning Off.....	6
3	Detailed Operation.....	7
3.1	Setting up and Powering PUMA.....	7
3.2	Making Evidential backup of Flash Card or USB stick.....	7
3.3	Turning Off.....	8
3.4	Checking for External Drive and PUMA Status Information.....	8
3.5	Using SoundByte with PUMA.....	8
3.6	Menu System.....	9
3.6.1	To Select a Menu Item.....	9
3.6.2	Main Menu List.....	9
3.6.3	Disk to Disk Sub-menu List (Dual Drive Only).....	9
3.6.4	Settings Sub-menu List.....	9
3.6.5	Utilities Sub-menu List.....	9
3.7	Main Menu Items.....	10
3.7.1	Make Working Copy (make simple file copy).....	10
3.7.2	Make Encrypted Copy.....	10
3.7.3	Make Master Copy.....	10
3.7.4	Hard Disk Master.....	10
3.7.5	Disk to Disk.....	11
3.7.6	Wipe Flash Card.....	11
3.7.7	Format Flash card.....	11
3.7.8	Adjust the Internal Time and Date.....	11
3.8	Disk to Disk Sub-menu.....	12
3.8.1	Disk Copy.....	12
3.8.2	Encrypted Disk Copy.....	12
3.8.3	Working from Master.....	12
3.9	Settings Sub-menu.....	12
3.9.1	Navigation and Settings.....	12
3.9.2	Set Master Disk Type.....	12
3.9.3	Set Working Disk Type.....	12
3.9.4	Enable JPEG creation on Working Copies.....	13
3.9.5	Adjust the Internal Time and Date.....	13
3.10	Utilities Sub-menu.....	13

3.10.1	Make Video DVD.....	13
3.10.2	Make Working HD.....	13
3.10.3	Verify Master Copy against Flash Card.....	13
3.10.4	Verify Multi-Disk Master Set.....	13
3.10.5	Restore the Master Copy to a Flash Card.....	13
3.10.6	Restore Multi-Disk Master Set.....	14
3.10.7	Calculate the Checksum of the Flash Card.....	14
3.10.8	Calculate the Checksum of the Master Disk Image.....	14
3.10.9	Software Installation Procedure.....	14
4	Technical Background.....	16
4.1	PUMA Master Copy (bit for bit copy).....	16
4.1.1	Full Image Master.....	16
4.1.2	Compact Master.....	16
4.1.3	Quick Master.....	17
4.1.4	The Compact Master process.....	17
4.1.5	Why archive the file system?.....	17
4.1.6	Partition Table.....	17
4.1.7	File allocation information.....	18
4.1.8	File un-deletion.....	18
4.1.9	Historical file data.....	18
4.1.10	Media history and fragmentation.....	18
4.2	PUMA ancillary functions.....	19
4.2.1	Disk Verify Read.....	19
4.2.2	Working Copy (file copy).....	19
4.2.3	Card and Disk Checksum.....	19
4.2.4	Flash Card Wipe (Erasing).....	19
4.2.5	AES 256 Encryption.....	20
4.3	System Architecture.....	20
4.4	Transfer Times.....	20
4.5	RAW File handling.....	20
5	Technical Support.....	21
5.1	System re-starting in the event of failure.....	21
5.2	Contact.....	21
5.3	Software Updates.....	21
6	Specifications.....	22
7	Disclaimer.....	22

1 Description

PUMA has become the de-facto standard tool for creating evidential Masters for use in UK courts.

PUMA is a rugged and evidentially secure system for archiving USB and flash card data to CDROM, DVD, or BD⁽¹⁾ media or to an external hard drive. Its automated backup procedure make it simple to use. It is aimed primarily at backing up flash based audio and video recorders and digital cameras and includes a RAW to JPEG image converter. PUMA will back up any type of file data and can be used to archive USB pen drives and other USB disk drives. The main features are as follows:

- Simple operation. Single, dedicated “Transfer” button initiates entire archive sequence.
- All disks are finalised after writing to prevent evidential tampering.
- Rugged construction with no hard drive and full-height CD/DVD/Blu-ray drive increases reliability and evidential security.
- Unique bit for bit copy of flash card provides ultimate evidential audit trail and reduces possibility of legal challenges without increasing back-up size.
- Three automated steps in transfer procedure: Transfer, data verify, and flash media overwrite/erase/format.
- Flash card, forensic wipe process ensures that deleted data cannot be recovered and removes any viruses.
- Fast transfer rates reduces back-up time. Up to four times faster than laptop for transferring files. 20Mbyte /sec transfer rate.
- Re-mounts and verifies disk after writing to ensure maximum reliability of backup.
- Supports wide range of BD-R⁽¹⁾, BD-R DL, DVD +/- R, +R/-R DL and CD -R media. Working copies can be made on USB drives (new in V2.8.18)
- Proprietary software tailored precisely to the needs of law enforcement and evidence gathering. Closed nature of operating system increases evidential security
- JPEG versions of RAW files generated on Working Copy. A list of supported RAW camera formats is given in APPENDIX 1.
- Can be powered from mains, vehicle power⁽²⁾ or external batteries⁽²⁾.
- Supports all common flash media (see Specification), USB hard drive.

New in Version 2.8

- Dual Drive Option (external DVD or Blu-ray Writer) with disk to disk functions such as disk copying and AES 256 encryption (Option) and Working Copy from Master Disk production. SoundByte recorders are supported from V2.8.14.

(1) Blu-ray support is an option.

(2) Requires optional adapter

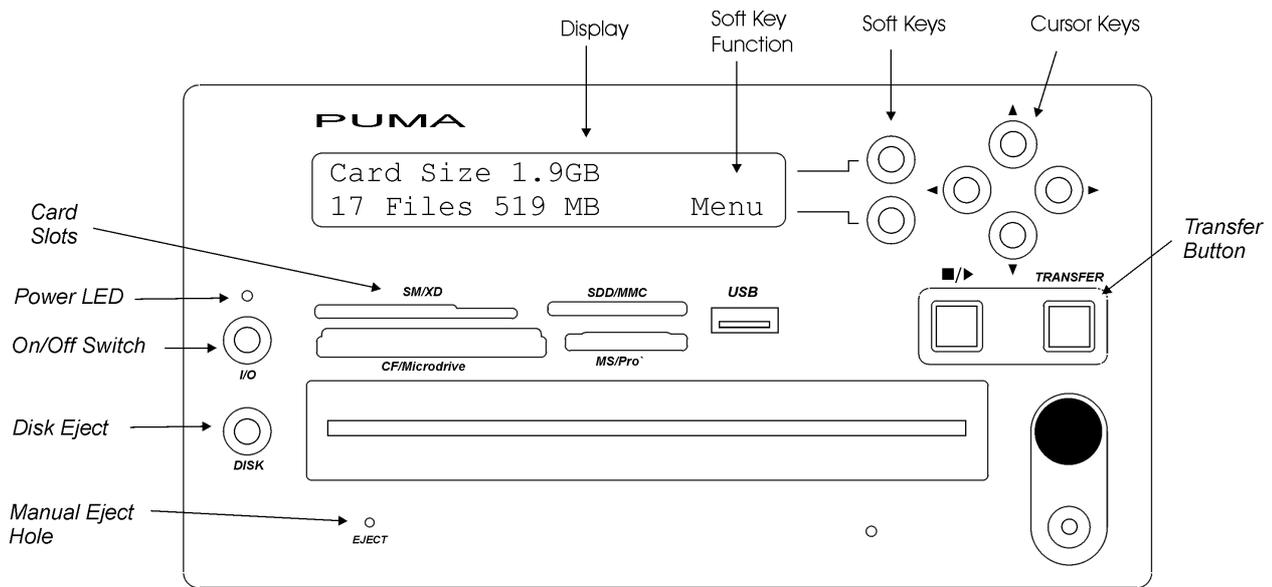


Fig 1. Front Panel

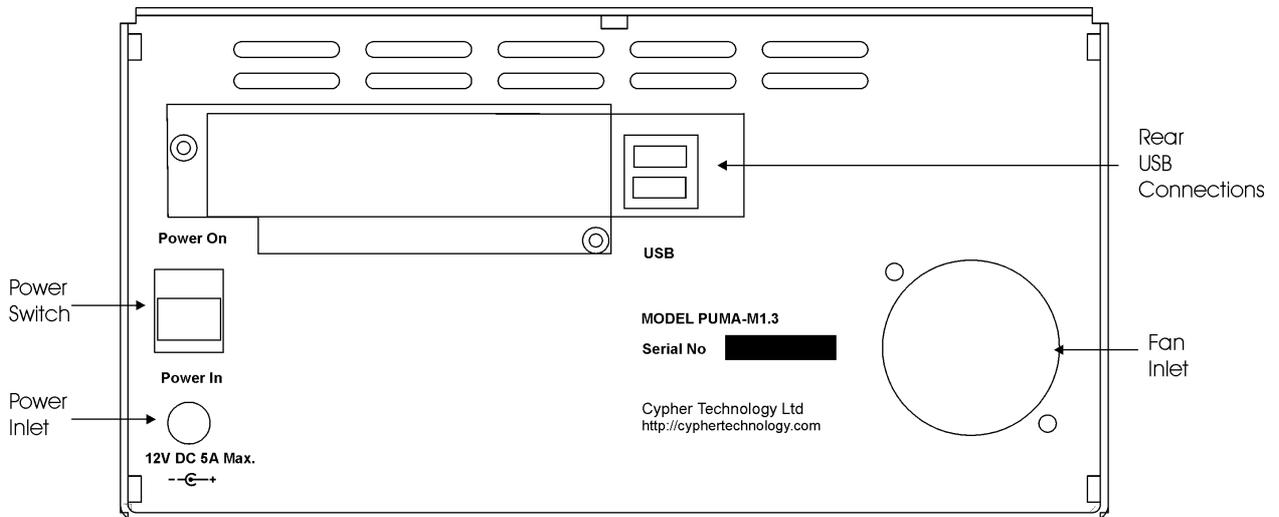


Fig 2. Rear Panel

2 Quick Start Guide

2.1 Making Master and Working Copies

1. Turn on switch on rear panel and when fully powered, after about 20 seconds, check that the displayed time and date on PUMA screen are correct.
2. If using a Working hard drive, connect this drive. Disk free space will be displayed. If not already designated, the Working hard drive will need to be created (See Utilities menu).
3. Insert the flash card into the appropriate front panel slot or a USB stick. or recording device may be plugged into one of the USB sockets on the rear panel or front panel. The PUMA display will show the size of the device and number of files.
4. Press the eject button on the DVD/Blu-ray drive to eject the disk tray. Place a BD⁽¹⁾, DVD or CD in the tray. For the Dual Drive version, press the eject button on the external drive and place a blank disk of the same size on the tray and close the drawer.
5. Press the TRANSFER button to start the transfer.
 - a) A Master copy is produced first. This consists of the transfer of the data from the card to the disk and a verification read pass. On successful completion the Master disk will be ejected and the checksum of the flash card and disk will be shown. This can be noted down for future reference. Where multiple disks are needed, follow the on-screen instructions and note down the separate disk checksums as well as the final checksum for the card and whole backup.

Single Drive:

- b) Remove the Master Copy disk and place a new disk on the tray. Press the lower soft key marked "Continue" to proceed. The Working copy is now produced. On successful completion the disk(s) will be automatically ejected.

Dual Drive:

- b) The Working copy will be ejected from the external drive at the same time as the Master. Remove the Master and Working Copy disks.
- c) The flash card or USB device may now be wiped and re-formatted. Press "N" when prompted if this is NOT required.

External Working Drive:

The files on the card will be copied to the Working Hard Disk.

6. The Transfer is now complete.

Note: If further copies are required, do not wipe the card and use the appropriate functions available in the "Menu". Press "Menu" soft key and the Up/Down cursor keys.

2.2 Turning Off

Press the I/O button below the green LED to shutdown. When "Switch Off" is displayed, turn off the rear panel Power Switch.

3 Detailed Operation

3.1 Setting up and Powering PUMA

Using in a vehicle. PUMA requires a regulated 12V power supply. If PUMA is to be used in a vehicle, please use the 12V stabiliser available from your supplier or Cypher Technology Ltd, NOT the vehicle power direct.

1. Remove any flash card.
2. Switch on the Power Switch on the rear panel (switch up).
3. After about 25 seconds the PUMA program will start and the system is ready for use.
4. PUMA has various settings that control the format of the Master and Working disks. These are saved after any changes are made and will normally not require further attention. Normally a "Compact Master" is used and a "File Copy" working disks. These settings can be inspected and changed in the Settings sub-menu.
5. Check that the displayed time and date are correct. If not, use the "Adjust Time" menu function to adjust the time and date (Section 3.9.5).

3.2 Making Evidential backup of Flash Card or USB stick

PUMA has an automated process for making an evidential archive of a flash card or USB storage device. This process is initiated by pressing the [Transfer] key. The Transfer consists of the sequence: Make Master, Verify Master, Make Working Copy, and then Wipe and format the storage device.

1. If using a Working Hard Disk, plug this in now. If this is not suitably formatted this must be done first. See Section 3.10.2. When recognised, PUMA will display the free space on the drive. Note: multiple Working copies can be made to the Working hard drive.
2. Place the flash card in the appropriate slot. If a USB drive or USB connected recorder is to be archived, plug this into either of the USB slots in the rear panel or the slot in the front panel (M1.3 on only).
3. Place a blank CD-R or DVD +/- R or BD-R⁽¹⁾ in the drive. The Master is generated first. The size of the flash card is shown on the display when it is inserted. A CD will hold 730MB a standard DVD 4,700 MB and a Blu-ray 25GB - 100GB. Where the data size is larger than the disk size, multiple disks will be produced. These disks will be automatically numbered as Master Disk #1, Master Disk #2 etc. The Master Copy has a log file which contains the time and date stamp of the backup as shown on the display on the front of the machine as well as other meta data. *Dual Drive mode only: place a blank disk of the same size as the Master in the external writer and close the tray.*
4. Press the Transfer button. The automated transfer and verify process begins. During the transfer the whole of the card is scanned, not just the file data. The display shows the % done and an estimate of time to go. (The "Cancel" soft key allows the transfer to be aborted)

5. When complete, PUMA ejects the verified Master Disk and displays the 8 digit Checksum. This Checksum should be noted down.

(Multiple disk transfer - If the data size is bigger than the disk size, further disks will be requested. Each disk has its own checksum, which is displayed at the end of each disk transfer. When all the data has been transferred, no new disks will be requested. Press {Continue} and the checksum of the whole Master Image will be shown. This should also be noted down. This final checksum is the same as the checksum produced for the card.)

If the process was not successful, the disk(s) will not be ejected and an error message will be displayed and the user will be prompted to re-burn that disk.

6. PUMA makes a Working copy after the Master is complete. This Working copy can be on optical media (CD, DVD etc) or to an external hard disk. Simply connect a Working hard drive and the Working copy will automatically go to this drive. If not connected, PUMA then prompts for another blank disk to be inserted for the Working Copy. If the size of the files on the flash card is bigger than the disk size, further disks will be requested. *Dual Drive mode only: the Working copy will be made on the external writer, (providing a blank disk has been inserted at the same time as the blank Master disk).*
7. If the whole Transfer process completed successfully the user will be prompted to wipe the Flash card or USB device:

Press {Y} to wipe flash card or {N} to proceed without wiping card. After the card is wiped it is automatically partitioned and re-formatted with a FAT32 file system.

The Transfer process is now complete. A new flash card may be inserted.

3.3 Turning Off

It is good practice to remove any flash cards or USB sticks from PUMA before powering down.

Press the I/O button below the green LED to shutdown. Press {Y} to confirm. When "Switch Off" is displayed, turn off the rear panel Power Switch.

If {N} is pressed the Software Revision and Serial Number (where appropriate) will be displayed and PUMA will resume operation.

3.4 Checking for External Drive and PUMA Status Information

Press the I/O button below the green LED to shutdown. If {N} is then pressed the Screen will show if an external drive is connected and also then show the Software Revision and Serial Number (where appropriate) and PUMA will resume operation.

3.5 Using SoundByte with PUMA

SoundByte audio recorders can be used with PUMA from Version 2.8.14 and will create Master and Working disks containing industry-standard, 32 bit IEEE wav files.

Simply plug in the SoundByte Recorder via a USB lead (or plug in the SD card from a SoundByte where it can be removed). The PUMA will recognise the SoundByte and show the number of Takes.

All functions will work as normal and the SoundByte can be wiped after the creation of the Master and Working copies.

3.6 Menu System

3.6.1 To Select a Menu Item

Press the {Menu} soft key to enter the Menu system. The Up/down arrow keys are used to select the desired function. Press the [Go] soft key to execute the function.

Pressing the {Exit} soft key returns to the top level.

The Menu is arranged as follows:

3.6.2 Main Menu List

Menu Item	Description
1 Working File Copy	Creates Working Copy disk from inserted card or device
2 Encrypted Copy	Creates password protected copy to DVD/CD
3 Make Master Copy	Creates Master of Flash card or USB drive to DVD/CD
4 Hard Disk Master	Makes a File Master of a Flash card or USB drive to another USB hard drive
5 Disk to Disk	Sub menu for disk to disk copying
6 Wipe Card	Overwrites flash card with "0"s and formats card
7 Format Card	Formats card as FAT32
8 Adjust Time	Adjusts PUMA internal time and date
9 Settings	Enters Settings sub menu
10 Utilities	Enters Utilities menu

3.6.3 Disk to Disk Sub-menu List (Dual Drive Only)

Disk Copy	External drive disk copied to internal drive disk
Encrypted Disk Copy	External disk copied to encrypted copy on internal drive
Working from Master	Makes Working Copy on internal drive from Master disk

3.6.4 Settings Sub-menu List

Set Master Type	Sets the format of the main Evidential Master
Set Working Type	Sets the format of the Working Copy
Enable JPEGs	Allows Jpeg creation on the Working Copy
Adjust Time	Adjusts PUMA internal time and date

3.6.5 Utilities Sub-menu List

Make Video DVD	Makes DVD or Blu-ray disk of video files
Make Working HD	Labels a FAT32 USB hard drive as a Working Drive

Verify Master	Verifies flash card against Master Copy
Restore Master	Creates clone flash card from Master Copy disk
Checksum Card	Calculates checksum of card
Checksum Master	Calculates checksum of data on Master Copy
Install Software	Install new software from DVD/CD

3.7 Main Menu Items

3.7.1 Make Working Copy (make simple file copy)

This is function will create a Working Copy from the flash card or USB stick. Normally all files are copied, including hidden and system files. Other Working Copy formats can be selected in the Settings sub-menu. By connecting a USB Working Hard Drive, the working copy can be made on the external drive. This drive needs to be labelled as a Working Hard Drive, so that PUMA can recognise the drive (See Utilities menu). Several Working Copies can be made to the same drive and the destination drive will be automatically recognised after its labelling and first use.

3.7.2 Make Encrypted Copy

This is an optional feature. It is used to make an AES 256 encrypted and password protected copy of the files on the flash card. PUMA will automatically generate a pseudo-random high security 14 character password. It is highly recommended that this be used for security reasons. Alternatively a password may be entered using the cursor keys. The [<],[>] keys select the character position and the [up],[down] keys select the character value. Press the {Use} softkey when the correct password is shown AND it has been noted down.

To Decrypt Files on the Encrypted Disk

A Decrypter program is copied automatically to the encrypted disk. To access the encrypted files, insert the disk into a Windows XP or later PC. The encrypted files can be seen in the "Files" folder. These files can be copied in the normal way but cannot be accessed until decrypted.

To decrypt, double click on the Decrypter icon in the top-level of the CD or DVD. Select the file or files to be decrypted using the Decrypter browser. When the selection is complete, click the Decrypt button. You will be prompted for the password and then to select a destination folder into which to copy the decrypted files. If the password is correct the files will be decrypted.

3.7.3 Make Master Copy

This function will create a Master Disk fro the flash card or USB stick. The PUMA Master contains all the data from the flash card on a write-once optical disk.

3.7.4 Hard Disk Master

This function creates a File Master copy of a large hard disk (or flash card or USB drive) on a second, empty hard drive.

All files are copied along with a log file that contains the MD5 hash codes of all the files so that the transferred material can be verified for added protection. It does not scan

unused areas of the drive and therefore should normally only be used where a full bit for bit Master is not required. The HD Master can also be used where it is impractical to create a standard PUMA Master and where, therefore, this could be regarded as “best practice”

First connect the empty backup drive to one of the USB ports on PUMA (in the top level of the Menu). The display should show the size of the disk and 0 files. If it shows any files or says “No file system” then the drive should be formatted using the Menu “Format card” option. After the format, exit the Menu and check that the display is now showing 0 files.

Then press {Menu} and scroll down to “Make HD Master”. Connect the source evidential drive and press and {Go}. The destination drive is automatically chosen as the empty drive.

Several backups can be made to the same drive and the destination drive will be automatically recognised after its first use.

3.7.5 Disk to Disk

Opens sub menu for all disk to disk copy functions (dual drive PUMAs only)

3.7.6 Wipe Flash Card

This function will perform a forensic wipe of the flash card. No data will be recoverable from the card after this operation (see below).

This function writes “0”s to the card. After the card is wiped, it is formatted as FAT32 and is ready for use.

3.7.7 Format Flash card

This function first overwrites the Master Boot Record of the card with binary “0”s thereby removing any boot sector viruses. It then re-partitions the card with a single primary partition of the maximum size and then formats this with a FAT32 file system. Note this function does not wipe the data area of the card. The Wipe card function must be used if this is required. See Section 3.7.6.

When complete “Formatted” is displayed.

3.7.8 Adjust the Internal Time and Date

This function allows the internal real-time clock to be adjusted. This clock is used to time and date stamp the Master.

The time and date is displayed in the top line of the display. E.g.

```
Adjust Time display           15:03:21 Tue Jan  9 2007  
                               Sel <> Adj Up Dn  Exit>
```

The hours number will flash and the [Up] and [Down] cursor keys can be used to adjust the value. The [<] and [>] cursor keys can be used to select other fields. When the correct time and date has been displayed, press the {Exit} soft key to exit back to the Menu list.

3.8 Disk to Disk Sub-menu

3.8.1 Disk Copy

Copies UDF or ISO disk (CD, DVD or Blu-ray) in the external drive to a blank disk in the internal drive. The external disk should be of the same or greater size than the source. This can be used to make further Working Copies from an existing Working Copy.

3.8.2 Encrypted Disk Copy

Copies UDF or ISO disk (CD, DVD or Blu-ray) in the external drive to a blank disk in the internal drive. The files are AES 256 encrypted. PUMA will generate a pseudo random password or the user may enter their own. This must be noted down as it is used for decryption. The external disk should be of the same or greater size than the source.

A decrypter application is copied to the disk and the disk is accessed on a Windows PC by entering the password into the application.

3.8.3 Working from Master

This function allows a Working Copy to be generated from a Master disk. This is useful where the original flash card is no longer available. The external disk should be of the same or greater size than the source.

3.9 Settings Sub-menu

3.9.1 Navigation and Settings

Use the Up/down cursor keys to select an item

Use Press the {Change} soft key or Up/down cursor keys to change the option.

Press the {Exit} soft key to save any changes and return to the Settings sub-menu.

3.9.2 Set Master Disk Type

This function sets the disk format for the Master. The options are Compact Master, Full Master or Quick Master.

Normally a Compact Master is generated. This copies all data from the flash card and includes the files, deleted files, the file system, partition information and all historical file data. As such it provides the most secure, evidential backup and allows the most complete evidential audit trail. It contains everything that was on the flash card and as such can be used to generate a clone of the original card.

A Quick Master only copies the files and is not so evidentially secure as a Compact Master but can be used where a Compact Master cannot be generated.

3.9.3 Set Working Disk Type

The Working copy is normally a file copy of the flash card. If the DVD authoring option is installed, the Working Copy can be configured to be a Video DVD instead.

3.9.4 Enable JPEG creation on Working Copies

This function will turn on the automatic creation of JPEG files on Working Copy disks. This will slow down the creation of the Working Copy where RAW image files are present.

3.9.5 Adjust the Internal Time and Date

This function allows the internal real-time clock to be adjusted. See above for explanation.

3.10 Utilities Sub-menu

3.10.1 Make Video DVD

This is an optional feature. It is used to make a standard PAL or NTSC video DVD of MPEG-2 files on the flash card. The card is automatically searched for “*.mpg” and the selection of NTSC or PAL is automatic. NOTE: the MPEG-2 files must be of a DVD compatible type. Supported formats are shown in the Appendix.

3.10.2 Make Working HD

This function creates a magic file on a connected external USB hard drive which designates the drive as a Working Hard Drive. When PUMA sees this drive is connected, all file Working copies will be made to the Working USB Drive and not to the optical drive. The Working drive must be formatted as FAT32 for PUMA to recognise the disk. If PUMA does not recognise the file system (reports “No file system” when the drive is connected), the drive must be formatted to FAT32. This can be done on PUMA. See Section 3.7.7

3.10.3 Verify Master Copy against Flash Card

This function will check that the contents of the inserted Master Disk are identical to the inserted flash card.

Where a multi-disk set has been produced, any numbered disk may be checked individually.

3.10.4 Verify Multi-Disk Master Set

To verify a Master disk set (i.e. all the disks in a multi-disk Master), the procedure is different for a Full and Compact Master

Full Master: Insert Disk #1 first, then 2, 3, 4 etc.

Compact Master: Insert LAST disk first and then feed disks in reverse order. So if there are 4 disks in the set, disk #4 first then 3, 2 and 1.

3.10.5 Restore the Master Copy to a Flash Card

This function will copy the contents of the inserted Master disk to the inserted flash card. This flash card will become a precise clone of the original card. Where the card is bigger than the original card, the excess data on the card will be zeroed.

Use a flash card that is the same size or bigger than the original.

When completed the checksum of the flash card (and the disk) is displayed. This card is functionally identical to the original. It may be inserted back into the camera or may be read on a computer and the images viewed or the files accessed.

3.10.6 Restore Multi-Disk Master Set

As above, use a flash card that is the same size or bigger than the original.

To restore a Master disk set (i.e. more than one disk for a particular flash card), the procedure is different for a Full and Compact Master

Use a flash card that is the same size or bigger than the original.

Full Master: Insert Disk #1 first, then 2 a3, 4 etc.

Compact Master: Insert LAST disk first and then feed disks in reverse order. So if there are 4 disks in the set, disk #4 first then 3, 2, 1.

3.10.7 Calculate the Checksum of the Flash Card

This function will generate a unique number from the contents of the flash card. This is called a checksum (see below). This number provides a useful and secure identification for the card and the Master Copy. The checksum of the card will be the same as the checksum of the Master image file for that card or the same as the sum of the checksums for the individual disks for a multi-disk set (modulo 32 bit).

3.10.8 Calculate the Checksum of the Master Disk Image

This function will generate a unique number from the contents of the inserted Master disk. This is called a checksum (see below). This number provides a useful and secure identification for the Master and the flash card.

Place the Master disk in the DVD drive and press the {Go} soft key to execute the function. When complete the checksum is displayed.

Where a multi-disk back up set has been produced, the checksum of the whole set can be found by starting with disk 1 in the set and following the on screen instructions.

3.10.9 Software Installation Procedure

This function installs new versions of the operating software. It is accessed from the Menu as function 14. The procedure from a “cold” start is as follows:

1. Boot up PUMA.
2. Press the {Menu} soft key to enter the menu.
3. Press the [Down Arrow] key until “Install Software” appears.

Either:

Press the [Disk] button to eject tray.

Place an upgrade disk on the tray and press [Disk] button once more to load the disk. The disk will take a few seconds to be recognised. Please wait.

Or:

Plug in a USB drive to the rear panel of the PUMA. This should have the install file and the data files copied to the root directory of the drive as described in the download instructions.

5. Press the {Go} soft key to start the software upgrade. The installation progress will be shown on the screen. **DO NOT SWITCH OFF DURING THIS PROCESS OR THE SYSTEM MAY BE UNUSABLE.**
6. When complete the system will display “Installation complete” or it will restart the new version of the program.
7. Switch off and reboot.
8. Check the Version number (displayed at boot up) is the same as that labelled on the Install CD or DVD.

4 Technical Background

4.1 PUMA Master Copy (bit for bit copy)

The PUMA Master Copy stores all the all of the data on the flash card and is therefore evidentially equivalent to the original flash card. Because the whole of the card is copied, the Master includes hidden files, deleted files, historical file data fragments, original “time-accessed” and “time-modified” data. Also the filing system (FAT), and the boot sector and partition information are stored.

The PUMA Master disk is finalised, which means no subsequent data modification can occur. This contrasts with personal computers which can leave disks sessions closed (so that they can be read on other computers) but, crucially, not finalised. For example, disks cannot be finalised with standard Windows 10 tools. Disks produced by PCs can therefore be edited and modified.

As such PUMA provides the most secure, evidential backup and allows the most complete evidential audit trail. It contains everything that was on the flash card.

UK courts have ruled that such a finalised disk Master is a Master for evidential purposes within UK courts and the original volatile media need not be kept and bagged but can be wiped and re-used.

There are two formats for the Master

4.1.1 Full Image Master

“*Full Image*”. This is the format originally used within PUMA. The Full Image Master contains a single file called “flash.img” which is a bit for bit copy of the whole of the flash card. It is the same size (in Kbytes) as the flash card. The flash.img file has its time created, modified and accessed values set to the time of the start of the transfer. This time is taken from the system time as displayed on the front panel of the machine at start-up.

When the flash card is bigger than the disk size, multiple disks are needed and each disk will contain part of the image. The first disk will contain a file called flash1.img , the second disk, flash2.img etc. These part images may be combined to form a single, complete image file.

The Master Copy can be used in two ways. On a PC with an Image Viewer program or by restoring the image back to a flash card or USB disk.

4.1.2 Compact Master

The “Compact” format was introduced in V2.2 and has two advantages over the Full Image Master:

- Files may be accessed directly in the Files folder
- Blank portions of the card are compacted: a wiped card, with only a few MBs of files creates a Master of only a few MBs.

4.1.3 Quick Master

A quick Master is used when it is not practicable to make a Compact Master. A Quick Master is simple file copy of the data on the evidential media (Flash card etc). It is not a bit for bit copy and does not copy forensic data such as deleted files and the file system. A clone of the original card cannot be made from a Quick master with the Restore function.

The guiding principal is to make the best evidential copy you can under the circumstances.

4.1.4 The Compact Master process

First the files are copied from the flash card into the "Files" folder on the Master disk. Having copied all the files, PUMA then scans the unused portion of the card (i.e.the area of the card not used by the files) and copies any meta data, deleted files or file fragments to the Master. This data is stored in Image files named Image_data0.dat, Image_data1.dat etc in the "AuxData" directory on the Master. An "Image_data.xml" file is also created in the AuxData directory and this records where the data in the files was stored on the flash card. This allows the original card to be precisely cloned during the Restore or Checksum processes.

A checksum is produced at the end of the disk creation. This is the checksum of all the data (files and any meta data) on that disk.

If the files and meta data are greater than the disk capacity, PUMA will prompt for further disks. These The checksum of each intermediate disk is displayed after each disk has been verified. When the Master set is complete, a further checksum is displayed, which is the sum of the individual disk checksums. This checksum is the same as the checksum of the flash card, as it is produced from the same data.

The Files folder may be accessed from a computer file browser in the usual way. Third party data recovery tools can be used on the Image files to, for example, recover JPEG images. Alternatively, the Master may be restored back to a storage device (flash card or USB drive) which is the same size or bigger than the original card. Standard data recovery techniques can then be used on this restored drive as they would on the original card.

4.1.5 Why archive the file system?

The file system used on removable flash media is the FAT file system.

A file is a digital container for digital data. As an example, one digital still image is normally stored in one file. The file has a name and this is how it is referenced and accessed by the computer and the user (e.g. DSC_0001.JPG).

A file entry on the disk or flash card is used to link this name with a FAT entry and hence, the position of the file data on the medium. The file entry also contains other information about the file such the time and date when the file was created and last modified.

4.1.6 Partition Table

Sometimes it is useful to divide one physical disk (e.g. a hard disk) into multiple, virtual drives (c: drive, e: drive etc.). A partition table describes how the drive is divided into different virtual disks. Flash cards and USB pen drives are normally partitioned but with only one partition, but can have more when the user wishes to hide information.

Note: Windows only sees the first partition on removable drives. So data on other partitions will not be seen or copied on a Windows PC . PUMA will copy all data from all partitions.

The partition table is not normally updated after it is created, but the way the partition table is written will vary from system to system and thus can give some knowledge of the history of the card.

4.1.7 File allocation information

Most flash media cards use the FAT16 or FAT32 file system. When a file (e.g. a JPEG picture file in a camera) is created, two things happen. Firstly the file data is written to the data area of the card and secondly the file system entry is created. This entry consists of a file information (name, date etc) and the location of the file data on the flash card stored in the File Allocation Table (FAT).

4.1.8 File un-deletion

When a file is deleted the actual file data is normally left unchanged on the storage device. The deletion involves marking the file name in the file entry to show that the file is no longer required and that the data space that was being used by the file can be used for new files. Because of this, if no further data is written to the card, the original deleted file may be retrieved or “un-deleted”. The Master allows for un-deletion of files where it was possible on the flash card. (See “How is the Master Copy used?” above). The Working Copy, of course, will not contain deleted files.

4.1.9 Historical file data

When a file is copied from the flash card to another storage device (as with the Working Copy) information about its creation may be lost. Most obviously this may include the original modification and creation times from the flash file table but also more subtle historical information may be lost relating to the media history.

4.1.10 Media history and fragmentation

When a file is created on a blank piece of media, the storage space is generally allocated from the beginning of the data area as continuous or contiguous space. Once several files have been created and then a few have been deleted “holes” appear on the file data area where the old file data resided. These holes will eventually be overwritten with new file data as new files are created, but because these new files may be of different sizes to the old files, one new file may have its data spread across the card at various locations. The more a flash card or drive is used, the more fragmented it becomes. This gives valuable information about the use of the media and the time of creation or modification of a file.

The Master Copy preserves all this information as it provides an exact snapshot of the state of the card when the copy is taken and because it leaves all the card data unchanged within the backup. The Master Copy is therefore the most complete evidential backup.

4.2 PUMA ancillary functions

4.2.1 Disk Verify Read

Most backup programs simply copy the data to the backup medium and assume it has been written correctly and can be re-read. With optical disks this is particularly dangerous. PUMA dramatically reduces the chance of producing unreadable disks by performing a verify read of the disk after it has been written. The verify pass itself, involves re-reading every data bit from the flash card and checking it against every bit on the Master.

4.2.2 Working Copy (file copy)

The Working Copy is a full copy of the directory tree of the flash card or USB drive. This means all files and directories are copied. Any file types can be copied. Hidden and system files are copied.

For the files on the flash card to be recognised by PUMA, the card must be formatted with a FAT file system.

The Working Copy disk uses an ISO9660 filing system and is recognised by most computing platforms. The system also implements the Joliet extension to the ISO 9660 standard which allows for long file names.

Where RAW image files are detected, PUMA can automatically convert them to a JPEG compressed image file with a compression ratio of about 7:1. The file has the same root name as the original, so that dcn0005.nef becomes dcn0005nef.jpg. For most picture content it will not be possible to readily observe any difference in quality between the JPEG and RAW images. This feature is disabled by default, but can be enabled in the Menu (see above).

A wide range of RAW file formats are supported and these are listed in the Appendix.

From V2.8.18 a Working file copy can be made to an external hard drive. See 3.7.1

4.2.3 Card and Disk Checksum

PUMA produces a 32 bit checksum of the flash card and Master Copy file. The checksum is a unique number derived from all the data on the card or from the whole image file on the Master. As such the checksum will always change if any data changes are made within the file or on the card. The Master and the card should always have the same checksum.

Where multiple disks are produced, the modulo 32 bit sum of the checksums of the individual disks are equal to checksum of the whole card. Note: this is not true for Compact Master disks pre V 2.6.34.

The chance of two flash cards, with different image data, having the same checksum is less than 1 in 4,000,000,000.

The checksum of a flash card or Master Copy can be found using the Menu functions (see above).

4.2.4 Flash Card Wipe (Erasing)

As mentioned above, when a file is deleted the file data remains on the medium. This file may be un-deleted and the file's data recovered. The only way to render the card

safe from data recovery is to re-write the whole card with new data. PUMA “Wipe Card” function writes binary zeros to the whole card. Also viruses may be present in the Master Boot Record (MBR). During the wipe process the MBR is overwritten also and is recreated during the format operation.

4.2.5 AES 256 Encryption

PUMA can make encrypted Working Copies (Option) and encrypted copies of CD, DVD and Blu-ray disks in UDF and ISO format (dual drive only). PUMA uses AES 256 as the encryption standard.

AES has three levels of security with 128, 192 and 256 bit keys. AES 256 is the most secure and the one used by PUMA. In 2003 AES 192 and above were deemed acceptable for documents classified as TOP SECRET by the NSA (US National Security Agency).

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.[12]

4.3 System Architecture

PUMA is based on a Linux platform and uses proprietary software. The proprietary nature of the software has allowed the transfer process to be tailored precisely to the needs of law enforcement and evidence gathering. For maximum reliability and security it contains no hard disk and boots from a read-only flash file system.

4.4 Transfer Times

PUMA uses a full height, high performance CD/DVD/BD⁽¹⁾writer. This type of drive provides transfer rates up to 20 Mbyte/sec compared with 8Mbyte/sec for laptop drives. Also, the larger size of the drive provides a higher reliability disk.

For reading, the maximum transfer rate (at the outside of the disk) is about 20 Mbytes/sec. A 4 Gbyte card can be copied in about 4 minutes.

4.5 RAW File handling

RAW to JPEG converter

The system incorporates a RAW image file format converter. This automatically detects the type of RAW file present and converts it to a standard JPEG image file which is added to the Working Copy along with the original RAW format file. The JPEG will typically be about 1/7th the size of the RAW file, and so will not add greatly to storage requirements. This software is maintained and new formats are supported as they arise.

The JPEG file will have the same root name as the RAW file. For example, if the RAW image file is D94L0948.DCR the JPEG will be D94L0948DCR.JPG.

5 Technical Support

5.1 System re-starting in the event of failure

Every effort has been made to allow PUMA cope gracefully with various fault conditions. It is possible, however, that the system will temporally lock-out. If the system does not respond during use (please wait for 3 minutes during a transfer), then the system should be powered down by switching off at the rear panel. Remove the flash card and re-start the system. The disk can only be ejected once the system is ready for use. In an emergency, when the system cannot be powered, the disk can be ejected by pushing with a blunt rod through the disk eject hole in the front panel.

5.2 Contact

In case any technical or user assistance is required please contact your distributor or Cypher Technology Limited,

5-7 Gravel Hill,

Leatherhead,

Surrey,

KT22 7HG

Tel +(44) 1372 375500

Fax +(44) 1372 378800

Email: mail@cyphertechnology.com

<https://www.cyphertechnology.com/>

5.3 Software Updates

The system can be updated with new application software when necessary. This software can be installed from CD or from a USB thumb drive. See section 3.10.9. Updates can be downloaded from:

<https://www.cyphertechnology.com/>

6 Specifications

Power	12 +- 0.4V dc 5A (max.) 1.5 A Idle.
Polarity	Centre pin +ve. 2.5mm connector
Supplied PSU	100-240Vac 1.5A 47-63 Hz
Card Types	Memory Stick, Memory Stick PRO, Microdrive, MultiMediaCard, SD Memory Card, SmartMedia Card, Memory Stick Duo, Memory Stick PRO Duo, CompactFlash Card, USB memory stick
Card Size	Any Size
Disk Types	PUMA BD only : BD-R 25GB, BD-R DL 50GB. PUMA BDXL only : BDXL 100GB PUMA BD and standard PUMA: DVD +/-R 4.7 GB DVD +/- R DL 8.5GB CD -R
Disk Format	Working Copy and Full Image ISO9660 Compact Master UDF2.01 Encrypted Copy UDF 2.01 Video DVD UDF1.02
Transfer rate	BD-R, DVD +R/-R up to 20 Mbyte/sec
Software	Proprietary Linux. Solid state flash read only
Start-up time	M1.4 26 secs
Size:	190w x 100h x 202d mm
Weight	1.92Kg

Note: (1) Items apply to PUMA BD only
(2) Optional external vehicle power adapter

7 Disclaimer

Although every effort is made to ensure that the information contained in this manual is accurate, Cypher Technology Limited cannot be held responsible for any errors or omissions.

Cypher Technology Limited cannot be held responsible or liable for any loss either direct or indirect which results from use of the equipment described in this manual.