Media MASSter NVMe M.2 Pro IT

User's Guide

Intelligent Computer Solutions
2380 Shasta Way Suite E
Simi Valley, CA, 93065
U.S.A

PUB-00412
Rev. 4.5

Sales/Technical Support
Phone: (818) 998-5805

E-Mail: sales@icsiq.com

www.icsiq.com

CONTENTS

Chapter 1: Introduction

Overview

The Media MASSter™ NVMe M.2 Pro IT unit is an Economical, High Speed, M.2, SATA and USB 3.0 Handheld Data Acquisition Device, designed as a low cost solution without sacrificing performance and versatility. The Media MASSter™ NVMe Pro IT unit offers built-in NVMe M.2 support using a High-end Intel Processor and advanced High Speed 6Gb/s drive controller technology, providing high performance for IT Data Acquisition Operations. The unit can acquire data from one Source to four Target SATA drives at speeds over 20GB/min, and from one M.2 to three M.2 drives at speeds exceeding 50GB min. Speeds can exceed 90GB/min when acquiring data from 1 NVMe M.2 Source drive to 1 NVMe M.2 Target drive.

The MM NVME M.2 PRO unit's key features includes four M.2 slide-in securable slots, SATA cable-free source and target drive caddies, and is designed with a slide out system drive for easy removal. Acquire Source drive's data as a *Mirror* Acquisition or an *Intelligent* Acquisition which copies only allocated files, greatly reducing copy time while automatically scaling and formatting partitions. The units are also configured with a 1Gbit Ethernet port for Network Connectivity.

Features

- **High Speed Operation:**

M.2 Transfer rates can exceed 90GB/min.

- **Multiple Media Support:**

Provides Native support for M.2, SATA and USB drives.

- **Preview Source Drive's Data:**

View Source Drive's Data in a write-protected environment.

- **Multiple Hash Modes:**

Hash using SHA-1, SHA-2 (Hardware Accelerated), MD5, CRC32

- **Write Protection:**

Protect Source drive's data against accidental overwrites.

- **WipeOut:**

Sanitize drives using the User Defined mode or DoD standard.

- **Log Information:**

Store and print detail operational Event Log and Audit Trail information.

- **LCD Touch Screen Display:**

Large, 7" Color LCD Touch Screen Display.

About this User Guide

The *MM NVMe M.2 Pro* User Guide will be updated as needed to reflect hardware and software modifications. Therefore, descriptions of features may be subject to change. The document makes use of hyperlinks to provide shortcut links.

Typical Conventions Used

Convention	Meaning
Highlighted	This is a hyperlink: shortcut link to a referred topic. Select it to jump to the topic. Use the MS Word **Back**  tool to jump back to previous location or <Alt + left-arrow> in Adobe Reader.
Bold	Indicates a screen menu item or function such as a setting or control button.
Italic	Indicates the name of an MM NVMe M.2 Pro feature, system, mode, or other important reference.
Note	Identifies additional important information regarding a topic or task.
	Indicates a warning or caution

Setup

1. Carefully remove the MM NVMe M.2 Pro unit from its shipping box.
2. Use the supplied parts list (Table 1) to complete an inventory check.
3. Follow the outlined steps in the Quick Start Setup Chapter.

Part	Part Number	Quantity
MM NVMe M.2 Pro Unit	F.GR-0160-400	1
DC Power Supply Adapter	CSAR-0418-000A	1
USB-to-SATA Adapter	CBM-00323	1
Stylus	CSAR-0130-000A	1
Restore Media - USB Thumb Drive	CSAR-0352-000A	1
MM NVMe M.2 Pro User's Guide	DOC-0156-000A	1

Quick-Reference Parts List
Table 1

System Specifications

Supply Voltage	100 - 240V / 50 - 60 Hz 180Watt Universal Auto switching input voltage
Power Consumption	30W
Operating Temperature	5 degrees - 55 degrees C
Relative Humidity	20% - 60% non-condensing
Net Weight	4.5 lbs (2 kg)
Overall Dimensions	14.5" x 12" x 7" (L x W x H) (368mm x 305mm x 178mm)

Chapter 2: Quick Start Setup

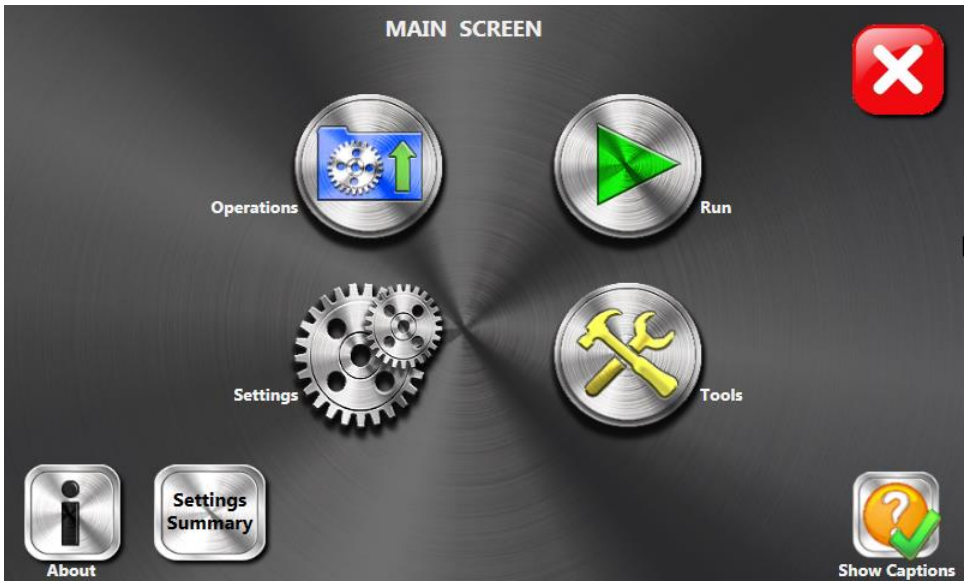
The following section describes the Quick Start procedure to start using the Single Capture mode with the default *Advanced Graphics* Interface.

1. Attach the unit's Power Adapter to the unit's Power-In port, located on the unit's right side I/O panel. The voltage may be either 110v or 220v. The Power Adapter will automatically switch to use either voltage.

2. Confirm that the unit is powered off.
3. Aligned the M.2 drive's key notch with the unit's M.2 connector's notch and connect the M.2 drives in the S1-M.2 Source location, and the T1-M.2, T2-M.2 and T3.M.2 Target locations. Secure the M.2 drives using the M.2 Slider Latch.

4. Power ON the unit by pressing the unit's Power ON button. The *MM NVMe M.2 Advanced Graphics Interface* will be displayed.

   NOTE: Refer to the section titled *MM NVMe M.2 Advanced Graphic Symbol Description* for a description of the *MM NVMe M.2 Pro Advance Graphic Control Buttons*.

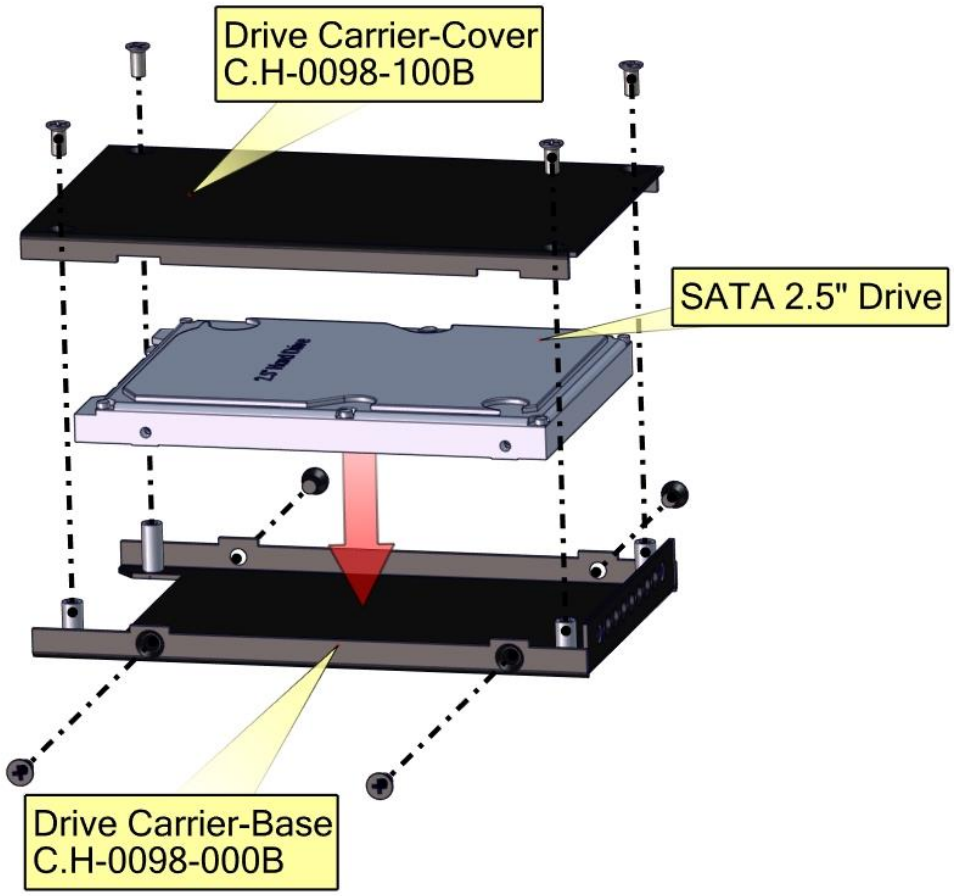


5. For 2.5” SATA drives, connect the drives using the *2.5” Drive Carrier*.
   a. Place the drive onto the *Drive Carrier Base*.

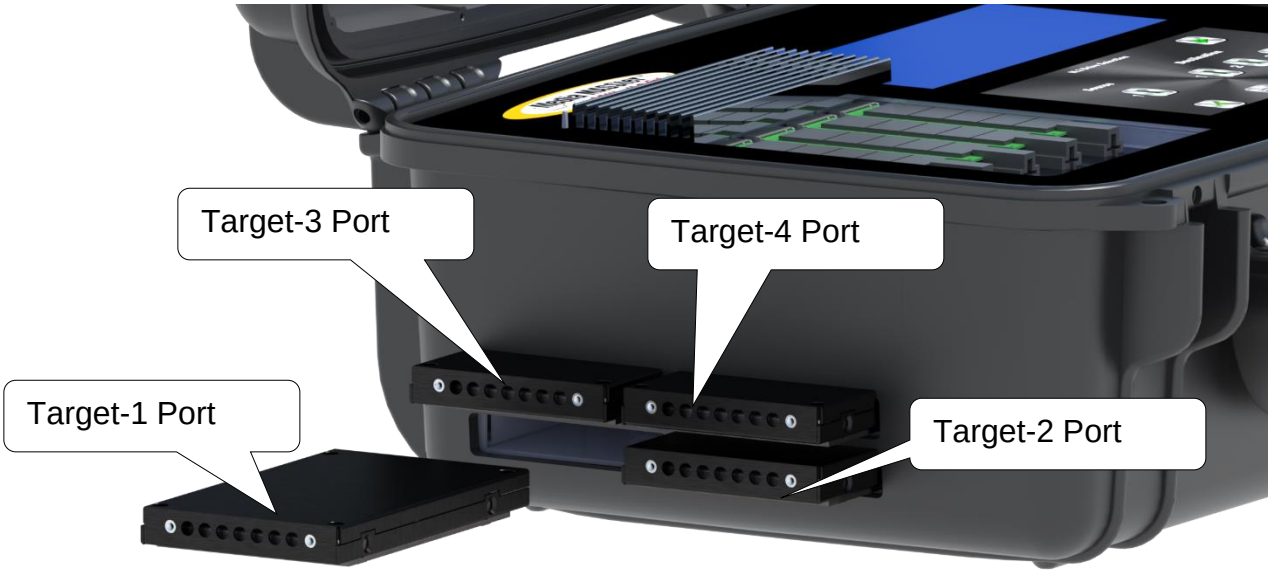
      NOTE: It is not necessary to secure the drive(s) using the supplied screws or the *Drive Carrier Cover*. It would only be recommended to secure the drive(s) if the drives will be transported with the unit.

   b. Insert the *2.5” Drive Carrier* into the unit’s Source and Target ports. Insert the *Drive Carrier* until it mates with its internal connector.

      NOTE: The *Drive Carrier* will extend out from the unit as shown below. Do not use extensive force when inserting and mating the modules.



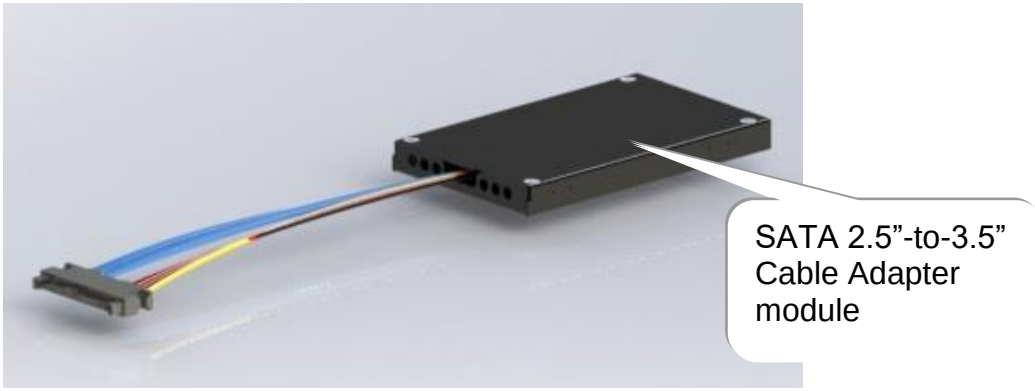
2.5” Drive Carrier



2.5” Drive Port Positions

6. For 3.5” SATA drives, connect the drives using the optional SATA 2.5”-to-3.5” Cable Adapter modules.
   a. Insert the SATA 2.5”-to-3.5” Cable Adapter modules into the unit’s Source and Target ports. Insert the module until it mates with its internal connector.
   b. Connect the 3.5” SATA drive to the cable connector side of the SATA 2.5”-to-3.5” Cable Adapter module.

   NOTE: The modules will extend out from the unit as shown below. Do not use extensive force when inserting and mating the modules. If the unit is powered on prior to connecting drives, power is applied to the drives when connected.

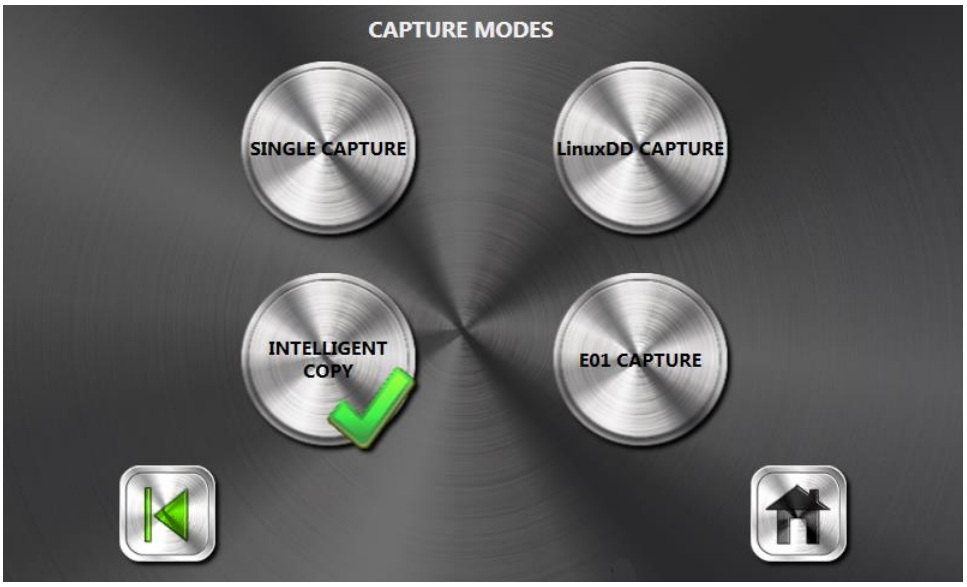


7. Select *Operations*  from the Main Screen to access the Operation Category Menu selection.

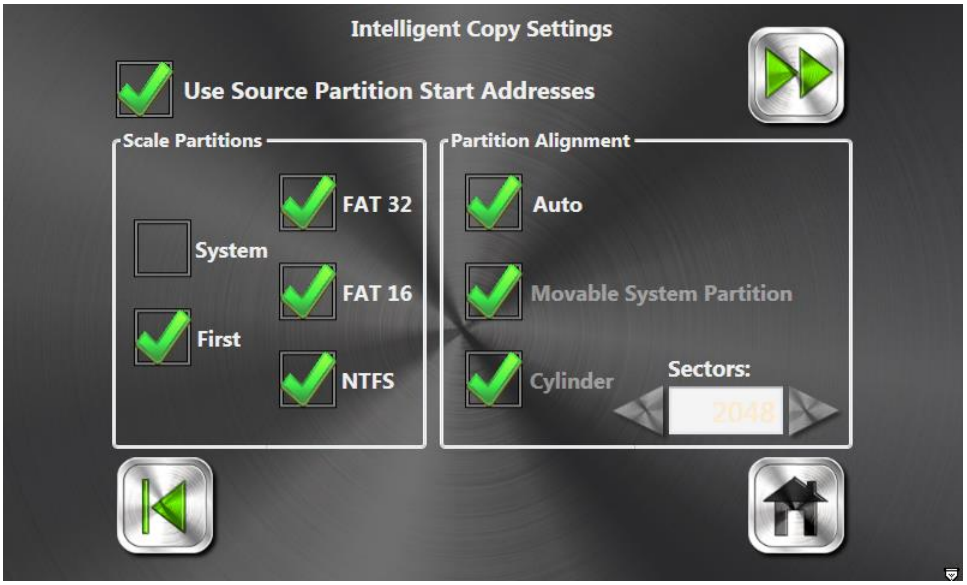
8. Select *Capture*  from the Operation Category screen to access the Capture Mode Menu Selection.

7. Select *Intelligent Copy* to access the *Intelligent Copy* Settings Menu.

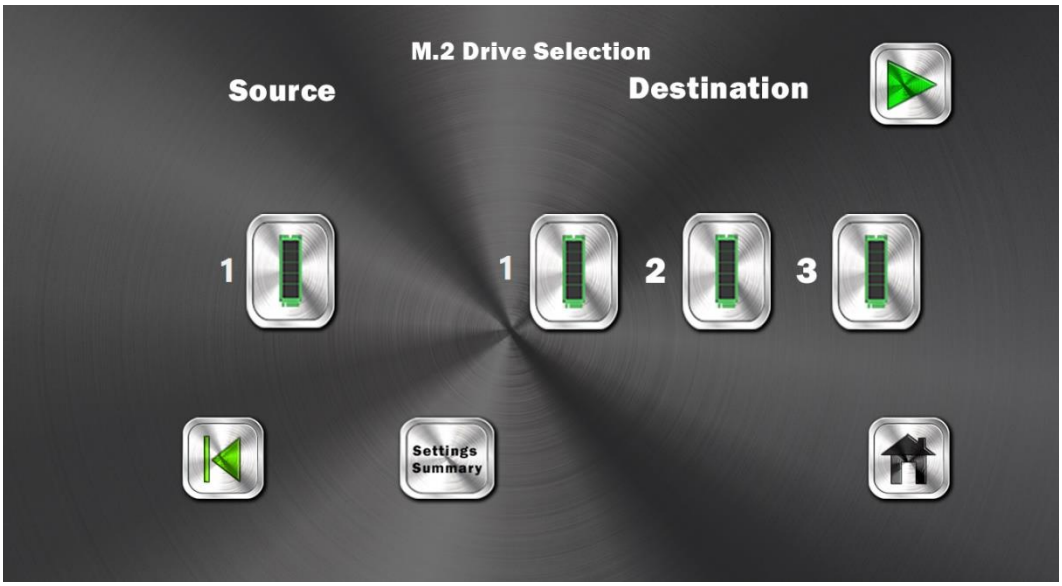
   Note: If the Source drive is configured with an O/S that is not Windows based, select *Single Capture* and following the steps outlined in the section titled *Mirroring Drives using Single Capture Mode*.



8. Set the *Intelligent Copy* Settings which are dynamically displayed in the Operation's Main Screen. See Table 3 for recommended settings.



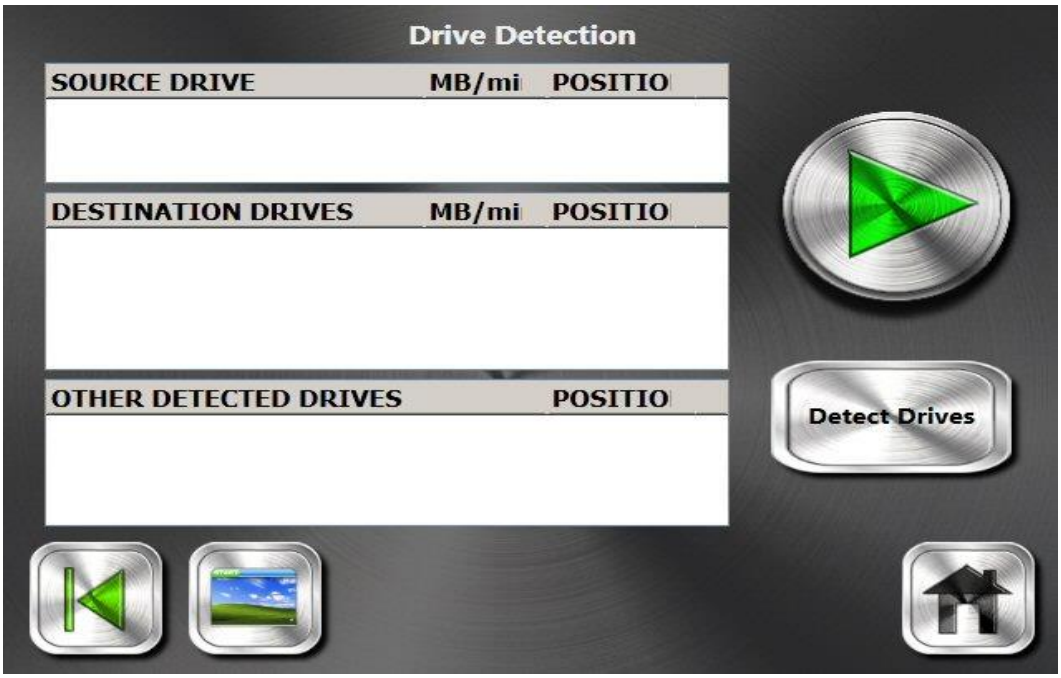
9. Select  to access the *M.2 Drive Selection* Screen and to select the drives to be used for the selected operation.



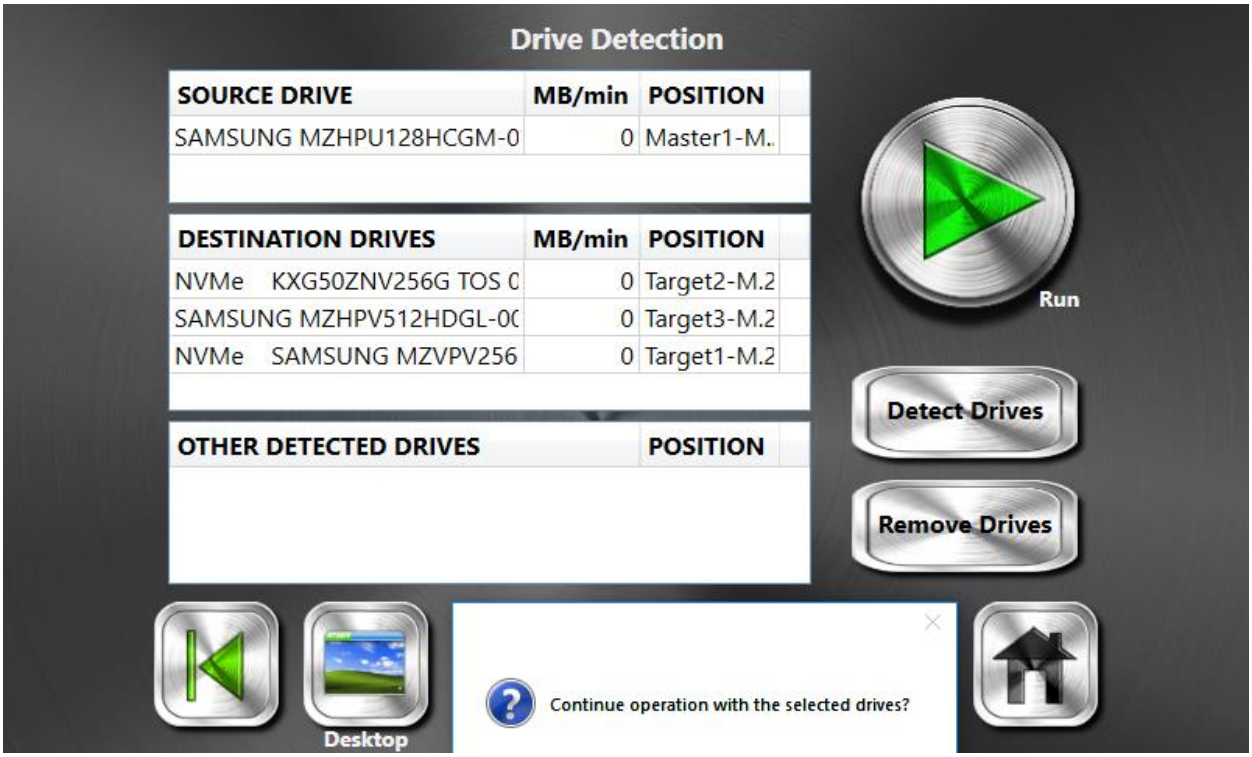
10. Select  to access the *SATA Drive Selection* Screen and to select the drives to be used for the selected operation.

The M.2 Source drive Data Transfer direction is from Left to Right. The SATA Source drive Data Transfer direction is Right to Left.

11. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.



12. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.



NOTE: If necessary, select "non-active" drive(s) listed in the *Other Detected Drives* panel and move them to either the *Source Drive* or *Destination Drives* panels. The drive(s) listed in the *Source Drive* or *Destination Drives* panels are considered "active" drives and will be used during data transfer operations. If necessary, also transfer "active" drives from the *Source Drive* or *Destination Drives* panel to the *Other Detected Drives* panel.

13. The *Run Screen* similar to the one shown below will be displayed indicating the status of the operation.

14. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. If M.2 drives are in use, it would be required to power off the unit prior to removing the drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

NOTE: Log files are automatically saved to the system drive and can be manually saved to an external USB drive connected to the unit's General Purpose USB port, using the LOGS function.

The unit can be powered OFF by pressing and releasing the unit's Power button, or by selecting *EXIT* from the Main menu.

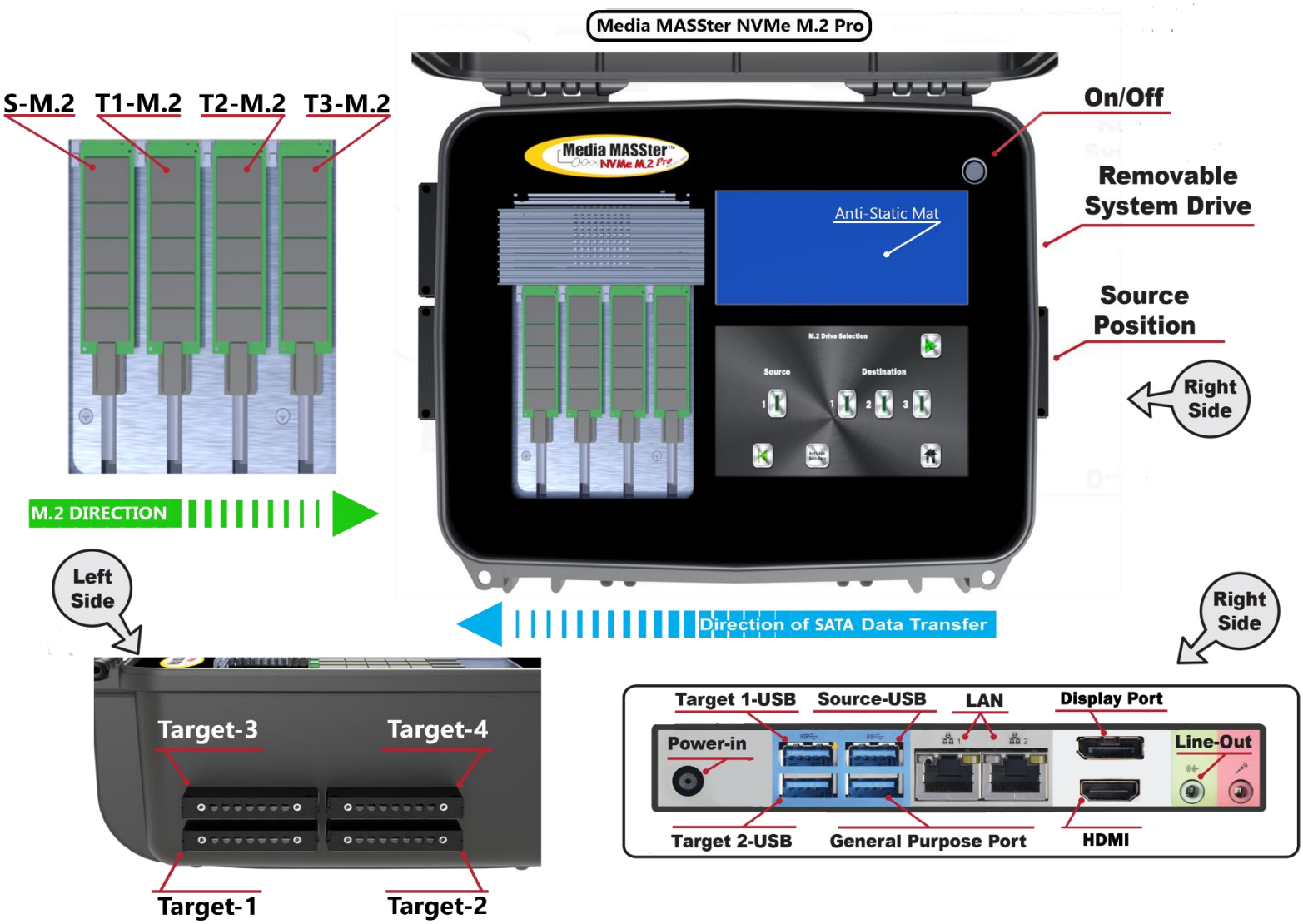
Chapter 3: Installation

Hardware Description

This section describes the hardware of the *MM NVMe M.2 Pro* unit.

Components and Functions

Top Panel (Fig. 1)	
Display	LCD Touch Screen Color Display.
Four M.2 Ports:	Provides native support for 4 PCIe M.2 drives.
Power ON Button	Used to power the unit ON and OFF.
Right Panel (Fig. 1)	
SATA Drive Source Port	Used to connect the Source SATA drives directly to the unit for “Direct” data seizure operations.
USB 3.0 Source, Target-1, Target-2 Ports	Used to connect the USB 2.0/3.0 Source and Target device(s) directly to the unit for “Direct” data seizure operations.
DC-IN Power Socket	Connect DC Power Adapter to this socket.
USB 3.0 General Purpose Ports	Provides 1 General Purpose USB v2.0/3.0 port for USB Mouse or Keyboard.
LAN Port	Provides a GBit Ethernet Network Interface.
L-in, MIC	Provides Audio Line Input and Microphone ports.
HDMI Port	Used to connect to an external monitor.
System Drive Port	Used by the removable System drive.
Left Side Panel (Fig.1)	
SATA Target-1 through Target-4 Drive Ports	Used to connect the Target SATA drives directly to the unit for “Direct” data seizure operations.



Layout View

Figure 1

Chapter 4: Operation

User Interface

The *MM NVMe M.2 Pro* provides a Windows based User Interface, which the user can use to setup and control the unit's various functions. All of the unit's menus and functions are controlled through the unit's Touch Screen Display. Screen menu items can be selected by touch or with use of the included Touch Screen Stylus Pen. An On-Screen Keyboard is available for an easy method to enter text related information. Optionally, an external keyboard, mouse or display can be connected. The *MM NVMe M.2* unit provides an *Advanced Interface* and an *Advanced Graphical Interface*. The *Advanced Graphics Interface* is a graphical, "button" driven interface and provides access to the unit's most common functions and settings. The *Advanced Interface* provides additional functions and settings that may not be available through the *Advanced Graphical Interface*. By default the unit's *Advanced Graphics Interface* will run at start up.

This chapter provides a detail description of the available functions.

MM NVMe M.2 Pro Advanced Graphics Interface

The *MM NVMe M.2 Pro Advanced Graphics Interface* provides the User with most common functions and controls necessary to quickly setup and use the MM NVMe M.2 Pro unit. The functional descriptions of the *Advanced Graphics Interface* are discussed in the following section.

Advanced Graphics Interface Control Functions

The following is a description of the *MM NVMe M.2 Pro Advanced Graphics Interface* Control Functions.

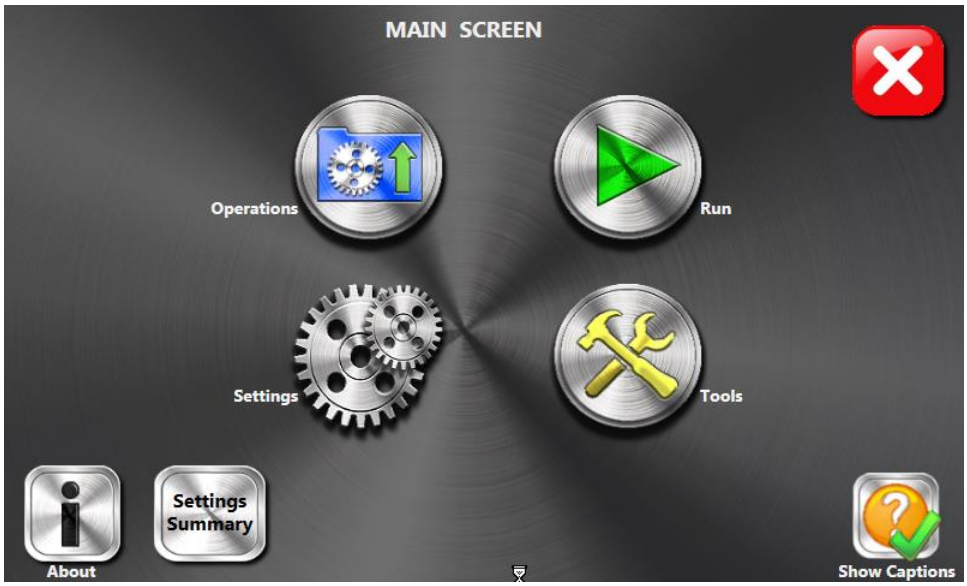
ICON	FUNCTION	DESCRIPTION
	Operational Mode Selection	Used to open the Operation Category Menu Selection Screen.
	Case Menu Selection	Used to open the Case Menu Screen.
	Settings Selection	Used to open the Settings Menu Screen.
	Tools Selection	Used to open the Tools Menu Screen.
	Run	Used to access the Drive Selection, Drive Detection or Run Menu Screens.
	About	Used to display the unit's Software Version and Serial Number.
	Capture Mode Selection	Used to open the Capture Mode Menu Selection Screen.
	Hash Only Mode Selection	Used to open the Hash Only Mode Menu Selection Screen.
	WipeOut Mode Selection	Used to open the Wipe Mode Menu Selection Screen.

	Restore Mode Selection	Used to open the Restore Mode Menu Selection Screen.
	Desktop Selection	Allows access to the Desktop or the Device Manager.
	Stop Selection	Used to Stop a selected operation.
	Home Selection	Used to return the Main Screen.
	Back Selection	Used to return to the previous Screen.
	Forward Selection	Used to quickly access the Drive Menu Selection Screen.
	HDD Selection	Used to select the HDD Drive position that will be used for a selected operation.
	USB Drive Selection	Used to select the USB Drive position that will be used for a selected operation.
	Add Network Location	Used to select a Shared Network Drive Folder that will be used for a selected operation.

Adv GUI - Main Menu

The *MM NVMe M.2 Pro Adv GUI Main* Screen provides access to all of the unit's main functions. The following functions are available from the *Main* Menu.

- Operational Mode
- Run
- Settings
- Tools
- About
- Settings Summary



MAIN MENU

Operational Mode

The *Operational Mode* Button provides the User with access to all of the available modes of Operation.

Run Mode Selection

The *Run Mode* Button provides the User with quick access to the *Drive Selection* Screen. It is usually selected to quickly begin an operation using previous settings.

Settings Mode Selection

The *Settings Mode* Button provides the User with access to the unit's General Settings.

Tools Mode Selection

The *Tools Mode* Button provides the User with access to the unit's Tools Functions.

About

Selecting About, displays information about the MM NVMe M.2 Pro unit, such as serial number and software version in use.

Settings Summary

Provides a list of the currently selected Operational Mode and associated Settings.

Adv GUI – Operational Category Menu

The *MM NVMe M.2 Pro Adv GUI Operational Category* Screen provides access to the unit's different modes of operation. The screen is accessed by selecting the *Operational Mode* Button from the Main Screen. The following selections are available.

- Capture Modes
- Hash Only Modes
- Wipe Modes
- Restore Modes
- Case

Capture Mode Selection

The *Capture Mode* Button provides the User with a selection of the available Capture Modes of Operation.

Hash Only Mode Selection

The *Hash Only Mode* Button provides the User with a selection of the available Hash Only Modes of Operation.

Wipe Mode Selection

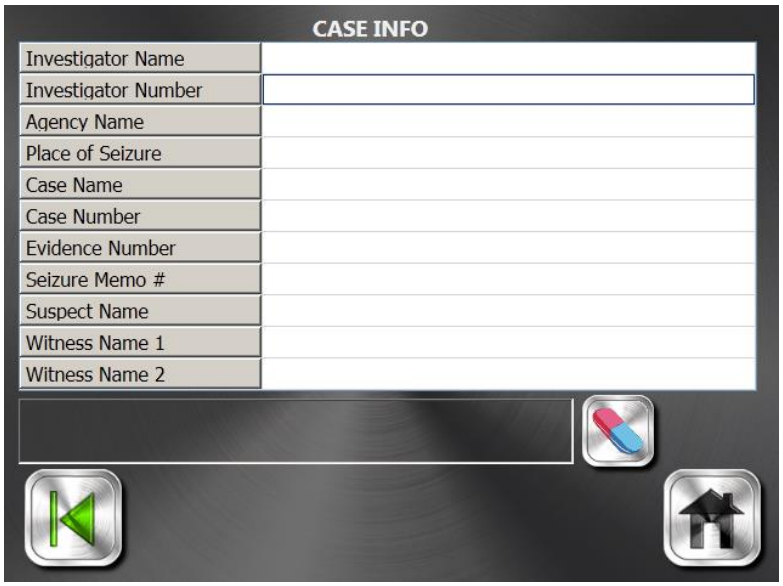
The *Wipe Mode* Button provides the User with a selection of the available Wipe Modes..

Restore Mode Selection

The *Restore Mode* Button provides the User with a selection of the available Restore Modes of Operation.

Case

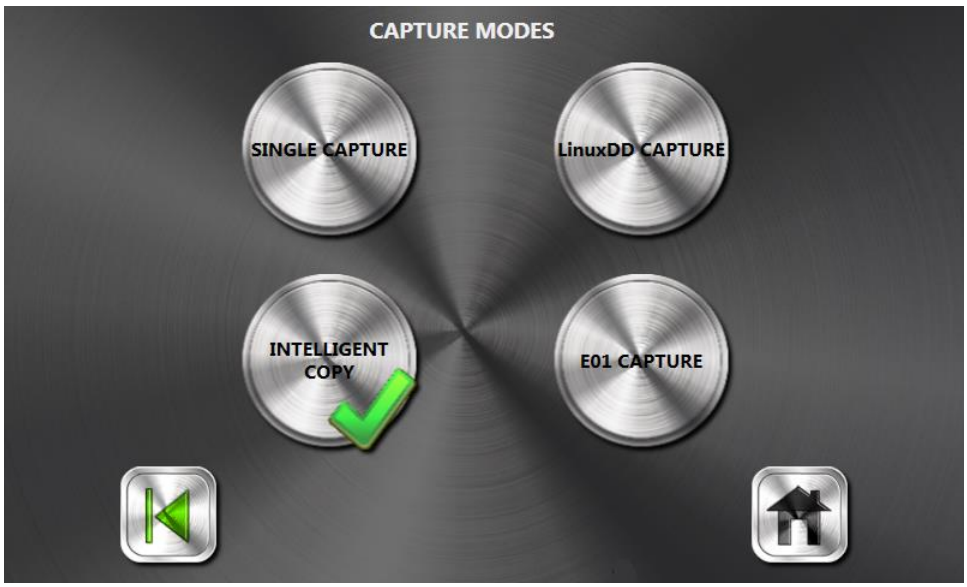
The *Case* Button provides the user with a list of specific Case Information to enter for the Capture Operation. This Case Information will be stored for Audit Trail output.



Adv GUI - Capture Menu

The *MM NVMe M.2 Pro Adv GUI Capture Mode* Screen provides access to the unit's different Capture modes of operation. The screen is accessed by selecting the *Capture Mode* Button from the *Operation Category* Screen. The following selections are available.

- Intelligent Copy
- Single Capture
- LinuxDD Capture
- E01 Capture (Not applicable for IT units.)



IQCopy

The *Intelligent Copy* operation provides an “intelligent” method of copying and scaling partitions. Only used clusters of known partition types are copied. This mode supports the FAT16, FAT32 and NTFS-file systems. All sectors of other partition types and sectors before the first partition are copied as well. This copy mode is the preferred method of copy when copying between different size drives. See *Intelligent Copy Settings* for more details.

Single Capture

The Single Capture operational mode will seize the entire contents of the Source drive to the Target drive. The operation will create an exact duplicate of all of the Source drive partitioned and un-partitioned areas as well as all used and unused sectors on the Source drive. The process of acquiring the data from the Source drive is methodical and contiguous, beginning from the first byte of the first sector on the drive, and ending on the last byte of the last sector of the drive. The data is copied to the corresponding sector on the Target drive. Only one seizure operation can be performed to the same Target drive. See Single Capture Settings for more details.

LinuxDD Capture

The LinuxDD Capture Mode will copy the entire contents of the Source drive to the Destination drives. The data will be written as individual segmented LinuxDD files and stored in an individual subdirectory on the Destination drive(s). The size of the individual LinuxDD files can be set by selecting a value within the Capture File Size pull down menu. The default setting is 650MB (CD). The File Name information entered by the user will be used as the name of the subdirectory where the Source LinuxDD files will be stored. This File Name will also be used as the filename of all LinuxDD files associated with this seizure. The Linux DD files will begin with the extension 000, and incremented by 1 for each additional file.

The Destination drive will be inspected prior to transferring data. The operation will verify if the first partition on the Target drive is based on the exFAT File System and will have “TARGET” as the volume label. A Destination drive that meets these criteria will be a valid Destination drive, a new subdirectory will be created, and the transfer will begin. A Destination drive that fails these criteria will cause the user to be prompted with a message asking whether or not to overwrite the current contents of the Destination drive in order to make it a valid LinuxDD Destination drive. The operation will abort unless the user agrees to overwrite the Destination drive.

Any number of “Loads” can be placed on the same Destination drive provided there is adequate space to save the transferred data on the Destination drive. See *LinuxDD Capture Settings* for more details.

E01 Capture

Not applicable for IT units.

Adv GUI - Restore Menu

The *MM NVMe M.2 Pro Adv GUI Restore Mode* Screen provides access to the unit's available Restore modes of operation. The screen is accessed by selecting the *Restore Mode* Button from the *Operation Category* Screen. The following selections are available.

- LinuxDD Restore
- E01 Restore (Not applicable for IT units.)

LinuxDD Restore

This function allows restoring the captured LinuxDD formatted Case to its original file format. This function requires the LinuxDD drive, containing the LinuxDD Case files, to be connected to one of the unit's Source positions and the "Destination" drive to be connected to the unit's Target position.

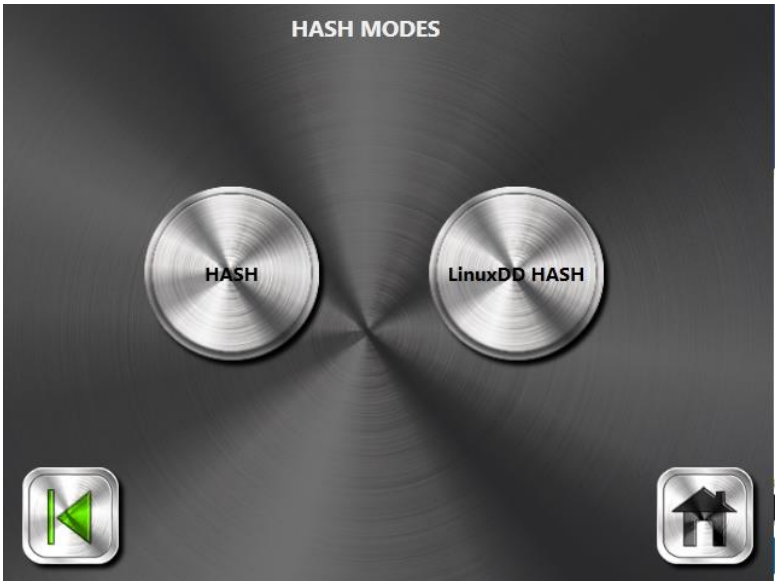
E01 Restore

Not applicable for IT units.

Adv GUI – Hash Only Menu

The *MM NVMe M.2 Pro Adv GUI Restore Mode* Screen provides access to the unit's available Hash Only modes of operation. The screen is accessed by selecting the *Hash Only Mode* Button from the *Operation Category* Screen. The following selections are available.

- LinuxDD Hash
- Hash



LinuxDD Hash

This function will generate a Hash value for the selected LinuxDD Case. The LinuxDD drive can be connected to either the Source or Target position.

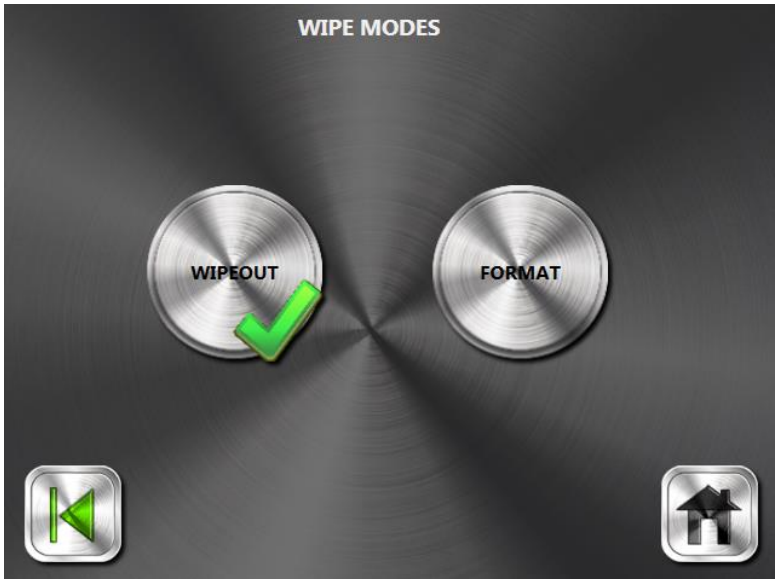
Hash

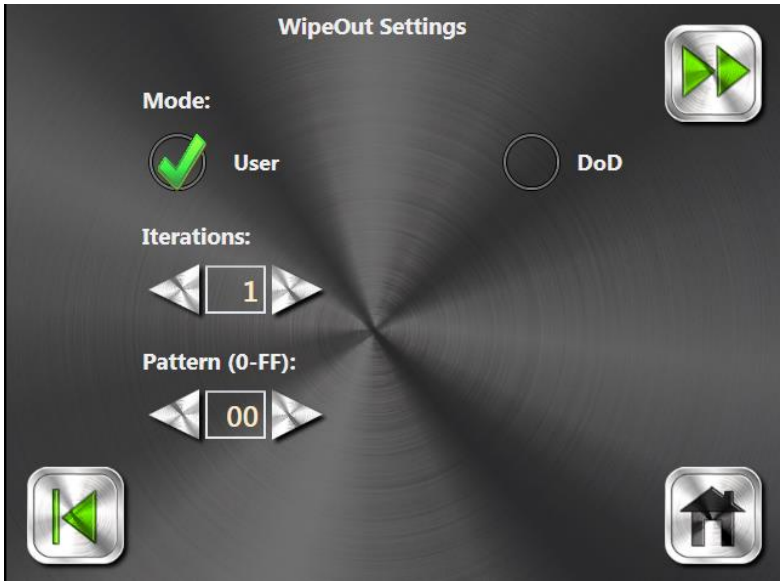
The ***Hash*** operation provides a method of generating a hash value for either the entire area of a drive or for a selected number of sectors of a drive. No data is written to the selected drives during this operation. When hashing the entire drive the process is methodical and contiguous, beginning with the first sector on the drive and ending with the last sector of the drive. See *Hash Settings* for more details.

Adv GUI – Wipe Menu

The *MM NVMe M.2 Pro Adv GUI Restore Mode* Screen provides access to the unit's available Wipe modes of operation. The screen is accessed by selecting the *WipeOut Mode* Button from the *Operation Category* Screen. The following selections are available.

- WipeOut-DoD
- WipeOut-Fast
- Format





WipeOut-DoD

The **WipeOut DoD** Operational mode provides a method of sanitizing a drive that meets the U.S. Department of Defense specification DOD 5220-22M for sanitizing drives. Using ordinary “DELETE” and “ERASE” commands, data on a hard drive remains accessible to a variety of intrusive procedures. The WipeOut DoD erasure technique provides a solution to this problem using a series of null-coded overwrites that completely removes all data from the hard drive. The process is performed in three iterations and two individual passes that completely over writes the drive connected to the internal drive position. Each iteration makes two write-passes over the entire drive. The first pass writes ONEs (Hex 0xFF) over the entire drive surface. The second pass writes ZEROes (Hex 0x00) over the entire drive surface. After the third iteration, a seventh pass writes the government designated code “246” (Hex 0xF6) across the entire drive surface, which is then followed by an eighth pass that inspects the drive with a Read-Verify review. See *Wipeout Settings* for more details.

WipeOut -Fast

The **Wipeout Fast** Operational mode provides a quick non-DoD method of sanitizing a drive of all previously stored data. The process involves writing a user defined hex pattern to the drive connected in the Target drive position, for a number of user defined iterations. The process is methodical and contiguous, beginning from the first byte of the first sector on the drive, and ending on the last byte of the last sector of the drive.

Format

This function can be used to quickly format drives and to prepare drives as exFAT LinuxDD Target drives. It may be necessary to manually transfer LinuxDD or E01 Target files from an NTFS based Target drive to an exFAT based Target drive. It also provides the function to quickly format drives using NTFS. Using the “Add Network Location” function to store images on a Large Volume RAID Storage device requires the device to be pre-formatted with NTFS or exFAT.

Adv GUI – Tools Menu

The *MM NVMe M.2 Pro Adv GUI Main* Screen provides access to the unit's Support functions. The screen is accessed by selecting the *Tools* Button from the *Main* Screen. The following Tool functions are available.

- Add/Remove Options
- Case
- Drive Port Assignment
- Logs
- Desktop

Add/Remove Options

The *Add/Remove Options* function allows adding or removing Software Options.

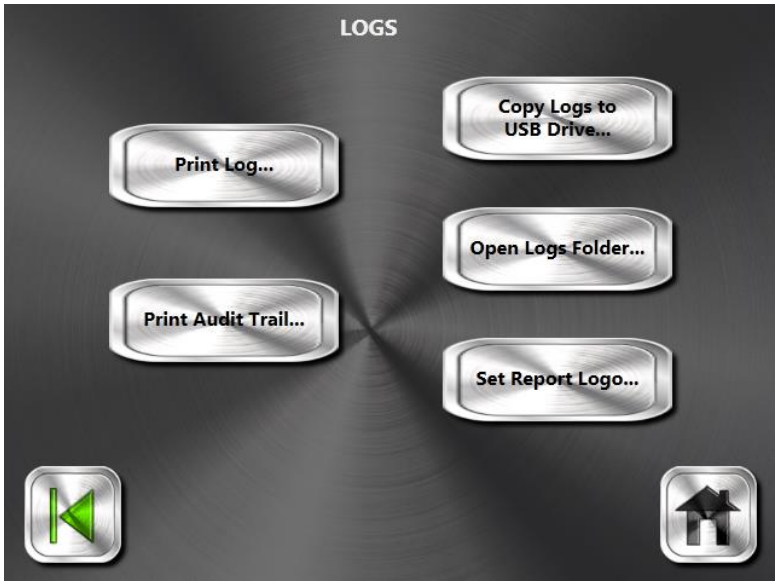
Desktop Tools

The *Desktop Tools* Option provides access to the unit's Desktop or to Device Manager.

Logs

The *Logs* Option provides the functions for viewing, transferring and printing Event Log and Audit information. Event Log and Audit files are automatically stored in the unit's local file folder. Files are stored using a DATE_TIME.TXT naming convention. The Audit Trail file will be referenced as such. The following Log functions are available:

- Print Logs
- Print Audit Trail
- Copy Logs
- Open Log Folder
- Set Report Logo



Print Logs

Provides the functions to print Event Log files and Audit Trail Log files to a connected printer.

Copy Logs

Provides the function to copy Event Log files and Audit Trail Log files to an external USB Drive. Audit Trails are saved in both a standard text format and a PDF format using 128-bit password encryption protection, so the Audit Trail contents cannot be changed.

Open Log Folder

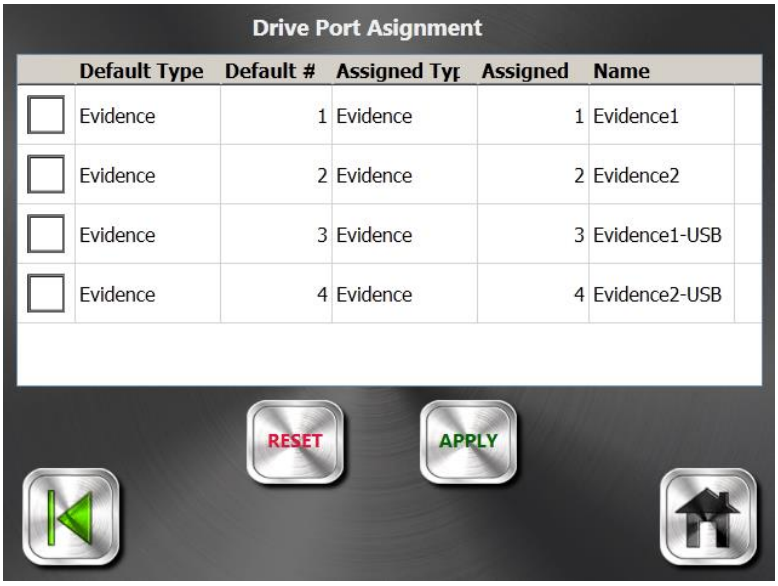
Provides access to the folder used to store the Log files, for viewing.

Set Audit Trail Logo

Provides the function to add a Company Logo onto the generated PDF Audit Trail.

Drive Port Assignment

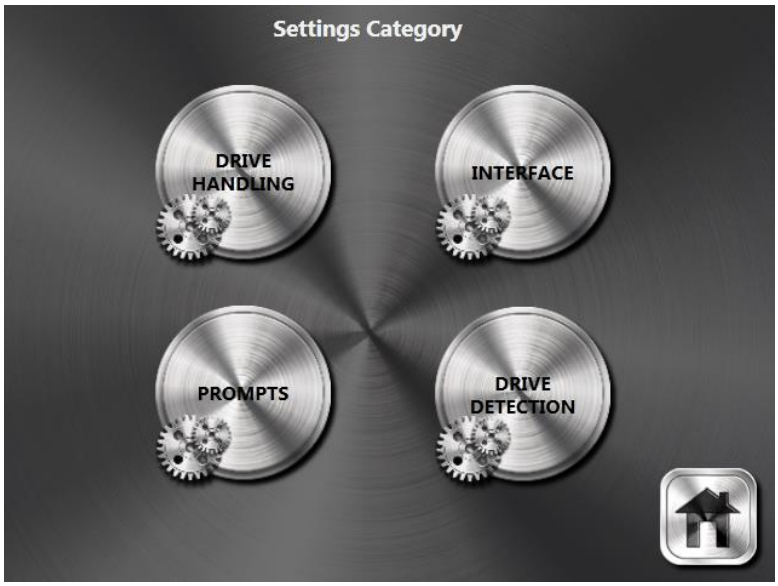
Opens the Drive Port Assignment Screen which can be used to reassign Target Ports with Source Port Write-Protect properties.



Adv GUI – Settings Menu

The *MM NVMe M.2 Pro Adv GUI Settings* Screen provides access to the unit's available User-Defined settings. The following Settings options are provided.

- Drive Handling
- Interface
- Prompts
- Drive Detection



Drive Handling

The *Drive Handling* menu provides data transfer and drive handling related settings. The screen is accessed by selecting the *Drive Handling* Button from the *Settings Category* Screen. The following *Drive Handling* Settings are provided.

- Bad Sector Handling
- Transfer Buffer Size
- Slow Drive Filter
- Read Back Verify
- Protected Area Support

- *Bad Sector Handling*

  This setting allows the user to select from a list of three methods of handling bad sectors when they are encountered on the source drive.

- *Skip Block*

  When enabled, the bad sector handling process time is reduced by skipping the entire transferred block in which the bad sector was encountered. Each transferred block is composed of 1280 sectors. When the block is skipped it results in writing '0's to Target drive's corresponding block. This process is significantly faster but would not capture any data that may exist in any of the good sectors of the block(s) containing bad sectors.

- *Skip Sector*

  The operation will log the location of the bad sector on the source drive and the bad sector will be skipped.

- *Abort drive*

  The operation will abort when encountering a bad sector on the source drive.

- *Transfer Buffer Size*

  The default setting of (10) instructs to operation to use a Transfer Buffer size of 640KB. In most cases a Transfer Buffer size of 640KB is optimal; however with some drive combinations it might be useful to change the value in order to achieve faster transfer rates.

- *Slow Drive Filter*

  Minimum transfer rate accepted before the drive is aborted. The decision to abort a drive is based on the individual drive speed and not on the average speed of the process. A value of 0 instructs the operation to ignore the Slow Drive Filter.

- *Read Back-Verify*

  Accessed from the Drive Handling Settings screen, this option provides additional data integrity checks during data transfers. When Read Back-Verify is selected, the operation will verify each block of data transferred during the data transfer process. Data written to the Target drive is read back and compared to the data read from the Source drive. Enabling this option results in reducing the transfer rate. Disabling this option will result in the data transfer process to make use of the drive's own Ultra DMA Mode error-detection handling mechanism known as cyclical redundancy checking (CRC-16) to check for Data Integrity. In most cases the CRC-16 error checking algorithm is sufficient. CRC is an algorithm that calculates an order and value sensitive checksum used to detect errors in a stream of data. Both the Source drive and the Target drives calculate a CRC value for each Ultra DMA burst. After the Source data is sent, the Target drive calculates a CRC value and this is compared to the original Source CRC value. If a difference is reported, the unit may be required to select a slower transfer mode and re-try the original request for data. The transfer rate will not be affected when using the drive’s CRC-16 mechanism for checking data integrity.

- *Protected Area Support*

  When selected, this function instructs the selected Operation to determine if a Source drive is configured with an HPA or DCO Area. If an HPA or DCO area exists on a Source drive, the Operation will copy all of drive’s data including the data stored in the drive’s HPA or DCO area.

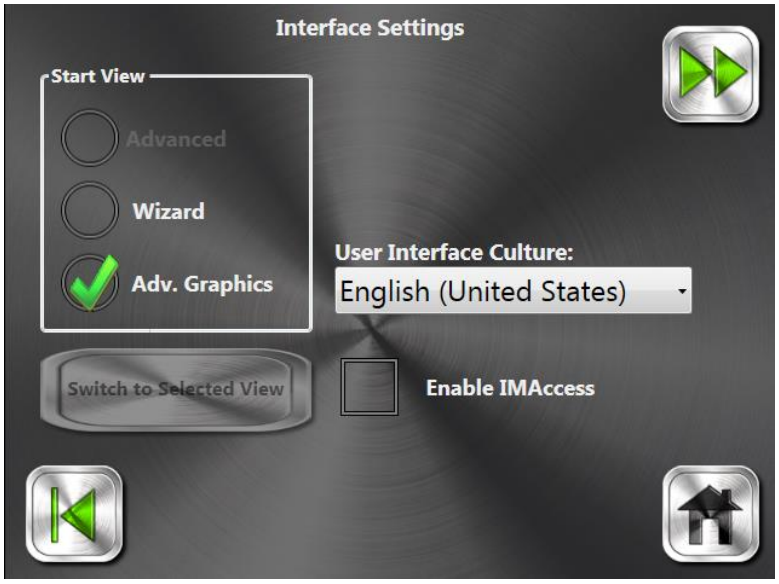
- *Set Target Protected Area*

  When enabled, this function instructs the operation to set the HPA or DCO Area of the Target drive if the Source drive is detected as having an HPA or DCO Area.

Interface Settings

The *Interface Settings* menu provides Interface usage options. The screen is accessed by selecting the *Interface Settings* Button from the *Settings Category* Screen. The following *Interface* Settings are provided.

- Start View
- User Interface Culture
- Enable IMAccess



- *Start View*

  The *Start View* menu provides optional Start Up Views.

- *User Interface Culture*[1]

  If the Language Options are activated, this function allows the user to select from a list of User Interface Languages.

- *Enable IMAccess*

  Allows 3rd Party application access to write-protected volumes for viewing purposes.

[1] Pending Development

Prompts

The *Prompt* menu provides the Operator with a method to enable or disable User Prompts. The screen is accessed by selecting the *Prompt* Button from the *Settings Category* Screen. The following *Prompt* Settings are provided.

- Confirm Drives
- Hash Advisory
- Drive Connection Advisory

- *Confirm Drives*

  Instructs the Operation to prompt the Operator and confirm if the detected Source and Target drives are the correct drives to use before starting the selected Operation. When the setting is disabled, the Operation will use the selected drives without prompting.

- *Hash Advisory*

  Prompts the User if the Hash options are not selected.

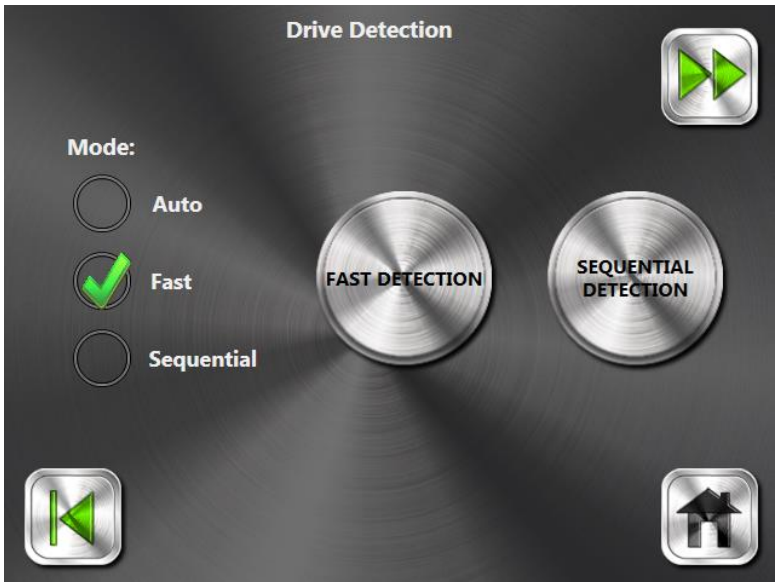
- *Drive Connection Advisory*

  Prompts the User if a selected drive's cable connection is faulty.

Drive Detection

The *Drive Detection* menu provides User-Defined settings to customize the unit's drive detect handling functions. The screen is accessed by selecting the *Drive Detection* Button from the *Settings Category* Screen. The following *Drive Detection* Settings are provided.

- Drive Detection Mode
- Sequential Detection
- Fast Detection



- *Drive Detection Mode*

  This setting allows the user to select from a list of three methods of handling bad sectors when they are encountered on the source drive.

  - Auto

    Automatically selects Drive Detection method based on the hardware detected. This mode will automatically select *Fast Detection* for the MM NVMe M.2 Pro systems.

  - Fast

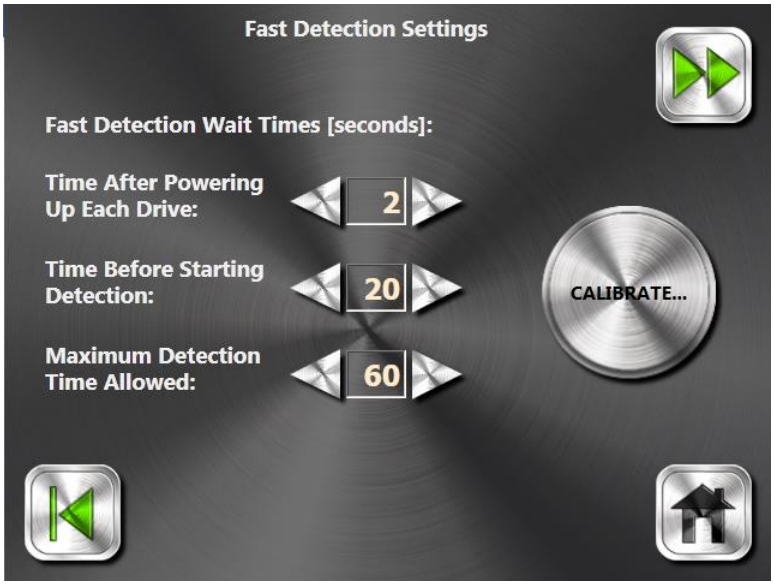
    Selects use of the *Fast Detection* method to detect drives. This method identifies the drive by the SATA controller's physical address location used by polling the drive. It is the quickest method to detect drives.

  - Sequential

    Selects the *Sequential Detection* method to detect drives. This method identifies the drive by sensing the drive's "current load" and then waiting for each individual drive to be detected before attempting to detect the next selected drive.

- *Fast Detection Settings*

  The *Fast Detection Settings* menu provides optional *Fast Detection* User-Defined settings.



- *Time After Powering Up Each Drive*

  This is the time allocated before powering Up the next selected drive. The default value is 2 seconds.

- *Time Before Starting Detection*

  This is the time allocated after powering Up each drive, and before checking the controller and O/S for detected drives. The default value is 20 seconds.

- *Maximum Detection Time Allowed*

  This is the time allocated for the O/S to detect “New Hardware” or discover each selected drive. The default value is 60 seconds.

  NOTE: Some drives may take longer to be discovered by the O/S. This setting limits the wait time.

- *Calibrate All Drive Positions*

  Used to restore the “map” which links the unit’s SATA controller’s physical addresses to the unit’s assigned drive positions, for all connected drives.

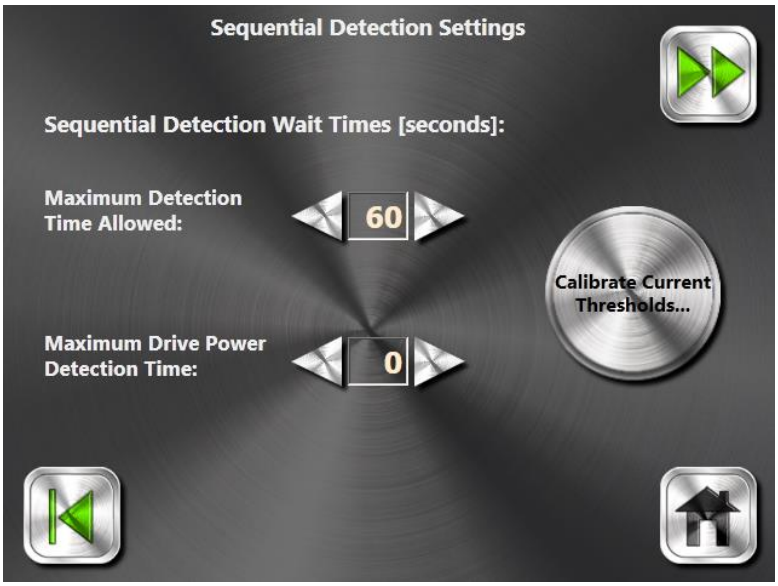
  NOTE: Calibration would only be necessary if the unit can no longer detect drives.

- *Calibrate Selected Drive Positions*

  The Calibration is performed for the selected drive position

- *Sequential Detection Settings*

  The *Sequential Detection Settings* menu provides optional *Sequential Detection* User-Defined settings.



- *Max Detect Time*

  This is the time allocated for the O/S to detect “New Hardware” or discover each selected drive. The default value is 60 seconds.

  NOTE: Some drives may take longer to be discovered by the O/S. This setting limits the wait time.

- *Max Detect Power Time*

  Maximum time allowed for the drive’s applied “current load” to be detected. After the set time, if the drive’s applied “current load” is not detected, the drive will be powered OFF.

- *Calibrate Current Threshold*

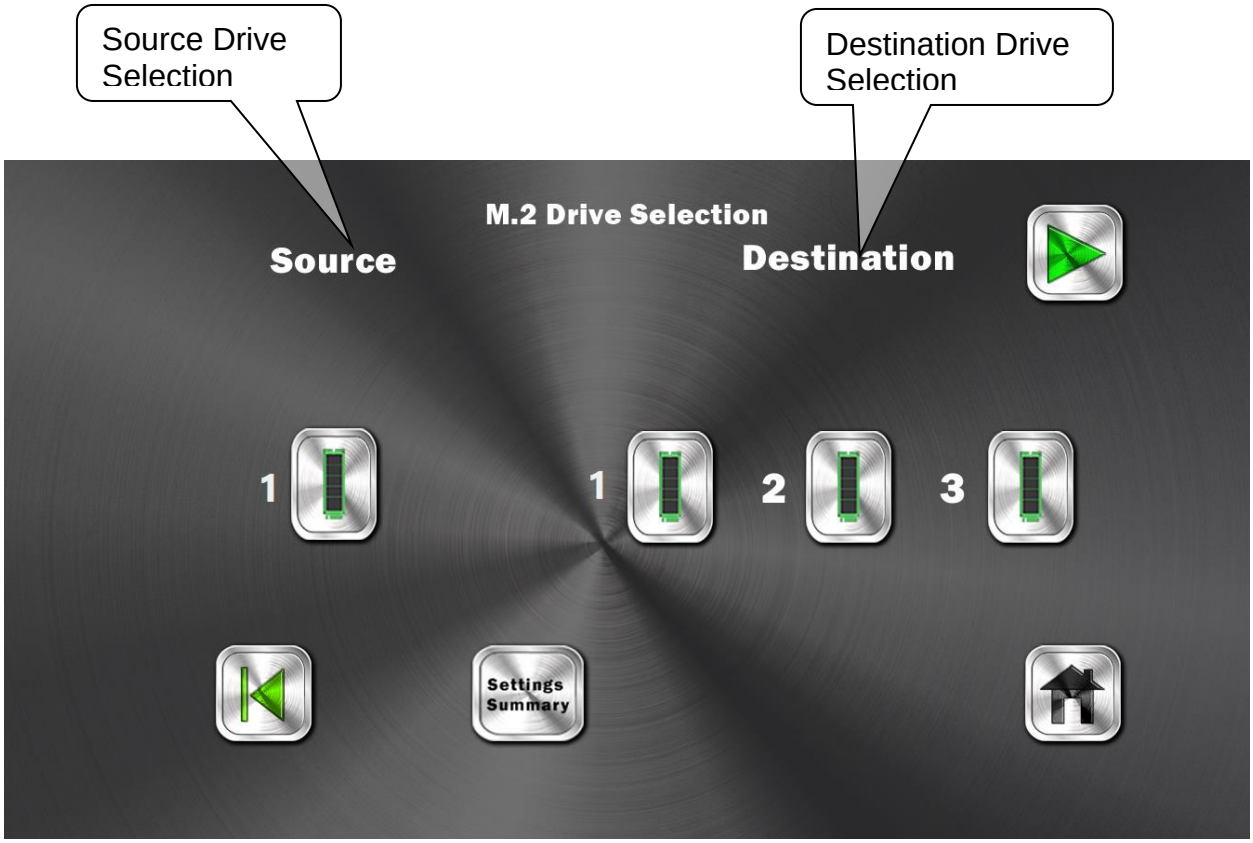
  The *Calibrate Current Threshold* function will measure the idle current used by the unit’s power control board. A current level measured that is greater than the Calibrated Current Threshold value will indicate that a device is connected.

  NOTE: Verify that NO drive is connected, while calibrating the current thresholds.

Adv GUI – Drive Selection Menu

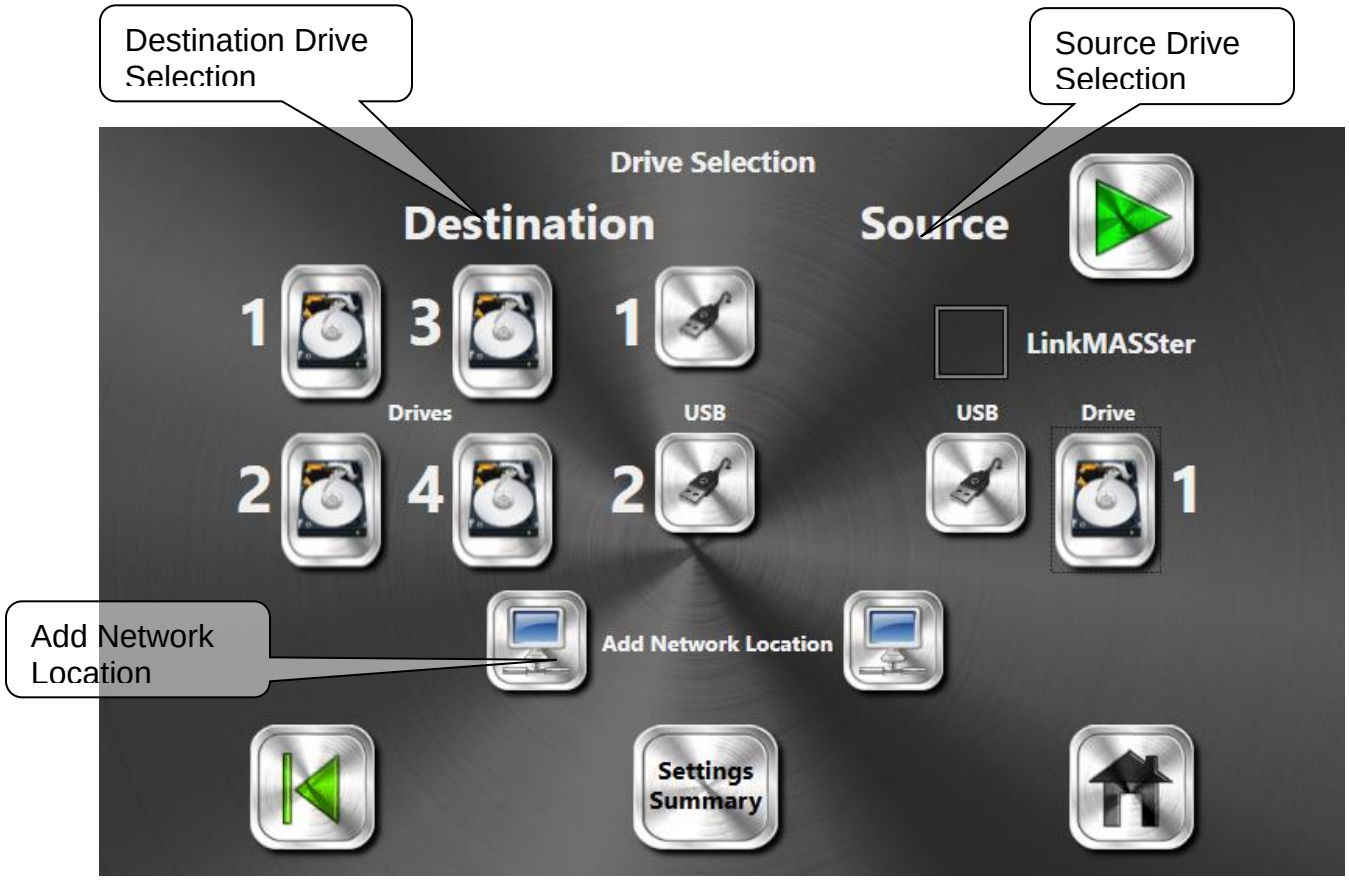
The *MM NVMe M.2 Pro Adv GUI Drive Selection* Screen provides the functions necessary to select the drives in use for the selected operation. A graphical representation of the Source and Target Drive Locations are provided. The screen is accessed by selecting the *Run* Button from the Main Menu or by selecting the *Fast Forward* Button. The following selections are available.

- Drive Select Buttons
- LinkMASSter
- Settings Summary
- Add Network Location



M.2 Drive Select Buttons

The *M.2 Drive Select Buttons* are used to select the M.2 drive positions which will be used for the selected operation. The unit provides one M.2 Source drive position and three M.2 Target drive positions. The M.2 Drive positions are located on the unit's top panel.



SATA Drive Select Buttons

The *SATA drive Select Buttons* are used to select the SATA drive positions which will be used for the selected operation. The unit provides one SATA Source HDD position, one USB Source drive position, four Target HDD drive positions and two USB Target drive positions. The SATA Source Drive position is located on the right side of the unit. The SATA Target Drive positions are located on the left side of the unit.

LinkMASSter

The *LinkMASSter* function allows capturing data from a drive installed in a Notebook or PC[2], using the unit's Ethernet port.

[2] The Detect Remote Drives Option, also known as the LinkMASSter Option requires purchase

Add Network Location

Allows a Source drive contents to be captured and stored in a Network or Locally Shared Folder. The Shared Folder location can be designated as the “Target” drive using the *Add Network Location* function. The *Add Network Location* function is available when running the LinuxDD Capture operations.

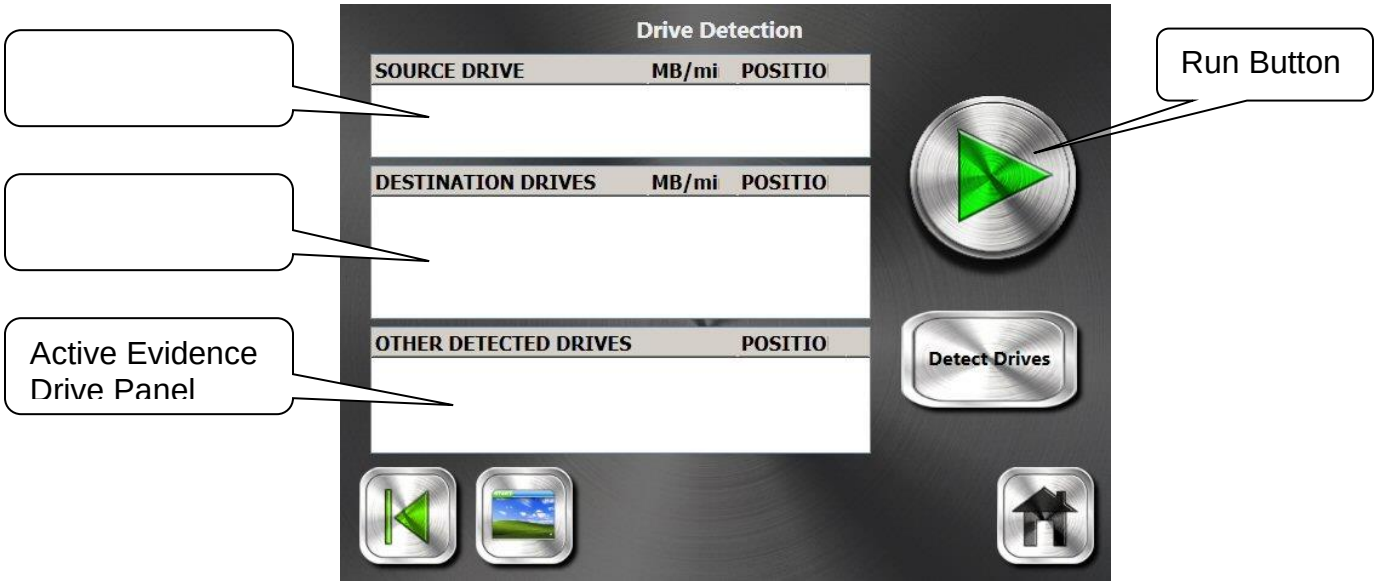
Settings Summary

Provides a list of the currently selected Operational Mode and associated Settings.

Adv GUI – Drive Detection Menu

The *MM NVMe M.2 Pro Adv GUI Drive Detection* Screen provides the functions necessary to detect the selected drives and to start the operation. The screen is accessed by selecting the *Next* Button from the *Drive Selection Screen*. The following selections are available.

- Run
- Drive Status Panels
- Detect Drives/Remove Drives
- LinkMASSter
- Desktop



Detect Drives

Select the *Detect Drives* Button to detect the selected the drive(s).

NOTE: By default, all ports are Write-Protected. The drive's Write-Protect property will automatically be disabled if the selected operational mode requires writing to the drive(s).

Run Button

Selecting *Run* will instruct the application begin the selected operation.

Remove Drives

The *Remove Drives* Button will be displayed after selecting the *Detect Drives* Button. Select *Remove Drives* to remove the selected the drive(s) from the Active Drive Panels.

Desktop Button

Allows access to the Desktop or the Device Manager.

Drive Status Panels

The *Active Drive Status Panels* lists the drives detected and their respective locations. The Panels will also indicate the drive's "burst" transfer rate during operation. Detected drives are listed in their respective Drive Status Panels.

NOTE: Drives can be manually transferred between *Drive Panels* using the *Drive Detect Tools* Menu. The menu is opened by selecting the listed drive. Source Drives cannot be moved to Target locations.

- *Active Source Drive Panel*

  The *Source Drive Panel* will list the detected and active Source drives for the active session. Drives listed in the *Other Detected Drives Panel* can be manually transferred to the *Active Source Drive Panel*. The drive listed in this panel is considered an "active" drive and will be used as the Source drive during the operation.

  NOTE: Drive(s) in the Source position(s) cannot be configured as Destination drives.

- *Active Target Drives Panel*

  The *Active Target Drives Panel* will list the detected and active Target drive(s) for the active session. Drives listed in the *Other Detected Drives Panel* can be transferred to the *Active Target Drives Panel*. The drive listed in this panel is considered an "active" drive and will be used as the Target drive during the operation.

  NOTE: Target drives can be configured as Source drives by transferring the drive from the *Active Target Drive Panel* to the *Active Source Drive Panel*.

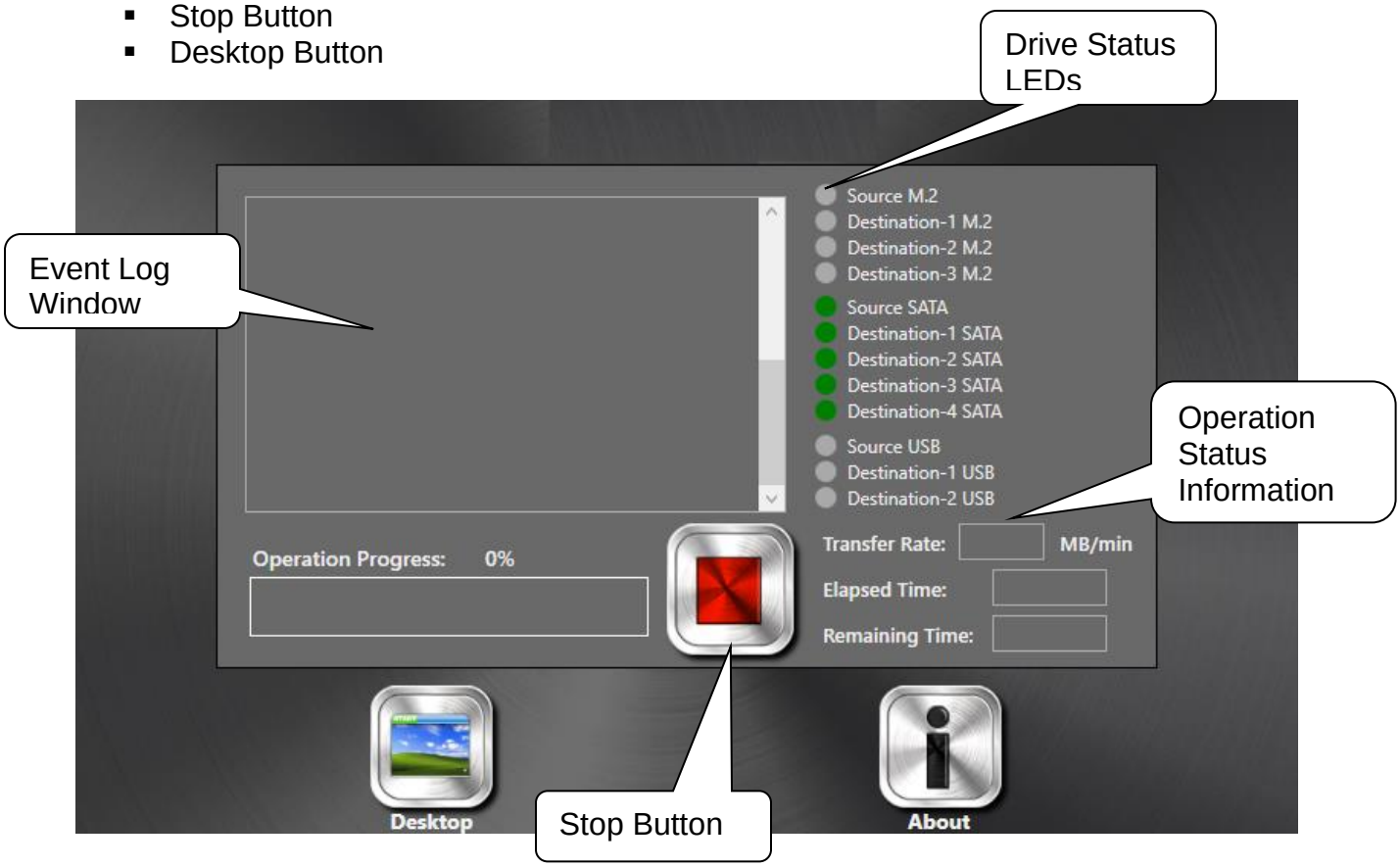
- *Other Detected Drives*

  The *Other Detected Drives Panel* will list the "non-active" drives detected on all ports other than the dedicated Source and Target ports. Drives listed in the *Source Drive* or *Target Drive Panels* can be transferred to the *Other Detected Drives Panel*. The drive(s) listed in this panel are "non-active" drives, and will not be used during an operation.

Adv GUI – Run Menu

The *MM NVMe M.2 Pro Adv GUI Run* Screen provides the status of the active operation. The screen is accessed by selecting the *Run* Button from the *Drive Detect Screen*. The following selections are available.

- Operation Status Information
- Drive Status LEDs
- Stop Button
- Desktop Button



Operation Status Information

The *Run Screen* provides *Operation Status Information* supplying the User with real time event information. The following Operation Status Information is available:

- *Speed*
  The Speed field displays the average transfer rate in megabytes per minute.

- *Progress Bar*
  Displays the percent of completion for the active operation.

- *Elapsed Time*
  Refers to the time elapsed during an operation. This field will also display the total elapsed time at the end of an operation.

- *Remaining Time*
  Refers to the time remaining to complete the operation.

Drive Status LED

Provides Drive Status information. The simulated drive status LEDs will be set to GREEN if the operation passes and RED if the operation fails or if the drive is not detected.

Stop Button

Selecting the *Stop* Button will instruct the application to terminate the selected operation. The Result Screen will be displayed after the Drives are removed from the Drive Status Panels.

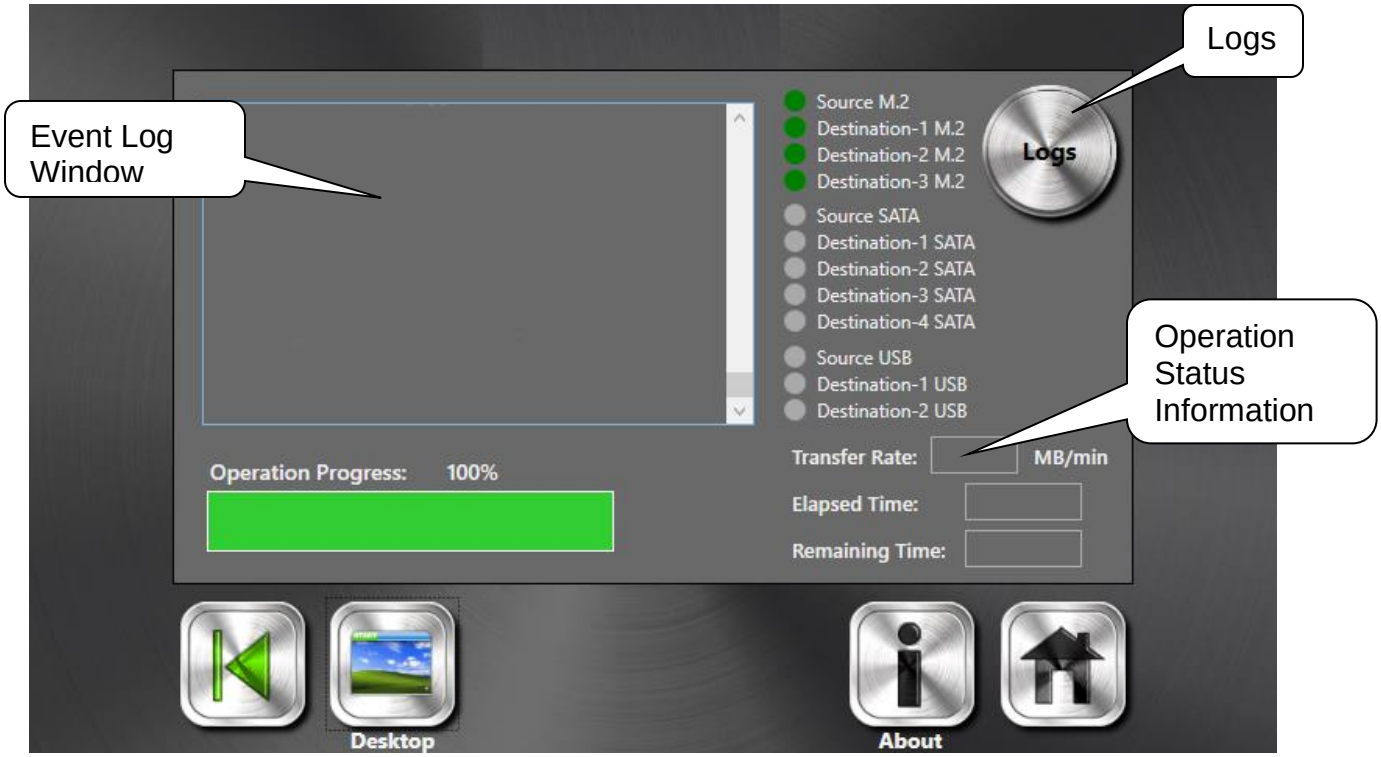
Desktop Button

Allows access to the Desktop or the Device Manager.

Adv GUI – Result

The *MM NVMe M.2 Pro Adv GUI Result* Screen provides the status result status of the completed operation. The screen is displayed after an operation is completed or aborted. The following selections are available.

- Operation Status Information
- Drive Status LEDs
- Logs
- Desktop



Adv GUI – Drive Detect Tools Menu

The *MM NVMe M.2 Pro Adv GUI Drive Detect Tools* Menu provides access to the Drive Property Edit functions. The menu is displayed by selecting the detected Drive from the *Drive Detect Screen*. The descriptions of the available functions are discussed in the following section.

- Change Drive Panel
- Mount Drives
- HPA/DCO Detection
- Disable Secure Erase Password

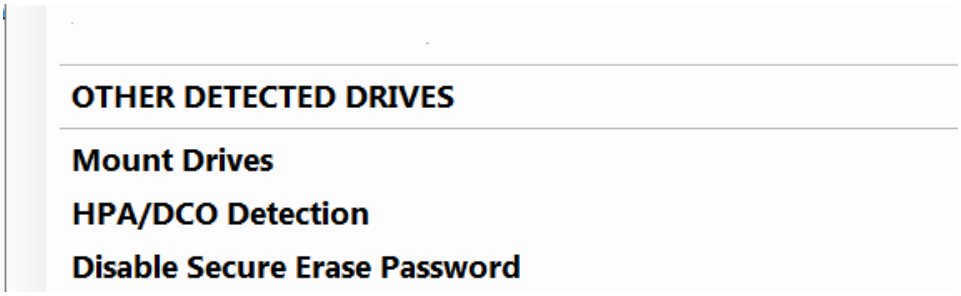


Figure 2

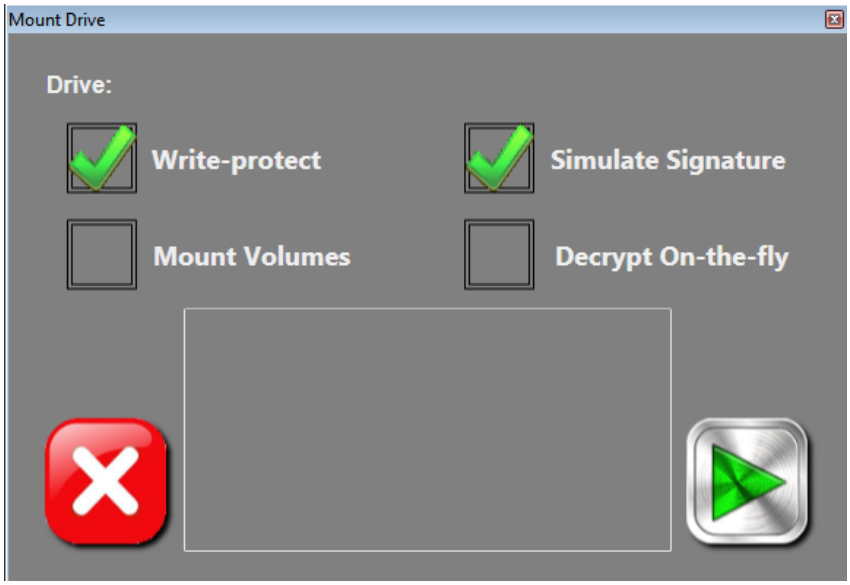
Change Drive Panel

Provides the available *Drive Panel* which the detected drive can be moved to.

Mount Drives

The *MM NVMe M.2 Pro Adv GUI Mount Drive* Menu provides access to the functions and controls necessary to change the state of the detected device *Write Protection* and *Mount Volume* properties. By default, all ports including the Target Drive ports and unit's USB ports are Write-Protected. In addition, the detected drive's partitions or volumes are "hidden" from the unit's O/S. The drive's properties will automatically be configured for the common Operational Modes. The recommended state of each device will depend on the operation to be performed with the detected devices. The menu is displayed by selecting the *Mount Drive* function from the *Drive Detect Tools* Menu. The descriptions of the available *Mount Drive* Settings are discussed in the following section.

- Write-Protect
- Mount Volumes
- Simulate Drive Signature
- Decrypt-On-The-Fly



- *Write-Protect*

  When selected, the detected drive will be Write-Protected. This setting should be enabled only when it is necessary to allow the unit's O/S or 3rd party application write access to the drive's volume.

  NOTE: By default, all ports are Write-Protected. The Write-Protect property of drives detected in the Source positions cannot be disabled.

- *Mount Volumes*

  When selected, the detected drive's volume will be accessible by the unit's Operating System. This setting should be enabled only when it is necessary to allow the unit's O/S or 3rd party application preview access to the drive's volume.

- *Simulate Signature*

  When selected, the O/S will be provided with a "simulated" Device Signature for the selected drive. The O/S requires each drive to have a different Device Signature. After the duplication operation, drives may have the same Device Signature. The drive's volume may not mount properly when attempting to mount the drive's volume under the unit's O/S if the same Drive Signatures are detected. If the setting is not selected, the Drive's unaltered Device Signature is presented to O/S or applications.

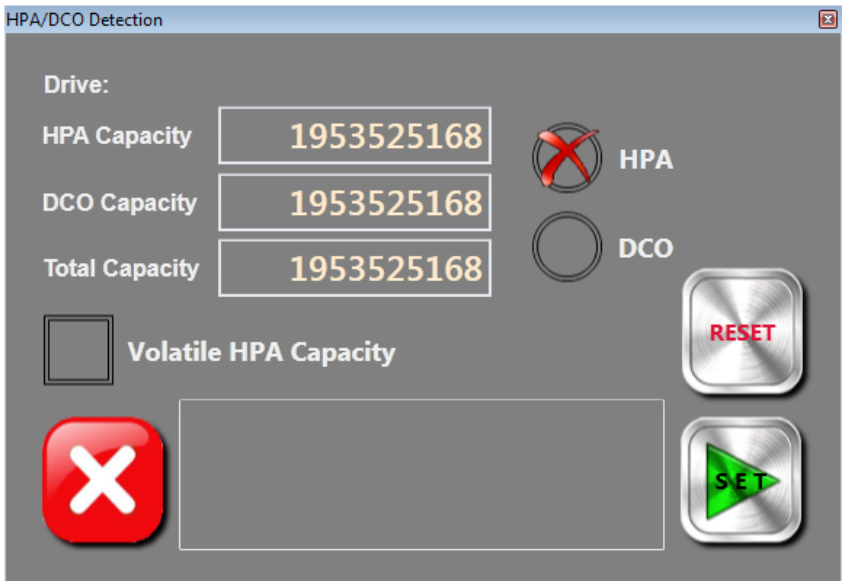
- *Decrypt-On-The-Fly*

  Allows Encrypted Drive Volumes to be Decrypted On-The-Fly for pre-viewing.

HPA/DCO Menu

The *MM NVMe M.2 Pro* **Advanced HPA Menu** provides the functions to view and modify the Target drive's Host Protected Area (HPA) and Device Configuration Overlay (DCO) Capacity feature set. The menu will only be available when the *Protected Area Support* Setting is Enabled. The menu is displayed by selecting the *HPA/DCO Detection* function from the *Drive Detect Tools* Menu. The descriptions of the available **HPA/DCO Menu** Settings are discussed in the following section.

- Protected Area Type
- HPA Capacity
- DCO Capacity
- SET
- Reset
- Volatile



- *Protected Area Type*

  Allows the User to select use of either HPA or DCO Support functions.

- *HPA/DCO Capacity*
  Value in sectors which will define the drive's programmed HPA or DCO capacity.

- *Total Capacity*
  Displays drive's Native capacity in sectors.

- *Set*

  Provides the function to program the Target drive's capacity using the HPA or DCO User Defined values.

- *Reset*

  Provides the function to reset the Target drive's capacity to its Native Capacity.

- *Volatile*

  Instructs the *Set Capacity* function to modify the drive's capacity only when the drive is power cycled.

Operational Mode Settings

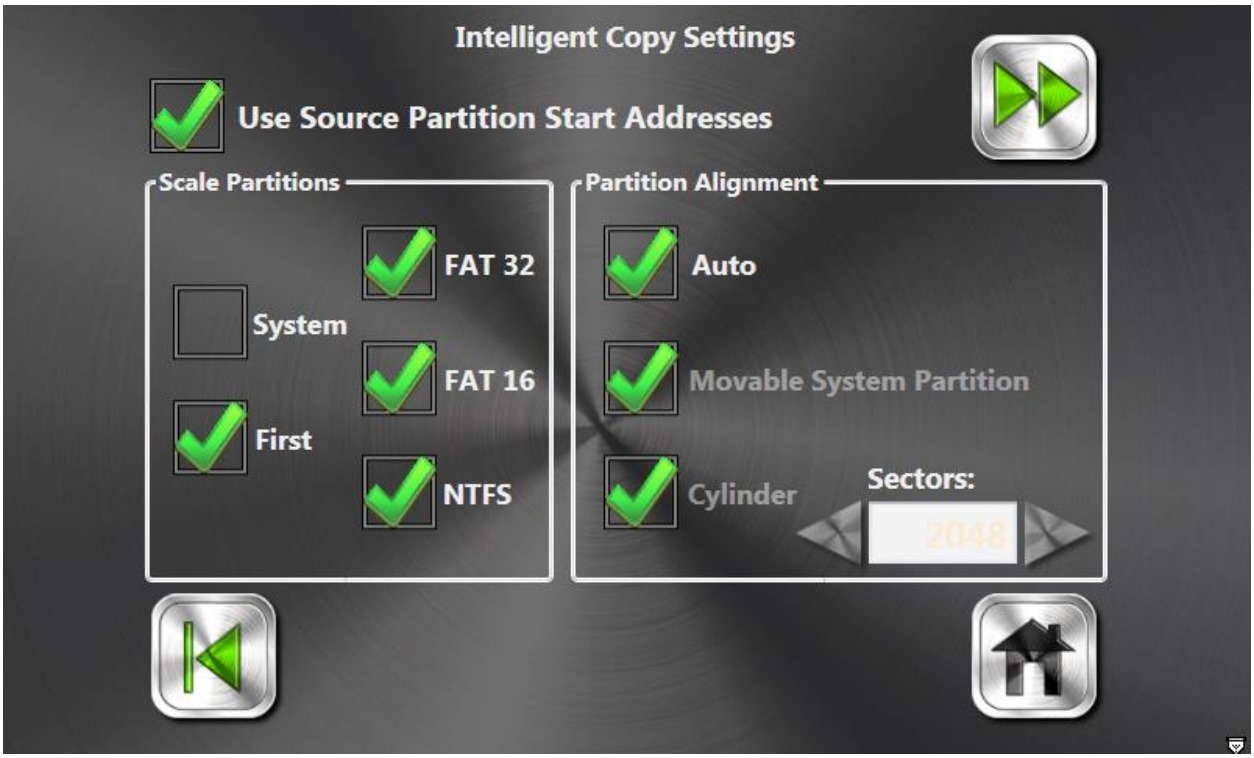
The *MM NVMe M.2 Pro* Advance Graphic Interface, provides access to the unit's Operational Mode Settings. The descriptions of the available Operational Mode Settings are discussed in the following section.

- Intelligent Copy
- Single Capture Settings
- Hash Only Settings
- LinuxDD Capture Settings
- LinuxDD Hash Settings
- LinuxDD Restore Settings
- WipeOut Settings
- Format Drives Settings

Intelligent Copy Settings

The **IQCOPY Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- Scale Partitions
- Partition Alignment
- Use Source Partition Start Addresses



Scale Partitions

The ***Scaling Options*** menu selection provides both an auto and manual method of selecting the proper partition scaling method to be used to configure the target drives. When all Scaling settings are enabled, IQCOPY will analyze the Source drive and scales target partitions in proportion to those on the Source drive. The following Scaling Options are available.

- **Scale System Reserve Partition**

When disabled, a System Reserve Partition will not be scaled.

- **Scale First Partition**

When disabled, the first partition will not be scaled.

- ***Scale FAT32 Partition***

When disabled, the FAT32 partition will not be scaled.

- ***Scale NTFS Partition***

When disabled, the NTFS partition will not be scaled.

- ***Scale FAT16 Partition***

When disabled, the FAT16 partition will not be scaled.

- **Use Source Partition Start Address**

Instructs IQCopy to use the Source Drive partition's Starting Address when creating the Target Drive's partitions.

Partition Alignment

The ***Partition Alignment*** menu selection provides customized IQCopy settings when copying a Windows VISTA Source drive. The default AUTO setting is recommended. Windows VISTA partitions use a 2048 starting sector alignment boundary by default. Other Windows O/S use a "disk cylinder size" starting sector alignment boundary by default. In addition, the start address of the bootable Vista partition is stored in the Boot Configuration Data (BCD) file. The BCD file needs to be updated if the Vista bootable partition's start address changes. When bootable Vista partitions are scaled, the partition's start address will change.

- **Auto**

  The ***Auto*** setting will recognize and use the Source drive's partition alignment method for the destination drives.

- **Cylinder**

  If enabled, partitions will be aligned on cylinder boundaries. If disabled, partitions will be aligned on boundaries specified by the ***Sectors*** setting.

- **Movable System Partition**

  If enabled, the bootable partition is allowed to be moved as a result of scaling.

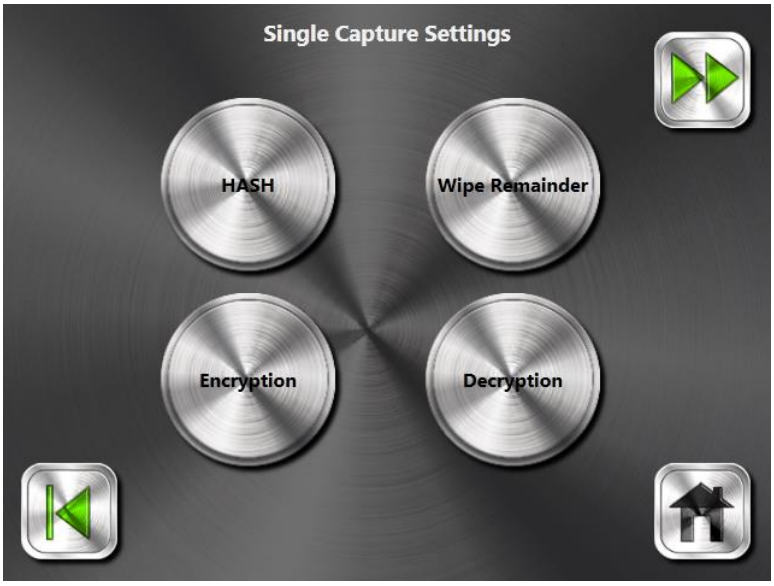
- **Sectors**

Select the sector number to be used for the partition's starting sector alignment boundary.

Single Capture Settings

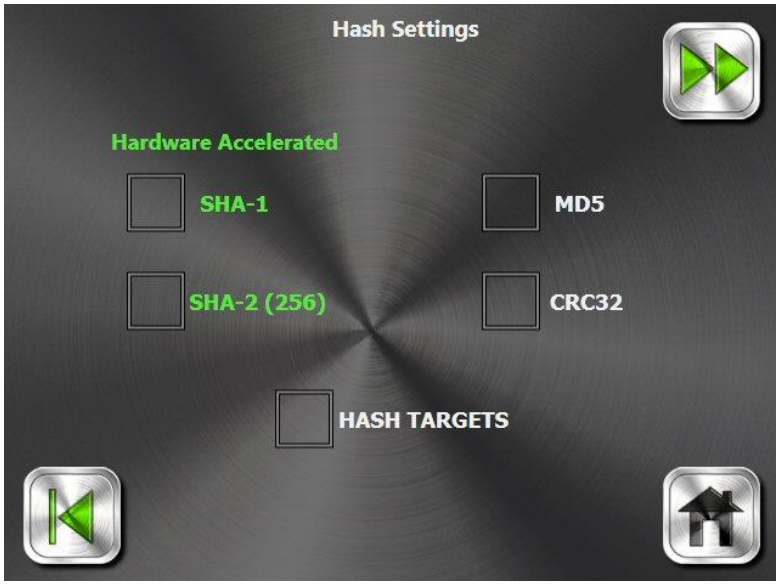
The associated **Single Capture** settings are described in this section.

- Hash Targets
- Hashing Methods
- Encryption/Decryption
- Wipe Remainder
- Read Back-Verify



Hash Targets

The *Hash Targets* function provides a method of generating Hash values for the Source drive's data and for the data written to the Target drives, in the same operation. The data is read back and hashed from the target drive(s) after each transferred block. Since data is read back during the operation the average transfer rate will decrease and the total time of completion will increase when this function is enabled.



Hashing Methods

The **Hashing Methods** menu selection provides the user with list of different Hash Algorithms to generate a Hash value for the Source drive's data. Hashing is a process that calculates a "unique signature" value for the contents of an entire drive.

- **CRC32**

Selecting CRC32 will result in the operation generating the CRC32 32-bit hash value for the data read from the source drive(s). Selecting the ***Hash Targets*** function will result in the operation generating the CRC32 Hash values for the data read from the Source drive and the data written to the Target drive.

- **MD5**

Selecting MD5 will result in the operation generating the MD5 128-bit hash value for the data read from the source drives. Selecting the ***Hash Targets*** function will result in the operation generating the MD5 Hash values for the data read from the Source drive and the data written to the Target drive.

- **SHA-1**

Selecting SHA-1 will result in the operation generating the SHA-1 160-bit hash value for the data read from the source drives. Selecting the ***Hash Targets*** function will result in the operation generating the SHA-1 Hash values for the data read from the Source drive and the data written to the Target drive.

NOTE: The SHA-1 Hash function uses Hardware Acceleration for calculations and therefore effects on transfer rates are limited.

- **SHA-2**

Selecting SHA-2 will result in the operation generating the SHA-2 256-bit hash value for the data read from the source drives. Selecting the ***Hash Targets*** function will result in the operation generating the Hash values for the data read from the Source drive and the data written to the Target drive.

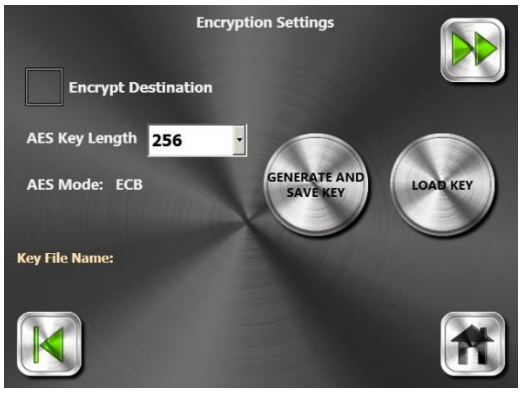
NOTE: The SHA-2 Hash function uses Hardware Acceleration for calculations and therefore effects on transfer rates are limited.

Wipe Remainder

The **Wipe Remainder** function instructs the capture operation to wipe (erase) remaining sectors after a capture operation is performed, if the Target drive is larger than the Source drive.

Encrypt/Decrypt

The **Encrypt/Decrypt** menu selection provides the user with the functions and settings necessary to configure an operation to Encrypt or Decrypt captured data.



- **AES Key Length (bits)**

Provides the user with the list of two AES Key Sizes to choose from. The choices are 192, and 256 bits.

- **AES Mode**

Indicates the AES Modes which will be used for Encryption. The MM NVMe M.2 uses the ECB Mode.

- **Encrypt Destination**

Instructs the operation to Encrypt the Target drive's partition and data during the data transfer operation.

- **Decrypt Source**

Instructs the operation to Decrypt data during the data transfer operation.

- **Generate and Save Key**

The Encryption Key used to Encrypt the Source drive's data is generated and saved.

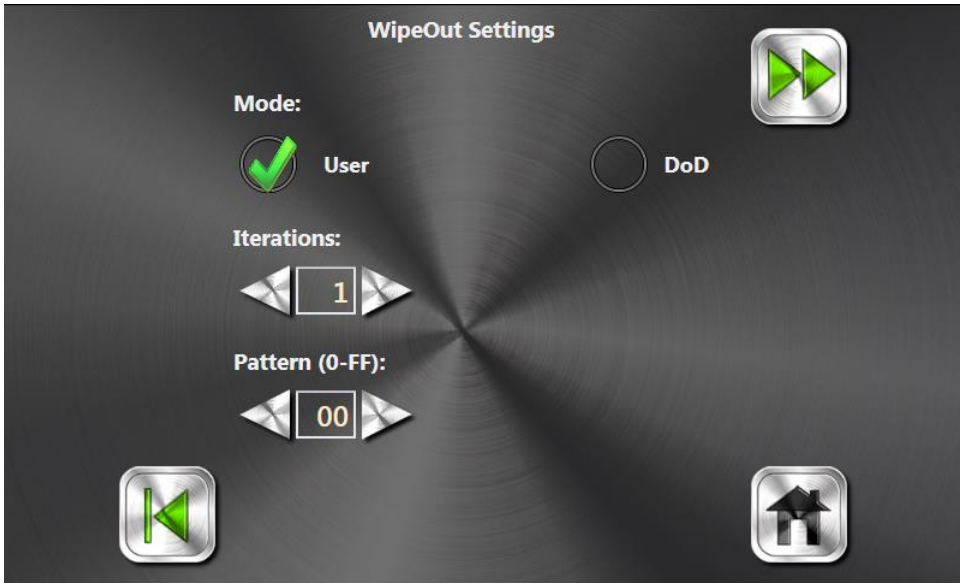
- **Load Key**

Provides the function to allow the User to select and load the Encryption Key which can be used to Decrypt the Target drive's Encrypted data.

WipeOut Settings

The **WipeOut Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- User
- DoD
- Iterations
- Pattern (0-255)



Mode

The WipeOut Mode provides the Operator with two methods of sanitizing drives.

- **User**

  The **Wipeout User** option provides a quick non-DoD method of sanitizing a drive of all previously stored data. The process involves writing a user defined pattern to the drive connected in the Target drive position, for a number of user defined drive passes (iterations). The process is methodical and contiguous, beginning from the first byte of the first sector on the drive, and ending on the last byte of the last sector of the drive.

- **DoD**

  The Wipeout DoD function provides a method of sanitizing a drive that meets the U.S. Department of Defense specification DOD 5220-22M for sanitizing drives.

  The operation is performed in three iterations and two individual passes that completely overwrites the destination drives. Each iteration makes two write-passes over the entire drive. The first pass writes ONEs (Hex 0xFF) over the

entire drive surface. The second pass writes ZEROes (Hex 0x00) over the entire drive surface. After the third iteration, a seventh pass writes the government designated code “246” (Hex 0xF6) across the entire drive surface, which is then followed by an eighth pass that inspects the drive with a Read-Verify review.

Iterations

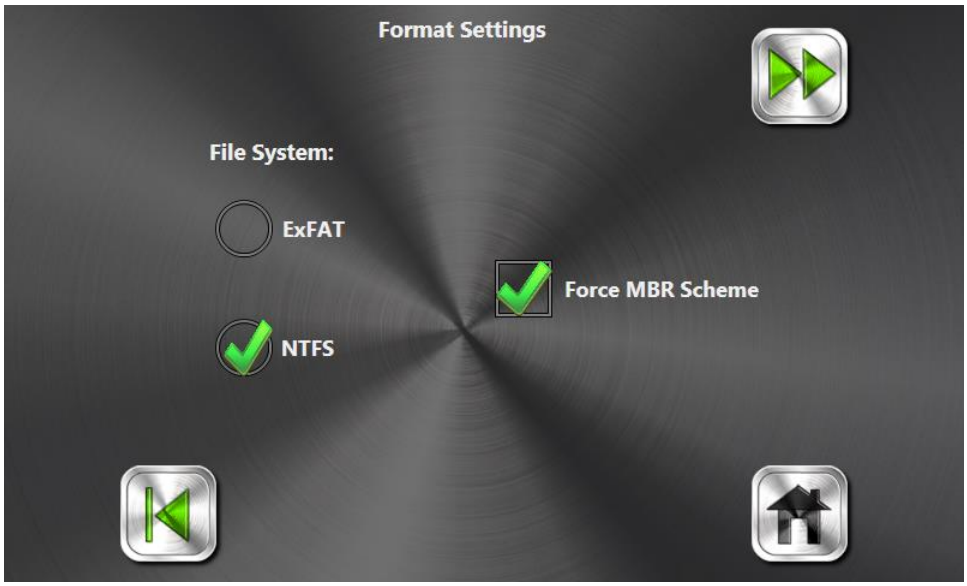
Allows the Operator to define the number of WipeOut-User iterations or passes to perform. Selecting 1 instructs the operation to sanitize the drive in one pass.

Pattern (0-255)

Allows the Operator to define the WipeOut-User Pattern to be used to sanitize the Target drive(s). The available range is 0-255.

Format Drives Settings

The **Format Drives Settings** menu provides the Operator with the function to format drives using NTFS or exFAT File Systems.



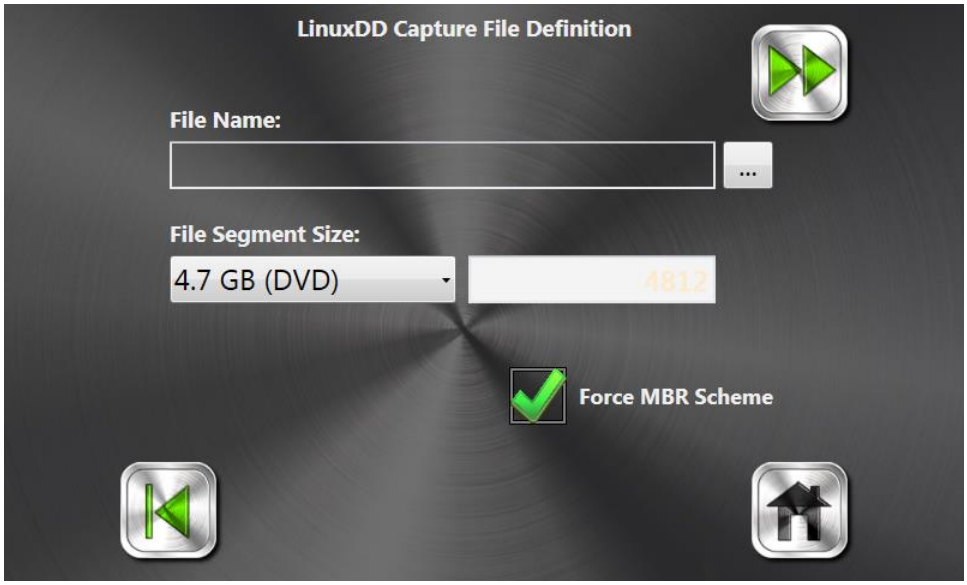
LinuxDD Capture Settings

The **LinuxDD Capture Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- File Segment Size
- Custom File Size (MB)
- File Name
- Read Back-Verify
- Hash Targets
- Hash Methods
- Encryption
- Force MBR Scheme

File Name

The *File Name* entry will be used as the name for the LinuxDD subdirectory, where the individual LinuxDD files will be stored. This File Name will also be used as the name of all LinuxDD files associated with the selected operation.



NOTE: If the File Name field is left blank, the operation will use a default LinuxDD file name referenced as “CASE<DATE><TIME>.”

File Segment Size

The size of the individual LinuxDD files can be set by selecting predefined values within the Capture File Size menu. The options are 640MB, 1GB, 2GB, 4.7GB, Whole Drive, and Custom. The default setting is 4.7GB.

Custom File Size (MB)

The size of the individual LinuxDD files can manually entered in Megabytes. The entry is active when the Custom value is selected in the Capture File Size menu.

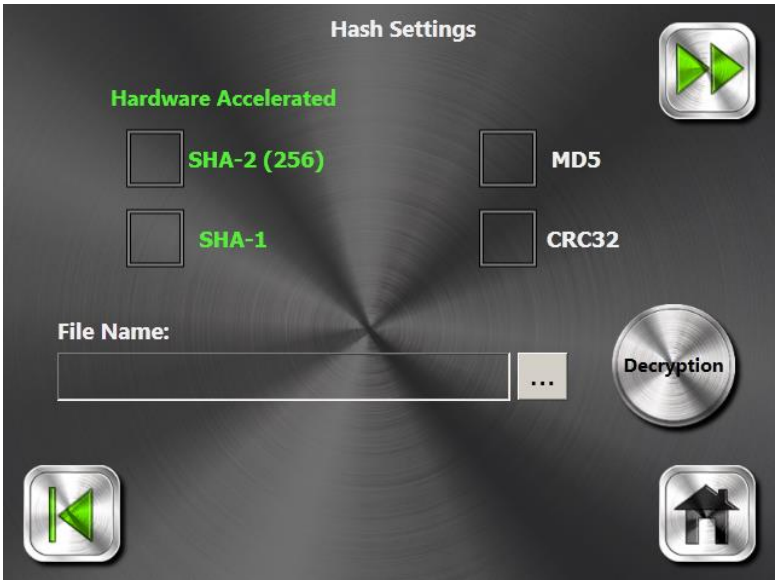
Force MBR Scheme

Instructs the operation to create MBR partitions instead of GPT partitions, for drives larger than 3TB in size.

LinuxDD Hash Settings

The **LinuxDD Hash Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- File Name
- Hash Methods
- Decryption



E01 Capture Settings

Not applicable for IT units.

LinuxDD Restore Settings

The **LinuxDD Restore Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- File Segment Size
- Custom File Size (MB)
- File Name
- Read Back-Verify
- Hash Targets
- Hash Methods
- Decryption

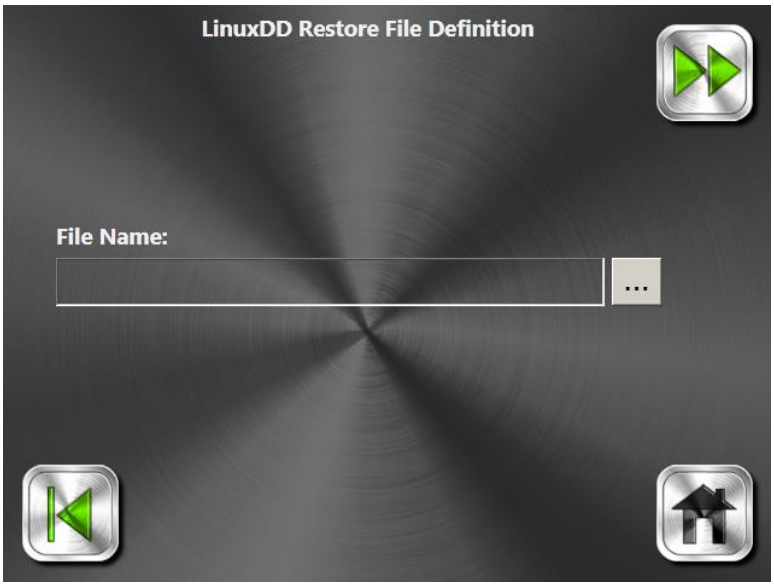
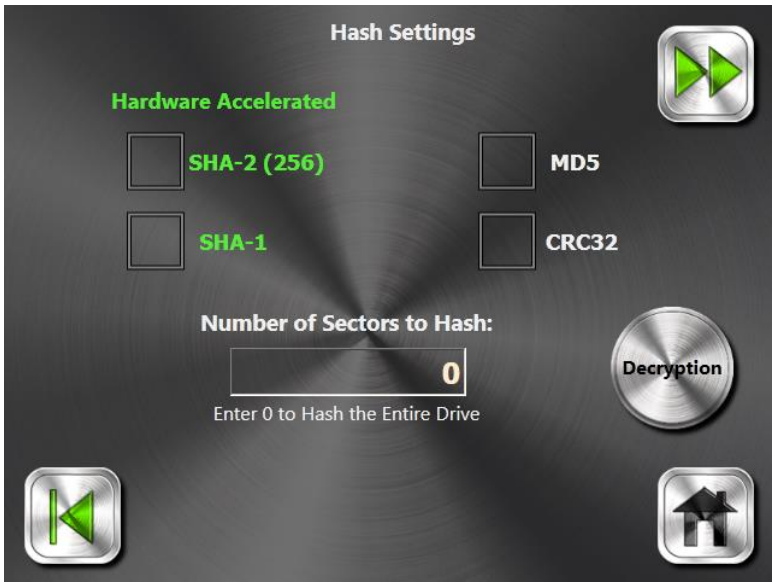


Figure 3

Hash Only Settings

The **Hash Only Settings** menu provides the Operator with a list of settings available for the selected operation. The menu is selected when the Operational Mode is selected from the Operational Mode Select Menu.

- Sectors to Hash
- Hash Methods
- Decryption



Sectors to Hash

Allows the Operator to define the number of sectors to hash. The default value of 0 will instruct the **Hash** operation to hash the entire drive.

Media MASSter 102 Pro IT Advanced Screen
Control Console

The *MM NVMe M.2 Pro IT* **Advanced Interface Control Console** may provide additional functions that are not currently available under the Advanced Graphical Interface. The Advanced Interface Control Console can be accessed from the Advanced Graphical Interface by selecting the *Advance Start View Settings* option. The functional descriptions of the unit's Advanced Interface Control Console functions are discussed in the following section.

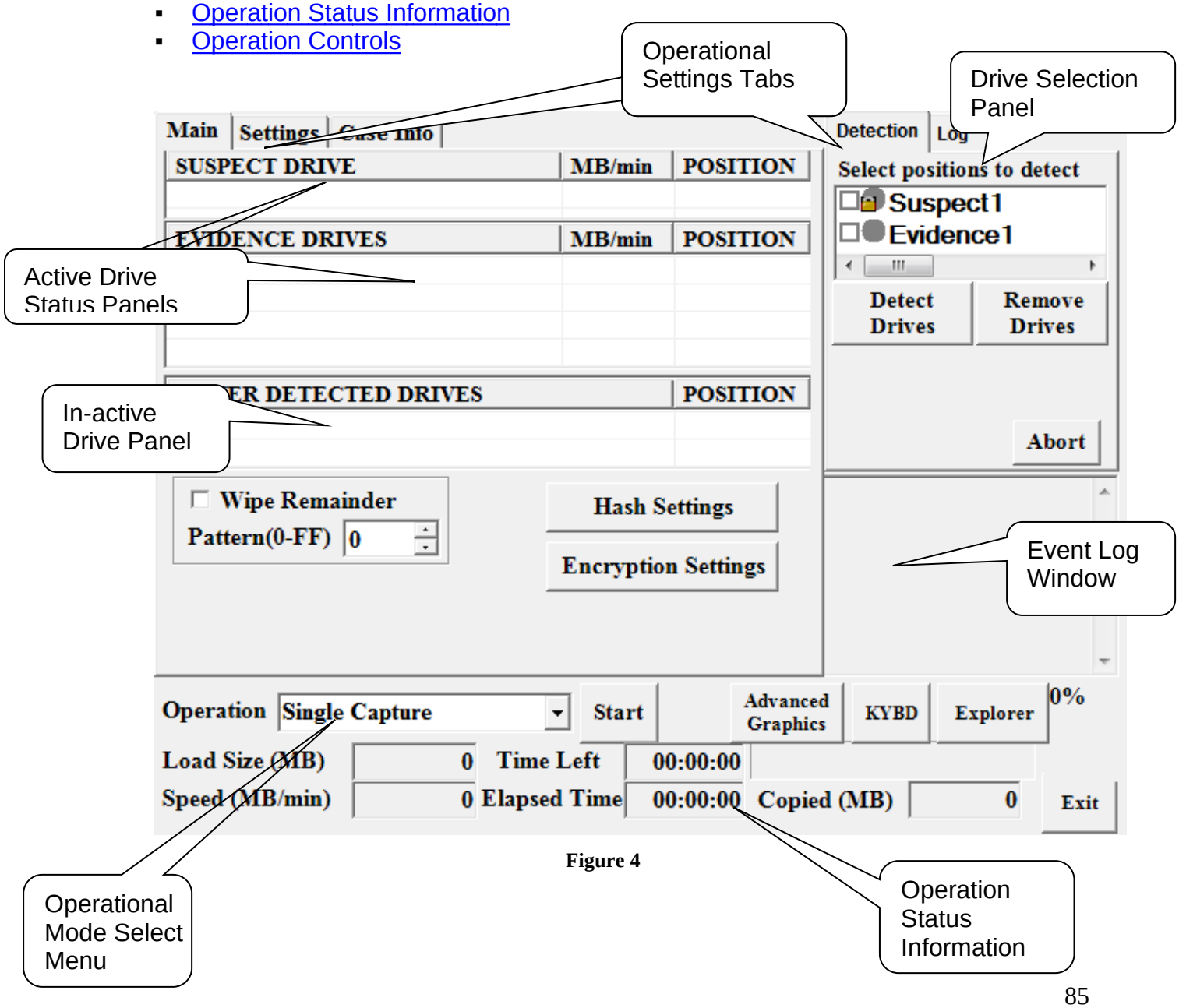


Figure 4

Advanced Interface – Main Screen

The *MM NVMe M.2 Pro IT* **Advanced Interface-Main Screen** will provide a list of the detected drives and allows detected drives to be configured as active or inactive drives. The Main Screen is displayed by selecting the Main Tab from the **Advanced Interface Control Console.** The descriptions of the available **Advanced Interface Drive Detect Menu** functions are discussed in the following section.

Drive Selection Panel

The *Drive Selection Panel* provides the settings and functions used to detect drives connected to the unit's dedicated Source and Target drive positions, including devices connected to the dedicated USB ports located on the side of the unit. The *Drive Select Panel* allows the operator to select the drive position(s) to scan during a drive detect operation.

Source Drive Select

Select the *Source* Check Box to select the drive in the "Source" position for detection. The unit provides a dedicated, Write-Protected position for a "Source" M.2, SATA or USB drive. The M.2 Source positions is located on the unit's top panel. The "SATA Source" position is located on the right side of the unit.

Target 1-4 Drive Select

Select the *Target Che*ck Box to select the drive(s) in the "Target" position(s) for detection. The unit provides three dedicated Target M.2 drive positions, four dedicated SATA drive positions and two USB "Target" drive positions. The M.2 drives are located on the unit's top panel. The SATA "Target 1 through 4" positions are located on the left panel. The "Target 1 and 2 USB" positions are located on the unit's right panel.

NOTE: The *Drive Select* menu provides a simulated power indicator for each drive position. The indicator will be GREY prior to drive detection, GREEN if the drive is detected or the operation passed, and RED if the drive is not detected or if the operation was not successful.

Detect Drives

Select the *Detect Drives* Button to detect the selected the drive(s).

NOTE: By default, all ports are Write-Protected. The drive's Write-Protect property will automatically be disabled if the selected operational mode requires writing to the drive(s).

Remove Drives

Select *Remove Drives* to remove the selected the drive(s).

Add Network Location

Allows a Source drive contents to be captured and stored in a Network or Locally Shared Folder. The Shared Folder location can be designated as the "Target" drive using the *Add Network Location* function. The *Add Network Location* function is available when running the LinuxDD Capture operations. The descriptions of the available settings are discussed in the following section.

- Browse

Figure 5

- **Browse**

Select ***Browse*** to select the Shared Folder Location.

Detect Remote Drives

The *Detect Remote Drives* function allows capturing data from a drive installed in a Notebook or PC[3], using the unit's Ethernet port.

[3] The Detect Remote Drives Option requires purchase

Drive Status Panels

The *Active Drive Status Panels* lists the drives detected and their respective locations. The Panels will also indicate the drive's "burst" transfer rate during operation. Detected drives are listed in their respective Drive Status Panels.

NOTE: Drives can be manually transferred between *Drive Panels* by selecting and "dragging" the listed drive using the Touch Screen or using an attached mouse. Source Drives cannot be moved to Target locations.

Active Source Drive Panel

The ***Source Drive Panel*** will list the detected and active Source drive for the active session. Drives listed in the ***Other Detected Drives*** **Panel** can be manually transferred to the ***Active Source Drive Panel***. The drive listed in this panel is considered an "active" drive and will be used as the Source drive during the operation.

NOTE: The Drive in the Source position cannot be configured as Destination drives.

Active Target Drives Panel

The ***Active Target Drives Panel*** will list the detected and active Target drive(s) for the active session. Drives listed in the ***Other Detected Drives Panel*** can be manually transferred to the ***Active Target Drives Panel***. The drive listed in this panel is considered an "active" drive and will be used as the Target drive during the operation.

NOTE: Target drives can be configured as Source drives by transferring the drive from the ***Active Target Drive Panel*** to the ***Active Source Drive Panel***.

Other Detected Drives

The ***Other Detected Drives Panel*** will list the "non-active" drives detected on all ports other than the dedicated Source and Target ports. Drives listed in the ***Source Drive*** or ***Target Drive*** **Panels** can be manually transferred to the ***Other Detected Drives Panel***. The drive(s) listed in this panel are "non-active" drives, and will not be used during an operation.

Chapter 5:
Operational Procedures

Prepare for Operation

This section describes the recommended procedure to follow when preparing to perform an operation with drives connected directly to the unit.

1. Prepare Source Drive

- Connect the M.2 Source drive to the unit's M.2 Source port, located on the unit's top panel or connect the SATA Source drive to the unit's SATA Source port, located on the Right Panel (Fig. 1). Refer to the *Quick Start* section for details.

  NOTE: It is required to power off the unit before connecting or removing M.2 drives. It is not necessary to power off the unit when connecting or removing SATA drives. The drive detected in this position will be listed in the Active *Source Drive Panel*.

2. Prepare the Target Drive

- Connect the M.2 Target drive(s) to the unit's M.2 Target ports, located on the unit's top panel. Connect the SATA Target drive(s) to the unit's Target ports located on the unit's Left Panel (Fig. 2). Refer to the *Quick Start* section for details.

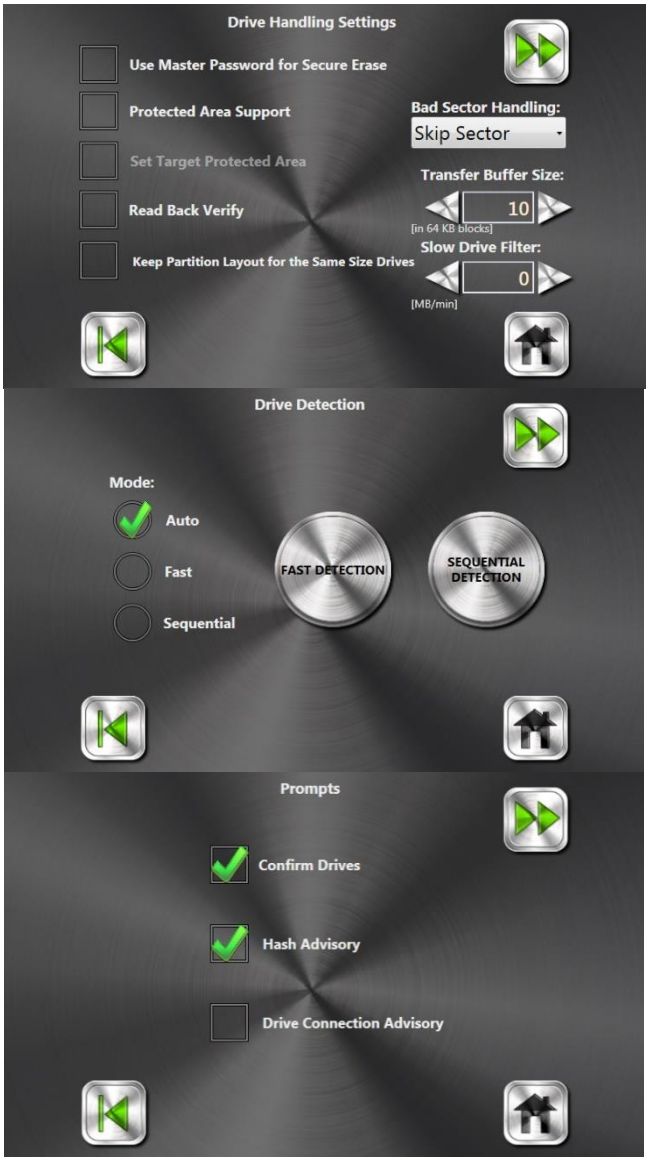
  NOTE: The drive detected in this position will be listed in the Active *Destination Drive Panel*.

  Reseat USB Drives between Drive Detect attempts. By default, all ports including the dedicated Target drive ports are Write-Protected. The Write-Protection feature of all Target drive ports will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

3. Configure the unit's Settings.

- Select the required operation using the unit's Advanced Graphics or Wizard Interface.
- Verify Settings of selected Operation. See Chapter 4 for Operational Mode recommended settings.
- Verify unit's Common Settings (See Table 2). The Common Settings are located in the Advanced **Settings** Screen.

Common Settings
Table 2



4. Removing Drives

- The *Drive Select* menu provides a simulated power indicator for each drive position. The indicator will be GREY prior to drive detection, GREEN if the drive is detected or if the operation passed, and RED if the drive is not detected or if the operation was not successful. It is required to power off the unit before connecting or removing M.2 drives. Though SATA drives will remain powered on after an operation completes, the drives can be physically removed after the listed drive is cleared from its assigned Active *Drive Status Panel*, without the need to power off the unit.

5. Follow the Operational Procedure instructions, in this chapter for the required operation.

Acquiring Drives using Intelligent Copy Mode

The following section describes the procedure to use the *Intelligent Copy* mode for acquiring Source drive's data from a drive that have been removed from its PC or Notebook.

1. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
3. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.
4. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection.
5. Select *Intelligent Copy* to access the *Intelligent Copy* Settings Menu.
6. Set the *Intelligent Copy* Settings which are dynamically displayed in the Operation's Main Screen. See Table 3 for recommended settings.
7. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.
8. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

9. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

    NOTE: If necessary, select "non-active" drive(s) listed in the *Other Detected Drives* panel and move them to either the *Source Drive* or *Destination Drives* panels. The drive(s) listed in the *Source Drive* or *Destination Drives* panels are considered "active" drives and will be used during data transfer operations. If necessary, also transfer "active" drives from the *Source Drive* or *Destination Drives* panel to the *Other Detected Drives* panel.

10. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

Intelligent Copy Recommended Settings
Table 3

Menu Item	Recommended Setting
Copy Mode	**Intelligent COPY**
ReadBack-Verify	**Disable** (Optional)
Partition Scaling	
• System • First • NTFS • FAT32 • NTFS	**Disable** **Enable** **Enable** **Enable** **Enable**
Partition Alignment	**Auto**
Use Source Partition Start Address	**Enable**

"Mirroring" Drives using Single Capture Mode

The following section describes the procedure to use the Single Capture mode for "Mirroring" a Source drive that have been removed from its PC or Notebook.

1. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.

3. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.

4. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection.

5. Select the *Single Capture* Button to access the Single Capture Settings Menu.

6. Set the Single Capture Settings which are dynamically displayed in the Operation's Main Screen. See Table 4 for recommended settings.

7. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.

8. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

9. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

   NOTE: If necessary, select "non-active" drive(s) listed in the *Other Detected Drives* panel and move them to either the *Source Drive* or *Destination Drives* panels. The drive(s) listed in the *Source Drive* or *Destination Drives* panels are considered "active" drives and will be used during data transfer operations. If necessary, also transfer "active" drives from the *Source Drive* or *Destination Drives* panel to the *Other Detected Drives* panel.

Hash values generated during the capture operation are generated for the data read from the Source drive not from the data read from the Target (target) drive unless the operation is instructed to hash the Target drive by enabling the *Hash Targets* function.

10. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

Single Capture Recommended Settings
Table 4

Menu Item	Setting
Operational Modes	Single Capture
Hash Method	SHA-1
Hash Targets	Enable (Optional)
Read Back-Verify	Disable (Optional)
Wipe Remainder	Disable (Optional)

Backup Multiple Source Drives using LinuxDD Segment Format

The following section describes the procedure to use the LinuxDD Capture mode for Capturing Source data from drive that has been removed from its PC or Notebook.

1. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.

3. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.

4. Select **CASE INFO** from the Operation Category Screen and enter the required information.

5. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection.

6. Select the *LinuxDD Capture* Button to access the LinuxDD Capture Settings Menu.

7. Select *File Format* and enter the name of the file to be used by the *LInuxDD Capture* operation for creating the segmented Case files.

8. Set the LinuxDD Capture Settings. See Table 4 for recommended settings.

9. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.

10. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

11. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

NOTE: If necessary, select "non-active" drive(s) listed in the *Other Detected Drives* panel and move them to either the *Source Drive* or *Destination Drives* panels. The drive(s) listed in the *Source Drive* or *Destination Drives* panels are considered "active" drives and will be used during data transfer operations. If necessary, also transfer "active" drives from the *Source Drive* or *Destination Drives* panel to the *Other Detected Drives* panel.

Hash values generated during the capture operation are generated for the data read from the Source drive not from the data read from the Target (target) drive unless the operation is instructed to hash the Target drive by enabling the *Hash Targets* function.

12. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

LinuxDD Capture Recommended Settings
Table 5

Menu Item	Setting
Operational Modes	LinuxDD Capture
Hash Method	SHA-1
Hash Targets	Enable (Optional)
Read Back-Verify	Disable (Optional)
Capture File Size	4GB

LinkMASSter-Capturing from an Unopened PC or Notebook

The following section describes the procedure for Capturing Source data from an Unopened PC or Notebook.

1. Connect the ICS supplied Crossover Ethernet Cable to the MM NVMe M.2 unit's Ethernet port and to the Notebook/PC Ethernet port. Alternately, connect the Gigabit USB-to-Ethernet Network Adapter to the Notebook/PC USB port and the Ethernet Cable connector end to the MM NVMe M.2 unit's Ethernet port. See the instructions titled "USB-to-Ethernet Connection", for additional details.
2. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).
3. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
4. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.
5. Select CASE INFO from the Operation Category Screen and enter the required information.
6. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection and select the required operation.
7. Set the Operational Mode Settings .
8. Select  to access the *Drive Selection* Screen and select the Target Drive(s) to be used for the selected operation.

   NOTE: Do not select any Source position from the Drive Selection Screen.
9. Select the *LinkMASSter* function from the *Drive Selection* Screen.
10. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

11. Configure the Source PC or Notebook BIOS to boot from its CD-ROM or DVD drive. If using the supplied LinkMASSter USB Boot media, configure the Source PC to boot from USB media.

    NOTE: Various PC or Notebook BIOS require pressing a specific key combination such as <F12> at boot up to change the default Boot Order. It is the user's responsibility to correctly setup the Source PC or Notebook BIOS.

12. Insert the LinkMASSter Bootable CD or USB media and allow the Source PC or Notebook to boot from the LinkMASSter CD or USB media.

13. The LinkMASSter Network Capture Agent Screen is display with the computer's detected drive information.

14. Select *Detect Drives* from the MM NVMe M.2 Pro *Drive Detection* Screen. The Source drive, located in the Source computer will be listed in the Source Drive panel list and the Target drive will be listed in the Destination Drives panel list.

15. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

16. After the operation completes, the SATA Target drive will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. Remove the LinkMASSter CD or USB media from the Source computer prior to powering OFF the computer. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails. Log files will automatically be stored internally and can be transferred to external media using the unit's USB ports, located on the back of the unit.

    NOTE: Prior to saving logs to external media, disable the LinkMASSter function from the Drive Selection Screen.

Capturing to a Shared Folder

The following section describes the procedure to use the LinuxDD Capture modes for capturing and storing Source data to a Shared Network Folder.

1. Connect and configure the Source drive as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: Attach an Target drive if capturing to both a local Target drive and a Network Shared Folder.

2. Configure a Shared Network Folder on the Network PC.
3. Connect the appropriate Ethernet Cable to the MM NVMe M.2 unit and to the Network PC.

   NOTE: An Ethernet Cross-Over cable would be required for direct connection.

4. Establish a Network Connection between the MM NVMe M.2 and the Destination Network PC using the MM NVMe M.2 O/S *DESKTOP/CONTROL PANEL/NETWORK and INTERNET CONNETIONS* Tools.

   NOTE: It is the responsibility of the User to properly configure the Network for proper connectivity and to properly configure the Shared Network Folder. The Shared Network Folder requires write access. If properly configured, the Shared Network Folder should be accessible from the MM NVMe M.2.

5. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
6. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.
7. Select **CASE INFO** from the Operation Category Screen and enter the required information.
8. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection.
9. Select *LinuxDD Capture*.
10. Select *File Format* and enter the name of the file to be used by the *LInuxDD Capture* operation for creating the segmented Case files.
11. Set the Operational Mode Settings .
12. Select  to access the *Drive Selection* Screen and select the Source Drive to be used for the selected operation.

NOTE: Do not select any Target position from the Drive Selection Panel unless an Target drive will also be used as a Destination drive.

13. Select the Target *Add Network Location* function from the *Drive Selection* Panel.
14. Select **Browse** from the "Add Network Location" menu screen.
15. Select "My Network Places" to locate and select the Shared Network Folder. The Shared Network Folder will be listed in the *Target Drives Panel*.
16. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.
17. Select *Detect Drives* from the MM NVMe M.2 Pro *Drive Detection* Screen. The Source drive will be listed in the Source Drive panel list and the Shared Folder Drive location will be listed in the Destination Drives panel list.
18. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Shared Folder Drive location should be listed in the *Destination Drives* panel's list.
19. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

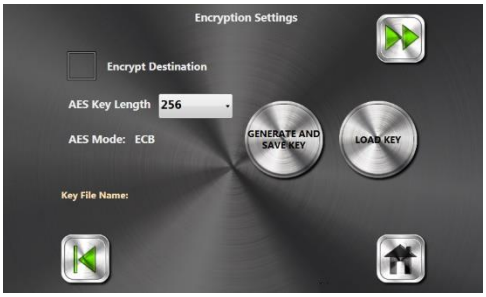
Encrypting Data During Data Capture

The following section describes the procedure to Encrypt data seized from the Source drive.

1. Connect and configure the Source drive as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: Sanitize (WipeOut) the Target drive(s) prior to Encrypting data. Do not use LinuxDD Target drives which contain captured cases which were not stored on a previously Encrypted drive.

1. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
2. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.
3. Select **CASE INFO** from the Operation Category Screen and enter the required information.
4. Select *Capture*  from the *Operation Category* screen to access the Capture Mode Menu Selection.
5. Select *Single Capture* or *LinuxDD Capture*.
6. Select *File Format* and enter the name of the file to be used by the *LInuxDD Capture* operation for creating the segmented Case files.
7. Select *Encryption* from the Operation's dynamically displayed settings menu.



8. Select the *AES Key Length*.
9. Select *Encrypt Destination*.
10. Select *Generate and Save Key*. Select a name for the Encryption Key and the Key's location.

    NOTE: In addition to unique password information, the saved Encryption Key will also contain the selected *AES Key Length* and *AES Mode* settings.

11. Set the Operational Mode Settings. See Table 6 for recommended settings.

12. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.

13. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

14. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

Hash values generated during the capture operation are generated for the data read from the Source drive not from the data read from the Target (target) drive unless the operation is instructed to hash the Target drive by enabling the *Hash Targets* function.

15. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

Encryption Capture Recommended Settings
Table 6

Menu Item	Setting
Operational Modes	Single Capture/ LinuxDD Capture
Hash Method	SHA-1
Hash Targets	Enable (Optional)
Read Back-Verify	Disable (Optional)
AES Key Length	256
AES Mode	ECB
Encrypt	Enable

Decrypting Data During Data Transfer

The following section describes the procedure to Decrypt data from an Encrypted Target drive.

1. Connect the Encrypted drive to the unit's Source position and the Destination drive(s) as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.

3. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.

4. Select **CASE INFO** from the *Operation Category* Screen and enter the required information.

5. If restoring an Encrypted drive previously created using *Single Capture*, select *Capture Mode*  from the *Operation Category* screen to access the Capture Mode Menu Selection, otherwise select *Restore Mode*  .

6. Select *Single Capture* or *LinuxDD Restore*.

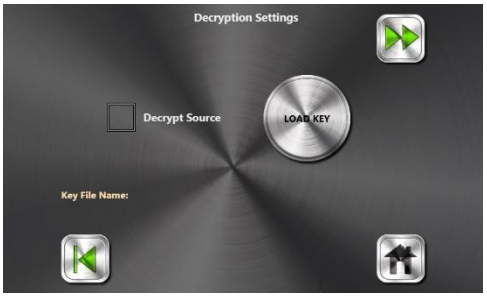
   NOTE: The supported Operational modes for Decryption are Single Capture, LinuxDD Restore. The "Hash Only" modes would also be supported to generate hash values based on decrypted data.

7. Select *File Format* and enter the name of the file which was used by the *LInuxDD Capture* operation for creating the segmented Case files.

8. Select *Decryption* from the Operation's dynamically displayed settings menu.

9. Select **Load Key** to select the saved Encryption Key which was used to Encrypt the drive.

   NOTE: Since the saved Encryption Key also contains the original *AES Key Length* and *AES Mode* settings, it is not necessary to manually enter these settings.



10. Select *Decrypt Source*.
11. Set the Operational Mode Settings. See Table 7 for recommended settings.
12. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.
13. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.
14. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

Hash values generated during the capture operation are generated for the data read from the Source drive not from the data read from the Target (target) drive unless the operation is instructed to hash the Target drive by enabling the *Hash Targets* function.

15. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

Decryption Capture Recommended Settings
Table 7

Menu Item	Setting
Operational Modes	Single Capture/ LinuxDD Restore
Hash Method	SHA-1
Hash Targets	Enable (Optional)
Read Back-Verify	Disable (Optional)
AES Key Length	N/A
AES Mode	N/A
Decrypt	Enable

Restoring from LinuxDD Segmented File Format

The following section describes the procedure to use the LinuxDD Restore mode to restore the captured Linux-DD segmented file formatted case to its original drive format.

1. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.

   NOTE: By default, all ports including the dedicated Target drive ports are Write-Protected. The port's Write-Protection will automatically be disabled if the selected operational mode requires writing to the Target drive(s).

2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
3. Select *Operations*  from the *Main Screen* to access the *Operation Category* Menu selection.
4. Select **CASE INFO** from the Operation Category Screen and enter the required information.
5. Select *Restore*  from the *Operation Category* screen to access the Capture Mode Menu Selection.
6. Select *LinuxDD Restore*.
7. Select *File Format* and enter the name of the file which was used by the *LInuxDD Capture* operation for creating the segmented Case files.
8. Set the LinuxDD Restore Settings. See Table 8 for recommended settings.
9. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.
10. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.

11. Select *Run* Button  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Source drive should be listed in the *Source Drive* panel's list, and the Target drive should be listed in the *Destination Drives* panel's list.

NOTE: If necessary, select "non-active" drive(s) listed in the *Other Detected Drives* panel and move them to either the *Source Drive* or *Destination Drives* panels. The drive(s) listed in the *Source Drive* or *Destination Drives* panels are considered "active" drives and will be used during data transfer operations. If necessary, also transfer "active" drives from the *Source Drive* or *Destination Drives* panel to the *Other Detected Drives* panel.

Hash values generated during the capture operation are generated for the data read from the Source drive not from the data read from the Target (target) drive unless the operation is instructed to hash the Target drive by enabling the *Hash Targets* function.

12. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

Restore Recommended Settings
Table 8

Menu Item	Setting
Operational Modes	LinuxDD Restore
Hash Method	Disable (Optional)
Hash Targets	Disable (Optional)
Read Back-Verify	Disable (Optional)
Capture File Size	Not Applicable

Sanitizing Drives Using WipeOut DoD

Use the Wipe Out DoD mode to sanitize drives using the U.S. Department of Defense DoD 5220-22M specification.

1. Connect and configure the target drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.
2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
3. Select Operations  from the *Main Screen* to access the *Operation Category* Menu selection.
4. Select **CASE INFO** from the Operation Category Screen and enter the required information.
5. Select *WipeOut*  from the *Operation Category* screen to access the *Wipe Mode* Menu Selection.
6. Select *WipeOut* to access the Wipe Settings Menu Screen.
7. Select the *DoD* Wipe Option.
8. Set the Operational Mode Settings which are dynamically displayed in the Operation's Main Screen. See Table 9 for recommended settings.
9. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.
10. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.
11. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Target drive should be listed in the *Destination Drives* panel's list.
12. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

WipeOut DoD SETTINGS

Table 9

Menu Item	Recommended Setting
Copy Mode	**WipeOut**
ReadBack-Verify	**Disable** (Optional)
WipeOut Mode	**DoD**

Sanitizing Drives Using WipeOut - User

The Wipe Out User operation can be used to sanitize drives in one pass rather than 7 passes which is required using the DoD Wipe Out method.

1. Connect and configure the target drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.
2. Verify the recommended Common Settings (Table 2) located in the **Settings** Screen.
3. Select Operations  from the *Main Screen* to access the *Operation Category* Menu selection.
4. Select **CASE INFO** from the Operation Category Screen and enter the required information.
5. Select *WipeOut*  from the *Operation Category* screen to access the *Wipe Mode* Menu Selection.
6. Select *WipeOut* to access the Wipe Settings Menu Screen.
7. Select *User* Wipe Option.
8. Set the Operational Mode Settings which are dynamically displayed in the Operation's Main Screen. See Table 10 for recommended settings.
9. Select  to access the *Drive Selection* Screen and to select the drives to be used for the selected operation.
10. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen.
11. Select *Run*  from the *Drive Detection* Screen to begin the operation. A prompt will be displayed requesting the Operator to verify that the detected drives are listed in the appropriate Drive Status panels. The Target drive should be listed in the *Destination Drives* panel's list.
12. After the operation completes, the SATA drives will remain powered ON but can be safely removed without the need to power off the unit. It would be necessary to power off the unit prior to removing M.2 drives. The simulated drive status LEDs will be set to GREEN if the operation passes or RED if the operation fails.

WipeOut-User SETTINGS

Table 10

Menu Item	Recommended Setting
Copy Mode	**WipeOut**
ReadBack-Verify	**Disable** (Optional)
WipeOut Mode	**User**
Iterations	**1**
Pattern	**0**

Transferring Audit Trail and Log Information

The following section describes the procedure to transfer Audit Trail and Log information from the unit's internal storage to an External USB Storage Device.

1. Select *Tools*  from the Main Menu.
2. Select *Logs* from the Tools Menu or the *Result* Screen.
3. Select *Copy Logs to a Removable Device*. A message will be displayed prompting the User to insert a USB Storage Device in the Target Position.
4. Insert a USB Storage Device into the unit's General Purpose USB port. Select **OK** to continue.
5. The USB Storage Device Volume will be mounted and the Device will be listed in the **Other Detected Drives Panel**. Disregard the Windows AutoPlay prompt if displayed and wait for the prompt indicating *Select Files to Copy*. Select the Event Log and Audit file(s) to copy.

   NOTE: If the USB Device is not properly detected, remove the USB Device and repeat steps 2-7.
6. Select **OPEN** from the *Select Files to Copy* prompt, to continue.
7. Select the destination folder on the USB Device to store the selected file(s) and select **OK** to store the selected files.
8. The USB Storage Device can be removed after the Device is removed from the *Other Detected Drives Panel*.

NOTE: Audit Trails are saved in both a standard text format and a PDF format using 128-bit password encryption protection, so the Audit Trail contents cannot be changed. The Company Logo can be added to the Audit Trail PDF by selecting its location using the "SET AUDIT TRAIL LOGO" function, located in the LOG menu screen.

Previewing Write-Protected Drive Data

The following section describes the procedure to securely view data from the drive(s) connected to the MM NVMe M.2 ports.

1. Connect and configure the drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.
2. Select *Run*  from the Main Menu to access the *Drive Selection* Screen and select the drives to be used for the selected operation.
3. Select *Next*  from the *Drive Selection* Screen to access the *Drive Detection* Screen and select *Detect Drives*.
4. Highlight and Select the drive to be previewed from the *Drive Status* Panel.
5. Select the *Mount Drive* function from the Drive Detect Tools Menu.
6. Verify that the *Write-Protect* function is Enabled (checked) in the **Mount Drive** Screen Menu.
7. Select (check) the *Mount Volumes* setting in the **Mount Drive** Screen Menu.
8. Select the **NEXT** Button. This operation will allow preview access to the drive's volume using the unit's O/S or 3rd party application.
9. Select the **DESKTOP** Button to preview the drive's volume.
10. To remove the drive after accessing the drive's volume, select **REMOVE DRIVES** from the *Drive Selection Screen*.

Enabling Manual Write-Access to Target Drive Positions

The following section describes the procedure to allow write operations to be performed manually to drives connected in the Target drive positions.

1. Connect and configure the Target drives as outlined in the *Quick Start* and *Prepare for Operation* sections of the manual.
2. Select *Run*  from the main menu to access the *Drive Selection* Screen and select the drives to be used for the selected operation.
3. Select *Run*  from the *Drive Selection* Screen to access the *Drive Detection* Screen and select *Detect Drives*.
4. Highlight and Select the drive to be previewed from the *Drive Status* Panel.
5. Select the *Mount Drive* function from the Drive Detect Tools Menu.
6. Select (check) the *Mount Volumes* setting in the **Mount Drive** Screen Menu. De-Select (uncheck) the *Write-Protect* setting in the **Mount Drive** Screen Menu.
7. Select **NEXT** Button. This operation will allow preview and write access to the Target drive's volume using the unit's O/S or 3rd party application.
8. Select **DESKTOP** Button to access the drive's volume.
9. To remove the drive after accessing the drive's volume, select **REMOVE DRIVES** from the *Drive Selection Screen*.

Appendix A: Operational Notes

Media MASSter™ NVMe M2 Pro Internet/Network Connection Disclaimer

Intelligent Computer Solutions, Inc. (ICS) assumes no liability for the security of the customer's computer/network systems. ICS assumes no liability for the security of the Media MASSter™ when it is connected to either the Internet or another Network. Utilizing the Media MASSter™ for data seizure from a network or uploading data to a network requires the unit to be connected to the network and this may cause a risk of the system being compromised. The user is responsible for taking the necessary steps to ensure the safety of both the Media MASSter™ and the network in use when the unit is utilized to either seize or upload data to/from a network.

The security of the Media MASSter™ when connected to the Internet or a network relies on the user's discretion; however, ICS recommends, at a minimum, to the user to take the following steps:

1) The Media MASSter™ is set to have Internet Connection and Automatic Windows Updates disabled as default. Users will need to enable Internet Connection when seizing or uploading data from/to a network. It is highly recommended that the user install ***anti-virus*** and ***firewall Hardware Device*** protection prior to connecting the Media MASSter™-102 to either the Internet or a network. A lesser protection can be achieved with ***personal firewall software***. Continuously running an updated version of anti-virus software with the Media MASSter™ may help prevent an intrusion into the unit or network. ICS recommends updating the ***anti-virus software program*** every time the Media MASSter™ is connected to the Internet or a network.

2) Users should always utilize a clean (scanned for viruses) USB Thumb Drive when updating the Media MASSter™ unit Software or Firmware.

3) Users should ***ONLY*** connect the Media MASSter™ to a network when either seizing or uploading data. It is imperative for users to ***REMOVE*** the Media MASSter™ connection when not actively performing these tasks.

These recommendations are provided to the user as a reference; however ICS cannot assure that the Media MASSter™ will not become compromised when connected to the Internet or a network. User assumes all responsibility for the data and security of the Network.

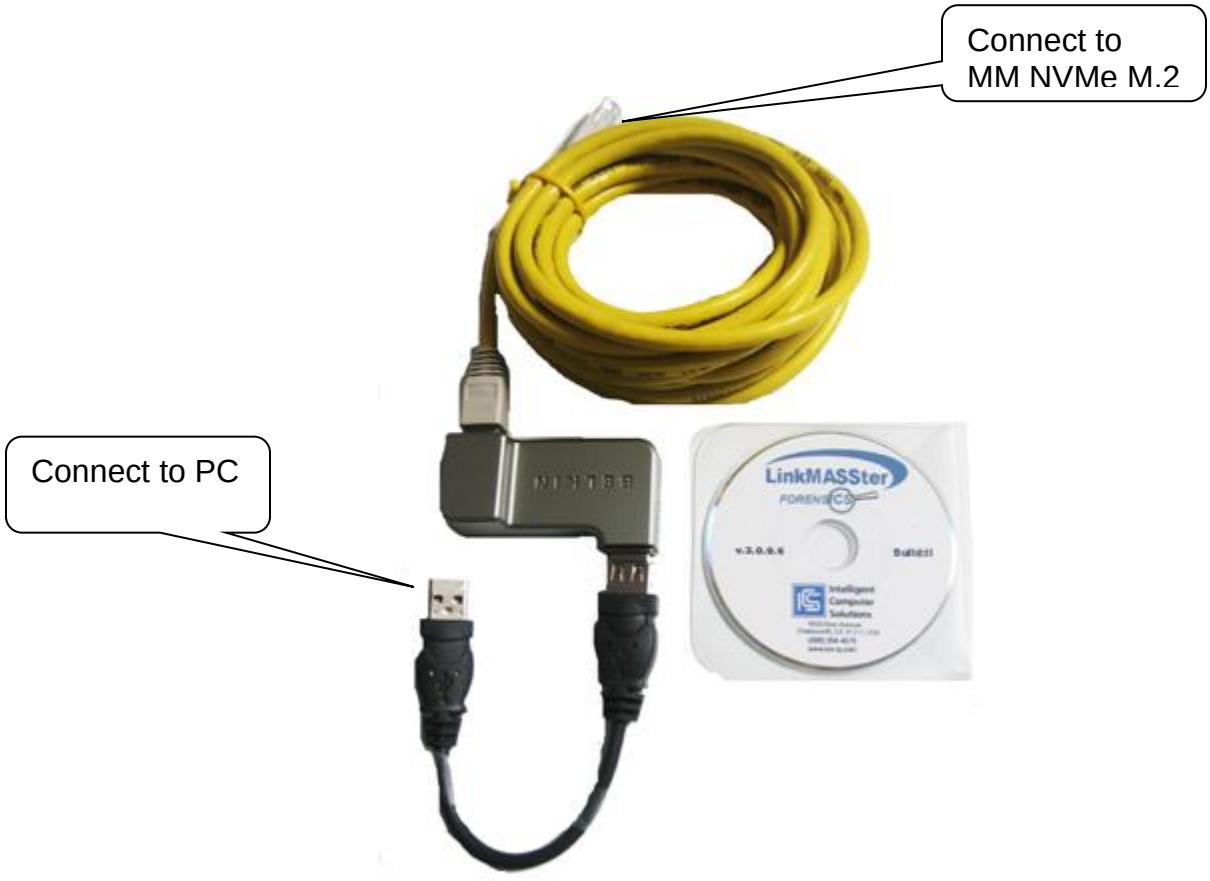
Customers understand and agree that the use of the Media MASSter™ implies acceptance to the terms and conditions specified in this disclaimer.

LinkMASSter USB-to-Ethernet Connection

The MM NVMe M.2 LinkMASSter Option will also include a *Gigabit USB-to-Ethernet Network Adapter* (CSAR-0265-000A) to allow connecting to a Notebook or PC which does not have an Ethernet port, or if drivers are unavailable for the computer's network interface. For improved performace, the *Gigabit USB-to-Ethernet Network Adapter* would also be recommended when connecting to a Notebook or PC which uses an Ethernet interface that offers less than a 1 Gigabit connection.

NOTE: When using the *Gigabit USB-to-Ethernet Network Adapter*, connect the Ethernet connector to the MM NVMe M.2 unit and connect the USB connector to the computer.

1. Connect the ICS supplied *Crossover Ethernet Cable* to the MM NVMe M.2 unit's Ethernet port.
2. Connect the *Crossover Ethernet Cable* to the *Gigabit USB-to-Ethernet Network Adapter*.
3. Connect the ICS supplied USB 8" Cable to the *Gigabit USB-to-Ethernet Network Adapter*.
4. Connect the USB 8" Cable to the Notebook/PC USB port.



MM NVMe M.2 USB FLASH RESTORE INSTRUCTIONS

The following are instructions to restore the unit's System Drive contents.

The following hardware is required:

- ICS Supplied USB Restore Drive.
- USB Keyboard.

1. Insert the MM NVMe M.2 USB Restore drive to one of the available general purpose USB ports, located on the back of the unit and connect a USB Keyboard.
2. Access the MM NVMe M.2 Boot Device Selection menu by pressing <F12> during Power ON when the POST Startup Screen is displayed.
3. Highlight and selected the listed USB Device.
4. Type "Restore" after the unit boots from the USB Restore drive. Type 'Y' to start the Restore process. The Restore process will take approximately 7 minutes. When the message is displayed indicating "Success," power off the unit and reboot.

   NOTE: The request to type "Y" is Case Sensitive. The operation will wait until the proper key is entered.
5. After the unit reboots, Windows SETUP will run for approximately 7 minutes.
6. Copy the following files from the USB Restore media to the unit's system drive C:\Support Files folder.

   a. s4v4.12.xxx.0 Setup_x64.msi

   b. icsflt.sys
7. Install the unit's ImageMASSter application by running s4v4.12.xxx.0 Setup_x64.msi..
8. Copy the icsflt.sys file, located in the root directory of the supplied USB Restore media or located in the unit's system drive C:\Support Files folder, into the unit's system drive C:\Windows\System32\Drivers folder.

   a. Select "Yes" to over write the existing file.

   IMPORTANT NOTE: The icsflt.sys driver must be updated to ensure proper operation.
9. Power cycle the unit.

NOTE: It would be required to activate the Windows License using the supplied Windows License Key after the Restore process completes.

DEFINITIONS

HASHING

Hashing is a process that calculates a "unique signature" value for the contents of an entire drive.

MD5 Hash

Message Digest Algorithm is a 128-bit cryptographic hash function.

SHA-1

Secure Hash Algorithm is a 160-bit cryptographic hash function. Designed by the NSA.

SHA-2

Variant of SHA-1 with increased output ranges. Secure Hash Algorithm-2 is a 256-bit cryptographic hash function.

CRC32

Cyclic Redundancy Check Algorithm based on a 32-bit size hash value.

Sanitize

Sanitize refers to the process of clearing a drive of all previously stored data. The WipeOut function can be used to sanitize a drive.

NVMe

Non-Volatile Memory Express is a protocol developed for flash memory to operate using the PCIe interface as an SSD drive.

M.2

M.2 is a form factor for non-volatile flash memory devices such as SSD drives. The M.2 form factor requires an M.2 connector.

M.2 SATA Drives

M.2 SATA drives use the M.2 form factor with the SATA interface. M.2 SATA drives normally use the M.2 ‘M’ and ‘B’-Keys as shown below and are designed for the SATA interface.

M.2 PCIe Drives

M.2 PCIe drives use the M.2 form factor with the PCIe interface. M.2 PCIe drives normally use the M.2 ‘M’ Key as shown below and are designed for the PCIe interface.

Host Protected Area (HPA)

HPA is defined as a reserved area for data storage outside the normal operating file system. This area is hidden from the operating system and file system and is normally used for specialized applications. Systems may wish to store configuration data or save memory to the hard disk drive device in a location that the operating systems cannot change. If an HPA area exists on a Source drive, the MM NVMe M.2 Pro seizure operation will detect this area and capture all the contents of the drive’s sectors, including all the HPA hidden sectors, to the Target drive.

Device Configuration Overlay (DCO)

DCO allows systems to modify the apparent features provided by a hard disk drive device. DCO provides a set of commands that allows a utility or program to modify some of the modes, commands and feature sets supported by the hard disk drive. DCO can be used to hide and protect a portion of the drive's area from the operating system and file system. If DCO is detected on a Source drive, the MM NVMe M.2 Pro seizure operation will capture all the contents of the drive's sectors, including all the DCO hidden sectors, to the Target drive.

Advanced Encryption Standard (AES)

AES is a 128-bit block cipher Encryption Standard, which supports a choice of three key sizes (128, 192 and 256-bits) according to the level of security required. AES has become the encryption algorithm of choice for applications requiring a high degree of data security.

AES Modes

AES Modes provide a method of implementing different AES properties. The AES modes are described as follows:

- Electronic Code Book (ECB)

  The message is divided into blocks and each block is encrypted separately.

- Cipher Block Chaining (CBC)

  Each block of plaintext is XORed with the previous ciphertext block before being encrypted.

- Cipher FeedBack (CFB)

  Makes a block cipher into a self-synchronizing stream cipher. A stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream), typically by an xor operation.

- Output FeedBack (OFB)

  Makes a block cipher into a synchronous stream cipher: it generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext

- Counter (CTR)

  Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter".

Appendix B: Product Information

Limited Warranty

Intelligent Computer Solutions, Inc. warrants that our products are free from defects in materials and workmanship for a period of twelve (12) months from the date of purchase by the **original buyer**. If you discover physical defects or malfunction, Intelligent Computer Solutions, Inc. will, at our discretion, repair or replace the product. You must return the defective product to Intelligent Computer Solutions, Inc. within the warranty period accompanied by an RMA number that has been issued by Intelligent Computer Solutions, Inc.

All products purchased from *Intelligent Computer Solutions, Inc.* include a seven-day unconditional money-back guarantee.

Intelligent Computer Solutions, Inc.'s products are shipped in cardboard boxes that have been designed and tested to ensure that our products can endure standard commercial shipping methods and still arrive in working order. We advise you to save your box and original packing materials in case you need to return the product(s) for any reason. If product(s) are returned without proper protective packaging, the warranty may be void.

When you received your product(s), please note the following:

-That the shipping box does not have dents or visible damage.
-What you have received conforms to the packing list.
-There is no apparent damage to the product(s) or accessories.

If any shipping damage is found:

-Please contact the shipper immediately to inspect.
-Please contact our Technical Support Department to report the damage.

What is Not Covered:

This limited warranty provided by *Intelligent Computer Solutions, Inc*. does not cover:

- Products which have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, or if repaired or serviced by anyone without prior authorization from Intelligent Computer Solutions, or if the model or serial number has been altered, tampered with, defaced or removed.
- Normal maintenance.
- Damage that occurs in shipment due to act of God and/or cosmetic damage.
- Accessories

Please note that External cables are covered by a 30-day warranty.

This Agreement also does not include service (whether parts or labor) necessitated by any natural cause such as flood, tornado, earthquake or other acts of nature.

Limitation of Liability

The following limitations of ICS liability apply:

ICS is not liable for any incidental or consequential damages, including, but not limited to property damage, loss of time, loss resulting from use of an ICS product, or any other damages resulting from breakdown or failure of a serviced product or from delays in servicing or inability to render service on ICS product. ICS will make every effort to ensure proper operation of its product. It is, however, the Customer's responsibility and obligation to verify that the output of ICS product meets the Customer's quality requirement. Customer acknowledges that improper operation of ICS product and/or software, or hardware problems, can cause defective formatting or data loading to target drive. It is the customer, not ICS, who is responsible for verifying that the drive meets the Customer's quality standards. ICS will make efforts to solve any problems identified by Customer.

Technical Support

For help in resolving a problem, contact *ICS Technical Support* at:

Phone: 1-818-998-5805 between 8 a.m. and 6 p.m. Pacific Time.

Please be prepared with the following information:

- ✓ serial number of the MM NVMe M.2 unit
- ✓ nature of the problem
- ✓ steps you have taken
- ✓ your phone and fax numbers
- ✓ error messages displayed on the screen