

Image MASter Solo 4 Forensic

Portable Forensic High Speed Data Acquisition Tool with built-in SAS

Features:

• Extreme Speed

Captures, authenticates and sanitises at full UDMA-6 speed (exceeding 7GB/min (with newest fastest SAS drive)

• Multiple "suspect" side connections

- 2 SATA/SAS connections and 1 USB 2.0 connection. Unit features built-in support imaging of a RAID drive pair (0, 1, JBOD).
- Optional Drive Adaptors will allow imaging of IDE drives, 1.8", 2.5", ZIF and proprietary interface/laptops drives, and Micro Media Formats including Compact Flash, Memory Sticks, SD, Micro SD, Multi Media Card, etc.
- Cross Copy Support allows user to image any "suspect Drive interface to any "Evidence" Drive interface.
- All Suspect connections are permanently write-protected at all times to prevent changing Suspect Data (can not be disabled).



• Multiple "Evidence" side connections

2 SATA/SAS connections & 2 USB2.0 connections. Optional Drive Adaptors will allow imaging to many other drive formats including external RAID devices.

• Drive Spanning

Solo 4 allows for the imaging from one large "Suspect" drive to multiple smaller "Evidence" drives.

Features:

• Operational Modes

- Captures "Suspect" drive to one "Evidence" drive (Single Copy Mode).
- Captures "Suspect" drive to two "Evidence" drives (Multi Copy Mode).
- Captures 2 "Suspect" drives to two "Evidence" drives (Parallel Copy Mode).
- Drive Wiping and sanitisation.
- Drive Hashing (MD-5, SHA-1 and SHA-256).
- Uploads suspect images to Network Storage and/or any attached Network Share.
- All processes are done simultaneously with no speed degradation.

• Multiple Imaging Formats

- 100% Copy: Bit-for-bit copy.
- Linux DD: Supports storing single or multiple DD images (industry standard) on a single "Evidence" Hard Drive or USB storage device. User can define the size of the Linux DD segments.
- IQ Copy: Captures actual "data only" greatly reducing the time needed to make a non-forensic copy for back-up or mass duplication purposes.
- Support for E01 files

"On the Fly" Drive Image Encryption

Built-in DiskCypher technology allows the full encryption (AES256) of Forensic Images. The process is done without speed degradation during the acquisition phase.

• Windows Embedded Standard Operating System

Solo-4 runs on the highly stable and proven Windows Embedded Standard Operating System.

- Unit can be customisable to many different languages.
- Unit can be customised for individual organisation needs upon request.
- Automatic Support to many PC peripherals.

• Linux DD Image Restore

Restore a previously captured DD image to a 100% copy (fully bootable working copy).

Data
Duplication Ltd

4 Station Approach, Wendover, Bucks HP22 6BN
Tel: 01296 621121 Fax: 01296 621125
e-mail: info@dataduplication.co.uk
www.dataduplication.co.uk

Features:

- **Drive Wiping**

Supports single pass drive wiping or full Department of Defence (DoD) Sanitisation.

- **Intuitive Easy to Use Interface**

8" Full Colour, User Friendly Touch Screen eliminates the need of external display, mouse, or keyboard. The user interface provides three graphical levels and the operational wizard allows user to easily operate the unit. The advantage settings mode can also be selected for low level control.

- **Unalterable "Suspect" Interface Write Protection**

ICS recognises the industry standard and permanently write protects any device connected to the Solo-4 "Suspect" position thereby preventing any unintentional alteration of suspect Data. Data alteration could occur if a device allows the user the option of turning off this protection mode.

- **Multiple Hash Verifications**

All "Suspect" and "Evidence" positions allow Multiple Hash Verifications including SHA-1 and SHA-256 during the acquisition process simultaneously and without speed degradation.

- **Uploads Suspect Images to Network Storage or any attached Network Share**

With the use of Windows Embedded Standard Operating System Solo-4 allows the upload of Suspect Data Images to networked storage area using a built-in 1 Gigabit Ethernet connection. This will allow user to take advantage of large storage repositories (SAN) for the purpose of processing and archiving forensic images.

- **Preview Suspect Data Directly on the Unit**

Preview active files on the Suspect Drive utilising a built-in file viewer that allows previewing Word, Excel, PDF, text or multimedia (pictures, video and audio) files prior to seizing the data. Unit also features a built-in Audio Head Phone Jack for discreet listening.

- **Drive Block Functionality for use with a Forensic Workstation**

Utilising the "Suspect" "always on" write protection connections Solo-4 can be attached to a Forensic Workstation via USB connection to allow the preview, capture or analysis of Suspect Data in a safe environment.

- **USB Card Reader Support**

Supports Micro Media Formats (Compact Flash, Memory Sticks, SD, Micro SD, Multi Media card, etc) expanding the option of types of "Suspect" Media that can be previewed, analysed or captured.

- **Data Integrity Check**

Read back verification of the two "Evidence" drives for extra data integrity checking.

- **Field Upgradable**

Free and easy to update firmware and software through USB port.

- **Logs and Auditing**

Complete and accurate auditing of all unit processes are provided in text file format that can be exported via USB connection.

Other Products:-

- Forensic Tools

- Hard Disk Duplicators

- Floppy Disk Copiers

- CD Duplicators

- CD Printers

Media Duplication Services For:-

- Blank Media Supply

- Floppy Disk

- CD

- DVD

- Tape

- Standard or Customised Packaging

- Fulfilment Service