



**Intelligent
Computer
Solutions**

Make the intelligent choice...

FEATURES:

- 1 Extreme Speed
- 2 Multiple "Suspect" side connections
- 3 Multiple "Evidence" side connections
- 4 Multiple Operational Modes
- 5 Multiple Imaging Formats
- 6 Multiple File Format Support
- 7 "On the Fly" Drive Image Encryption
- 8 Windows XP Operating System
- 9 Drive Spanning
- 10 Image Restore
- 11 Drive Wiping
- 12 Intuitive Easy to Use Interface
- 13 Unalterable "Suspect" Interface Write Protection
- 14 Multiple Hash Verifications
- 15 Upload Suspect Images to Network Storage or any attached Network Share
- 16 Preview Suspect Data Directly on the Unit
- 17 Drive Block Functionality for use with a Forensic WorkStation
- 18 USB Card Reader Support
- 19 Data Integrity check
- 20 Field Upgradable
- 21 Logs and Auditing
- 22 Affordable

Hand-Held Duplicators

Image MASter™

Solo-4

A "Quantum Leap" forward in Forensic Imaging technology

This "Next Generation" device from the legendary Image MASter product line brings value, versatility, speed and cutting edge features with a simple "State-of-the-Art" user interface.



**Now Supports
E01
file format**



www.ics-iq.com

www.icsforensic.com

Image MASter Solo-4

A “Quantum Leap” forward in Forensic Imaging technology.

This “Next Generation” device from the legendary Image MASter product line brings value, versatility, speed and cutting edge features with a simple “State-of-the-Art” user interface.

FEATURES

1 **Extreme Speed Built for Today’s and Tomorrow’s Hard Drive Technology**

Built to work with the fastest hard drives available, Solo-4 captures, authenticates, and sanitizes at full SATA-2 speed (18GB/ min top capability). This technology not only allows the unit to take advantage of today’s fastest hard drive speeds but also allows the user to be prepared for tomorrow’s future hard drive speed improvements.

2 **Multiple “Suspect” Side Connections**

- 2 SATA/SAS connections and 2 USB 2.0 connection. (Operator can choose to use either the SAS/SATA connection or the USB connection for each of the two “Suspect” positions)
- Unit features built-in support for imaging of a RAID drive pair (0, 1, JBOD).
- IDE Drive Adapter included.
- Optional drive adapters for 1.8”, 2.5”, ZIF, and proprietary Interface /Laptop 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. (ie. IDE “Suspect” drive to SATA “Evidence” drive)
- All Suspect connections are permanently write-protected at all times to prevent changing Suspect Data (can not be disabled).

3 **Multiple “Evidence” Side Connections**

2 SATA/SAS connections and 2 USB 2.0 connections. Optional Drive Adapters will allow imaging to many other drive formats including external RAID devices.

4 **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 Sanitization
- Hashing (MD-5, SHA-1 and SHA-2) of “Suspect” Hard Drive and Linux DD Images
- Uploads suspect Images to Network Storage and or any attached Network Share.
- All processes can be done simultaneously

5 **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.
- E01 files: Supports imaging to EnCase® Forensic Image file.
- Drive Images: allows storing of multiple source images on a single hard drive or Shared Network folder using “Segmented” File formats or using the Microsoft Virtual Hard Drive (VHD) image format.

6 **Multiple File Format Support**

Seize Data using Raw Mirror Capture Format, Raw Segment File Format or Encase (E01) File Format. The Mirror Capture Format transfers data to the Destination drive using the same LBA location which was read from the Source Drive . The Raw Segment File Format creates an NTFS partition on the Destination Drive and transfers data as Raw Segment files to a Destination folder. The Encase (E01) Segment file format creates an NTFS partition on the Destination drive and transfers data using the Encase Segment file format, to a destination folder. The Segment files size can be defined as 640 MB, 1GB, 2GB, 4.7GB, Whole Drive or Custom Size.

7 “On the Fly” Drive Image Encryption

Built-in DiskCypher technology allows the full encryption (AES 192/256) of Forensic Images. The process is done without speed degradation during the acquisition phase.

8 Windows Operating System

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

- Unit can be customizable to many different languages.
- Unit can be customized to individual organization needs upon request.
- Automatic Support to many PC peripherals.

9 Drive Spanning

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

10 Image Restore

Restore a previously captured Linux DD or E01 image to a 100% copy (fully bootable working copy).

11 Drive Wiping

Supports single pass drive wiping, or full Department of Defense (DoD) Sanitization, and the Secure Erase feature supported by many of today’s modern drives.

12 Intuitive Easy to Use Interface

8” Full Color, 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.

13 Unalterable “Suspect” Interface Write Protection

ICS recognizes 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.

14 Multiple Hash Verifications

All “Suspect” and “Evidence” positions allow Multiple Hash Verifications including SHA-1 and SHA-2 during the acquisition process simultaneously and without speed degradation.

15 Upload Suspect Images to Network Storage or Any Attached Network Share

With the use of Windows 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.

16 Preview Suspect Data Directly on the Unit

Preview active files on the Suspect Drive utilizing Windows file viewers that allow previewing 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.

17 Drive Block Functionality for use with a Forensic WorkStation

Utilizing 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.

18 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, analyzed or captured.

19 Data Integrity check

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

20 Field Upgradable

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

21 Logs and Auditing

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

22 Affordable

Unparallel performance and built-in features at an affordable price makes Solo-4 the perfect and most complete forensic solution for any investigator today.

PRODUCT SPECIFICATIONS AND ADDITIONAL OPTIONS FOR SOLO-4 FORENSIC

SOFTWARE SUPPORT OPTIONS

- HPA/DCO
- Bad sector management
- Multi Images support
- Multi language support
- Image Formats
 - 100%
 - linux DD
 - E01 (EnCase® format)
 - VHD
- File Systems
 - FAT
 - NTFS
 - Linux
 - HFS+ (MacOS)
 - UDF

OPTIONAL GADGETS

- USB GPS receiver.
- Bluetooth GPS.
- Miniature Keyboard.
- Miniature USB Hub.
- Small Speakers.
- 1.8" Adapter.
- ZIF Adapter.
- Micro SATA Adapter.
- USB (12-in-one) Memory Card Reader.
- USB Wi-Fi Card.

UNIT SPECIFICATIONS

Unit Net Weight: 5.35 LBS

Overall Dimensions:

10.6"W x 3.8"H x 7.7"D (270 x 98 x 194 mm)

- PCI-e expansion box: Equipped with 3 PCI-e one lane expansion slots (Cards limited to 12 volts per slot) for upgradability and additional device support.
- The expansion box includes:
 1. PCI-e SCSI 320Mbit/sec Controller, for SCSI drive support (Additional adaptors may be required).
 2. PCI-e FireWire Controller with two 1394B ports and 1394A port
 3. PCI-e Express Card Reader controller for use with Express Memory Card (not USB based card) or other express plug in cards.

Individual Controllers can be replaced with special purpose controller such as WiFi card.

HARD DRIVE SUPPORT

- E-SATA drives.
- SAS drives all kinds.
- SATA drives all kinds.
- USB drives all kinds.
- IDE drives with included ICS IDE to SATA Adapter.
- Micro SATA drives with optional ICS Micro SATA Adapter.

External devices that require power need to be powered from external power source.

- Open Drive Tray
- IDE Host and Drive Caddy
- 2.5"/1.8" Host and Drive Caddy
- 3.5" Host and Drive Caddy
- Optional Adapters for e-SATA drives, IDE drives, Micro SATA drives, 2.5", 1.8" Notebook drives and ZIF drives
- Solid State Express Card Drive
- Memory card reader (12-in-one)
- USB Mini Keyboard
- Miniature USB Hub
- USB to Wi-Fi

Drive Tray and Fan

LinkMASster Option to capture data from unopened PCs and Laptops.

- 2.5" Drives with included ICS 2.5" Adapter.
- 1.8" Drives with optional ICS 1.8" Adapter.
- ZIF drives with optional ICS ZIF Adapter.
- Notebook drives with optional ICS Notebook Adapter.
- Solid State Drives all kinds.
- SD series /MS series/XD/M2/TF/CFI/CFII.

WARRANTY

One Year Parts and Labor.

Second Year Extended

Warranty

ABOUT INTELLIGENT COMPUTER SOLUTIONS, INC.

ICS is a pioneer in disk drive duplication, having first introduced this technology to the world in 1991, in a US patented device. For over seventeen years ICS has been focused on providing cutting-edge solutions to the state, local and federal government Law Enforcement communities and the growing, private digital forensics investigation sector. These tools include the leading digital forensics hardware and software technology used in some of the most complex digital forensics investigations today which include, Handheld Forensic Duplicators, Forensic Portable Stations, Hard Drive Encryption, Hard Drive Sanitization Stations, Write Protectors and more.



**Intelligent
Computer
Solutions**

**9350 ETON AVE.
CHATSWORTH, CA 91311
PHONE: (888) 994-4678
FAX: (818) 998-3190
WWW.ICS-IQ.COM
WWW.ICSFORENSIC.COM**