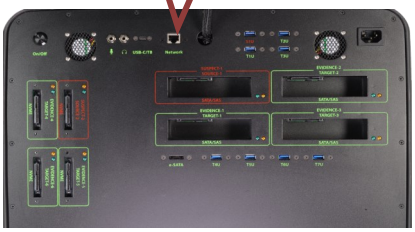
SuperImager® Plus Portable Rugged Forensic Lab

A Digital Forensic Imaging & Complete Investigation Platform

Configured with Dual Open OS, Linux for Forensic Imaging & Windows 10 For Forensic Analysis & Cellphone capture

With the use of one unit (Cost-effective):

- ◊ Capture data simultaneously from many "Suspects" hard disk drives and SSD with different storage interfaces at extreme speed.
- ◊ Run Virtual Drive Emulator on "Suspect" drive
- ◊ Run Multiple Cellphones Data Extraction
- ◊ Run Full Forensic Analysis, Triage, RAID re-construing other useful applications
- ◊ Efficient Parallel Imaging sessions with 3 HASH engines, Encryption, E01 compressing, Keyword Search - all on the fly



Part #: SIR-0050. The Main Hardware Built and Features:

- Portable Rugged Carrying Case
- **15.6" color LCD Display**
- **4 U.2 NVMe ports (Including M.2 NVMe vertical adapters)**
- **4 SAS/SATA ports in drive's slots**
- **8 USB3.2 Gen-2 (10Gigabit/s) ports, Thunderbolt 4 (USB-c) port**
- **10 Gigabit Ethernet**

The Linux SuperImager Forensic Application:

- **Simple user interface with easy navigation icons and screens.**
- **Supports multiple sessions in parallel independent operations.**
- **Optimized for Multiple Core CPU, with multi-threading to achieve extreme speed, especially when running E01 format compression operation.**
- **Flexible in re-assigning the role of Evidence port to be Source for network images upload or for multi imaging.**
- **Mix operations such as HASH, Erase, Capture data from digital storage devices all in multiple sessions operation with no limitation on the number of sessions.**
- **Capture Methods: Mirror Imaging, VHD, Linux-DD, Triage Files.**

Dual Open OS

For Data Capture:

- ♦ Perform Forensic Imaging under most efficient Linux OS for a faster & more secure operation.

To Analyze the Captured Data:

- ♦ Use a third-party applications to perform data analysis, cellphone extraction and other useful application.
- ♦ Supports: HDD, SSD
- ♦ Supports:, SAS/SATA/NVMe/USB

MediaClone, Inc. 6900 Canby Ave, Unit 107, Reseda, CA 91335 Tel: 818-654-6286 www.media-clone.net, info@media-clone.com

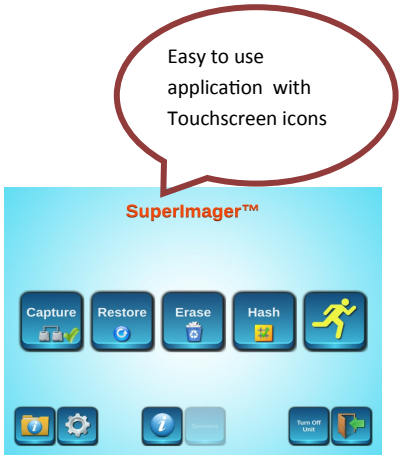
SuperImager® Plus Rugged Portable Forensic Lab

FEATURES

- Drives form factors: 2.5”, 3.5”, MSATA, Micro SATA, M.2, U.2
- USB3.2 ports can be converted to SATA ports with the use of USB to SATA adapters
- Preview data of the “Suspect” drive in a secure environment
- Captures and saves images across many ports and interfaces
- Forensic image from multiple “Suspect” drives to one large “Evidence” drive
- Standalone HASH authentication engines MD5/SHA1/SHA2 on a drive or captured image
- Imaging and Verify: The user can select to run forensic imaging with 3 HASH engines and also enable the "HASH the target and compare HASH" feature. That is kind of a stand operation to make sure the captured image is not altered or corrupted. Reading speed from a source drive (32GB/min SATA, 202GB/min NVMe).
- Targeted Imaging: Sometimes the forensic investigator does not have the time to do a full data capture of the Suspect drive. Now the user can use the Selective Imaging feature to select only partitions, files, or folders (like the Windows User-Folders or Windows User-Documents and User-Pictures). With the use of preset file extension filters or adding its own filters, the Forensic Investigator can narrow their capture scope and shorten its acquisition time.
- Drive Spanning: Supports spanning the captured data onto many “Evidence” drives when the Evidence drives are not large enough (also supports restore images that are spanned over multiple drives). Also support parallel drive spanning when the source drive is much faster than the target (for example when source is NVMe).
- Encryption: AES256 on-the-fly and decrypt at remote location
- Network: Save Images (DD, E01) to Network (NFS, CIFS, SAMBA)and capture from a Network via iSCSI storage protocols. An easy upload setting to upload captured images from 8 ports to 10Gigabit network
- Capture Modes: bit by bit mirror copy, Linux-DD, E01,/EX01 with up to 16 compression engines, Mix E01 and DD, Files and Folders, VHD.

To use the unit as a platform the user can:

- Run a third-party Cellphone/Tablets Data Extraction and Analysis tools
- Complete a full field investigation by running Encase, FTK, Axion, ADF, Nuix, Forensic Explorer, and many more



MediaClone, Inc. 6900 Canby Ave, Unit 107, Reseda, CA 91335 Tel: 818-654-6286 www.media-clone.net, info@media-clone.com