

















HDD DATA RECOVERY LAB TOOLS:

APPLIES TO

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| CAR INFOTAINMENT  | CCTV - DVR  | LAPTOP  | SERVER  | USB HDD  | NAS UNIT  | WORKSTATION  | INDUSTRIAL MACHINE  |
| SMARTPHONE  | GPS  | SIM CARD  | DRONE  | DASH CAM  | FLASH CARDS  | DIGITAL CAMERA  | USB PENDRIVE  |

Hard Disk Drives are actually installed on many different devices like car infotainment systems, CCTV and DVR, laptop, servers, USB HDD, NAS units, desktop computers, industrial machines etc. The first step in forensic analysis is acquisition of a target

GENESIS ADVANCED IMAGER

It's a hardware and software complex able to copy SATA drives connected to source channels (according to the model can be 1,2 or 4 channels) performing a sector level copy to a physical drive target or ISO image file, with advanced utilities for the following brand and series:

- WESTERN DIGITAL ROYL series
- SEAGATE F3 series
- HITACHI / HGST series (ARM CPU)
- SAMSUNG SATA drives
- FUJITSU SATA drives
- TOSHIBA SATA drives

GENESIS PC Version is composed by a PCI express card, 1 USB box (5,25" bay) for power on/off and comport communication with the drives.



The kit includes the controller, adapters, all the main utilities for copying with firmware access.

This tool works in AHCI SATA3 standard with 64bit drivers (Windows™ 10) in order to ensure greater stability and to maximize performances.

GENESIS software includes firmware support to skip heads and ATA passwords, cloning and mount (in read only mode)

Source channels are write protected to ensure forensically sound copy to be validated through ASH Code. With Genesis is possible to copy drives locked by ATA password as some DVR/CCTV protected drives, manage bad sectors and read errors.

Genesis max supported speed is SATA III native (6 Gb/s), with AHCI support to let the controller manage hdd instability issues.

Friendly user graphic interface makes easy to create image file or physical copy to load into extraction software.

With genesis is possible to stop a task and resume when needed without starting each time from zero, a map of skipped sectors will be created for report creation



E.D.R. TOOLS SRL

for Digital Forensics & Data Recovery

head office: viale Giovanni Paolo II, 15/4 - 33100 UDINE (ITALY)

headquarters: via Roveredo, 20/B - 33170 PORDENONE (ITALY)

www.edrtools.eu info@edrtools.eu

Genesis will copy HDDs at a sector level checking (through firmware) real size allowing to image Hidden area by DCO or HPA, the result can be a physical drive to drive copy or an ISO image file as selected by the operator during task creation.

VENDOR SPECIFIC and GENERIC utilities:

the imaging software can be splitted into “generic” and “vendor specific” utility.

With the generic option we can image any hdd using SATA standard both mechanical and SSD drives, with this utility the tool will manage drive reading unstability creating maps for skipped or unreadable sectors letting the examiner create a first “gross” copy skipping bad sectors and bad areas and then refine the copy in the following passes. Genesis will parse the skipped and unread sectors maps in order to copy only needed sectors and areas, this way is possible to use different reading settings for each pass and to stop and then finish on a second time and already saved task.

Hash code can be created after finishing the copy such as a report with all the operations related to the task.

The Vendor Specific Utility in addition to the features of the Generic version, has further advanced functions related to the brand of the disk allowing, through firmware access, to disable ATA passwords set by the bios of a computers or by devices such as video decoders or some DVRs.

A data recovery option present in the vendor specific utility is selecting which heads to use for copying by modifying the reading settings based on the operating status of the single head.



EDRTOOLS
for Digital Forensics & Data Recovery

E.D.R. TOOLS SRL

for Digital Forensics & Data Recovery

head office: viale Giovanni Paolo II, 15/4 - 33100 UDINE (ITALY)

headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)

www.edrtools.eu info@edrtools.eu