Singapore | Indonesia | Malaysia | Thailand | Philippines | South Korea
Hong Kong | Macau | Shenzhen | Guangzhou

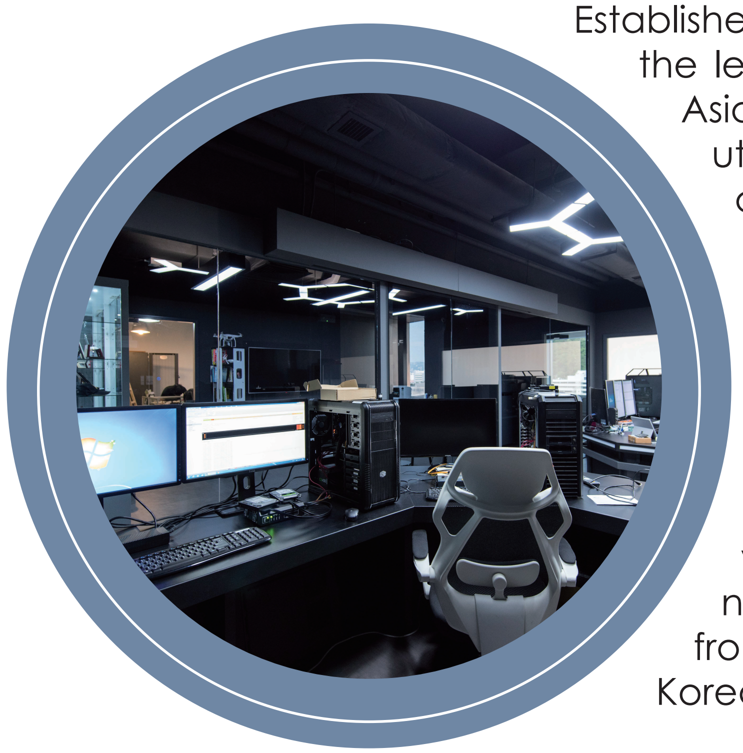
www.dataexpert.asia

enquiry@dataexpert.asia

Company Brochure

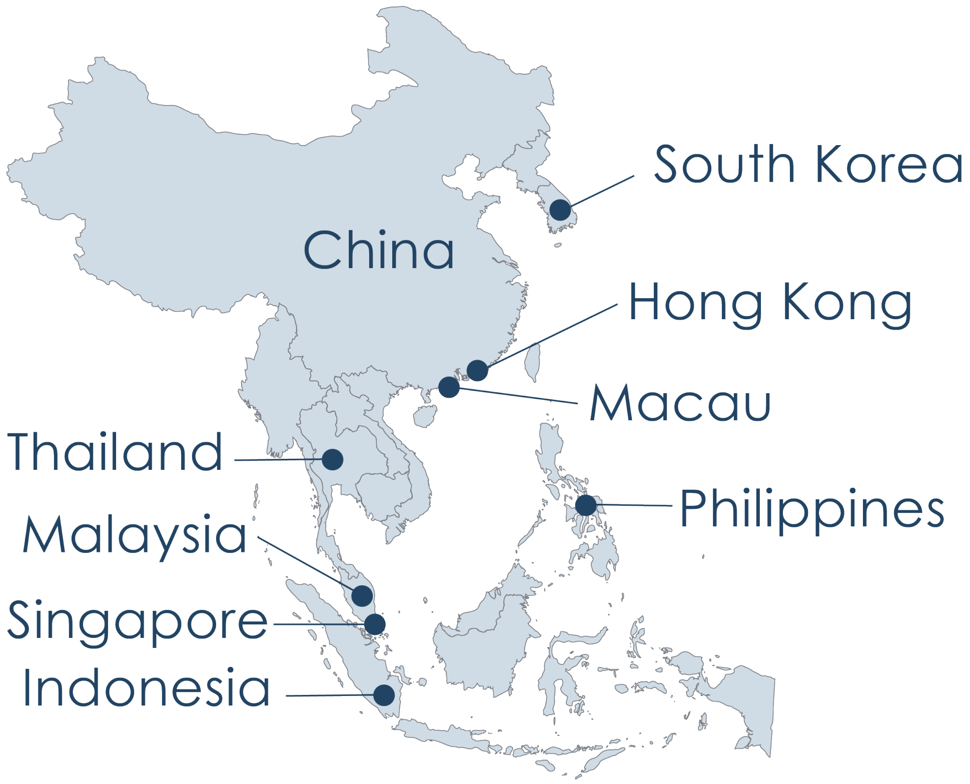
bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED

About Us



Established in 2005, DataExpert has been one of the leading suppliers in IT security industry in Asia. We develop, manufacture and distribute professional products in the fields of data recovery, data erasure, data destruction and digital forensics. Closely following the latest technologies, we always provide the most advanced IT assets management solutions for our clients, including government departments, organizations, enterprises, banks, SMEs and individuals all over the world. We have constructed close partnership with competitive companies from Greater China, Singapore, Japan, Korea, Russia, US, Canada and other regions.

Our Offices



Our Business

Digital Forensics and Incident Response(DFIR)

DataExpert Digital Forensics Laboratory is the first and only private owned full-service digital forensics lab in Hong Kong. Our team members have over 20 years of experience in digital forensic services, work closely with clients from law enforcements, government departments, law firms and corporates. We know what you want, and also know how technologies can help you.

We provide...

Products

Services

Laboratory

IT Asset Disposition(ITAD)

Inappropriate discard out-of-date IT asset may lead to the risk of data leakage. DataExpert started its secure data disposal business in 2005. Equipped with the large-scale data wiping machines, NSA degaussers, multifunctional shredders and a millimeter-level SSD Dis-integrator in Data Disposal Center, DataExpert has been one of the leading service and product suppliers in data security industry.

We provide...

Products

Services

Digital Forensic Products

Forensic Workstations

Cyber MZR-X
Digital forensic desktop

Cyber MZR-DT Workstation
Digital forensic workstation

Forensic Cube V4
(Keyboardless)
On-scene forensic workstation

Forensic Cube V4
(With keyboard)
On-scene forensic workstation

Forensic Laptop
Digital forensic laptop

Talino Laptop
Sumuri forensic laptop

Talino Workstation
Sumuri forensic workstation

Computer Forensic

Atola Insight Forensic 2.0
Portable forensic tool for imaging and recovering data and support damaged drives

Atola TaskForce
Portable high-performance forensic imager with 18 ports

Atola TaskForce 2
High-performance forensic imager with 26 ports

DE Forensic Write Blocker
Multi-interface write blocker

Portable Write Blocker Series
Compact write blockers

CSI Responder
PC imaging without dismantling

Belkasoft N
Digital incident investigation software

Belkasoft X
Computer, mobile and cloud forensic tool

Elcomsoft Premium Forensic Bundle
Computer and mobile extraction tool

Cyacomb Examiner Plus
Contraband scan software

Cyacomb Offender Manager
On-scene triage software

Mobile Forensic

GMDSOFT MD-NEXT
Data extraction software

GMDSOFT MD-RED
Data analysis software

GMDSOFT MD-LIVE
Live extraction and analysis software

SecurCube PhoneLog
CDR & cell site location cross-analysis solution

MOBILedit Forensic Express
Data extraction and analysis software

MOBILedit Cloud Forensic
Solution for cloud extraction

Elcomsoft Mobile Forensic Bundle
Acquisition, decryption and analysis software

Cyacomb Mobile Device Triage
Triaging software for mobile devices

macOS Forensic

Sumuri RECON ITR
macOS Imaging tool

Sumuri RECON LAB
Advanced Mac analysis tool

IOT Forensic Solution

GMDSOFT MD-DRONE
Drone extraction and analysis software

GMDSOFT MD-VIDEO
Video extraction and analysis software

GMDSOFT MD-CLOUD
Cloud extraction and analysis software

BTS Tracker
Cell tower analyzer

MOBILedit Smartwatch Forensics
Smartwatch extraction kit

Data Recovery

ruSolut VNR
Chip-off data recovery and analysis solution

GMDSOFT MD-READER
Chip-off memory extraction hardware

Regen-i Rework Station
BGA rework station

Digital Forensic Lab Solution

Examiner Work Desk
Single person digital forensic workbench

L-shape Workbench
Single person digital forensic workbench

3-Person 120° Workbench
Multi-person digital forensic workbench

3-Person Long Workbench
Multi-person digital forensic workbench

Cyber Colab
Collaboration hub

Evidence Preservation and Reception Workbench
Evidence preservation and reception workbench

Conference Table
Digital forensic lab furniture

Disassembly and Repair Work Table
Device disassembly work table

Smart Evidence Locker
Evidence locker with recording function

Display Screen
Digital forensic lab display

ITAD Products

Degaussers

MagWiper NSA Degausser
NSA EPL listed degausser

MagWiper MW-15X
17-second charged degausser

MagWiper MW-25X
Middle model degausser can erase hard disk without remove the mounting brackets

MagWiper MW-30X
Large model degausser can erase B4 notebook or 51 units of 2.5" HDDs simultaneiusly

Hard Disk Shredder / Crusher

Standard Hard Disk shredder
Small server hard disk shredder for office use

Standard Combo Hard Disk Shredder
20mm and 5mm combo blade shredder for office use

Combo Hard Disk Shredder
18mm & 9mm combo blade shredder

iPad & Hard Disk Shredder
H4 lv shredder for iPad, tablet and laptop

H5 Level Hard Disk Shredder
DIN 66399 standard H5 level HDD shredder

Flash, SSD & Mobile Phone Shredder
SSD shredder with 2*2mm particle size

Industrial E-Waste Shredder
Light e-waste solution for computers and printers

HDD Crusher
NSA- and DoD-compliant HDD crusher

CD & Paper Shredder

4x40mm² - 35 sheets
P4 CD & Paper Shredder

2x15mm² - 30 sheets
P5 CD & Paper Shredder

1x2mm² - 5 sheets
P7 CD & Paper Shredder

1x2mm² - 25 sheets
P7 CD & Paper Shredder

Disintegrator

Circuit Board & Chip Disintegrator
High security disintegrator for chipsets.

Duplicator & Wiper

Blancco Drive Eraser
Data sanitization solution

Clonix NetClon Portable
Network-based Disk Duplicator & Wiper

Clonix NetClon (16 ports)
Network-based Disk Duplicator & Wiper

Clonix DiskClon Portable
Disk duplicator & wiper

Clonix DiskClon (16 ports)
Disk duplicator & wiper

YEC DEMI PG520
Super compact SATA duplicator

YEC Demi YG2022
Light weight duplicator and wiper

YEC Demi YG2040
Dependable and versatile duplicator

YEC HIT MG2060
PCIe M.2 & SATA duplicator

YEC HIT YG3210
Industrial grade SATA duplicator.

DataExpert Asia
https://www.dataexpert.asia/

Professional Services

Digital Forensic Service

Experienced and professional service for finding the electronic evidence.

Our advantages

- ✓ Over 20 years in digital forensic services
- ✓ 1st digital forensics laboratory in HK
- ✓ Professional Service Ethics
- ✓ Comprehensive Service Scope

What is Digital Forensic?

Digital forensics, as a science, is the process used to acquire, preserve, analyze, and report on electronically stored information using scientific methods that are demonstrably reliable, verifiable, and repeatable.

Digital forensic can apply for:

- Employees fraud
- Investigation of personal computer
- Private investigation of cellular phone
- Inappropriate data duplication
- Intellectual property fraud
- Breach of contract
- Inappropriate Internet & Email Usage

Digital Forensics Procedure

ACQUISITION

Evidence Identification

Triage

Collection

Preservation

ANALYSIS

Pictures and Videos

System Registry

Emails

Mobile APPs

Browsing History

Instant Messengers

Office Documents

Peer-to-peer Platform

Data Recovery

Encrypted Files

REPORTING

Chain of Custody

Examination Report

Court Testimony

Digital Forensic Service

Data Expert

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Our Services

Awareness Training & Consultancy
Evidence Acquisition & Preservation
Forensic Examination
Litigation Support

Service Scope

- Digital Evidence Acquisition & Preservation
- E-discovery
- Forensic Data Recovery
- Password Cracking
- Forensic analysis
- System Emulation
- Keyword Searching
- Chats & Instant Messenger History Analysis
- User Artifacts Analysis
- Timeline Analysis
- Document Authentication
- File Attribution Identification
- Email Investigation
- Deleted/Damaged/Encrypted Data Recovery
- Smartphone Unlock
- Embedded images extraction and OCR

Our Promise

Digital Forensic Service Principles

Principles

- Actions taken should not affect the integrity of original data
- Investigator conducting examination must be well trained and positioned at senior level
- Actions taken during seizure, examining, storage or transfer must be documented timely and accurately
- Determine the course of each action in forensic sound manner

Our Team

Qualifications

- IACIS Certified Forensic Computer Examiner (CFCE)
- IACIS Certified Mobile Device Examiner (ICMDE)
- Cellebrite Cellphone Certified Investigator in CCPA and CCLO
- HancomWITH Certified Mobile Forensic Professional
- Meiya Pico Certified Examiner of Mobile Forensic System
- Meiya Pico Certified Examiner of Forensic Master
- Certified Information Systems Security Professionals (CISSP)
- Microsoft Certified System Engineer + Internet (MCSE+I)
- SUMURI Mac Forensics Examiner
- Magnet Certified Forensic Examiner (MCFE)
- Belkasoft Certified Examiner (BelkaCE)
- HRSS Digital Forensic Examiner (Intermediate)
- Cisco Certified Network Associate (CCNA)
- Flash Device Pinout Analyst
- CipherTrace Certified Cryptocurrency Examiner

Membership

- Member of High Technology Crime Investigation Associate (HTCIA)
- Member of International Association Computer Investigation Specialists (IACIS)

Data Recovery Service

Data Expert™

bsi. ISO/IEC 27001 Information Security Management CERTIFIED

Forensics Laboratory & Class 100 Cleanroom Based Data Recovery Service.

Our advantages

- ✓ ISO/IEC 27001:2022 certified
- ✓ Chip-off data recovery for severe damage
- ✓ Class 100 Cleanroom
- ✓ Recovery for different types of media, OS and file

Our Promise

Your data is unparalleled safe in DataExpert

- DataExpert Technology Limited got **ISO/IEC 27001:2022 Information Security Management** certified by BSI under certificate number IS 642998, for the scope of "The provision of data recovery and disposal services".
- We shall treat all material supplied by the client as confidential and shall not divulge any confidential information to any person.
- All employees in DataExpert have signed NDA and guarantee not to disclose any client information.

Types of Failures

Logical Failure

- Delete files wrongly
- Boot failure
- Data loss due to formatting/OS upgrade
- Database failure
- Unusual encryption

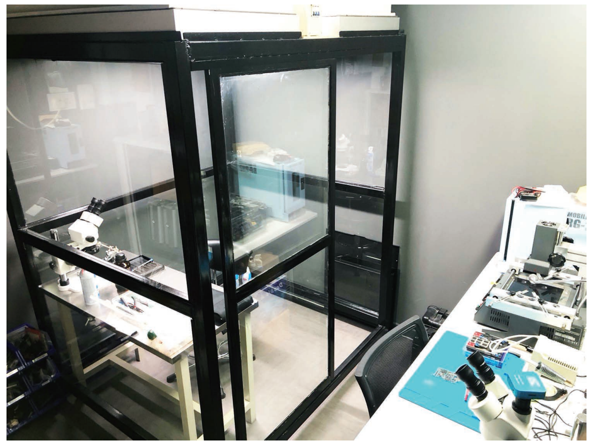
Physical Failure

- Wear and tear of parts
- Collision
- Flooding
- Fire

* Open case checking or chip-off data recovery may be needed

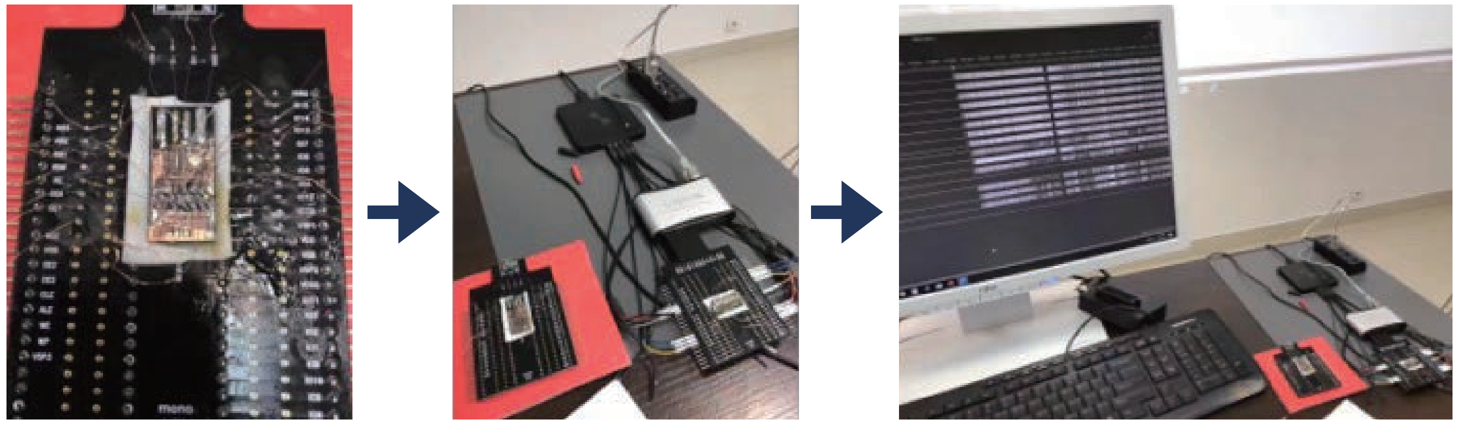
Class 100 Cleanroom

As to maximum the chance of recovering your data, DataExpert is beware on every step may affect the possibility of data recovery. The contaminants in the air can cause physical media damage and destroy the data if the hard disk open in normal surrounding. Therefore, DataExpert setup a **Class 100 Cleanroom** which ensures the **air contains no more than 100 dust particles per cubic foot** to prevent the physical damage.



Chip-Off Data Recovery

For the severe damage, we need to remove the chips from the failed devices and read the chip contents by flash data recovery tools.



Data Recovery Service

DataExpert™ — bsi ISO/IEC 27001 Information Security Management CERTIFIED

Support Types

Media

- Hard drive, micro drive, RAID, NAS, SAN, etc
- CD/DVD/Blue ray optical disc
- PC, tablet, cellphone, smartphone
- SSD drive, CF, SD card, Mico SD, MS, USB drives
- Magnetic tape (DLT, LTO etc)
- Digital albums frame, MP3/MP4 player, PDA
- iMac, Macbook, Powerbook, iPhone, iPad, iPod, etc
- SyQuest, MO, JAZ, ZIP, floppy diskettes

OS

- Windows 2000/XP/Vista/7/8/10/11
- Windows 95/98/98SE/ME
- Mac OS
- Unix, Linux
- Novell NetWare
- All database systems
- Windows NT/Server2003/Server2008/Server2012
- DOS/Windows 3.X
- APFS
- iOS, Android, Windows Mobile, Symbian, etc
- OS/2

File

- Pictures and videos
- Browsing history
- Instant messengers
- Peer-to-peer software
- System files
- Emails
- Mobile applications
- Office documents
- Windows registry
- Encrypted files

Implementation Plan

Service	Stage 1: Analysis	Stage 2: Data Recovery
Priority	1 - 2 workdays	1 - 2 workdays
Standard	3 - 4 workdays	3 - 4 workdays
Onsite	1 workday	1 workday

Work Flow

Consultancy

- Contact your consultant by sending email to **info@dataexpert.com.hk** or calling at **+852 3590 2115**.
- **No consulting fee.**

Media Collection

- Hand over your media to DataExpert office, or Media Collection
- Make an reservation of onsite collection **(free of charge)**

Analysis

- Analyse the media to find out the cause of fault.

Analysis Report & File List

- Generate a list of file that can be recovered.

Data Recovery

- IT engineer will recover the files assigned by client.

Delivery

- We will return the original media and a new media with recovered files to client.

Technical Support

- All recovered data will be **kept for 30 days** before permanently deleted, feel free to contact us for futher

Case Study

Hard disk data recovery for a school fire

In 2007, there was a fire in a Hong Kong secondary school. The server which contained all final exam questions were burnt severely and some of the hard disks were burnt or deformed. DataExpert tried to recover the data by open case data recovery in Class 100 Cleanroom and RAID data recovery. Finally, 50% of the data were recovered successfully which included all the exam questions.

Digital Forensic Laboratory

Build your own digital forensic laboratory (DFL).

Why Digital Forensic Laboratory is Needed?

Advantages of DFL

Optimize electronic devices management processes to better support digital forensic practitioners.

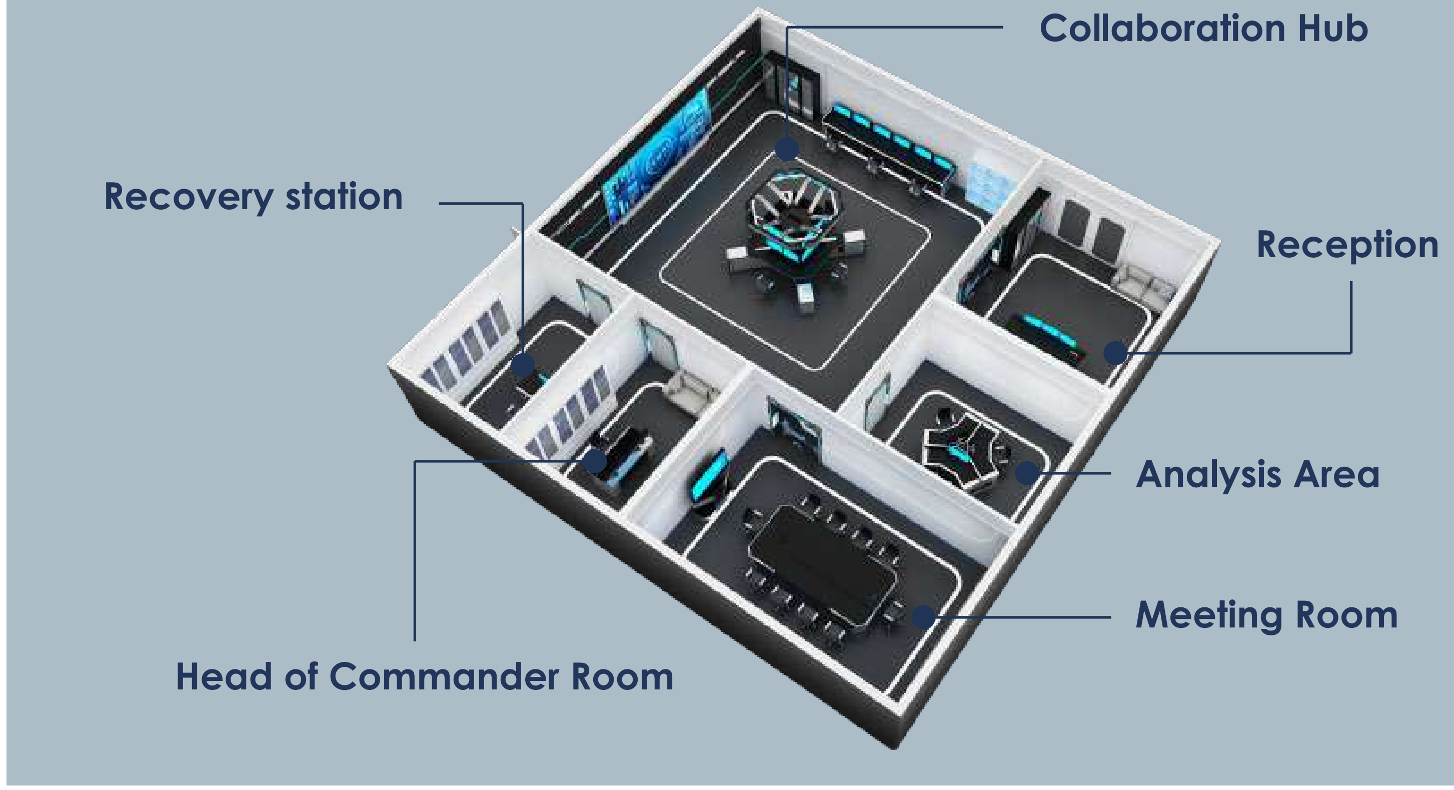
Enhance digital forensics capabilities in high-tech crimes investigation.

Establish guidelines for the intake, marking, tracking, protection, handling and return of the evidence in the Digital Forensic Laboratory.

Get access to fully validated hardware and software to produce the court acceptable results.

Our advantages

- ✓ Consist of a highly experienced team of talented digital forensic professionals
- ✓ First and only commercially operated digital forensic laboratory in Hong Kong
- ✓ Commit to more than 20 high quality DFLs to law enforce agencies worldwide
- ✓ Meet the unique requirements by providing a customized solution



One-Stop Service

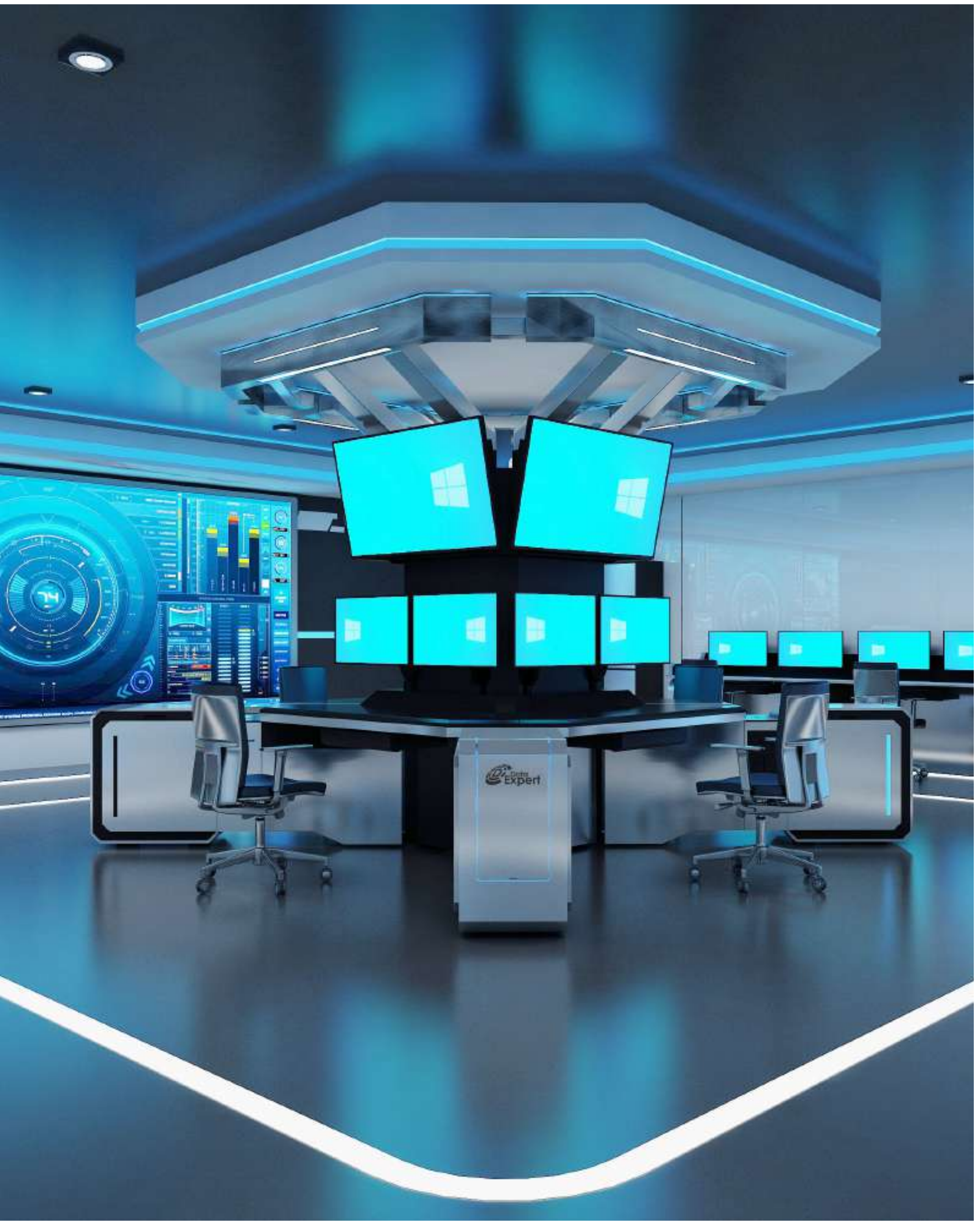
Planning & Budgeting → Design → Construction → Accreditation

Digital Forensic Laboratory

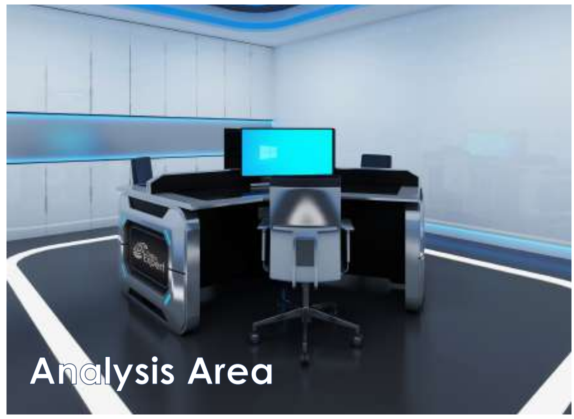
DataExpert

DataExpert
DataExpert

Meeting Room



Head of Commander Room

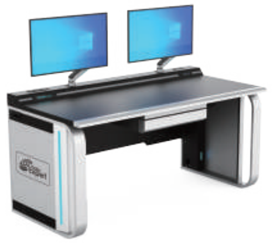


Analysis Area

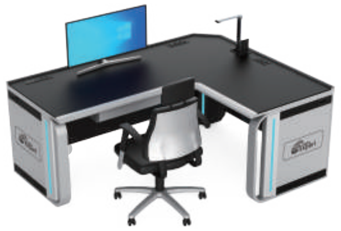
DataExpert

Analysis Area

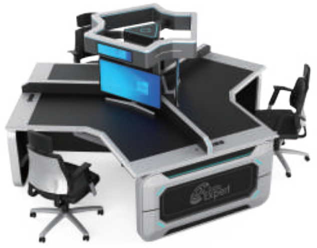
Components



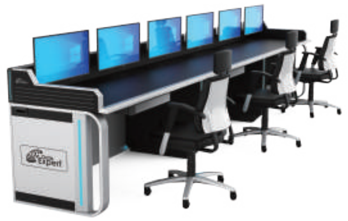
Examiner Work Desk
DE1902-PLUS
L1600*W800*H750



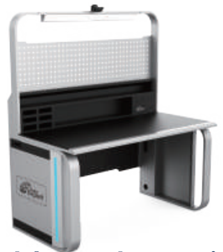
L-shape Workbench
DE1902-L
L1900*W1500*H750



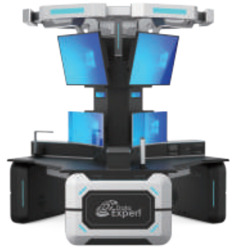
3-Person 120° Workbench
DE1902-T
L2900*W2500*H750



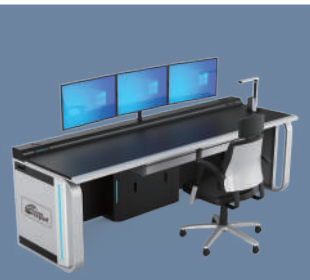
3-Person Long Workbench
DE1902-M3
L1200*W800*H750



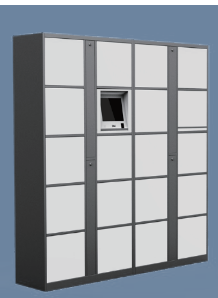
Disassembly and Repair Worktable
DE1904
L1400*W800*H750 (Destop Panel: H1600)



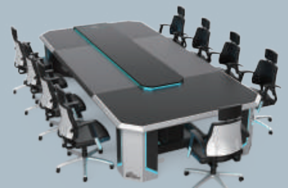
Cyber Colab
Cyber Colab
L2620*W3400*H750



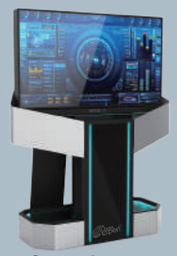
Evidence Preservation and Reception Workbench
DE1902-P3
L2500*W800*H750



Smart Evidence Locker
DE1904
L900*W490*H1850



Conference Table
DE1902-D
L3300*W1600*H750



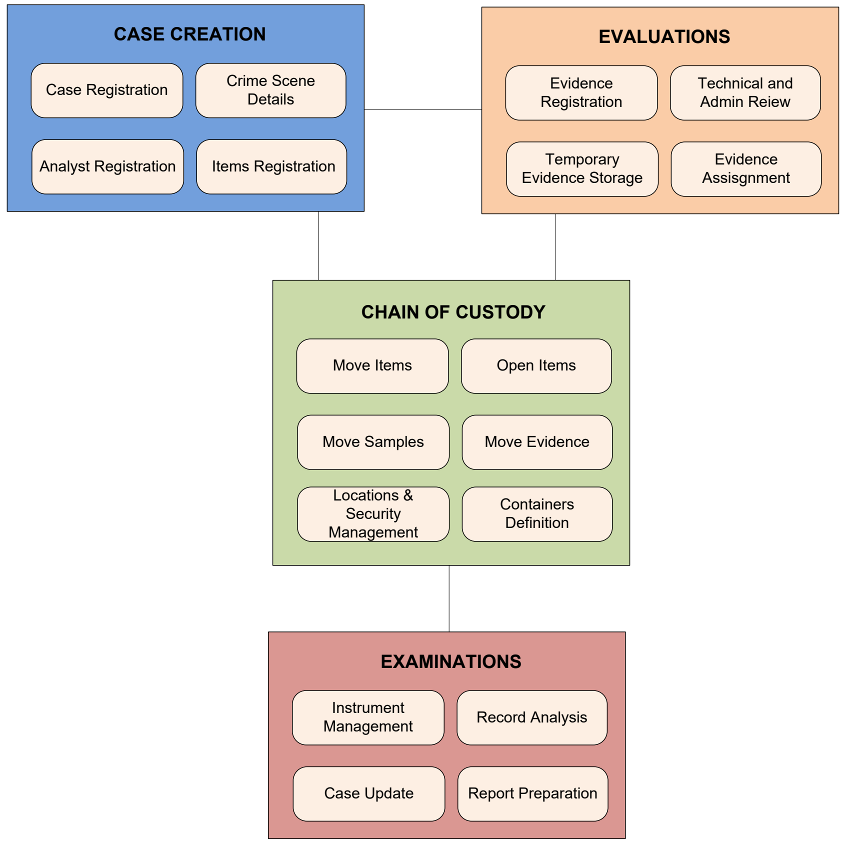
Display Screen
DE1901-ES
L1625*W580*H2000

COMPLIANCE

Our FLIMS ensures that the process implemented in the Forensic Lab, follows the ISO/IEC 17025 General Requirements for the competence of testing and calibration laboratories to ensure that all instruments and calibration are done in accordance to the International Standards, that governs the laboratory :

- ISO Procedures
    - Publications and Forms
    - Laboratory Wide Documents
    - Procedures
- Technical Procedures
    - Digital Evidence Management
    - DNA Database
    - Drug Chemistry
    - Firearm and Tool Mark
    - Forensic Biology
    - Latent Evidence
    - Toxicology
    - Trace Evidence

Example of Simple FLIMS Model



CASE CREATION

Case Registration

Crime Scene Details

Analyst Registration

Items Registration

EVALUATIONS

Evidence Registration

Technical and Admin Reiew

Temporary Evidence Storage

Evidence Assisgnment

CHAIN OF CUSTODY

Move Items

Open Items

Move Samples

Move Evidence

Locations & Security Management

Containers Definition

EXAMINATIONS

Instrument Management

Record Analysis

Case Update

Report Preparation

DataExpert Technology Limited
Unit 803 & 805, 8/F., Tower 1, Ever Gain Plaza, No.88 Container Port Road,
Kwai Chung, NT, Hong Kong.
Tel : ++852 3590 2115

Forensic
FLIMS
Lab Information Management System

IT Consulting
Forensic
Defense
Intelligence
Cyber Security

Forensic Lab Information Management System—FLIMS

SOLUTION OVERVIEW

Forensic laboratories rely heavily on lab centric technologies to collect and analyze evidence. To keep pace with increasing volumes, it is important that these organizations leverage technology to enhance the productivity and accountability of their examiners and overall operations. FLIMS is a full featured Forensic Laboratory Information Management System (FLIMS) that offers the flexibility, scalability and reliability necessary to ensure the smooth operation of a forensic laboratories.

FLIMS utilizes Thin Client technologies that allows a centralized management system from the Central Forensic Laboratory System to managed multiple Laboratories in different Sites, FLIMS also designed as modular software, which allows multiple phase implementation in order to provide better cost management for the Laboratories. These module includes ; Case Management System, Chain of Custody systems, Evidence Management System, Integrated Cyber Security System, and other Tailored Functions.

F-LIMS

- CASE MANAGEMENT
- CHAIN OF CUSTODY
- EVIDENCE MANAGEMENT
- INTEGRATED CYBER SECURITY
- DOCUMENT MANAGEMENT
- ISO/IEC 17025 COMPLIANCE SYSTEM
- ADVANCED USER MANAGEMENT
- TAILORED FORENSIC DIVISION SYSTEM
- MOBILE MANAGEMENT SYSTEM
- MONITORING SYSTEM.

Turn Key Solutions for your Laboratory Needs

FORENSIC LIMS THAT PROVIDES A TOTAL END TO END SOLUTION.

SCALABLE & INTEGRATED

FLIMS featured a fully scalable and integrated solution that allows the Laboratory managers to decide on which module they would like to implement first, and how many locations they need to be integrated with the LIMS with centralized repository system, it also features the following capabilities :

- Thin Client Architecture
- Web Based Applications
- Centralized or Distributed Repository System
- Distributed Processing
- Smart Resource Management

END TO END

FLIMS provided end to end features to suits the Forensic Laboratory requirements in different institutions or in different countries, it can also ensure that the Business Process and Standard Operating Procedures complied with the ISO/IEC 17025 Standards for Lab Accreditation recognized internationally. It caters all requirements from the Chain of Custody, Evidence and Case Management, and more importantly it features a mobile apps that can be accessed by Lab Analyst in the field.

TAILORED SOLUTIONS

The difference between FLIMS compared to other solutions in the market is that FLIMS are able to be fully customized for different Forensic Laboratories standard, .while at the same time able to maintain the Internationall Best Practice Standards. It can also be integrated with a Monitoring System for Laboratory Manager and Management to monitor Case progress, Budget and Expenditures, to better managed the Lab in more efficient manner.

Our Turn Key Solutions Capability Summary

- Platform Independent Model
- Web Based / Application Based
- Supports Mobile Platform
- Integrated Monitoring Center
- Integration with other Laboratory System
- Forensic Laboratory Equipment Procurement

CUSTOM SOLUTIONS

Smarter Forensic Lab
Reduced Integration Cost
Improved Quality and Compliance
Improved Efficiency
Easily Support New Requirements
Scalable Systems
Integration With Legacy Systems

WEB SOLUTIONS

Reduced Implementation Cost
Centralized Repository System
Improved Case Management
Secure Evidence Management
User Access Control
Accessibility Everywhere
Distributed Processing

MOBILE SOLUTIONS

On Demand Access
Mobile Lab for Analyst
Increase Processing Speed
Improved Chain of Custody
Evidence Documentation
Multiple Analyst Deployment

IT Asset Disposition Service

All-rounded data disposal services fit for different compliance and standards.

Our advantages

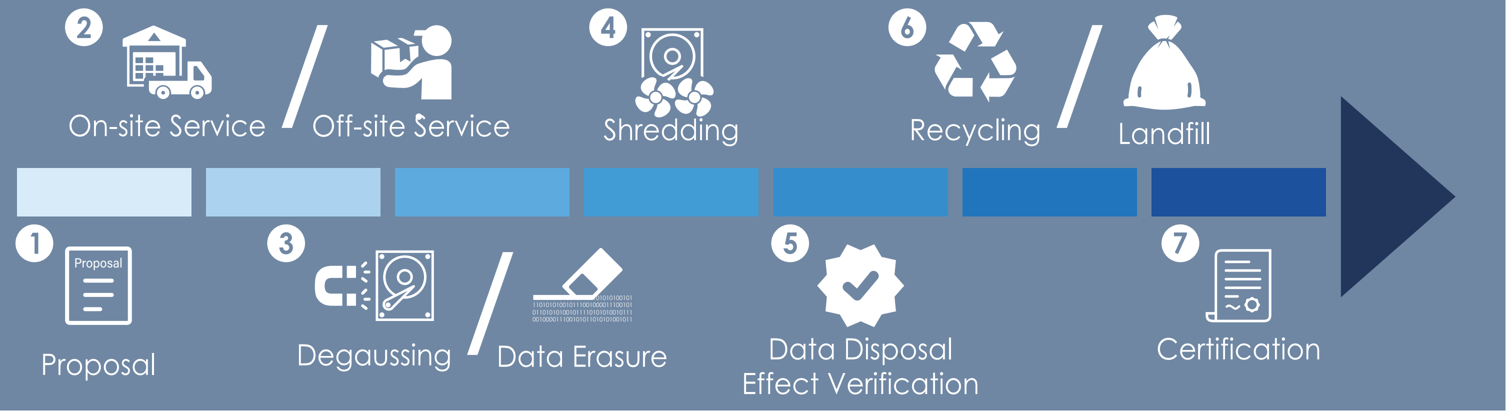
- ✓ **ISO/IEC 27001:2022 certified**
- ✓ **Wide-ranging solutions for different standard**
- ✓ **All-rounded solutions for different media**
- ✓ **One-stop Service**

Our Promise

Your data is unparalleled safe in DataExpert

- DataExpert Technology Limited got **ISO/IEC 27001:2022 Information Security Management** certified by BSI under certificate number IS 642998, for the scope of "The provision of data recovery and disposal services".
- We shall treat all material supplied by the client as confidential and shall not divulge any confidential information to any person.
- All employees in DataExpert have signed NDA and guarantee not to disclose any client information.

Work Flow


1 Proposal
2 On-site Service / Off-site Service
3 Degaussing / Data Erasure
4 Shredding
5 Data Disposal Effect Verification
6 Recycling / Landfill
7 Certification

Compliance & Standards

- NSA Standard
- NIST SP 800-88
- Hong Kong Government Guidelines
- EPA regulations
- FACTA
- Sarbanes-Oxley Act
- NIAP EAL 4+
- US Air Force System Security Instruction 5020
- US National Computer Security Center TG-025
- German VSITR
- Australian Defense Signals Directorate ACSI-33(X1-P-PD)
- CIS GOST P50739-95
- Standard single pass overwrite
- US DoD 5220.22M
- NISPOM
- Infosec 5
- HIPPA
- GLBA
- ISO 27001
- US Army AR380-19
- US Navy Staff Office Publication P-5329-26
- NATO NIAPC
- Australian Defense Signals Directorate ACSI-33(X0-PD)
- Canadian RCMP TSSIT OPS-II Standard Wipe
- CSEC ITSG-06

Media Types & Destruction Methods

		Logical Destruction		Physical Destruction	
		Degaussing	Wiping	Shredding	V-shape Bending
Magnetic Media	Hard Disk	✓	✓	✓	✓
	Magnetic Tape	✓	x	✓	x
	Floppy Disk	✓	x	✓	x
	Zip Drive	✓	x	✓	x
	MO Disk	✓	x	✓	x
Flash Memory	SSD	x	✓	✓	x
	USB Drive	x	✓	✓	x
	Memory Card	x	✓	✓	x
	Cellphone	x	✓	✓	✓
Optical Disc	CD	x	x	✓	x
	DVD	x	x	✓	x
	Blue-ray Disc	x	x	✓	x

IT Asset Disposition Service

Proposal

1. Receive your enquiry of **media type**, **number** and **standards & compliance**.

2. Assign a **project manager** to follow up your case.

3. Project manager will prepare a proposal which fit for your need.

Logical Destruction

Degaussing

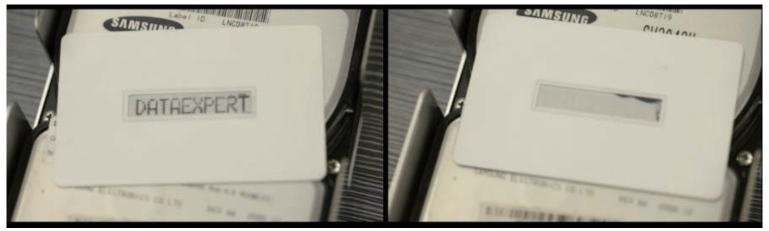
Conduct degaussing on each magnetic media with a qualified degausser which can generate magnetic field at least **1.5 times** higher than the coercivity (resistance to demagnetization) of the media.

Degausser Magnetic Field Intensity

MagWiper MW-15X	MagWiper MW-25X	MagWiper MW-30X	MagWiper NSA Degausser
Approx. 10,000 Oe			Approx. 20,000 Oe

Degaussing Effect Verification - Magnetic Checker Cards (Recommended 20% samples)

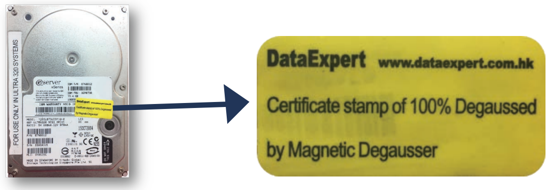
1. Before being degaussed, check checker card shows the given pattern of "DATAEXPERT".
2. Place the magnetic checker card into degausser chamber together with the target media.
3. After degaussing, the particles of the card are randomly distributed if the media has been degaussed successfully.



Before Degaussing **After Degaussing**

Labeling

Label each magnetic media as **"100% degaussed"** after full completion of degaussing.


DataExpert www.dataexpert.com.hk
Certificate stamp of 100% Degaussed
by Magnetic Degausser

Wiping/Erasure

Wiping offers a secure data destruction solution by **overwriting the media in specific patterns**. It allows client to erase data permanently and securely , while **keeping the media usable**. However, wiping is not always successful when dealing with malfunctioning media.

Physical Destruction

Shredding

By cutting storage media into small particles, it provides an additional protection for degaussed media, and an unparalleled choice for media which failed to wipe normally.

Shred Size Specification (in mm)

	DED-SHS	DED-CDS2	DED-MMS3	DED-MMS2	DED-CDPS	DED-SSD01	DED-SSD2XS	DED-HDS35
Server HD	40*R	-	-	-	-	-	-	20*20
3.5" HD	40*R	-	-	40*R	-	-	-	20*20
2.5" HD	20*R	-	10*R	5*R	-	-	-	20*20
SSD	20*R	-	10*R	5*R	-	0.5*0.5	2*2	-
USB	20*R	-	2*5	5*R	-	0.5*0.5	2*2	-
CD/DVD/Blueray Disk	-	1*5	4*20	40*R	1.6*4	0.5*0.5	2*2	-
Magnetic Tapes	40*R	-	-	40*R	-	-	-	50*≤50
Memory Cards	-	1*5	2*5	5*R	-	0.5*0.5	2*2	-
Cell Phone	20*R	-	40*R	5*R	-	-	-	-
Chips	-	-	40*30	5*R	-	0.5*0.5	2*2	-
Paper	-	-	40*20	-	1*5	-	-	-

Dimension: mm R: Random

Recycling and Disposal

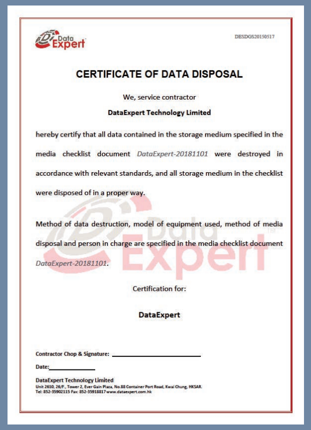
Recycling

Recycle degaussed/wiped media by Hong Kong Environment Protection Department (EPD) authorized computer recycler.

Landfill (for non-recyclable E-waste only)

Landfill non-recyclable residue according to the Waste Disposal Ordinance under Hong Kong Law.

Reporting



DESDGS20150517

CERTIFICATE OF DATA DISPOSAL

We, service contractor

DataExpert Technology Limited

hereby certify that all data contained in the storage medium specified in the media checklist document *DataExpert-20181101* were destroyed in accordance with relevant standards, and all storage medium in the checklist were disposed of in a proper way.

Method of data destruction, model of equipment used, method of media disposal and person in charge are specified in the media checklist document *DataExpert-20181101*.

Certification for:

DataExpert

Contractor Chop & Signature: ______________________

Date:____________

DataExpert Technology Limited
Unit 2610, 26/F., Tower 2, Ever Gain Plaza, No.88 Container Port Road, Kwai Chung, HKSAR.
Tel: 852-35902115 Fax: 852-35918817 www.dataexpert.com.hk

Document and Certificates

DataExpert services are in accordance with international data security standards. We can provide auditable tracking document and certificates.

gstruc err_fmove ,("ERROR: couldn't op
gstruc err_fread ,("ERROR: unable to m
struc err_write ,("ERROR: couldn't read
CR,LF> malicious virus ,("ERROR: unable to write
truc msg ,("Boot sector was successfu
bjReq SCAN_REQ
ObjRep
EQ

Digital Forensic and Incident Response

Forensic Workstation

Data Expert™

Cyber MZR-X

All-in-one solution for digital forensic laboratory.

Hardware specifically designed for forensic

Forensically sound design

Easy to distinguish write blocker & read write area to reduce the human error.

Multi-interface write blocker

Built-in write blocker with multiple interfaces for forensic investigation of various devices or media.

High performance hardware

Allows customize the hardware to support several high-demand forensic software.

Forensically sound design

Build-in forensic imaging software

4 main functions of software

Software with essential functions for investigation needs

The software encompasses imaging, hashing, wiping, and audit report functions, catering to the fundamental requirements of investigators.

Multi-languages interface

The software offers a user interface in three languages: English, Japanese, and Chinese.

Phone Connection Panel

Auto detect connected devices' information

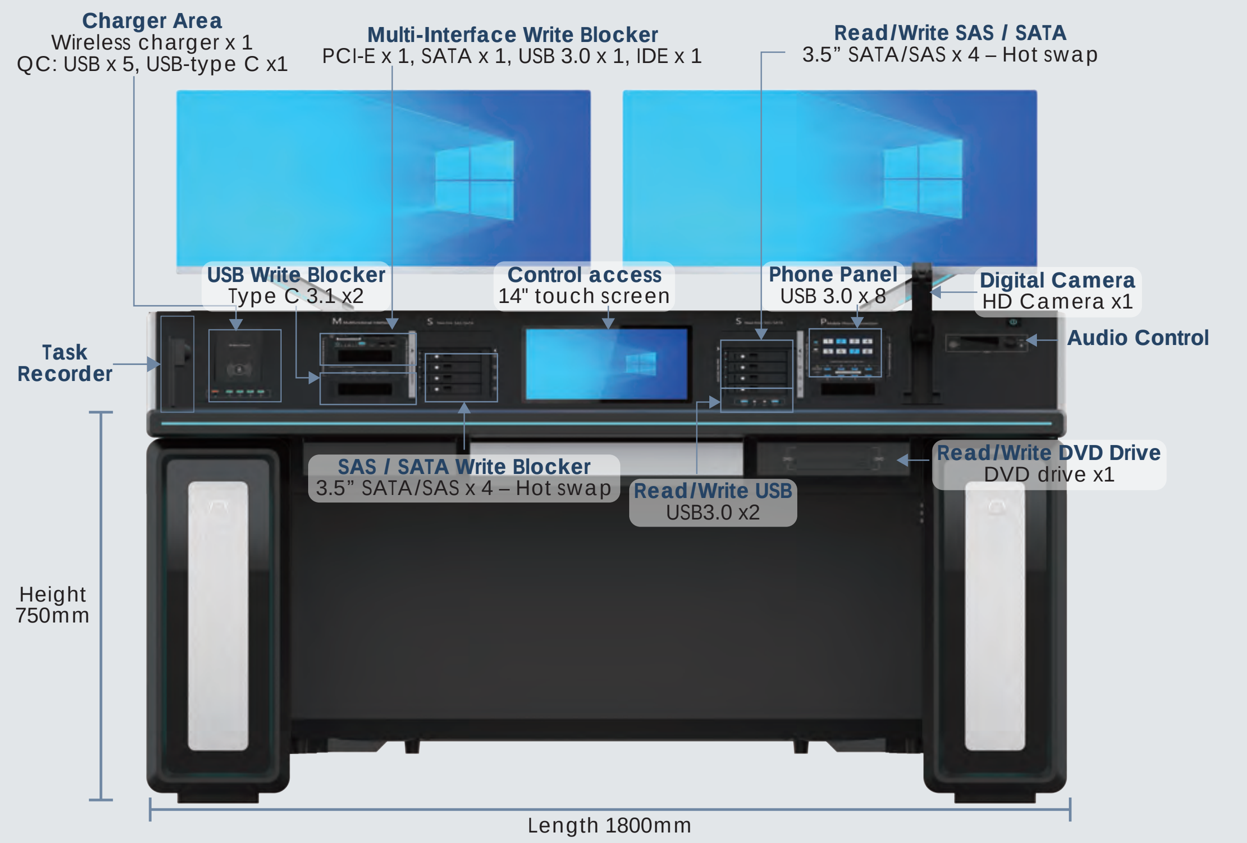
Devices' brand, model, and serial number would show automatically after connection.

Multiple phone connections for multitasking

Supports multi-tasking of mobile extraction for high-demanding investigative needs.

Phone Connection Panel

Write-Blocker & Read/Write Interfaces



Specification

Model	**Cyber MZR-X**
OS	Win11 64 bits OS
CPU	Intel Z790 Chipset CPU Intel i9-14900K
Memory	128GB DDR5 4800MHz
Hard Drive	2TB M.2 SSD HDD (operating system) 2TB SATA SSD (Temp storage) 8TB Hard Drives x 3 (Data Storage)
Graphic Card Display	Nvidia RTX 4070 12G GDDR6X
Write-blocker Interfaces	
Multi interface Write blocker^	PCI-E x 1, SATA x 1, USB 3.0 x 1, IDE x 1
USB Write Blocker	Type C (USB3.1) x 2
SAS / SATA Write Blocker	3.5" SATA/SAS x 4 – Hot swap
Read/Write Interfaces	
Read/Write Interface	USB3.0 x2 3.5" SATA/SAS x 4 – Hot swap
Phone Panel	USB 3.0 x 8 port (power independent)
Others	
Other Hardware	Built-in Wireless charger x 1 DVD R/W Driver x 1 RJ45 10GB x 2 ports 3.5 earphone jack x 2 WiFi and Bluetooth module x 1 Built-in rear speaker Digital Camera Built-in HD Document Camera Task Recorder Camera Control access Built-in 14" touch screen
Software	DE D-BOX Duplication Software with Hashing Win 11 64bit English Version Optional: Belkasoft Evidence X / Hancom MD-Series / Mobiledit Forensic Pro
Display	2 unit Samsung or equivalent 34 inch Curve 21:9 with 1800R WQHD 3440 x 1440 (2K) - 100Hz, Type-C port.
Power	Power adapter 1200W
Dimension	1800*900*750 mm (L*W*D)

^ Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.

* Customized Configuration available. Powered by DataExpert.

* Specifications are subject to change without notice.

Cyber MZR-DT

All-inclusive forensic workstation for rapid analysis of artifacts.

Hardware specifically designed for forensic

Forensically sound design

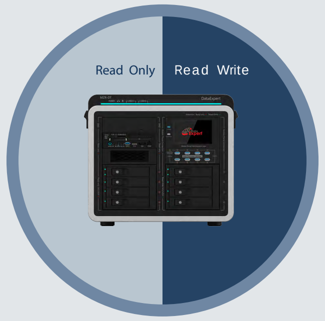
Easy to distinguish write blocker & read write area to reduce the human error.

Multi-interface write blocker

Built-in write blocker with multiple interfaces for forensic investigation of various devices or media.

High performance hardware

Allows customize the hardware to support several high-demand forensic software.



Forensically sound design

Build-in forensic imaging software

4 main functions of software

Software with essential functions for investigation needs

The software encompasses imaging, hashing, wiping, and audit report functions, catering to the fundamental requirements of investigators.

Multi-languages interface

The software offers a user interface in three languages: English, Japanese, and Chinese.

Phone Connection Panel

Auto detect connected devices' information

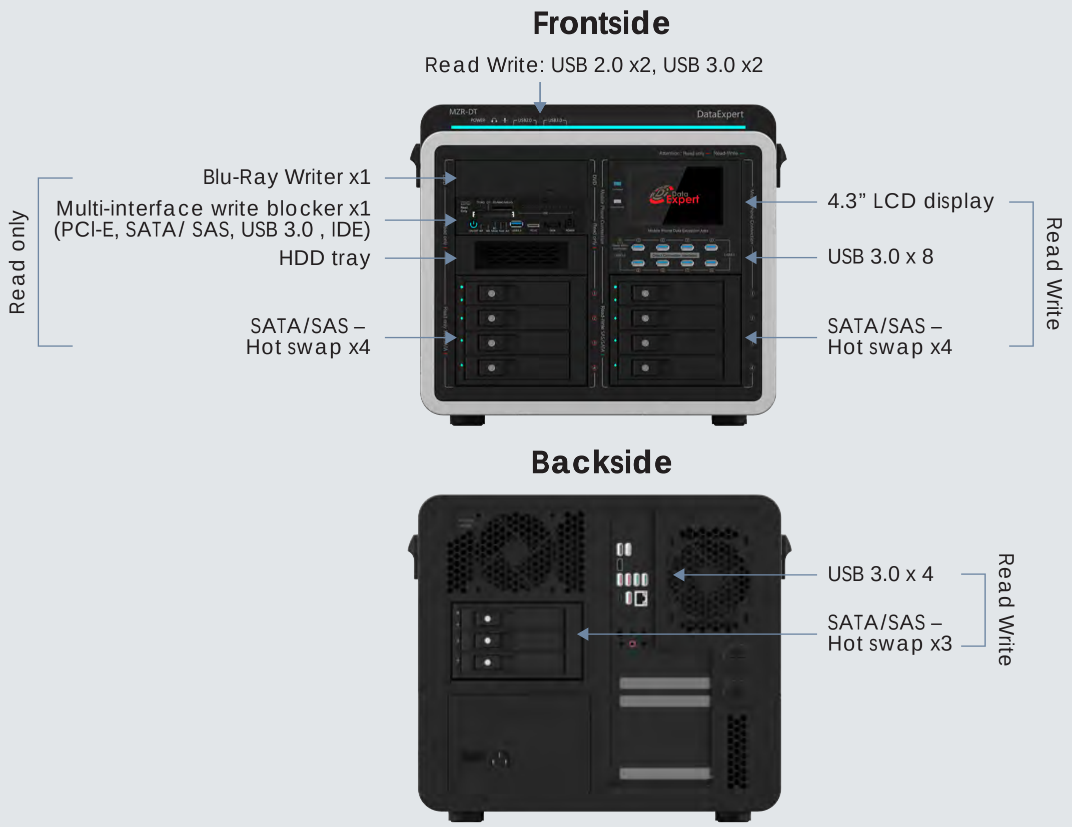
Devices' brand, model, and serial number would show automatically after connection.

Multiple phone connections for multitasking

Supports multi-tasking of mobile extraction for high-demanding investigative needs.

Phone Connection Panel

Write-Blocker & Read/Write Interfaces



Specification

Model	Cyber DZR-DT
System Configuration	
OS	Microsoft Windows 11 Pro 64 bit
Internal Memory	64GB DDR4 UDIMM non-ECC RAM Memory (2X32GB)
CPU	Intel i9-10900X (10 Core, 19.25M Cache, base 3.7GHz, up to 4.5GHz)
Storage system	ONE (1) 1TB GB M.2 NVME SSD (System installed on this Drive) ONE (1) 8TB 7200rpm SATA Hard Drive for Temporary Files and Processing ONE (1) 8TB 7200rpm SATA Hard Drive for evidence storage
Graphic Card Display	One (1) Nvidia Quadro T400, 4GB GDDR5 for Graphics Processing Unit (customizable)
DVD Drive	Blu-Ray Writer
Power Supply System	One (1) 1000 Watt Power Supply Unit
Dashboard Configuration	
Write Blocker (Read Only)	Writeblocker with PCI-E, SATA/ SAS, USB 3.0, IDE^
Read/ Write	3.5" SATA/SAS x 4 – Hot swap At rear: USB 3.0 x4 , at top: USB 2.0 x 2 + USB 3.0 x2, front panel: USB3.0 x 8
Phone Connection Panel	4.3" LCD display with 8 phone connected or disconnected status panel
Forensics Software	
Build-in software	D-Box Forensic Imaging Software
Optional Computer Forensics	Belkasoft Evidence X
Optional Phone Forensic	Hancom MD-Series / Mobiledit Forensic Pro
Warranty	THREE years limited warranty

^ Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.

* Customized Configuration available. Powered by DataExpert.

* Specifications are subject to change without notice.

Data Expert™

Forensic Cube V4

All you need for on-scene investigation.

Hardware specifically designed for forensic

Forensically sound design

Easy to distinguish write blocker & read write area to reduce the human error.

Multi-interface write blocker

Built-in write blocker with multiple interfaces for forensic investigation of various devices or media.

High performance hardware

Allows customize the hardware to support several high-demand forensic software.

Forensically sound design

4 main functions of software

Build-in forensic imaging software

Software with essential functions for investigation needs

The software encompasses imaging, hashing, wiping, and audit report functions, catering to the fundamental requirements of investigators.

Multi-languages interface

The software offers a user interface in three languages: English, Japanese, and Chinese.

Specifically designed for on-scene

Army-grade casing

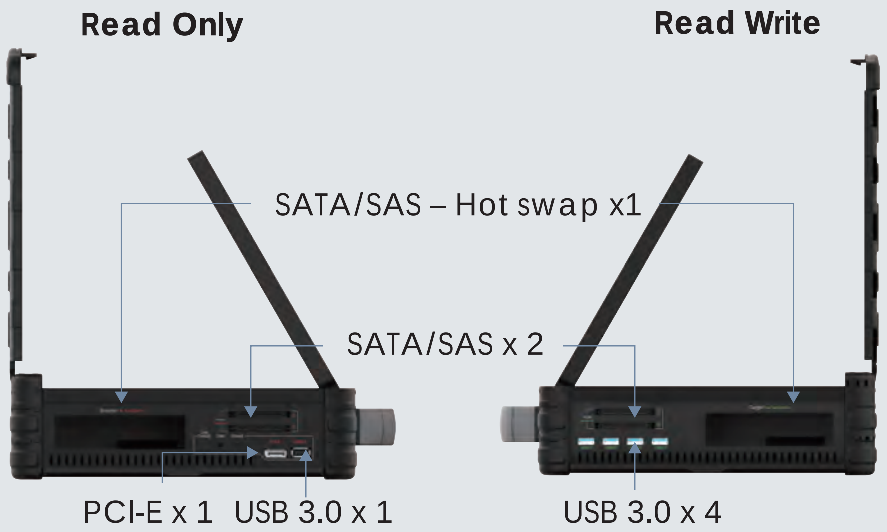
The casing is made of sturdy metal material, durable and impact-resistant.

Dedicated carrying bag

The bag offers excellent protection for MZR-P, and its internal compartment is designed to conveniently store accessories.

Dedicated carrying bag

Write-Blocker & Read/Write Interfaces



Versions

Keyboardless version

Keyboard version

Specification

Model	MZR-P
OS	Win11 64 bits OS
CPU	Intel® Core™ i9-13900T
Memory	64GB
Hard Drive	HDD 1: 4TB M.2 SSD HDD 2: 4TB SATA SSD
Write-Blocker Interfaces	PCI-E x 1 USB 3.0 x 1 SATA/SAS – Hot swap x1 SATA/SAS x 2
Read/Write Interface	USB 3.0 x 4 SATA/SAS – Hot swap x1 SATA/SAS x 2 External multi-in-one card reader x1
Software	D-Box Forensic Imaging Software
Display	14 inch High Brightness Touch Screen
Dimension (W x D x H)	355mm* 275mm* 75mm
Net Weight	6.72kg

* Customized Configuration available. Powered by DataExpert.
* Specifications are subject to change without notice.

Forensic Laptop

High perfermance laptops design for field or lab forensic investigation.

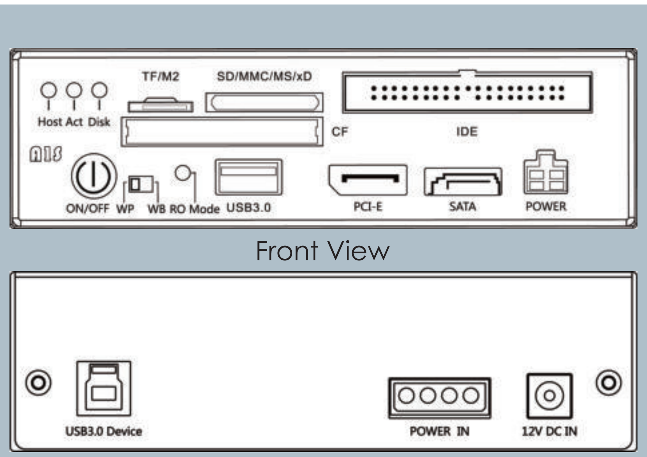
Specification

Model	Forensic Laptop
OS	Windows 10 Operation system
CPU	11th Generation Intel® Core™ i9-11900H Processor
Internal Memory	128GB Dual Channel DDR4
Storage system	One (1) 2TB SSD M.2 NvMe for the Operating System THREE (3) 2TB M.2 NvMe SSD for Evidence Files
Graphic Card Display	NVIDIA GeForce RTX 3080 GPU with 16GB GDDR6 Video Memory
Display	17.3" Full HD (1080P) 300Hz

* Customized Configuration available. Powered by DataExpert.
* Specifications are subject to change without notice.

Forensics Write Blocker

Integrated write-blocker supports 7 storage media types.



Front View

Back View

Supported storage media :

USB 3.0/2.0/1.0,PCI-E(with PCIe Adapter),SATA, CF/M2/TF/SD/MMC/MS/xD

Specification

Model	DE-WB-A1S
	Interface Front Panel
PCI-E	One PCIe Custom data + Power connector
SATA/ SAS	One SATA data connector
USB 3.0	One USB 3.0 Standard-A Connector
IDE	One IDE Signal Connector
DC Out	One DC out 4pin drive power connector (for IDE, SATA, SAS & PCIe)
	Switch
DIP Switch	Two position DIP Switch configures Write Protect (WP) or Write Blocker (WB)
	Other feature
Status LED	4 LEDs: Host (Detect), Activity(Act), Write-Block(Disk), Read-Write (RO)
	Host/Computer Interface Compatibility
USB 3.0 Controllers	Most USB 3.0 Controllers should be compatible
Host OS	Windows 7, 8 10 Macintosh OS X Most modern Linux distributions
HPA	Support HPA Unlock and Reset
LED Indicator	Color LED Indicators for “Host”, “Write Block” or “Read/Write” mode visibility
Size:	158 x 146 x 43 mm (L x W x H)
Warranty	One Year Warranty and Free Firmware upgrade

*Remark: Made in Hong Kong and powered by DataExpert
*Specifications are subject to change without notice

Portable Write Blocker Series

Compact write blocker for securely access digital data during forensic investigations in everywhere.

Product Detail

Write Blocker U

- Lightest model
- Device information and transmission speed are displayed on the screen.

Write Blocker P

- Folding design
- Extract data from both PCIE U.2 and SATA ports without requiring any accessories

Write Blocker M

- Comprehensive solution for extracting devices from multiple interfaces
- With Apple transfer kit which can extract data from MacBooks of different models

Specification

	Write Blocker M	Write Blocker P	Write Blocker U
Model	**DE-U2MS**	**DE-U2PS**	**DE-U2US**
Write-Blocker Interfaces			
SATA	1	1	/
USB 3.0	1	/	1
PCI-E(U.2)	1	1	/
TF	/	/	1
Features			
PCIE NVME Protocol	✓	✓	/
PCIE AHCI Protocol	✓	/	/
Hidden Area	Supports automatic identification and full reading of HPA hidden areas.	/	/
Non-Intrusive Read-Only for MacBook	✓ Target disk mode	/	✓ Target disk mode
Performance Parameter			
Maxmium Transmission Rate	10GB/MIN (PCI-E/ M.2/SATA/USB SSD)	50GB/MIN (USB SSD)	14GB/MIN (USB SSD)
Connection Port	USB 3.0	USB 3.2	USB 3.0
Mode			
Read-Only Mode	✓	✓	✓
Virtual Writing Mode	✓	/	✓
Other			
Screen	/	/	Optional
Power	DC 12V 4A	DC 12V 4A	DC 5V 3A
Size (W x D x H)	141*81*26mm	121*73*25mm	104*68*29mm

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

THE POWER AND VERSATILITY OF TALINO - ACCEPT NO SUBSTITUTES

Here at SUMURI we take the greatest pride in building the very best forensic workstations anywhere. All of our TALINOs are designed by Certified Forensic Computer Examiners because we believe that the person who best understands what the modern examiner needs is someone who knows forensics! Using our unique and proprietary chassis, we accomplish two major goals:

1.) Separate the electrically sensitive components from those that produce more EMI and heat.
2.) Since the entire chassis is made of aluminum, we can utilize its entire surface area to help spread and dissipate heat.

Both of these effects help ensure your TALINO runs as smoothly as possible and lasts as long as an examiner needs it!

We use only the highest quality components that have been tested and vetted here in our lab. Our Laptops are designed and optimized for forensics and come with an industry leading 3 year warranty.

Every all TALINO workstations and laptops are built based... on your unique requirements and to our exacting standards. No competitor offers ANYTHING close!

Every TALINO workstation is burned in for 72 hours using multiple stress testing and benchmarking tools. The goal of our quality assurance team is to try and “break” the workstation before shipping it. From logical stress tests to actually physically altering the airflow in the TALINO we do everything in our power to make sure no TALINO leaves the lab until it has been put through the wringer. This is backed by our industry leading 3 year warranty and lifetime access to our support line for every TALINO user. Day or night we are there when you need us.

FORENSIC LAPTOPS

TALINO KA-L ALPHA

The SUMURI TALINO KA-L Alpha is an extremely portable Forensic Workstation specifically designed to perform faster than most desktop forensic workstations. We introduced this system for several reasons as many agencies just need a really good laptop that they can depend on to process small cases, work out in the field, collect mobile phone data, or a variety of other tasks.

TALINO KA-L GAMMA

The SUMURI TALINO KA-L Gamma is a portable Forensic Workstation specifically designed to perform just as fast as other desktop forensic workstations. This system was created to meet the needs of agencies who've both come to expect the speed and power from our renowned portable TALINO Forensic Workstations, and are looking for a middle ground between our other portable offerings.

TALINO KA-L OMEGA

The SUMURI TALINO KA-L Omega is the fastest portable Forensic Workstation specifically designed to perform just as fast as most desktop forensic workstations. In fact, this powerhouse might actually be more powerful than your current forensic workstation, unless you have a full sized TALINO desktop Forensic Workstation.

TALINO KA-L eDISCOVERY

The SUMURI TALINO KA-L eDiscovery & Incident Response laptop is our high-end eDiscovery incident response laptop aimed specifically for the modern-day forensic examiner tasked with handling incident response type examinations. The SUMURI TALINO KA-L eDiscovery & Incident Response laptop, is our high end eDiscovery incident response laptop aimed specifically for the modern-day forensic examiner tasked with handling incident response type examinations.

RUGGEDIZED LAPTOP

The SUMURI TALINO TRL-65 is our no compromise ruggedized laptop. When you need both dust proofing and water resistance in one package along with as little sacrifice as possible when it comes to performance, the TRL-65 is your very best choice! It features a whopping six-foot drop protection, and like all TALINOs, there are tons of customization options and you will find the same awesome three year warranty you've come to know and love.

TALINO WORKSTATIONS

CRYPTANALYSIS WORKSTATION

An extremely fast and efficient decryption system featuring Intel CPUs and NVIDIA Graphics Cards combined with our proprietary 3mm aluminum heat dispersing chassis. All the horsepower you need to run Passware, Elcomsoft or any other cryptanalysis solution.

FORENSIC WORKSTATION

The SUMURI TALINO KA brand of computers is built on the most reliable and stable platform designed by Certified Forensic Computer Examiners. Each custom workstation is built with expandability and a future proof mindset so that you are not replacing the computer every few years with an entirely new computer.

eDISCOVERY WORKSTATION

An extremely fast and efficient decryption system featuring Intel CPUs and NVIDIA Graphics Cards combined with our proprietary 3mm aluminum heat dispersing chassis. All the horsepower you need to run Passware, Elcomsoft or any other cryptanalysis solution.

NUIX POWERED WORKSTATION

The SUMURI TALINO NUIX Forensic Workstation is our specialized high-end dual Intel CPU system. This system was designed by our certified forensic computer examiners and NUIX engineers specifically to run NUIX. The power of TALINO married to the strength of NUIX is a match made in heaven.

TALINO SERVERS

SERVER SOLUTION

The SUMURI TALINO KA Server Solution family brings everything great about TALINO KA workstations to server form factor computing in the big data arena, all designed by Certified Forensic Computer Examiners. Whether you're looking to store several hundred Terabytes for your lab or you need Petabytes for body camera footage we've got you covered. With multiple processing nodes available our designers can build you the server that you need at a price you can't beat.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

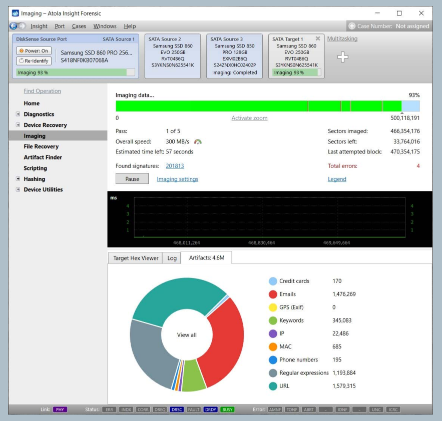
Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

Computer Forensic

Atola TECHNOLOGY Insight Forensic 2.0

The first and only forensic data acquisition tool that works with both good and damaged media.

Damaged drive support



- In-depth automated drive diagnostics
- Multi-pass imaging of damaged drives
- Automated imaging of freezing media
- Bad sector recovery
- Segmented hashing for bad drive's image verification
- HDD current monitoring for continuous diagnosis

Functions

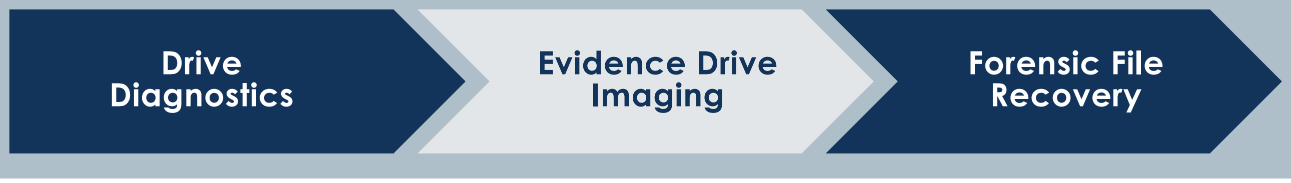
Forensic Imaging

- 3 simultaneous imaging sessions + multi-tasking
- Imaging session speed up to 500 MB/s
- E01, AFF4 or Raw target images created in the network or on target drives
- Up to 3 targets per imaging session
- Support of SATA, IDE, USB drives
- Via extensions: SAS, Apple PCIe (2013 - recent models), NVMeand M.2 PCIe SSDs
- Built-in hardware write blocker for all source ports

Forensic feature set

- Unknown ATA password extraction
- Locate sectors - detect which files and partitions they belong to specified drive sectors
- On-the-fly sector-level Artifact finder based on Intel Hyperscan engine
- Hash calculation (linear and segmented): MD5, SHA1, SHA224, SHA256, SHA384, SHA512
- Wiping methods including DoD 5220.22-M, Secure Erase, NIST 800-88, Pattern Erase
- Forensic file recovery for NTFS, APFS (with encrypted volumes), XFS, ext4/3/2, ExFAT, HFS/HFS+, FAT32, FAT16
- Case management system automatically generates detailed reports
- Comparison of 1 drive against 3 drives or images
- Detection and lifting of HPA and DCO restricted areas
- SSD Trim

Workflow



Drive Diagnostics → Evidence Drive Imaging → Forensic File Recovery

Product comparison

	Atola TaskForce 2	Atola TaskForce	Atola Insight Forensic
Imaging			
Simultaneous imaging sessions	25+	12+	3
Cumulative imaging speed	25 TB/hour	15 TB/hour	4 TB/hour
Automated RAID configuration detection	Support RAID 0, 1, 5, 6, 10 and JBOD		-
Automation	Web API		-
Damaged drive support	Damaged heads, freezing drives, short circuit detection, worn-out HDDs/SSDs		
Head selection support	✓	✓	✓
Network	2 x 10Gb Ethernet ports		
Express mode	up to 25 imaging sessions	up to 17 imaging sessions	-
Logical imaging to L01	✓	✓	-
Imaging targets	E01/RAW/AFF4 files located on other drives (Veracrypt-encrypted as option), E01/RAW/AFF4 files located on a server or NAS, bit-to-bit copy on other drives		
Max. targets per imaging session	5	5	3
Hardware unit			
Ports	26 ports with source/target switch	18 ports with source/target switch	10 ports Cannot switch source/target
Port types	4 NVMe M.2/U.2 PCIe 4.0 8 SATA 8 SAS/SATA 4 USB 1 IDE Extension port	6 SATA 6 SAS/SATA 4 USB 1 IDE Extension port	6 SATA 6 SAS/SATA 4 USB 1 IDE Extension port
Write protection	on all ports (configurable)	on all ports (configurable)	on source ports
Extension modules	M.2 NVMe/PCIe/SATA Apple PCIe Thunderbolt	M.2 NVMe/PCIe/SATA Apple PCIe Thunderbolt	M.2 NVMe/PCIe/SATA Apple PCIe Thunderbolt SAS
Interface	web-based (offline)		Windows application
Wi-Fi mode	External adapter (optional)		-
Standalone mode	Kiosk mode	✓	-
Server rack compatibility	✓		
Other features			
Drive diagnostics	PCB, Heads, Media scan, Firmware, File system. Imaging time estimate.		
Wiping	Zero-fill, Custom pattern, LBA number, Secure Erase, DoD 5220.22-M, NIST 800-88, Random, Format NVM and Sanitize for NVMe drives		
Hashing	MD5, SHA1, SHA256, SHA512		
Case management	✓	✓	✓
Automatic report generation	✓	✓	✓
Other Common features	SSD Trim, HPA, DCO, AMA recovery, Segmented hashing, Source drive files preview		
Special features for Insight Forensic Only	-	-	Unknown ATA password recovery, Locate sectors, Artifact Finder (sector-level), File recovery, Scripting, Disk editor (HEX)

Atola TaskForce

An on-scene and large-scale acquisition tool capable of working with both good and damaged media, developed specifically for forensic use.

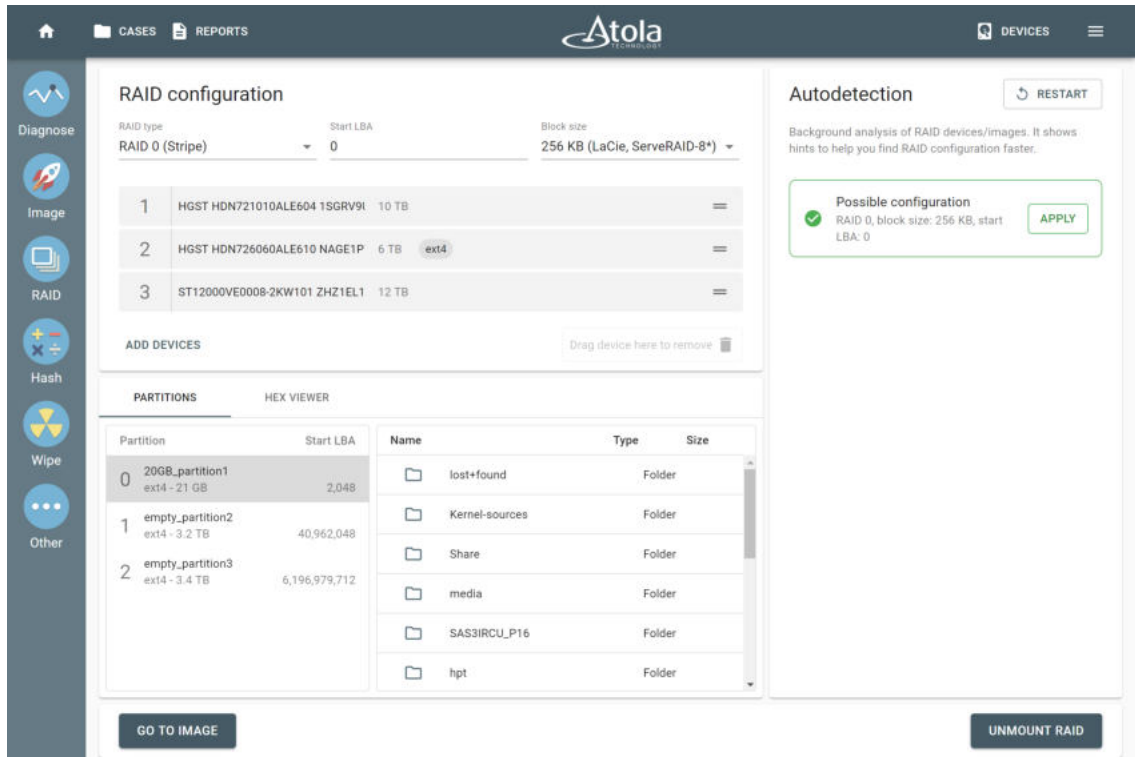
RAID configuration autodetection and imaging

- RAID identification by data parcing on connected drives and/or image files
- RAID types: RAID 0, 1, 5, 10 and JBOD
- File systems: NTFS, ext4/3/2, XFS, exFAT, HFS/HFS+, FAT32/16
- Instant identification of mdadm-created RAID
- One-click application of a suggested configuration
- Partition preview
- Rebuild of RAID with a missing or damaged device (for certain types of redundancy-enabled RAID)
- Max number of auto-checked RAID configurations: 100,000,000

Functions

Forensic Imaging

- 15 TB/h cumulative speed of imaging
- 12+ simultaneous imaging sessions
- Imaging to up to 5 targets
- Automation via Web API
- Physical imaging to E01, AFF4 and RAW files
- Logical imaging to L01 file
- Source/target switch on all ports
- Hardware write protection in Source mode on all ports



RAID configuration

RAID type: RAID 0 (Stripe)
Start LBA: 0
Block size: 256 KB (LaCie, ServeRAID-8*)

1	HGST HDN721010ALE604 1SGRV9(	10 TB
2	HGST HDN726060ALE610 NAGE1P	6 TB ext4
3	ST12000VE0008-2KW101 ZHZ1EL1	12 TB

Drag device here to remove

	Partition	Start LBA
0	20GB_partition1 ext4 - 21 GB	2,048
1	empty_partition2 ext4 - 3.2 TB	40,962,048
2	empty_partition3 ext4 - 3.4 TB	6,196,979,712

Name	Type	Size
lost+found	Folder	
Kernel-sources	Folder	
Share	Folder	
media	Folder	
SAS3IRCU_P16	Folder	
hpt	Folder	

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

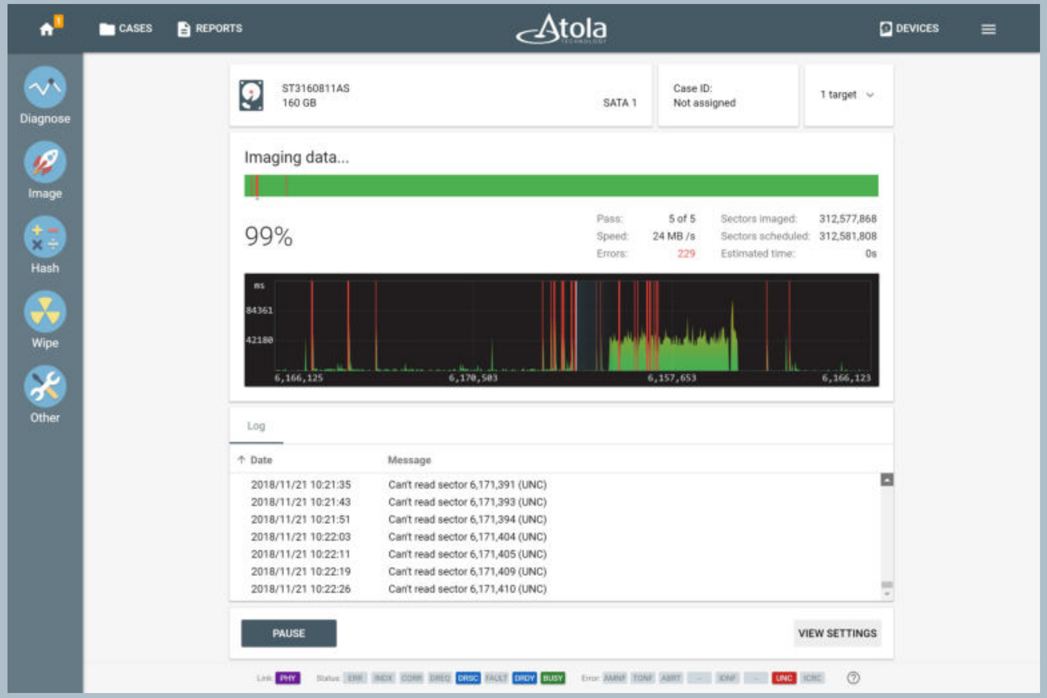
Possible configuration
RAID 0, block size: 256 KB, start LBA: 0

ISO/IEC 27001 Information Security Management CERTIFIED

Atola TaskForce

Damaged drive support

- Imaging data from good heads only
- Imaging freezing drives
- Imaging drives with surface scratches and firmware issues
- In-depth drive diagnostics
- Pause/resume an imaging sessions, optimizing the settings to retrieve more data
- Current sensor on all SATA, SAS/SATA, IDE ports
- Automatic overcurrent and short-circuit protection



ST3160811AS
160 GB
SATA 1

Case ID:
Not assigned

1 target

Imaging data...

99%

Pass: 5 of 5
Speed: 24 MB /s
Errors: 229
Sectors imaged: 312,577,868
Sectors scheduled: 312,581,808
Estimated time: 0s

Log

```
↑ Date                 Message
2018/11/21 10:21:35    Can't read sector 6,171,391 (UNC)
2018/11/21 10:21:43    Can't read sector 6,171,393 (UNC)
2018/11/21 10:21:51    Can't read sector 6,171,394 (UNC)
2018/11/21 10:22:03    Can't read sector 6,171,404 (UNC)
2018/11/21 10:22:11    Can't read sector 6,171,405 (UNC)
2018/11/21 10:22:19    Can't read sector 6,171,409 (UNC)
2018/11/21 10:22:26    Can't read sector 6,171,410 (UNC)
```

Two ways to manage TaskForce

10Gb Ethernet network

Standalone mode

Supported Drives

- 1.8-inch, 2.5-inch, 3.5-inch IDE
- USB hard drives
- SATA, SAS
- USB Flash media

(Optional) With extension modules:

- M.2 NMVe/PCIe/SATA SSDs

- Latest Apple SSDs via Thunderbolt extension

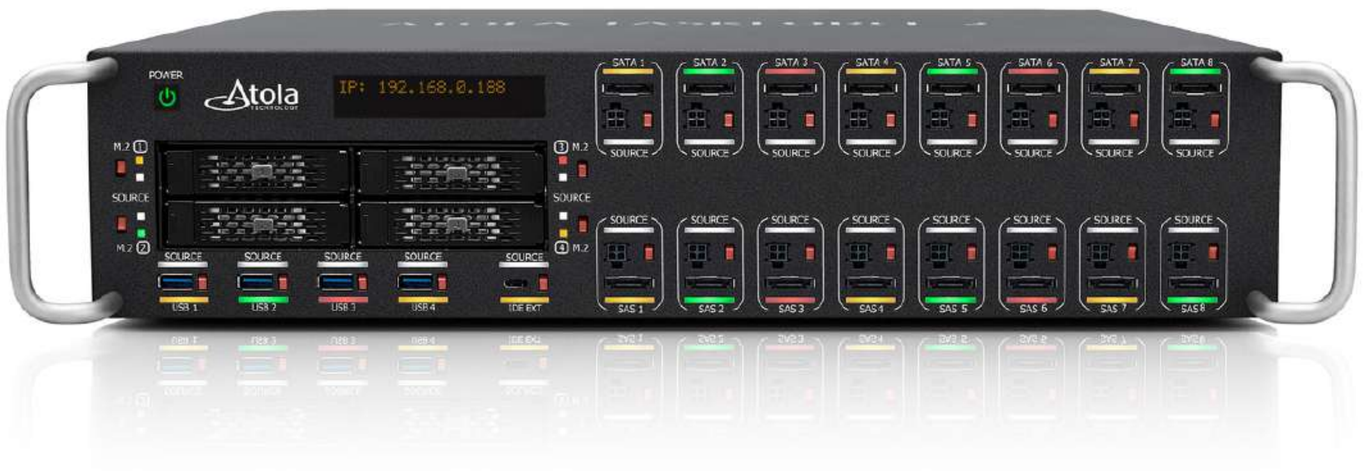
- The newest PCIe SSDs from Apple MacBooks (2013 - 2015)

Other features of TaskForce forensic imager

- Wiping with various methods: Pattern, Secure Erase, NIST 800-88, DoD 5220.22-M, Random, LBA number
- Browse files on any connected device
- SMART viewing + recording it before and after image acquisitions
- Hash calculation (linear and segmented): MD5, SHA1, SHA256, SHA512
- HPA & DCO control and recovery
- Automatic report generation
- Case management system

*** For further information, please visit https://www.atola.com/products/taskforce/**

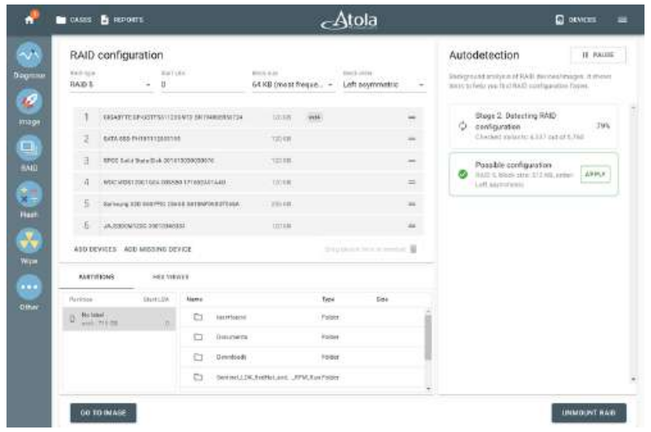
Atola TaskForce 2

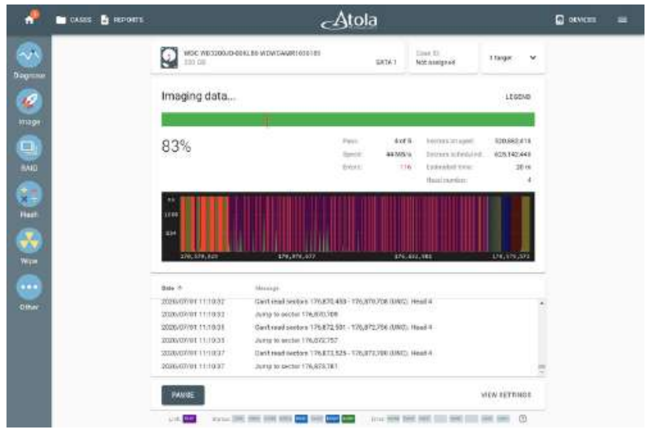


Atola TaskForce 2 is a top-performance forensic imager capable of running **25+ imaging sessions** in parallel, automatically retrieve data from damaged media, detect and reassemble unknown RAID arrays.

TaskForce 2 has **26 ports**: 8 SATA, 8 SAS/SATA, 4 NVMe (M.2 and U.2), 4 USB, IDE and extensions for Thunderbolt and Apple PCIe SSDs. Two 10Gb Ethernet ports are available for fast data transfer. Device racks for convenient and secure drive organization.

TaskForce 2 can be connected to a network and operated by multiple users in Google Chrome browser on their own devices. An offline Kiosk mode use is available, too.





Imaging 25+ drives simultaneously at 25 TB/hour

Atola TaskForce 2 lets you multi-task using the fastest imaging engine thanks to its server-grade motherboard, 16-thread Xeon CPU 3.7 GHz and ECC RAM

- 25+ imaging sessions in parallel plus other tasks
- **25 TB/hour** cumulative speed of imaging
- imaging at 500+ MB/sec on SSDs, 4 GB/sec on NVMe
- Source/target switch on all ports for maximum flexibility
- Hardware write protection in Source mode on all ports
- Integration with **workflow automation** tools via Web API
- Pause and resume any imaging session
- Imaging to up to 5 targets including E01, RAW, AFF4 files in the networks, on other drives, VeraCrypt-protected drives
- Express mode (configure, activate and connect drives to have them imaged without further clicks into the selected destination)
- Powerful **logical imaging** module with smart filters for files and folders, time and size ranges to save time and target space

RAID autodetection, reassembly and imaging

Autodetection for RAID arrays with an unknown configuration:
- identifies RAID type by reading data on selected members
- processes thousands of potential configuration variants
- one-click application of a suggested configuration
- partition preview for visual assessment of a reassembled RAID
- rebuild of RAID even with a missing or damaged device (for redundancy-based RAID)
- physical or logical imaging of a complete RAID or its elements
- Currently supported: RAID 0, 1, 5, 10, JBOD

Damaged drive support

Atola's data recovery engine is fully automated and is designed to retrieve maximum data fast and avoid further damage.

- In-depth drive diagnostics
- Automated data recovery with a multi-pass algorithm
- Selective head imaging
- Automatic reset of freezing drives
- Current sensors on all SATA, SAS/SATA, IDE ports
- Overcurrent and short-circuit protection on all ports
- Segmented hashing for damaged drive image verification

Atola TaskForce 2

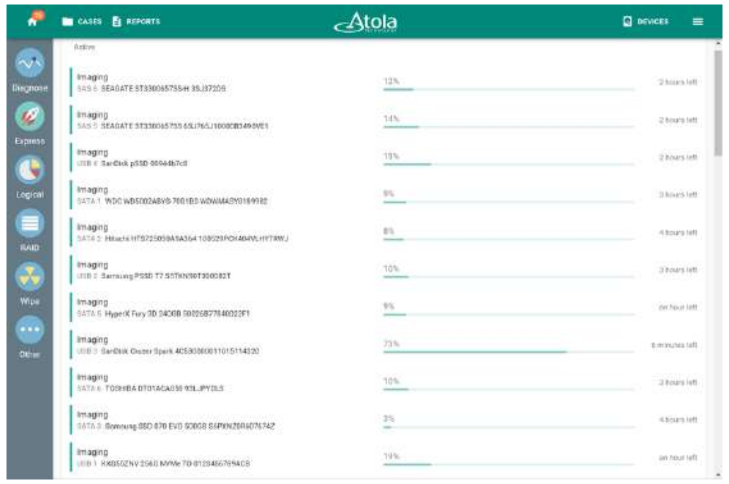
Connectivity options

1. 10Gb Ethernet network
Open TaskForce interface on any device within the same local network by entering the IP address displayed on the front panel in Google Chrome. The system has two 10Gb ports.

2. Kiosk mode
For offline use, plug in a monitor, a keyboard and a mouse to the system. The interface will be immediately available.

3. Wi-Fi connection
TaskForce has an optional Wi-Fi adapter, by plugging which you can operate the unit in a secure network via a laptop, tablet or smartphone.

Multi-user access & user interface



The interface is designed for examiners with all levels of technical proficiency:

- Operated via Chrome browser
- Simultaneous use by multiple operators
- User management system limiting access to others' cases
- Launch of any operation within 2 - 5 clicks
- Highly intuitive task-oriented user interface

Other features

- **Drive content triage** via Browse file feature and in the Logical imaging module
- Wiping on all ports (26 devices in parallel)
- HPA, DCO & AMA control and recovery
- Hash calculation: MD5, SHA1, SHA256, SHA512
- Wiping (SecureErase, NIST800-88, DoD 5220.22-M, etc.)
- Case management system and automated reports
- S.M.A.R.T. view
- Supported file systems NTFS, ext4/3/2, XFS, APFS (with encrypted volumes), exFAT, HFS/HFS+, FAT32/16
- **Device racks** for convenient and secure drive organization
- Server rack compatibility

Lifetime warranty

Atola stands behind its products. We offer the best warranty in the industry. Keep annual subscriptions active for:

- 2-3 software updates
- training and knowledge refresh sessions for the users
- lifetime warranty on hardware
- support from the team of developers

The Leading macOS Imaging, Triaging, and Reporting Solution

RECON *ITR* is a one-of-a-kind solution that acquires and processes Intel and Apple Silicon Macs like no other tool on the market. This marvel of forensic innovation is built from the ground up on macOS using Mac's full power instead of fighting against it.

RECON *ITR* requires no reverse engineering and is not ported from other operating systems, which means more data and more accurate results.

SUMURI has designed RECON *ITR* with the customer in mind, ensuring examiners have the most versatile tool available when changes occur to Apple hardware or Mac operating systems. RECON *ITR* accomplishes this and much more by including unique and revolutionary features while keeping the price significantly lower than competitors.

- Includes Three Imaging Solutions Suited for Any Case (LIVE and Bootable)
- Supports live and bootable imaging of Intel and Apple Silicon Chips
- Only True Triage Solution for Live Running Macs or Macs Connected in Target Disk Mode
- Contains Full Report Capabilities with Sequential Processing of Proper macOS Timestamps
- Correctly Uses Apple Extended Metadata with macOS Native Libraries
- Automatically Collects Volatile Data
- Ability to Automatically Triage Boot Camp and iOS Backups
- Includes PALADIN PRO for Windows and Linux Support

RECON ITR
macOS IMAGE TRIAGE REPORT

SUMURI
RECON ITR
macOS IMAGE TRIAGE REPORT
MAC FORENSICS SIMPLIFIED
Designed for both novice and advanced investigators
Find thousands of artifacts from Mac, Bootcamp, iOS and more!
SAMSUNG Official Partner
PALADIN
Samsung Portable SSD T7 Touch

THREE IMAGING SOLUTIONS FOR THE PRICE OF ONE

With the advent of new technologies like Apple Silicon that are continuously changing, some situations allow for a bootable solution, some call for targeted acquisition, and some may even require a live acquisition. RECON ITR includes both a Live and Bootable imager to ensure that you are ready for every situation.

Every purchase of RECON ITR includes two state of the art SAMSUNG drives:

- Samsung T7 SSD with Live and bootable versions RECON ITR for live triage, and reporting, along with both physical and logical imaging options
- SAMSUNG DUO 128 GB USB with PALADIN PRO with built-in CARBON (demo available) for Windows and Linux support

Support for Intel and Apple Silicon Processors

The Mac environment has undergone another massive shift in processors, moving from the long-used Intel processors to an ARM-based Silicon processor. RECON ITR now supports both Intel and Apple Silicon processors to cover almost any situation you may encounter when imaging a Mac!

The Only True macOS Triage Solution

RECON ITR is the only solution to truly have the ability to provide answers in seconds with its revolutionary triaging feature in a single tool at no extra cost. It automatically parses important information from both Live and through Target Disk Mode within minutes. Other solutions require you to purchase more tools and take longer to get answers.

FULL REPORT CAPABILITIES

To compliment true macOS triage, RECON ITR has built-in reporting features that allow you to produce professional reports in seconds. Build comprehensive reports using the Global Search and Global Timeline to locate and bookmark only the most critical data and quickly present information in an understandable format with Sequential Processing of proper macOS timestamps.

CORRECT USE OF APPLE EXTENDED METADATA

RECON ITR was built from the ground up on macOS to ensure that RECON ITR supports proprietary metadata used in the Mac environment. Being native to macOS helps ensure that our tool can correctly identify and preserve the Apple Extended Metadata that other tools do not properly integrate.

ABILITY TO TRIAGE BOOT CAMP AND IOS BACKUPS

Like RECON LAB, RECON ITR supports more than just Mac data. RECON ITR has robust support for triaging Boot Camp partitions and iOS Backups.

INCLUDES PALADIN FOR WINDOWS AND LINUX SUPPORT

PALADIN PRO, a full forensic lab with over 150 forensic tools, is now included with all new orders of RECON ITR to image Windows, Linux, and all Intel Macs without having to erase and reinstall your software. PALADIN PRO customers can also try CARBON which is preinstalled for examiners who would like to purchase a license.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

SUMURI

Instant Virtualization is here!
No imaging, No disassembly!

CARBON is SUMURI's premier tool for virtualization with support for almost any Windows system or forensic image.

CARBON allows examiners to see evidence as the user, bypass passwords with the push of a button, and boot into a forensically sound virtual environment avoiding the need for disassembly. Make reports more straightforward and easy to understand by including screenshots and screen recordings form the virtualized environment. Get actionable information and generate professional reports in minutes with RECON for Windows. CARBON includes automated triaging and reporting to allow you to triage Windows machines and images with ease. Advanced data carving capabilities lets you use signature analysis to carve files in unallocated space in Windows machines and images.

- Instant Virtualization of Windows Computers and Forensic Images
- BitLocker Support
- RECON for Windows: Triage Capabilities
- Advanced File Search
- Advanced Data Carving
- Snapshot Differential Analysis
- PALADIN Toolbox - Imagers and Write-Blocking Included
- Now merged with PALADIN!

CARBON
VIRTUAL FORENSIC SUITE

INSTANT VIRTUALIZATION OF WINDOWS COMPUTERS AND FORENSIC IMAGES

CARBON has the ability to virtualize any Windows-based computer without the user's password in seconds. Boot forensics images of Windows machines to analyze them in a native environment. Virtualizing with CARBON lets the examiner see and document the computer in the exact state that the original user saw it without making any changes to the source device.

BITLOCKER SUPPORT

CARBON can virtualize Windows machines that are BitLocker encrypted with ease! Enter the recovery key upon booting the device, and within seconds, you will be logged into the user's account! Combining this with our unique ability to bypass Windows passwords allows CARBON to virtualize virtually any computer.

RECON FOR WINDOWS: TRIAGE CAPABILITIES

Examiners can instantly triage any Windows machine or forensic image using the included RECON for Windows. It also includes a reporting feature to easily generate professional reports within minutes.

ADVANCED FILE SEARCH

CARBON's Advanced File Search allows examiners to locate specific files by searching for file names, keywords, file signatures, and even custom defined file signatures.

ADVANCED DATA CARVING

Advanced File Carving allows examiners to recover hundreds of different file types in unallocated space and complete space using a built-in signature database for easy carving options as well as creating customizable signature sets.

SNAPSHOT DIFFERENTIAL ANALYSIS

SnapCompare lets examiners inspect a system for modification or tampering by comparing two Windows machine snapshots to assist with incident response and Malware investigations.

PALADIN TOOLBOX - IMAGERS AND WRITE-BLOCKING INCLUDED

PALADIN Toolbox is included for all your imaging and write-blocking needs! Images created in the PALADIN Toolbox can later be virtualized within CARBON!

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

Reputation is everything.
We help you keep it.

RECON LAB is SUMURI's flagship forensic analysis suite designed from the ground up on macOS to utilize Mac's power and give examiners access to an entirely new realm of data. RECON LAB takes traditional computer forensics and revitalizes it to be more in line with 21st century technologies through many unique and revolutionary features using native macOS libraries, sequential processing into both analysis and reporting, fully automated processing of many different operating systems, and much more.

SUMURI designed RECON LAB with every type of examiner in mind. Our three-stage approach to analysis makes sure that brand new examiners and seasoned veterans alike can get accurate results fast. Step One is automated analysis that supports the automated parsing of thousands of artifacts from macOS, Windows, iOS, Android, and Google Takeout. Step Two is semi-automated analysis using our advanced forensic viewers that assist in parsing and examining macOS Property Lists, SQLite Databases, Windows Registry and Raw Data. Step Three includes Sequential Processing and WYSIWYG reporting features through the use of StoryBoard reporting. Hundreds of revolutionary features built into RECON LAB makes manual analysis easier.

- Native to macOS
- Correctly Uses Apple Extended Attributes and Apple Timestamps with macOS Native Libraries
- Automated Analysis of macOS, Windows, iOS, Android, and Google Takeout
- Sequential Processing (Timeline Analysis)
- StoryBoard - First of its Kind WYSIWYG Forensic Reports

WYSIWYG means " what you see is what you get "

RECON LAB
FORENSIC SUITE

SUMURI
RECON LAB
FORENSIC SUITE
SEE MORE, MISS LESS - 3 STAGE PROCESSING - OVER 250 TIMESTAMPS SUPPORTED
Mac
SUMURI.COM

NATIVE TO macOS
RECON LAB is developed natively on macOS and utilizes native Mac libraries to offer the most accurate representation of acquired data. These native features allow RECON LAB to display Apple Extended Attribute data with the proper macOS Timestamps missed by other forensic tools. Being designed on macOS allows RECON LAB to include a unique Hybrid Processing Engine, enabling images to be mounted and processed faster than other tools. Combining these attributes and our automated analysis functions creates one of the world's most powerful forensics suite.

CORRECT USE OF APPLE EXTENDED ATTRIBUTES
RECON LAB stands alone to integrate and support Apple Extended Attributes and proper macOS Timestamps fully. This unique and Mac-native form of metadata supports hundreds of extended attributes that can completely change a case's outcome and provide unparalleled information to examiners. Other forensic tools overlook this data, while RECON LAB makes these an essential part of the tool. RECON LAB utilizes Apple Extended Metadata, POSIX, and application-specific timestamps to give examiners as much information as possible.

AUTOMATED ANALYSIS OF macOS, WINDOWS, iOS, ANDROID, AND GOOGLE TAKEOUT
RECON LAB automates the analysis of thousands of supported artifacts, spanning macOS, Windows, iOS, Android, and Google Takeout! Simply by loading a forensic image, folder, or backup and selecting the plugin will pull all associated data and present it in an easy-to-understand format.

SEQUENTIAL PROCESSING (TIMELINE ANALYSIS)
RECON LAB features two unique ways to display information sequentially with Super Timeline and Artifact Timelines. Super Timeline generates global level timelines in a CSV or SQLite database to show all events as they transpired. Meanwhile, the Artifact Timeline visually represents events based on the timestamps collected through automated analysis. Both can provide a way to present the collected data visually to significantly reinforce case opinions.

STORYBOARD
RECON LAB's revolutionary reporting feature, StoryBoard, features many innovations to automate and enhance the reporting process. StoryBoard includes features to add bookmarked files in chronological order and include external files to help make the report more coherent. RECON LAB includes the first of its kind revolutionary WYSIWYG forensic report editor - StoryBoard. With StoryBoard's report editor, examiners can fully customize and tailor their reports to provide the most comprehensive, user-friendly, and coherent reporting experience of any tool on the market.

ABOUT SUMURI
SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, RECON ITR, RECON LAB, and TALINO Forensic Workstations

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

binary data

CSI RESPONDER

CSI Responder utilizes customized hardware and software to initiate target devices in compliance with legality, bypass system or disk encryption, and create high-speed disk images of the target device content using built-in imaging tools, in conjunction with CSI Responder 's high-speed data interface and high-quality storage. Additionally, the customized Windows system includes various common device drivers and computer forensic analysis software, operating system emulation software. Users can also install various forensic software as needed for rapid analysis of the target device.

CSI Responder primarily addresses the following pain points:

- The increasing prevalence of non-removable storage in laptops / tablets
- Growing use of built-in encryption chips (TPM/T2/Apple Silion) for disk encryption
- Increasing capacity of hard drives and the limited time available on-site investigation

Hardware

Storage Interfaces	Dual-channel interface compatible with the latest Thunderbolt 3/4, USB4, featuring built-in 2TB*2 high-performance NVMe SSD
Bootable Drive	The Windows forensic disk includes WinToGo, X64FE, X86FE, ARM64FE. (Default source write blocker) The Mac forensic disk includes MacOS 15.6 boot system and X-ImagerMac imaging tool
External Hub	USB 3.2 Gen2 x2 (Type-A, 10Gbps),USB 3.2Gen2 x1 (Type-A, 10Gbps),100W PDx1 and other.

Build-in Software

CSI Imager：Self developed high-speed imaging tool with support for creating full disk decryption images

X-Imager: Self developed imaging tool for Apple computers, supporting the acquisition of Sparseimage or DMG images from T2 or Apple Silicon Apple computers.

WinToGo: The forensic system supports built-in third-party imaging tools or forensic analysis software.

CSIRESPONDER

Key Features

1 Non-dismantling Imaging

CSI Responder supports imaging hard drives of laptops, Windows tablets, and desktop computers without dismantling.

1. Compatible with over 95% of laptops, desktop computers, and Apple computers in the market with both Intel and ARM architectures.
2. Built-in disk offline write protection function in the forensic system, enabling non-dismantling read-only acquisition of the source disk image.
3. Multi-channel parallel imaging cache, tested with Thunderbolt 3/4, USB4 interfaces achieving speeds of up to 120GB/min with dual-channel access, and speeds exceeding 60GB/min for single-channel access.
4. Supports non-dismantling forensics of the latest ARM architecture tablets, such as Surface Pro X, Huawei

2 Disk Decryption

TPM (Trusted Platform Module)

MAC - T2 & Apple Silicon（M1/M2/M3）

3 Unbreakable Fast

Protocol	Thunderbolt + USB quad channel
Imaging Speed	120-150GB / min

Device Specifications

Dimensions: 120mm*100mm*20mm (Length x Width x Height)

Storage Channel Interfaces: Thunderbolt 3 x 2, USB-C x 2

External Interfaces: USB-A (3.1 Gen2, 10Gbps) x 2

Power Input: 12V (18W), supports power supply from power banks and charging adapters

4 Operations without 220V power supply

Our main unit supports powering devices via portable power banks, enabling on-site forensic work even without utility power.

Belkasoft X
Evidence Center

RELIABLE END-TO-END SOLUTION TO ACCELERATE DIGITAL FORENSICS AND INCIDENT RESPONSE INVESTIGATIONS

Belkasoft
forensics made easier

Learn more
belkasoft.com

702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085 United States
(650) 272-03-84
email: sales@belkasoft.com

DATA SOURCES

- **Mobile devices** Android, iOS, Windows
- **Computers & laptops** hard drives, disk images, virtual machines
- **RAM**
- **Cloud**
- **Third-party images**

BELKASOFT EVIDENCE CENTER X

ACQUIRE

- E01/DD imaging
- Jailbreak Support
- Agent-Based Acquisition
- Checkm8

EXAMINE

- Chat Apps
- Browsers
- Mailboxes
- Documents
- Pictures & Videos
- Audio
- System Files
- Mobile Apps
- Payment Apps
- Online Games
- Clouds
- P2P

REVIEW & ANALYZE

- File System Explorer
- Artifacts Viewer
- SQLite Viewer
- Registry Viewer
- Plist Viewer
- Timeline
- Hash Set Analysis
- Advanced Picture and Video Analysis
- Connection Graph
- Cross-Case Analysis
- Incident Investigations
- WDE and File Decryption

REPORT

- Customizable Reports In Multiple Formats
- Free Portable Case Viewer

Belkasoft N

Incident investigations

Belkasoft Incident Investigations (Belkasoft N) is a tool for digital incident investigations and is aimed to incident response professionals, working in a corporate environment. The product helps to identify traces left over from malware and hacking attempts on a Windows computer.

https://belkasoft.com/get

KEY FEATURES

- Detect suspicious traces in most typical locations, including registries, event logs and less known files
- Analyze how malicious code persisted in the system by analyzing services, scheduled tasks, WMI subscriptions, Applinit DLLs and so on
- Learn how and when malware was executed by examining various artifacts such as Amcache and Shimcache, Syscache, BAM and DAM
- Extract remote connections details including IP and time stamps for RDP and TeamViewer
- Find potential initial attack vector by analyzing recently opened documents and browser links, latest downloads and so on
- Search inside extracted information, bookmark important data and create reports in multiple formats

WHY SHOULD YOU CONSIDER BELKASOFT N?

Quick

Quickly respond to hacker attacks thanks to all necessary data conveniently presented on a single screen.

Comprehensive analysis

Detect impactful security events by analyzing numerous sources, such as registry, event logs, other system files and less known sources.

Search, bookmarking and reporting

Search inside found artifacts, bookmark important data and generate comprehensive incident reports right after the analysis stage.

Compatibility with other tools

Benefit from the analysis functionality of images acquired by Belkasoft X, Belkasoft R, and Belkasoft T as well as by the third-party tools.

Affordable

Comparing to the pricing of the alternative products, it will fit your budget easily.

USE CASES

- Endpoint attacks
- Malicious email activity
- Anomalous user activity
- Remote access attacks
- Attacks correlation with known vulnerabilities

Belkasoft
forensics made easier

Learn more
belkasoft.com/n

702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085 United States
+1 (650) 272-03-84
email: sales@belkasoft.com

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Premium Forensic Bundle

Every tool we make in a deeply discounted value pack. Extract data from mobile devices, unlock documents, decrypt archives, break into encrypted containers, view and analyze evidence with all-in-one Premium Forensic Bundle.

DIGITAL FORENSICS USING PREMIUM TOOLS

Support for more than 500 types of data

Our tools support 500+ application versions and file formats allowing users to recover passwords to Microsoft Office and OpenDocument files, Adobe PDF files, PGP disks and archives, Windows and email accounts, MD5 hashes and Oracle passwords, and remove many more types of password protection (list of supported formats).

Accessing data instantly

In many cases, Elcomsoft Premium Forensic Bundle is capable of instantly recovering passwords for a wide range of applications. Our tools exploit every known vulnerability to unlock documents instantly or near instantly, while employing smart attacks and high-end hardware acceleration techniques to quickly recover strong passwords.

Targeting the human factor

Our products offer a range of highly intelligent attacks based on the knowledge of human nature. By targeting the human factor, our smart attacks significantly reduce the number of passwords to try and increase the chance of successful recovery.

Support for popular password managers

Support for some of the most popular password managers including 1Password, KeePass, LastPass and Dashlane. Attacking and recovering a single master password provides access to dozens of passwords to a wide range of resources that are kept in the encrypted database.

25 to 250 times faster attacks with hardware acceleration

Our tools utilize dedicated high-performance cores found in video cards manufactured by NVIDIA and AMD, as well as GPU cores built into Intel CPUs including Intel HD Graphics, UHD Graphics and Intel Iris. Our thoroughly optimized algorithms enable reaching recovery rates that are up to 250 times faster compared to CPU-only benchmarks (CPU vs GPU benchmarks).

Linear scalability on up to 10,000 computers

Our tools enable massively parallel operations and scale linearly to as many as 10,000 workstations and cloud instances with no scalability overhead. Distributed attacks scale over the LAN, Internet, or both. Minimum bandwidth requirements ensure no scalability overhead even for the slowest connections.

Dictionary attack

Using the prepared dictionaries based on leaked password databases or building own password dictionaries based on instantly recovered passwords. Automatic distribution of custom dictionaries across running agents.

Cloud computing

Quickly add computing power on demand by utilizing Amazon's GPU-accelerated EC2 Compute Units or Microsoft Azure instances. Password recovery running in an Amazon or Microsoft cloud is a perfect solution when additional computational power is needed.

Comprehensive Mobile Forensic Solution

The Elcomsoft Mobile Forensic Bundle includes the most essential tools for safe and forensically sound acquisition, decryption and analysis of evidence from a wide range of mobile platforms and cloud services.

Forensic analysis of Apple devices

The newest jailbreak-free low-level access to data offers direct, safe and forensically sound extraction for Apple devices running all versions of iOS from iOS 11 through iOS 13. This new agent-based acquisition provides full file system extraction and keychain decryption without a jailbreak and literally no footprint. The complete forensic acquisition using jailbreak is also available.

More information at www.elcomsoft.com/epfb.html

Obtain iCloud backups, download photos and synced data, access iCloud passwords

Try the most comprehensive iCloud data acquisition on the market enabling forensic access to evidence stored in the cloud with and without the Apple ID password. Access cloud backups, call logs, messages, passwords (iCloud Keychain), contacts, iCloud Photo Library, iCloud files, Apple Health and Screen time, geolocation data and a lot more.

Break passwords to iOS system backups

Brute-force passwords protecting encrypted iOS backups with a high-end tool. GPU acceleration using AMD or NVIDIA boards helps achieve unprecedented performance, while access to users' stored passwords enables targeted attacks with custom dictionaries.

Full over-the-air acquisition of Google Accounts

Google collects massive amounts of information from registered customers. The Premium bundle includes the powerful and lightweight forensic tool to extract information from the many available sources, parse and assemble the data to present information in human-readable form. Extract and analyze user's detailed location history, search queries, Chrome passwords and browsing history, Gmail messages, contacts, photos, and a lot more.

Support for popular instant messengers: WhatsApp, Skype, Signal etc.

Extract, decrypt and view WhatsApp, Skype, Signal and Telegram communication histories from a wide range of devices or cloud services. Instantly retrieve the login and password information protecting user accounts in more than 70 instant messengers for desktop.

YOUR BENEFITS

All in one

A single purchase delivers all ElcomSoft products in their respective top-of-the-line editions that allow recovering passwords and decrypting encrypted data.

Research and development

The password recovery suite features the latest and most advanced cryptanalysis algorithms developed by ElcomSoft research department. We continue to deliver cutting-edge technologies in password recovery and data decryption.

Industry-certified technologies

Elcomsoft is Microsoft Silver Certified Partner, Intel Software Partner and member of NVIDIA CUDA/GPU Computing Registered Developer Program.

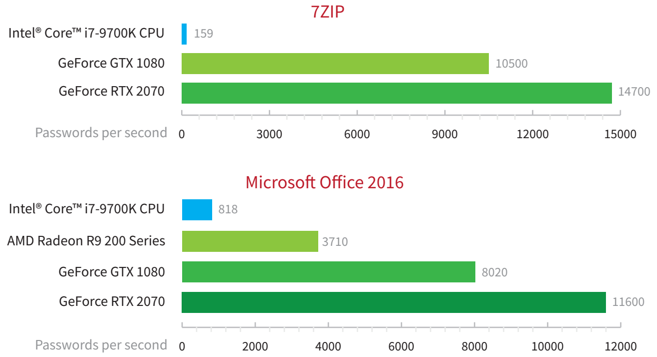
Patented technologies

ElcomSoft pioneered many software innovations that have made it easier to access protected data. The GPU acceleration, which is patented (U.S. Pat. No. 7,787,629 and 7,929,707) and unique to ElcomSoft products, making password recovery up to 250 times faster compared to traditional methods, is just one of the innovations.

Education and consulting

We offer comprehensive three-to-five-day courses offering hands-on experience in unlocking and extracting evidence from mobile devices, accessing password-protected and encrypted computer data.

ElcomSoft Distributed Password Recovery | Version 4.20



ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

www.elcomsoft.com
blog.elcomsoft.com
sales@elcomsoft.com

RUSOLUT

Visual Nand Reconstructor

Chip-off Data Recovery & Digital Forensic analysis of broken flash storage devices.

Application

Physical Damage

Firmware Failure

Electrical Damage

Thermal Damage

Analysis “non-addressed areas”

Non-recognizable disk

Workflow

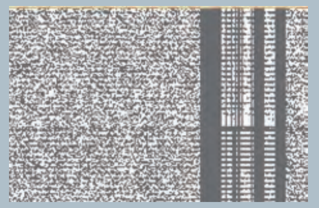
1

Put the chip into the adapter

2

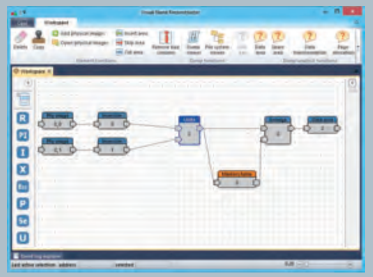
Connect the adapter to the reader and press “Read memory chips.”

3



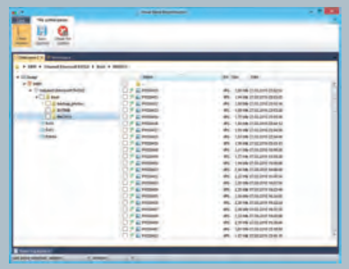
Binary dump file of physical image is produced

4



Rearrange the physical NAND blocks into the logical block by using VNR software

5



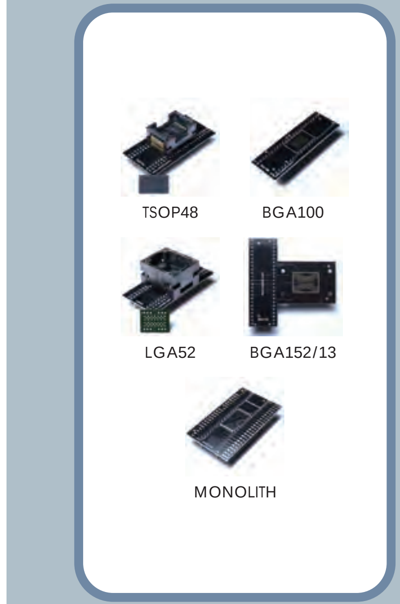
Full file-system structure is shown

Features

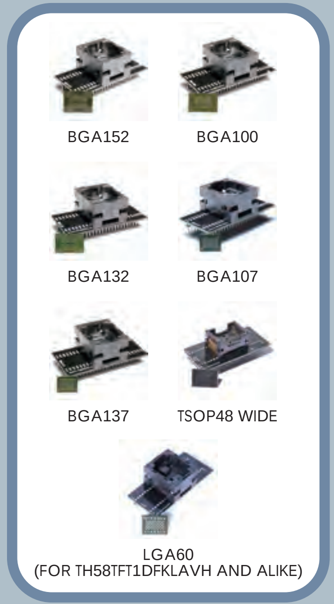
- Data recovery from broken Flash devices
- Forensic analysis of NAND physical image
- Analysis of hidden/obsolete/bad blocks of NAND memory
- Automatic analysis modes
- Largest set of adapters on market
- Powerful manual analysis and reverse engineering modes
- Unique dump viewer modes
- Support of microSD and other monolithic devices
- Flexible software conception and intuitive GUI with database
- Power adjustment for weak and mobile chips (1.8V...4.0V) separately for core and IO bus

Options

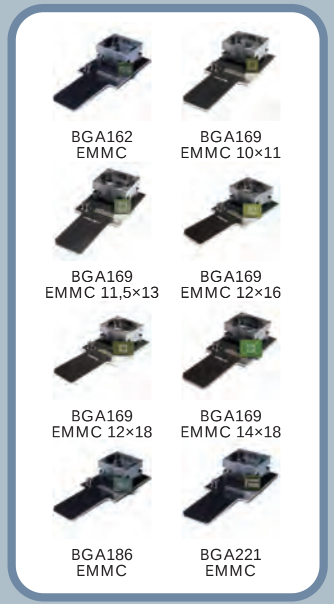
Starter Kit



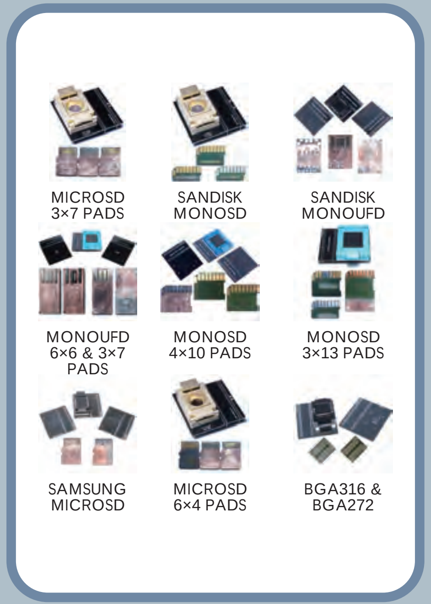
Standard Kit



EMMC Adapter Kit



Monolithic NAND Adapters



*** For further information, please visit https://rusolut.com/**

Data Expert

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CYACOMB FORENSICS

www.cyacomb.com

The game-changing rapid triage tool Cyacomb Examiner Plus

The ultimate in speed, ease of use, and thoroughness

BOOK 21 DAY TRIAL

BOOK DEMO

Cyacomb Examiner Plus offers our core technology for on-scene triage - Contraband Scan. Using a combination of block level hashing, statistical sampling, and our proprietary Contraband Filters, illegal content can be found on suspect devices up to 100x times faster than traditional file hash technology.

#1 choice of investigators who want results in seconds

Mobile Device Triage, available as a feature of Cyacomb Examiner Plus, is a vital evolution of our game-changing tools. In a world where an astounding 95% of people access the internet through their mobile phones, you can now scan Android and iOS mobile devices for known CSAM and get evidence in seconds.

With Cyacomb Examiner Plus, you will get:

- ✓ Accelerated on-scene triage by finding evidence in seconds, even from large or slow devices
- ✓ Simple-to-use intuitive interface – scan in 3 steps
- ✓ Easy-to-read traffic light results to support your decision to seize
- ✓ Identified previously known files and showed their category/classification
- ✓ Rapidly detected remnants of deleted and partially downloaded files without the need to carve for files
- ✓ Rapidly detected and flagged encryption for further investigation
- ✓ Simultaneous Contraband Filter scans on multiple devices (mobile devices and hard drives)
- ✓ Detailed HTML reports (can be saved in PDF)
- ✓ Previews and report creation, with optional evidential thumbnails
- ✓ Flexibility to run from a forensic computer, bootable media, or live on suspect devices
- ✓ Scan PCs, Macs, Apple iOS, Android, external drives and SD cards
- ✓ Full control of scan options

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT OUR SALES TEAM
EMEA/APAC +44 131 608 0195 | US +1 202 660 1869 | sales@cyacomb.com

CYACOMB FORENSICS

www.cyacomb.com

> *"We connected 2 external hard drives (500GBs each) and 3 thumb drives (16GBs, and 2 64GBs) to Cyacomb's tool. We received an initial positive hit for the presence of child sexual abuse material in approximately 10 – 15 seconds and within 45 seconds had positive hits on all the devices for the presence of child pornography/child sexual abuse material.*
>
> *Cyacomb has taken a process that until now has taken hours to complete and reduced that time down to less than a minute."*
>
> **DETECTIVE MIKE FONTENOT OF DALLAS PD**

Along with Mobile Device Triage and Contraband Filter Scan, **Cyacomb Examiner Plus** also offers **Filename Scan.** It allows suspect devices to be quickly scanned for file names that contain indicative or relevant keywords.

Now your time to first evidence while on-scene can be reduced from hours to minutes

Cyacomb Examiner, which offers our core technology for on-scene triage - Contraband Scan, remains available.

	CYACOMB EXAMINER	CYACOMB EXAMINER PLUS
INSTALLED	CONTRABAND SCAN	CONTRABAND SCAN FILENAME SCAN MOBILE DEVICE TRIAGE
LIVE	CONTRABAND SCAN	CONTRABAND SCAN FILENAME SCAN

Both Cyacomb Examiner and Cyacomb Examiner Plus can be used from the user's own forensic workstation or directly on target devices using a USB. With installed mode, you can scan multiple devices simultaneously.

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT OUR SALES TEAM
EMEA/APAC +44 131 608 0195 | US +1 202 660 1869 | sales@cyacomb.com

CYACOMB FORENSICS

↗ www.cyacomb.com

Cyacomb Offender Manager

Empowering frontline investigators to easily detect illegal content and produce clear, easy-to-understand results in seconds

↗ BOOK DEMO

Fast
Use on scene to get results in seconds

Simple
Intuitive to use, portable and easy to deploy

Thorough
Identify illegal material with 99.9% confidence

- ✓ No deep digital forensic knowledge required
- ✓ Simply plug and scan
- ✓ Make informed decisions to seize while on scene

IF YOU HAVE ANY QUESTIONS, PLEASE GET IN TOUCH WITH OUR SALES TEAM
EMEA/APAC +44 131 608 0195 |
US +1 202 660 1869 |
sales@cyacomb.com

CYACOMB FORENSICS

↗ www.cyacomb.com

Cyacomb Offender Manager

Built for front line investigators, by front line investigators

> *Cyacomb has taken a process that until now has taken hours to complete and reduced that time down to less than a minute."*
>
> DETECTIVE MIKE FONTENOT OF DALLAS PD

Cyacomb technology has been created to find evidence faster to protect more people.

Now your time to first evidence while on-scene can be reduced from hours to minutes!

Using a combination of block level hashing, statistical sampling, and our proprietary Contraband Filters, Cyacomb Offender Manager can find evidence of known child abuse or terrorist activity on suspect's devices up to 100x faster than traditional methods.

It can be pre-configured by digital forensic experts, making on-scene use simple plug-and-play, generating fast, accurate, and clear results.

With Cyacomb Offender Manager, you will get:

- ✓ Accelerated on-scene triage by finding evidence in seconds, even from large or slow devices
- ✓ Simple-to-use intuitive interface – scan in 3 steps
- ✓ Easy-to-read traffic light results to support your decision to seize
- ✓ Free Training

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT OUR SALES TEAM
EMEA/APAC +44 131 608 0195 | US +1 202 660 1869 | sales@cyacomb.com

Forensics Acquisition of Web Sites

Take authentic online content
to civil and criminal court.

What is FAW?

All data acquired using FAW have legal value and can be used in court.

FAW is a software that includes a set of tools to capture any type of web page: static and dynamic, CMS, Mobile, E-Commerce, Social Network, Dark Web, Intranet, etc.

FAW makes the process of collecting content easy by doing it for you. The entire acquisition process is fully automated by the software to avoid the risk of human error typical of manual procedures, guaranteeing the undeniable validity of the collected data.

FAW is the first forensic browser, the best known in the world and the only one that guarantees the authenticity, compliance and unalterability of the web pages it captures.

Characteristics of FAW

EASY TO USE
It works like a browser. Everyone, even users without any IT knowledge can collect digital evidence independetly.

SECURE STORAGE
All files are stored on your computer and can be accesed offline whenever you wish. Integrity is guaranteed.

CERTAIN DATE
Each document you download has a certain and certified date. This guarantees their authenticity and integrity over time.

TRAINING AND SUPPORT
Provide training resources and technical support for investigators on the effective use of the digital forensics application.

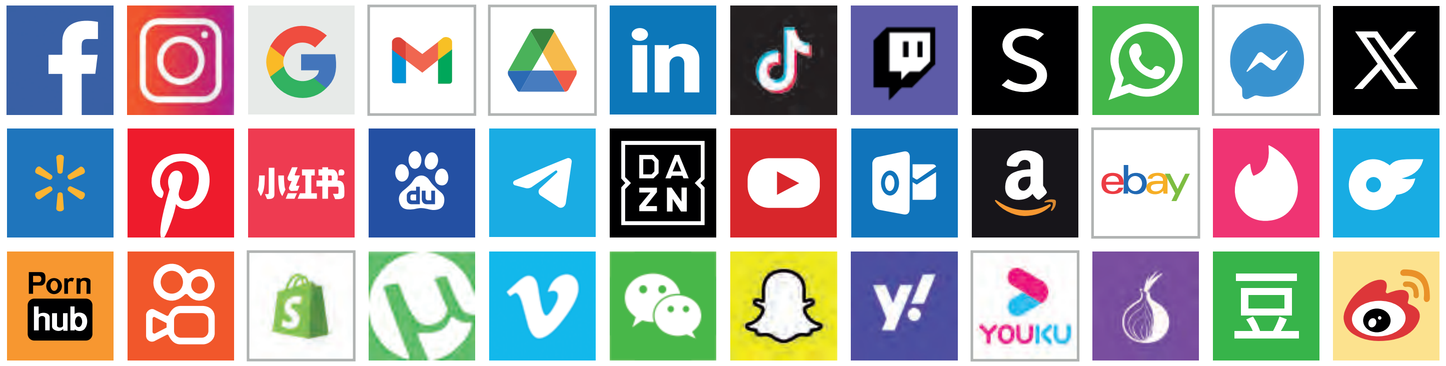
LEGAL VALIDITY
Recognized by the computer forensics community. All documents downloaded using FAW are legally valid.

UNLIMITED ACQUISITION
You can repeat the acquisitions as many times as you wish. Once the license is purchased, there are no usage limits of any kind.

USED BY LAW ENFORCEMENT
Trusted by the majority of law enforcement agencies in the world, the version is designed to store data on the servers.

FORENSICS REPORT GENERATION
Generate detailed and customisable forensic reports that document the evidence collected and analyses performed.

What can you capture?



Why choose FAW?

We are the first and only forensics browser since 2011 and supported by an extensive worldwide reseller network offering technical support to users.

It's easy to use and without the possibility of making mistakes and also, the most complete forensics capture software on the web with automated forms for the most important social networks.
It was created and developed by indipendent and established companies (not start-ups) and it is supported by an extensive worldwide reseller network offering technical support to users.

FAW is the most ethical, suited to the needs of students, professors, and associations with free licenses to spread knowledge of the digital forensics best practices and it is available in many languages
and tested by the world's leading forensics communities.

Compliance

CERTIFIED ★★★ CERTIFIED ★★★ CERTIFIED

The "FAW – Forensics Acquisition of Web sites" software was developed and is kept updated following the regulatory indications of international standards on the subject of computer data acquisition, it also complies with the other standards, in terms of Network Forensics and Cloud Forensics, established and recognized by the technical-scientific community at national and international level.

FAW is compliant with the International Organization for Standardization, ISO/IEC 27037/2012: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

Acquisition modes

FAW offers a wide range of capture modes. All its features have been developed in accordance with national and international legislation, scientific articles and best practice in digital forensics.

FACEBOOK
Grabs Facebook URLs with extensive configuration on the types of pages and items to grab.

YOUTUBE
Capture YouTube pages, download and certify the videos present and all the linked items.

STOP
It allows you to capture the overall behavior of pages and multimedia content over time and keeping the recording of the screencast.

MAIL
The module allows you to connect to mail servers and to download and certify all the emails in your mailbox.

MULTI
FAW in multi-page version, allows the automatic capture of a list of web pages. Perfect for capturing entire websites.

REPORT
With this tool you can create a detailed report of all the activities carried out with the FAW suite.

TORRENT
Captures through the most popular p2p protocols all streams from both files and servers through URLs.

WHATSAPP
With this tool you can capture entire Whatsapp chats. Download and capture any item present in the chats.

TOR
Capture web pages on the Darkweb through the TOR network. Carefully evaluate the risks and act responsibly.

BOT
It is a crawler aimed at finding all the pages linked to the main page. Allows you to search sites with login-protected areas.

FTP
This tool allows you to capture entire websites in FTP and SFTP mode without changing metadata of copied files.

Our licenses

On Demand

The ideal solution to make all the acquisitions you want within 24 hours, at an extremely affordable price.

It is ideal for those who need to have all the advanced features of the product to acquire any type of web page with legal value.

Suitable for technical consultants and professionals who need automated acquisitions.

Professional

The most comprehensive forensic web page capture software.

Suitable for technical consultants and professionals who need automated acquisitions, TOR network and advanced tools to speed up the acquisitions optimizing time and resources.

Verify that you can correctly acquire the web pages you are interested in.

Law Enforcement

Forensic web page capture software designed for the Law Enforcement.

All the features of the Professional version with more functionalities required by operators of the sector.

Each license has an annual duration and is combined with a workstation.

Can only be purchased by law enforcement and government agencies.

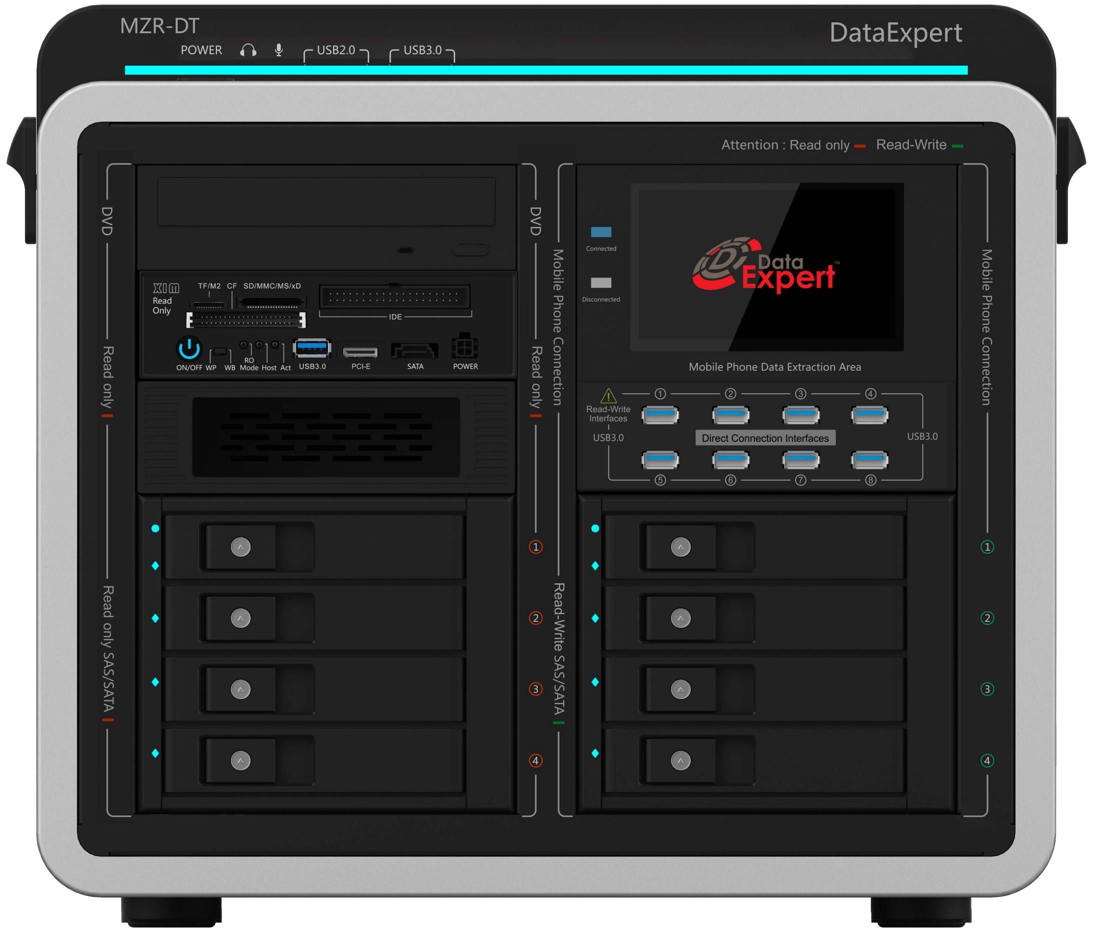
For more info contact us directly from our website:
https://en.fawproject.com/

Follow us on our youtube channel:
FAW - Forensics Acquisition of Websites

Reseller

Data Expert™
https://www.dataexpert.asia/

Envolve Forensics LTD - 41 DEVONSHIRE STREET, GROUND FLOOR
LONDON W1G 7AJ - COMPANY NUMBER 12690094



Mobile Forensic

compelson

MOBILedit Forensic

All-in-one phone forensic tool from pioneers in the field

MOBILedit Forensic is an all-in-one solution for data extraction from phones, smartwatches and clouds. It utilizes both physical and logical data acquisition, has excellent application analysis, deleted data recovery, a wide range of supported devices, fine-tuned reports, concurrent processing, and easy-to-use interface. With a brand new approach, MOBILedit Forensic is much stronger in security bypassing than ever before.

MOBILedit Forensic offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools with its data compatibility.

SECURITY BYPASSING WITH LIVE UPDATES

MOBILedit Forensic has built-in security bypassing for many phone models, allowing you to acquire a physical image even when the phone is protected by a password or pattern. Bypass the lock screen on a wide range of Android phones, so you can keep the investigation moving forward. We are introducing a new approach to security bypassing with Live Updates technology - new phone models can be added even without a MOBILedit reinstallation, just like updating antivirus software!

PHYSICAL DATA ACQUISITION AND ANALYSIS

In addition to advanced logical extraction, we also provide Android physical data acquisition, allowing you to extract physical images of investigated phones and create exact binary clones. Physical analysis allows you to open image files created by this process, or those obtained through JTAG, chip-off or other tools, to recover deleted files plus all other deleted data.

SMARTWATCH FORENSICS

With the rise in popularity of wearable devices, smartwatch forensics plays an essential role and is vital if a smartwatch is the only digital evidence available. MOBILedit Forensic supports smartwatches made by manufacturers such as Apple, Garmin, Samsung, TCL, Huawei, Amazfit and others, via special readers which are available in our Smartwatch Kit.

CLOUD FORENSICS

Besides phone content acquisition, cloud extraction is a necessity to get all possible data. MOBILedit Cloud Forensic supports the most popular cloud-based services such as Dropbox, Box, Microsoft OneDrive, Google Drive, Facebook, Instagram, LinkedIn, Twitter, Facebook Messenger, Slack and many others. This powerful feature is available as a standalone product or can be integrated within MOBILedit Forensic Pro.

DELETED DATA RECOVERY

Deleted data is almost always the most valuable information in a device. It often hides in applications, and we deliver great results in finding deleted data. Our special algorithms look deeply through databases, invalidated pages and within caches to find any data that still resides in a phone.

ADVANCED APPLICATION ANALYSIS WITH LIVE UPDATES

Applications are the most important source of evidence in the phone. The majority of phone activities, including messaging, phone calls, internet browsing and others take place within apps. This is the strongest point of MOBILedit Forensic, we dedicate a large part of our team specifically for application analysis. Data is analyzed for its meaning so you see it on a timeline as a note, a photo, a video or a flow of messages no matter what app was used to send them.

SMART SCREENSHOTS

The Smart Screenshots feature provides a solution for obtaining evidence from applications that cannot be accessed through logical extraction. This advanced feature enables the extraction of conversations and other information from popular messaging apps like Instagram, Signal, Skype, Telegram, Viber, and WhatsApp. The screenshotting is automatic without requiring any user interaction on the device.

CONCURRENT EXTRACTIONS

Speed up your investigation process by extracting multiple phones at the same time, and generating multiple outputs for each one. All you need is a USB hub, cables and a computer powerful enough to perform concurrent jobs. You can finish a week's worth of work overnight!

OBJECT AND FACE RECOGNITION – THE POWER OF ARTIFICAL INTELLIGENCE

Use Artificial Intelligence to find the evidence and speed up your work. This state-of-the-art tool is equipped with the latest deep-learning technology and is designed to rapidly identify photos and videos of what an investigator is searching for. Simply specify a folder of photos and videos and choose items you are searching for, such as pistols, knives, narcotics, money, documents, people, and many others. With this tool, you can now also recognize faces in videos, allowing you to quickly and accurately identify individuals of interest. This advanced feature can help you solve cases more efficiently by automatically detecting and recognizing faces in surveillance footage or other video evidence.

CAMERA BALLISTICS – SCIENTIFIC IMAGE ANALYSIS

The scientific forensic tool that matches a photo to a camera, like a bullet to a gun. When combined with MOBILedit Forensic you are able to identify which images present on the analyzed phone were actually taken by the phone's camera.

DIVE COMPUTER FORENSICS

Delve into underwater data with MOBILedit dive computer forensic analysis. Uncover reasons behind incidents, protocol adherence, and vital dive details. Extract key metrics like water temperature, depth, dive duration, and gas tank readings from over 200 dive computer models, including major brands like Suunto, Oceanic, Cressi and more. Crucial functionality for regions with aquatic landscapes.

INTEGRATE WITH OTHER TOOLS

We all know that it is a good practice to use multiple tools in a lab. We've designed MOBILedit with the ability to integrate with other forensic tools. Import and analyze data files exported from Cellebrite UFED reports to get even more data. We also extract all data into open data format, so you get all the files directly as they are in the phone. This allows you to use many open-source tools.

compelson

www.mobiledit.com
sales@compelson.com

compelson

MOBILedit
Cloud Forensic

Get a complete digital footprint of a suspect

People interact within today's digital universe through their phones and applications, leaving digital footprints everywhere. For a full and successful digital investigation, it is necessary to analyze all traces. Phone forensics is extremely important, but what is stored in a mobile device is only a snapshot of the overall data. The evidence found in clouds, message platforms, and social networks brings complete insight into a person's life. Understand their lifestyle, activities, personality, likes/dislikes, preferences, and social activities through services such as Facebook, Instagram, LinkedIn, Twitter, Slack, or Google apps.

With a successful phone examination provided by MOBILedit Forensic PRO, you have almost everything necessary for a successful cloud extraction. This is because phone applications hold precious login information for most cloud services.

Even without a phone, you can still access data from cloud services that are used by millions of people multiple times a day, every day.

MOBILedit Cloud Forensic is a complete cloud data forensic downloader and report generator for the most popular services. It can immediately start downloads when authentication information is found in a phone, and it can run multiple extractions concurrently when time is of the essence.

CLOUD FORENSICS IS AVAILABLE IN TWO OPTIONS TO CATER TO BOTH NETWORK FORENSIC INTERCEPTION AND MOBILE DEVICE EXAMINERS:

Integration with MOBILedit Forensic PRO

With this option, you can extract data from clouds via a mobile device connected to MOBILedit Forensic Pro. The credentials are extracted from the device, and cloud extraction is started as part of the phone examination process. These credentials are also saved so that an investigator can either use the token or the account login details at a later date.

MOBILedit Cloud Forensic as a standalone product

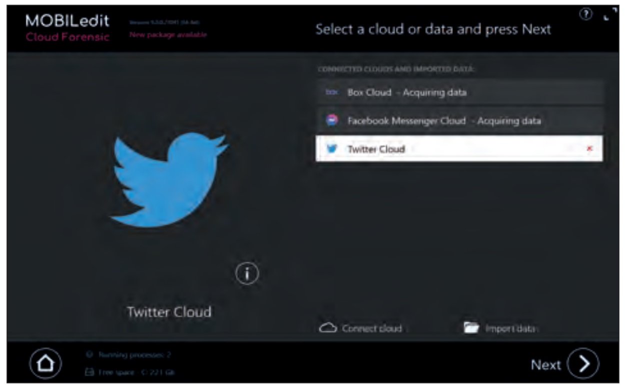
For investigating cloud storage and cloud services without the need to examine mobile devices. Access to clouds using this method requires a password and a username or a token imported from another source.

In both cases, you can investigate more than one cloud at a time, and extractions will run concurrently to help you work faster and retrieve more evidence quickly.

The extractable amount of data is as big as the cloud account. Therefore, you will have to take storage capacity into consideration or filter by time frame at the point of extraction. Additionally, tokens do have an expiration date depending on the service provider.

FEATURES

- Automatic download of clouds using either an authorization token or a username and password credentials. These can be found, extracted, and saved from a phone during extraction and analysis with MOBILedit Forensic PRO.
- Both authorization token access and username and password access are supported. An authorization token is a file saved on a computer or mobile device. It recognizes a device and account to allow a user to log in to a service without having to enter a username and password every time.
- Manual access by entering a user name and password.
- Immediate and concurrent downloads that enable an investigator to work effectively while extracting the maximum amount of data in the shortest time possible. Time is critical because a user can wipe all data, a token could expire, or a password could be changed.
- Professional reports and exports in the following formats: pdf, html, xml, ufdr, and Excel.
- Full file structure download.



MOBILedit Cloud Forensic

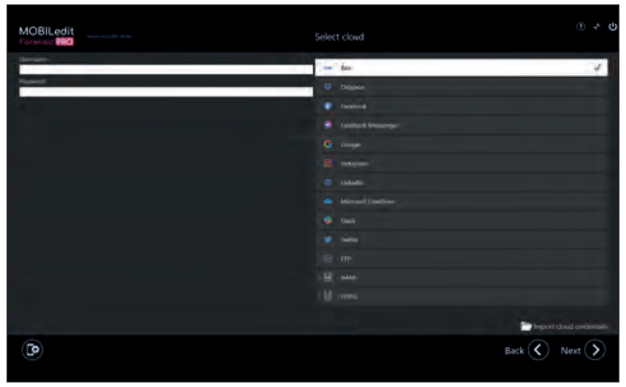
Select a cloud or data and press Next

CONNECTED CLOUDS AND IMPORTED DATA:

Box Cloud - Acquiring data

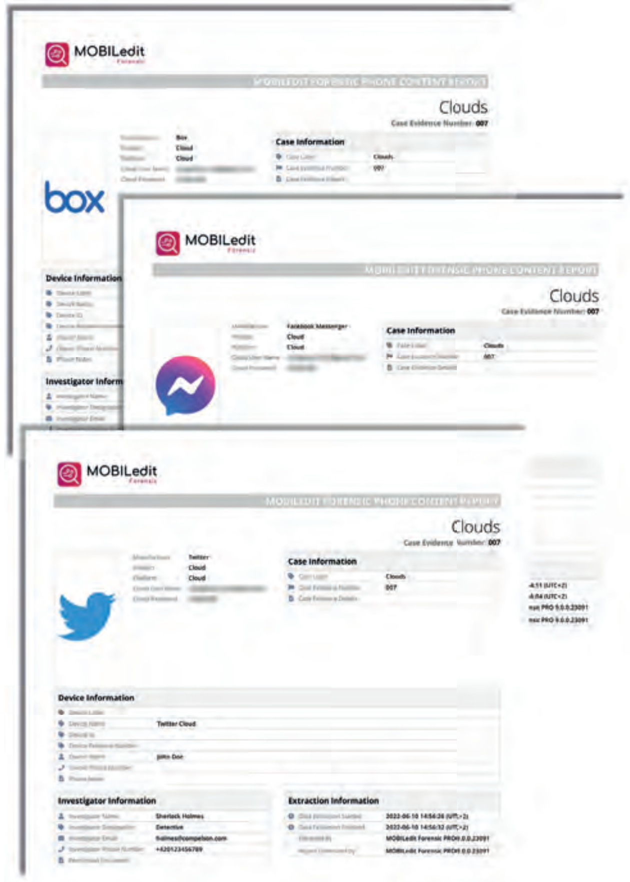
Facebook Messenger Cloud - Acquiring data

Twitter Cloud



SUPPORTED SERVICES

- Box
- Dropbox
- Google Drive
- Microsoft OneDrive
- FTP
- Facebook
- Facebook Messenger
- Google Contacts, Calendar, Keep
- Instagram
- LinkedIn
- Slack
- Twitter
- Emails such as Gmail, Outlook, and many others through POP3, IMAP protocols
- and more



WHY CLOUDS?

- By 2025 it is estimated that half of the world's data will be in the cloud, accounting for 100 zettabytes. That's 100 billion terabytes of data. (Cybercrime Magazine - Page One For The Cybersecurity Industry)
- The average person is storing 500 GB of data in their personal cloud storage. Regarding text documents alone, the average person stores around 130 GB of these in the cloud, which equates to 10 million pieces of paper. Now imagine the possible amount of evidence hiding there. (pCloud - The Most Secure Cloud Storage)
- Facebook Messenger is one of the leading messaging platforms in the US, with more than 2 million monthly downloads. More than 20 billion messages are exchanged between businesses and users monthly on Facebook Messenger. (Home - Review42)

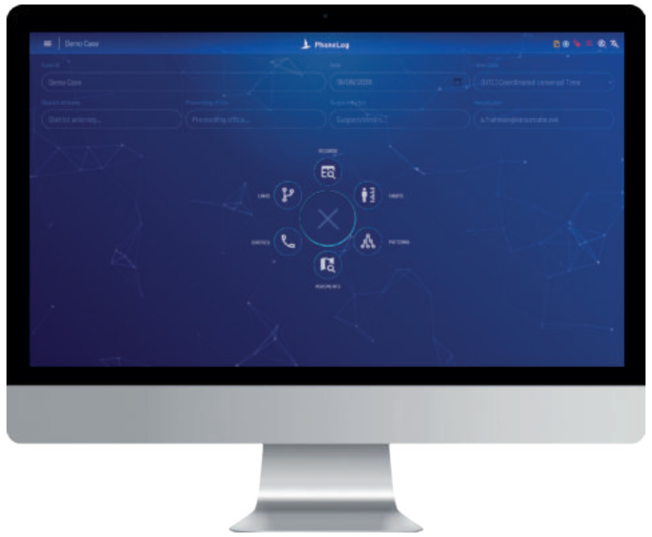
compelson

www.mobiledit.com
sales@compelson.com

PhoneLog

Multi Level Phone Records Analytics
Digital Evidence Correlation
3D mapping

Two Steps Ahead – One of a Kind Complete



PhoneLog is the software for the cross-analysis of digital evidence:

- All types of Call Detail Record research, statistics, and mapping
- Integrated Cell Sites Location data management
- Cell Site real signal coverage surveys and knowledge
- Third party mobile extractions, GPS tracks, wiretaps, and much more

Data Validation is key when using a variety of digital sources. **PhoneLog will unlock this potential.**

Visualize and examine multiple sources at the same time with a solid and logical method for the in-depth reconstruction of mobile digital alibis.

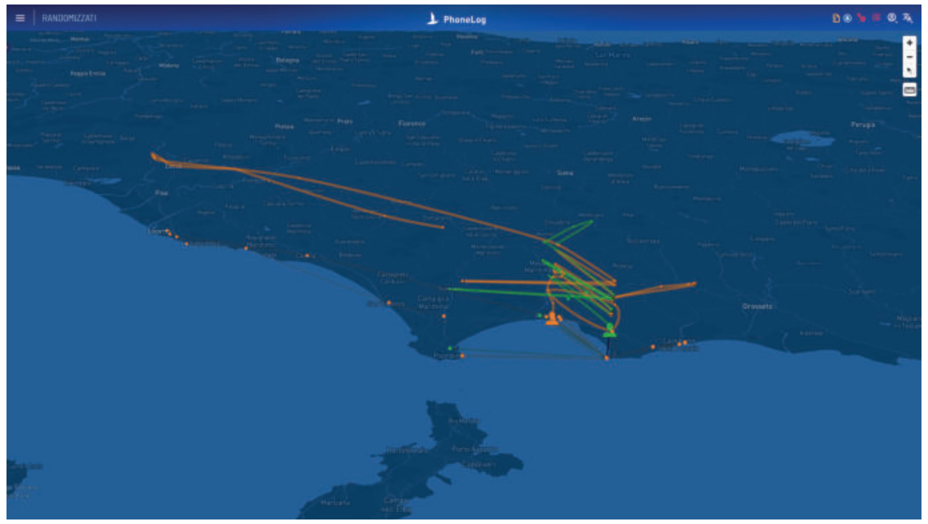
Place all your evidence on a state of the art 3D map and visualize events and user movements.

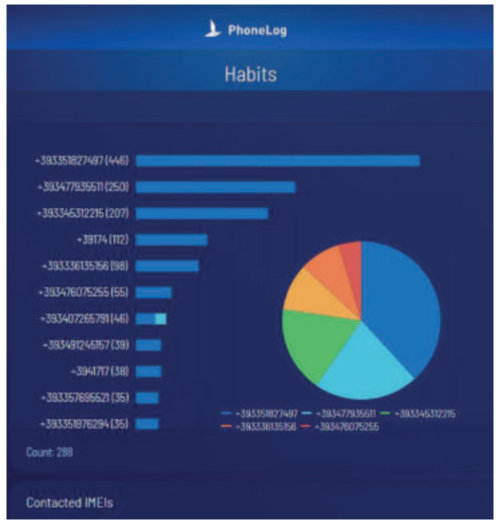
Maintain evidence integrity and protect it with a forensic hash code system based on international best practices.

PhoneLog is the answer

Discover how powerful functions will make your digital investigation soar:
it's extremely smart, fast, and easy to use.

SecurCube®





CDRs matched to other digital sources, to name a few:

- MSAB XRY, Cellebrite UFED, Oxygen Forensics, MOBILedit Compelson and other mobile extractions
- Cell Towers real coverage data collected with SecurCube BTS Tracker
- Wiretaps, GPS logs, CCTV camera feeds

Integrate all this and more to PhoneLog

Choose PhoneLog and you have:

- Artificial Intelligence to quickly import any CDR format
- Two software configurations for your needs: client server browser environment or desktop interface
- Statistical data mining: habits, heatmaps, connections, and movements - no data limits
- Video animations of your results on complete 3D maps
- Easy to understand diagrams and custom courtroom presentations

SecurCube Cell Service: the easy to click global cell site data management search engine.

All the info You need on every cell tower for every carrier.

- Installation details
- Change of location or ID realignments
- Theoretical cell signal coverage
- Cell site real coverage collected with SecurCube BTS Tracker

NO CONFUSION NO MISTAKES

TRUST OUR YEARS OF EXPERIENCE IN STUDYING CELL NETWORKS WORLDWIDE

SecurCube® is a world leader in phone records (CDR) and cell site (BTS) real coverage in the field of digital forensics.

Daily cooperation with law enforcement, prosecuters, and judges providing software and hardware, consulting, analysis and training.

We develop the tools and also work alongside digital experts and know, first hand, how to conduct professional cases with success.

Our software has been created to answer real everyday digital investigations.

Cutting-edge forensic systems in line with international best practices and our experience.

CONTACT US FOR A FREE WEBINAR AND PRESENTATION OF OUR FORENSIC SOLUTIONS.

✉ **info@securcube.net** 🌐 **www.securcube.net** ☎ **+39 345 574 4134**

SecurCube®

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Mobile Forensic Bundle

The complete mobile forensic kit in a single pack. Perform physical, logical and over-the-air acquisition of smartphones, tablets and wearable devices, break mobile backup passwords and decrypt encrypted backups, view and analyze information stored in mobile devices and cloud services.

TOOLS FOR MOBILE FORENSICS

Comprehensive Mobile Forensic Solution

The Elcomsoft Mobile Forensic Bundle includes the most essential tools for fast, safe and forensically sound acquisition, decryption and analysis of evidence from a wide range of mobile platforms and cloud services.

Forensic analysis of Apple devices

The newest jailbreak-free low-level access to data offers direct, safe and forensically sound extraction for Apple devices running all versions of iOS from iOS 11 through iOS 13. The new agent-based acquisition provides full file system extraction and keychain decryption without a jailbreak and literally no footprint. The complete forensic acquisition using jailbreak is also available.

Obtain iCloud backups, download photos and synced data, access iCloud passwords

Try the most comprehensive iCloud data acquisition on the market enabling forensic access to evidence stored in the cloud with and without the Apple ID password. Access cloud backups, call logs, messages, passwords (iCloud Keychain), contacts, iCloud Photo Library, iCloud files, Apple Health and Screen time, geolocation data and a lot more.

Break passwords to iOS system backups

Brute-force passwords protecting encrypted iOS backups with a high-end tool. GPU acceleration using AMD or NVIDIA boards helps achieve unprecedented performance, while access to users' stored passwords enables targeted attacks with custom dictionaries.

GPU acceleration: patented technology significantly reduces password recovery time

The company's patented GPU acceleration applied to breaking passwords protecting iOS backups is unmatched by competition. ElcomSoft pioneered asynchronous GPU acceleration, enabling simultaneous use of multiple video cards by different makes, models and architectures (AMD and NVIDIA) in a single PC for faster and more cost-effective attacks.

Dictionary attack

Using the prepared dictionaries based on leaked password databases or wordlists with highly customizable mutations targeting the human factor and common password patterns. The tool supports a variety of mutations, trying hundreds of variants for each dictionary word to ensure the best possible chance to recover the password.

Full over-the-air acquisition of Google Accounts

Google collects massive amounts of information from registered customers. The Mobile bundle includes the powerful and lightweight forensic tool to extract information from the many available sources, parse and assemble the data to present information in human-readable form. Extract and analyze user's detailed location history, search queries, Chrome passwords and browsing history, Gmail messages, contacts, photos, and a lot more.

Support for popular instant messengers: WhatsApp, Skype, Signal etc.

Extract, decrypt and view WhatsApp, Skype, Signal and Telegram communication histories, attachments and contact lists from a wide range of devices or cloud services. The downloading of the conversation histories, when available, only takes minutes!

Fast download, search and analysis

With Elcomsoft mobile forensic tools investigators can save time by reviewing essential bits of information in just a few moments. By quick downloading selective information, instant filtering and quick search functionality examiners obtain essential information in a matter of minutes.

Reporting and Exporting

A wide range of HTML reports are available. HTML reports can be easily printed or viewed in any Web browser. In addition, data can be exported into an Excel-compatible XLSX file for further processing and analysis.

More informaton at www.elcomsoft.com/emfb.html

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

YOUR BENEFITS

All in one

A single purchase delivers all ElcomSoft products in their respective top-of-the-line editions that allow recovering passwords and decrypting encrypted data.

Industry-certified technologies

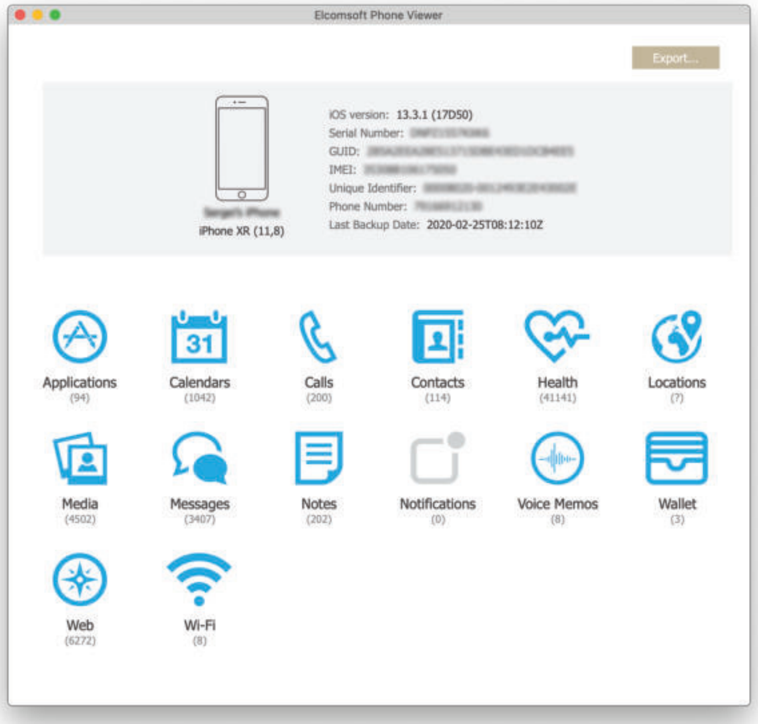
Elcomsoft is Microsoft Silver Certified Partner, Intel Software Partner and member of NVIDIA CUDA/GPU Computing Registered Developer Program.

Research and development

The password recovery suite features the latest and most advanced cryptanalysis algorithms developed by ElcomSoft research department. We continue to deliver cutting-edge technologies in password recovery and data decryption.

Patented technologie

ElcomSoft pioneered many software innovations that have made it easier to access protected data. The GPU acceleration, which is patented (U.S. Pat. No. 7,787,629 and 7,929,707) and unique to ElcomSoft products, making password recovery up to 250 times faster compared to traditional methods, is just one of the innovations.



Elcomsoft Phone Viewer

Export...

[redacted]
iPhone XR (11,8)

iOS version: 13.3.1 (17D50)
Serial Number: [redacted]
GUID: [redacted]
IMEI: [redacted]
Unique Identifier: [redacted]
Phone Number: [redacted]
Last Backup Date: 2020-02-25T08:12:10Z

Education and consulting

We offer comprehensive three-to-five-day courses offering hands-on experience in unlocking and extracting evidence from mobile devices, accessing password-protected and encrypted computer data.

More informaton at www.elcomsoft.com/emfb.html

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

www.elcomsoft.com
blog.elcomsoft.com
sales@elcomsoft.com

CYACOMB FORENSICS

www.cyacomb.com

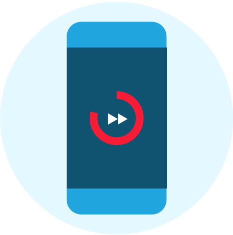
Digital triage for mobile devices

Vital evolution of our game-changing rapid triage tools in a world where 95% of people access the internet through their mobile phones

BOOK 21 DAY TRIAL

BOOK DEMO

Mobile Device Triage, available as a feature of Cyacomb Examiner Plus, scans Android and iOS mobile devices for known illegal content in a matter of seconds.



Conducting rapid Mobile Device Triage using Contraband Scan, known illegal content will be found on suspect devices up to 100 times faster than traditional file hash technology. With our simple-to-use interface, traffic light results that can be reviewed on the screen, your time to first evidence while on-scene can be reduced from hours to minutes.

With Mobile Device Triage feature in Cyacomb Examiner Plus, you will get:

- ✓ Contraband Filter scan for mobile devices, which has already helped our users catch offenders
- ✓ iOS and Android Contraband Filter scans
- ✓ Up to 100x faster scans
- ✓ The same super simple-to-use, intuitive user interface
- ✓ Simultaneous Contraband Filter scans on multiple devices (mobile devices and hard drives)
- ✓ Accurate results in seconds to support your decision to seize
- ✓ Previews and report creation, with optional evidential thumbnails

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT OUR SALES TEAM
EMEA/APAC +44 131 608 0195 | US +1 202 660 1869 | sales@cyacomb.com

CYACOMB FORENSICS

www.cyacomb.com

Cyacomb Contraband Scan is also available on DATAPILOT 10 devices.

BOOK DEMO

Purpose built handheld computers that are rugged and portable, the combined tools help law enforcement officers to make informed decisions on scene.

Conducting rapid Mobile Device Triage using Contraband Scan, known illegal content will be found on suspect devices up to 100 times faster than traditional file hash technology.

With our simple-to-use interface, traffic light results that can be reviewed on the screen, your time to first evidence while on-scene can be reduced from hours to minutes.

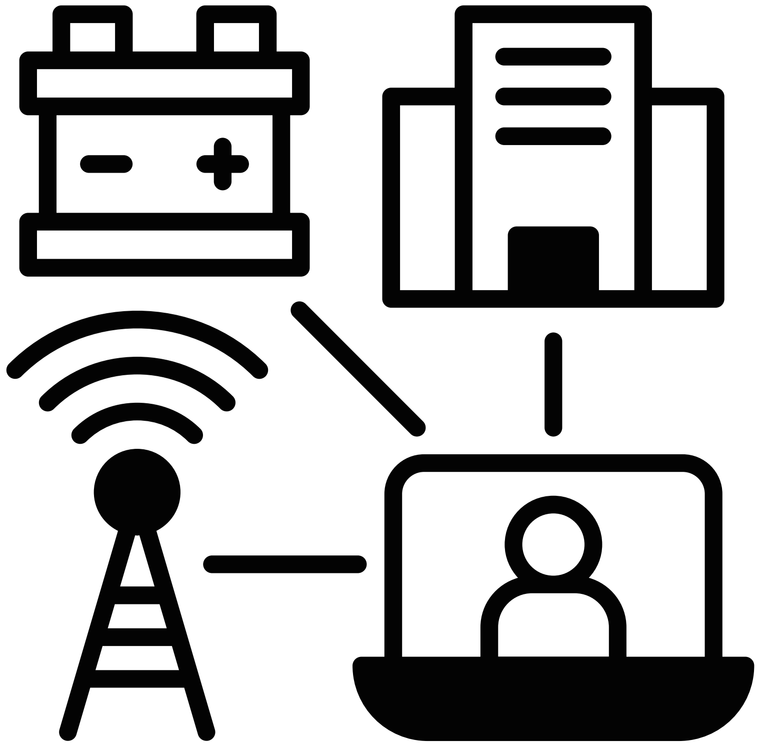
1. Arrive on scene
2. Scan devices
3. Fast results

Additional benefits of DATAPILOT DP10:

- ✓ Data slice capability, enabling collection of contacts, calls, messages, images, files and app data
- ✓ Mirror evidence directly from the target device in real time
- ✓ Create evidence with built-in cameras
- ✓ Powers target devices
- ✓ Optical character recognition search
- ✓ Search and reporting features
- ✓ Works on IOS and Android devices

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT OUR SALES TEAM
EMEA/APAC +44 131 608 0195 | US +1 202 660 1869 | sales@cyacomb.com

IoT Forensic Solution



Smartwatch Forensics

Get the extra evidence from the most popular wearable devices

Smartwatches are the world's most popular wearable devices with unquestionable importance when it comes to forensic examinations. The personal data found in smartwatches can lead investigators in the right direction, especially when the phone is nowhere to be found. MOBILedit Forensic can extract heartbeat details, which gives the investigator an intimate look into the life of the user. This data can reveal moments of excitement, stress, and even time of death. For a successful investigation, examining smartwatches is not only an option but a necessity for every digital forensic professional.

Why smartwatch forensics?

Smartwatch forensic analysis can bring critical data beyond what is available from phone forensic investigations.

1 **RICH SOURCE OF PERSONAL DATA**
Smartwatches collect a broad range of highly personal information, such as heart rate, body temperature, blood oxygen levels, health statistics, location history, and messages. This makes them a valuable resource for understanding an individual's detailed activities or behavior patterns.

2 **LOCATION TRACKING**
Smartwatches often feature GPS capabilities, making them key in tracing movements, which is essential in cases of kidnappings or when verifying alibis. It is also common for individuals to leave their phones at home and use smartwatches as the only device during sports activities.

3 **SMARTWATCHES AS THE SOLE SOURCE OF EVIDENCE**
When a phone is missing or damaged, smartwatches may serve as the sole source of digital evidence, offering unique insights that cannot be obtained from other devices.

4 **SYNCHRONIZATION GAPS PROVIDE ADDITIONAL DATA**
Gaps in the synchronization of data between a phone and a smartwatch can reveal critical evidence. For instance, photos long deleted from an iPhone may still be present on an Apple Watch.

5 **COMMUNICATION AND SOCIAL MEDIA ACTIVITY**
Users can access a wide array of apps on their smartwatches, generating valuable data. Linked to social and communication apps, smartwatches offer insights into texts, emails, and social media notifications that are relevant to investigations.

ALL MAJOR BRANDS SUPPORTED

As smartwatches gain popularity, the market's expansion to hundreds of brands makes forensic analysis challenging. The MOBILedit team, leading in smartwatch forensics since 2019, is focusing not only on all major brands including Apple, Samsung, Garmin, Huawei, Alcatel, TCL, Amazfit, Huami, Suunto, but also on many local brands of smartwatches.

MOBILedit Smartwatch Kit

Essential hardware for smartwatch forensic analysis

What's in the Kit?

This kit focuses on Apple Watch, Samsung, and Garmin smartwatches, while many other brands can be connected using the manufacturer's cables or Bluetooth. To perform smartwatch forensic analysis, the MOBILedit Forensic software is required alongside this kit.

SAMSUNG GALAXY WATCH READERS

The unique Samsung Galaxy Watch readers are designed and engineered by the MOBILedit team. With these two readers, data such as messages, geolocations, health data, heartbeats, and more can be obtained from the Samsung Galaxy Watch 2 up to the latest versions. Under certain conditions, it is possible to gain root access and extract the full, unencrypted file system. This means all the data stored on the smartwatch, and potentially more evidence for your investigation, can be accessed.

ALL-IN-ONE READER FOR APPLE WATCHES

This device can read data through a special diagnostic connector from Apple Watch Series 0 to Series 6.

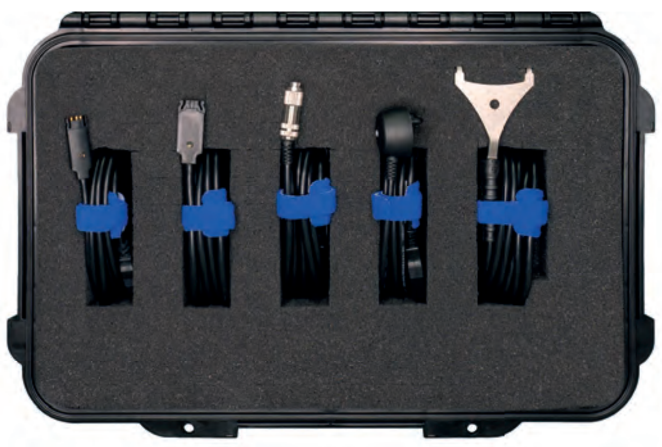
GARMIN WATCH CABLES

Covering most models, these cables connect to Garmin watches through standardized connectors, providing access to a wide range of data.

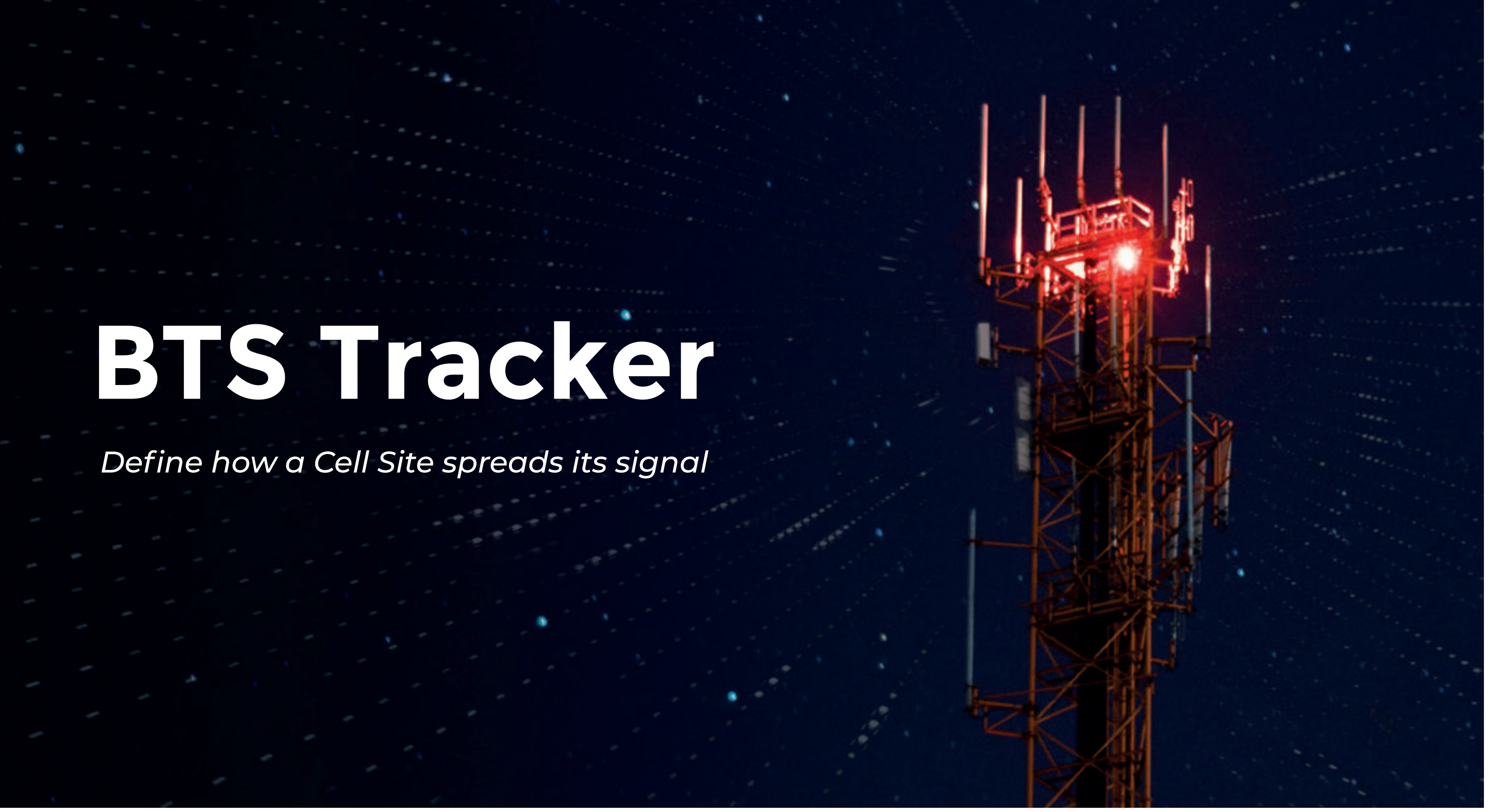
The kit also includes several adapters for various Samsung Galaxy Watch models, tools for smartwatch handling, accessories for smartwatch connection, and both USB-C and Lightning cables.

MOBILedit Dive Kit

Dive computers are akin to smartwatches for divers, crucial when lives depend on them. In the event of an accident, dive computers retain comprehensive details about the dive, tracking adherence to safe diving protocols by the second. The MOBILedit Dive Kit is an essential hardware not just for coastal countries but also for those with lakes and deep waters, essentially covering almost all nations worldwide. To utilize this hardware, MOBILedit Forensic software is required. MOBILedit Forensic is capable of providing a complete and detailed dive log from over 200 models across all major manufacturers such as Suunto, Oceanic, Mares, Aqualung and others.

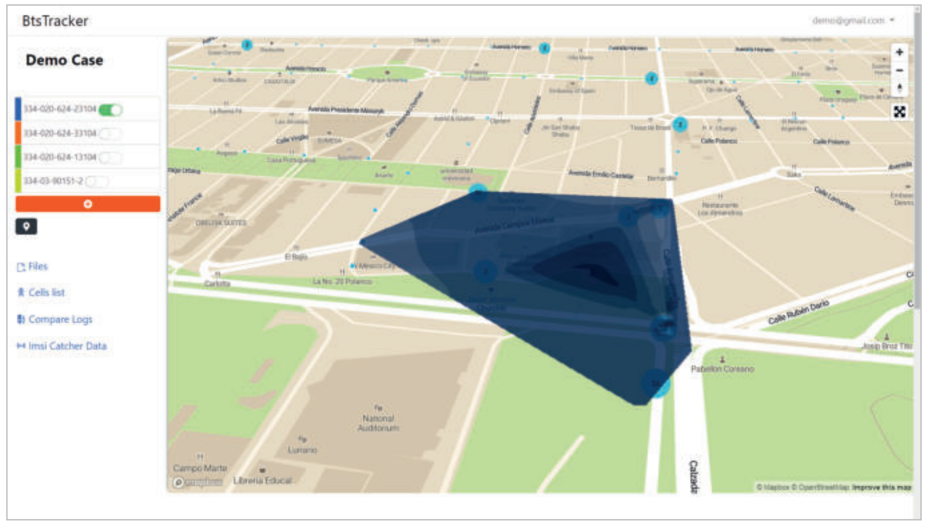


www.mobiledit.com
sales@compelson.com



BTS Tracker

Define how a Cell Site spreads its signal



Cell Site Signal Examination And Mapping

Base Transceiver Stations Coverage

Cell signals surround us, but the digital environment they create is always subject to change.

A cell tower signal set to one direction is often warped, reflected, reversed.

This is a risk when tracing a suspect's alibi. A solid court case needs hard facts and certainty.

SecurCube BTS Tracker Technology

It surveys, absorbs, and charts where and how every cell tower connects to a smartphone.

The software organizes and maps your cell site survey and investigation. It also checks daily signal changes and creates a statistical analysis of the real coverage scenario.

Ranges, power, and location. The reality of BTS networks. Bring your evidence to light.

Complete digital investigations

Correlate real BTS cell site coverage analysis with your CDR phone record analytics.

Locate a mobile device with more accuracy where the signal is really being spread making your case map real.

From a realistic outlook – **not a theoretical one** – locate digital evidence and validate your criminal case.

Save the historical data of these scans and make them all available to your team using SecurCube Cell Service.

SecurCube®

Smartphones and Cell Towers - They go hand in hand

- Phone records investigation requires the knowledge of both: a deep understanding of this dual environment
- Knowing where a cell signal covers an area may be the key between a successful case or a lost opportunity
- Only using phone records data is not enough. You need to go there and capture reality
- No more untruthful assumptions. Analyze what the signal coverage really is

Complete Your knowledge on multiple interconnected levels:

- Extract cell towers of interest from the events in the CDR phone records with PhoneLog
- Define all historical location, coverage and accessory information with Cell Service
- Survey and understand the cell towers real signal coverage with SecurCube BTS Tracker

TRACE YOUR EVIDENCE AND DIGITAL MOVEMENTS ON AN ANIMATED 3D MAP

YOUR 360° STRONG HOLD ON DIGITAL INVESTIGATIONS

SecurCube® knows mobile communication: generate strong, validated, and complete digital forensics investigations.

Call Detail Records evidence is enhanced by a deep understanding of how BTS cell networks work.
They are one and the same. With SecurCube you can maximize both.

For over a decade our team has created the tools. Learn how we can work for you. Our research, development and technology is at the forefront in cell forensics that will make you discover more.

Complex mobile network data become valuable, clear and a source of evidence and stronger justice.

JOIN US! WE LOOK FORWARD TO SHARING OUR TECHNOLOGY WITH YOU.

✉ info@securcube.net   www.securcube.net   ☎ +39 345 574 4134

SecurCube®

RUSOLUT

VEHICLE DATA RECONSTRUCTOR (VDR)

The Vehicle Data Reconstructor (VDR) is developed to set a new standard in digital forensics for vehicles. Designed to surpass existing solutions, VDR ensures comprehensive, reliable, and efficient data acquisition of crucial digital evidences from vehicles, providing forensic experts with easy-to-use tool with extensive possibilities and advanced features.

COMPREHENSIVE DATA ACQUISITION

VEHICLE-RELATED DATA

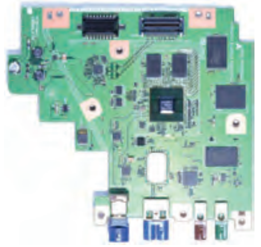
- ✓ **Vehicle System Data:** VIN, serial and part numbers, FW version, MAC/IP addresses, etc.
- ✓ **Events:** WIFI/Bluetooth/USB connections, vehicle power on/off, start/stop, reboots, door/light data, odometer, fuel consumption, system logs, etc.
- ✓ **GPS navigation data:** routes, tracklogs, POIs, trackpoints, destinations, GPS sync events, saved locations, etc.
- ✓ **Built-in applications:** Traffic, weather, radio, etc.

USER-RELATED DATA

- ✓ **Connected devices:** Smartphones, USB/SD cards, WIFI/Bluetooth logs, device list, timestamps, serial numbers, etc.
- ✓ **Smartphone synchronized data:** Device list, Calls, Phonebooks, SMS, Media, App data, etc.
- ✓ **Device identifiers:** Bluetooth/WIFI MAC addresses, phone names, WIFI access point info, installed apps.

HOW DOES IT WORK?

1 Data acquisition is performed either via chip-off or solderless adapter whether it's NAND or eMMC for all systems based on supported memory chips such as TSOP48, BGA63 (two sizes), BGA100, BGA153/169, BGA137, BGA107 and a universal adapter.



2 During physical image acquisition process the raw dump of the memory is extracted and converted into file system.

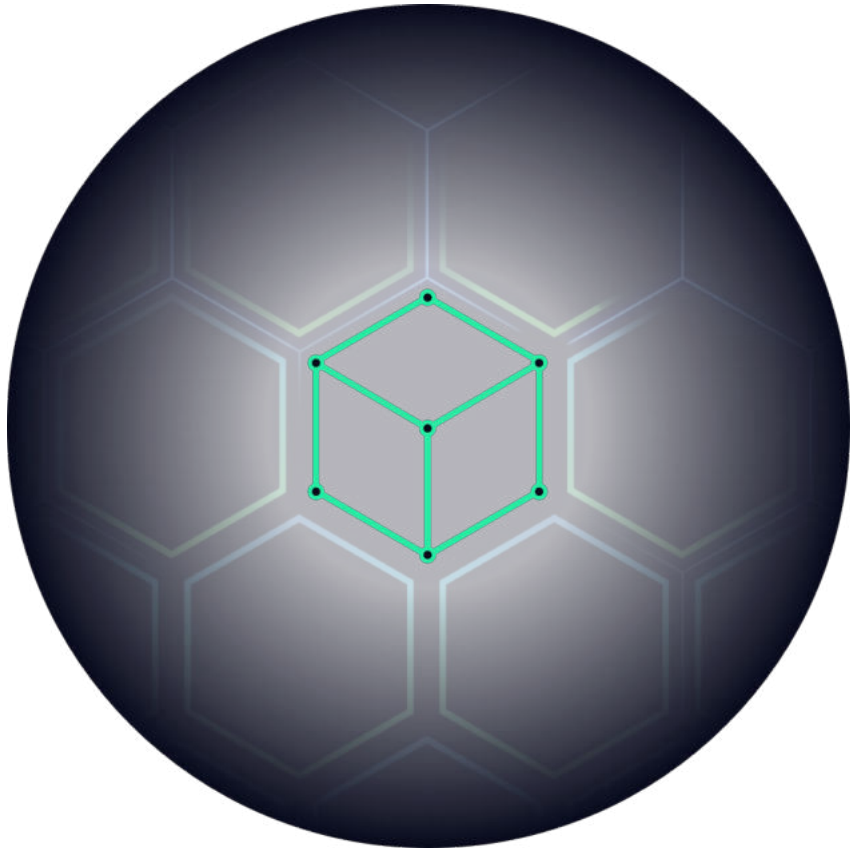
3 Files are analyzed and data is parsed according to the vehicle model and electronic unit. The case package is extracted for further analytics and report generation

4 A standalone data analytics and report generation software „VDR Report Manager" is used to process data case package and generate report.

WHAT'S INCLUDED

- ✓ Powerful software for physical dump acquisition and further vehicle data extraction, including parsers for File systems: QNX6, UBIFS, YAFFS2, FAT12,FAT16,FAT32,exFAT, Ext2, Ext3, Ext4, NTFS, HFSX, others embedded systems based on FTLs.Embedded FTLs
- ✓ VNR software
- ✓ Set of chip-off adapters for NAND Flash and eMMC memory chips:
  TSOP48 NAND, BGA63 11x9 NAND, BGA63 13x8.5 NAND, BGA100 NAND, BGA107 NAND, BGA137 NAND, BGA162 NAND, BGA100 14x18 eMMC, BGA153/169 11.5x13 eMMC, BGA153/169 12x16 eMMC, BGA153/169 14x18 eMMC, Soldering adapter
- ✓ VNR adapters: TSOP48 ZIF, LGA52 ZIF, BGA100, BGA152, Monolith
- ✓ 1 year of Support Subscription
- ✓ Vehicle Data Reconstructor Report Manager - Forensic managing and report generating tool
- ✓ Rusolut Reader for reading NAND chips and adapters control
- ✓ Non-invasive ISP NAND and eMMC adapters enabling direct data extraction from memory chips similar to the chip-off method but without the need to unsolder the chips, thus preserving the integrity of the system without any destroys*
- ✓ Widest database of solutions for vehicle electronic modules

* The number of adapters is updated at the time of purchase



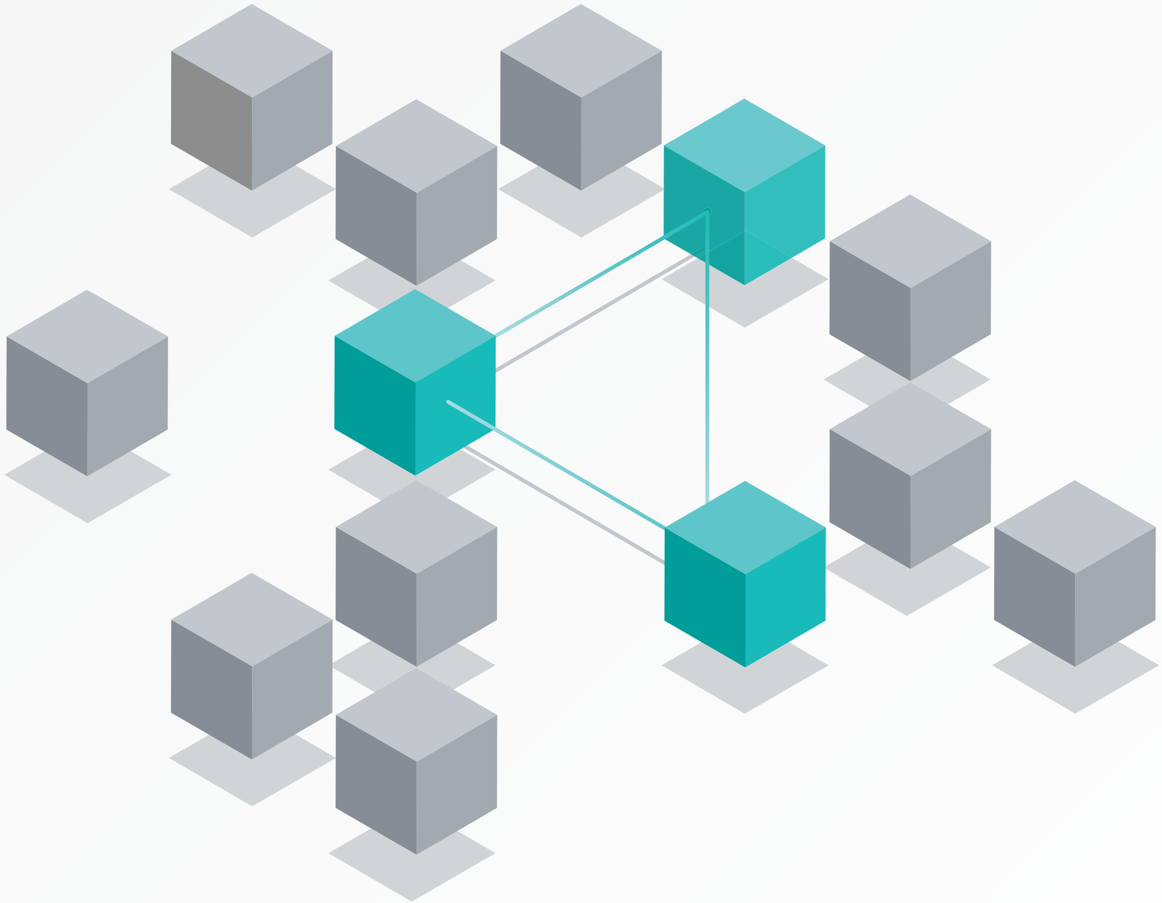
Cyber Security

REAQTA
an IBM Company

IBM

IBM Security ReaQta

AI-powered, automated endpoint security



IBM Security ReaQta offers a unique, forward-thinking approach to endpoint security.

The solution uses exceptional levels of intelligent automation, taking advantage of AI and machine learning, to help detect and remediate sophisticated known and unknown threats in near real-time. With deep visibility across endpoints, the solution combines expected features, such as MITRE ATT&CK mapping and attack visualizations, with dual-engine AI and automation to propel endpoint security into a zero trust world.

Why ReaQta?

1

Continuously learns as AI detects and responds autonomously in near real-time to new and unknown threats

2

Helps secure isolated, air-gapped infrastructures, as well as on-premises and cloud environments

3

Maps threats against the MITRE ATT&CK framework and uses a behavioral tree for easy analysis and visualizations

4

Offers a bidirectional API that integrates with many popular security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools

5

Provides heuristic, signature and behavioral techniques in its multilayered defense

6

Allows users to build custom detection strategies to address compliance or company-specific requirements without the need to reboot the endpoint

7

Simplifies and speeds response through guided or autonomous remediation

8

Offers automated, AI-powered threat detection and threat hunting including telemetry from indicators that can be customized for proprietary detection and granular search

9

Makes remediation available with automated or single-click remote kill

10

Provides deep visibility with NanoOS, a unique hypervisor-based approach that works outside the operating system and is designed to be invisible to attackers and malware

IT ASSET DISPOSITION

Degausser

POWER
ERROR
Digital Media MagWiper
***** Mag Wiper ****
Door Open
Erase Count 0
Total Erasures 24
ADVANCED DESIGN CORP.
CHARGING
ERASE/READY
MagWiper

ADC MagWiper MW-15X Degausser

The world's first 10,000+ Oe high-power degausser with a quick 17-second charge.

Model: DEA-MW15000X

Simultaneous Erasing Capacity

HDD 3.5"HDD: 1 unit | 2.5"HDD: 6 units

Charging time

17 seconds

Magnetic Field Generated

800 kA/m (Approx. 10,000 Oe)

Features

17-second quick charge, the fastest in the industry

The first 10,000+ Oe high-power degausser with a quick 17-second charge which means can erase data with higher efficiency.

World's first degausser using a diagonal magnetization system

The most effective for erasing data from perpendicular magnetic-recording HDDs, improving erasing efficiency by roughly 50% over conventional methods. (Erasing capacity equivalent to 1200 KA/m.)

Magnetic force checking function

The monitor displays the strength of the magnetic field after it is generated. The ability to check the strength of the magnetic field each time improves the reliability of the erasing operation.

Can also use to erase magnetic data stored on tape

Erases cartridge tapes, including open reel, LTO/DAT/DLT/CMT/9940/3592/VHS, as well as floppy disks and other magnetic-recording media in one speedy operation.

ADC MagWiper MW-25X Degausser

Erase 100units of 3.5-inch HDDs about 17 minutes without remove the mounting brackets.

Model: DEA-MW25000X

Simultaneous Erasing Capacity

HDD 3.5"HDD: 2 units | 2.5"HDD: 10 units

Charging time

20 seconds

Magnetic Field Generated

800 kA/m (Approx. 10,000 Oe)

Features

Can Erase data without removing the mounting brackets

Erases magnetic data from two HDDs simultaneously no need to remove the mounting brackets.

World's first degausser using a diagonal magnetization system

The most effective for erasing data from perpendicular magnetic-recording HDDs, improving erasing efficiency by roughly 50% over conventional methods. (Erasing capacity equivalent to 1200 KA/m.)

Magnetic force checking function

The monitor displays the strength of the magnetic field after it is generated. The ability to check the strength of the magnetic field each time improves the reliability of the erasing operation.

Can also use to erase magnetic data stored on tape

Erases cartridge tapes, including open reel, LTO/DAT/DLT/CMT/9940/3592/VHS, as well as floppy disks and other magnetic-recording media in one speedy operation.

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

MagWiper MW-30X Degausser

Large model can simultaneiusly erase up to 51 units of 2.5” HDDs and B4 notebooks without dismantling.

Model: DEA-MW30000X

Simultaneous Erasing Capacity

3.5”HDD: 14 units | 2.5”HDD: 51 units

Charging time

25 seconds

Magnetic Field Generated

800 kA/m (Approx. 10,000 Oe)

Features

Can erase data from a B4-size laptop intact (100% degaussing)
The large chamber enables erasure of this large number of media simultaneously. You can even erase the data from a B4-size or A4-size notebook PC without removing the HDD.

World's first degausser using a diagonal magnetization system
The most effective for erasing data from perpendicular magnetic-recording HDDs, improving erasing efficiency by roughly 50% over conventional methods. (Erasing capacity equivalent to 1200 KA/m.)

Magnetic force checking function
The monitor displays the strength of the magnetic field after it is generated. The ability to check the strength of the magnetic field each time improves the reliability of the erasing operation.

Can also use to erase magnetic data stored on tape
Erases cartridge tapes, including open reel, LTO/DAT/DLT/CMT/9940/3592/VHS, as well as floppy disks and other magnetic-recording media in one speedy operation.

Facilitates centralized management and control (key entry system)
To enhance safety, this model will not function without insertion of a power key in the front panel. The power key remains in the care of a manager to prevent illicit erasure of data and accidents.

Comes with a special mobile lifter
The special lifter improves operational efficiency by enabling you to move the unit safely from one site to another without the need to load and unload it on a mover each time.

MagWiper NSA Degausser

NSA EPL listed compact, lightweight and efficient instant degausser.

Model: DEA-MW1B

✓ NSA EPL Listed

Simultaneous Erasing Capacity

3.5”HDD: 1 unit | 2.5”HDD: 8 units

Charging time

15 seconds

Magnetic Field Generated

1,592 KA/m (Approx.20,000 Oe)

Features

Safety
The MagWipers have been tested to validate safe operation with low-level field leakage.

Erase Simple Operation
Only need to insert the target in the chamber, push the “Erase” button, and remove the target.

Malfunction Alarm
If the magnetic flux density drops below a specified value, an alarm LED lights.

Cooling Function
A cooling fan operates as required during the operation.

Door Lock
The chamber door locks on closure to prevent operator hand insertion, or target ejection.

APPROVED Government Standards
Meets PCI DSS, Data Security Standard, NIST Guidelines, NIST SP 800-36, NIST SP 800-88,

Portable
Relatively small and light. Easily transported to various locations for on-site media erasure.

Flux Density Display
A front-panel LCD displays the magnetic flux density used for the data erasure.

Operating Indicator
A flashing light at the chamber door edge visually confirms that a magnetic field is generated.

LCD Display
The LCD shows total number of erasures and magnetic field intensity used for the last erasure.

Use of Trays
Permits preparation of next load during recharge.

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

MagWiper Series

Standard
DEA-MW15000X

Hybrid
DEA-MW25000X

All In One
DEA-MW30000X

NSA EPL Listed
DEA-MW1B

Specification

Model No.	DEA-MW15000X	DEA-MW25000X	DEA-MW30000X	DEA-MW1B
NSA EPL Listing	✗	✗	✗	✓
Erasable media	Hard disks, LTO, DDS/DAT, DLT, CMT, 9940, 3592, AIT, FD etc	Hard disks (including thick hard disks), LTO, DDS/DAT, DLT, CMT, 9940, 3592, AIT, FD, VHS etc	B4 notebook PCs (sizes up to B4), hard disks (including thick hard disks), open reel, LTO, DDS/DAT, DLT, CMT, 9940, 3592, AIT, VHS, FD etc	3.5" and 2.5" HDD, LTO, DDS/DAT, AIT, FD, etc.
Hard disk recording formats supported	Perpendicular and In-plane (longitudinal)			
Charging time	17 seconds	20 seconds	25 seconds	15 seconds
Data erasing time	0.1 seconds			
Magnetic field generated	800 kA/m (Approx. 10,000 Oe)			1,592 KA/m (Approx.20,000 Oe)
Power Source	AC100 /115 /200 / 220 / 240V 50/60Hz			
Power consumption (maximum when charging)	100V/10A, 220V/3A	100V/13A, 220V/8A	100V/15A, 220V/8A	115V/14A
Power consumption (standby mode)	100V/0.05A, 220V/0.03A	100V/0.05A, 220V/0.03A	100V/0.07A, 220V/0.04A	115V/1A
External dimensions	264 (W) × 240 (H) × 454 (L) mm	333 (W) × 285 (H) × 625 (L) mm	550 (W) × 463 (H) × 670 (L) mm	333 (W)×285 (H)×630 (D) mm
Erasable area	115 (W) × 70 (H) × 145 (L) mm	131 (W) × 119 (H) × 263 (L) mm	315 (W) × 90 (H) × 364 (L) mm	106 (W)×43 (H)×162 (D) mm
Weight	22.9kg	37.5kg	123kg	46kg
Operating environment	5°–35°C (41°–95°F), humidity 20–80% (condensation-free environment)			
Accessories	HDD rack, AC power cable, usage instructions, warranty	HDD rack, bar to hold HDDs in place AC power cable, usage instructions, warranty	HDD tray, all-purpose tray AC power cable, usage instructions, warranty	Media Rack, Instruction manual, One-year limited warranty

Duplicator & Wiper

CLONIX

DiskClon DC6000 Series

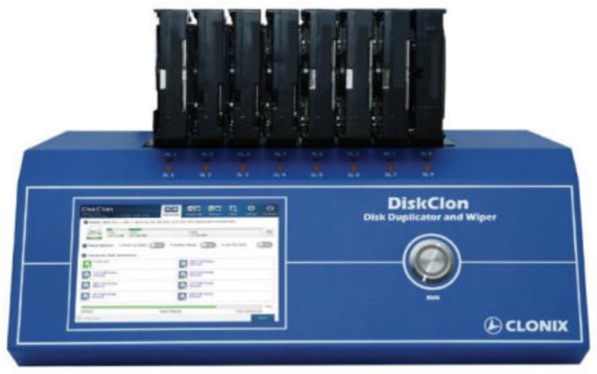
Disk Duplicator & Wiper

DiskClon is the product to duplicate and wipe various media (HDD, SSD, CF, SD, mSATA, NGFF) at fast and stable speed of 7GB/min on average, which enables to manage the original disk using the disk image file method and duplicate it optionally as the disk has a disk backup function.

This is the best solution for duplication and wipe that enables to maximize small quantity batch production, maintenance of various products, convenience of data wipe, and work efficiency as it is available to work on all ports individually when duplicating images or wiping data.

What is a duplicator with disk imaging method?

DiskClon can back up the contents of original hard disk in the device as disk image file for storage and management. It is available to duplicate the stored image disks without master hard disk.



- Easy to connect disk by jig
- Support interfaces such as IDE, SATA, SAS
- Manage and duplicate by disk image file
- Wipe disks completely and create a report

Main Feature

- Fast and stable duplication and deletion speed at average 7GB/m ~ max. 20GB/m
- Support Disk to Disk and Image to Disk
- Support Multi Image Copy
- Backup the manage the original disk image files from all ports
- Wipe by international standard method (DoD)
- Support hot swap (Wipe each port)
- Create wipe report
- Compare the original data and the duplicated data by sector unit and if an error is discovered during inspection, correct the error in real time.
- If the size of disk to duplicate is different, readjust the partition of the target disk automatically
- Record log file of used history

CLONIX

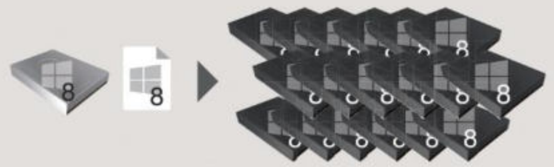
DiskClon DC6000 Series

Disk Duplicator & Wiper

Why DiskClon Needed?

❶ Mass media production & maintenance

Duplicate the contents of original media in the target disk in large quantities and and conduct the maintenance

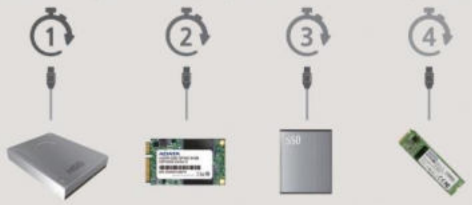


❷ Plug & Wipe

Reduce a great deal of time to delete using the function of deletion by port

❸ Small quantity batch production and various media management

Available for duplication of different media for each port, which enables to duplicate multiple products and different products



❹ Create a report for the result of deletion automatically after deleting

After deleting, create a report that records details such as PC, storage media, working time, working method etc.

Specification

Hardware Specification and Support Environment

Model name	DiskClon Portable	DiskClon DC6000-08IL	DiskClon DC6000-16HL
Port No.	4	8	16
Dimension	195mm x 140mm x 60mm	439mm x 268mm x 134mm	500mm x 268mm x 134mm
Weight	1.6kg	8.7kg	10.5kg
Power	60W/Full range (100-240)	550W/Full range (100-240)	700W/Full range (100-240)
Display	800 x 600 color LCD / touch screen	800 x 600 color LCD / touch screen	800 x 600 color LCD / touch screen
Internal storage	mSATA 120G	2.5" HDD 1TB	2.5" HDD 1TB
Ports	USB 2.0 x 2, USB 3.0 x 2	USB 2.0 x 5, USB 3.0 x 2, e-SATA x 1, HDMI x 1	USB 2.0 x 2, USB 3.0 x 4, e-SATA x 1, HDMI x 1
Network	2 x 1000 BASE-T	1 x 1000 BASE-T	2 x 1000 BASE-T
Duplication speed	7GB/m - 12GB/m		
Wipe speed	15GB/m - 20GB/m		
User interface	Window-based full GUI		
Support BUS type	IDE, SATA, SAS		
Support file system	Windows (NTFS, FAT16/32), Linux (Ext2/3/4, ReiserFS, XFS, btrfs)		
Support media	All media that support IDE, SATA, and SAS (HDD, SSD, CompactFlash, SecureDigital, mSATA, NGFF, etc.)		

*For the improvement of product quality, the specification of hardware is subject to change without prior notice.

CLONIX Co., Ltd.

Backup / Restore / Cloning Solution Provider
8F KyungDong Bldg. 4, SunaeRo 46 BeonGil BunDangGu, SeongNamSi GyeonGiDo, Korea
Tel. +82 70 7090 8280 Fax. +82 70 7016 2380 www.clonix.com

Recruitment of Partner Company & Dealers

Contact sales@clonix.com

CLONIX

NetClon NC1000 Series

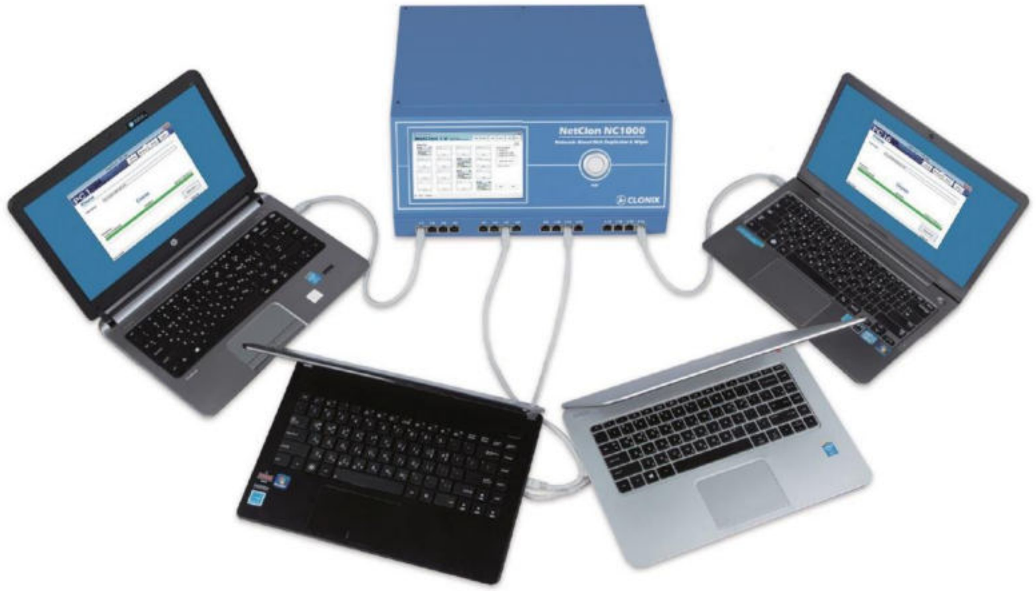
Network-based Disk Duplicator & Wiper

NetClon is network-based media duplicator and wiper that enables to duplicate, wipe and manage the original image through network interface without separation the storage from device in the world only.

This allows duplication and wipe regardless of types of embedded storage media as it controls the target system using a network booting technology. It is not necessary to purchase an additional device for each media type and this can reduce unnecessary work time.

What is a Network-based Disk Duplicator & Wiper?

NetClon can backup to internal storage from original disk by image and duplicate to target device by network connection. In addition, it is available to secure wipe without separation disk from device



Duplicate/wipe all type of storage media without separation from the device

Main Feature

- Network-based duplication and wipe (RJ-45 port)
- Duplicate, wipe and manage without separation disk from target device
- Duplicate and wipe regardless of disk type and interface of target device
- Support duplication that allows booting even if hardware of backup target device and duplication target device is not the same (support the duplication between different models)
- Manage by image file of backup
- Support simultaneous duplication function of the same image suitable for mass production and maintenance
- Support individual image duplication function by product suitable for small quantity batch production and maintenance
- Automatic duplication when connecting by image file registration and settings by model of duplication target device
- Support international DoD wipe method, which does not allow restoration
- After secure wipe, create a report for details of work automatically
- After secure wipe, proceed with automatic duplication and after completion, support the automatic closing

CLONIX

NetClon NC1000 Series

Network-based Disk Duplicator & Wiper

Why NetClon Needed?

❶ **An increasing number of storage media having various interfaces**

Available to work with various storage media such as HDD, SSD, mSATA, NGFF, eMMC, SD Card, Flash Memory, DOM, CF Memory, etc. as well as future storage media

❷ **Small quantity batch production and maintenance of various products**

Available for simultaneous duplication of different systems for each port, which enables to duplicate multiple product and different models at the same time

❸ **Duplication solution optimized for Cell production method**

Unification of duplication process regardless of media type and available to duplicate and inspect after production of finished products. Optimal for cell production method.

❹ **Reduction of product damage**

Reduce the product damage or risk of part loss due to frequent removal of storage media, as well as unnecessary work time

Specification

Hardware Specification and Support Environment

Model name	NetClon Portable	NetClon NC1000-08IL	NetClon NC1000-16HL
Port No.	5	8	16
Dimension	205mm x 140mm x 65mm	340mm x 365mm x 165mm	390mm x 365mm x 161mm
Weight	1.6kg	5kg	9.6kg
Power	60W/Full range (100-240)	120W/Full range (100-240)	700W/Full range (100-240)
Display	800 x 600 color LCD / touch screen	800 x 600 color LCD / touch screen	800 x 600 color LCD / touch screen
Internal storage	SSD 250G	SSD 500G	SSD 500G
Ports	USB 2.0 x 3, eSATA x 2	USB 2.0 x 1, USB 3.0 x 2, e-SATA x 1	USB 3.0 x 2, e-SATA x 1
Network			2 x 1000 BASE-T
Duplication / Wipe speed	7GB/m - 20GB/m		
User interface	Window-based full GUI		
Support BUS type	Gigabit Network		
Support file system	Windows (NTFS, FAT16/32), Linux (Ext2/3/4, ReiserFS, XFS, btrfs)		
Support media	All media (HDD, SSD, Compact Flash, SecureDigital, mSATA, NGFF, etc.)		

*For the improvement of product quality, the specification of hardware is subject to change without prior notice.

CLONIX Co., Ltd.

Backup / Restore / Cloning Solution Provider
8F KyungDong Bldg. 4, SunaeRo 46 BeonGil BunDangGu, SeongNamSi GyeonGiDo, Korea
Tel. +82 70 7090 8280 Fax. +82 70 7016 2380 www.clonix.com

Recruitment of Partner Company & Dealers

Contact sales@clonix.com

blancco

Blancco Drive Eraser for ITAD

Market-leading Data Sanitization for HDDs/ SSDs in PCs, Laptops, Chromebooks, and Servers

Why Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

View Our Certifications

Request Your Free Trial

Get Started Today

Blancco Drive Eraser is a robust data sanitization solution for PC, laptop, Chromebook, server and storage environments.

Organizations concerned with data security and compliance are feeling the pressure to build and maintain robust security policies, safeguard their sensitive data, and dispose of their assets responsibly.

With Blancco Drive Eraser, organizations can add an essential level of protection to endpoint security policies by permanently erasing sensitive data from HDDs and SSDs, including NVMes in desktop/laptop/Chromebook computers and servers.

Our secure overwriting process sanitizes data on a wide variety of storage devices, offering organizations the means for safe re-sale, re-purposing or disposal of data assets at end-of-life.

Key Benefits

- ✓ Guarantees your data has been erased from any drive, from HDDs to SSDs and NVMEs, including self-encrypting drives
- ✓ Receive a tamper-proof audit trail for all assets, with a digitally-signed Certificate of Erasure for each erasure instance
- ✓ Process loose drives and Chromebooks with ISO Image Installer, including a report viewer to track progress and specifically designed key diagnostics
- ✓ Increase efficiency and minimize manual processes with Intelligent Business Routing (IBR) workflows (including offline)
- ✓ Generate post-processing labels per asset with Blancco Label Printer
- ✓ Implement hardware tests to assist with diagnostics
- ✓ Full NIST compliance with support for NIST Purge and Clear, featuring full records of unsupported incidents for transparent auditing
- ✓ Support for internal drive erasure commands

blancco

Technical Specifications

ERASURE

- Locally or remotely controlled data erasure via the Blancco Management Console
- High-speed, simultaneous erasure of multiple drives, including the ability to customize drive batch sizes and drive speed thresholds
- RAID dismantling and direct access to the underlying physical drives
- SSD detection and secure erasure with Blancco´s patented SSD method
- Automated detection and unlocking of freeze locked drives
- Detection, notification and erasure of hidden areas (DCO, HPA) and remapped sectors
- Support for internal drive erasure commands, including cryptographic erasure and TCG feature set on self-encrypting drives
- Ability to reformat SATA and SAS drives after erasure

MINIMUM SYSTEM REQUIREMENTS

- 1 GB RAM memory in most cases (2 GB for PXE booting)
- Local erasure:
  - CD/DVD drive or USB port for booting the software
  - SVGA display and VESA compatible video card
  - USB port for saving reports
- Remote erasure (requires Blancco Management Console):
  - Ethernet NIC
  - DHCP Server running on local network for PXE booting, remote erasure and report collection

USABILITY

- Accelerated NIST Purge erasure
- Multi-tasking to allow the hardware diagnostics and updating the report during the erasure time
- Screensaver displaying the erasure progress to monitor the process remotely
- Resume an erasure that has been interrupted without consuming extra licenses
- Dedicated interface for loose drive erasure
- Support for LAN and WLAN networks, including 802.1x authentication

REPORTING

- Digitally-signed Certificate of Erasure
- Choose between asset level or drive-level reports
- Save reports locally or send them through the network to the Blancco Management Console
- Detailed reports enabled by enhanced hardware detection
- Extensive erasure information, including HDD details for seamless audit procedures
- User extendable report (with option to add "custom fields")

DEPLOYMENT

- Blancco Drive Eraser is platform independent
- Local control with HASP dongles, standalone images, or centralized control through the Blancco Management Console or Blancco Cloud
- Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)

HARDWARE DETECTION & DIAGNOSTICS

- 13+ hardware tests, including: RAM, CPU, Motherboard, Battery (current capacity & discharge), PC Speaker, Display, Pointing Devices, Keyboard, Optical Drive, Webcam, USB Ports, WiFi card, SMART Tests for drives, BIOS logo
- Hot swap capabilities
- Backwards compatibility with other Blancco products (BDECT, BMC, BUSBC)

CONFIGURABILITY & AUTOMATION

- Customize erasure software to fit specific needs
- Customize input fields in erasure reports
- 4 levels of process automation: workflow, manual, semi-automatic, automatic
- Ability to communicate back and forth with an Asset Management System or other external system (IBR workflows) on asset and drive level
- Fine-tune erasure process (speed/time limit, configurable conditions, etc.)
- Execute customized workflows defined on the Blancco Management Console or Blancco Cloud, locally or remotely; automate the processing across all company assets

HARDWARE SUPPORT

- Erase data securely from PCs, laptops, servers and storage environments based in x86 and x86-64 architectures
- BIOS & UEFI machines including Intel-based Macs, Apple T2 and Secure Boot
- IDE/ATA, SATA, SCSI, SAS, USB, Fibre Channel, FireWire hard disk drives of any size/blocksize
- SATA and SAS solid state drives of any size/blocksize
- eMMC drives of any size/blocksize
- NVMe drives of any size/blocksize
- SAS, SCSI, ATA and NVMe self-encrypting drives

AUDITING

- Verification algorithms to automatically check the overwritten patterns
- Hexviewer provides fast visual verification of the erasure for compliance
- Reports offer tamper-proof reporting and can include a customized digital signature
- Embed reports in the drives for a fast erasure audit
- Search and export reports via APIs

LANGUAGE SUPPORT

- English, German, Japanese, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian
- Up to 20 different keyboard layouts supported

Demi PG520

Super Handy SATA Duplicator

2.5" and 3.5" HDD & SSD support

Super light 1.4 lbs (650g)

Duplicate
Erase
Resize
Diagnosis
Drive Information

SATA
IDE*
mSATA*

* Options

Control Buttons & LCD Screen

Stand-alone Operations

Backed by 34 years of expertise and engineering in digital storage technology, built for IT professionals in need of compact duplicator to carry around anywhere, Demi PG520 is a must-have.

Super Compact Platform
The footprint is almost the size of two 3.5" HDD with user-friendly operation control buttons and LCD display. Only 6.9 x 6.7 x 1.2" in handy size, weighing 1.4 lbs.

Multi-Interface Support
It is a great advantage of Demi PG520 supporting SATA II 300MB/s speed in addition to mSATA* and IDE*. High speed copy of 8 seconds/GB (tested).

Cross-Interface Copy
It accommodates migrating old, phasing-out interface drive to new technology in various form factors and interface types. For instance, backing up data from IDE to SATA, or mSATA to SATA. For more see the next page.

Test & Erase Scripts
Demi PG520 sanitizes drives with the method compliant with **DoD 5220.22**, **NSA (National Security Agency) Erase, Security Erase** and **One-time Erase**. Short SMART Self Test Mode quickly tests the drive connected to the target port.

More Than A Duplicator
This tool erases, resizes and diagnoses to get a critical job done just in one small machine.

File System and Error Skip Copy make copy fast
File System Copy Mode duplicates data area formatted in FAT, FAT32, NTFS, EXT2 and EXT3 using MBR and GPT. **Error Skip Copy** skips a weak and unstable sector and continues duplication without endless retries for read/write.

YEC

"Trusted by digital technology professionals for over three decades."

See more in the back

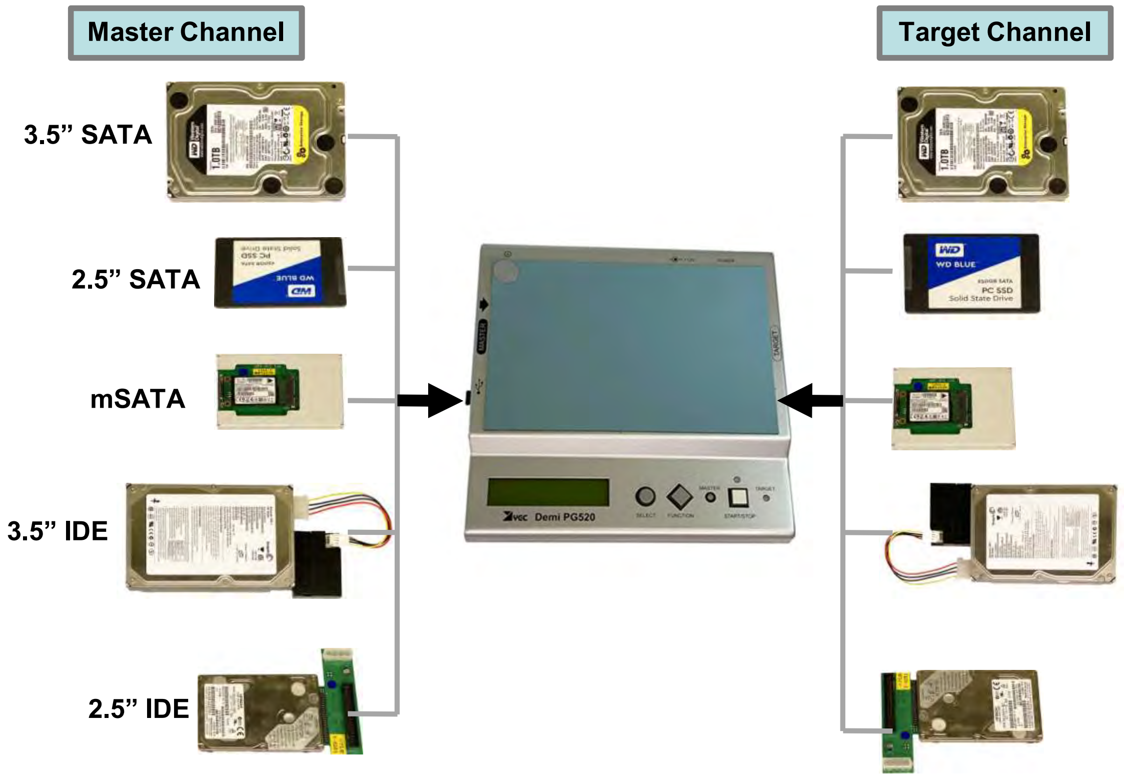
For more information, please visit www.yecglobalsolutions.com or call **(657) 298-3276.**

DEMI PG520

FEATURES

- **DUPLICATION** All copy, All copy & compare, All compare, Error skip copy, File system copy & compare, File system copy, File system compare
- **ERASURE** DoD 5220.22 erase, One-time erase, NSA erase, Security Erase, Erase data check
- **DIAGNOSIS** Short SMART self test
- **RESIZE** HPA auto resize, HPA removal
- **DRIVE INFO** Device sense, Device info, Error info

Cross-Interface Copy Options



Master Channel

Target Channel

3.5" SATA

2.5" SATA

mSATA

3.5" IDE

2.5" IDE

SPECIFICATIONS

	Descriptions
Model	DEMI PG520
Part No.	Y-2090
Supported Interface	SATA 3 Gbps
Optional Interface	IDE(2.5" 3.5") , mSATA
Port Connections	1 to 1 duplication, 2 x erase, 2 x test

	Descriptions
Dimensions	6.9 x 6.7 x 1.2" (175 x 171 x 31mm)
Weight	1.4 Lb (650g)
Power Specifications	AC 100-240V 50/60Hz
Power Consumption	0.5A 12V
Operating Environment	Temperature 10 - 35℃ (50 – 95°F) Humidity 30 - 80% No Condensation

www.yecglobalsolutions.com

www.kk-yec.co.jp

Global Sales and Support
YEC Global Solutions, Inc.
10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A.
T: 657-298-3276 sales@yecglobalsolutions.com

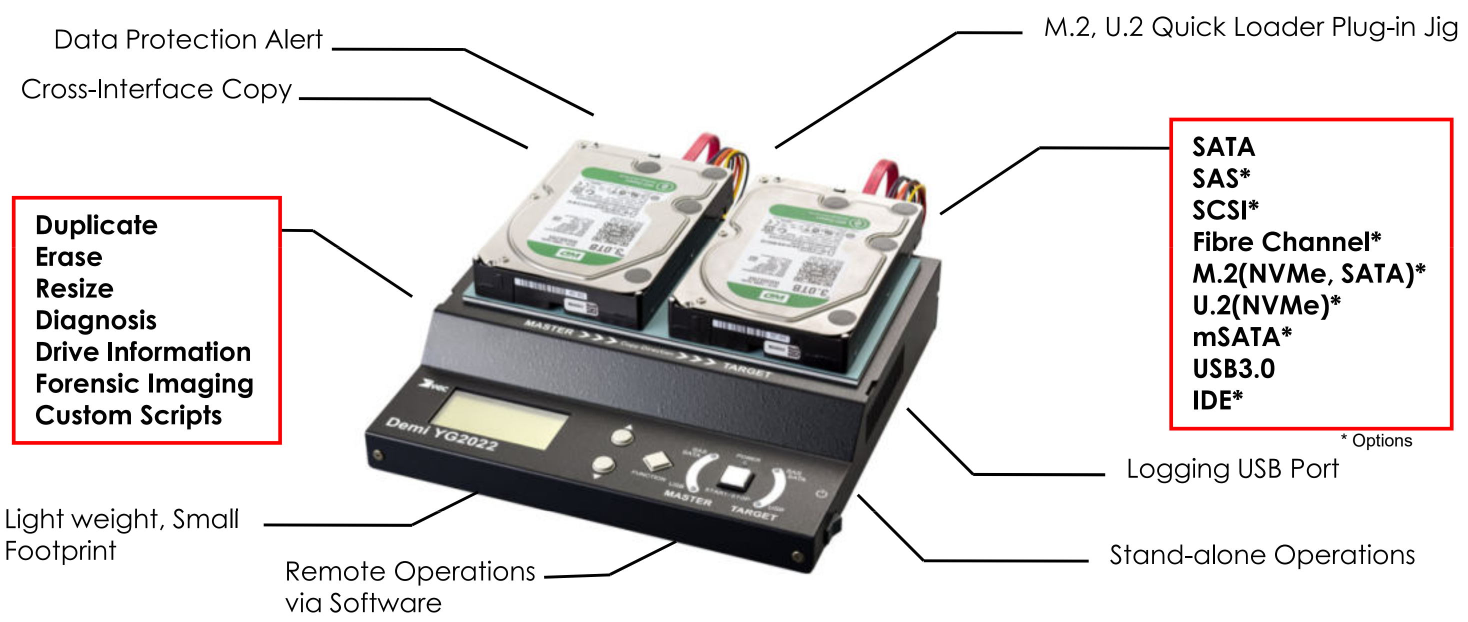
Developed and Manufactured
YEC Co. Ltd.,
3-44-45 Minami-machida, Machida, Tokyo 194-0005 Japan
T:+81- 42-796-8511 F: +81- 42-796-2367

* The specifications and design of the product are subject to change without notice.

2407 200

Demi YG2022

Compact and Multi Interface Duplicator



Backed by 30 years of experience and engineering in digital storage technology, built for professionals in the IT community demanding full flexibilities in one unit, Demi YG2022 is the answer to their voice.

Multi Interface Support

Native interface SATA 6G and USB3.0 accelates the process speed to the limit. In addition, Demi YG2022 is capable of connectionswith **SAS**, **SCSI** and **Fibre Channel**, not mention to IDE and mSATA (Full and Half Size). 50–68pin and 80–68pin SCSI adapters available.

Latest M.2 and U.2 SSD Support

Demi YG2022 has capabilities for connection of M.2 NVMe/SATA and U.2 NVMe devices via PCIe Gen3 x 4 bus. **72GB/m*** tested read speed by M.2 NVMe device. Proprietary Quick Loader plug-in jig ensures easy yet smooth loading and unloading without damaging any parts. (* varies by model)

NIST 800.88 Standards Compliant

DEMI YG2022 sanitizes drives with a method in compliant with NIST 800.88 standards in addition to DoD 5220.22-M , Security Erase and other scripts. The most requested erasure methods by IT and health care professionals.

Cross-Interface Copy

It helps backing-up old, phasing-out drives to new technology among various interface types. For example, backing up data from SCSI to SATA, or Fibre Channel to SATA. For details see the next page.

Safeguarding Data Against Unintended Overwrite

It would be a shocking moment when realizing critical data is overwritten unintentionally in error! When the master drive is connected in target drive position or the target drive contains data, HIT MG2060 proactively checks before proceeding overwrite and warns the user that the data still exists.

More Than A Duplicator

Multi interface duplication is not the only advantage YG2022 offers. As an all-round capabilities machine, it erases, resizes, and diagnoses, getting critical jobs done just in one unit.

File System and Mapping Copy modes make copy fast

File System Copy Mode duplicates data area only using MBR and GPT. **MAP COPY** function cuts down copy time drastically when copying a large volume. Utilizing the master data information for repeating copy events efficiently.

Data Recovery Copy Modes

ERROR SKIP COPY and **REVERSE COPY** are must-have tools to retrieve as much data as possible from a drive with issues. Error Skip Copy skips a weak sector and continues duplication. Reverse Copy allows for better chances to salvage data from a hard-to-read drive by copying backward from the ending sector .**ADVANCED REVERSE SKIP COPY** is more powerful for this task.

Use Device As External Drive

Drive connected to YG2022 can be mounted as an external master or target drive for PC via Ethernet connection. Master drive is write-protected when being accessed without risking data integrity.

Increase Power With Software

Optional software adds advantages furthermore in using Demi YG2022. It executes a script remotely and creates log files, work reports and CSV database and save them in PC. Sold separately.

"Trusted by digital technology professionals for over three decades. "

For more information, please visit www.yecglobalsolutions.com or call (657) 298-3276.

DEMI YG2022

FEATURES

- **DUPLICATION** All copy, Compare, Error skip copy, Reverse copy, Range copy, Data only copy, Mapping copy, Cross-interface copy
- **ERASURE** NIST Purge, Clear, Verify, DoD(3), DoD ECE (7), Security Erase, One time Erase, , NSA (National Security Agency) Method, NCSC (National Counterintelligence & Security Center) Method, US Army Method, US Navy Method, US Air Force Method
- **DATA RECOVERY** Bad sector skip copy, Reverse copy, Advanced Skip Copy, Advance Reverse Skip Copy
- **DIAGNOSIS** SMART Status, Short and extended self test, Read all and random, Write, Verify all and random, Read-Write-Compare, Cycle test, Test Repair
- **RESIZE** HPA, DCO, AMAC, SCSI Format
- **DRIVE INFO** Drive info, Partition info, Map data info, Erase map, Error info
- **FORENSIC IMAGING** DD Create, E01 Create, Ex01 Create, DD Hash, E01 Hash, Ex01 Hash, Format FAT32, Format ExFAT, Format NTFS, Restore image t HDD, Mount master to HDD, Mount target to HDD
- **CUSTOM SCRIPTING**
- **REPORTING** Detailed process logs, *Work reports, *CSV database (* via software)

CROSS-INTERFACE CONNECTIONS MATRIX

Master Drive

Target Drive

	SATA	SAS	SCSI	Fibre Channel	USB3.0	mSATA	IDE	M.2 NVMe/ SATA	U.2 NVMe
SATA	○	○	○	○	○	○	○	○	○
SAS	○	○			○	○	○		
SCSI	○		○		○	○	○		
F C	○			○	○	○	○		
USB3.0	○				○	○	○	○	○
mSATA	○	○	○	○	○	○	○	○	○
IDE	○	○	○	○	○	○	○	○	○
M.2	○				○	○	○	○	
U.2	○				○	○	○		○

OPTIONS
SAS Kit
SCSI Kit
Fibre Channel Kit
mSATA Adapter
IDE Kit
M.2 NVMe/SATA
U.2 NVMe
Software

SPECIFICATIONS

	Descriptions
Model	DEMI YG2022
Part No.	Y-2260
Supported Interface	SATA 6G USB3.0
Optional Interface	SCSI, Fbre Channel, M.2 NVMe/SATA, U.2 NVMe, mSATA, IDE (SCSI daisy-chained 68-50, 68-80 available)
Port Connections	1 to 1 duplication, 2 x erase, 2 x test
Dimensions	9.8 x 10.2 x 2.2" (250 x 258 x 55mm)
Weight	4.4 Lb (2.0kg)

	Descriptions
Cross-Interface Copy	SATA-SAS-SCSI-FC-mSATA-IDE-USB
Power Specifications	AC 100-240V 50/60Hz
Power Consumption	1.92A (Max)
Communication Port	Ethernet (1000BASE-T / 100BASE-TX / 10BASE-T)
Operating Environment	Temperature 10 - 35℃ (50 – 95°F) Humidity 30 - 80%
Logging Port	USB2.0 Type A
Maximum HDD Capacity	SATA: 144PB SAS: 9.4ZB

www.yecglobalsolutions.com

www.kk-yec.co.jp

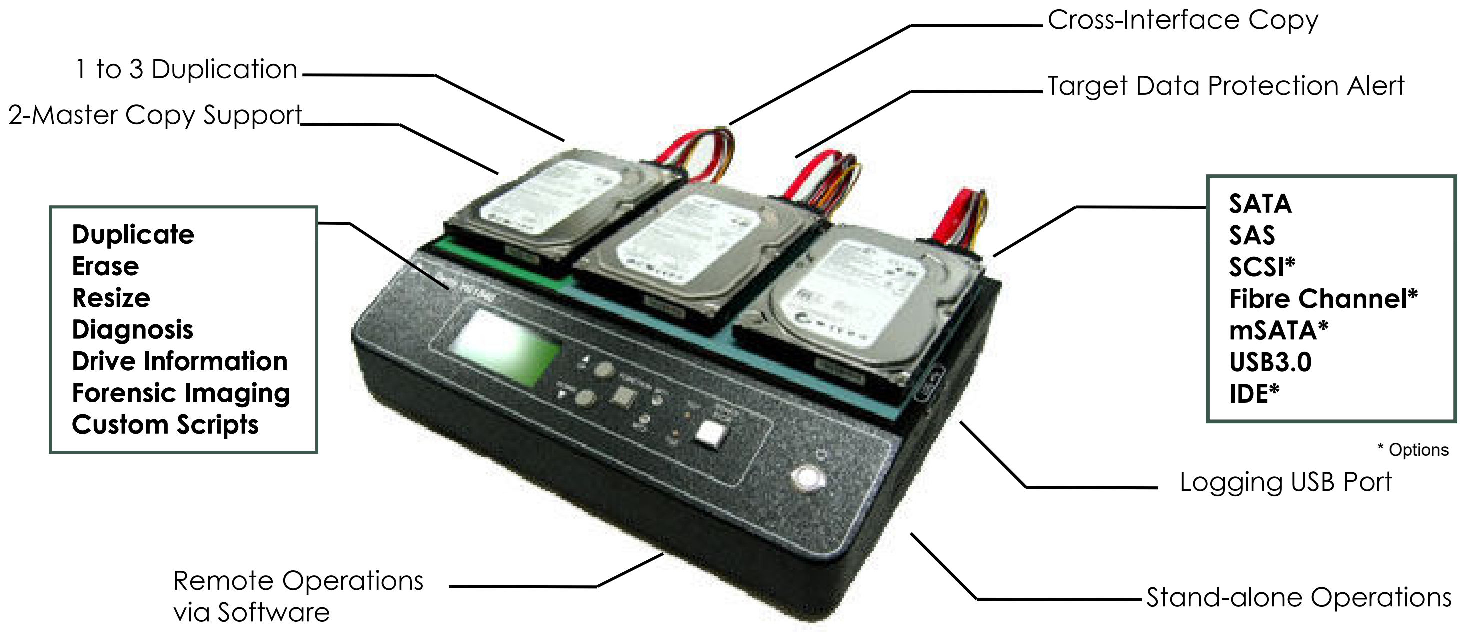
Global Sales and Support
YEC Global Solutions, Inc.
10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A.
T: **657-298-3276** **sales@yecglobalsolutions.com**

Developed and Manufactured
YEC Co. Ltd.,
3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan
T:**+81- 42-796-8511** F: **+81- 42-796-2367**

* The specifications and design of the product are subject to change without notice.

Demi YG2040

Dependable, Versatile Duplicator



Cross-Interface Copy

1 to 3 Duplication

2-Master Copy Support

Target Data Protection Alert

Duplicate
Erase
Resize
Diagnosis
Drive Information
Forensic Imaging
Custom Scripts

SATA
SAS
SCSI*
Fibre Channel*
mSATA*
USB3.0
IDE*

* Options

Logging USB Port

Remote Operations
via Software

Stand-alone Operations

Backed by 30 years of experience and engineering in digital storage technology, built for professionals in IT and law-enforcement communities in need of full flexibility in one small unit, that is what Demi YG2040 is all about.

A Wide Range of Interface Support

Native interface SATA 6G, SAS 6G and USB3.0 accelerates the process speed to the limit. In addition, Demi YG2040 is capable of connections with **SCSI** and **Fibre Channel**, not mention to IDE and mSATA (Full and Half Size). 50–68pin and 80–68pin SCSI adapters available.

Dual Master Drive Configuration Copy

Demi YG2040 is versatile in copy scenarios. Basic 1 to 1 copy, 1 to 2 copy, 1 to 3 copy. 2 concurrent copy sessions of 1 to 1 duplicating two SATA and SAS master drives to 2 target drives. Cutting down the duplication time almost in half.

Cross-Interface Copy

It helps backing-up old, phasing-out drives to new technology among various interface types.. For example, backing up data from SCSI to SATA, or Fibre Channel to SATA. For details see the next page.

Proactive Data Protection from Unintended Overwrite

It would be a shocking moment when realizing critical data is overwritten unintentionally! When Master drive is connected to Target port or Target drive still contains data, Demi YG2040 proactively checks before proceeding to the overwrite mode and alerts user of potential accident.

More Than A Duplicator

Multi interface duplication is not the only advantage YG2040 offers. As an all-round capabilities machine, it erases, resizes, diagnoses, and images forensically on a professional level as well, getting all critical jobs done just in one unit.

File System and Mapping Copy modes make copy fast

File System Copy Mode duplicates data area only using MBR and GPT. **MAP COPY** function cuts down copy time drastically when copying a large volume. It Utilizes the master data information for repeating copy events efficiently.

Data Recovery Copy Modes

ERROR SKIP COPY and **REVERSE COPY** are must-have tools to retrieve as much data as possible from drive with issue. Error Skip Copy skips a weak sector and continues duplication on. Reverse Copy allows for better chances to salvage data from a hard-to-read drive by copying backward from the last sector to beginning .**ADVANCED REVERSE SKIP COPY** is more powerful for this task.

Use Device As External Drive

Drive connected to YG2040 can be mounted as an external master or target drive for PC via Ethernet connection. Master drive is write-protected when being accessed without risking data integrity.

Increase Power With Software

Optional software adds advantages furthermore in using Demi YG2040. It executes script remotely and creates log files, work reports and CSV database saving them in PC. Sold separately.

“Trusted by media device technology professionals for over three decades. “

For more information, please visit www.yecglobalsolutions.com or call (657) 298-3276.

DEMI YG2040

FEATURES

- **DUPLICATION** All copy, Compare, Error skip copy, Reverse copy, Range copy, Data only copy, Mapping copy, Multi target copy, Cross-interface copy
- **ERASURE** NIST Purge & Clear, DoD(3), DoD ECE (7), Security Erase, One time Erase, N times Erase, NSA, NCSC, US Army, US Navy, US Air Force
- **DATA RECOVERY** Bad sector skip copy, Reverse copy, Advanced Skip Copy, Advance Reverse Skip Copy
- **DIAGNOSIS** SMART Status, Short and extended self test, Read all and random, Write, Verify all and random, Read Write compare, Cycle test, Test Repair
- **RESIZE** HPA, DCO, AMAC, SCSI Format
- **DRIVE INFO** Drive info, Partition info, Map data info, Erase map, Error info
- **FORENSIC IMAGING** DD Create, E01 Create, Ex01 Create, DD Hash, E01 Hash, Ex01 Hash, Format FAT32, Format exTAT, Format NTFS, Restore image to HDD, Mount master to HDD, Mount target to HDD
- **CUSTOM SCRIPTING**
- **REPORTING** process logs, work reports, CSV database

CROSS-INTERFACE CONNECTIONS MATRIX

Master Drive

Target Drive

	SATA	SAS	SCSI	Fibre Channel	USB3.0	mSATA	IDE
SATA	○	○	○	○	○	○	○
SAS	○	○			○	○	○
SCSI	○		○		○	○	○
F C	○			○	○	○	○
USB3.0	○				○	○	○
mSATA	○	○	○	○	○	○	○
IDE	○	○	○	○	○	○	○

OPTIONS
SCSI Kit
Fibre Channel Kit
USB Kit (Target)
mSATA Adapter
IDE Kit
Terminal Software

SPECIFICATIONS

	Descriptions
Model	DEMI YG2040
Part No.	Y-2255
Supported Interface	SATA 6G SAS 6G USB3.0
Optional Interface	SCSI, Fbre Channel, mSATA, IDE (SCSI daisy-chained:68-50, 68-80 available)
Port Connections	1 to 3 duplication, 2 sessions x 1 to 1 duplication, 4 x erase
Dimensions	10 “x 10“ x 2.5” 350 255 77
Weight	3.25lb 2.8k

	Descriptions
Cross-Interface Copy	SATA-SAS-SCSI-FC-mSATA-IDE-USB
Power Specifications	AC 100-240V 50/60Hz
Power Consumption	1.92A (Max)
Communication Port	Ethernet (1000BASE-T / 100BASE-TX / 10BASE-T)
Operating Environment	Temperature 10 - 35℃ (50 – 95°F) Humidity 30 - 80%
Logging Port	USB2.0 Type A
Maximum HDD Capacity	SATA: 144PB SAS: 9.4ZB

www.yecglobalsolutions.com

www.kk-yec.co.jp

Global Sales and Support
YEC Global Solutions, Inc.
10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A.
T: **657-298-3276** **sales@yecglobalsolutions.com**

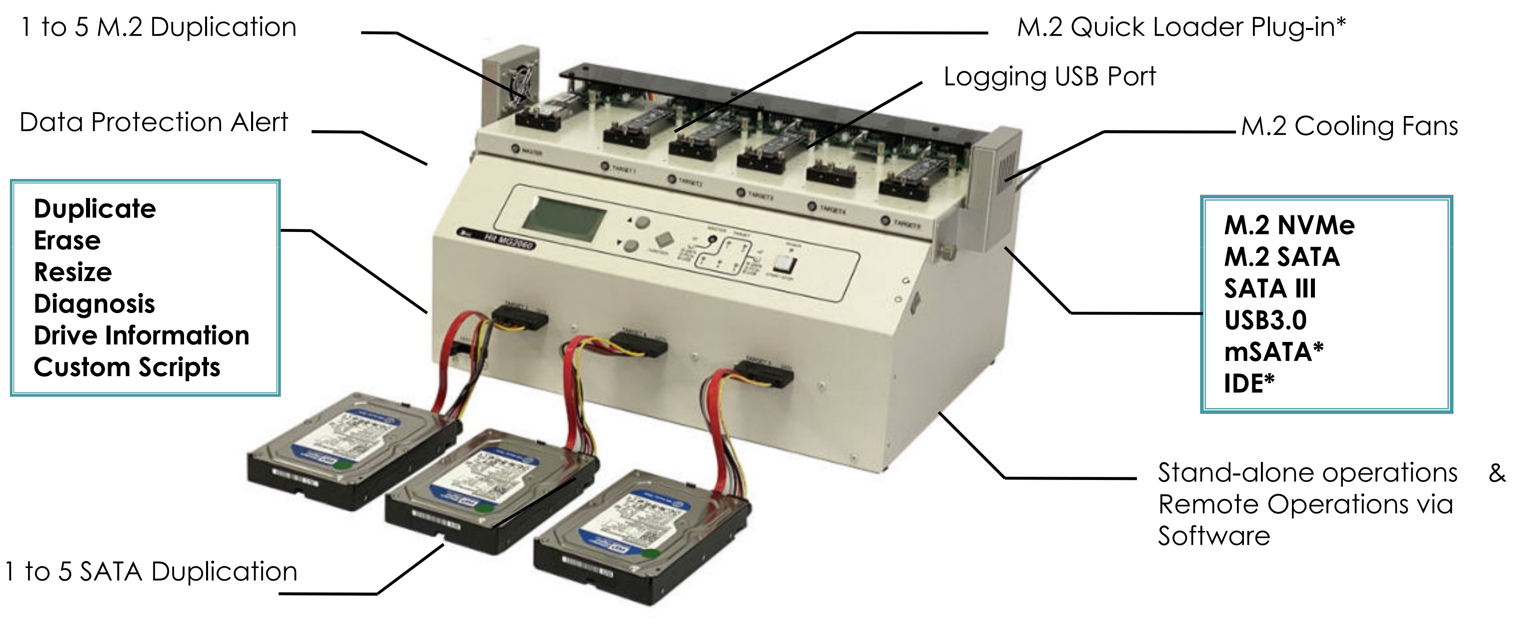
Developed and Manufactured
YEC Co. Ltd.,
3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan
T:**+81- 42-796-8511** F: **+81- 42-796-2367**

* The specifications and design of the product are subject to change without notice.

2201 21

HIT MG2060

PCIe M.2 & SATA Duplicator



* SATA plug-in jig option available

Backed by 30 years of experience and engineering in digital storage technology, HIT MG2060 offers advanced M.2/SATA duplication solutions for manufacturing industry and IT professionals.

M.2 and SATA Interface Support

Supporting ultra fast **M.2 NVMe via PCIe Gen3 x 4**. **179GB/m*** tested read speed by M.2 NVMe device. SATA III and USB 3.0 are supported natively as well. Legacy interface connection, IDE** and mSATA**, are also supported.
(*varies by device) (** optional)

M.2 Quick Loader Plug-in and Cooling Fans

YEC's proprietary M.2 Quick Loader provides reliable connection quick and easy with M.2 device size of 2230, 2242, 2260, 2280 and 22110. Cooling fans improve data transfer performance. Quick Loader for SATA HDD is available as an option.

Slow Drive Elimination – Reliable Performance

User can specify minimum transfer speed. When one of the drives performs slower, the entire duplication time gets prolonged. In order to avoid speed drop coming from it, HIT MG2060 constantly monitors the data transfer speed of every single target drive during the duplication process. The device slower than the minimum speed will be checked and eliminated from the duplication event automatically thus achieving the fastest result possible. Using the real-time transfer rate displayed in the control screen, User can abort the slow drive manually without interrupting other drives being processed as well.

Proactive Data Protection from Unintended Overwrite

It would be a shocking moment when realizing critical data is overwritten unintentionally! When Master drive is connected to Target port or Target drive still contains data, HIT YG3210 proactively checks before proceeding to the overwrite mode and alerts user of potential accident.

Reporting

Detailed logs are automatically generated, recording every process events. In case an error occurs, the system will log when and what issue has caused it. **CSV database** and **Work Report** features are available as option.

More Than A Duplicator

Multi interface duplication is not the only advantage that MG2060 offers. As an all-round capabilities machine, it erases, resizes, and diagnoses, getting critical jobs done just in one unit.

NIST 800.88 Standards Compliant

NIST 800.88 Purge and Clear scripts are included in addition to DoD 5220.22-M , Security Erase and other scripts. Great erasure methods for health care and ITAD professionals.

File System and Mapping Copy modes make copy fast

File System Copy Mode duplicates data area only using MBR and GPT. **MAP COPY** function cuts down copy time drastically when copying a large volume. It utilizes the master data information for repeating copy events efficiently.

Low Maintenance

Replacing M.2 jig board is so easy. No tools required. All It takes is remove one thumb screw.

Increase Power With Software

Optional software adds advantages furthermore in using HIT MG2060. It executes a script remotely, creates log files, work reports and CSV database and saves them in PC. Sold separately.

YEC

"Trusted by digital technology professionals for over three decades. "

For more information, please visit www.yecglobalsolutions.com or call (657) 298-3276.

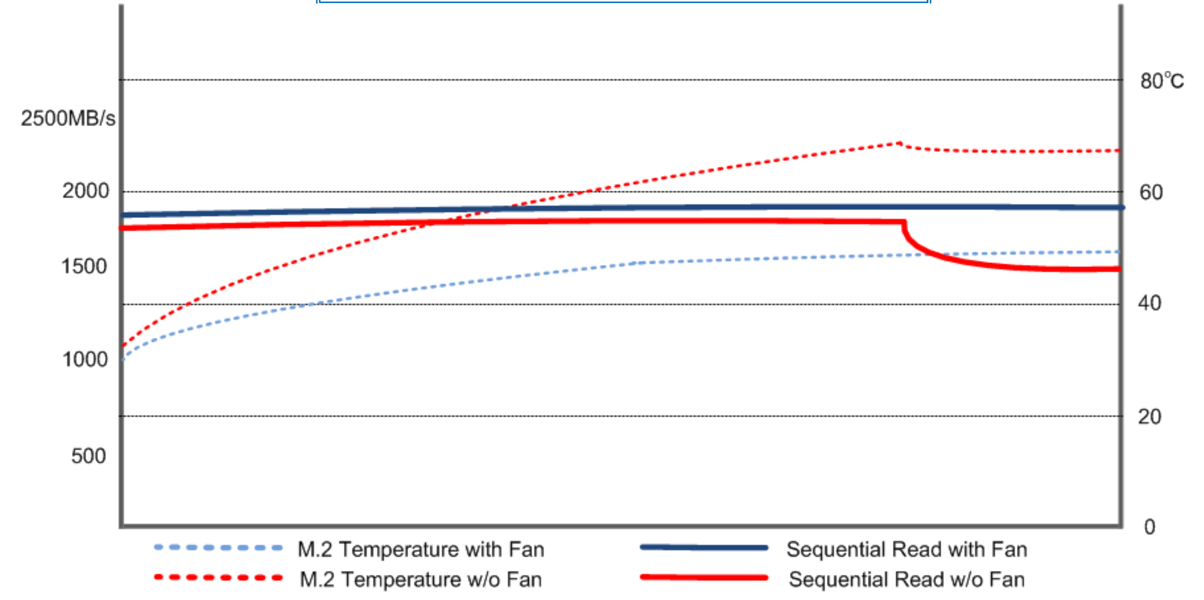
HIT MG2060

FEATURES

- **DUPLICATION** All copy, Compare, Error skip copy, Reverse copy, Range copy, Data only copy, MAP copy, Cross-interface copy
- **ERASURE** NIST 800.88, DoD 5220.22-M, Security Erase, One time Erase, N times Erase, NSA (Nat'l Security Agency), NCSC(Nat'l Counterintelligence & Security Center)
- **DIAGNOSIS** SMART Status, Short and extended self test, Read all and random, Write, Verify all and random, Read Write compare, Cycle test, Test Repair
- **RESIZE** HPA, DCO, AMAC
- **DRIVE INFO** Drive info, Map data info, Erase map, Error info
- **CUSTOM SCRIPTING**
- **REPORTING** Detailed process log, work report*, CSV database * (* via optional software)

- **RECOMMENDED USE:** Manufacturing, Testing Labs, Health Care, Education, Defense

EFFECTIVENESS OF COOLING FAN



SPECIFICATIONS

	Descriptions
Model	HIT MG2060
Part No.	Y-2530
Supported Interface	M.2 (NVMe, SATA) SATA 6G USB3.0
Optional Interface	IDE, mSATA
Port Connections	1 to 5 duplication, 6 x erase
Dimensions	L17 "x W12" x H9" (430 x 310 x 234mm)
Weight	23lb (10.5 kg)

k
G

	Descriptions
Cross-Interface Copy	SATA – M.2 –USB – IDE - mSATA
Power Specifications	AC 100-240V 50/60Hz
Power Consumption	150VA
Communication Port	Ethernet (1000BASE-T / 100BASE-TX / 10BASE-T)
Operating Environment	Temperature 10 - 35℃ (50 – 95ºF) Humidity 30 - 80% (No Condensation)
Logging Port	USB2.0 Type A
Maximum HDD Capacity	SATA: 144PB M.2: 9.4ZB

www.yecglobalsolutions.com

www.kk-yec.co.jp

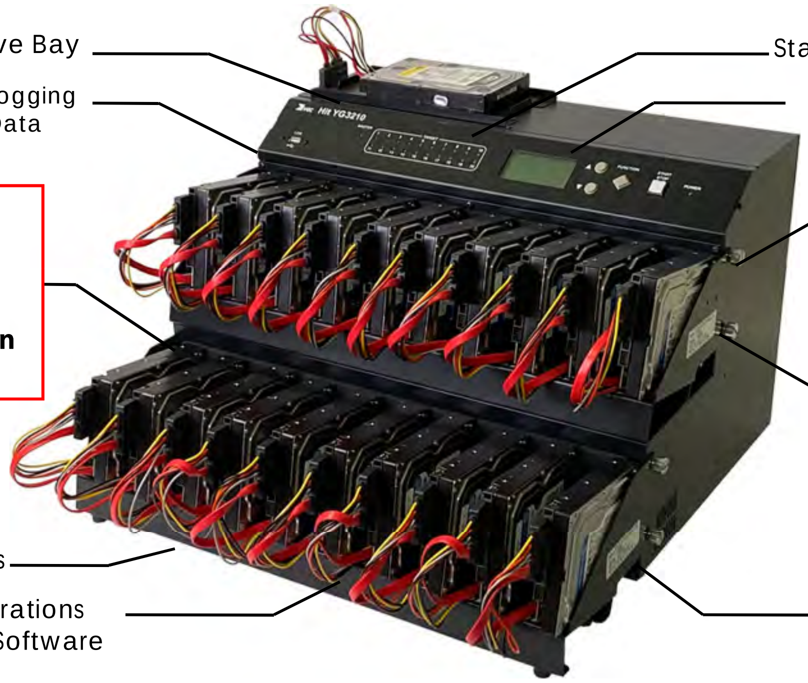
Global Sales and Support
YEC Global Solutions, Inc.
10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A.
T: **657-298-3276** **sales@yecglobalsolutions.com**

* The specifications and design of the product are subject to change without notice.

Developed and Manufactured
YEC Co. Ltd.,
3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan
T:**+81- 42-796-8511** F: **+81- 42-796-2367**

HIT YG3210

Industrial Grade SATA Duplicator



Master Drive Bay

USB Port for Logging & Mapping Data

Duplicate
Erase
Resize
Diagnosis
Drive Information
Custom Scripts

Stand-alone Operations

Remote Operations via Terminal Software

Status LED lights

Control Panel
Data Protection Alert

SATA
eSATA

20 Target Drive Bays

2.5” & 3.5” Quick Loading
Plug-in Jigs Option Available

Backed by 30 years of engineering and experience in digital media technology, HIT YG3210 performs volume tasks reliably and efficiently in highly demanding industrial and business settings.

Industrial Grade Duplicator

Native SATA III interface at 36GB/m* accelerates copy speed to the limit. Built for high demanding use settings: copying to 20 target drives with one push button operation, cable-less plug-in jig** facilitating quick drive loading and reliable results. HIT YG3210 is in a small footprint with 20 vertically seating bays.

Slow Drive Elimination – Keeping Copy Speed Fast

User can set minimum transfer speed in the Configuration Management. When one of the drives performs slower, the entire duplication time gets prolonged. In order to avoid speed drop coming from it, HIT YG3210 constantly monitors the data transfer speed between the master device and every single device during the duplication process. The device slower than the minimum speed will be checked and eliminated from the duplication event automatically thus achieving the fastest results possible. Since the control panel displays the slowest transfer rate, user can deactivate the slow drive manually from the copy chain without interrupting other drives as well.

18 Duplication Scenarios

HIT YG3210 covers a whole wide range of copy tasks meeting many duplication requirements the user may have. That includes **All Copy & Compare**, **Error Skip Copy**, **File System Copy & Compare,** to name just a few.

Proactive Data Protection from Unintended Overwrite

It would be a shocking moment when realizing critical data is overwritten unintentionally in error! When the master drive is connected in target drive position or the target drive contains data, HIT YG3210 proactively checks before proceeding overwrite and warns the user that the data still exists.

More Than A Duplicator

Mass target duplication is not the only advantage HIT YG3210 offers. As an all-round capabilities machine, it diagnoses, erases and resizes, getting demanding jobs done just in one unit.

File System and Mapping Copy modes make copy fast

File System Copy Mode duplicates data area only using MBR and GPT. **MAP COPY** function cuts down copy time drastically when copying a large volume. Utilizing the master data information for repeating copy events efficiently.

Increase Power with Software*

Optional software adds advantages furthermore in using HIT YG3210. It executes a script remotely, creates log files, work reports and CSV database and saves them in PC.

*Varies by device model
** Options

“Trusted by digital technology professionals for over three decades. “

For more information, please visit www.yecglobalsolutions.com or call (657) 298-3276.

HIT YG3210

FEATURES

- **DUPLICATION** All copy, All copy & Compare, All compare, Error skip copy, File System copy, File System copy & Compare, File System compare, MAP copy, MAP copy & Compare, MAP compare, HPA all copy, HPA all copy & Compare, HPA File System copy, HPA File System copy & Compare, DCO all copy, DCO all copy & Compare, DCO File System copy, DCO File System copy & Compare
- **ERASURE** DoD5220.22(3), Security Erase, One time and N tme Erase & Compare, NSA (National Security Agency) Method, NCSC (National Counterintelligence & Security Center) Method, US Army Method, US Navy Method, US Air Force Method, Data Compare
- **DIAGNOSIS** All read, Random read, All Verify, Random Verify, Random write, Read & Write & Compare, Running test, Test repair, SMART enable & disable, SMART read data, SMART view data, SMART Status, SMART short test, SMART extended test
- **RESIZE** HPA (MB), HPA (LBA), DCO (MB), DCO (LBA), HPA removal, DCO removal
- **DRIVE INFO** Device sense, Device info, MAP data info, MAP data erase, MAP erase all data, Error info
- **CUSTOM SCRIPTING**
- **REPORTING** Detailed process logs, Work reports*, CSV database* (*Terminal software required)

- **RECOMMENDED USE** Digital cinema distribution, Manufacturing, Defense, Schools and Colleges

Status Indicator LED

Detachable Plug-in Jig Option

SPECIFICATIONS

	Description
Model	HIT YG3210
Part No.	Y-2140
Supported Interface	SATA 6G eSATA 6G
Port Connections	Master to 20 Targets
Dimensions	20”x 14“ x 12” 500 x 340 x 310(mm)
Weight	18.6 lbs 13kg

	Description
Power Specifications	AC 100-240V 50/60Hz
Safety and Protection	Primary Power Input Protection (3A fuse)
Operating Environment	Temperature 10 - 35℃ (50 – 95°F) Humidity 30 - 80%
Logging Port	USB2.0 Type A
Maximum HDD Capacity	SATA: 144PB
Options	Terminal Software, Quick Plug-in Jig

www.yecglobalsolutions.com

Global Sales and Support
YEC Global Solutions, Inc.
10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A.
T: **657-298-3276** **sales@yecglobalsolutions.com**

www.kk-yec.co.jp

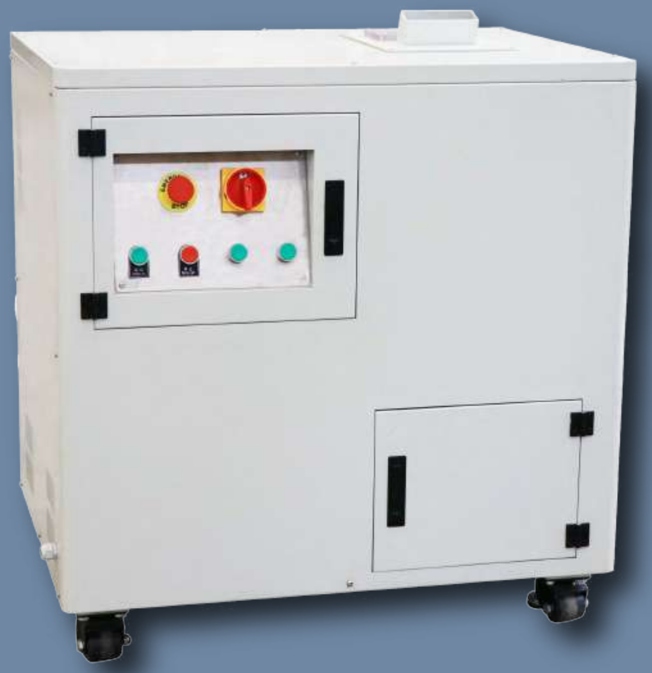
Developed and Manufactured
YEC Co. Ltd.,
3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan
T:**+81- 42-796-8511** F: **+81- 42-796-2367**

* The specifications and design of the product are subject to change without notice.

Media Shredder & Destroyer

Standard hard disk shredder

Small Hard disk shredder for office use which can shred server hard disk.



Supported Media

SSD HDD mobile Tape

Shredding Particle Size

20mm * random

Security Level (DIN 66399)

O-1 T-1 E-3 H-4

Shredding Capacity

60 pcs / hr

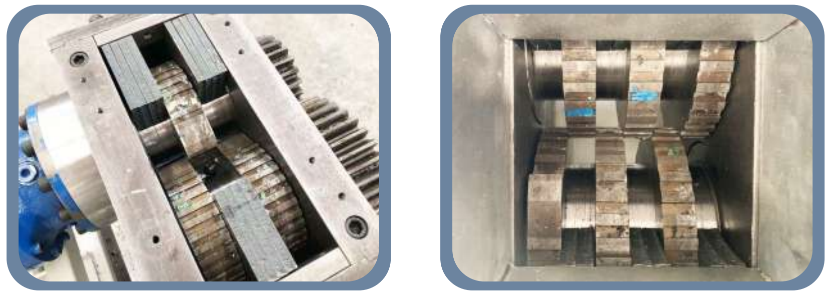
Advantages

- Fully destroy hard disk physically.
- Fulfill the DIN 66399 O-1, T-1, E-3, H-4 standard.
- Small size and save space.
- Specifically design for office environments.
- Automatically reverse rotation when it gets jam.

Shredding size

Electrical cabinet

Shredding blade



Specifications

Model	**DEZ-HS1000**
Shredding materials	Enterprise 3.5” HDD, 2.5” HDD, SSD, Tape (LTO/DLT/DDS)
Shredding particle size	20mm * random
DIN66399 Level	O-1, T-1, E-3, H-4
Blade thickness	20mm or customized 40mm
Shredding capacity	60 pcs / hr
Feeding Conveyor	116x 35 mm
Power	0.75 KW, single phase 230V, 13A, 50HZ
Waste collection Bin	25L
Machine size:	894(L) x 650(W) x 1000(H) mm
Machine weight	358Kg
Characteristic	Planetary gear box, automatically reverse rotation when it gets jam, wooden package, Heavy duty wheels

iPad & hard disk shredder

Shredder with double feeding ports designed for iPads and HDDs with H4 level.

Supported Media

SSD HDD Floppy CD & DVD

Mobile Phone Tablet Laptop

Shredding Particle Size

18mm * random

Security Level (DIN 66399)

H-4

Shredding Capacity

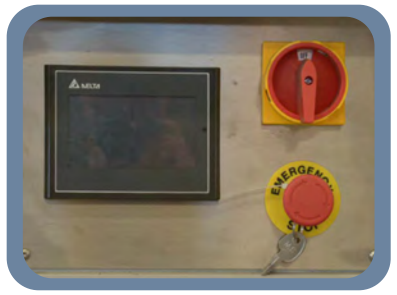
200 pcs / hr

Feeding Ports

Shredding blade

Shredding size

Control panel



Advantages

- Compact size and single phase designed ideal for offices.
- Design with dual feeding ports: one for HDDs and the other for iPads and laptops.
- Auto reverse for easy clearing of jams.
- Ergonomic easy switch with auto start/stop, reverse, and door open indicator.
- Energy Savings Mode (ESM) shuts off power when not in use.
- Special Conveyor designed for controlling feeding speed.

Specifications

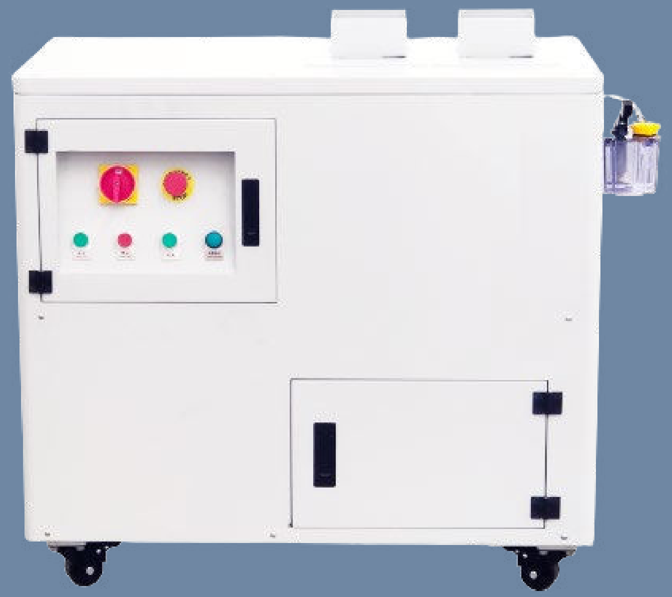
Model	**DEZ-HS2800**
Shredding materials	Hard Disk / Solid State Drive / CD / Floppy / Moblie / Tablet/laptop
Shredding particle size	18mm * random
DIN66399 Level	H-4
Blade thickness	18mm & 12mm
No. of Cutting Shaft	2
No. of Blades	15 pcs for HDD and iPad
Shredding capacity	200 pcs / hr
Shredding Time	12s
Feeding Ports	260 mm & 116x36 mm
Waste collection Bin	Total 30L
Power	220V single phase (16A/20A) or 380V three phase
Machine size:	1144(L)x620(W)x1190(H)mm
Characteristic	Planetary gear box, automatically reverse rotation when it gets jam, Touch screen, Heavy duty wheels

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Standard Combo Hard Disk Shredder

Small Hard disk shredder for office use with two sets blade for shredding HDD and SSD.



Supported Media

SSD | HDD | Tape | CD & DVD | mobile

Shredding particle size

20mm or 5mm

Security Level (DIN 66399)

O-3 T-2 E-3 H-4

Shredding Capacity

50 pcs / hr

Advantages

- Combo blades with 20mm and 5mm to meet any shredded result for HDD and SSD destruction.
- Specifically designed for office environments.
- Solid hardened steel knife which is able to shred the hard drive and its internal components including the data disk.
- Use 0.75KW motor which can use in 13A plug
- Includes planetary gear box and button control.

Shredding blade

Shredding size

Specifications

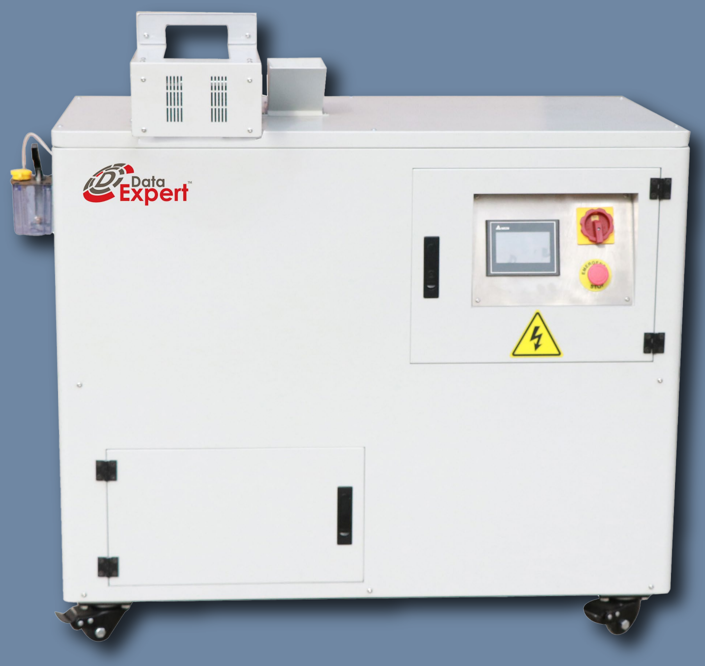
Model	DEZ-HS2900
Shredding method	Combo blade design, 20mm for HDD, 5mm for SSD
Shredding materials	Server HDD, SSD, Mobile phone, magnetic tape, USB drive, CD
Shredding particle size	HDD: 20mm*random, SSD：5mm*random
Blade thickness	20mm+5mm
Shredding capacity	HDD: 50 pcs / hr, SSD: 60 / hr
Feed opening	Dual opening
Power	0.75 KW
Electricity	Single phase or three phase
Waste collection Bin	Two bins, 17L & 13L
Machine size	1004(L) x 540(W) x 1007(H) mm
Machine weight	400Kg

Data Expert

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Combo hard disk Shredder

A heavy duty shredder for HDD and SSD which can shred 200 pcs HDD per hour.



Supported Media

SSD HDD Floppy CD & DVD mobile

Shredding particle size

18mm or 9mm

Security Level (DIN 66399)

O-1 T-1 E-3 H-4

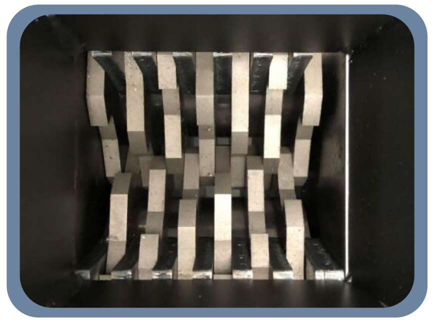
Shredding Capacity

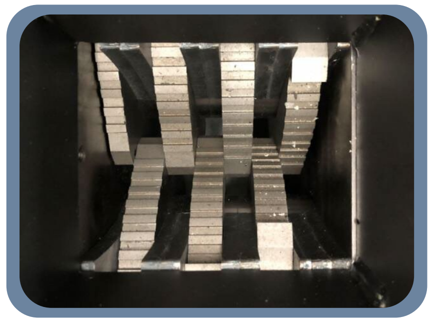
200 pcs / hr

Advantages

- Combo blades with 18mm and 9mm to meet any shredded result for HDD and SSD destruction.
- Specifically designed for office environments.
- Solid hardened steel knife it is able to shred the hard drive and its internal components including the data disk.
- Simply pushing a button.
- Compliance with safety requirements of CE.
- Security switch, auto reverse and cut-off to avoid shredding jam, bin-full auto sensor, cabinet door open/closed sensor and dust proof closed housing.

Shredding blade





Shredding size

Specifications

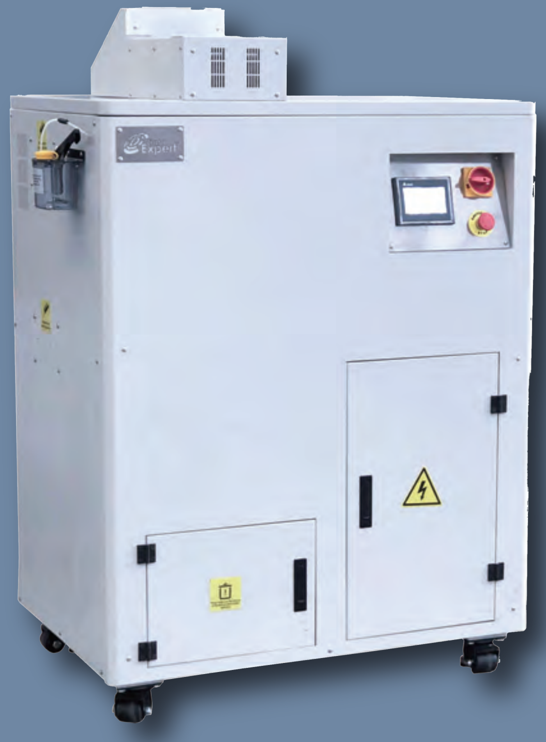
Model	DEZ-HS3000
Shredding method	Combo blade design, 18mm for HDD, 9mm for SSD
Shredding materials	Enterprise 3.5'' HDD, 2.5'' HDD, SSD
Shredding particle size	HDD: 18mm*random, SSD:9mm*random
Blade thickness	18mm+9mm
Shredding capacity	200 pcs / hr
Feeding Conveyor	230 x 115 mm
Power	3 KW, 3 phase 380V or single phase 230V, 50HZ
Waste collection Bin	40L, HDD:21L. SSD:19L
Machine size	1144(L) x 630(W) x 1175(H) mm
Machine weight	650Kg
Characteristic	With Touch screen and PLC control, wooden package, Heavyduty wheels

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

H5 Level hard disk Shredder

H5 Level HDD Shredder with dual step shredding construction for high security data destruction.



Supported Media

SSD HDD Tape CD & DVD mobile Floppy

Shredding particle size

More than 80% in 9*9mm

Security Level (DIN 66399)

H-4 H-5

Shredding Capacity

Approx in 320mm²

Advantages

- Fulfill the DIN 66399 H5 standard.
- Dual step shredding construction.
- Heavy duty two shaft shredding system with durable blade.
- Planetary gear box drive system.
- Working capacity more than 60pcs HDD per hour.
- Smart control PLC system

Shredding blade

Shredding size

Specifications

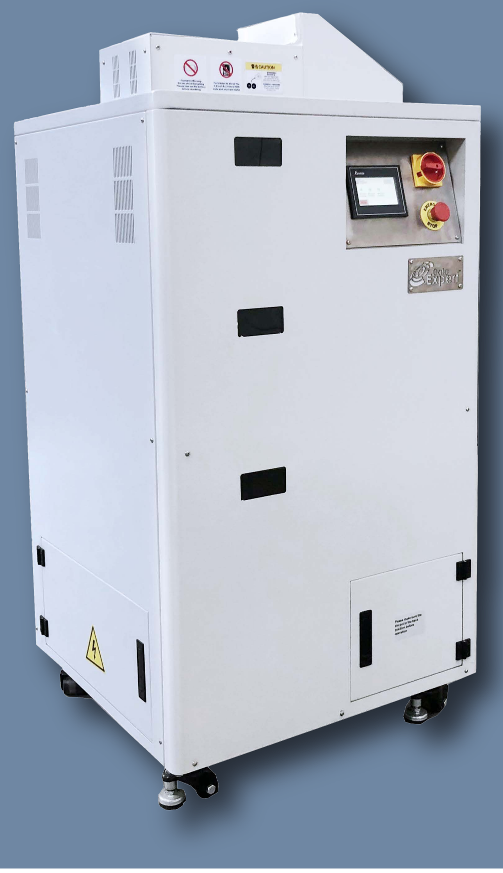
Model	DEZ-HS3500
Shredding method	Two step shredding with two motor and two shredder
Shredding materials	HDD, SSD, CD, Floppy, Mobile Phone, IPAD
Shredding particle size	More than 80% in 9*9mm, approx in 320mm²
DIN66399 Level	H-4,H-5
Blade thickness	9mm + 9mm
Shredding capacity	120 pcs / hr
Feeding Conveyor	230 x 115 x 70mm
Power	5.26 KW, 3 phase 380V or single phase 230V, 50HZ
Waste collection Bin	40L
Machine size:	1044(L) x 620(W) x 1500(H) mm
Machine weight	842Kg
Characteristic	With Touch screen and PLC control, wooden package, Heavyduty wheels

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Flash, SSD & Mobile Phone Shredder

A movable and high security data destruction designed shredder for SSD and mobile phone.



Application

SSD · mobile · Memory chip · CD & DVD · Credit Card · SIM Card

Shredding Particle Size

2*2mm

Security Level (DIN 66399)

E-4 E-5

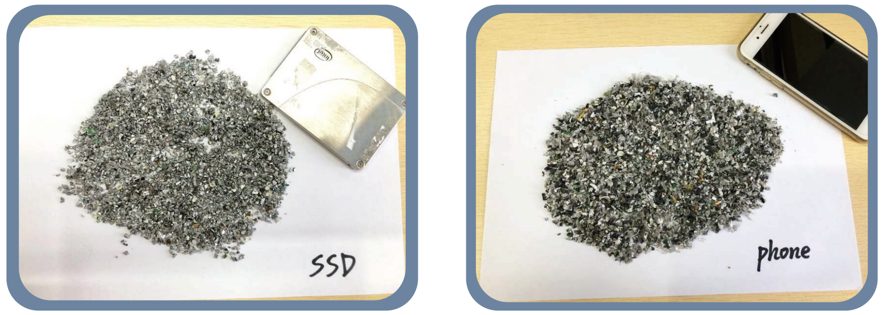
Shredding Capacity

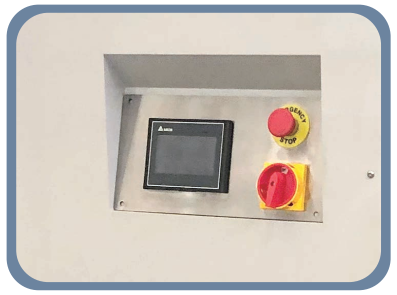
150 - 200pcs / hr

Other Advantages

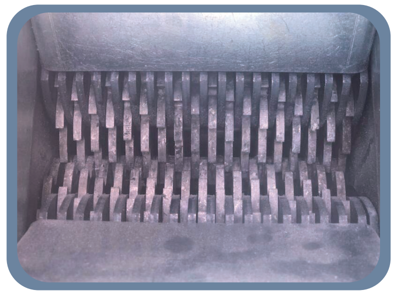
- Combo blades with 4mm and 2mm with three step shredding construction.
- Specifically design for office environments.
- Compliance with safety requirements of CE.
- Security switch, auto reverse and cut-off functions to avoid shredding jam
- Bin-full auto sensor, cabinet door open/closed sensor and dust proof closed housing.

Shredding size





Touch screen control



Shredding blade

Discharge bin

Model: DEZ-SSD2X2

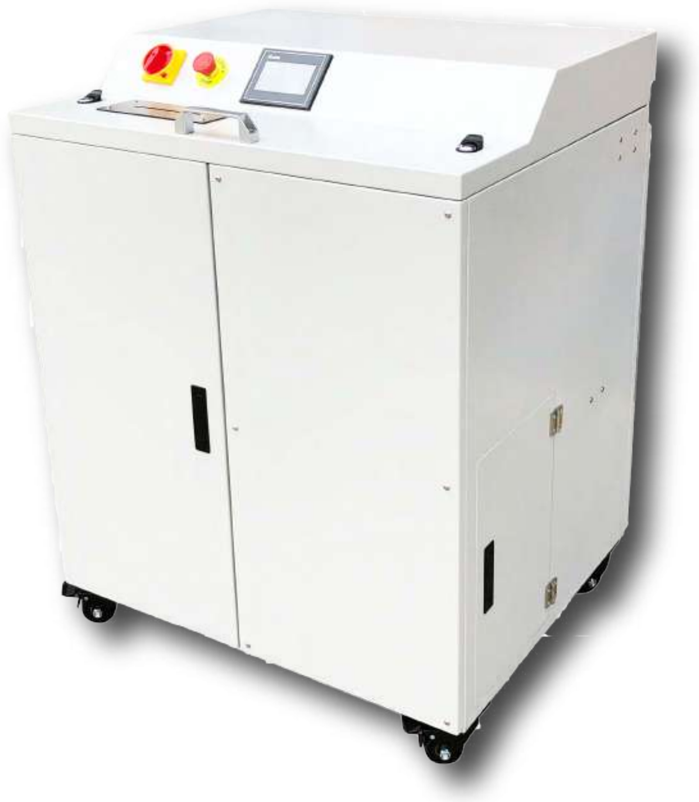
Shredding method	3 step shredding with 2 * dual shaft shredder
Shredding materials	SSD, Mobile Phone,CD USB, RAM, CARD
Blade thickness	First step with 4mm thickness blade, second and third step 2 mm thickness blade
Shredding particle size	2*2mm
Chamber box size	200*160mm
Throughout hard drive	150 - 200pcs / hr
Feeding Conveyor	230(L)*115(W)*70(H)mm
Power	2.25KW0.75 KW for each motor /(single phase)
Waste collection Bin	35L (500 * 250 * 280mm)
Machine size	740(L)*620(W)*1470(H) mm
Machine weight	423Kg
Package size	480KG
Package weight	China
Characteristic	With Touch screen and wooden package
Country of Origin	China

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Circuit Board & Chip Disintegrator

High security disintegrator which is designed to shred memory chips and microchips.



Supported Media

- SSD Chip
- Memory chip
- ID Card
- Sim Card
- CD & DVD

Shredding Particle Size

Optional
A. 0.5*0.5 mm²
B. 1*1 mm²
C. 2*2 mm²

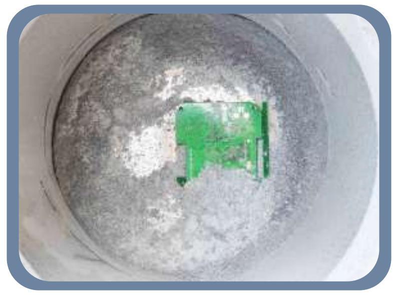
Shredding Capacity

5 - 10kg / hr

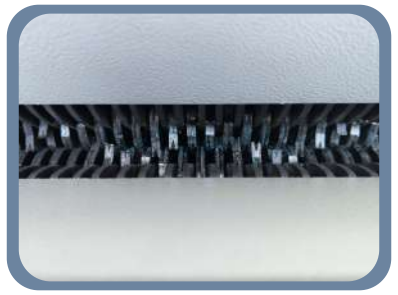
Advantages

- Shred into small partucles.
- Optional shredding particle size with 0.5*0.5 / 1*1 / 2*2 mm² or customized
- To meet higher security requirements for the data destruction.
- Commercial cross-cut shredder is designed for busy professionals.
- Automatically stops and starts for convenience.
- Working capacity more than 5 - 10kg per hour.
- Smart control PLC system.

Crushing size

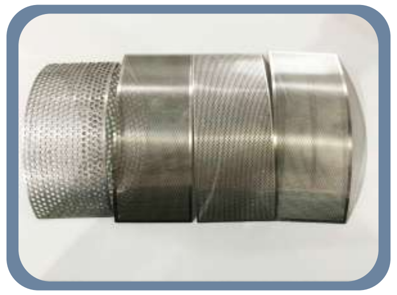


Shredding blade



Electrical cabinet

Screen mesh



Filter system

Specifications

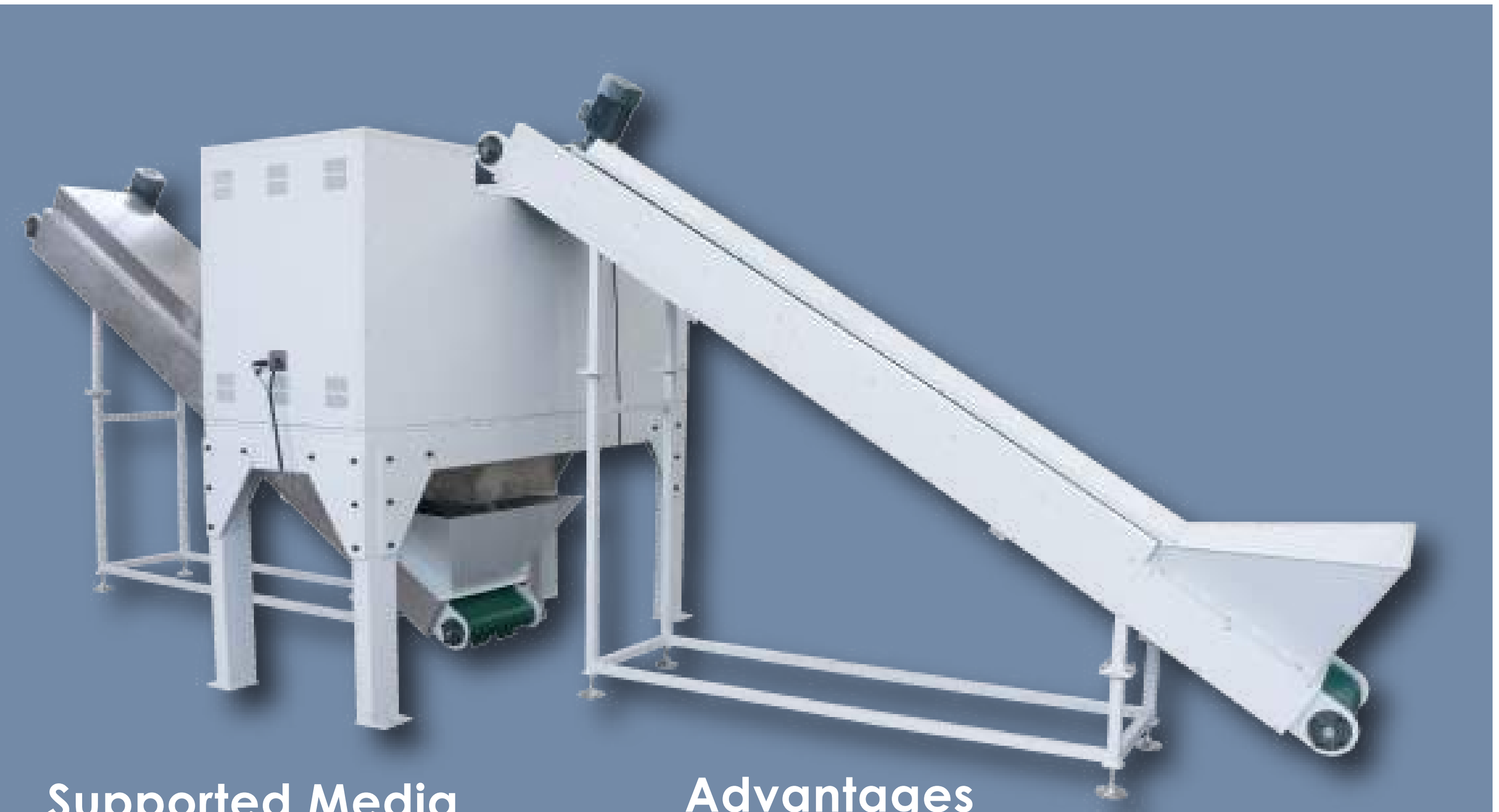
Model	**DEZ-SPD2**
Destruction method	Shredding and Crushing
Crushing materials	SSD chips, memory chips, Card, ID card, SIM Card or small quantity of CD, DVD
Crushing particle size	0.5*0.5 / 1*1 / 2*2mm² or customized
Screen mesh size	Replaceable screen mesh for 1mm，2mm，3mm to reach different particle size in one machine
Crushing capacity	One pcs of Chip each time
Working capacity	5 – 10kg / hr
Feeding Port	130 x 8 mm
Power	3.12 KW, single phase 220V-230V, 13A，50HZ
Waste collection Bin	11L
Machine size:	820(L) x 680(W) x 1070(H)mm
Machine weight	About 216Kg
Characteristic	With Touch screen and PLC control, wooden package, Heavy duty wheels, filter

Data Expert™

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Industrial E-Waste Shredder

Powerful and efficient light e-waste solution for computers and printers.



Supported Media

HDD Computer printer PCB

Shredding particle size

20mm * random or customized

Shredding Capacity

500 kg / hr

Advantages

- Compact and space-saving design for small appliance disposal
- With durable blades and corrosion resistance feature
- Safety and ease of operation
- Process from 1 to 20 tons of materials per hour

Front view

Side view

Back view

Shredding size

Shredding blade

Control panel

Specifications

Model	**DEZ-SPT5**
Shredding method	Dual Motors Two shaft shredder with conveyor
Shredding materials	E waste，3.5 inch HDD，laptop，small printer, PCB ect.
Shredding particle size	20mm width * random or customized
Rotating Speed	13rpm
Blade thickness	20mm * 25 pcs
Shredding chamber box size	500* 455 mm
Shredding capacity	More than 500 kg / hr （more than 800 pcs HDD per hour）
Conveyor inner width	429mm width, With feeding conveyor and discharge conveyor
Total Power	33KW, 3 phase 380v, 50HZ
Shredder and conveyor power	Two motors: 11KW each, two conveyors: 1.5KW each
Machine size	6933.7(L) * 2310(W) * 2622.1(H)mm
Machine weight	About3 300kgs
Characteristic	With electrical control cabinet, planetary gear box, one year warranty

Server Hard Disk Shredder

Powerful server hard disk and desktop shredder.

* Optional Recording System

Application

SSD HDD Tape CD & DVD mobile Floppy

Shredding Particle Size

20*40 - 90mm²

Security Level (DIN 66399)

H-4

Shredding Capacity

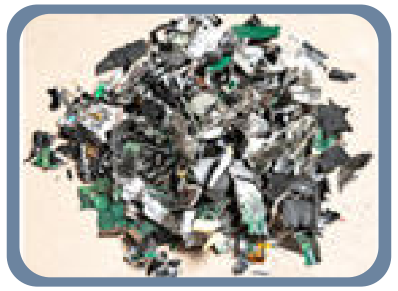
More than 300 pcs / hr

Other Advantages

- Special Hardened Cutting Mechanism
- Auto-Sensor Stop
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning
- Door Safety Auto Sensor System
- Auto Control Reverse System
- Manual Function
- Safety Circuit Breaker
- High Quality Geared Motor

Optional Recording System

Shredding size



Waste collection Bin

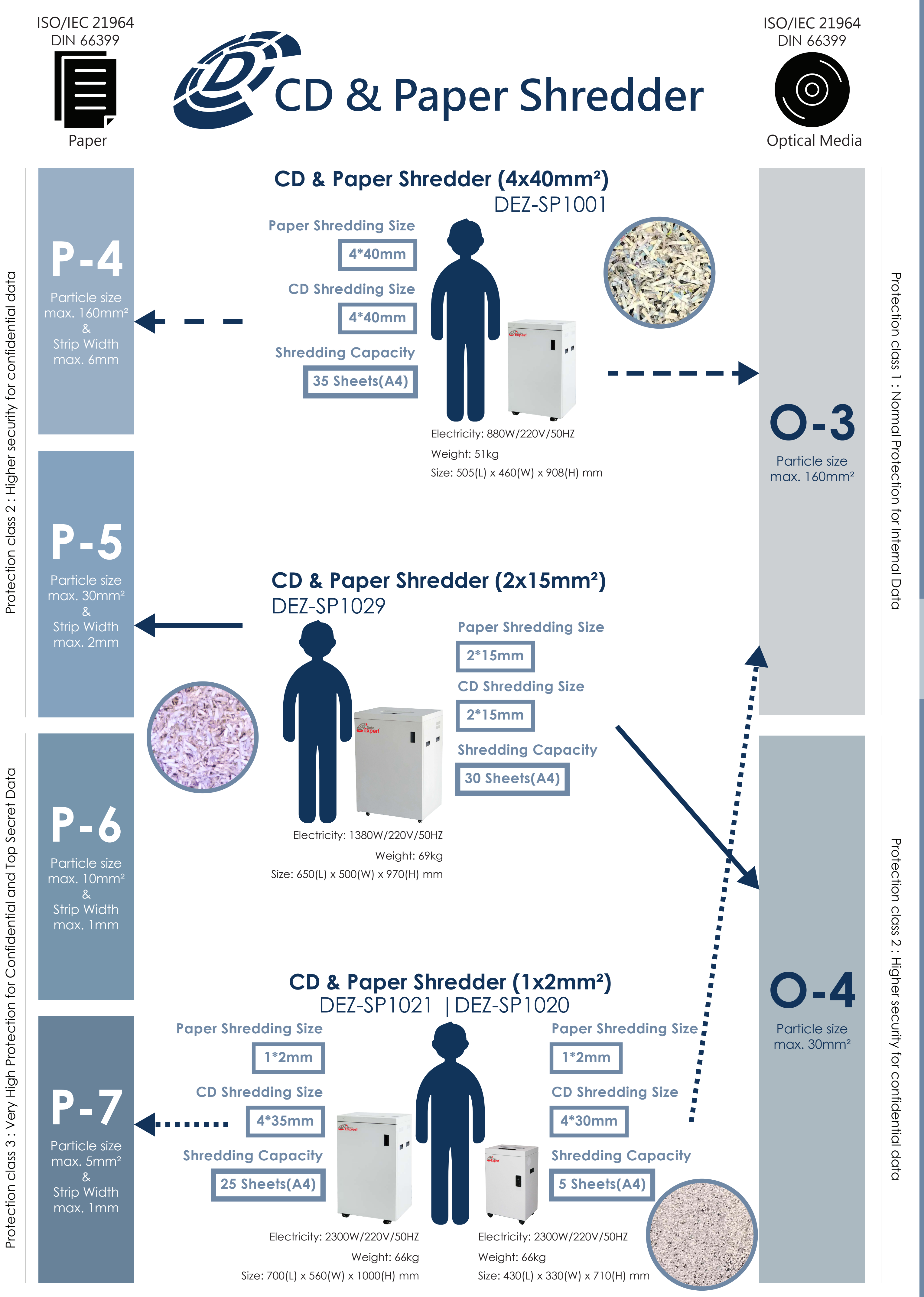
Feeding Conveyor

Model: DED-SHS

Shredding materials	SSD, HDD, mobile phone, CD, floppy disk, USB drive, tape
Shredding particle size	20 * 40 - 90mm²
Shredding capacity	More than 300 pcs / hr
Feeding Conveyor	150mm
Motor Power	5HP
Power	3 Phases, 380V/60Hz
Machine size	800(L) x 1120(W) x 1232(H) mm
Machine weight	780Kg
Optional component	Recording System

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CD & Paper Shredder



ISO/IEC 21964
DIN 66399
Paper
ISO/IEC 21964
DIN 66399
Optical Media
Protection class 2 : Higher security for confidential data
Protection class 3 : Very High Protection for Confidential and Top Secret Data
P-4
Particle size max. 160mm² & Strip Width max. 6mm
P-5
Particle size max. 30mm² & Strip Width max. 2mm
P-6
Particle size max. 10mm² & Strip Width max. 1mm
P-7
Particle size max. 5mm² & Strip Width max. 1mm
O-3
Particle size max. 160mm²
O-4
Particle size max. 30mm²
Protection class 1 : Normal Protection for Internal Data
Protection class 2 : Higher security for confidential data

CD & Paper Shredder (4x40mm²)

DEZ-SP1001

Paper Shredding Size

4*40mm

CD Shredding Size

4*40mm

Shredding Capacity

35 Sheets(A4)

Electricity: 880W/220V/50HZ

Weight: 51kg

Size: 505(L) x 460(W) x 908(H) mm

CD & Paper Shredder (2x15mm²)

DEZ-SP1029

Paper Shredding Size

2*15mm

CD Shredding Size

2*15mm

Shredding Capacity

30 Sheets(A4)

Electricity: 1380W/220V/50HZ

Weight: 69kg

Size: 650(L) x 500(W) x 970(H) mm

CD & Paper Shredder (1x2mm²)

DEZ-SP1021 | DEZ-SP1020

Paper Shredding Size

1*2mm

CD Shredding Size

4*35mm

Shredding Capacity

25 Sheets(A4)

Electricity: 2300W/220V/50HZ

Weight: 66kg

Size: 700(L) x 560(W) x 1000(H) mm

Paper Shredding Size

1*2mm

CD Shredding Size

4*30mm

Shredding Capacity

5 Sheets(A4)

Electricity: 2300W/220V/50HZ

Weight: 66kg

Size: 430(L) x 330(W) x 710(H) mm

Features

- Durable shredding blade system
- Auto reverse function for jamming paper
- Full bin indicator
- Motor overheat indicator
- Sleep mode for saving energy

Specification

Model	SP1020	SP1021	SP1029	SP1001
Paper Shredding Size	1*2mm	1*2mm	2*15mm	4*40mm
CD Shredding Size	4*30mm	4*35mm	2*15mm	4*40mm
Security Level DIN 66399	P-7 /O-5	P-7 /O-3	P-5 / O-4	P-4 /O-3 /F-1
Shredding Capacity (70g/m²)	5 sheets(A4)	15 Sheets（A4)	30 Sheets（A4)	35 Sheets(A4)
Shredding Speed	2.2m /minute	2.2m /minute	2.2m/minutes	2.5m/minutes
Insertion Width	240mm	310mm	310mm	240mm
Bin Capacity	50L	100L	165L	90L
Power / Voltage / Frequency	550W/220V/50HZ	2300W/220V/50HZ	1380W/220V/50HZ	880W/220V/50HZ
Continue Working	30 mins on, 30 mins off	30 mins on, 30 mins off	60 mins on, 30 mins off	More than 2 hrs
Machine Weight	32KGS	66KGS	69KGS	51KGS
Machine Size	430x330x710mm	700x560x1000mm	650x500x970mm	510x460x1045mm

Data Expert Optical Disk Shredder

Cut CD/DVD into 2x2 mm Super-small Particles to Securely Delete Data.

Application

CD & DVD

Shredding Particle Size

2 * 2 mm²

Security Level (DIN 66399)

O-6

Shredding Capacity

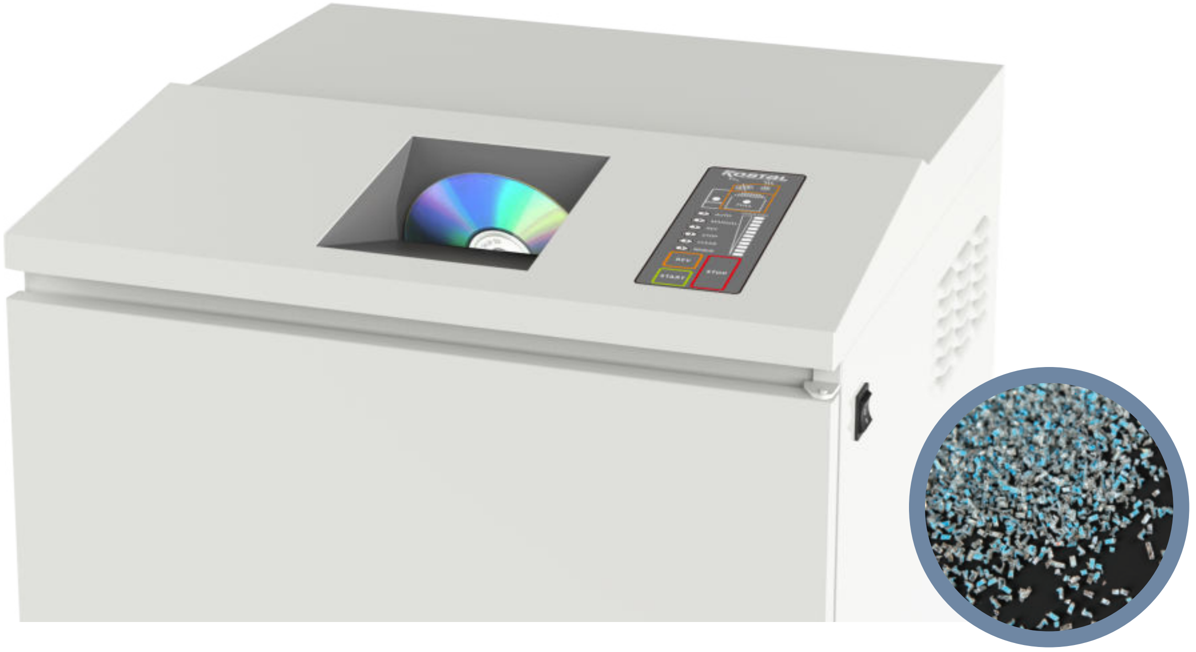
1000 pcs / hr

Advantages

- Special Hardened Cutting Mechanism
- Auto-Sensor Stop
- Auto-Start by Micom System
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning
- Door Safety Auto Sensor System
- Optical Sensor Sensitivity Recovery
- Auto Control Reverse System
- Manual Function
- Safety Circuit Breaker
- Oiler System
- High Quality Geared Motor

Model: DED-CDS2

Shredding materials	CD & DVD
Shredding particle size	2*2 mm²
Entry Port	130 mm (CD/DVD)
Shredding unit per time	1 CD/DVD
Shredding capacity	1000 pcs / hr
Bin Capacity	75L
Motor Power	400W
Power Consumption	1,000W
Power Source	220V / 50Hz
Machine size	500(L) x 500(W) x 850(H) mm
Machine weight	76Kg
Optional Function	Auto Oiler



CD & Paper Shredder

Perfect solution for top secret and classified shredding of paper and optical media.

Application

CD & DVD

Paper

Shredding Particle Size

CD	Paper
1.6 * 4 mm²	1 * 5 mm²

Security Level (DIN 66399)

O-5 P-7

Shredding Capacity

CD	Paper
600 pcs / hr	4,800 pcs / hr

Model: DED-CDPS

Shredding materials	CD & DVD, Paper
Shredding particle size	Paper: 1 * 5 mm² CD: 1.6 * 4 mm²
Entry Port	Paper: 230 mm CD: 125 mm
Shredding unit per time	10-12 pcs 75g paper 1 pc CD/DVD
Shredding capacity	Paper: 4,800 pcs / hr CD: 600 pcs / hr
Bin Capacity	Paper: 52 L CD: 32 L
Power Consumption	2,600W
Power Source	220V / 50Hz
Machine size	670(L) x 550(W) x 1090(H) mm
Machine weight	170 Kg

Advantages

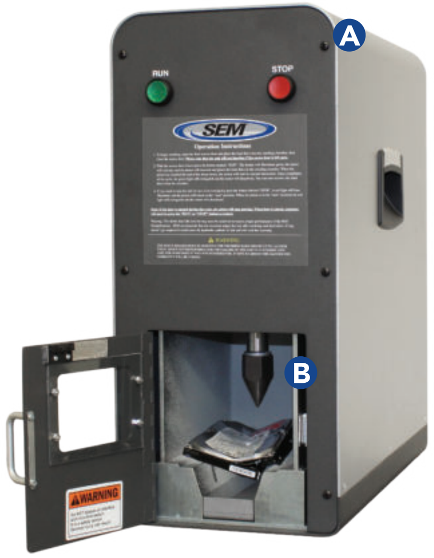
- Special Hardened Cutting Mechanism
- Auto-Sensor Stop
- Auto-Start by Micom System
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning
- Optical Sensor Sensitivity Recovery
- High Quality Geared Motor
- Manual Function
- Auto Control Reverse System
- Safety Circuit Breaker
- Oiler System
- Auto Oiling Alarm
- Door Safety Auto Sensor System

HDD Crusher

Level H-3 Hard Drive Crusher Listed on NSA/CSS EPL for Hard Disk Destruction Devices

Global Leader in High Security Information End-of-Life Solutions for Over 50 Years

Model No. : DED-HDC01



A Easy to use operator interface

B Delivers 12,000 pounds of force

Specifications:

Speed	8 seconds per cycle
NSA Durability Rating	204 drives per hour
HDD Capacity per Cycle — PC / Server	1 HDD up to 1.85" thick
HDD Capacity per Cycle — Notebook	4 standard notebook HDDs or 6 ultra-thin HDDs
Media Dimensions	Up to 5.625"W x 1.85"H x 9"D
Electrical	115/1/60 International voltage available
Power Consumption / HP	7 Amps @120V / 1/3 HP – single phase
Dimensions – HxWxD	22" x 10" x 19"
Weight	115 lbs.
Warranty	1 year non-wear parts/90 days labor

Standard Features:

- Destroys all hard drives regardless of size, format, or type up to 1.85" thick
- **Drives mounted in caddies used in most rack mount server environments can be crushed without having to remove them from the caddies**
- Delivers 12,000 pounds of force, causing catastrophic trauma by bending and boring a hole through the drive while also destroying the data holding platters
- Safety interlocks prevent the unit from operating with the door open
- Made in the USA — TAA compliant

Options and Accessories:

- Spare anvil
- Heavy duty stand
- Dust cover
- Deployment case
- Mobile cart
- Shelf insert for laptop enterprise drives in caddies
- International voltage
- At-site set-up, installation, training
- Preventive maintenance contract
- Extended warranty

Security Engineered Machinery

5 Walkup Drive
Westboro, MA 01581
800.225.9293 I 508.366.1488
info@semshred.com
www.semshred.com

HDD Crusher

Level H-3 Hard Drive Crusher Listed on NSA/CSS EPL for Hard Disk Destruction Devices

CONFIGURATIONS

0101-SSDKIT

Includes an SSD anvil along with wear and press plates that are factory installed in the 0101 crusher to destroy SSD data storage controller boards. Kit includes SSD anvil, wear plate and press plate. Must be ordered at time of purchase, no retrofitting available. Weight: 120 lbs.

0101-DEP

Includes a hard case with custom foam inserts, lockable latches, heavy duty casters, and removable front and rear panels that allow for operation while in case.

Dimensions:	31"H x 15.5"W x 24"D
Weight (empty):	64 lbs.
Weight (with 0101):	184 lbs.

5 Walkup Drive
Westboro, MA 01581
800.225.9293 I 508.366.1488
info@semshred.com
www.semshred.com

DED-OMS01

Level 0-5 Optical Media Shredder
NSA/CSS EPL Listed for CDs

Global Leader in High Security Information
End-of-Life Solutions for Over 50 Years

Specifications:

☒

Media Accepted	Optical media (CDs, DVDs, BDs)
Final Particle Size	2.2mm x 4mm
Hourly Throughput	Up to 1,583 discs
Media Feed Opening	4.72 in. | 12cm
Waste Collection Bin	15 gallon
Dimensions (HxWxD)	40 in. x 21.5 in. x 23.35 in.
Weight	231 lbs.
Electrical	120/1/60 or 220/1/50 Requires dedicated line
Power	1HP
Warranty	1 year non-wear parts/90 days labor

Standard Features:

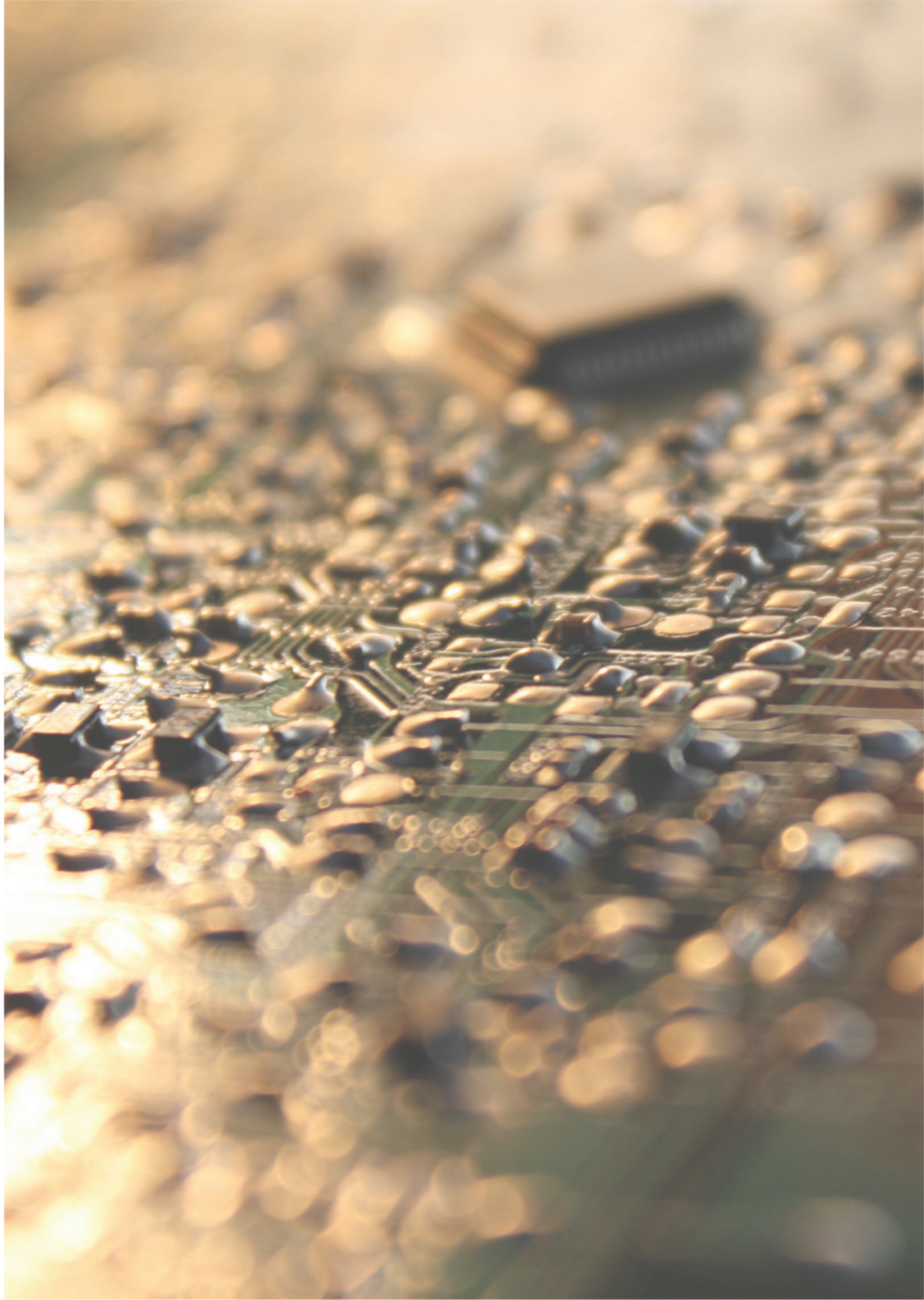
- NSA EPL listed for CD destruction
- Waste bin full/door open indicator with auto stop
- Energy savings mode shuts off power when not in use
- Ideal for other unclassified items such as DVDs, Blu-ray Discs, credit cards and access cards
- TAA compliant
- Includes premium start-up package with two one-gallon oil jugs and 50 anti-static waste collection bags*
- 1-gallon auto oiler prevents the need for manual lubrication*
- 15-gallon collection bin allows for more shredding before changing bags*
- Easy button controls with feed meter and reverse button*
- Anti-static waste bin and anti-static bags*

*Unique to SEM

Options and Accessories:

- Anti-static collection bags
- Oil packs

0201-DEP	
	The deployment case is rugged and incorporates custom filled foam inserts for maximum protection. It is lockable and water-tight with a telescopic handle and wheels.



Technology Makes Possibility

Follow us

Website Facebook YouTube LinkedIn