

IT Asset Disposition

Digital Forensic



Singapore | Hong Kong | Korea | Indonesia | Malaysia | Canada  
Thailand | Philippines | China | Macau



[www.dataexpert.asia](http://www.dataexpert.asia)



[enquiry@dataexpert.asia](mailto:enquiry@dataexpert.asia)



# DataExpert Asia

Company Brochure



# 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, US, Canada and other regions.

Established in    No. of Branch offices    No. of Clients    Our Clients' Countries

**2005**

**12**

**500+**

**15+**

No. of Lab we build

**8**

Dispose Hard Disks Per Year

**1000000+**

Recover Devices Successfully

**500+**

# Our Network



# Milestone

Founded DataExpert.

Built a class-100 clean room.

Achieved ISO27001 certification.

Launched 1st generation DataExpert forensic workstations.

Established Shenzhen branch office.

Developed first data recovery training in Hong Kong.

GMDSOFT's Exclusive Partner in Hong Kong

NovaTrace's Exclusive Partner

2005

2006

2008

2009

2010

2011

2012

2014

2015

2016

2020

2021

2022

2025

2026

Atola's exclusive Asia partner.

ADC's exclusive Asia partner.

Launched first self-developed hard disk destroyer.

Established Thailand branch office.

Constructed first automated digital forensic lab(DFL) in Hong Kong.

Completed our 1st DFL for law enforcement: Jakarta Police Academy.

Established South Korea and Canada branch offices.

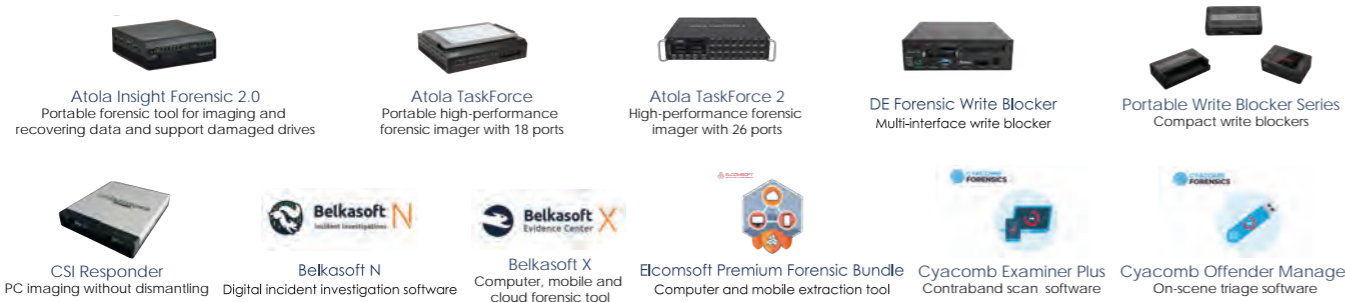
## Digital Forensic Products

### 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, Ecomsoft Premium Forensic Bundle Computer and mobile extraction tool, Cyacomb Examiner Plus Contraband scan software, Cyacomb Offender Manager On-scene triage software

### Mobile Forensic



GMSOFT MD-NEXT Data extraction software, GMSOFT MD-RED Data analysis software, GMSOFT 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, Ecomsoft Mobile Forensic Bundle Acquisition, decryption and analysis software, Cyacomb Mobile Device Triage Triage software for mobile devices

### macOS Forensic



Sumuri RECON ITR macOS Imaging tool, Sumuri RECON LAB Advanced Mac analysis tool

### Data Recovery



ruSolut VNR Chip-off data recovery and analysis solution, GMSOFT MD-READER Chip-off memory extraction hardware, Regen-i Rework Station BGA rework station

### IOT Forensic Solution



GMSOFT MD-DRONE Drone extraction and analysis software, GMSOFT MD-VIDEO AI Video extraction and analysis software, GMSOFT MD-CLOUD Cloud extraction and analysis software, BTS Tracker Cell tower analyzer, MOBiledit Smartwatch Forensics Smartwatch extraction kit

### 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 simultaneously

### 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.





**Professional Services**

Experienced and professional service for finding the electronic evidence.

## Our advantages

- ✓ Over 20 years in digital forensic services
- ✓ 1<sup>st</sup> 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:



## 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

## 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
- HancowITH 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)

## Forensics Laboratory & Class 100 Cleanroom Based Data Recovery Service.



### 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.



### 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

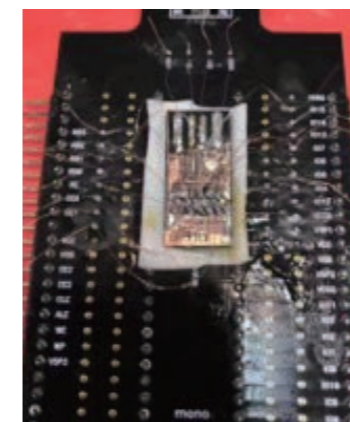
### Your data is unparalleled safe in DataExpert

- 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.



### 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.



## 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](mailto: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.

Build your own digital forensic laboratory (DFL).



## Why Digital Forensic Laboratory is Needed?

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.



Advantages of DFL

## 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



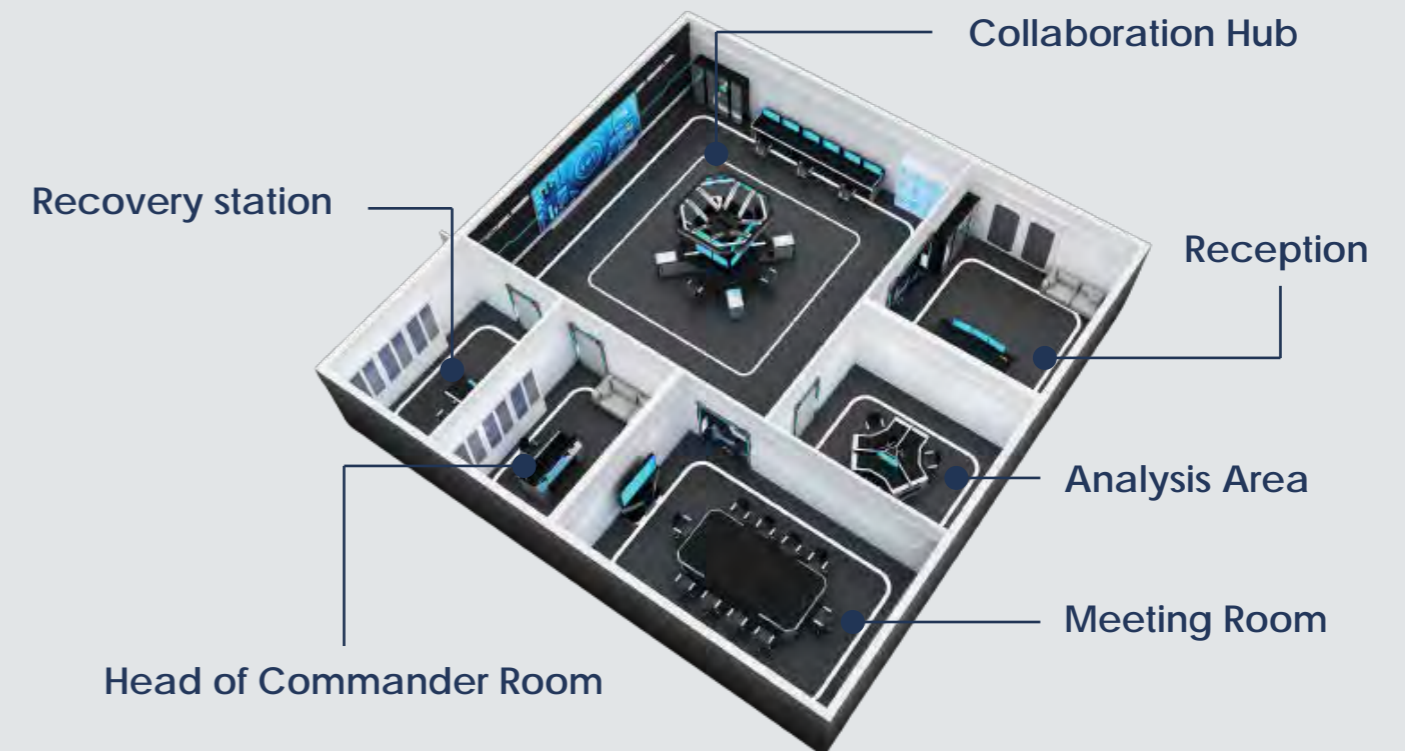
Design



Construction



Accreditation





Reception



Meeting Room



Collaboration Hub



Head of Commander Room



Analysis Area



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 (Desktop 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



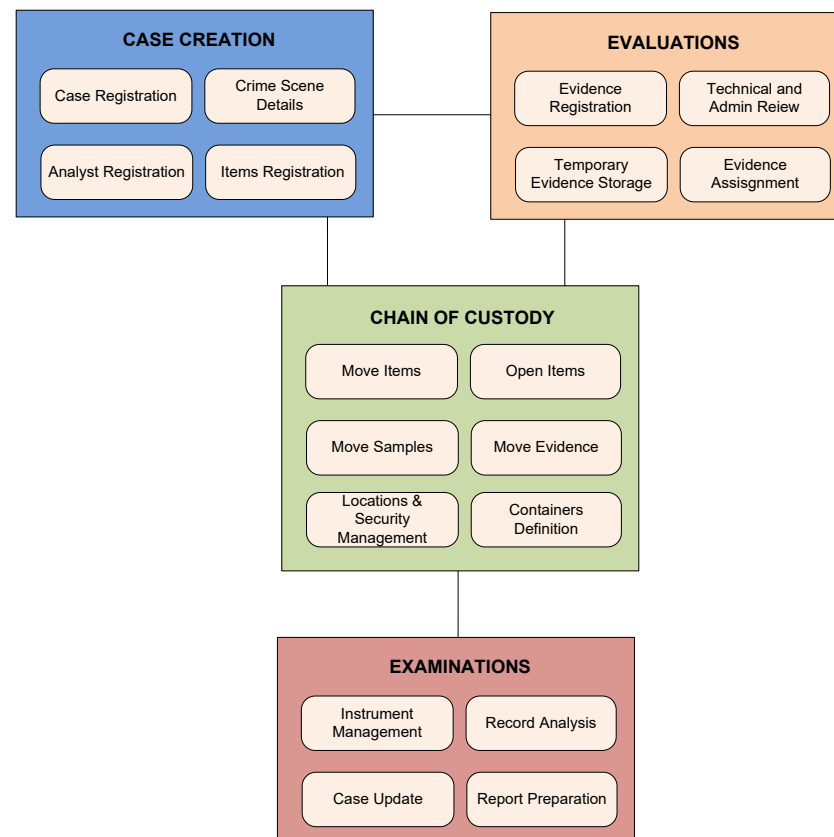
**Display Screen**  
DE1901-ES  
L1625\*W580\*H2000

## 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



## Forensic FLIMS Lab Information Management System



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

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

### 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.

## FORENSIC LIMS THAT PROVIDES A TOTAL END TO END SOLUTION.

### 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 International 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



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

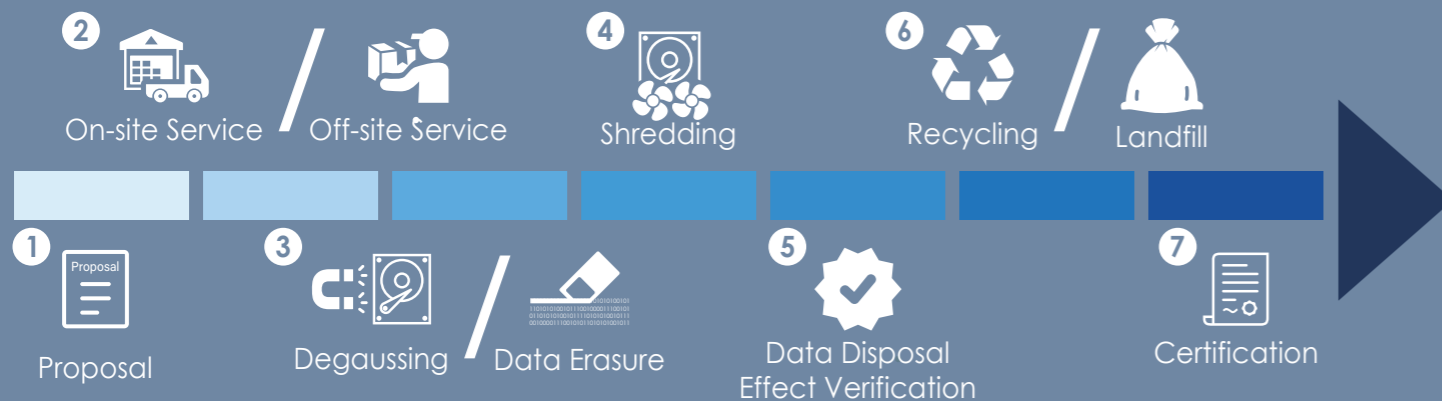


### Our Promise

### 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



### 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.



### 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



### Document and Certificates

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



malicious virus; Install:  
Boot sector was successfully installed

Digital Forensic and  
Incident Response

# Forensic Workstation





## 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



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.

Build-in forensic imaging software

Phone Connection Panel

### Auto detect connected devices' information

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

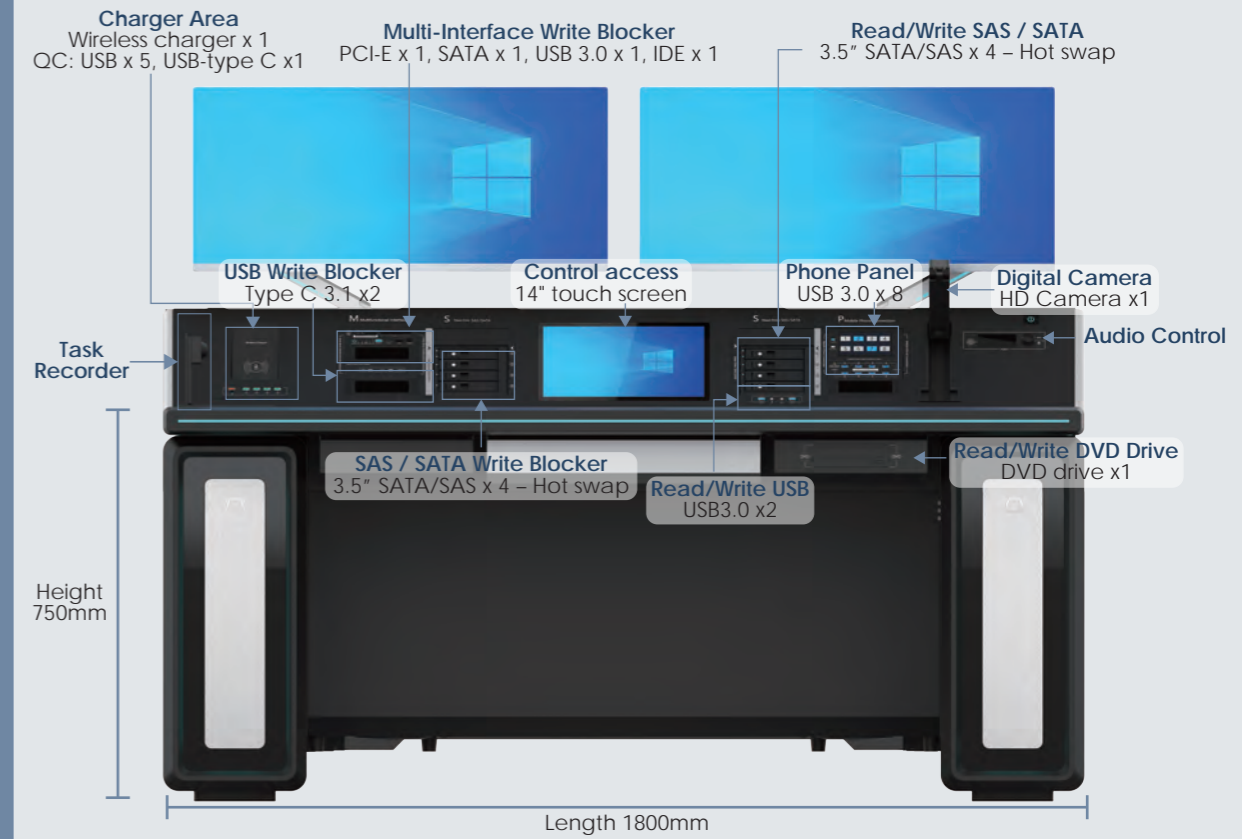
### Multiple phone connections for multitasking

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
<b>Write-blocker Interfaces</b>	
Multi interface Write blocker <sup>^</sup>	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
<b>Read/Write Interfaces</b>	
Read/Write Interface	USB3.0 x 2 3.5" SATA/SAS x 4 - Hot swap
Phone Panel	USB 3.0 x 8 port (power independent)
<b>Others</b>	
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 / Hancome MD-Series / Mobeidit 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)

<sup>^</sup> Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.

\* Customized Configuration available. Powered by DataExpert.

\* Specifications are subject to change without notice.

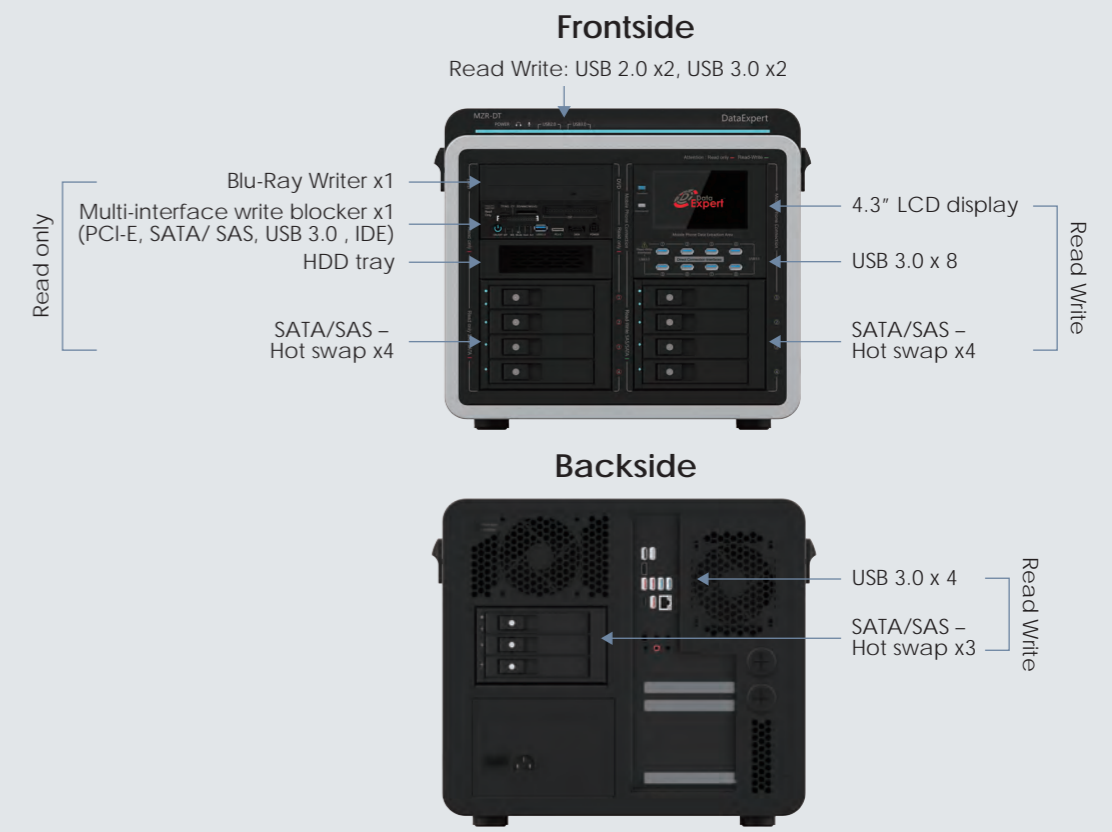


# Cyber MZR-DT

All-inclusive forensic workstation for rapid analysis of artifacts.



## Write-Blocker & Read/Write Interfaces



## Specification

Model	Cyber DZR-DT
<b>System Configuration</b>	
OS	Microsoft Windows 11 Pro 64 bit
CPU	Intel I9-12900K (16 core 24 Processor 3.90GHz-5.1GHz)
Chipset	Intel Z790 Chipset
Internal Memory	64GB DDR4 UDIMM non-ECC RAM Memory (2X32GB)
Storage system	ONE (1) 1TB 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	Nvidia RTX 3060 12GB DDR6 Video Card
DVD Drive	Blu-Ray Writer
Power Supply System	1200 Watt Modular Power
<b>Dashboard Configuration</b>	
Write Blocker (Read Only)	Hot Swap Tool Free SAS/SATA 12Gb Removable Hard Drive Bays *4 DataExpert Writeblocker with PCI-E, SATA/ SAS, USB 3.0, IDE^
Read/ Write	Hot Swap Tool Free SAS/SATA 12Gb Removable Hard Drive Bays *4 At rear: USB 3.0 *4 , at top: USB 2.0 *2 + USB 3.0 *2, front panel: USB3.0 *8
Phone Connection Panel	4.3" LCD display with 8 phone connected or disconnected status panel
<b>Others</b>	
	Intel® I219-V Gigabit Ethernet port *1 Realtek RTL8125-CG 2.5G Ethernet port *1 7.1 Channel High Def Audio-Back Munted PCI-E 3.0 x16 *3 M.2 Interface: PCI-E 3.0 x4 (Form Factor: 2280, 22110) *2 Keyboard and Mouse-Wireless
<b>Forensics Software</b>	
Build-in software	D-Box Forensic Imaging Software
Optional Computer Forensics	Belkasoft Evidence X
Optional Phone Forensic	GMDSOFT MD-Series / Mobiledit Forensic Pro
Warranty	THREE years limited warranty
Dimension	530*423*362mm
Weight	40KG

^ Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.

\* Customized Configuration available. Powered by DataExpert.

\* Specifications are subject to change without notice.

## 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

### 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.

## Build-in forensic imaging software



4 main functions of software

## 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.



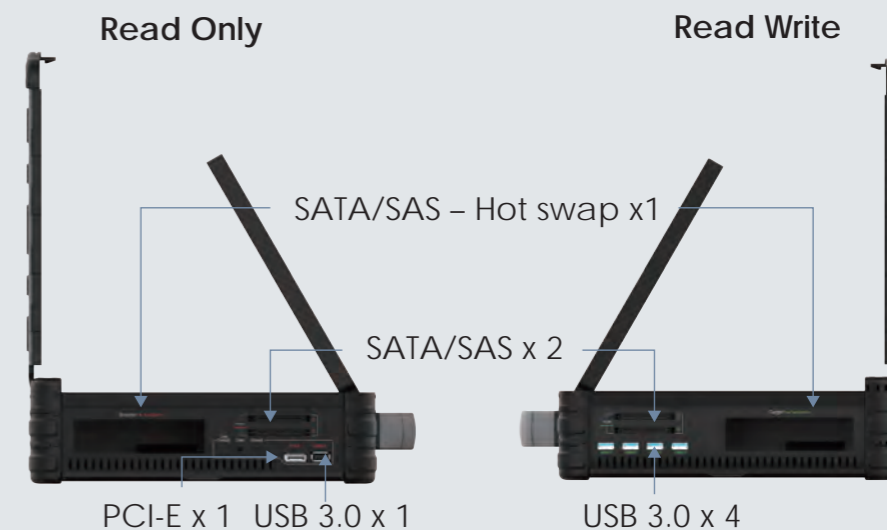
Phone Connection Panel



## Forensic Cube V4

All you need for on-scene investigation.

### Write-Blocker & Read/Write Interfaces



Keyboardless version



Keyboard version

### Versions

### 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.

### 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

#### 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.

### Build-in forensic imaging software

### 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



## Tri-Fold Workstation

Minimize space, maximize efficiency for your investigations.

### Write-Blocker & Read/Write Interfaces



### Different Perspectives

### Specification

Model	MZR-TF
OS	Windows 10/11 64 Bit Professional (Eng)
CPU	Intel i9-12900T (16 Core; 24 thread; 1.4GHz max 4.9GHz)
Memory	32GB (16GB x 2) DDR4 3200MHz (upgradeable to 64GB)
Hard Drive	2TB M.2 NVME SSD 4TB SATA SSD (optional)
Write-Blocker Interfaces	PCI-E x 1 USB 3.0 x 1 SATA/SAS x 2
Read/Write Interface	USB 3.0 x 8 SATA/SAS x 2
Others Interface	Bluetooth 4.0 / WiFi Bulit-in Mechanic Keyboard and mouse pad Audio in/out RJ45 Ethernet Port
Display	Trifold 14 inch FHD Display with 1920 x 1080 resolution
Dimension	360 x 310 x 108 mm (L x W x H)
Accessories	13A AC power Cable 180W DC power source Carrying Case

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

### Hardware specifically designed for forensic

#### Forensically sound design

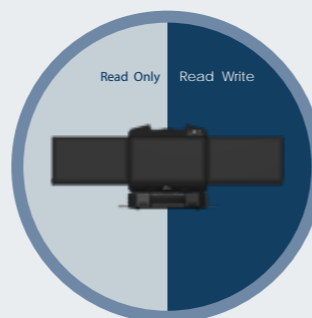
Easy to distinguish write blocker & read write area to reduce the human error.

#### 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

#### 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.

### Build-in forensic imaging software

### Specifically designed for on-scene

#### Tri-fold monitor with a compact design

The tri-fold monitor's compact design saves space while delivering versatile multi-screen productivity.

#### Dedicated carrying case

The carry case offers excellent protection for Forensic Cube v5, and its internal compartment is designed to conveniently store accessories.



Folded view



# Forensic Laptop

High performance laptops design for field or lab forensic investigation.



## Specification

Model	Forensic Laptop
Operating System	Windows 11 Pro 64-bit
CPU	Intel Core Ultra 9 275HX ( Max Turbo boost up to 5.40 GHz ), 8 P-cores & 16 E-cores / 24 threads
Internal Memory	128GB Dual Channel DDR5 SDRAM @ 4000MHz (2x64GB)
GPU	NVIDIA GeForce RTX 5080 (16GB GDDR7 VRAM)
Storage system	2TB M.2 NVMe SSD for the Operating System 2TB M.2 NVMe SSD for Evidence Drive 2TB M.2 NVMe SSD for Temp Files 2TB M.2 NVMe SSD for Storage
Display	18" QHD+ (2560x1600) 240Hz WVA, 72% DCI-P3, Matte
Dimensions	39 x 28 x 2.5 cm
Weight	3.5 kg
Warranty	3-Year Limited Warranty

\* Customized Configuration available. Powered by DataExpert.

\* Specifications are subject to change without notice.



# Forensics Write Blocker

Integrated write-blocker supports 7 storage media types.



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
<b>Interface Front Panel</b>	
PCI-E	One PCIe Custom data + Power 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
<b>Switch</b>	
DIP Switch	Two position DIP Switch configures Write Protect (WP) or Write Blocker (WB)
<b>Other feature</b>	
Status LED	4 LEDs: Host (Detect), Activity(Act), Write-Block(Disk), Read-Write (RO)
<b>Host/Computer Interface Compatibility</b>	
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	148 x 81 x 43mm (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.



## Specification



Write Blocker M



Write Blocker P



Write Blocker U

## 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

Model	U2MS	U2PS	U2US
<b>Write-Blocker Interfaces</b>			
SATA	✓	✓	X
USB 3.0/2.0/1.0	✓	X	✓
PCIe (M.2)	✓	✓ (Optional Add-on)	X
PCIe (U.2)	X	✓	X
IDE	X	X	X
Memory Card	X	X	✓ (TF)
SAS	X	X	X
Mac Task Disk Mode (Type-C/Thunderbolt 3)	✓	X	✓
<b>Features</b>			
PCIe NVME Protocol	✓	✓	X
PCIe AHCI Protocol	✓	X	X
HPA Identification and Read	✓	X	X
Mac Task Disk Mode (Type-C/Thunderbolt 3)	✓	X	✓
<b>Performance Parameter</b>			
Max. Data Transfer Speed	PCIe/SATA/USB: 10GB/min	PCIe: 46.87GB/min SATA: 26.36GB/min	USB: 14.6GB/min TF Card: 2.9GB/min
Connection Port	USB 3.0	USB 3.2	USB 3.0
<b>Mode</b>			
Read-Only Mode	✓	✓	✓
Virtual Writing Mode	✓	X	✓
<b>Other</b>			
Screen	X	X	✓
Host Connection	SuperSpeed USB3.0 (USB 3.2 Gen 1)	USB3.2	SuperSpeed USB3.0 (USB 3.2 Gen 1)
Power	DC 12V 4A	DC 12V 4A	DC 5V 3A
Size (W x D x H)	140.6*80.6*26.6mm	121*73*25mm	103.6*68.2*29.1mm



**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

**THE POWER AND VERSATILITY OF TALINO - ACCEPT NO SUBSTITUTES**



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.

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!

# Computer Forensic

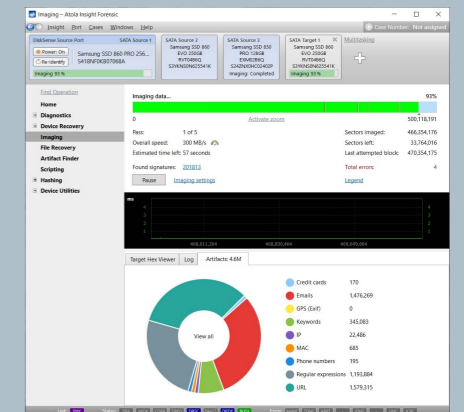


The first and only forensic data acquisition tool that works with both good and damaged media.



## 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



## 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



## 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), NVMe and M.2 PCIe SSDs
- Built-in hardware write blocker for all source ports

## Workflow



# Atola TECHNOLOGY Product comparison



	Atola TaskForce 2	Atola TaskForce	Atola Insight Forensic
<b>Imaging</b>			
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
<b>Hardware unit</b>			
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	✓		
<b>Other features</b>			
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)

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



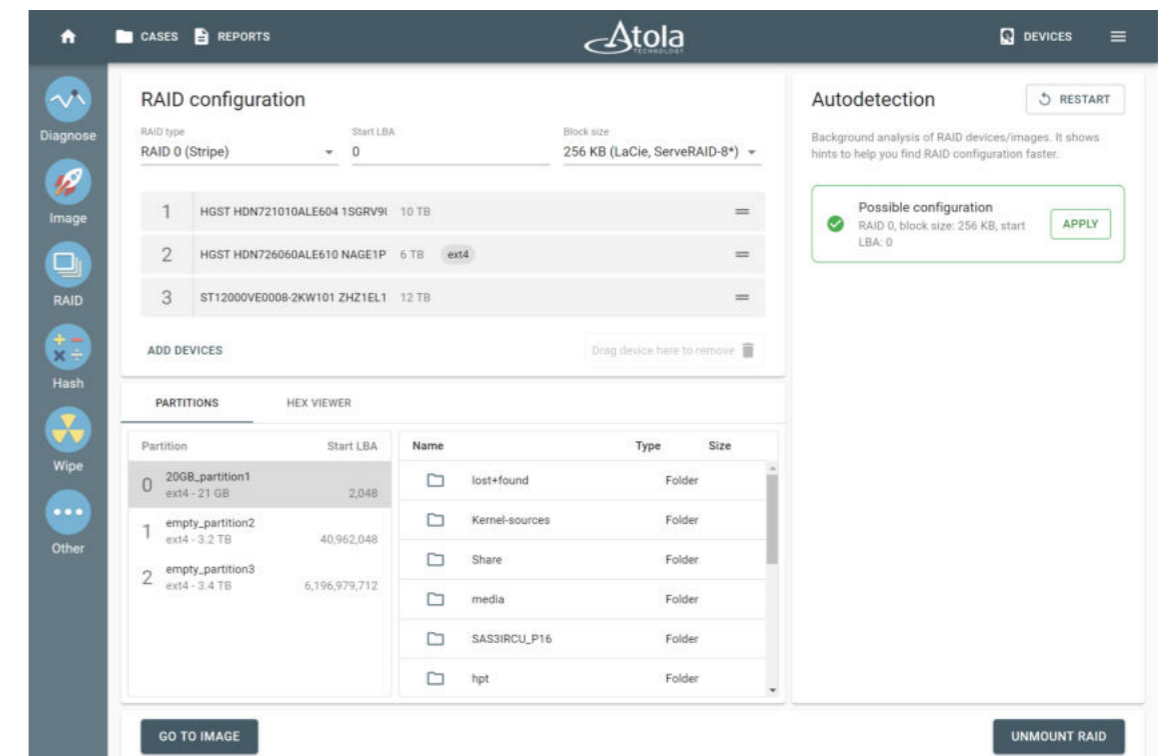
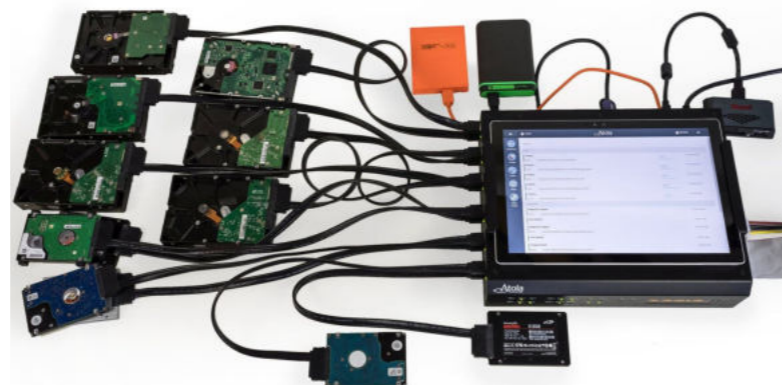
## RAID configuration autodetection and imaging

- RAID identification by data parsing 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

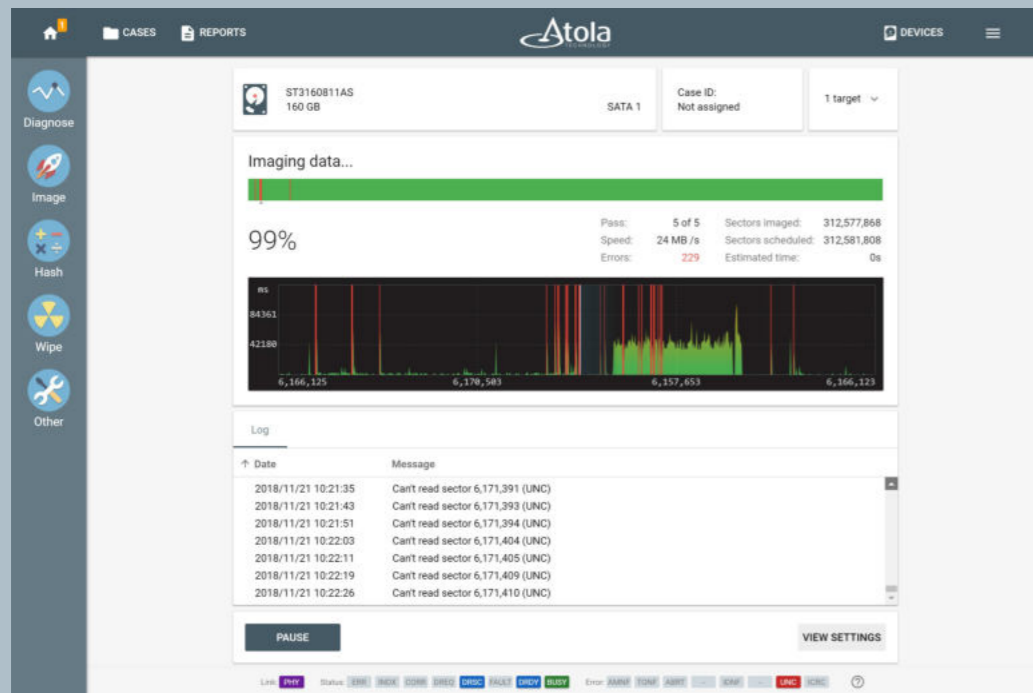
### Forensic Imaging

- 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



## 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



## Two ways to manage TaskForce



10Gb Ethernet network



Standalone mode



## Supported Drives

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

### (Optional) With extension modules:

- M.2 NVMe/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/>

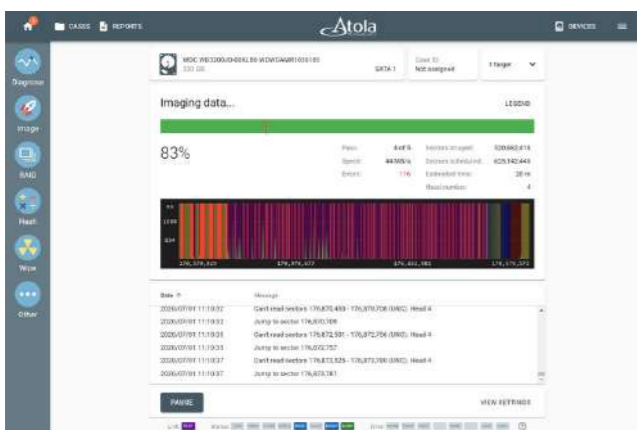
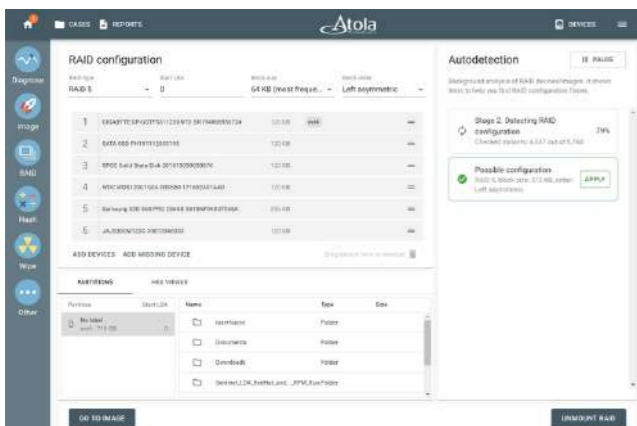
# Atola TaskForce 2



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

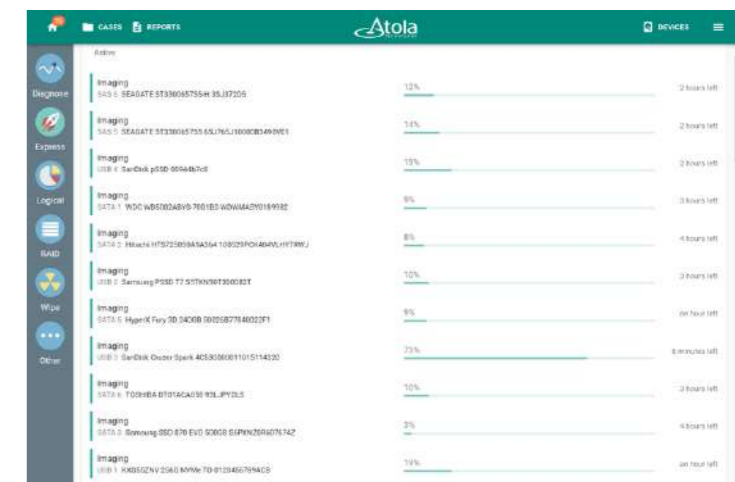
## Other features

- **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





# 711 MagicBox



## Forensically-Sound Solution

- ✓ **No Disassembly Required**  
Extracts recovery key without opening
- ✓ **Offline Operation**  
No internet connection needed; fully DFL-compliant
- ✓ **Non-Brute-Force Method:**  
Saves significant time and resources
- ✓ **Forensically Sound:**  
Leaves storage data untouched and intact
- ✓ **Plaintext Key Extraction:**  
Recovers the full recovery key in readable

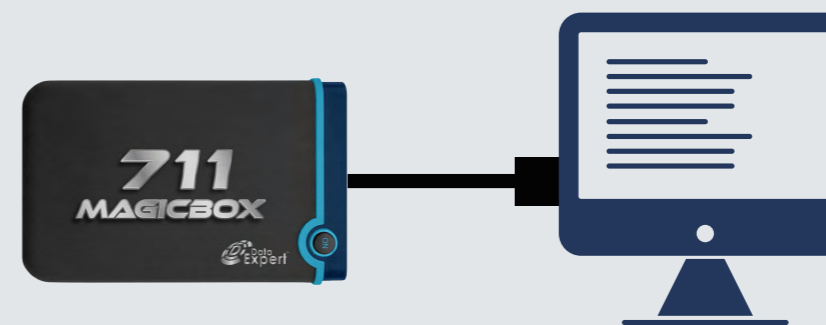
## Pre-Scan Phrase



### Pre-Scan Devices

1. Insert the "711 Pre-Scan USB Drive" into the target PC.
2. Boot the PC from the USB drive (external boot).
3. Run the diagnostic program from the USB.
4. Verify compatibility:  
The program displays whether "711 MagicBox" is supported on the PC.

## Retrieval Phrase



### Extract Devices

1. Connect the "711 MagicBox" to the target PC by LAN cable.
2. Boot the PC from the "711 MagicBox" (external boot).
3. Click "One-Click Extraction" in the "711 MagicBox" interface.
4. Key is shown in the PC screen.

## Extraction Procedure

### Forensically-Sound Solution

Non-Disassembly    Non Brute-Force    Internet-Free

### Suitable for On-Scene

Portable Hardwares

### High Compatibility

Compatible to Various Window PC

### Easy to Use

Pre-Scan Function    One-Click Extraction    Quick Extraction

## Compatible PCs



- Most PCs
- Windows 10/11 systems
- Protected with TPM + BitLocker
- Manufactured before 2025

\* This product is intended solely for use by law enforcement agencies.

RECON

ITR

SUMURI



## A complete rebuild for modern Mac forensics

**RECON ITR** v26.0 has been rebuilt from the ground up in native Swift, designed specifically for macOS using Apple frameworks. This is not an update—it is a new application built to acquire and triage modern Mac systems with accuracy and reliability.

**RECON ITR** supports Apple Silicon systems including M1 through M5, as well as the latest MacBook Neo (A18), along with Intel and T2-based Macs. Built to work with macOS—not against it—it preserves critical Apple-native data structures and metadata during acquisition.

### Key Capabilities

- Native macOS architecture using Apple frameworks
- Acquisition and triage of live systems and Target Disk Mode devices
- Support for Apple Silicon, Intel, and T2 Macs
- Integrated search, timeline, and reporting
- Preservation of Apple Extended Metadata
- Flexible imaging options through **RECON ITR** and included **PALADIN PRO**
- Integrated search, timeline, and reporting

### Triage and Analysis

**RECON ITR** includes 101 macOS triage plugins designed to extract and parse key artifacts, along with 456 iOS artifacts via iLEAPP integration. Results are returned as structured, actionable data—not raw files—allowing examiners to quickly identify relevant evidence.

### Reporting

Global Search, Global Timeline, and Global Report enable examiners to locate artifacts, build timelines, and generate clear reports directly on-site.

### Open and Verifiable

All images are created using Apple-native or open formats and can be independently verified using standard tools. No proprietary lock-in. Evidence remains accessible and defensible.

RECON

ITR



### Flexible Imaging Options

**RECON ITR**, together with the included **PALADIN PRO**, provides support for Apple-native and industry-standard imaging formats, including DMG, SparselImage, ASIF, E01/EX01, DD, and logical acquisition formats—giving examiners the flexibility to choose the right approach for each case.

### Flexible Imaging Options

Built natively on macOS, **RECON ITR** correctly captures:

- Apple Extended Attributes
- Spotlight metadata
- Resource forks
- File system structure

### Time Machine Local Snapshots

Access and triage Time Machine local snapshots to analyze point-in-time system states maintained by macOS.

### Volatile Data Collection

Capture system state, running processes, network connections, and other volatile artifacts through structured triage plugins.

### BootCamp and iOS Support

Triage BootCamp partitions and iOS backups alongside macOS data for a more complete investigation.

### Independent Validation

Images can be verified using standard tools on any Mac system, supporting defensible forensic workflows.

### Included: **PALADIN PRO**

Every **RECON ITR** license includes **PALADIN PRO**, a bootable forensic environment for imaging and triage across Windows, Linux, servers, and RAID systems.

### **PALADIN PRO** provides:

- Physical and logical imaging
- Built-in write protection
- BitLocker decryption support
- Network-based imaging (SMB/NFS)
- Integrated open-source forensic tools

This extends **RECON ITR** beyond macOS, allowing examiners to handle multiple platforms using a single solution.

### 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



**Modern Forensic Analysis  
built for macOS**

**RECON LAB** is a forensic analysis platform designed to process and examine digital evidence across multiple operating systems using native macOS architecture.

**Three-Stage Analysis Workflow**

- 1.) Automated Analysis  
Processes artifacts from macOS, Windows, iOS, Android, and cloud sources.
- 2.) Assisted Analysis  
Provides tools for examining SQLite databases, plists, registry data, and raw files.
- 3.) Reporting  
Generates structured reports using timeline-based and storyboard-style outputs.

-  Native to macOS
-  Automated artifact parsing
-  Timeline analysis
-  Structured reporting
-  Multi-platform support

**RECON LAB** is designed to help both new and experienced examiners move from data collection to actionable findings efficiently.



**Native macOS Processing**

Ensures accurate handling of Apple timestamps, metadata, and file structures.

**Automated Artifact Processing**

Parses thousands of artifacts across supported platforms with minimal manual effort.

**Advanced Data Review**

- Includes viewers for:
- SQLite databases
  - Property lists
  - Windows Registry
  - Raw data

**Timeline and Reporting**

Sequential processing enables clear timeline reconstruction and consistent reporting.

**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](mailto: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 Silicon) 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 3.2 Gen2 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.



# CSI RESPONDER

## Key Features

### 1 Non-dismantling Imaging

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

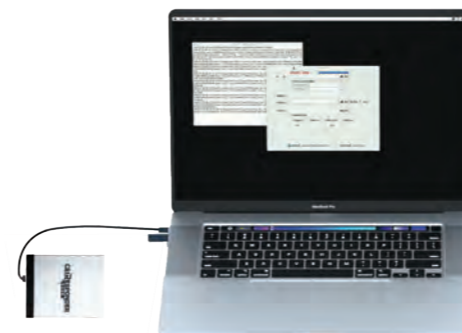
1. Compatible with over 95% of laptops, desktop computers, and Apple computers in the market with both Intel and ARM architectures.
2. Built-in disk offline write protection function in the forensic system, enabling non-dismantling read-only acquisition of the source disk image.
3. Multi-channel parallel 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.





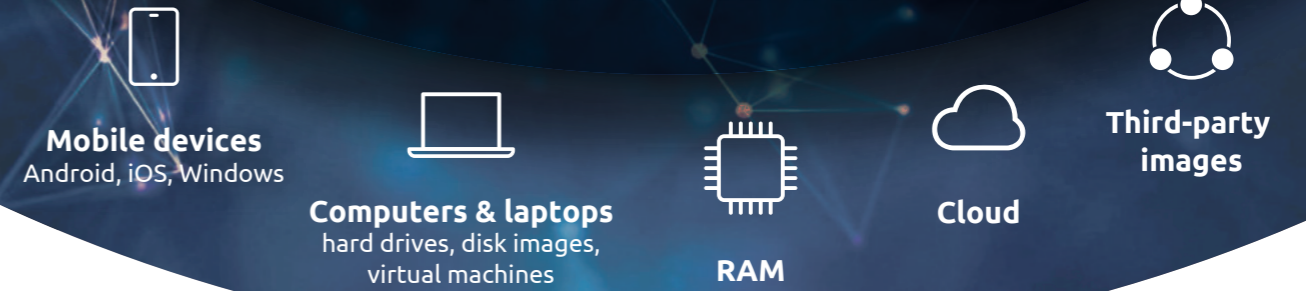
**RELIABLE END-TO-END  
SOLUTION TO ACCELERATE  
DIGITAL FORENSICS AND  
INCIDENT RESPONSE  
INVESTIGATIONS**



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



## 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



Learn more  
[belkasoft.com/n](https://belkasoft.com/n)

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



## 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.

#### 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.



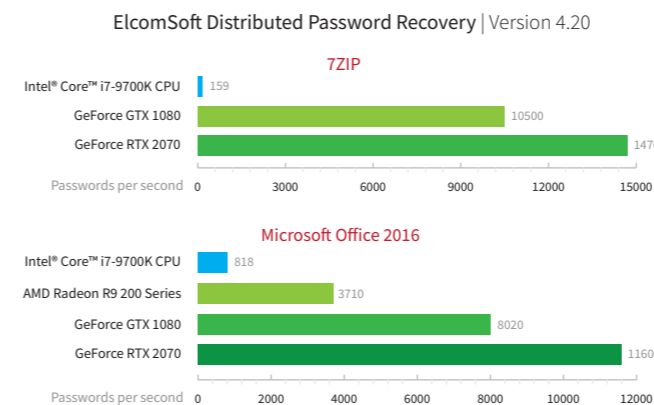
#### Patented technologies

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**  
DESKTOP, MOBILE & CLOUD FORENSICS

[www.elcomsoft.com](http://www.elcomsoft.com)  
[blog.elcomsoft.com](http://blog.elcomsoft.com)  
[sales@elcomsoft.com](mailto:sales@elcomsoft.com)



More information at [www.elcomsoft.com/epfb.html](http://www.elcomsoft.com/epfb.html)

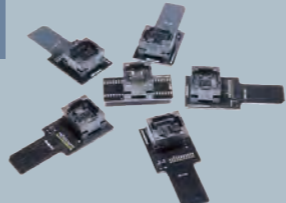

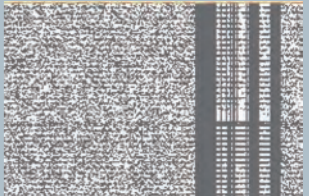

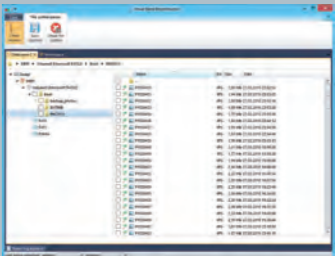
Chip-off Data Recovery & Digital Forensic analysis of broken flash storage devices.



### Application

	Firmware <del>X</del>
Physical Damage	Firmware Failure
	
Electrical Damage	Thermal Damage
	Recognize <del>X</del>
Analysis "non-addressed areas"	Non-recognizable disk



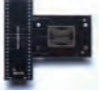
### Workflow

-  Put the chip into the adapter
-  Connect the adapter to the reader and press "Read memory chips."
-  Binary dump file of physical image is produced
-  Rearrange the physical NAND blocks into the logical block by using VNR software
-  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
 <p>TSOP48 BGA100</p> <p>LGA52 BGA152/13</p> <p>MONOLITH</p>	 <p>BGA152 BGA100</p> <p>BGA132 BGA107</p> <p>BGA137 TSOP48 WIDE</p> <p>LGA60 (FOR TH58TF1DFKLAHV AND ALIKE)</p>	 <p>BGA162 EMMC BGA169 EMMC 10x11</p> <p>BGA169 EMMC 11.5x13 BGA169 EMMC 12x16</p> <p>BGA169 EMMC 12x18 BGA169 EMMC 14x18</p> <p>BGA186 EMMC BGA221 EMMC</p>	 <p>MICROSD 3x7 PADS SANDISK MONOSD SANDISK MONOUFD</p> <p>MONOUFD 6x6 &amp; 3x7 PADS MONOSD 4x10 PADS MONOSD 3x13 PADS</p> <p>SAMSUNG MICROSD MICROSD 6x4 PADS BGA316 &amp; BGA272</p>

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



*“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**



**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.

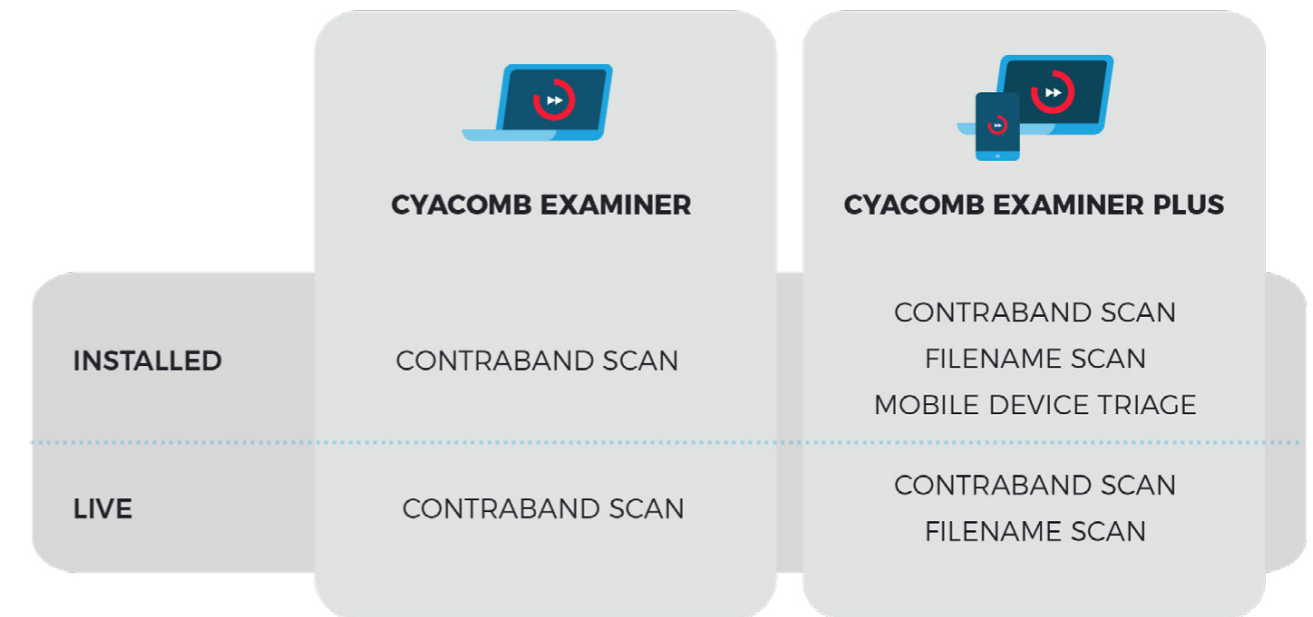
### With Cyacomb Examiner Plus, you will get:

- ✓ 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

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.



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.

# Cyacomb Offender Manager

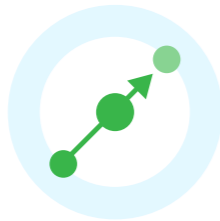
Empowering frontline investigators to easily detect illegal content and produce clear, easy-to-understand results in seconds

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 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 independently.

### SECURE STORAGE

All files are stored on your computer and can be accessed 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.

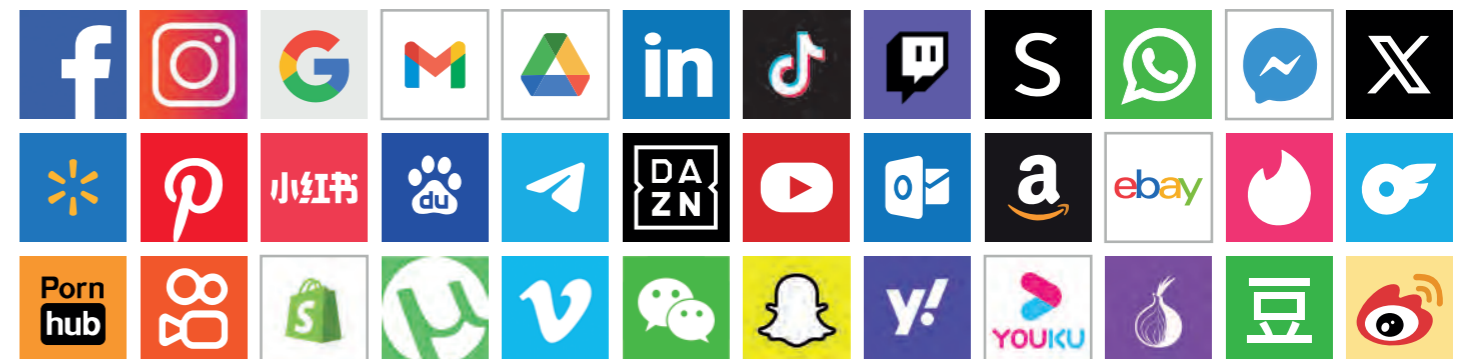
### USED BY LAW ENFORCEMENT

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 customizable 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 independent 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.

## 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.



## Compliance



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

## Our licenses



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.



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.



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.

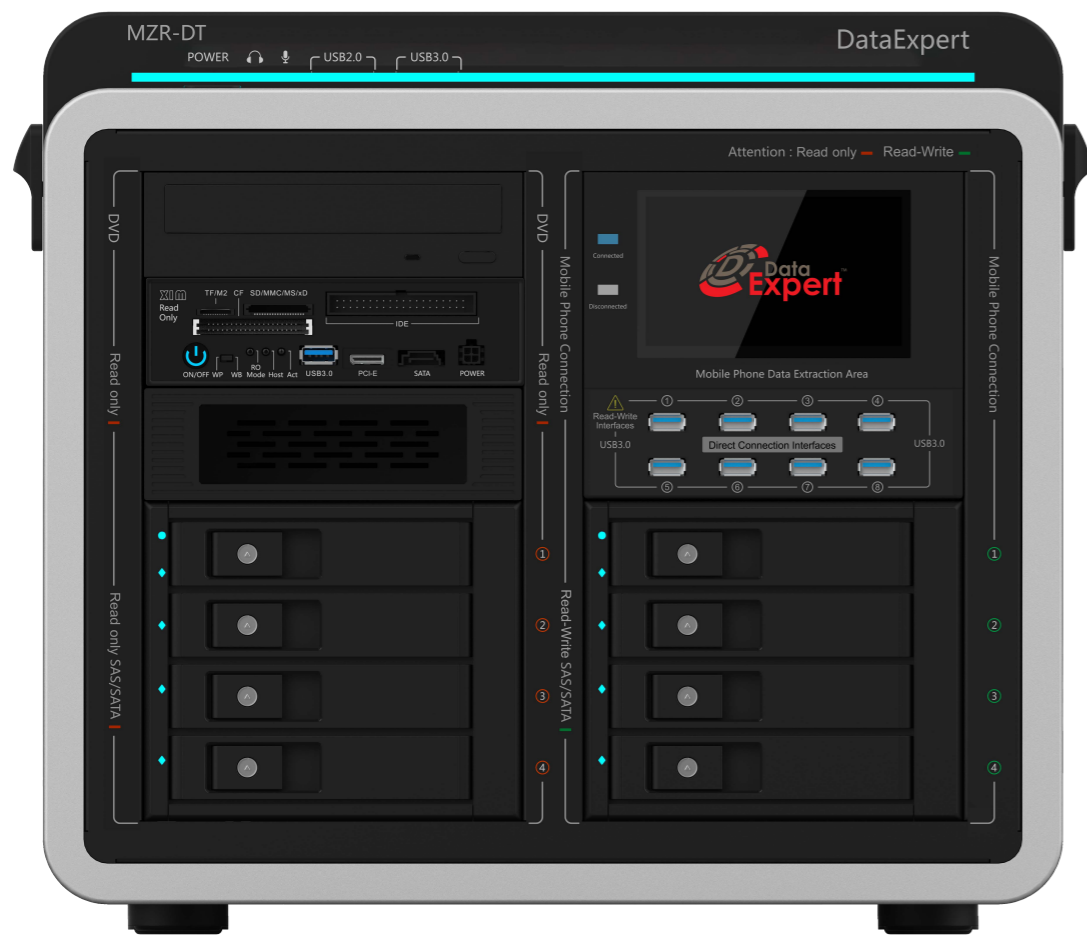


Envolve Forensics LTD - 41 DEVONSHIRE STREET, GROUND FLOOR  
LONDON W1G 7AJ - COMPANY NUMBER 12690094

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

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





# Mobile Forensic

# MD-NEXT

MD-NEXT is a forensic software for data extraction from diverse mobile and digital devices. It supports physical and logical extraction methods across various operating systems.



## Device & OS Support

### 15,000+ Models Supported

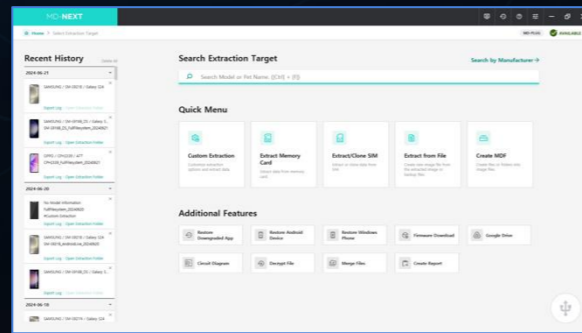
- Supports smartphones, feature phones, tablets, IoT devices, smart devices, wearables and embedded industrial PC board

### Universal Chipset Compatibility

- Extraction support for devices with all major chipsets, such as Qualcomm, MediaTek, Samsung Exynos, Apple and UNISOC

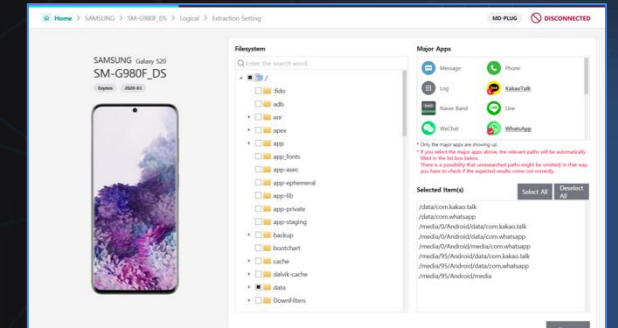
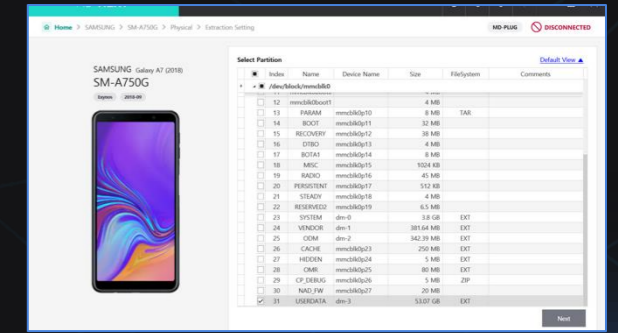
### Diverse mobile OS supported

- iOS, Android, Windows, Kai OS, Bada OS, Tizen OS



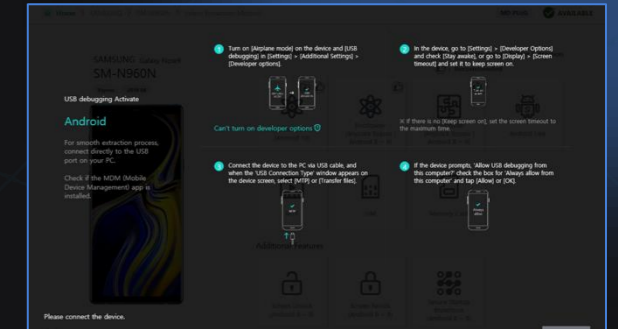
## Extraction Utilities

- Provides utilities for resuming failed extractions and merging multiple image files
- Selective extraction by partition, by apps and by folders
- Features smart automation for custom extraction and automatic partition decryption
- Restores firmware and downgraded apps
- Support for clone of SIM cards
- Support for automatic analysis with MD-RED after extraction



## Intuitive User Interface

- Offers an easy-to-use graphical UI with clear guides and automatic device detection
- Displays real-time progress, estimated time, and data size
- Includes a built-in Hex viewer for data preview



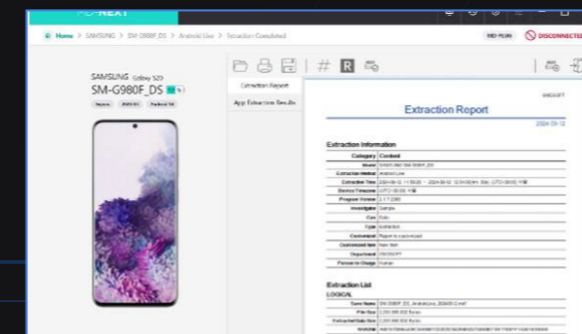
## Powerful Extraction

### Physical & Logical Extraction

- Employs various physical methods like Bootloader, ADB Pro, Custom Image, SD Card, USIM, JTAG, and Chip-off
- Unlocking of FDE enabled phones
- Brute-forcing of Secure Boot Startup
- Android/iOS FFS (Full Filesystem) extraction
- Android Logical Extraction – Android Live Pro (Keystore), Android Live (ADB Backup, Manufacturer backup, App backup, Extraction agent)
- iOS Logical Extraction – AFC, iOS backup
- MTP extraction, Tizen Live extraction

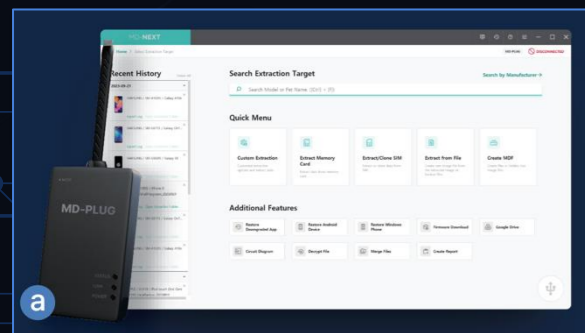
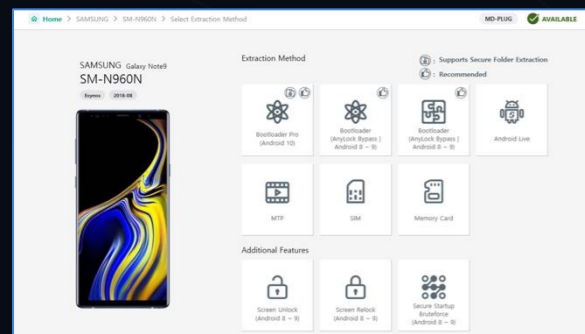
### MD-PLUG : Advanced Extraction

- Hardware for secure data extraction including keystore
- Advanced FFS – MTK, Qualcomm, Exynos and UNISOC chipset devices of FBE enabled
- Android Live Pro – Keystore extraction



## Saving & Reporting

- Supports for saving extraction images as .bin file compatible with other analysis tools
- Ensures data integrity with write-protection
- Generates comprehensive reports in PDF, Excel, Word and HTML formats
- Support for 10 different hash algorithms for extracted files
- Generates extraction log files



MD-PLUG hardware for advanced extraction

# MD-RED

MD-RED is an AI-powered data analysis software for Recovery, Decryption, Visualization, Analytics, and Reporting of evidence data from mobile and digital devices



## Apps and Data Analysis

### Analysis of 2,500+ apps

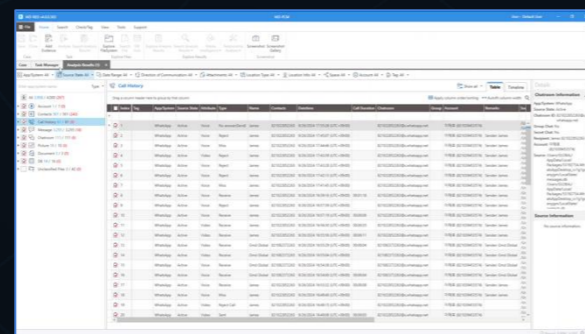
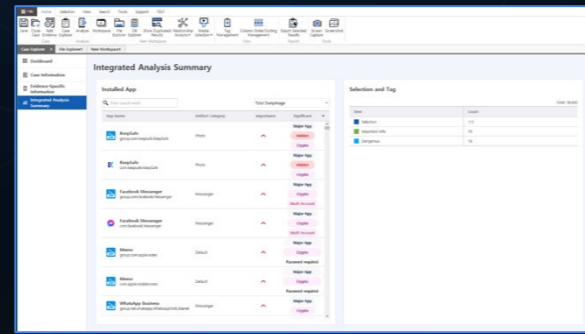
- Analysis of 2,500+ popular mobile apps
- Multi-Account & Space Analysis
- Decoding, Deserialization and Decryption of app data
- Anti-forensic Apps Detection

### Malware Scanning

- Malware detection on APK by scan engine
- Malware detection on files by Yara rules (\*.yar, \*.Yara)

### File System and Image Analysis

- Recovery of file system: EXT2/3/4, HFS+, APFS, NTFS, FAT12/16/32, exFAT, F2FS, VDFS, RSFS, XFS, and YAFFS
- Support for 3rd party forensic tools' images from Encase, GrayKey, UFED, PC-3000 Mobile PRO
- Recovers deleted files and data from unallocated space



## Visualized Analysis Result

- Map view for GPS data and cell tower location
  - Offline/Online map (Region/Country/City)
  - Tracking based on time flow
- Gallery view of multimedia files
- Timeline view of analyzed data
- Link view for social relationship
- Chat view for communication
- Web browser for internet history review
- Hex data, PList, Documents, Video, Audio viewers
- DB Hub for database files table view

## Reporting and Export

- Tagging, filtering, keyword and hash set search
- Supported reports: Excel, PDF, HTML, XML, SQLite DB
- Exports reports form for Relativity and Nuix
- Wizard for configuring report and exports
- MD-Explorer: Distributable viewer for review and tag

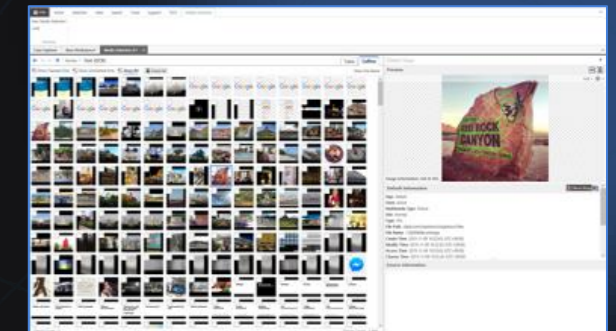
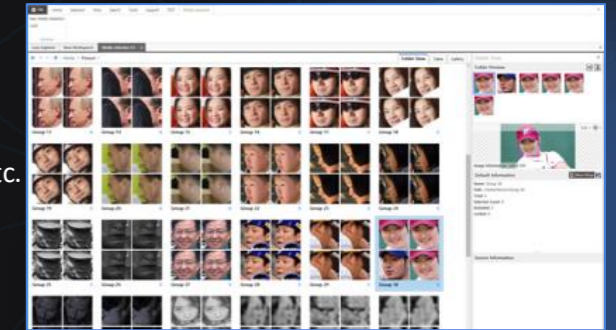
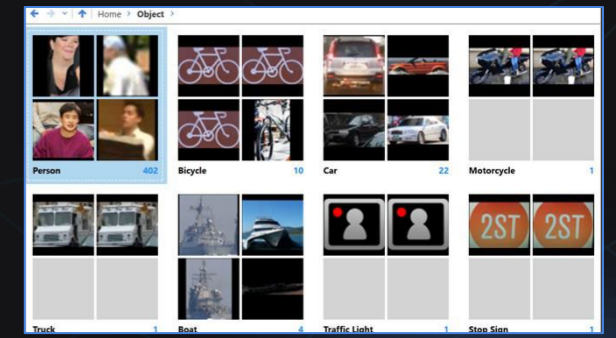
## Multimedia Intelligence

### AI-Powered Deep Analysis

- GPU acceleration for AI processing (Nvidia GPU support)
- AI inference engine of GMDSOFT proprietary

### Image Analysis

- Facial Detection and Search
  - Detects faces in images to group by same face
  - Deep faked face detection
- Supports over 80 objects detection
  - Key objects: Car, Truck, Knife, Rifle, Pistol, Person, etc.
- Camera Analysis: Device type, photo information

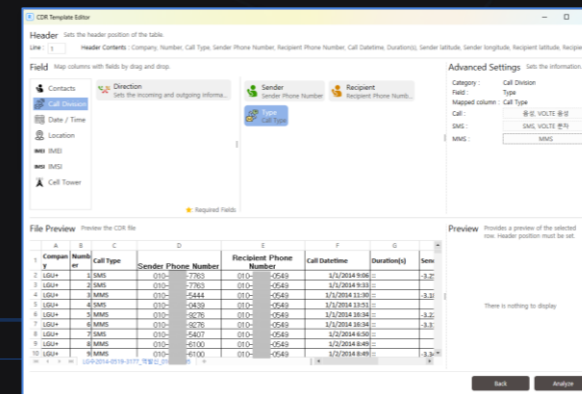


### Language Analysis

- OCR results can be found in analysis result and media selection result
  - Supporting language: English, Korean
- Scanned images or taken pictures of documents are categorized as document images
- STT(Speech To Text): Converts recognized speech into text in the selected language
- MT(Machine Translation): Converts recognized speech into text in the selected language

## CDR Analysis

- Call Detail Record Analysis
- Create a template for analyzing CDR file supplied by mobile carrier
- Relationship analysis together with mobile communication data

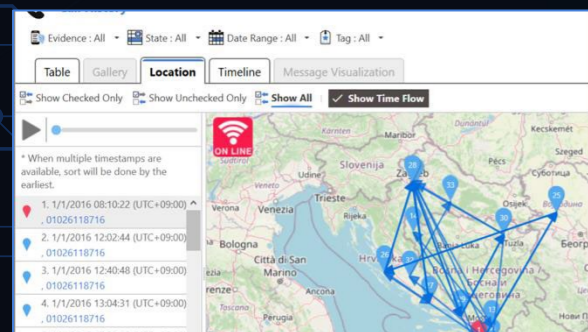
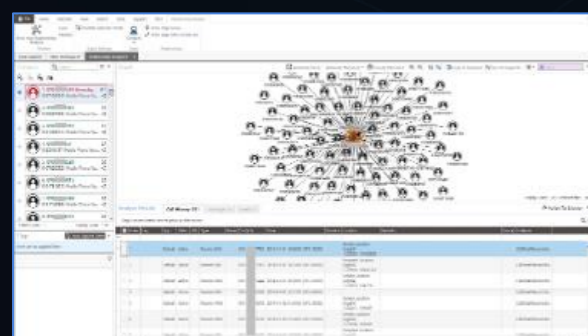
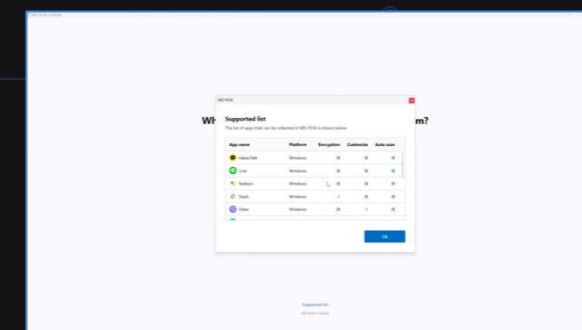


## Project VIC (VICS, CAID)

- Filter images identical or similar to those of Child Sex Use Material (CSAM) registered with Project VIC
- A file having the same or similar hash value may be classified for multimedia based on VICS and CAID

## PC Messenger Analysis

- WhatsApp, WeChat, Facebook, Zalo, Zoom, Telegram, Unigram, IMO, Wickr, Viber, LINE
- Add-on license for PCM analysis required



# MD-LIVE

MD-LIVE is a forensic software designed for triage, specific evidence collection and rapid on-site investigations of mobile devices. It enables quick scanning, selective data extraction, real-time analysis, and secure evidence reporting.



## Data Extraction

### Selective Extraction

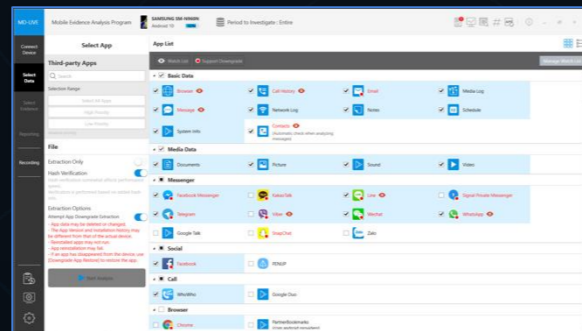
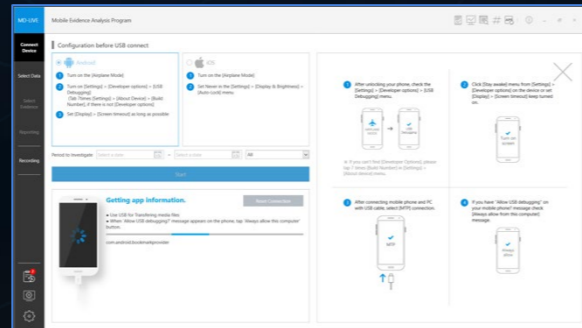
- Scanning & Recording investigation before extraction
- Period specification with detailed OS connection guides
- Selective extraction by file, category, and application
- Option mode: Extraction only mode, Hash verification
- Hash set search (Project VIC, CAID support)

### Android Support

- ADB Backup
- Manufacturer backup (Smart Switch, HiSuite, Bridge)
- Extraction Agent app installation
- App Downgrade for 80+ applications

### iOS Support

- iTunes backup with encrypted backup decryption
- Temporary backup password setting and removal



## Recording Investigation

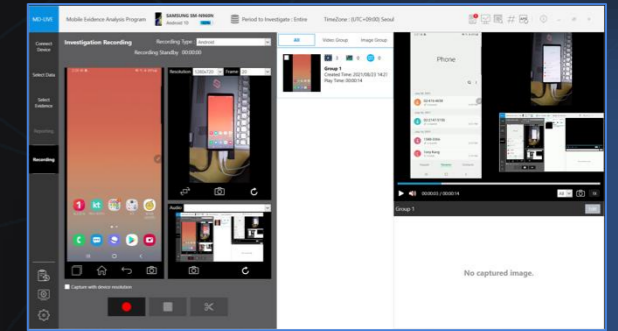
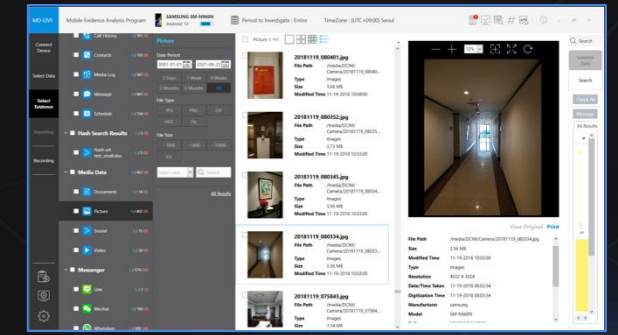
- MD-CAMERA: External camera for evidence/process recording
- Phone Screen Mirroring: Remote control, capture and recording without phone operation
- Program Screen Recording: Video/audio recording of MD-LIVE program screen to reproduce or verify its forensic process



\* MD-CAMERA

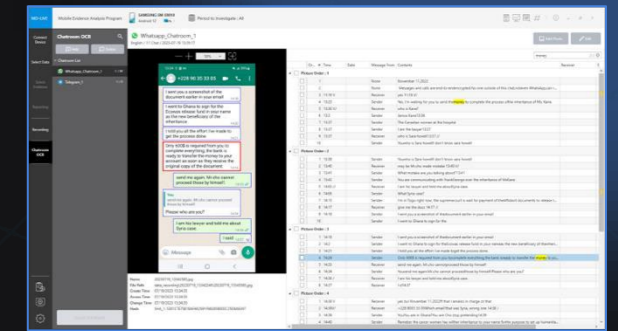


\* HDMI capture card



## Chat Scanner

- Convert chat screenshots into chat text by OCR
- Import Screenshots from Auto Scroll Captured recording, screen recording or extracted pictures
- Correction of OCR results of words or symbols
- Messenger Applications: WhatsApp, Telegram, Facebook Messenger, Signal, Instagram DM, WeChat, Line, KakaoTalk



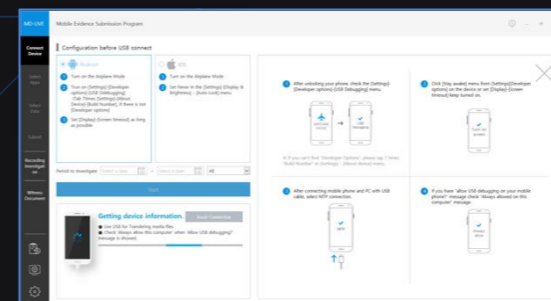
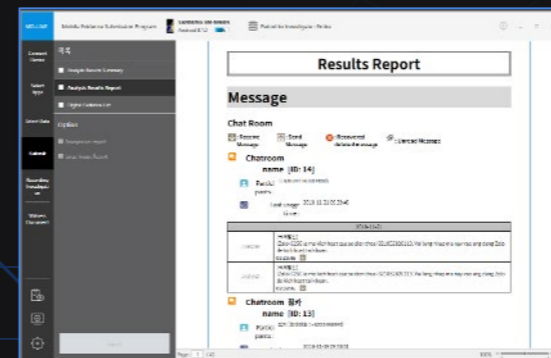
## Data Analysis

### Analysis Capabilities

- 2500+ Android and iOS applications analysis
- Popular Messengers: WhatsApp, WeChat, Signal, Facebook Messenger, Discord
- Basic Data: Browser, Call History, Contacts, Map History, SMS/MMS
- Social Media: Facebook, X (Twitter), Instagram
- Multimedia: Documents, Pictures, Audio, Video
- Android Log Analysis: Recent usage tracking
- Process Monitoring: Active application analysis

### Evidence Selection

- Category and application-specific filtering
- Watch list apps and data type
- Keyword search support (.xlsx, .csv, .txt, .keyword)
- Visualization with maps, chat display, gallery



## Reporting

- PDF Reports: Summary & detailed analysis with document editor
- Message Visualization: Timeline view with anonymization option
- Multiple Formats: Excel (.xlsx), Database (.sqlite), MDF
- Archive Creation: ZIP, TAR, DD formats
- Multimedia Export: Separate file extraction option

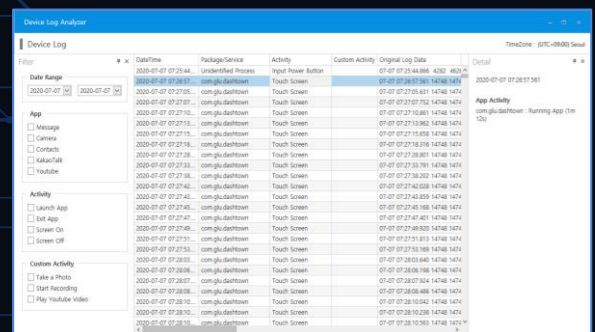
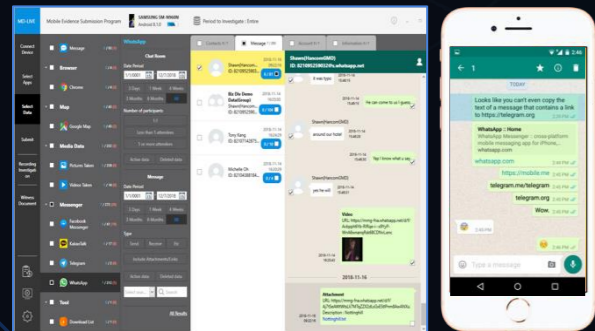
## Management

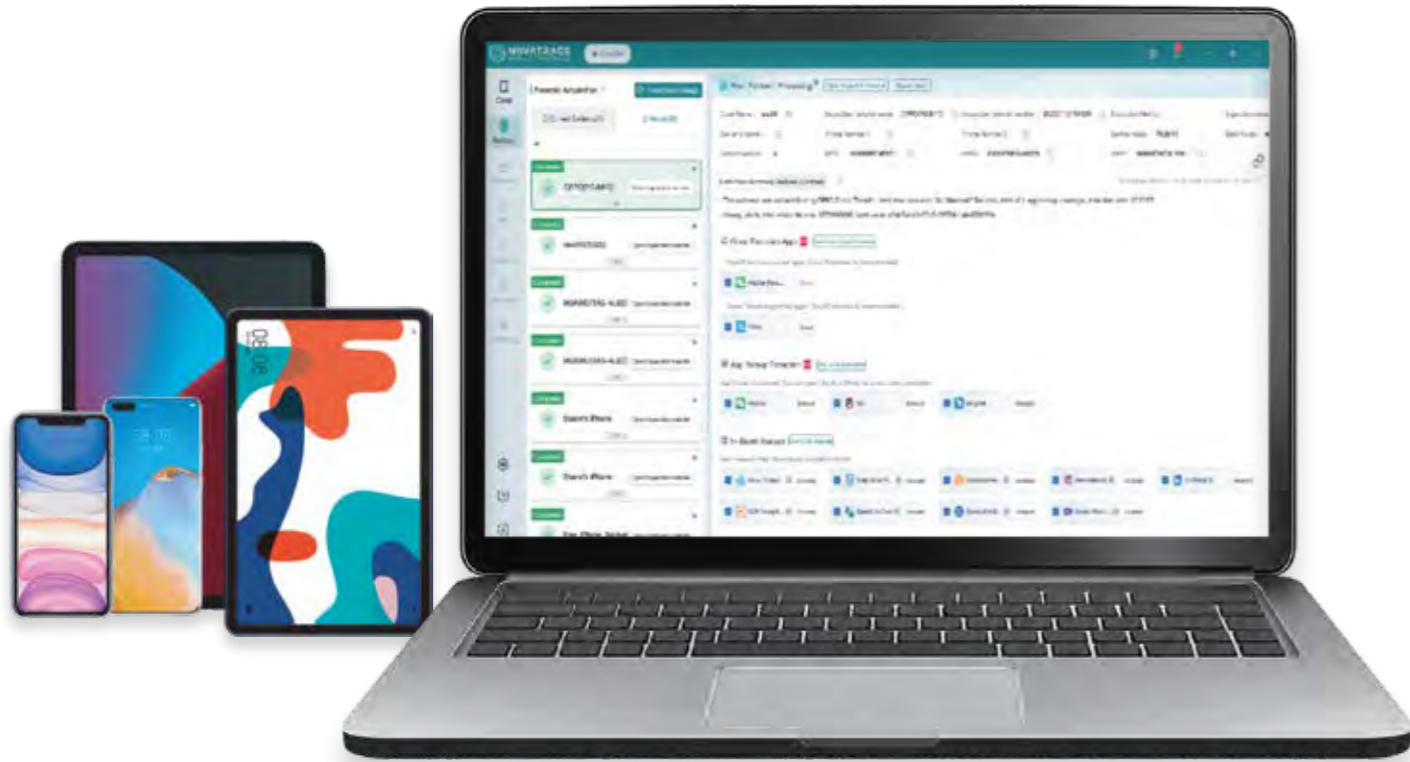
### Easy to Use Guide

- Auto-Scan device information
- Step-by-step guide to connect and to investigate

### Case & Language Support

- Case Management: Create, save, open investigations
- Languages: English, Chinese, Japanese, Arabic, Indonesian, Russian





# NovaTrace

Parallel Mobile Forensics System



**Data Extraction**



**Data Recovery**



**Data Analysis**

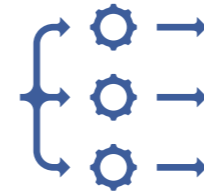


**Data Retrieval**



**Report Export**

The NovaTrace Parallel Mobile Forensics System is a comprehensive, all-in-one forensic solution designed for the modern digital investigator. It combines unparalleled acquisition flexibility with powerful, AI-driven analysis tools to streamline workflows and uncover critical evidence efficiently.



## 01 MULTICHANNEL ACQUISITION VERSATILITY

Acquire data from virtually any source: multiple devices in parallel, all major OS (Android, iOS, HarmonyOS), vendor backups, PC clients via QR code, and isolated WiFi, without needing root or complex downgrades.

## 02 DEEP CHINESE ECOSYSTEM & CLOUD SUPPORT

Gain unmatched access to data from over 300 popular Chinese applications and critical cloud services like WeChat Pay, Alipay, and Baidu Netdisk, ensuring no key evidence is missed.



# AI

## 03 AI-POWERED EVIDENCE PROCESSING

Automate the discovery of critical evidence with AI-driven image analysis (faces, IDs, transactions) and speech-to-text conversion, transforming multimedia files into actionable intelligence.

## 04 TARGET-CENTRIC INVESTIGATIVE INTELLIGENCE

Focus your investigation efficiently. The "Target Person" feature automatically correlates identities across all data, while cross-device analysis and visual timelines reveal hidden connections and the full story.



## 05 COMPREHENSIVE FORENSIC WORKFLOW TOOLS

Manage the entire process within one platform, from static/dynamic APK analysis and custom scripting for new apps to built-in screen recording for impeccable audit trails.

## 06 PROFESSIONAL-GRADE REPORTING & COMPLIANCE

Customizable report templates, merge capabilities across cases, historical task management, built-in screen recording, and a portable report viewer with search and filtering. Supports forensic workflow standards, evidence tagging, audit logs, and isolated acquisition modes to maintain data integrity and chain of custody.



# 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 ARTIFICIAL 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.



# 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

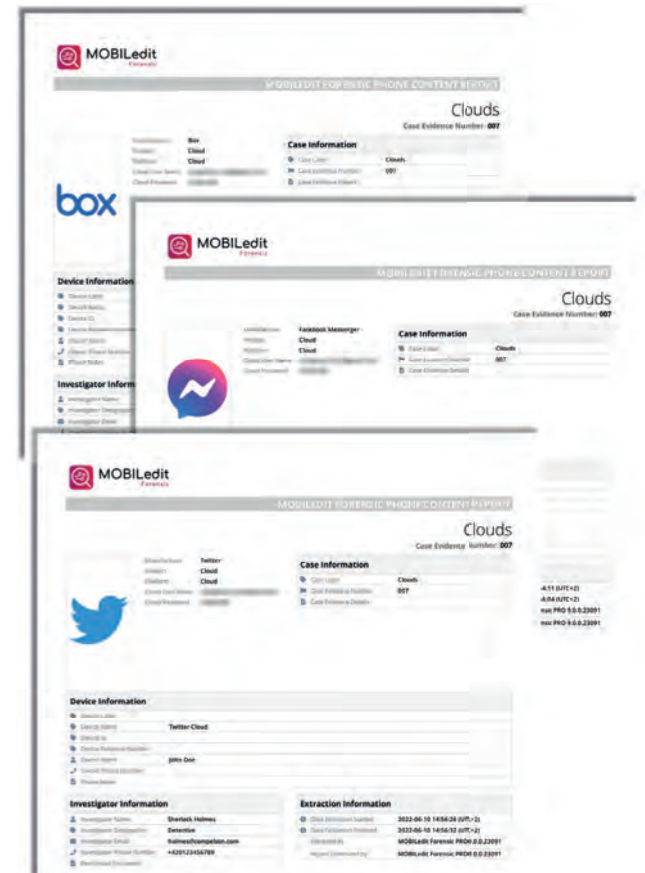
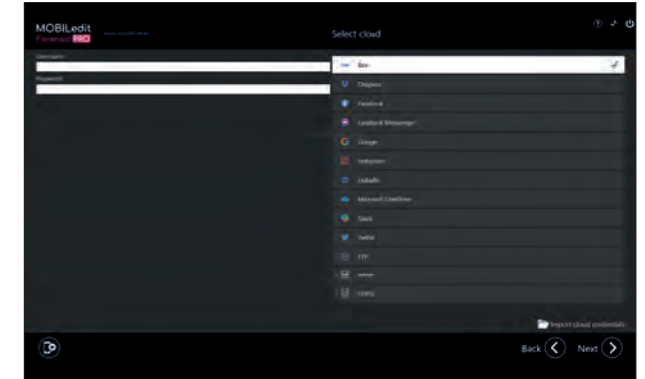
- Automatic download of clouds using either an authorization token or a username and password credentials. These can be found, extracted, and saved from a phone during extraction and analysis with MOBILedit Forensic PRO.
- Both authorization token access and username and password access are supported. 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, ufd, and Excel.
- Full file structure download.

## 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

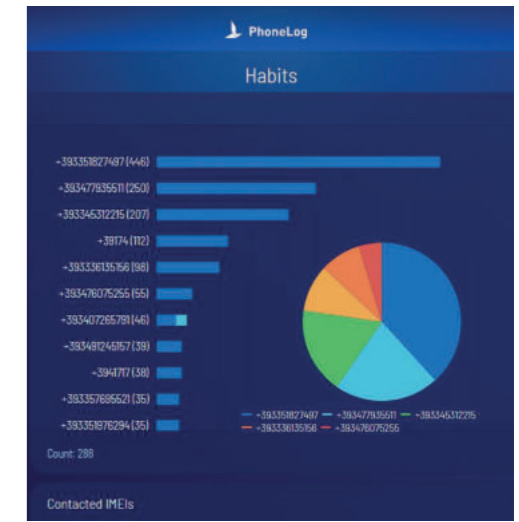
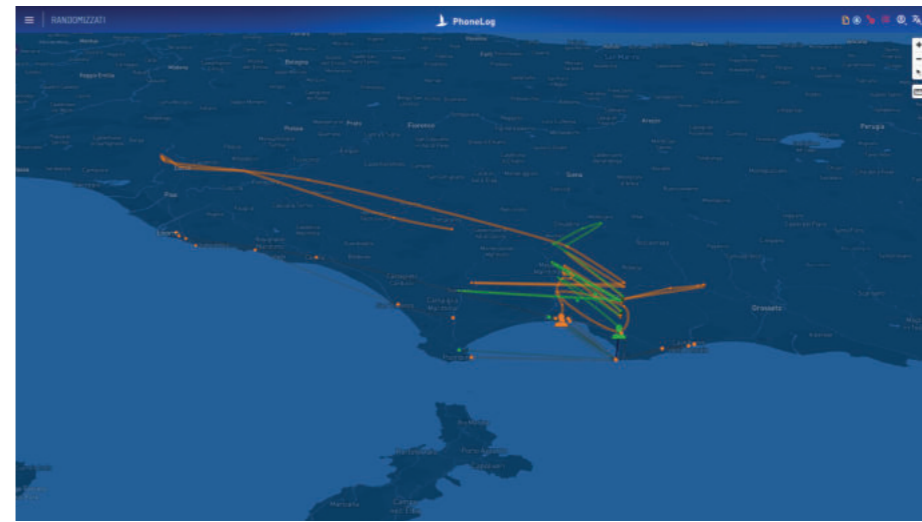
## WHY CLOUDS?

- 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)



# PhoneLog

Multi Level Phone Records Analytics  
Digital Evidence Correlation  
3D mapping



## 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](#)

## 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.**

### 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, prosecutors, 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





## 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.

## 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.

## 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.

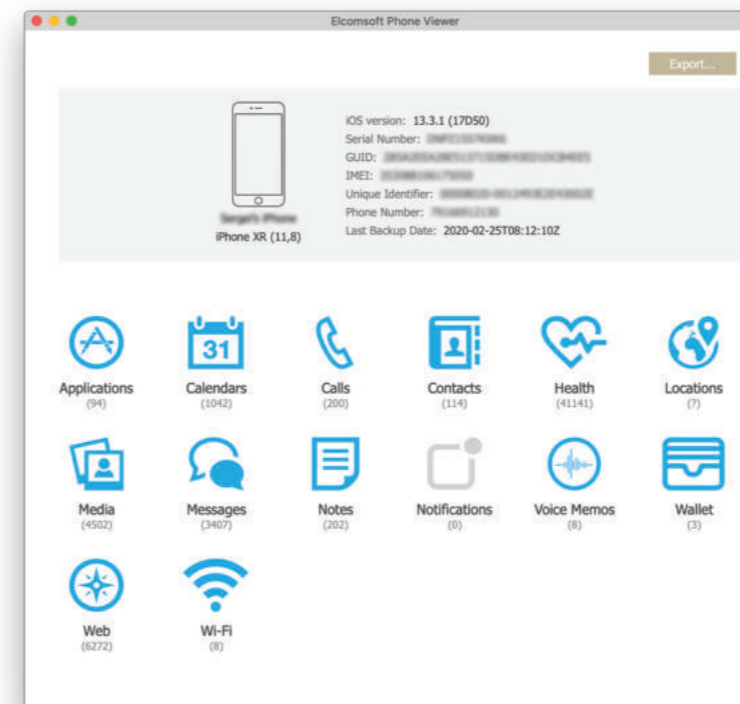
Extract, decrypt and view WhatsApp, Skype, Signal and Telegram communication histories, attachments and contact lists from a wide range of devices or cloud services. The downloading of the conversation histories, when available, only takes minutes!

### 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.



### 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](http://www.elcomsoft.com/emfb.html)

More informaton at [www.elcomsoft.com/emfb.html](http://www.elcomsoft.com/emfb.html)



# Digital triage for mobile devices

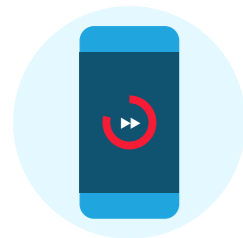
Vital evolution of our game-changing rapid triage tools in a world where 95% of people access the internet through their mobile phones

[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

# 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.

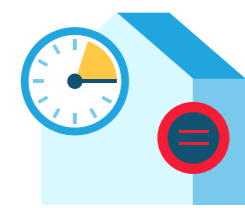
With our simple-to-use interface, traffic light results that can be reviewed on the screen, your time to first evidence while on-scene can be reduced from hours to minutes.



1. Arrive on scene



2. Scan devices

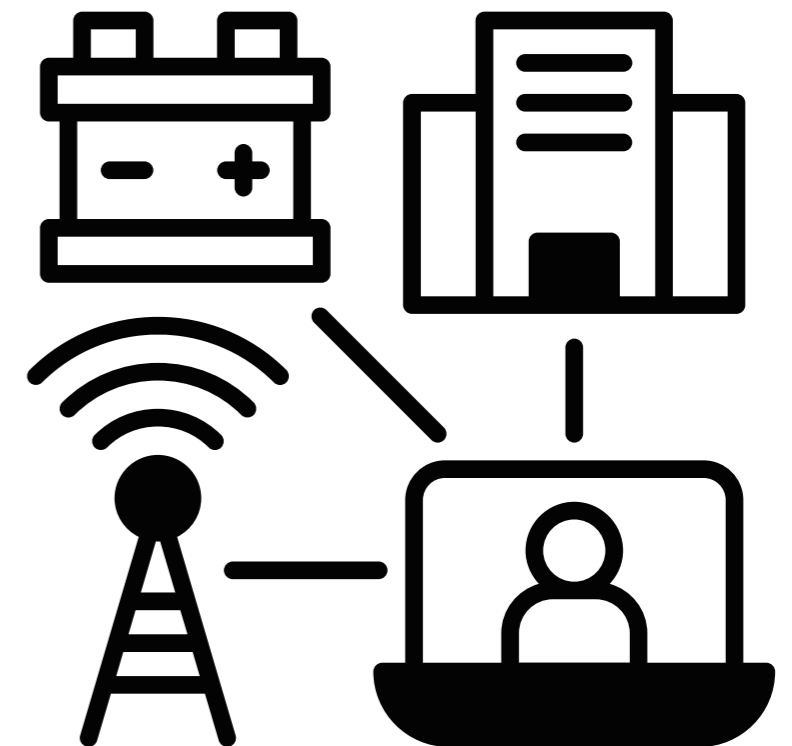


3. Fast results

## 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

# IoT Forensic Solution



# XCOUSTIC mini X40

## Remote Audio Monitoring Device

Powered by Laser & Light Wave Technology



mini X  
XCOUSTIC

Up to  
**40m**  
Effective Range

### PRODUCT OVERVIEW

The system adopts Doppler diffuse reflection optical laser technology, matrix detection technology, auto digital focusing technology and other innovative achievements.

With long distance, no preset, and non-contact application environment, it can realize the synchronization of target sound information tens of meters away. Collection, which effectively meets the needs of relevant departments for the collection of target sound information, is an important means to obtain sound information.

The system has obvious advantages in sub-nanometer weak vibration measurement and weak return light detection capability, and has outstanding advantages in target medium adaptability, working distance, window angle and so on.

The system is highly integrated, easy to operate, easy to carry, and quick to deploy, and;

### HIGHLIGHT FEATURES

- **Distance sound pickup** - Equipped with automatic focusing function, it can accurately locate the sound pickup area, and the sound pickup distance up to tens of meters;
- **Lightweight and convenient** - The equipment weighs less than 2.5KG, making it the smallest and lightest among similar equipment and easy to carry;
- **Easy to operate** - There are few steps to operate: power on-> point-> focus->play sound, the device is quickly deployed and easy to use. Mobile phones, tablets, and computers can all pick up sound through mobile networks or Wi-Fi connections, and operate through software to achieve human-machine separation and wireless control;
- **Strong penetrating power and wide application range** - Lasers can penetrate glass and collect audio information.
- **Scope of application:** Including common indoor furnishings (paper boxes, curtains, paper table tags, paper bags, etc.); common outdoor furnishings (billboards, trash cans, license plates, etc.);
- **High stability and anti-interference** - The laser collects audio in a small range to avoid interference from the surrounding environment, and uses advanced algorithms to perform multiple processes such as noise reduction, equalization, and filtering on the audio to restore stable, high-fidelity audio;
- **Audio and video integration** - The software interface has video functions to achieve audio and video integration;
- **With ranging function** - Ranging range: Up to 40m, ranging accuracy:  $\pm 3\text{cm}$ .
- **Monitoring capabilities on a wide range of materials:** It is possible to pass through single clear glass windows. Paper, leather, cloth, plastic, metal and other material objects can be used as the target medium.
- **Optional additional noise reduction functions** that has high voice recognition ability.
- **Multi-functional mobile operation terminal** is wirelessly connected with the host, which integrates "viewing, aiming, listening, recording and transmitting" to realize remote control operation.
- **Using invisible infrared laser**, low power and safe.
- **Multi-power mode**, (optional) built-in battery design improves the flexibility of the system.

MAIN COMPOSITION	
1. Xcoustic Unit	2. Android Operating Terminal
3. Headphones	4. Tripod (optional)
5. High-Precision Fine-Tuning Gimbal (optional)	6. Cable Set
7. Field backpack / Rugged Field Equipment Case	8. Accessory

TECHNICAL SPECIFICATION	
Working Distance	Up to 40m
Transfer Method	Wired/Wireless transmission
Recording ability	Long range recording, stable, recognition rate $\geq 90\%$ 65dB (In A Good Environment)
Laser	1550nm Infrared laser wavelength
Camera	Built-in wide-angle color CCD telephoto sensitivity $\leq 1\text{lux}$ night vision CCD
Communication	Built-in Wi-Fi module for wireless connection with operator terminal
Interface	Power interface
	Data transfer interface
	Wifi antenna interface
Power Supply	AC220V/battery Working voltage: 12V
	Built-in time: ~3 hours Lithium battery capacity: >300mAh
Host Weight	2.5kg
Host Size (mm)	160x160x68
Operating Temperature	-10°C~+40°C
Recording	Audio and video simultaneous recording format: mp4



Rugged Field Equipment Case Color option

**Custom Design Available**



*Custom designs are available for clients such as law enforcement agencies, specifically tailored to meet the stringent environmental and operational requirements essential for successful covert operations. These designs enhance their ability to gather intelligence efficiently and effectively while maintaining a discreet low profile in public area.*

**Note:** All design, features, contents, functionality and specifications of products described are subject to change without notice. Please check for the latest update.

# XCOUSTIC X2

*Remote Audio Monitoring Device*  
*Powered by Laser & Light Wave Technology*



**X<sup>2</sup>**  
XCOUSTIC

Up to  
**200m**  
Effective range

## PRODUCT OVERVIEW

The system adopts Doppler diffuse reflection optical laser technology, matrix detection technology, digital focusing technology and other innovative achievements.

With long distance, no preset, and non-contact application environment, it can realize the synchronization of target sound information hundreds of meters away. Collection, which effectively meets the needs of relevant departments for the collection of target sound information, is an important means to obtain sound information.

The system has obvious advantages in sub-nanometer weak vibration measurement and weak return light detection capability, and has outstanding advantages in target medium adaptability, working distance, window angle and so on.

The system is highly integrated, easy to operate, easy to carry, and quick to deploy, and;

## HIGHLIGHT FEATURES

- **Long distance sound pickup in environments such as inside vehicles, buildings, or other locations** - Equipped with automatic focusing function, it can accurately locate the sound pickup area, and the sound pickup distance up to hundreds of meters;
- **Lightweight and convenient** - The equipment weighs less than 5KG, making it the smallest and lightest among similar equipment and easy to carry;
- **Easy to operate** - There are few steps to operate: power on->point->focus->play sound, the device is quickly deployed and easy to use. Mobile phones, tablets, and computers can all pick up sound through mobile networks or Wi-Fi connections, and operate through software to achieve human machine separation and wireless control;
- **Strong penetrating power and wide application range** Lasers can penetrate glass and collect audio information. Scope of application: Including common indoor furnishings (paper boxes, curtains, paper table tags, paper bags, etc.); common outdoor furnishings (billboards, trash cans, license plates, etc.);
- **High stability and anti-interference** - The laser collects audio in a small range to avoid interference from the surrounding environment, and uses advanced algorithms to perform multiple processes such as noise reduction, equalization, and filtering on the audio to restore stable, high fidelity audio;
- Simultaneous audio and video monitoring;
- **Audio and video integration** - The software interface has video functions to achieve audio and video integration;
- **With ranging function** - Ranging range: >200m, ranging accuracy: <math>\pm 3\text{cm}</math>.
- It is possible to pass through single clear glass windows.
- Paper, leather, cloth, plastic, metal and other material objects can be used as the target medium.
- Optional additional noise reduction functions that has high voice recognition ability.
- Multi-functional mobile operation terminal is wirelessly connected with the host, which integrates "viewing, aiming, listening, recording and transmitting" to realize remote control operation.
- Using invisible infrared laser, low power and safe.
- Multi-power mode, (optional) built-in battery design improves the flexibility of the system.

MAIN COMPOSITION	
1. Xcoustic Unit	2. Android Operating Terminal
3. Headphones	4. Tripod
5. High-Precision Fine-Tuning Gimbal	6. Cable Set
7. Field backpack / Rugged Field Equipment Case	8. Accessory

*Note: Design, features, functionality and specifications are subject to change without notice. Please check for the latest update.*



Rugged Field Equipment Case Color option

TECHNICAL SPECIFICATIONS	XCOUSTIC X1	XCOUSTIC X2
Working Distance	Up to 100m	Up to 200m
Transfer Method	Wired/Wireless transmission	
Comprehension Rate (In A Good Environment)	≥ 90% 65 dB (in good environments)	
Laser Wavelength	1550nm	
Laser power	≤ 16mW	
Dual Vision Lens	25 mm wide-angle lens	
Camera	Built-in wide-angle color CCD and two sets of telephoto sensitivity ≤1lux night vision CCD	
Communication	Built-in Wi-Fi module for wireless connection with operator terminal	
Interface	Power Port	
	Wi-Fi Antenna Port	
	RJ45 Data Port	
	3.5mm Headphone Port	
Power Supply	Built-in time: >3 hours	
	AC220V/battery (<15W)	
Host Weight	≤2.0kg	≤5.0kg
Host Size (mm)	200×130×80	274×125×184
Operating Temperature	-10°C~+40°C	
Recording	Audio and video simultaneous recording format: mp4	

# MD-VIDEO AI

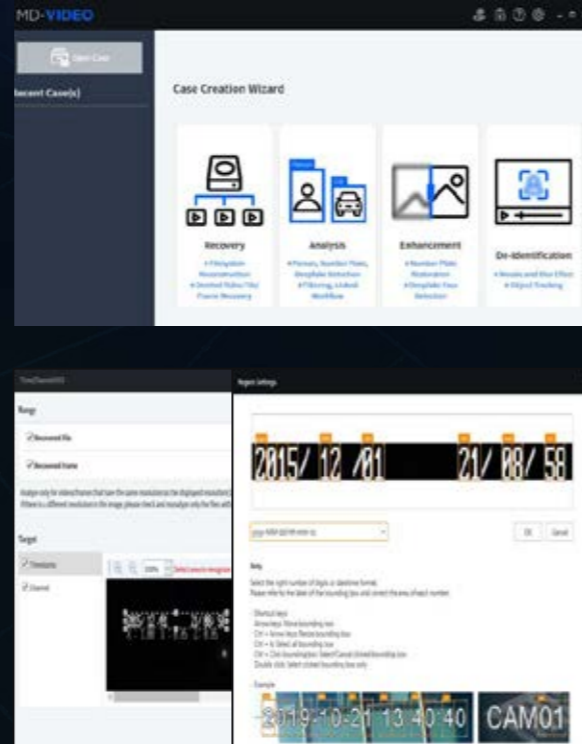
MD-VIDEO AI is an AI powered video forensic software solution designed for the recovery, enhancement and in-depth analysis of media files from a wide range of recording devices, including CCTV/DVR systems, vehicle dashcams, drone cameras, IoT cameras, and more.



## Multimedia Recovery

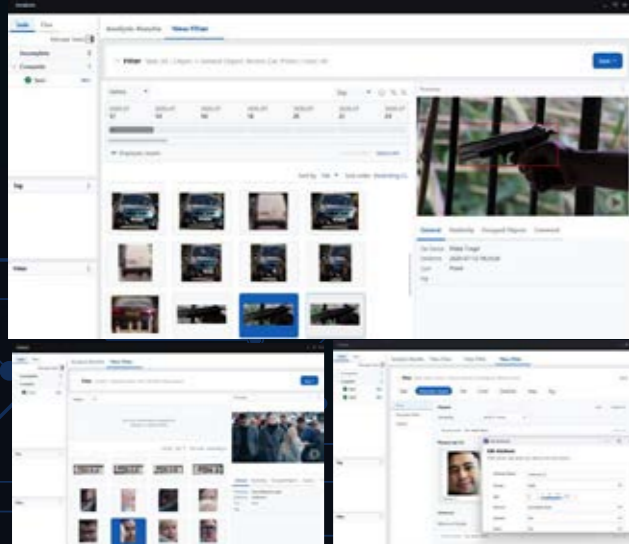
### Video/Audio/Frame

- Recovery of deleted video, audio and frame data
- Frame extraction from video files
- Codec and Container-based recovery
- Partial recovery using time and metadata (H.264/H.265)
- Supports forensic image formats (E01, DD, 001, BIN, MDF)
- Supports recovery from RAID 0 and RAID 5 storage systems
- Broad support for DVR and Dashcam models
- Supports standard/proprietary filesystems and video formats
- File conversion to AVI/MP4, MP3/AMR, JPEG/PNG formats
- Audio extraction from video files
- Built-in advanced media player for forensic video investigation



### Channel / Time Information

- Supports recovery of date/time information from file meta-data
- OCR based extraction of time and channel information
- Date/Time offset correction and adjustment



## Video Analysis

### Object and Anomaly detection

- Detect 80+ types of objects
- Specialized detection for Weapons (Knife, Pistol), License plates, and Faces
- Find one or more objects from one of more videos at once
- Detect small sized objects out of good resolution videos
- Robust filters mechanism to find clues out of detected objects
- Date/Time, Object, Color, Files, Area filters
- Video briefing by required detected objects for court
- Supports NVIDIA GPU models for accelerated video analysis

### Search Suspects, Vehicle license plates

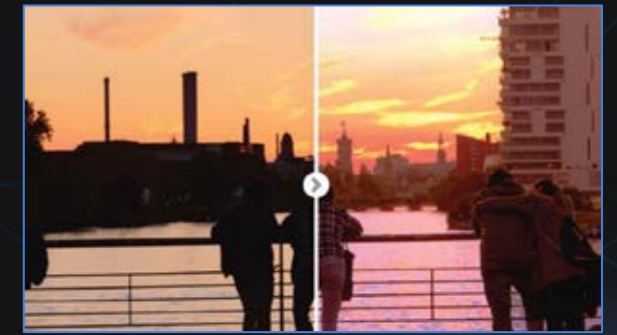
- Abnormal scene detection
- Find suspects out of multiple video footages
- Detect and Search specific digits of vehicle license plates
- Detect potential deepfake manipulations in facial content

## Image/Frame Enhancement

- AI powered image and video frame enhancement functions
- Precision frame Cropping and Zoom (20~1000%)
- Image enhancement filters for Low-Light scenes
- Advanced Color, Sharpness & Noise control filters
- Corrects motion blur, camera shake and out of focus frames
- Perspective Correction & Image rotation
- Upscales low resolution frames using SRGAN and other deep-learning algorithms
- AI models for Estimating object length and vehicle speed
- Complete Enhancement Workflow with forensic reporting

## Number Plate Restoration

- AI driven country specific License Plate restoration models
- Single and multi frame reconstruction for higher accuracy
- Intelligent candidate number prediction and refinement
- Works on Car, motorcycle, tricycle, truck and other vehicles



## Face Restoration & Deepfake

- AI based deepfake detection for manipulated faces
- Provides deep fake confidence score (%) for analyzed faces
- Face restoration models to enhance blurry faces
- Restoration models optimized for facial attributes to improve enhancement accuracy

## De-Identification

- Hide or blur sensitive areas in photo and video
- Track moving objects across video frames
- Trim and Split required or unwanted video segments
- Flexible & Precise editing tools for de-identification workflows
- Seamless export for reporting and court submission
- Privacy protection with GDPR compliance support

# MD-CLOUD

MD-CLOUD is a forensic software for the extraction and analysis of data from cloud services. It supports a wide range of global and regional cloud platforms.



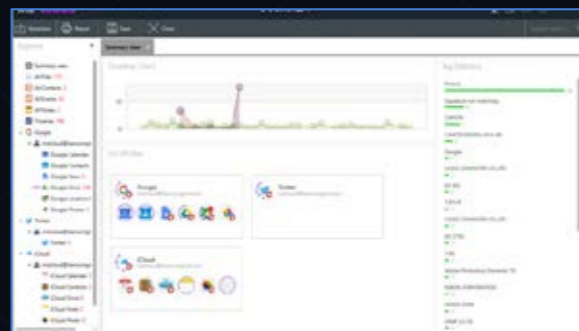
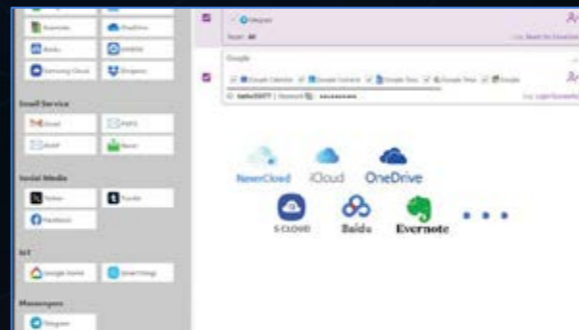
## Global Service support

### Global Cloud Support

- **Cloud Service:** Google Cloud, iCloud, OneDrive, Dropbox, Baidu Cloud, Naver Cloud
- **Email Services:** Gmail, IMAP/POP3, Naver Mail
- **Social Media:** Telegram, Facebook, X(Twitter), Tumblr
- **Productivity:** Evernote, MYBOX document storage

### Region-Specific Services

- Selective/integrative analysis specialized for regional cloud platforms (e.g., Naver Cloud, Baidu Cloud)
- API-level data acquisition capabilities
- Localized authentication to support region-specific environments



## Advanced Authentication

### Multi-Layer Security

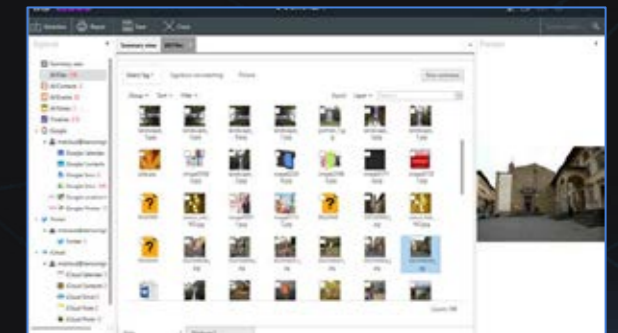
- **Various authentication methods:** ID/Password authentication, Captcha security authentication, 2-step security authentication, Authentication using Credential information
- **Auto Login:** Credential reuse and token preservation

### Real-Time Monitoring

- **Progress Tracking:** Live extraction status updates
- **Data Integrity:** 3 hash algorithms (MD5, SHA-1, SHA-256)

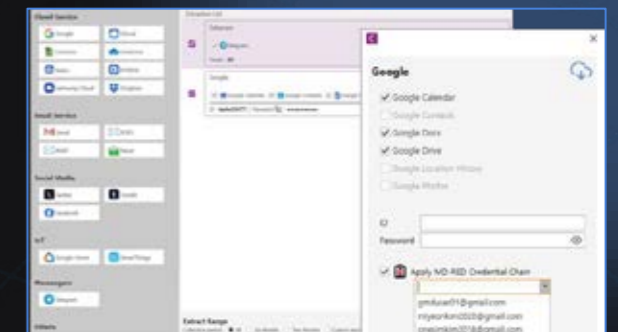
## Data visualization

- **Timeline Analysis:** Chronological data organization
- **Map Visualization:** Location-based evidence mapping
- **Tag System:** Pre-categorized data for fast search
- **Built-in Viewers:** Image, video (H.264/H.265), documents, emails



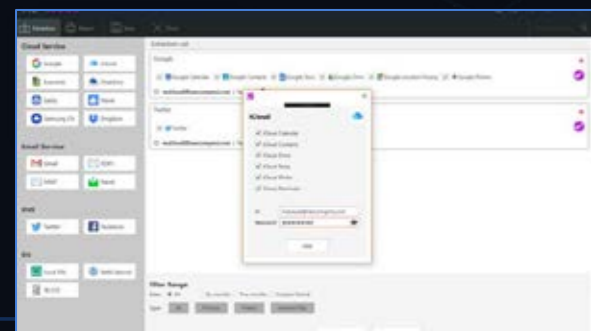
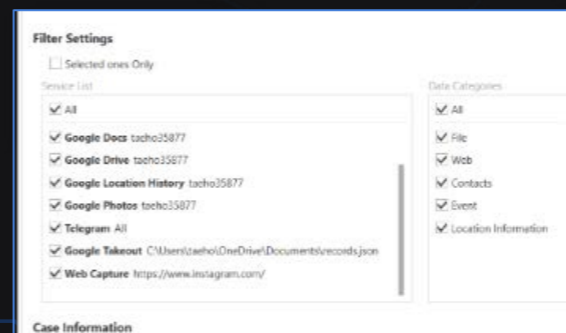
## Interwork with MD-RED

- Supports analysis for extracted data by MD-CLOUD with MD-RED
- Supports reuse of session token in MD-CLOUD taken from data analyzed by MD-RED



## Reporting

- Supports report format as PDF
- Supports export of original cloud data files



# MD-DRONE

MD-DRONE is a forensic software designed to extract and analyze data from a wide range of UAV/Drone data sources. It supports multiple extraction methods across diverse models and delivers AI-powered analysis for advanced investigation of drone normal incidents and accidents.



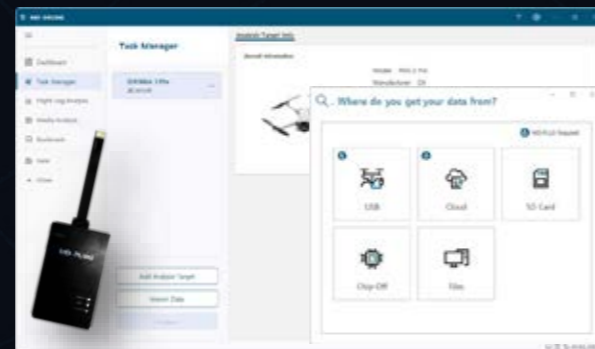
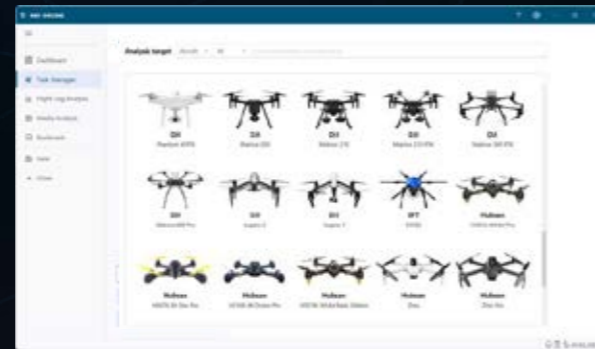
## Data Extraction

### Multiple Extraction Methods

- **Logical & Physical:** Comprehensive data recovery from drone storage sources
- **Chip-off Extraction:** Direct memory chip analysis for damaged devices
- **Extraction Media:** USB connection, Wi-Fi interface and external memory card readers, MD-PLUG, MD-READER
- **MD-PLUG Integration:** Advanced extraction support for modern drone models

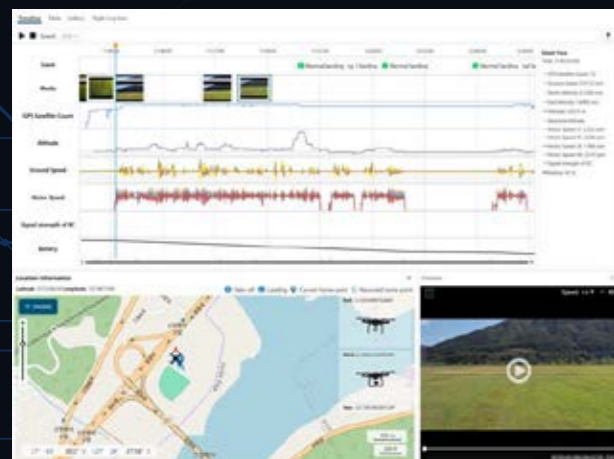
### Data Source Support

- **Drone and Flight Controllers:** Broad model support with guided extraction workflows
- **Mobile Applications:** Extraction from Android drone apps and flight log data
- **Remote Controllers:** Direct data acquisition from RC devices
- **File Format support:** DAT, ULG, BIN, PUD, TXT, MDF, DRF, TLOG and SRT formats
- **DJI Integration:** DJI Assistant files and manufacturer-specific data



## Flight Log Analysis

- **Integrated Analysis:** Flight log analysis across multiple targets
- **Multiple Visualizations:** Analyzed data presented in Timeline and Tabular views
- **Flight Parameters:** GPS coordinates, Speed, Altitude, Battery status and more
- **Map Visualization:** Flight path display with takeoff and landing points
- **In-built Media Viewer:** Multimedia previews synchronized with the timeline
- **Collision Analysis:** AI-based drone accident analysis



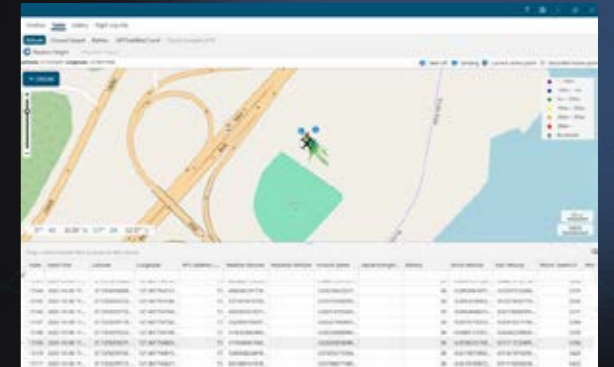
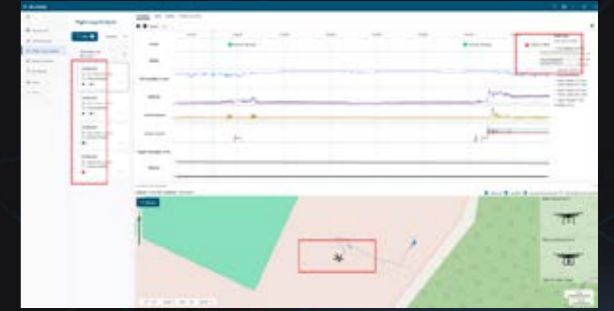
## AI-Based Collision Analysis

### Intelligent Event Detection

- **Collision Identification:** Automatic crash and impact events
- **Battery Analysis:** Power depletion and failure warnings
- **Abnormal Behavior:** Identification of unusual flight patterns and maneuvers
- **Landing Classification:** Detection of normal and abnormal landing events

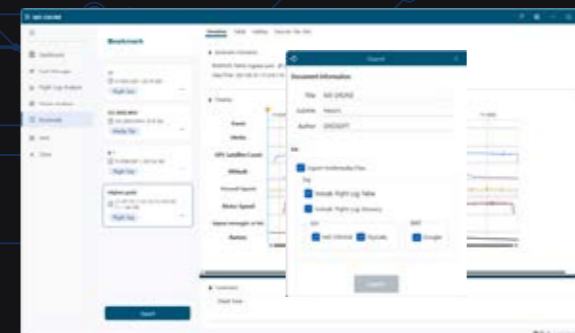
### Event Visualization

- **Multimedia Gallery:** Preview synchronized with corresponding flight logs and timeline
- **Color Coding:** Green (normal) and red (abnormal) event markers for quick identification
- **Events on Map:** Visualization of takeoff, landing, and other major events using color coded flight paths
- **Event Counting:** Statistical overview of normal and abnormal events per flight log
- **Confidence Indicators:** AI analysis accuracy ratings



## Bookmarks and Reports

- **Flexible Selection:** Flight time ranges, specific images, and videos
- **Comment System:** Add investigative notes to bookmarked evidence
- **PDF Reports:** Generate professional forensics reports with bookmarked evidence
- **Data Export:** Export DAT files in CSV format and flight paths in KML for GIS integration
- **Video Generation:** Export animated flight path visualizations as video file
- **Media Preservation:** Preserve original multimedia files with complete metadata
- **Multi-language Support:** English, Bahasa Indonesia, Japanese, Vietnamese



# 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.



## 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.



### 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.

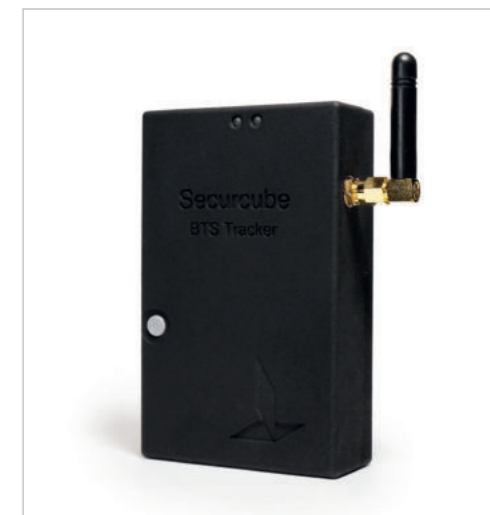
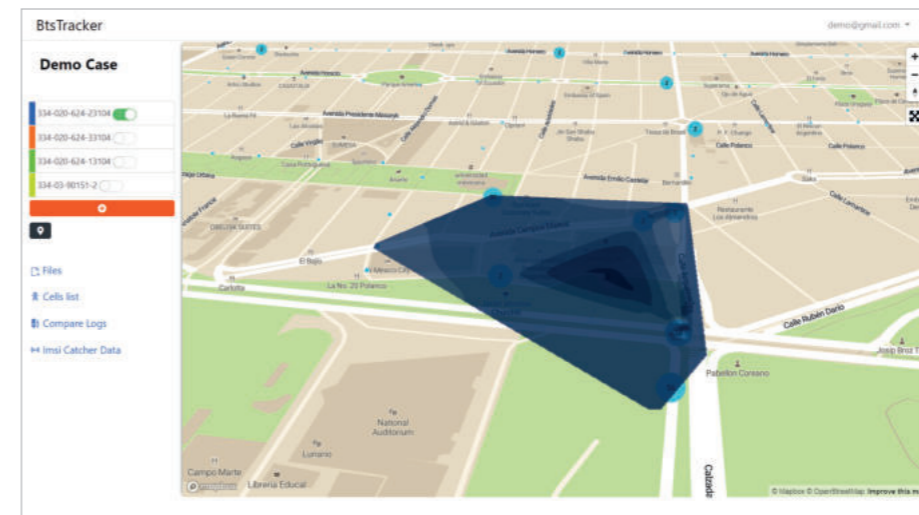
## MOBILedit Dive Kit

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.



# 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.

### 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





## 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

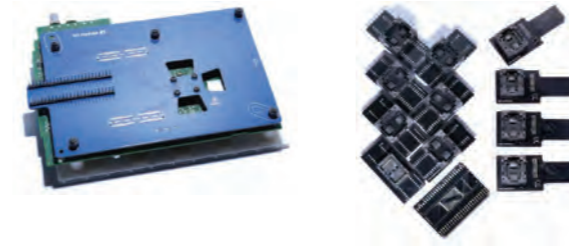
- ✓ **Vehicle System Data:** VIN, serial and part numbers, FW version, MAC/IP addresses, etc.
- ✓ **Events:** WIFI/Bluetooth/USB connections, vehicle power on/off, start/stop, reboots, door/light data, odometer, fuel consumption, system logs, etc.
- ✓ **GPS navigation data:** routes, tracklogs, POIs, 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

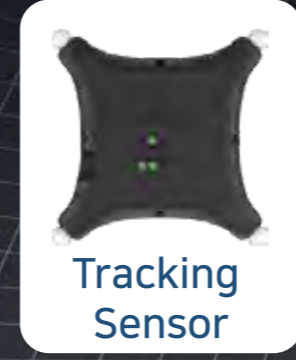
- ✓ Powerful software for physical dump acquisition and further vehicle data extraction, including parsers for File systems: QNX6, UBIFS, YAFFS2, FAT12,FAT16,FAT32,exFAT, Ext2, Ext3, Ext4, NTFS, HFSX, others embedded systems based on FTLs.Embedded FTLs
- ✓ VNR software
- ✓ Set of chip-off adapters for 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

Convergence of civil Virtual Reality development technology and military training



Large-space hybrid simulation training system based XR technology for strengthening of combat power



Examples of personal training equipment

IR camera based Position and motion tracking

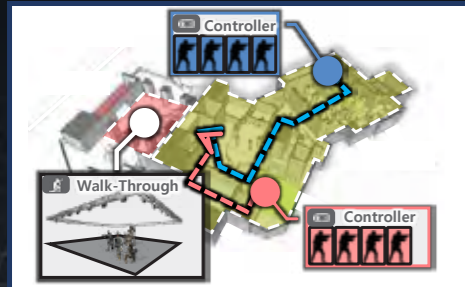
x 8 Multiplayer (Maximum of 8)

A Large Space Walk-Through Training

Hybrid VR integrated training implementation example

Training Editor & Monitoring System

# Large-space hybrid simulation training system based XR technology for strengthening of combat power



**HYBRID Virtual Movement**

Both large-scale tactical training and CQB (Close Quarter Battle) training are possible by mixing walk-through and controller operation methods.



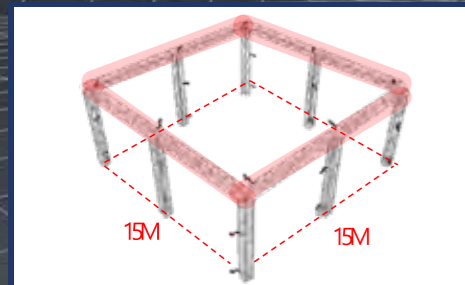
**Up to 8 multi-play**

Up to 8 or individual or team play



**Haptic & Real-like device**

Real-like gun Glove for hands tracking



**Large Space Virtual Training**

The Largest Training Area



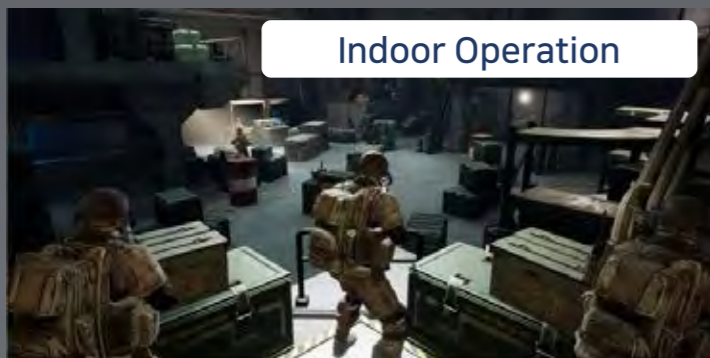
**Scenario Editor**

Detailed training settings such as environment, climate, AI, etc.



**Real-like Graphic**

High quality of graphic for real-like experience



**Indoor Operation**



**Outdoor Operation**

The world's first VR gun shooting game development and large space virtual reality training simulator specialized developer.

## Limitations of Existing Military Training

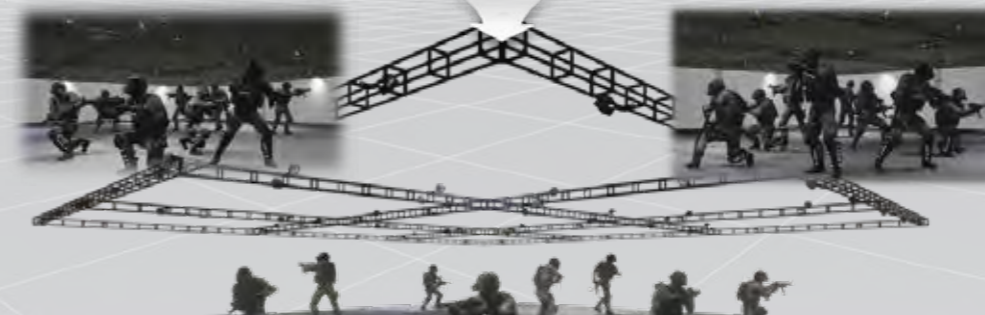
Increasing demand for advanced Science training

Limitations

Lack of location, cost, time & Training content

Lacking teamworking Training program

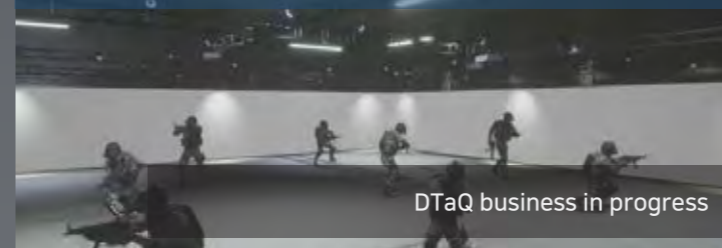
Testing facilities for a large space-based training



**Large-space hybrid simulation training system based XR technology for strengthening of combat power**

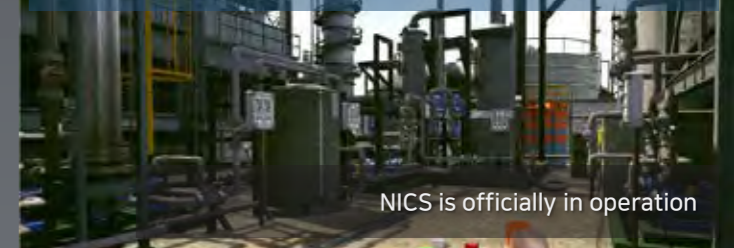


**special warfare virtual simulation training**



DTaQ business in progress

**Chemical accident response training**



NICS is officially in operation

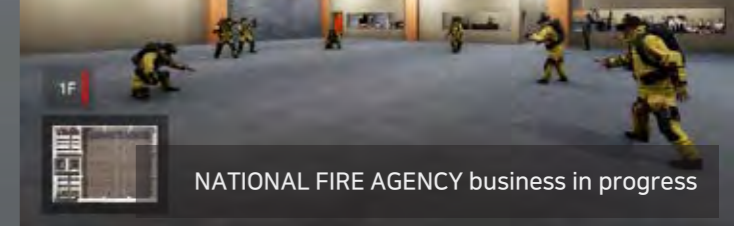
Possessing experience in supplying VR solutions to domestic and overseas VR experience zones, public institutions, and military bases.

**Police officer field response virtual reality training**



KOREA NATIONAL POLICE AGENCY business in progress

**Fire Situation Response Training**



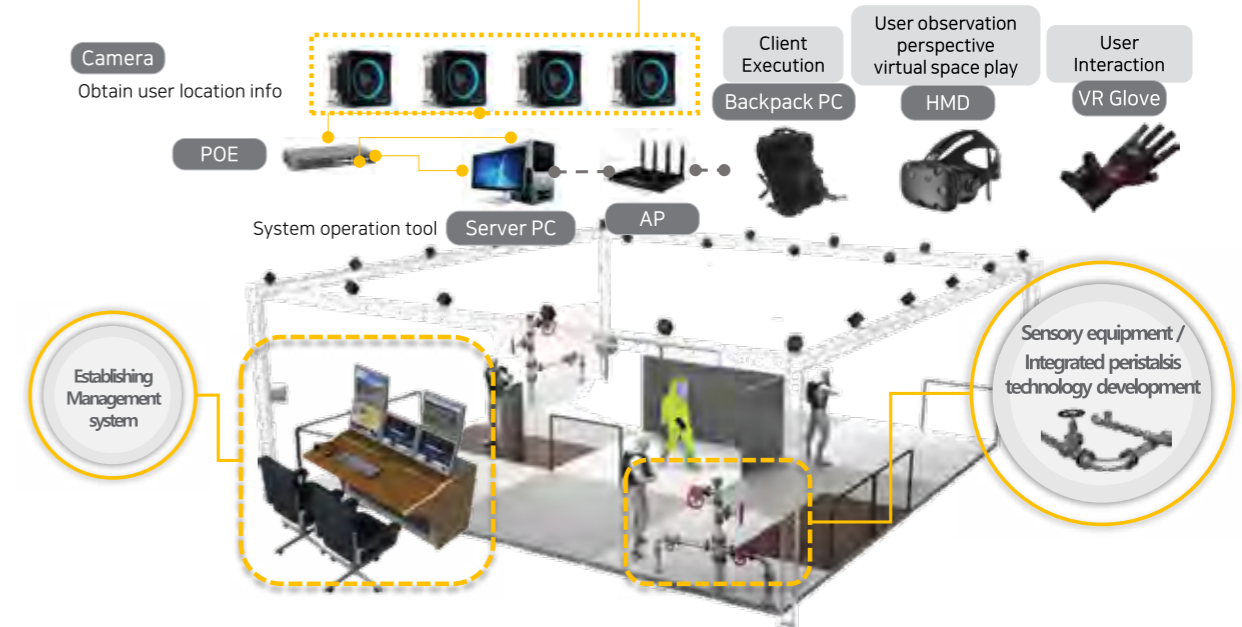
NATIONAL FIRE AGENCY business in progress



# COMPOSITION OF VR TRAINING SYSTEM

XR TRAINING SIMULATOR  
Response Training System for Chemical Leak Accidents

Track the motion of multiple users by utilizing a location tracking camera, establish a system that shares location information data generated from the trainee's equipment to the server



A training system based on real-time location and motion tracking using an optical motion capture camera

# OVERCOMING LIMITATIONS IN PHYSICAL

XR TRAINING SIMULATOR  
Response Training System for Chemical Leak Accidents

# CONTENTS

XR TRAINING SIMULATOR  
Response Training System for Chemical Leak Accidents

- Danger and hazards of the substance itself → Building a world that doesn't exist in reality
- Difficulty in Reproduction → Impossible manipulations are possible in VR
- Implementation of various incidents (equipment, process, etc.) → Optimization of training for specific functions
- Difficulty of experiencing → Able to have a realistic experience



<p>Chlorine Leak Response Scenario: For One Person</p> <p>Storage facility</p>	<p>Multi-collaboration response training</p> <p>Storage facility</p> <p>Charging facility</p>	<p>Multi-collaboration response training</p> <p>Hydrochloric acid factory</p> <p>Hydrofluoric acid factory</p>
--	---	--

- Training with 'Vive' VR Devices
- 17 scenarios according to the space of storage and charging facilities
- Chlorine: Consists of a total of 17 scenarios, Basic, Beginner, Intermediate progress sequentially according to the training scenario
- For the advanced, 1-5 people participate to solve various accidents through collaboration
- Hydrochloric acid & Hydrofluoric acid : Consists of a total of 22 & 20 scenarios each.
- Those scenarios have a lot of freedom of action
- For the advanced, 1-5 people participate to solve various accidents through collaboration

Content design/ Scenario production and inspection/ Training evaluation criteria and index design  
More than 60 training scenarios verified by experts

The world's VR gun shooting game development and VR·XR simulator specialized developer

Increasing demand for advanced training system

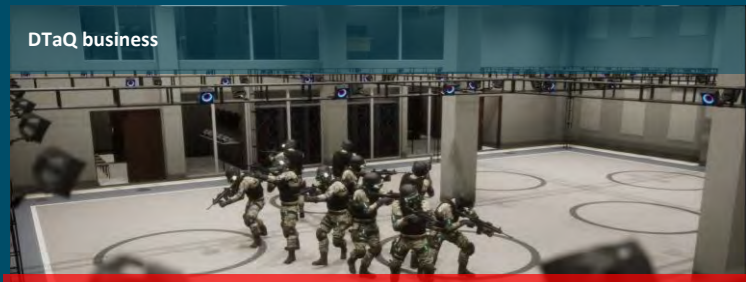
Limitations of existing system

Insufficient of cost, time & trainig contents

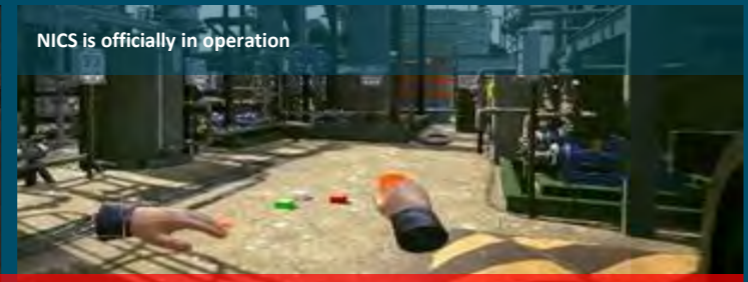


# POLICE ONE

XR technology tangible training system for law enforcement of police officers



DTaQ business



NICS is officially in operation

Skonec has supply experience in VR Solution to domestic public institutions, military and overseas VR game park



National Fire Agency business



Air Force Business



Virtual Reality program to law enforcement for police officers



Portable VR system





1SET

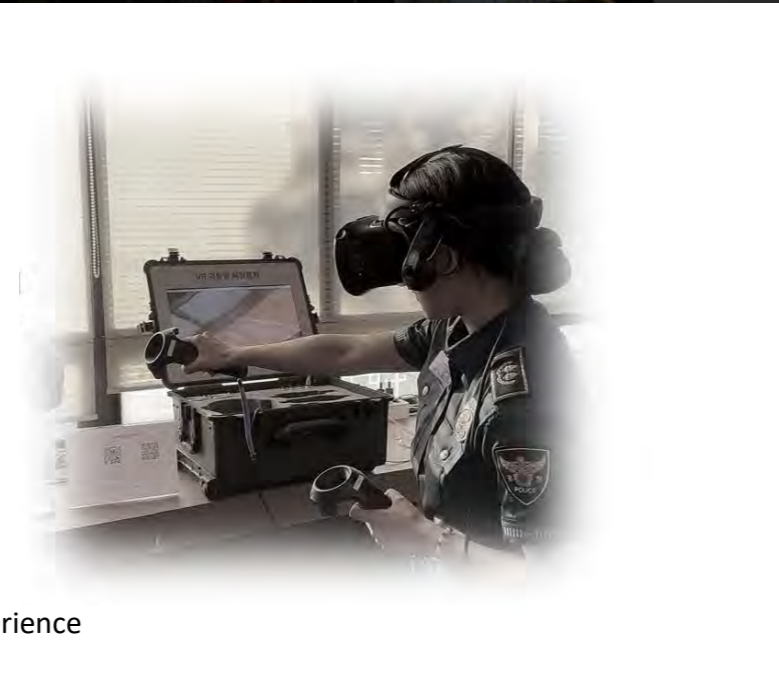
Touch-Monitor

PC

HMD

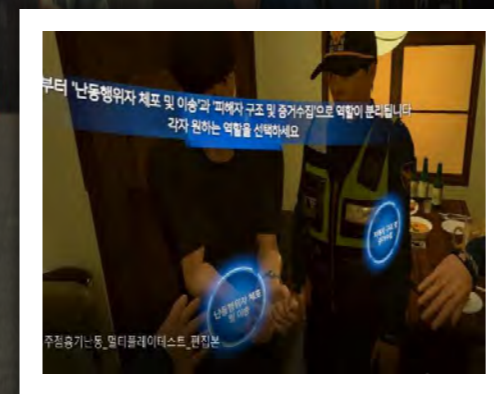
Integrated VR base station

-  Ensure stability in training  
Enables safer police education and training
-  Improved on-site response capabilities  
Achieve on-site response capabilities through VR
-  Time cost savings  
Train at the time and place you want
-  Spreading understanding of the police officer  
More easily understand and experience the police officer



# POLICE ONE

XR technology tangible training system for law enforcement of police officers



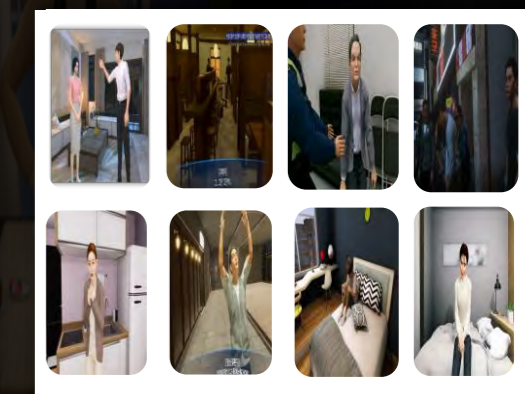
Cooperative Training system

Real-like cooperative training system, for two people



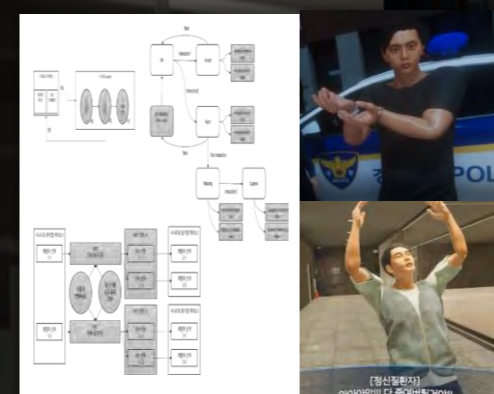
Portable VR training system

Portable VR All-in-One equipment



Variable multi-scenario

8 types of scenarios corresponding to actual sites in preparation for various sudden situations



Development of intelligent NPC behavior simulation

NPCs save behavioral information in the knowledge base system



VR GUI interface

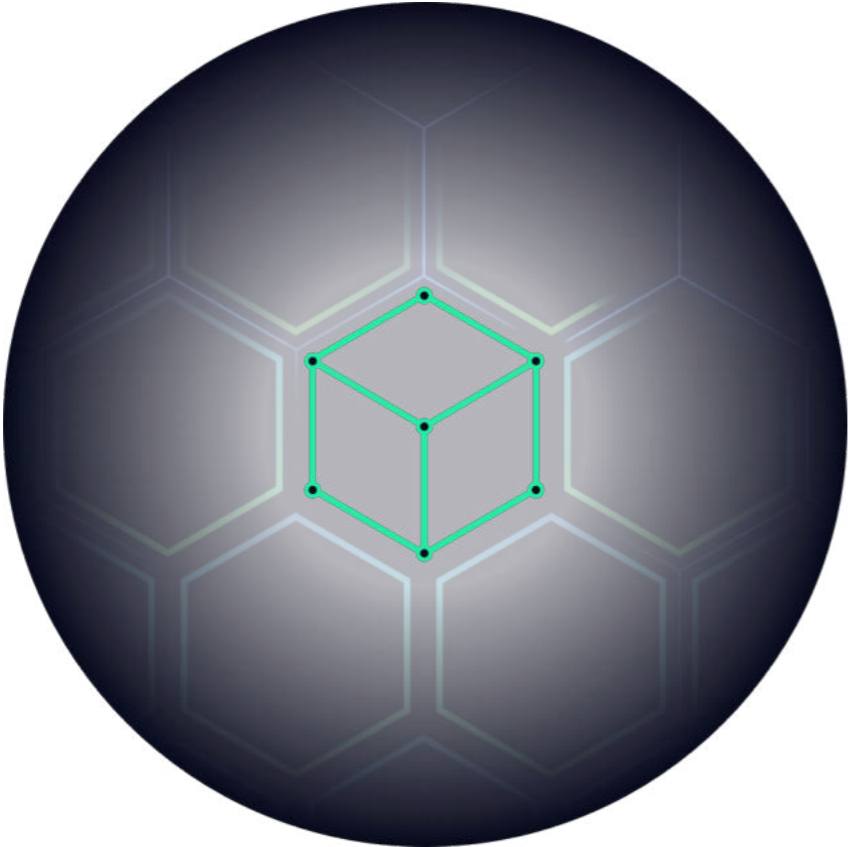
Set up an information space GUI that anyone can easily recognize



After action review system

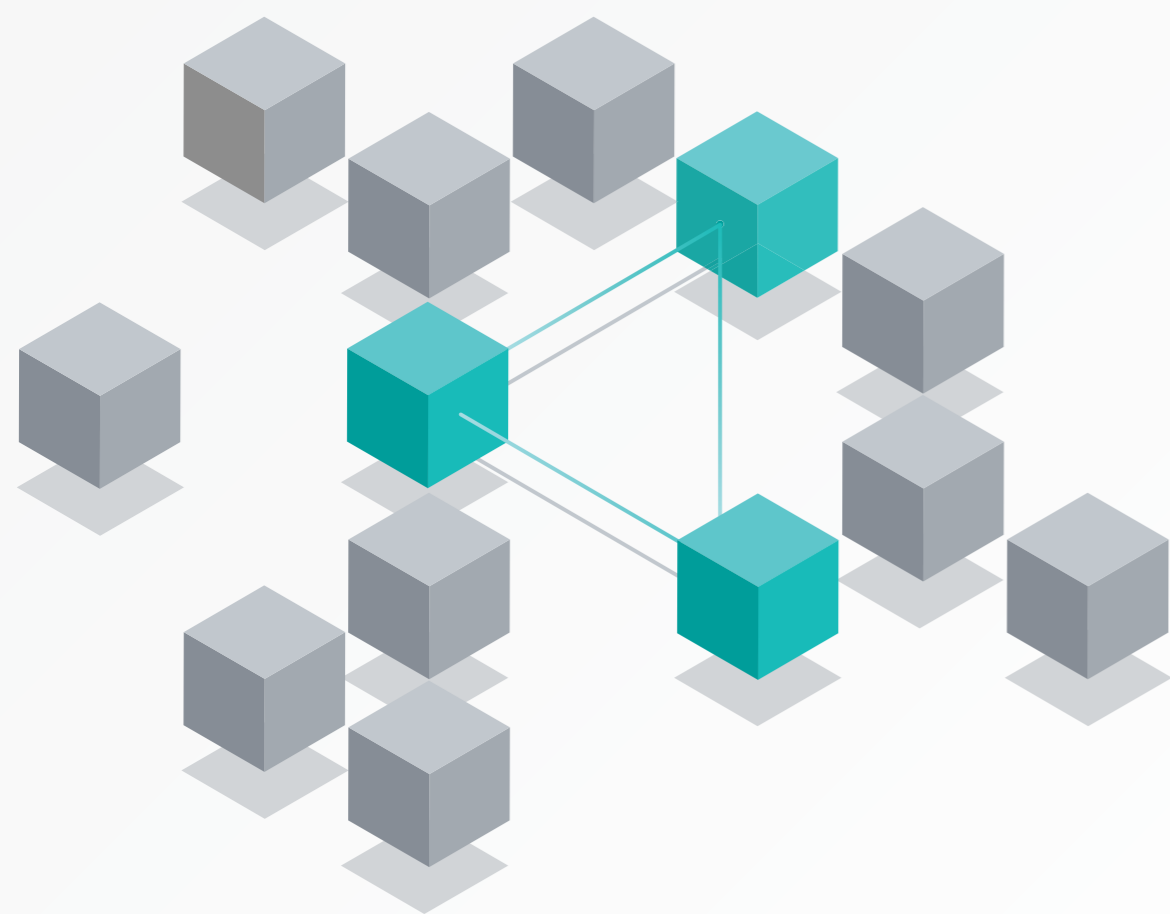
Trainee evaluation managing system

# Cyber Security



# 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



# 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

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

## Charging time

17 seconds

## Magnetic Field Generated

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

# ADC MagWiper MW-25X Degausser

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



Model: DEA-MW25000X

## Simultaneous Erasing Capacity

 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



### 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.

## 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.

# ADC MagWiper MW-30X Degausser

Large model can simultaneously 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)

# ADC 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



### 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.

## 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.



### 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.





**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





# 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



# DiskClon DC6000 Series

Disk Duplicator & Wiper

## Why DiskClon Needed?

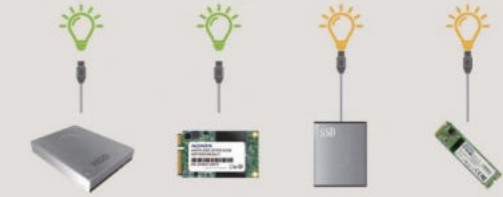
### 1 Mass media production & maintenance

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



### 2 Plug & Wipe

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



### 3 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



### 4 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 GyeongGiDo, Korea  
Tel. +82 70 7090 8280 Fax. +82 70 7016 2380 [www.clonix.com](http://www.clonix.com)

## Recruitment of Partner Company & Dealers



Contact [sales@clonix.com](mailto:sales@clonix.com)



# 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



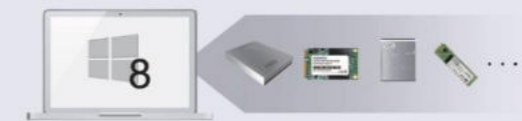
# NetClon NC1000 Series

Network-based Disk Duplicator & Wiper

## Why NetClon Needed?

### 1 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



### 2 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



### 3 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.



### 4 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](http://www.clonix.com)

Recruitment of Partner Company & Dealers



Contact [sales@clonix.com](mailto:sales@clonix.com)

# Blanco Drive Eraser for ITAD

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



## Technical Specifications

ERASURE	MINIMUM SYSTEM REQUIREMENTS
<ul style="list-style-type: none"> <li>Locally or remotely controlled data erasure via the Blanco Management Console</li> <li>High-speed, simultaneous erasure of multiple drives, including the ability to customize drive batch sizes and drive speed thresholds</li> <li>RAID dismantling and direct access to the underlying physical drives</li> <li>SSD detection and secure erasure with Blanco's patented SSD method</li> <li>Automated detection and unlocking of freeze locked drives</li> <li>Detection, notification and erasure of hidden areas (DCO, HPA) and remapped sectors</li> <li>Support for internal drive erasure commands, including cryptographic erasure and TCG feature set on self-encrypting drives</li> <li>Ability to reformat SATA and SAS drives after erasure</li> </ul>	<ul style="list-style-type: none"> <li>1 GB RAM memory in most cases (2 GB for PXE booting)</li> <li>Local erasure:               <ul style="list-style-type: none"> <li>CD/DVD drive or USB port for booting the software</li> <li>SVGA display and VESA compatible video card</li> <li>USB port for saving reports</li> </ul> </li> <li>Remote erasure (requires Blanco Management Console):               <ul style="list-style-type: none"> <li>Ethernet NIC</li> <li>DHCP Server running on local network for PXE booting, remote erasure and report collection</li> </ul> </li> </ul>

USABILITY	REPORTING
<ul style="list-style-type: none"> <li>Accelerated NIST Purge erasure</li> <li>Multi-tasking to allow the hardware diagnostics and updating the report during the erasure time</li> <li>Screensaver displaying the erasure progress to monitor the process remotely</li> <li>Resume an erasure that has been interrupted without consuming extra licenses</li> <li>Dedicated interface for loose drive erasure</li> <li>Support for LAN and WLAN networks, including 802.1x authentication</li> </ul>	<ul style="list-style-type: none"> <li>Digitally-signed Certificate of Erasure</li> <li>Choose between asset level or drive-level reports</li> <li>Save reports locally or send them through the network to the Blanco Management Console</li> <li>Detailed reports enabled by enhanced hardware detection</li> <li>Extensive erasure information, including HDD details for seamless audit procedures</li> <li>User extendable report (with option to add "custom fields")</li> </ul>

DEPLOYMENT	HARDWARE DETECTION & DIAGNOSTICS	CONFIGURABILITY & AUTOMATION
<ul style="list-style-type: none"> <li>Blanco Drive Eraser is platform independent</li> <li>Local control with HASP dongles, standalone images, or centralized control through the Blanco Management Console or Blanco Cloud</li> <li>Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)</li> </ul>	<ul style="list-style-type: none"> <li>13+ hardware tests, including: RAM, CPU, Motherboard, Battery (current capacity &amp; discharge), PC Speaker, Display, Pointing Devices, Keyboard, Optical Drive, Webcam, USB Ports, WiFi card, SMART Tests for drives, BIOS logo</li> <li>Hot swap capabilities</li> <li>Backwards compatibility with other Blanco products (BDECT, BMC, BUSBC)</li> </ul>	<ul style="list-style-type: none"> <li>Customize erasure software to fit specific needs</li> <li>Customize input fields in erasure reports</li> <li>4 levels of process automation: workflow, manual, semi-automatic, automatic</li> <li>Ability to communicate back and forth with an Asset Management System or other external system (IBR workflows) on asset and drive level</li> <li>Fine-tune erasure process (speed/time limit, configurable conditions, etc.)</li> <li>Execute customized workflows defined on the Blanco Management Console or Blanco Cloud, locally or remotely; automate the processing across all company assets</li> </ul>

HARDWARE SUPPORT	AUDITING	LANGUAGE SUPPORT
<ul style="list-style-type: none"> <li>Erase data securely from PCs, laptops, servers and storage environments based in x86 and x86-64 architectures</li> <li>BIOS &amp; UEFI machines including Intel-based Macs, Apple T2 and Secure Boot</li> <li>IDE/ATA, SATA, SCSI, SAS, USB, Fibre Channel, FireWire hard disk drives of any size/blocksize</li> <li>SATA and SAS solid state drives of any size/blocksize</li> <li>eMMC drives of any size/blocksize</li> <li>NVMe drives of any size/blocksize</li> <li>SAS, SCSI, ATA and NVMe self-encrypting drives</li> </ul>	<ul style="list-style-type: none"> <li>Verification algorithms to automatically check the overwritten patterns</li> <li>Hexviewer provides fast visual verification of the erasure for compliance</li> <li>Reports offer tamper-proof reporting and can include a customized digital signature</li> <li>Embed reports in the drives for a fast erasure audit</li> <li>Search and export reports via APIs</li> </ul>	<ul style="list-style-type: none"> <li>English, German, Japanese, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian</li> <li>Up to 20 different keyboard layouts supported</li> </ul>

## Why Blanco

Blanco is the industry standard in data erasure and mobile device diagnostics software. Blanco 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.

Blanco 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](#)

## Blanco 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 Blanco Drive Eraser, organizations can add an essential level of protection to endpoint security policies by permanently erasing sensitive data from HDDs and SSDs, including NVMe 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 NVMe, 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 Blanco 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

# Demi PG520

## Super Handy SATA Duplicator



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.

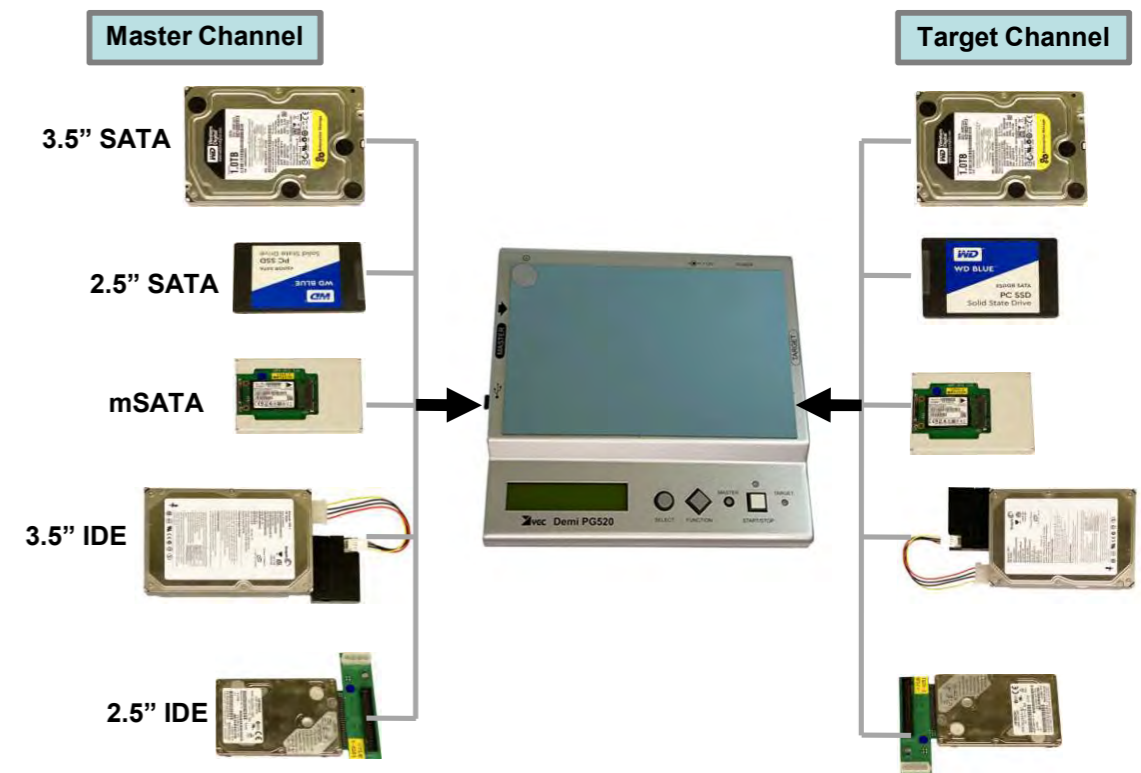


# DEMI PG520

## 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



## 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°C (50 - 95°F) Humidity 30 - 80% No Condensation



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

See more in the back

For more information, please visit [www.yecglobalsolutions.com](http://www.yecglobalsolutions.com) or call (657) 298-3276.

[www.yecglobalsolutions.com](http://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

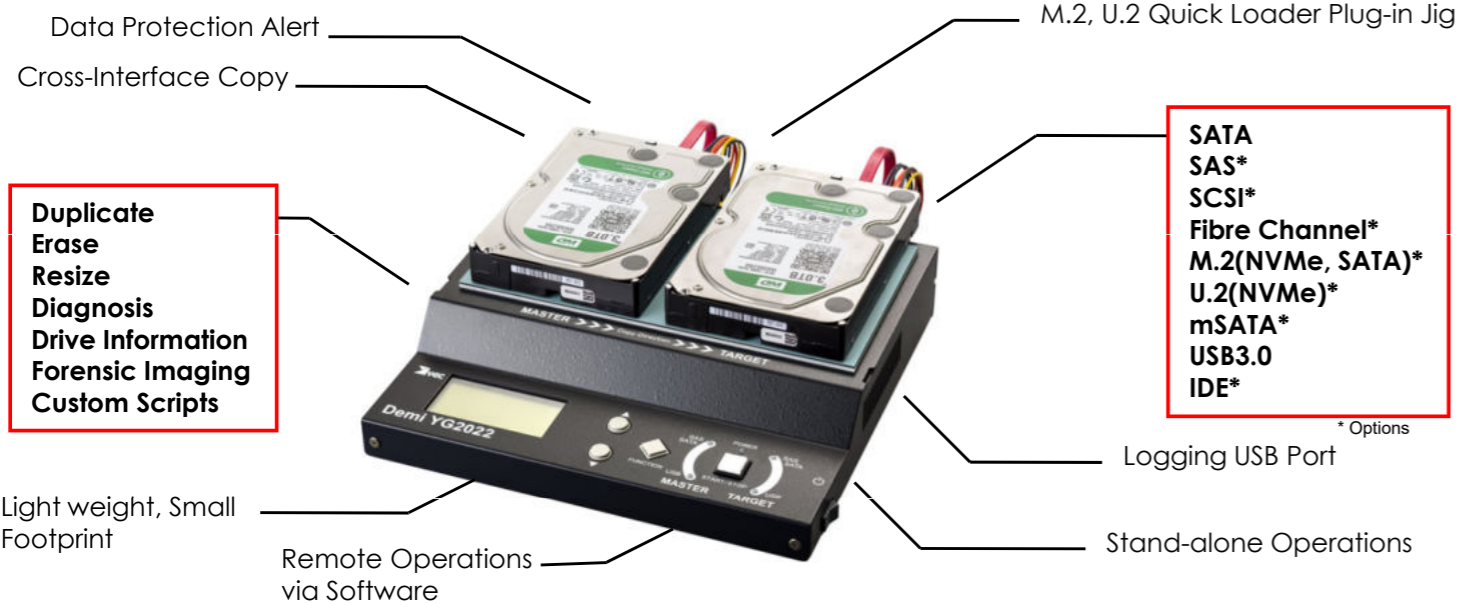
\* The specifications and design of the product are subject to change without notice.

[www.kk-yec.co.jp](http://www.kk-yec.co.jp)

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

# 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 accelerates the process speed to the limit. In addition, Demi YG2022 is capable of connections with **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.

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

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

[www.yecglobalsolutions.com](http://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](http://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.

2111 104

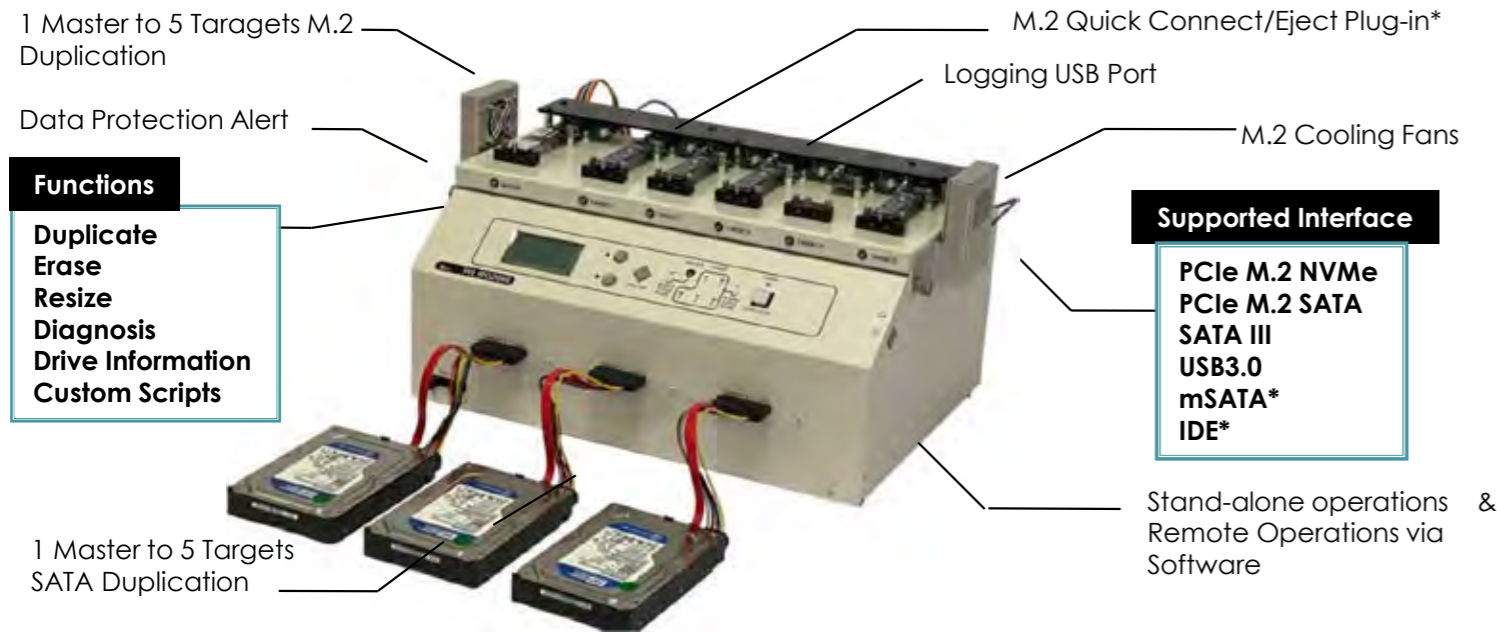


"Trusted by digital technology professionals for over three decades."

For more information, please visit [www.yecglobalsolutions.com](http://www.yecglobalsolutions.com) or call (657) 298-3276.

# HIT MG2061

## SATA & PCIe M.2 Duplicator Eraser



**Functions**  
 Duplicate  
 Erase  
 Resize  
 Diagnosis  
 Drive Information  
 Custom Scripts

**Supported Interface**  
 PCIe M.2 NVMe  
 PCIe M.2 SATA  
 SATA III  
 USB3.0  
 mSATA\*  
 IDE\*

\* SATA plug-in jig option available

Backed by 35 years of expertise and engineering in digital storage technology, HIT MG2061 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 x4. 179GB/m\*** tested read speed by M.2 NVMe device. SATA III and USB 3.0 are supported natively as well. Legacy interface as IDE\*\* and mSATA\*\*, are also supported. (\*varies by device) (\*\* optional)

### Efficient with M.2 Quick Connect/Eject Plugin and Cooling Fans

YEC's proprietary M.2 Quick Connect/Ejector makes connection quick and easy reliably for M.2 device size of 2230, 2242, 2260, 2280 and 22110. Cooling fans improve data transfer performance. Ask for optional SATA Quick Connect/Eject jig.

### Slow Drive Elimination – Reliable Performance

User can specify minimum transfer speed for duplication. When one of the drives performs slower, the total duplication time gets prolonged. In order to avoid speed drop coming from this, HIT MG2061 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 run automatically thus achieving the fastest completion possible. Using the real-time transfer rate displayed in the control screen, operator can abort the slow drive manually without interrupting other drives being processed as well.

### Proactive Data Protection Against Unintended Overwrite

It would be a shocking moment when realizing critical data is overwritten and lost unintentionally! HIT MG2061 proactively checks target drives before proceeding to the overwrite mode and alerts the user of potential eventuality

### Reporting

**Detailed logs** are automatically generated, recording every step of process events. Logs can be utilized for process and error analysis. Simultaneously all process events are saved in **CSV database** useful for various purposes and analyses. **Work Report** template is customizable allowing rearrangement of data field layout as many as needed.

### More Than A Duplicator

Multi-interface duplication is not the only advantage MG2061 offers. As an all-round solutions tool, it erases, resizes, and diagnoses to get critical jobs done just in one machine.

### NIST 800.88 Sanitize Standards Compliant

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

### File System and Mapping Copy 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

M.2 jig board is so easy to replace. No tools required. All it takes is remove and put back on with one thumb screw.

### Increase Power With Software

Optional software adds advantages furthermore in using HIT MG2061. It executes a script remotely, creates log files, work reports and CSV database and saves them in PC. Sold separately.

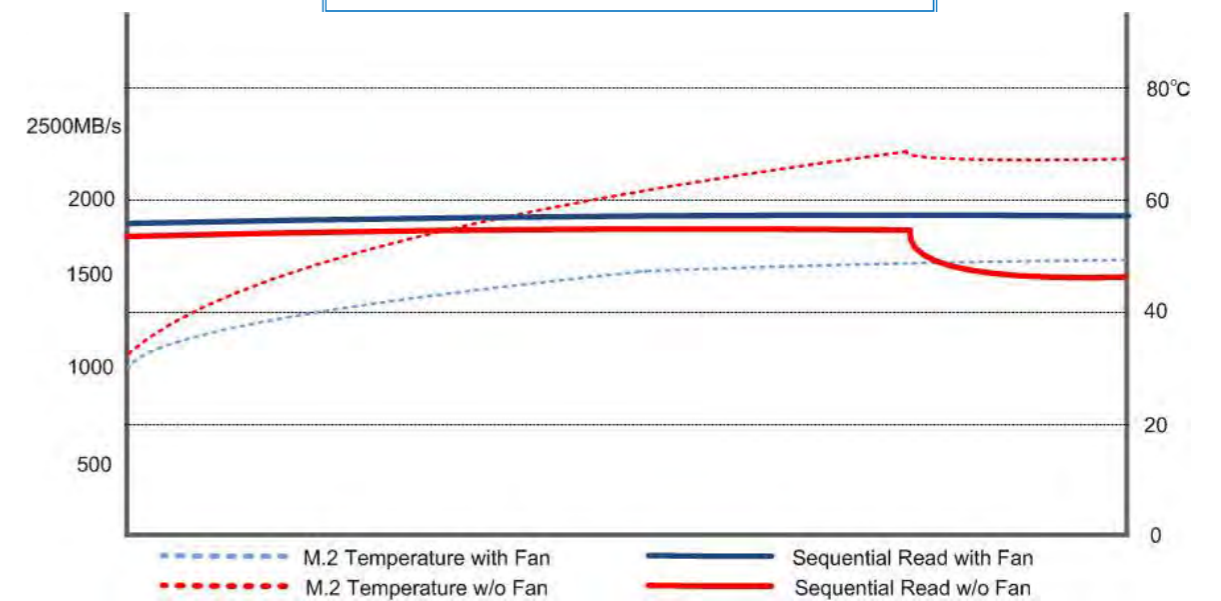
See more in the back

# IIIT MG2061

## FEATURES

- **DUPLICATION** All copy, Compare, Error skip copy, Reverse copy, Range copy, Data only copy, MAP copy, Cross-interface copy
- **ERASURE** NIST 800.88 Purge and Clear, DoD 5220.22-M, Security Erase, One time Erase, Multi-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 \* (\*optional software required)
- **RECOMMENDED USE:** ITAD, Manufacturing, Testing Labs, Health Care, Education, Defense

## EFFECTIVENESS OF COOLING FAN



## SPECIFICATIONS

	Descriptions
<b>Model</b>	HIT MG2061
<b>Part No.</b>	Y-2531
<b>Supported Interface</b>	M.2 (NVMe, SATA) SATA 6G USB3.0
<b>Optional Interface</b>	IDE, mSATA
<b>Port Connections</b>	1 to 5 duplication, 6 x erase
<b>Dimensions</b>	L17 "x W12" x H9" (430 x 310 x 234mm)
<b>Weight</b>	23lb (10.5 kg)

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

[www.yecglobalsolutions.com](http://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

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

[www.kk-yec.co.jp](http://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



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

For more information, please visit [www.yecglobalsolutions.com](http://www.yecglobalsolutions.com) or call (657) 298-3276.

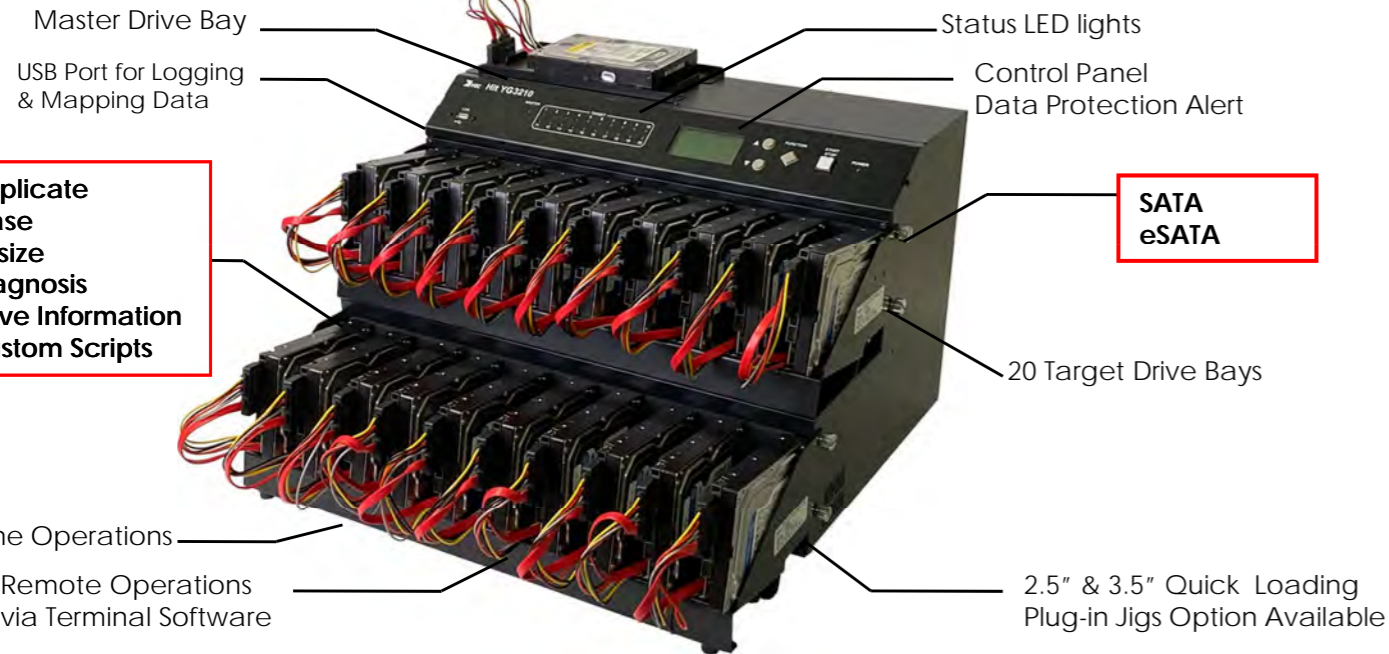
# HIT YG3210

## Industrial Grade SATA Duplicator

# 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



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.



Status Indicator LED



Detachable Plug-in Jig Option

**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.

### SPECIFICATIONS

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

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



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

\*Varies by device model  
\*\* Options

[www.yecglobalsolutions.com](http://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](http://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.

For more information, please visit [www.yecglobalsolutions.com](http://www.yecglobalsolutions.com) or call (657) 298-3276.

# 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	<b>DEZ-HS1000</b>
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



## Shredding Particle Size

18mm \* random

## Security Level (DIN 66399)

**H-4**

## Shredding Capacity

200 pcs / hr

## Feeding Ports



## Shredding blade



## Shredding size



## Control panel



## Specifications

Model	DEZ-HS2800
Shredding materials	Hard Disk / Solid State Drive / CD / Floppy / Mobile / 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

## 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.



# Standard Combo Hard Disk Shredder

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



## Supported Media



## Shredding particle size

20mm or 5mm

## Security Level (DIN 66399)

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

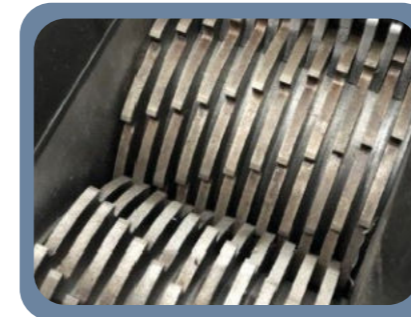
## Shredding Capacity

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

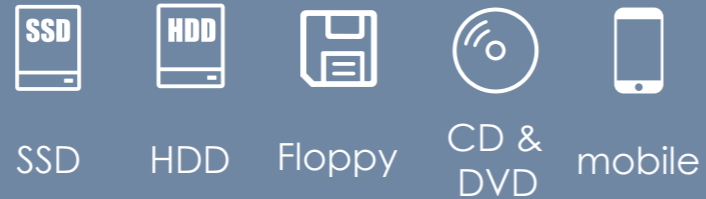


# Combo hard disk Shredder

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



## Supported Media



## Shredding particle size

18mm or 9mm

## Security Level (DIN 66399)

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

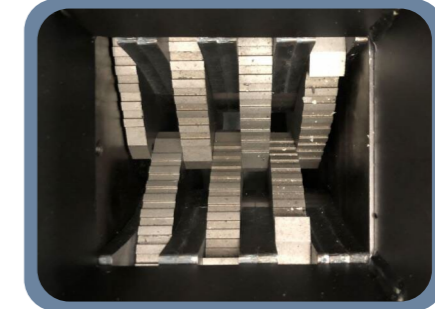
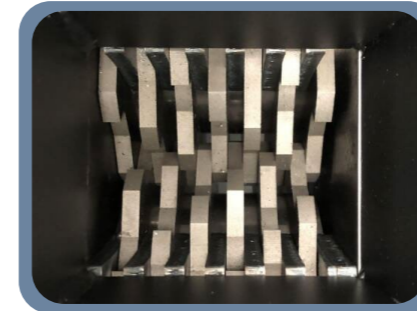
## Shredding Capacity

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





# H5 Level hard disk Shredder

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



### Supported Media



### Shredding particle size

More than 80% in 9\*9mm

### Security Level (DIN 66399)

H-4 H-5

### Shredding Capacity

>120 pcs / hr

### 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 120 pcs 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 320mm <sup>2</sup>
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



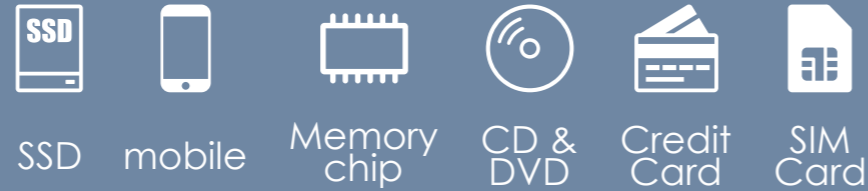


# Flash, SSD & Mobile Phone Shredder

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



## Application



## Shredding Particle Size

2\*2mm

## Security Level (DIN 66399)

E-4

E-5

## Shredding Capacity

150 - 200pcs / hr

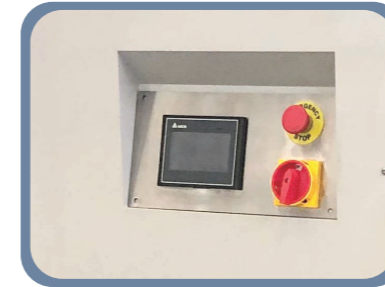
## Other Advantages

- 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.

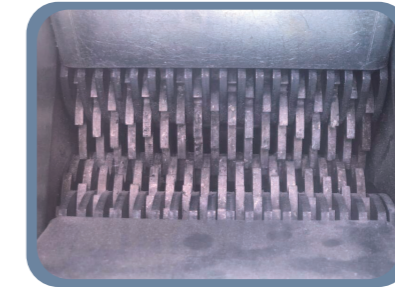
## Shredding size



## 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

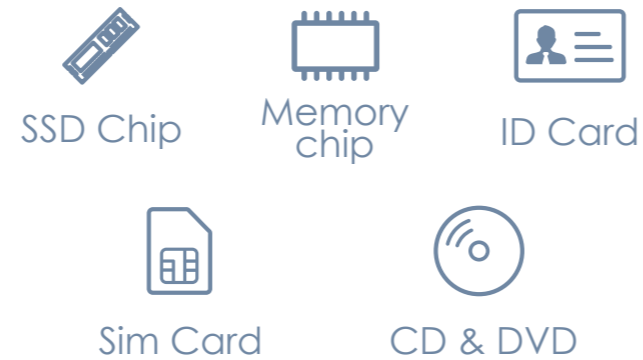




# Circuit Board & Chip Disintegrator

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

## Supported Media



## Shredding Particle Size

Optional  
A. 0.5\*0.5 mm<sup>2</sup>  
B. 1\*1 mm<sup>2</sup>  
C. 2\*2 mm<sup>2</sup>

## Shredding Capacity

5 - 10kg / hr

Crushing size



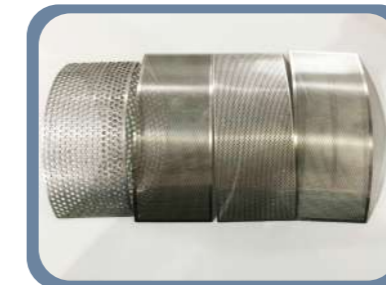
Shredding blade



Electrical cabinet



Screen mesh



Filter system



## Specifications

Model	<b>DEZ-SPD2</b>
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*2mm <sup>2</sup> 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

## Advantages

- Shred into small partucles.
- Optional shredding particle size with 0.5\*0.5 / 1\*1 / 2\*2 mm<sup>2</sup> 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.



# 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



Shredding size



Side view



Shredding blade



Back view



Control panel

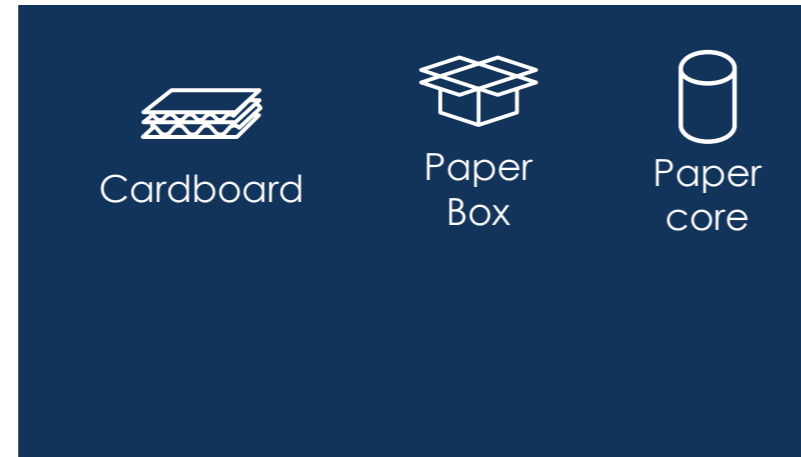


## Specifications

Model	<b>DEZ-SPT5</b>
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	About 3 300kgs
Characteristic	With electrical control cabinet, planetary gear box, one year warranty



## Industrial Cardboard Shredder



## Product Details



Shredding Blade



Chain Wheel



Motor



Shredding Particle



Control Panel



Side View



**Shredding Capacity**  
500-1000 kg/hr



**Max. Feeding Width**  
1500mm



**Max. Thickness**  
80mm

## Advantages

- Triple-shaft design for guaranteed feed of any paper type.
- Long-lasting blades forged from premium, specially hardened steel.
- High-strength, specially profiled blades efficiently capture and destroy cores.
- An intelligent control system ensures safe and reliable operation.
- Integrated with air aspiration and hydraulic baling systems.

## Specifications

Model	DEZ-IPS1500
Shredding construction	3
Shredding materials	Cardboard, paper, box and paper core
Max. Cardboard Feeding Width	1500mm
Max. Paper Core Diameter	220mm
Max. Paper Core Thickness	30mm
Max. Cardboard Thickness	80mm
Blade Shaft Rolling Speed	480 r /min
Shredding Capacity	500-1000 KG/hr
Power	15KW /380V Three Phase /60HZ
Waste collection bin	30L
Machine size	2130 (L)x1630 (W)x1849 (H) mm
Machine weight	2800Kg

# Data Expert™ Server Hard Disk Shredder

Powerful server hard disk and desktop shredder.



## Application



## Shredding Particle Size

20\*40 - 90mm<sup>2</sup>

Security Level (DIN 66399)

H-4

## Shredding Capacity

More than 300 pcs / hr

\* Optional Recording System

## 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



## Waste collection Bin



## Shredding size



## Feeding Conveyor



Model: DED-SHS

Shredding materials	SSD, HDD, mobile phone, CD, floppy disk, USB drive, tape
Shredding particle size	20 * 40 - 90mm <sup>2</sup>
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

ISO/IEC 21964  
DIN 66399



# CD & Paper Shredder

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. 160mm<sup>2</sup>  
&  
Strip Width  
max. 6mm

## CD & Paper Shredder (4x40mm<sup>2</sup>) 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

**O-3**

Particle size  
max. 160mm<sup>2</sup>

**P-5**

Particle size  
max. 30mm<sup>2</sup>  
&  
Strip Width  
max. 2mm

## CD & Paper Shredder (2x15mm<sup>2</sup>) 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

**P-6**

Particle size  
max. 10mm<sup>2</sup>  
&  
Strip Width  
max. 1mm

## CD & Paper Shredder (1x2mm<sup>2</sup>) 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

**O-4**

Particle size  
max. 30mm<sup>2</sup>

Protection class 1 : Normal Protection for Internal Data

Protection class 2 : Higher security for confidential data

## 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/m <sup>2</sup> )	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 mm<sup>2</sup>

## Security Level (DIN 66399)

O-6

## Shredding Capacity

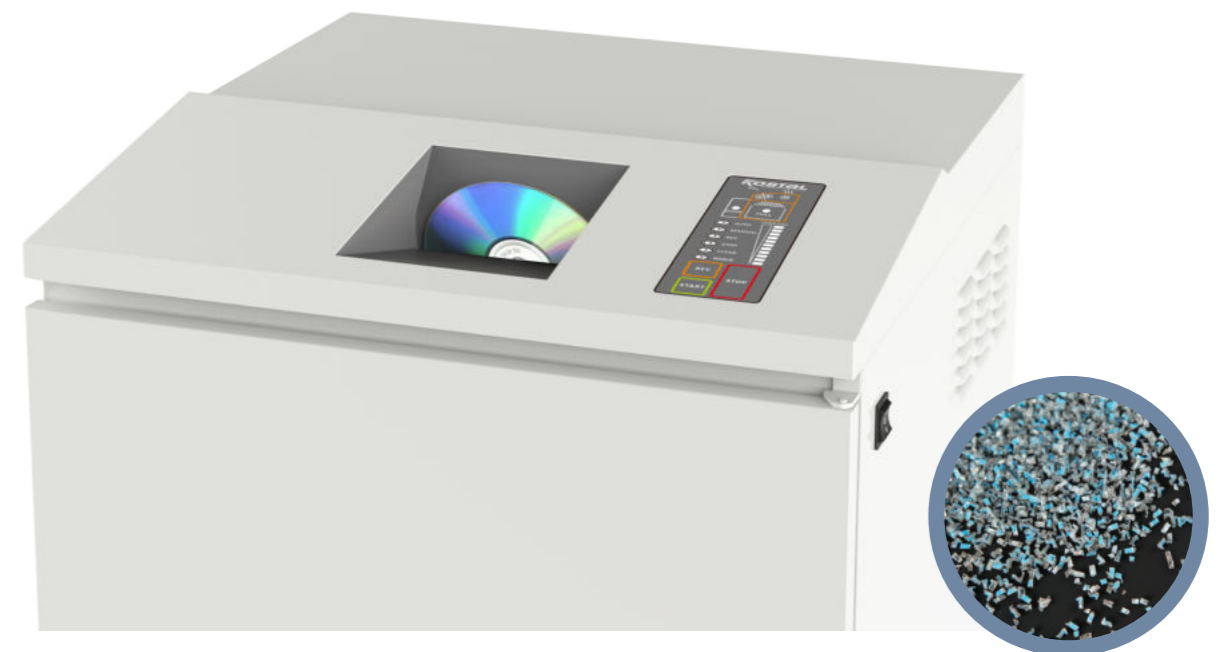
1000 pcs / hr

## 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 mm <sup>2</sup>
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

1.6 \* 4 mm<sup>2</sup>

Paper

1 \* 5 mm<sup>2</sup>

## Security Level (DIN 66399)

O-5

P-7

## Shredding Capacity

CD

600 pcs / hr

Paper

4,800 pcs / hr

## Advantages

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

### Model: DED-CDPS

Shredding materials	CD & DVD, Paper
Shredding particle size	Paper: 1 * 5 mm <sup>2</sup> CD: 1.6 * 4 mm <sup>2</sup>
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



# HDD Crusher

## Level H-3 Hard Drive Crusher

### Listed on NSA/CSS EPL for Hard Disk Destruction Devices

Model No. : DED-HDC01



- A** Easy to use operator interface
- B** Delivers 12,000 pounds of force

#### 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

#### 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

# 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.

#### Security Engineered Machinery

©2021 Security Engineered Machinery | All rights reserved  
 SS-022 | 02.15.2021

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



5 Walkup Drive  
 Westboro, MA 01581  
 800.225.9293 | 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:

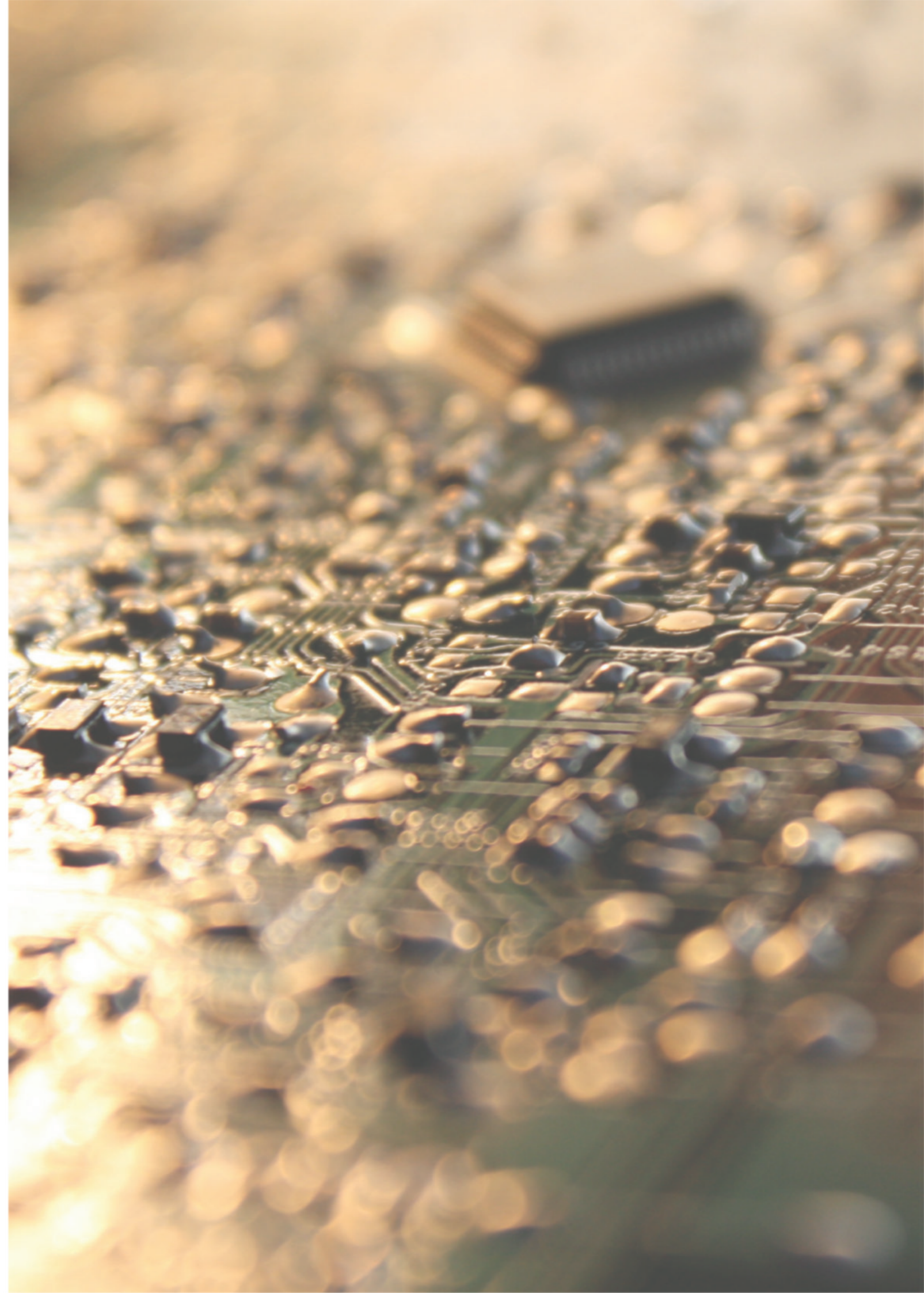
- Anti-static collection bags
- Oil packs



### 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.



# DataExpert Asia

## Singapore (Headquarter)

DataExpert Technology Pte Limited

## Hong Kong

DataExpert Technology Limited

## South Korea

DataExpert Technology Korea Co., Ltd.

## Indonesia

PT. DataExpert Technology Indonesia  
PT CYBER XPERT NUSANTARA

## Malaysia

DataExpert Technology Sdn.Bhd.

## Canada

DataExpert Technology (Canada) Inc.

## Thailand

DataExpert (Thailand) Company Limited

## Philippines

DataExpert (Philippines) Company Limited

## China

DataExpert Technology Limited (Shenzhen, China)  
Foshan DataExpert Technology Ltd

## Macau

DataExpert (Macau) Co., Ltd.



TECHNOLOGY MAKES POSSIBILITY

