



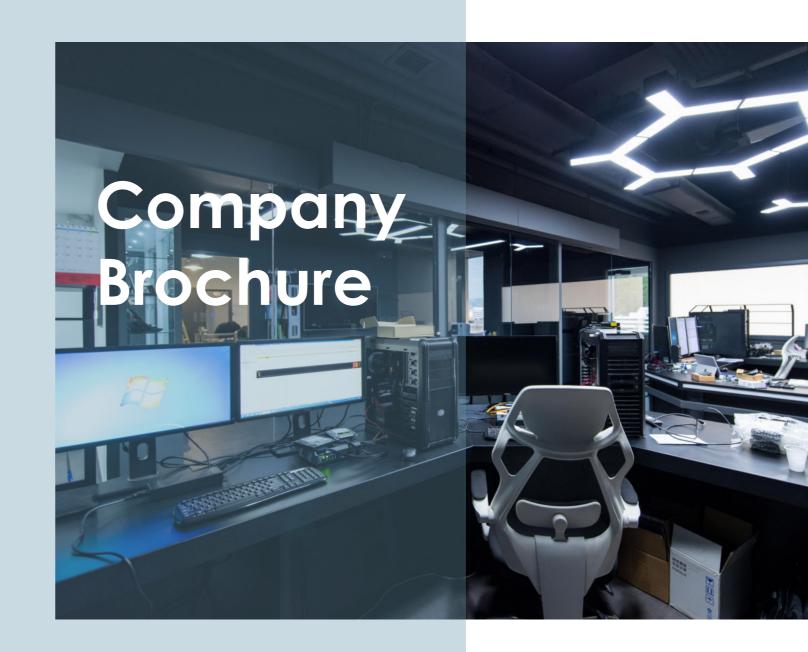
Singapore | Thailand | Philippines Hong Kong | Macau | Shenzhen | Guangzhou | Shanghai



www.dataexpert.asia



info@dataexpert.asia







## **About Us**

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

# **Our Offices**



### **Our Business**

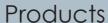
# Digital Forensics and Incident Response(DFIR)



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

### We provide...







Services



Laboratory

# IT Asset Disposition(ITAD)



Inappropriate discard out-of-date IT asset may lead to the risk of data leakage.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

### We provide...







Services



### **Digital Forensic Products**

Cyber MZR-DT Workstation



Cyber MZR-DI Workstation (Keyboardless) (With keyboard)
Digital forensic workstation On-scene forensic workstation On-scene forensic workstation



Forensic Cube V4



Forensic Cube V4 Digital forensic laptop





Talino 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 forension imager with 26 ports



Portable Write Blocker Series Compact write blockers DE Forensic Write Blocker Multi-interface write blocker



Forensic Laptop





PC imaging without dismantling Digital incident investigation software

cloud forensic tool

Computer and mobile extraction tool

Belkasoft X
Computer, mobile and
Computer, mobile and
Computer and mobile averaged problem of the computer and mobile averaged problem. Control of the computer and mobile averaged problem.

**Mobile Forensic** 



MD-RED

**GMD SOFT** 













MOBILedit Forensic Express MOBILedit Cloud Forensic Elcomsoft Mobile Forensic Bundle Cyacomb Mobile Device Triage at a extraction and analysis software Solution for cloud extraction Acquisition, decryption and analysis software Triaging software for mobile devices

#### **IOT Forensic Solution**



GMDSOFT MD-DRONE Drone extraction and analysis software



GMDSOFT MD-VIDEO Video extraction and analysis software



GMDSOFT MD-CLOUD Cloud extraction and analysis software



Evidence Preservation and Reception Workbench Conference Table

Evidence preservation and reception workbench Digital forensic lab furniture

**MOBILedit Smartwatch Forensics** Smartwatch extraction kit



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

#### **Data Recovery**

macOS Forensic





ruSolut VNR GMDSOFT MD-READER Chip-off data recovery and analysis solution Chip-off memory extraction hardware



Regen-i Rework Station

#### **Digital Forensic Lab Solution**



Examiner Work Desk



L-shape Workbench





3-Person 120° Workbench

Disassembly and Repair Work Table

Device disassembly work table



3-Person Long Workbench



Smart Evidence Locker



Evidence locker with recording function Digital forensic lab display

### **ITAD Products**

#### **Degaussers**





MaaWiper MW-15X 17-second charged degausser



MaaWiper MW-25X without remove the mounting brackets



MaaWiper MW-30X or 51 units of 2.5" HDDs simultaneiusly

#### Hard Disk Shredder / Crusher



Standard Hard Disk shredder





Standard Combo Hard Disk Shredder Small server hard disk shredder for office use 20mm and 5mm combo blade shredder for office use



**CD & Paper Shredder** 





Industrial F-Waste Shredder -waste solution for computers and printers NSA- and DoD-compliant HDD crusher

1x2mm<sup>2</sup> - 25 sheets

P7 CD & Paper Shredder





Circuit Board & Chip Disintegrator

#### **Duplicator & Wiper**



Blancco Drive Eraser Data sanitization solution

Super compact SATA duplicator

4x40mm<sup>2</sup> - 35 sheets



2x15mm2 - 30 sheets

Light weight duplicator and wiper



1x2mm<sup>2</sup> - 5 sheets

P7 CD & Paper Shredder

Network-based Disk Duplicator & Wiper



Dependable and versatile duplicator



Disk duplicator & wiper



PCle M.2 & SATA duplicator



Disk duplicator & wiper



Industrial grade SATA duplicator.













# 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:



Employees fraud



Investigation of personal computer



Private investigation of cellular phone



Inappropriate data duplication



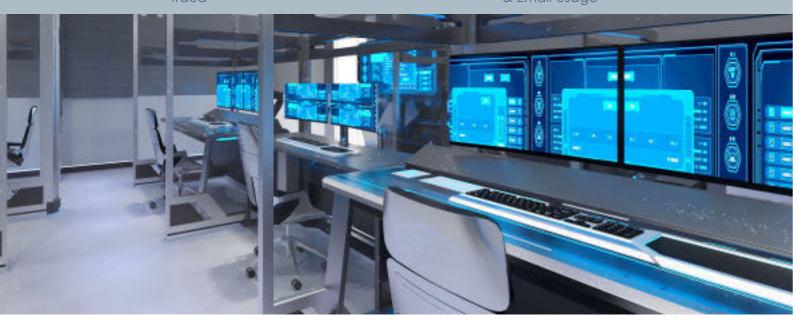
Intellectual property fraud



Breach of contract



Inappropriate Internet & Email Usage



# Digital Forensics Procedure

# **ACQUISITION**



Evidence Identification



Triage



Collection



Preservation

## **ANALYSIS**



Pictures and Videos



System Registry



Email



Mobile APPs



Ps Browsing History



Instant Messengers



Office Documents



Peer-to-peer Platform



Data Recove



Encrypted Files

### REPORTING





Court Testimony









### Our Services



### 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**



- Actions taken should not affect the integrity of original data
- Investigator conducting examination must be well trained and positioned at senior
- 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
   Belkasoft Certified Examiner (BelkaCE)
- HancomWITH Certified Mobile Forensic Professional
- Meiya Pico Certified Examiner of Mobile Forensic System
- Meiya Pico Certified Examiner of Forensic Master
- Certified Information Systems Security Professionals (CISSP)
- Microsoft Certified System Engineer + Internet (MCSE+I)

- SUMURI Mac Forensics Examiner
- Magnet Certified Forensic Examiner (MCFE)
- 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.



## Our advantages









### **Our Promise**

## Your data is unparalleled safe in DataExpert



- DataExpert Technology Limited got ISO/IEC 27001:2013 Information Security Management certified by BSI under certificate number IS 642998, for the scope of "The provision of data recovery and disposal services".
- We shall treat all material supplied by the client as confidential and shall not divulge any confidential information to any person.
- All employees in DataExpert have signed NDA and guarantee not to disclose any client information.

## Types of Failures



#### Logical Failure

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

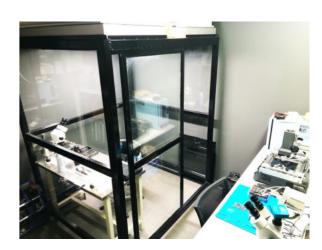


### Physical Failure

- Wear and tear of parts
- Collision
- Flooding
- Fire
- \* Open case checking or chip-off data recovery may be needed

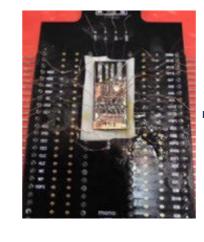
### Class 100 Cleanroom

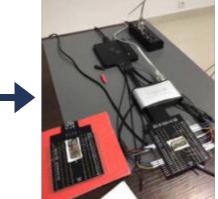
As to maximum the chance of recovering your data, DataExpert is beware on every step may affect the possibility of data recovery. The contaminants in the air can cause physical media damage and destroy the data if the hard disk open in normal surrounding. Therefore, DataExpert setup a Class 100 Cleanroom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



## Chip-Off Data Recovery

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









# Data Solution ISO/EC 27001 Information CERTIFIED

### Support Types

### Media

- Hard drive, micro drive, RAID, NAS, SAN, etc
- CD/DVD/Blue ray optical disc
- PC, tablet, cellphone, smartphone
- SSD drive, CF, SD card, Mico SD, MS, USB drives

### OS

- Windows 2000/XP/Vista/7/8/10/11
- Windows 95/98/98SE/ME
- Mac OS
- Unix, Linux
- Novell NetWare
- All database systems

### File

- Pictures and videos
- Browsing history
- Instant messengers
- Peer-to-peer software
- System files

- 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
- Windows NT/Server2003/Server2008/Server2012
- DOS/Windows 3.X
- APFS
- o iOS, Android, Windows Mobile, Symbian, etc
- OS/2
- Emails
- Mobile applications
- Office documents
- Windows registry
- Encrypted files

## Implementation Plan

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

### Work Flow



### Consultancy

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



Media Collection

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



**Analysis** 

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



Analysis Report & File List

• Generate a list of file that can be recovered.



**Data Recovery** 

• IT engineer will recover the files assigned by client.



Delivery

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



Technico 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).



### 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



# Why Digital Forensic Laboratory is Needed?

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

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



Enhance digital forensics capabilities in high-tech crimes investigation.

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











# 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



Disassmembly and Repair Worktable

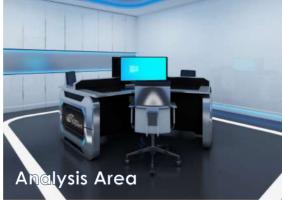
L1400\*W800\*H750 (Destop Panel: H1600)



**Cyber Colab** Cyber Colab L2620\*W3400\*H750











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



**Smart Evidence Locker** DE1904 L900\*W490\*H1850



**Conference Table** DE1902-D L3300\*W1600\*H750



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

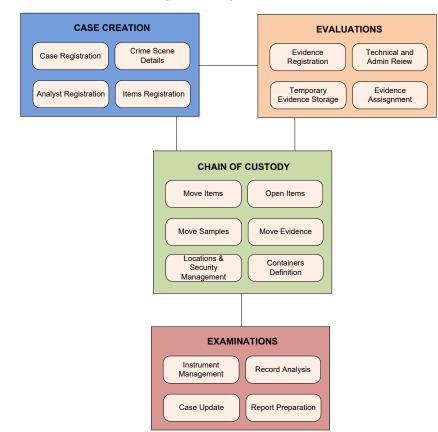
#### COMPLIANCE

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

- ISO Procedures
  - Publications and Forms
  - Laboratory Wide Documents
  - Procedures
- Technical Procedures
  - Digital Evidence Management
  - DNA Database
  - Drug Chemistry

- Firearm and Tool Mark
- Forensic Biology
- Latent Evidence
- Toxicology
- Trace Evidence

#### **Example of Simple FLIMS Model**







# 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.





#### **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

# **Turn Key Solutions for**

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

# 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.



The difference between FLIMS compared to other solutions in the market is that FLIMS are able to be fully customized for different Forensic Laboratories standard.



while at the same time able to maintain the Internationall Best Practice Standards. It can also be integrated with a Monitoring System for Laboratory Manager and Management to monitor Case progress, Budget and Expenditures, to better managed the Lab in more efficient manner.

Our Turn Key Solutions Capability Summary

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



F-LIMS

CASE MANAGEMENT

CHAIN OF CUSTODY

• EVIDENCE MANAGEMENT

• DOCUMENT MANAGEMENT

• INTEGRATED CYBER SECURITY

• ISO/IEC 17025 COMPLIANCE SYSTEM

• TAILORED FORENSIC DIVISION SYSTEM

ADVANCED USER MANAGEMENT

MOBILE MANAGEMENT SYSTEM

• MONITORING SYSTEM.







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

# Our advantages











### Our Promise

### Your data is unparalleled safe in DataExpert



- DataExpert Technology Limited got ISO/IEC 27001:2013 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
	Hard Disk	✓	✓	✓	✓
⊇	Magnetic Tape	✓	X	✓	Х
Magnetic Media	Floppy Disk	✓	X	$\checkmark$	X
a g e q	Zip Drive	✓	X	$\checkmark$	X
<b>\$ \$</b>	MO Disk	$\checkmark$	X	$\checkmark$	X
	SSD	X	$\checkmark$	$\checkmark$	X
ا و	USB Drive	X	$\checkmark$	$\checkmark$	X
Flash	Memory Card	X	$\checkmark$	$\checkmark$	X
Ĕ₹	Cellphone	X	$\checkmark$	$\checkmark$	✓
=	CD	X	X	$\checkmark$	X
Optical Disc	DVD	Х	Χ	$\checkmark$	X
Opti Disc	Blue-ray Disc	X	Χ	$\checkmark$	X



# Proposal











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





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**

MW-15000X	MW-25000X	MW-30000X	MW-1B
	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 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

	DED- SHS	DED- CDS2	DED- MMS3	DED- MMS2	DED- CDPS	DED- SSD01	DED- SSD2XS	DED- HD\$35
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

- 1. Provide transportation to deliver destroyed media to recycler.
- 2. Recycle degaussed/wiped media by Hong Kong Environment disposal grea. Protection Department (EPD) authorized computer recycler.
- 3. E-waste can become new material after proper processing Waste Disposal Ordinance under Hong Kong Law. and categorization.



Landfill (for non-recyclable E-waste only)

- 1. Provide transportation to deliver destroyed media to
- 2. Landfill non-recyclable residue according to the





# Data Solution (Series) Expert bsi 150/ 270 160/ Marie Cert

### **Document And Certificate**

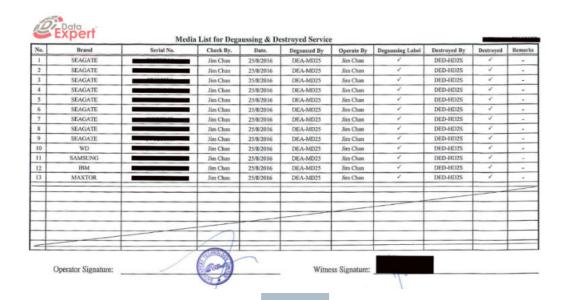
### **Object Receive Note**

Checking list of obsolete media, recorded media type, quantity, model, serial number, service date, person in charge, etc. Both DE project operator and client should sign on it, to confirm media collection information.



#### **Media List**

A checking list Media marked degaussing and physical destruction information, include media type, quantity, model, serial number, service date, time, equipment model and name of operator.



#### Certificate of Degaussing



#### **Certificate of Disposal**





# Forensic Workstation







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

Build-in forensic imaging software

## Phone Connection **Panel**

#### Auto detect connected devices' information

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

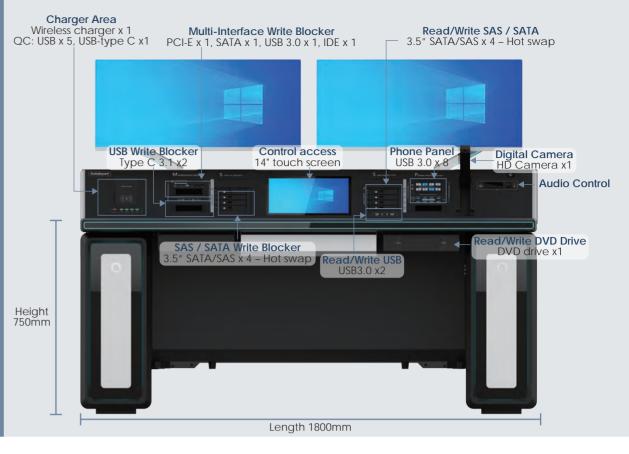
#### Multiple phone connections for multitasking

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



**Phone Connection Panel** 

Write-Blocker & Read/Write Interfaces



	op comeanon
Model	Cyber MZR-X
OS	Win11 64 bits OS
CPU	Intel C612 Chipset
	Intel i9-10 CPU
Memory	32GB DDR4 2133MHz (Upgradeable to 128GB)
Hard Drive	500GB SSD HDD (operating system)
	8TB Hard Drive (Storage) x 3 unit
	Write-Blocker Interfaces
Multi-Interface Write Blocker	PCI-E x 1 SATA x 1 USB 3.0 x 1 IDE x 1
USB Write Blocker	Type C 3.1 x2
SAS / SATA Write Blocker	3.5" SATA/SAS x 4 – Hot swap
	Read/Write Interface
Read/Write	3.5" SATA/SAS x 4 – Hot swap
Interface	USB3.0 x2
	DVD R/W Driver x 1
Phone Panel	USB 3.0 x 8 port (power independent)
	Others
Other Hardware	Digital Camera Built-in HD Camera for evidence recording
	Control access Built-in 14" touch screen
	3.5 earphone jack x 2
	RJ45 10GB x 2 port
	WiFi and Bluetooth module x 1
	Built-in Wireless charger x 1 Quick charger: USB x 5, USB-type C x1
	Control access Built-in 14" touch screen
Software	Build-in: D-Box Forensic Imaging Software
Sultwale	Optional: Belkasoft Evidence X / Hancom MD-Series / Mobiledit
	Forensic Pro
Display	2 unit Samsung or equivalent 34 inch Curve 21:9 with 1800R WQHD
1 - J	3440 x 1440 (2K) - 100Hz Type-C port
Dimension	1800*900*750 mm (L*W*D)

- ^ Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.
- \* Customized Configuration available. Powered by DataExpert.
- \* Specifications are subject to change without notice.



**Cyber MZR-DT**All-inclusive forensic workstation for rapid analysis of artifacts.



Hardware specifically designed for forensic

#### Forensically sound design

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

#### Multi-interface write blocker

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

#### High performance hardware

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





### 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

#### Multiple phone connections for multitasking

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



**Phone Connection Panel** 

Write-Blocker & Read/Write Interfaces



	Specification
Model	Cyber DZR-DT
	System Configuration
OS	Microsoft Windows 11 Pro 64 bit
Internal Memory	64GB DDR4 UDIMM non-ECC RAM Memory (2X32GB)
CPU	Intel i9-10900X (10 Core, 19.25M Cache, base 3.7GHz, up to 4.5GHz)
Storage system	ONE (1) 1TB GB M.2 NVME SSD (System installed on this Drive) ONE (1) 8TB 7200rpm SATA Hard Drive for Temporary Files and Processing ONE (1) 8TB 7200rpm SATA Hard Drive for evidence storage
Graphic Card Display	One (1) Nvidia Quadro T400, 4GB GDDR5 for Graphics Processing Unit (customizable)
DVD Drive	Blu-Ray Writer
Power Supply System	One (1) 1000 Watt Power Supply Unit
	Dashboard Configuration
Write Blocker (Read Only)	Writeblocker with PCI-E, SATA/ SAS, USB 3.0, IDE^
Read/ Write	3.5" SATA/SAS x 4 - Hot swap At rear: USB 3.0 x4 , at top: USB 2.0 x 2 + USB 3.0 x2, front panel: USB3.0 x 8
Phone Connection Panel	4.3" LCD display with 8 phone connected or disconnected status panel
	Forensics Software
Build-in software	D-Box Forensic Imaging Software
Optional Computer Forensics	Belkasoft Evidence X
Optional Phone Forensic	Hancom MD-Series / Mobiledit Forensic Pro
Warranty	THREE years limited warranty
A Optional to un grade to T	Tableau Forancia Universal Pridge T254700iu

- ^ Optional to upgrade to Tableau Forensic Universal Bridge T356789iu.
- \* Customized Configuration available. Powered by DataExpert.
- \* Specifications are subject to change without notice.





Forensic Cube V4

All you need for on-scene investigation.

Hardware specifically designed for forensic

### Forensically sound design

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

#### Multi-interface write blocker

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

#### High performance hardware

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





4 main functions of software

### 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

Write-Blocker & Read/Write Interfaces





**Keyboard version** 

Versions

**Keyboardless version** 

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

<sup>\*</sup> Customized Configuration available. Powered by DataExpert.

<sup>\*</sup> Specifications are subject to change without notice.



High perfermance laptops design for field or lab forensic investigation.



# Specification

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

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

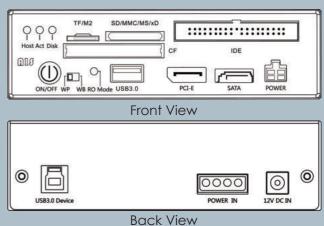






## Integrated write-blocker supports 7 storage media types.





### Supported storage media:

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

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

<sup>\*</sup>Remark: Made in Hong Kong and powered by DataExpert

<sup>\*</sup>Specifications are subject to change without notice







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







# Product Detail

### Write Blocker U



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

### Write Blocker P





Write Blocker M

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

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







Write Blocker M	Write Blocker P	Write Blocker U
DE-U2MS	DE-U2PS	DE-U2US
Write-Blocker I	nterfaces	
1	1	/
1	/	1
1	1	/
/	/	1
Feature	es	
✓	✓	/
✓	/	/
Supports automatic identification and full reading of HPA hidden areas.	/	/
✓ Target disk mode	/	✓ Target disk mode
Performance P	arameter	
10GB/MIN (PCI-E/ M.2/SATA/USB SSD)	50GB/MIN (USB SSD)	14GB/MIN (USB SSD)
USB 3.0	USB 3.2	USB 3.0
Mode	•	
✓	✓	✓
✓	/	✓
Other		
/	/	Optional
DC 12V 4A	DC 12V 4A	DC 5V 3A
1.41*91*94mm	121*73*25mm	104*68*29mm
	DE-U2MS  Write-Blocker I  1  1  1  /  Feature  Supports automatic identification and full reading of HPA hidden areas.  Target disk mode  Performance P  10GB/MIN (PCI-E/M.2/SATA/USB SSD)  USB 3.0  Mode	Write-Blocker Interfaces  1







# THE POWER AND VERSATILITY OF TALINO - ACCEPT NO SUBSTITUTES

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

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

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



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



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



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

SUMURI.COM

#### **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

Copyright ©2022 SUMURI. All rights reserved.

SUMURI.COM



# Computer Forensic





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



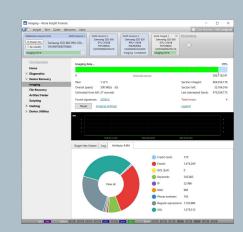
# **Functions**

# Forensic Imaging

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

# 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



### Workflow

**Diagnostics** 

**Imaging** 

**Forensic File** Recovery



Drive

**Evidence Drive** 

# Atola Product comparison







	Atola TaskForce 2	Atola TaskForce	Atola Insight Forensic
		Imaging	
Simultaneous imaging sessions	25+	12+	3
Cumulative imaging speed	25 TB/hour	15 TB/hour	4 TB/hour
utomated RAID configuration detection	Support RAID 0, 1	, 5, 6, 10 and JBOD	-
Automation	Wel	b API	<u>-</u>
Damaged drive support		Damaged heads, freezing drives, short circuit detection, worn-out HDDs/SSDs	
Head selection support	✓	<u>√</u>	✓
Network		2 x 10Gb Ethernet ports	
Express mode	up to 25 imaging sessions	up to 17 imaging sessions	-
Logical imaging to L01	✓	✓	<del>-</del>
Imaging targets	E01/RAW/AFF4 files located on other	r drives (Veracrypt-encrypted as option), E01/RAW/AFF4 files located on a server or NAS, I	bit-to-bit copy on other drives
Max. targets per imaging session	5	5	3
		Hardware unit	
	26 ports	18 ports	10 ports
Ports	with source/target switch	with source/target switch	Cannot switch source/target
	4 NVMe M.2/U.2 PCIe 4.0	Will Jource/Talger 3Wileti	
	8 SATA	6 SATA	6 SATA
		6 SAS/SATA	6 SAS/SATA
Port types	8 SAS/SATA	4 USB	4 USB
	4 USB	1 IDE	1 IDE
	1 IDE		
	Extension port	Extension port	Extension port
Write protection	on all ports (configurable)	on all ports (configurable)	on source ports
	M.2 NVMe/PCIe/SATA	M.2 NVMe/PCIe/SATA	M.2 NVMe/PCIe/SATA
	Apple PCIe	Apple PCIe	Apple PCIe
Extension modules	Thunderbolt	Thunderbolt	Thunderbolt
			SAS
Interface	web-based (offline)		Windows application
Wi-Fi mode	External ada	oter (optional)	-
Standalone mode	Kiosk mode	✓	-
Server rack compatibility	✓		
		Other features	
Drive diagnostics		PCB, Heads, Media scan, Firmware, File system. I maging time estimate.	
Wiping	Zero-fill, Custom pattern,	LBA number, Secure Erase, DoD 5220.22-M, NIST 800-88, Random, Format NVM and Sanitize	e 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	<u>-</u>	-	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.



# **Functions**

# **Forensic Imaging**

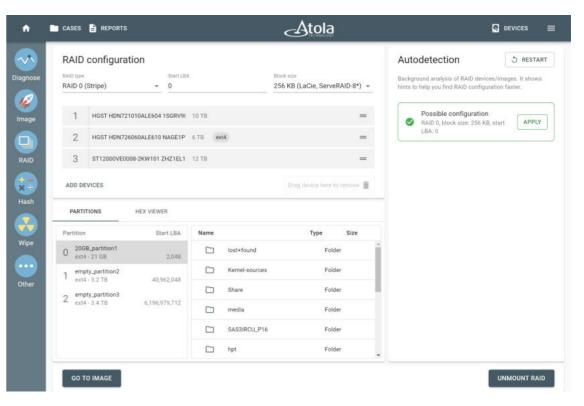
- 15 TB/h cumulative speed of imaging
- 12+ simultaneous imaging sessions
- Imaging to up to 5 targets
- Automation via Web API
- Physical imaging to E01, AFF4 and RAW files
- Logical imaging to L01 file

- Source/target switch on all ports
- Hardware write protection in Source mode on all ports



# RAID configuration autodetection and imaging

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

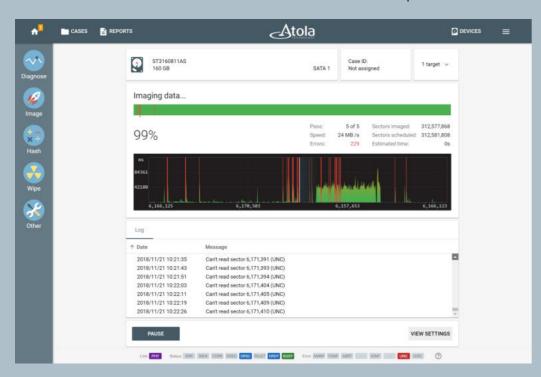






# Damaged drive support

- 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 NMVe/PCIe/SATA SSDs
- Latest Apple SSDs via Thunderbolt extension
- The newest PCIe SSDs from Apple MacBooks (2013 2015)

# Other features of TaskForce forensic imager

- Wiping with various methods: Pattern, Secure Erase, NIST 800-88, DoD 5220.22-M, Random, LBA number
- Browse files on any connected device
- SMART viewing + recording it before and after image acquisitions
- Hash calculation (linear and segmented): MD5, SHA1, SHA256, SHA512
- HPA & DCO control and recovery
- Automatic report generation
- Case management system
- \* For further information, please visit https://www.atola.com/products/taskforce/





# **Atola TaskForce 2**

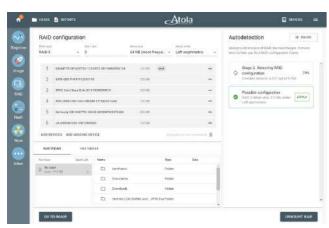




Atola TaskForce 2 is a top-performance forensic imager capable of running **25+ imaging sessions** in parallel, automatically retrieve data from damaged media, detect and reassemble unknown RAID arrays.

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

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





#### Imaging 25+ drives simultaneously at 25 TB/hour

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

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

#### **RAID** autodetection, reassembly and imaging

Autodetection for RAID arrays with an unknown configuration:

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

### **Damaged drive support**

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

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

# **Atola TaskForce 2**



#### **Connectivity options**

#### 1. 10Gb Ethernet network

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

#### 2. Kiosk mode

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

#### 3. Wi-Fi connection

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

#### Multi-user access & user interface

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

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

#### Other features

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

#### **Lifetime warranty**

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

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



	The state of the s	
Astro		
8maging 549 8 SEABATE ST838085735-H 35J87209	128	2 hours h
tinaging SAS 3 SEAGATE STEEMONSTEES 6SLIPECTHONOCRES4490VET	34%	2 hours )
limaging UTB 6 Sarchisk pSSD 0004467cB	15%	2 hours to
Imaging 0478-1 WDC WB5002ABYS 7801B3 W0WM45Y8169980	94	2 koys i
imaging 5474 2 Hearts HT9225059434364 108023F0K464VLHR78W.)	<u>n</u>	(hous)
thiaging UTD 1 Serraing PSSD 77 SSTRNS0T300082T	70%	3 tours
Imaging 647A 5 HyperX Fury 3D 0406B 50205B77844022F1	15	ther house to
Imaging UIS 3 SanDisk Outer Sperk 40590800011015114520	72%	E-MONUME I
Briaging SATA 6 TOSHBA BROTACASSO 93E PYZES	10%	2 tours
Imaging 0.616.0 Somouse SSO 670 EVD SD008 S6799/2004076742	25	(boars)
Imaging UIB 1 RXB50ZNV 2540 NVW- 7D 01284567694CB	79%	an nout t





### The Leading macOS Imaging, Triaging, and Reporting Solution

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

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

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



Includes Three Imaging Solutions Suited for Any Case (LIVE and Bootable)



Supports live and bootable imaging of Intel and Apple Silicon Chips



Only True Triage Solution for Live Running Macs or Macs Connected in Target Disk Mode



Contains Full Report Capabilities with Sequential Processing of Proper macOS Timestamps



Correctly Uses Apple Extended Metadata with macOS Native Libraries



Automatically Collects Volatile Data



Ability to Automatically Triage Boot Camp and iOS Backups



Includes PALADIN PRO for Windows and Linux Support

51 h 41 lD1 50h 4





#### THREE IMAGING SOLUTIONS FOR THE PRICE OF ONE

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

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

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

#### Support for Intel and Apple Silicon Processors

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

#### The Only True macOS Triage Solution

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

#### **FULL REPORT CAPABILITIES**

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

#### CORRECT USE OF APPLE EXTENDED METADATA

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

#### ABILITY TO TRIAGE BOOT CAMP AND IOS BACKUPS

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

# INCLUDES PALADIN FOR WINDOWS AND LINUX SUPPORT

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

#### **ABOUT SUMURI**

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

SUMURI.COM

sales@sumuri.com +1 302.570.0015

Our Mailing Address: P.O. Box 121 Magnolia,

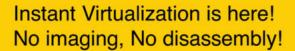
DE 19962, USA

Copyright ©2022 SUMURI. All rights reserved.

Copyright ©2022 SUMURI. All rights reserved.







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

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



Instant Virtualization of Windows Computers and Forensic Images



BitLocker Support



**RECON for Windows: Triage Capabilities** 



Advanced File Search



Advanced Data Carving



Snapshot Differential Analysis



PALADIN Toolbox - Imagers and Write-Blocking Included



Now merged with PALADIN!





# INSTANT VIRTUALIZATION OF WINDOWS COMPUTERS AND FORENSIC IMAGES

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

#### BITLOCKER SUPPORT

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

#### **RECON FOR WINDOWS: TRIAGE CAPABILITIES**

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

#### ADVANCED FILE SEARCH

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

#### ADVANCED DATA CARVING

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

#### **SNAPSHOT DIFFERENTIAL ANALYSIS**

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

# PALADIN TOOLBOX - IMAGERS AND WRITE-BLOCKING INCLUDED

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

#### **ABOUT SUMURI**

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

sales@sumuri.com +1 302.570.0015

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

SUMURI.COM

Copyright ©2022 SUMURI. All rights reserved.

**SUMURI.COM** 



# Reputation is everything. We help you keep it.

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

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



Native to macOS



Correctly Uses Apple Extended Attributes and Apple Timestamps with macOS Native Libraries



Automated Analysis of macOS, Windows, iOS, Android, and Google Takeout



Sequential Processing (Timeline Analysis)



StoryBoard - First of its Kind WYSIWYG Forensic Reports



# RECON LAB

### FORENSIC SUITE



#### **NATIVE TO macOS**

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

#### **CORRECT USE OF APPLE EXTENDED ATTRIBUTES**

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

# AUTOMATED ANALYSIS OF macOS, WINDOWS, iOS, ANDROID, AND GOOGLE TAKEOUT

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

#### **SEQUENTIAL PROCESSING (TIMELINE ANALYSIS)**

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

#### **STORYBOARD**

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

#### **ABOUT SUMURI**

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

Copyright ©2022 SUMURI. All rights reserved.

Copyright ©2022 SUMURI. All rights reserved.

**SUMURI.COM** 



# **CSI RESPONDER**

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

CSI Responder primarily addresses the following pain points:

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

# Hardware

Storage Interfaces Dual-channel interface compatible with the latest Thunderbolt 3/4, USB4, featuring built-in 2TB\*2 high-performance NVMe SSD

Bootable Drive The Windows forensic disk includes WinToGo, X64FE, X86FE, ARM64FE. (Default source write blocker) The Mac forensic disk includes MacOS 15.6 boot system and X-ImagerMac imaging tool

External Hub USB 3.2 Gen2 x2 (Type-A, 10Gbps),USB 3.2Gen2 x1 (Type-A, 10Gbps),100W PDx1 and other.

# **Build-in Software**

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

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

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





# Key Features

# Non-dismantling Imaging

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

- 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

Disk
Decryption

**TPM (Trusted Platform Module)** 



MAC - T2 & Apple Silicon (M1/M2/M3)



# 3 Unbreakable Fast



Device

Specifications \

Thunderbolt + USB quad channel

Imaging Speed

120-150GB / min



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

# Operations without 220V power supply

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







Learn more belkasoft.com Sunnyvale CA 94085 United States (650) 272-03-84

# **DATA SOURCES**









Cloud



Android, iOS, Windows

Computers & laptops hard drives, disk images, virtual machines

RAM

# BELKASOFT EVIDENCE CENTER X

### **ACQUIRE**

E01/DD imaging •••



Agent-Based Acquisition

Jailbreak Support 🏋





Chat Apps



System Files

Mailboxes

Payment Apps

Documents

Online Games

Pictures & Videos Audio

Browsers

°C P2P



### **REVIEW & ANALYZE**

File System Explorer



Hash Set Analysis

SQLite Viewer

Connection Graph

Registry Viewer

Plist Viewer

Cross-Case Analysis Incident Investigations

Timeline 😂

WDE and File Decryption

Advanced Picture and Video Analysis

### **REPORT**

Customizable Reports In Multiple Formats



Free Portable Case Viewer



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

702 San Conrado Terrace, Unit 1 Sunnyvale CA 94085 United State: +1 (650) 272-03-84 email: 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

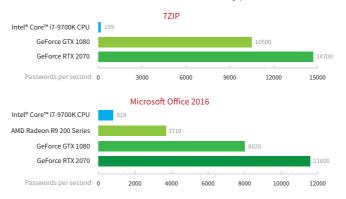
A single purchase delivers all ElcomSoft products in their respective top-of-the-line editions that allow recovering passwords and decrypting encrypted data.



#### 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.

ElcomSoft Distributed Password Recovery | Version 4.20



## 300° 20°C

#### 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.

www.elcomsoft.com

blog.elcomsoft.com

sales@elcomsoft.com



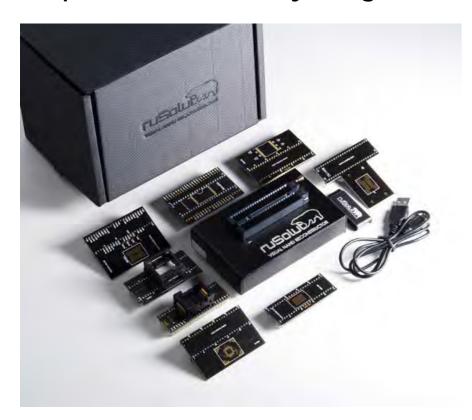








### Chip-off Data Recovery & Digital Forensic analysis of broken flash storage devices.



### **Application**





Physical Damage





Thermal Damage



Electrical

Damage



Analysis "non-addressed areas"

Nonrecognizable disk

## Workflow





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



<sup>\*</sup> 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** 



#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



We connected 2 external hard drives (500GBs each) and 3 thumb drives (16GBs, and 2 64GBs) to Cyacomb's tool. We received an initial positive hit for the presence of child sexual abuse material in approximately 10 - 15 seconds and within 45 seconds had positive hits on all the devices for the presence of child pornography/child sexual abuse material.

Cyacomb has taken a process that until now has taken hours to complete and reduced that time down to less than a minute."

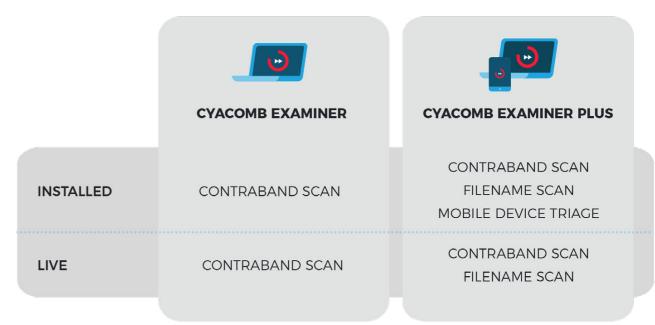
**DETECTIVE MIKE FONTENOT OF DALLAS PD** 



Along with Mobile Device Triage and Contraband Filter Scan, Cyacomb Examiner Plus also offers Filename Scan. It allows suspect devices to be guickly 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



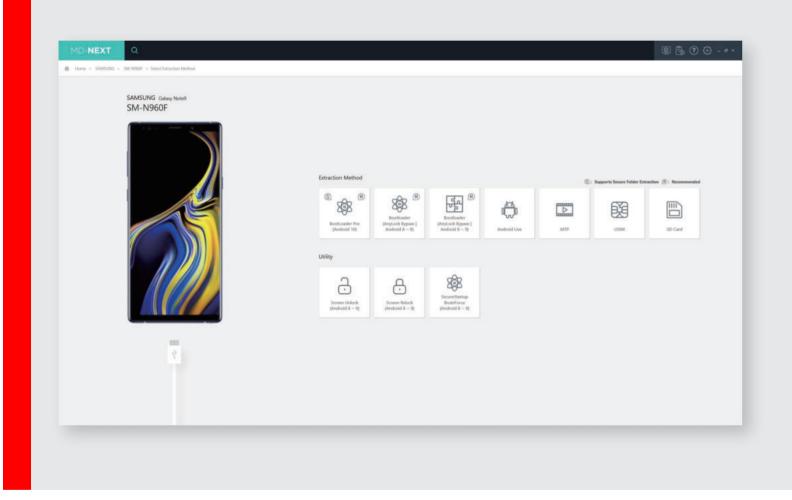


## Mobile Forensic

#### **MD-NEXT**

#### Mobile Data Extraction and Unlock Tool for Asian Manufacturers Phone Models

MD-NEXT is the forensics software to extract data from mobile and digital devices of manufacturers worldwide, including latest Smart-phones, Feature phones, IoT devices, Smart TVs, Drones, Chip-off memory, and JTAG boards. Physical and logical extraction methods for various types of OSs, backup files, and media cards are available.



#### **System Requirements**

OS Windows 8/10/11 (64 bit)

CPU i5 or above
RAM 4GB or above
Disk 1TB or above
Display 1024x768 or above

USB 2 or more USB 2.0/3.0/3.1 ports

Microsoft.Net Framework 4.6.2

#### **Product Components**

MD-NEXT Installation Software (USB Memory/Online)
USB Dongle Key 1 EA
Warranty 1 Year

#### > Product Specification

#### Powerful Extraction Tool that Covers Wide Range of Devices

- Supports more than 15,000 models of
- Global smartphone manufacturers (Samsung/Apple/LG/Nokia/Microsoft and etc.)
- Chinese manufacturers (Huawei/Xiaomi/Oppo/Vivo and etc.)
- Drone extraction: DJI (Phantom, Maverik), Parrot
- Al Speaker extraction: Amazon Echo, Kakao Mini, Naver Clova
- Smart TV extraction: Samsung, LG, Android TV, Apple TV
- IoT device, Smart TV, IP Camera, and Car dashboard



#### **Android Extraction**

- Samsung: Qualcomm Full filesystem extraction, Exynos Full filesystem, Bootloader Pro, Bootloader AnyLock Bypass (Unlock/Relock/SecureStartup BruteForce), Bootloader, ADB pro T4, Android Live logical extraction (Smart Switch, Extraction Agent, ADB Backup with App Downgrade)
- LG: Physical extraction by Android system exploit, Physical extraction, Android Live logical extraction (Bridge, Extraction Agent, ADB Backup with App Downgrade)
- Huawei: Kirin Full filesystem extraction, Physical extraction, Android Live logical extraction (HiSuite, Extraction Agent, ADB Backup with App Downgrade)
- Other manufacturers
- Xiaomi, OPPO, Vivo, Google, Pantech physical extraction(Chinese, Indian)
- Physical extraction for Japanese manufacturer model: Sharp, Sony
- Qualcomm, MTK chipset extraction

#### iOS Extraction

- iOS Full file system by Checkm8, and iOS Agent program
- iOS backup extraction
- iTunes backup file extraction
- iOS physical extraction

#### Extraction from the Backup files

- Extraction from iOS backup file, ADB backup file in PC
- Extraction from backup files in Samsung, LG, Huawei, Xiaomi OPPO, Gionee smartphones

#### Physical Data Extraction from Media card

- Trace32 JTAG debugger
- UP828 Memory chip reader
- SD Memory Reader
- UFS Memory Reader
- USIM Reader

#### **Extraction Performance**

- Max.32GB/20min extraction performance
- Multiple device extraction
- $\hbox{-} Extraction sequence management (Sequential/Simultaneous) \\$

#### **Assurance of Evidence Data Integrity**

- Supports write-protection to every evidence data
- $\hbox{- Supports 10 hash algorithms such as MD5, SHA1/224/256/384/512, RIPEMD128/160/256/320}\\$

#### Reporting

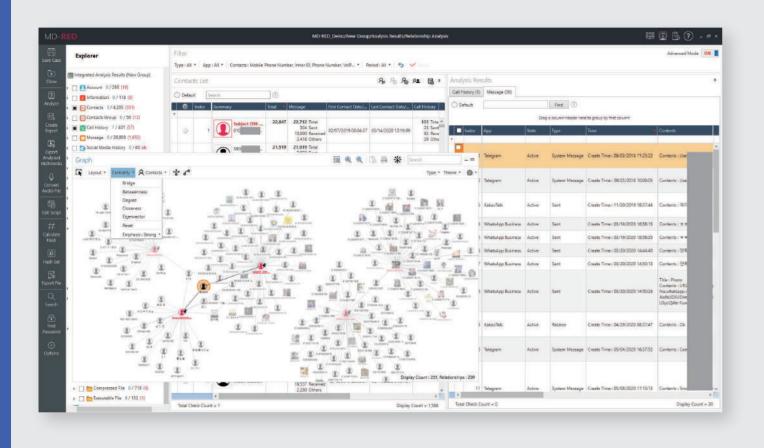
- Extraction information Hash value, Time, Method and File name
- Report file formats PDF, Excel and HTML
- 'Extracted File List' generation with hash value of each file
- 'Witness Document' generation
- Regeneration of 'Extraction Reports'

\*Contact us for more detailed product spec information.

#### **MD-RED**

#### Data Analysis Software for Recovery, Decryption, Visualization, Analytics, and Reporting

MD-RED is the forensics software for recovery, decryption, visualization, analytic data mining, and reporting evidence data. Advanced analysis feature allows to decrypt encrypted data from messages, messengers, emails, etc., and users can easily review the analyzed result through the various data filters, and embedded viewer. All the analysis results can be exported as a report and reviewed with a standalone viewer MD-Explorer.



#### **System Requirements**

OS Windows 8/10/11 (64 bit)

CPU i7 or above
RAM 8GB or above
Disk 1TB or above
Display 1024x768 or above

USB 2 or more USB 2.0/3.0/3.1 ports

Microsoft.Net Framework 4.6.2

#### **Product Components**

MD-RED Installation Software (USB Memory/Online)
USB Dongle Key 1 EA

Warranty 1 Year

#### > Product Specification

#### Parsing and Recovery of Various Images and File systems

- Images: SD Card, phone data partition, MDF, E01, GrayKey, UFED image format
- File systems: FAT12, FAT16, FAT32, NTFS, exFAT, HFS+, EXT2, EXT3, EXT4, F2FS, VDFS, APFS, TAT16, TAT32,
- NxFS, IKVISION, DHFS4.1, WFS0.4, TANGO, RSFS, WOW, VDFS, XFS, YAFFS, EFS2, TFS4
- Data carving for unused area

#### **Analysis of Mobile Data and Apps**

- Multimedia files taken by phone camera
- Call log, Address book, SMS/MMS, Email, Memo, Internet history
- SNS, Map, Navigation, Health, Banking and Lifestyle apps
- Detects Steganography, anti-forensic apps
- Deserialization, Decryption and Recovery of data

#### **Advanced Analysis of Popular Messengers**

- Description of encrypted messenger data
- Decryption and analysis for multiple backup files of WhatsApp
- Multiple account analysis

#### **Data Visualization and Social Relationship Analysis**

- Map view for GPS data and cell tower location
- Timeline view
- Communication visualization
- Web browser for internet history review
- Social relationship analysis
- Community analysis by centrality

#### **Multiple Space Analysis**

- Samsung secure folder(KNOX space) analysis
- Huawei PrivateSpace analysis
- Android Multi-Space analysis

#### **Data Decryption and Recovery**

- Identifies encrypted document
- Decrypts encrypted chat message, email, file and app data
- Recovery of deleted file and multimedia data

#### **Dynamic Data Filter and Search**

- Filtering by file system, signature, time and etc.
- Dynamic filtering operators, sorting, grouping and etc.
- Search by regular expression
- Keyword registration
- Bookmarking of selected data
- Multimedia filter by app, status, size, type, property, path and etc.

#### Reporting

- Export of original or converted files with file hash value
- Report file formats PDF, Excel, ODS, HTML, XML and SQLite DB
- 3rd party report file formats NUIX, Relativity and ForensIQ one
- Electronically stored information can be included in a report
- Analyzed result can be reviewed with a stand-alone data viewer 'MD-Explorer'

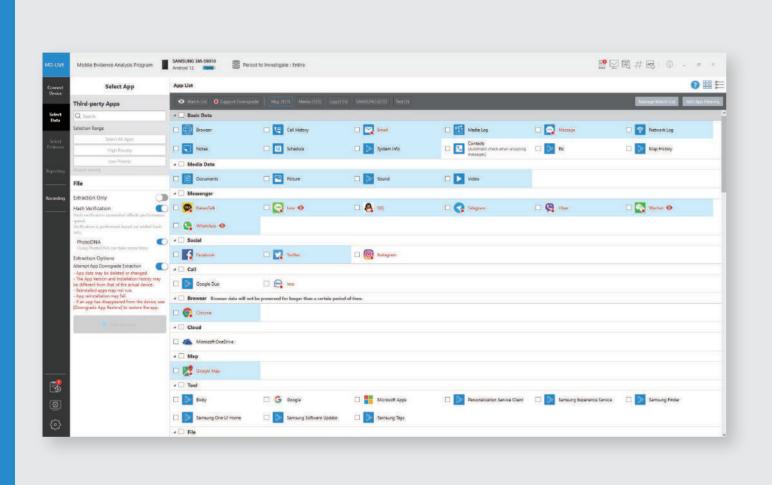
\*Contact us for more detailed product spec information.



#### **MD-LIVE**

#### Mobile Data Extraction and Analysis Tool for On-The-Spot Investigation and Triage

MD-LIVE supports quick on-site investigation with device scanning, extraction, analysis, and reporting features. Selective extraction, Watch List, Keyword, and Hash search features enable time-efficient investigation and prevent privacy infringement.



#### **System Requirements**

OS Windows 8/10/11 (64 bit)

CPU i5 or above

RAM 8GB or above

Disk 256GB or above

Display 1200x700 or above

USB 2 or more USB 2.0/3.0/3.1 ports

Microsoft.Net Framework 4.6.2

#### **Product Components**

MD-LIVE Installation Software (HDD/USB Memory/Online)

USB Dongle Key 1 EA Warranty 1 Year

#### **Hardware Package Option (MD-PORTABLE)**

Rugged case
Laptop or Tablet
Cable sets

HDMI Capture board

MD-CAMERA (External HD Camera)

#### > Product Specification

#### Extraction

- Automatic recognition of smartphone model
- Detail information view for installed apps
- Various filtering option for installed apps
- Extraction guides and notifications per OS type
- Displays extraction progress by app
- Multi-space notification
- Selective extraction by app or by time period
- Notification of the battery level before extraction



#### **Analysis**

- App analysis
- Over 2,000 of Android and iOS apps
- Messenger data decryption Facebook Messenger, WeChat, Signal, Wickr, Discord and etc.
- Multi-account app analysis WeChat, Telegram, Instagram, Facebook Messenger and etc.
- Various DB format analysis SQLite, Realm, Bolt, ESE and etc.
- Various file system analysis
- Signature-based multimedia analysis

#### **Analysis Result View**

- Customized filters by analysis result types
- View selected items or search results
- Messenger view
- GPS geolocation visualization support with the online and offline maps
- Keyword List search by import of external file or manual input
- Watch List and the user-defined filter of apps
- Hash set search by import of external file, manual input, Project VIC (UK, US, CA), and Photo DNA
- Internal viewers for documents, database, hex, text, image, audio and video
- Browser for Internet browsing history view

#### **Recording Investigation**

- Photographing, video/audio recording of evidence and investigation process by MD-CAMERA (External HD Camera) or HDMI capture board supplied as option items
- Mirrored and remote–controlled smartphone screen can be captured and recorded  $\,$
- PC screen recording of MD-LIVE to reproduce or to verify its forensics process
- Log analysis to track the recent history of smartphone app usage and system history
   Monitoring active phone process for malware or specific active app investigation

#### Reporting

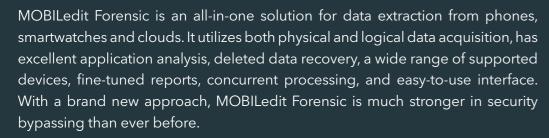
- Report types
- Analysis results summary
- Analysis results report (Result details)
- Electrically stored information (Extracted files list)
- Report options
- Anonymous report Protects the witness or the victim by hiding their information
- Report with large image Displays one image on each page not to scales down
- Archive report file as MDF/ZIP/TAR/DD
- Report file formats PDF, Excel
- HASH algorithm options MD5, SHA1/224/256/384/512, RIPEMD128/160/256/320

\*Contact us for more detailed product spec information.



## MOBILedit Forensic

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



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



#### **SECURITY BYPASSING WITH LIVE UPDATES**

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



#### PHYSICAL DATA ACQUISITION AND ANALYSIS

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



#### **SMARTWATCH FORENSICS**

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



#### **CLOUD FORENSICS**

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



#### **DELETED DATA RECOVERY**

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



#### ADVANCED APPLICATION ANALYSIS WITH LIVE UPDATES

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



#### **SMART SCREENSHOTS**

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



#### **CONCURRENT EXTRACTIONS**

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



#### **OBJECT AND FACE RECOGNITION - THE POWER OF ARTIFICAL INTELLIGENCE**

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



#### **CAMERA BALLISTICS - SCIENTIFIC IMAGE ANALYSIS**

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



#### **DIVE COMPUTER FORENSICS**

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



#### INTEGRATE WITH OTHER TOOLS

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





## MOBILedit Cloud Forensic

Get a complete digital footprint of a suspect

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

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

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

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

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

#### **Integration with MOBILedit Forensic PRO**

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

#### **MOBILedit Cloud Forensic as a standalone product**

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

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

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

#### **FEATURES**

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

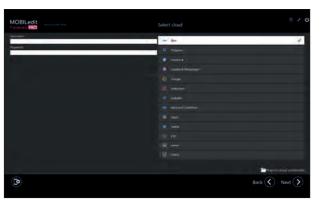
#### SUPPORTED SERVICES

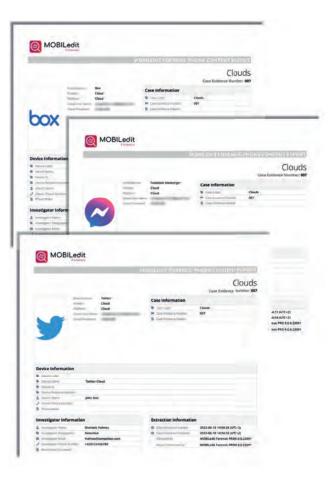
- Box
- Dropbox
- Google Drive
- Microsoft OneDrive
- FTP
- Facebook
- Facebook Messenger
- Google Contacts, Calendar, Keep
- Instagram
- LinkedIn
- Slack
- Twitter
- Emails such as Gmail, Outlook, and many others through POP3, IMAP protocols
- and more

#### 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)











### 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.

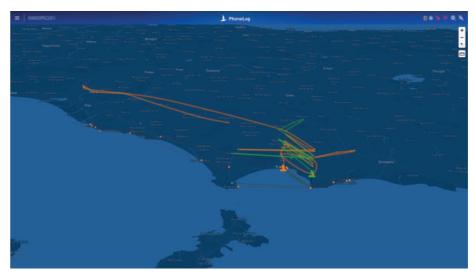
Place all your evidence on a state of the art 3D map and visualize events and user movements.

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.







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

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

#### Integrate all this and more to PhoneLog

#### Choose PhoneLog and you have:

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

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

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

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

#### **NO CONFUSION NO MISTAKES**

#### TRUST OUR YEARS OF EXPERIENCE IN STUDYING CELL NETWORKS WORLDWIDE

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

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

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

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

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

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















### Elcomsoft Mobile Forensic Bundle

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

#### TOOLS FOR MOBILE FORENSICS

#### Comprehensive Mobile Forensic Solution

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

#### Forensic analysis of Apple devices

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

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

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

#### Break passwords to iOS system backups

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

## GPU acceleration: patented technology significantly reduces password recovery time

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

#### Dictionary attack

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

#### ■ Full over-the-air acquisition of Google Accounts

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

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

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

#### Fast download, search and analysis

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

#### Reporting and Exporting

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



#### 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 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.





#### **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 information at 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

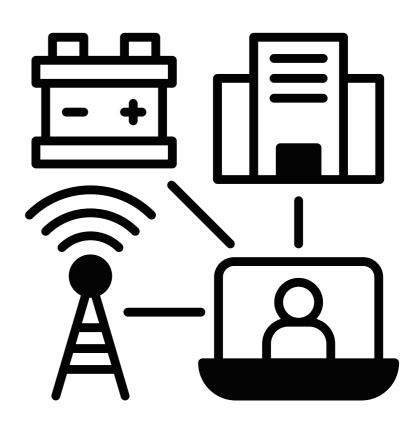
3. Fast results

#### 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

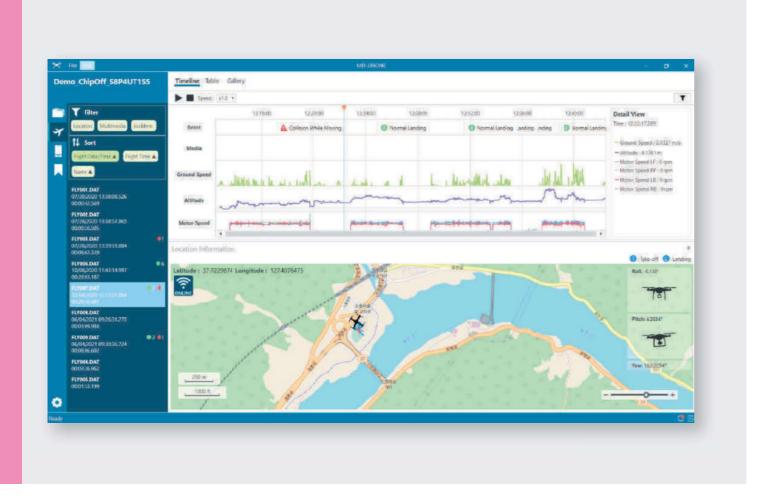
## IoT Forensic Solution



#### **MD-DRONE**

#### Drone(UAVs) Data Extraction and Al-based Flight data Analysis Tool

MD-DRONE is a drone forensic software for extracting and analyzing data from various data sources of UAV/Drone from of global manufacturers such as DJI, Parrot etc. Timeline-based flight parameter values(speed, altitude, value of each motor, etc.) can be viewed in graphical & tabular formats. Moreover, ML/Al-based drone accident or abnormal landing analysis feature is available.



#### **System Requirements**

OS Windows 8/10 (64 bit)

CPU i5 or above

RAM 8GB or above

HDD 1TB or above

Display 1200 x 700 or above

USB 2 or more USB 2.0/3.0/3.1 ports

Microsoft .Net Framework 4.6.2

#### **Product Components**

MD-DRONE Installation Software (USB/Online)

USB Dongle Key 1EA Warranty 1 Year

#### > Product Specification

#### Various Extraction methods for wide range of Drone

- Extraction through the drone USB connection
- Extraction through the network connection (WIFI)
- Extraction from SD card
- Chip-off extraction (Requires chip socket + chip reader)
- Drone App data can be extracted with MD-NEXT and exported with MD-RED
- Provides an extraction guide for each method

#### Timeline-based Integrated Flight data Analysis

- Timeline-based flight parameter values (speed, altitude, value of each motor, etc.) can be viewed in graphical & tabular formats
- Selective evidence data according to the flight time
- Check the drone's position and posture (Yaw, Roll, Pitch) information on the timeline
- Integrated view of flight path history and media data
- Playback and reconstruct flight history
- Preview of the selected media file in the timeline chart

#### Deep analysis of flight data by AI and machine learning

- Learning of accidental or abnormal flight log data
- Find out the collision, battery exhaustion, normal landing, and abnormal flight position/time

#### Detail flight data view and selection

- Check the detailed values of the flight log
- Classify meaningful flight log values such as altitude, ground speed, battery, and signal strength and display in different colors on the map
- Tabular view of GPS-based drone track, latitude, longitude and movement history
- Check the drone position value by time  $% \left( 1\right) =\left( 1\right) \left( 1\right$
- Sorting flight data in time order
- Intuitive drone movement check through table view
- Detailed values of the flight log in the table and visualization on the map

#### Multimedia Gallery

- Check the multimedia (video, photo) file with the corresponding time information in the flight record
- Check the Information such as the path, creation date, and size of the saved multimedia file
- Intuitive analysis through the preview
- Filter & Sorting of the flight logs by multimedia file, Location, Date & Time, Log file name etc. by path, creation date, and size

#### Bookmark

- Supports bookmark feature for flight time range, image and video

#### Notification Alarm

– Displays and saves important notifications during extraction and analysis while using MD-DRONE

#### Reporting

- Supports exporting of reports in PDF format based on the bookmarked content
- Supports exporting of each manufacturer's flight log glossary in csv format

\*Contact us for more detailed product spec information

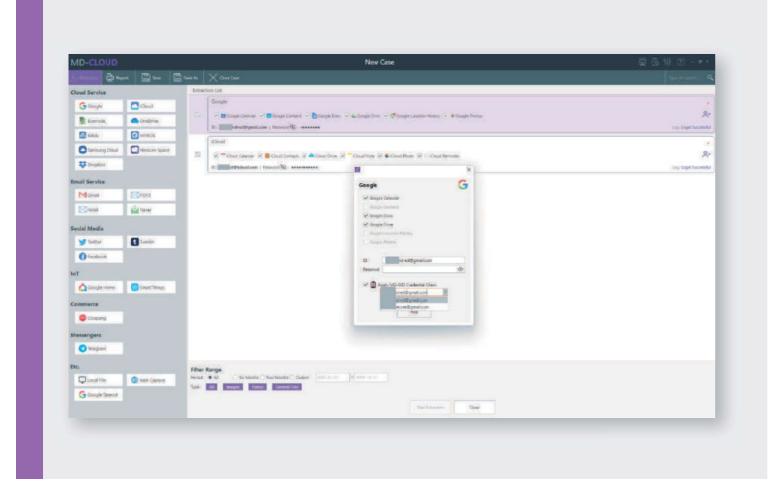
16



### **MD-CLOUD**

#### Mobile Forensic Software for Cloud data Extraction and Analysis

MD-CLOUD is the most intuitive digital forensic software tool that extracts and analyzes the data from the cloud data storage. It supports broad range of cloud services such as Google, iCloud, Samsung Cloud and etc..



#### **System Requirements**

OS Windows 8/10/11 (64 bit)

CPU i5 or above

RAM 4GB or above

Display 1024x768 or above

USB 2 or more USB 2.0/3.0/3.1 ports

Network Internet connection via wired or wireless LAN

#### **Product Components**

MD-CLOUD Installation Software (USB/Online)

USB Dongle Key 1EA Warranty 1 Year

#### > Product Specification

#### Various Cloud Services

– Google, iCloud, IMAP/POP3, Evernote, One Drive, Dropbox, Twitter, Tumblr and Instagram, Telegram, Facebook, Google Takeout

#### Acquisition of IoT Cloud

- IoT data extraction from Al speaker and Smart home kit (Google Home, Samsung SmartThings)
- Official and unofficial APIs for authentication

#### **Various Authentication Methods**

- ID/PASSWORD authentication
- Captcha security authentication
- 2-factor security authentication
- Authentication using credential information

#### Web Capture

- Supports capturing data from web pages without APIs provided

#### Monitoring the Progress of Data Acquisition

- Supports real-time monitoring progress during data acquisition

#### Interwork with MD-RED

- Supports extra data acquisition from cloud using ID/PASSWORD
- Supports reuse of session token, ID/PASSWORD information left in analyzed data by MD-RED

#### Quick Search using Extracted 'Tag' Information

- Supports extraction of 'Tag' information from cloud data
- Supports easy and fast search with pre-categorized 'Tag'

#### Various Built-In Viewers

- Image, video, document, web page and email can be previewed

#### Assurance of Evidence Data Integrity

– Supports 10 hash algorithms such as MD5 and SHA256  $\,$ 

#### Reporting

- Report file format: PDF
- Supports export of original cloud data files

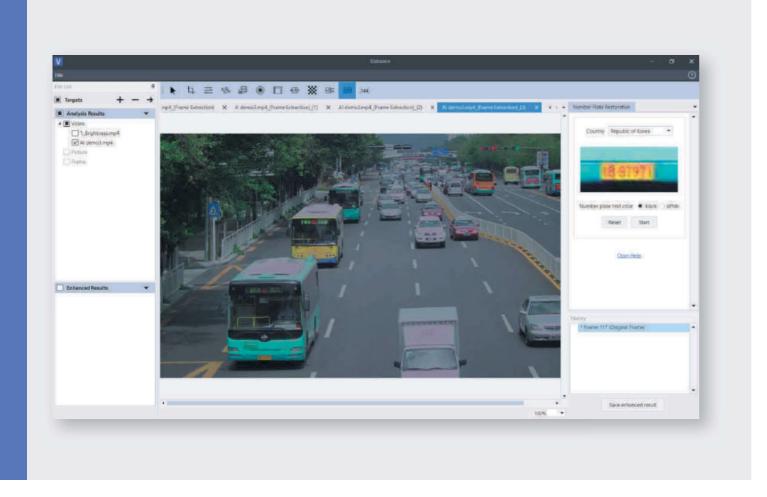
\*Contact us for more detailed product spec information.



#### **MD-VIDEO AI**

#### Video Forensic Software for Recovery, Al-based Image Enhancement & Analysis

MD-VIDEO is a video forensic software that supports recovery, and analysis of video files. Deleted and damaged video frames can be recovered, and enhancement feature supports to improve the quality of the target frame. Moreover, Al-based video analysis feature enables time-efficient investigation. More than 80 kinds of objects can be detected & recognized. The efficient filtering & sorting options help investigators to easily find the object.



#### **System Requirements**

OS Windows 10(64bit) or above

CPU i7 or above

GPU 1 or more multi-core GPU card for acceleration

RAM 8GB or above HDD 8TB or above

USB 2 or more USB 2.0/3.0/3.1 ports

Resolution 1024 x 640 or above

#### **Product Components**

MD-VIDEO AI Installation Software (USB/Online)

USB Dongle Key 1EA Warranty 1 Year

#### > Product Specification

#### Video/Audio Recovery

- Auto-scanning of partition
- Deleted and damaged file recovery
- Supports extraction from various data sources
- Supports various video filesystems
- FAT12, FAT16, FAT32, TAT16, TAT32, NxFS
- NTFS, exFAT, HFS+, EXT, EXT2, EXT3, EXT4, F2FS, VDFS, APFS
- · YAFFS, EFS2, TFS4
- HIKVISION, DHFS4,1, WFS0,4, TANGO, RSFS, WOW, XFS, WEBGATE, STL
- Signature-based file recovery (DAV, MP4, MOV, MKV, MPEG, SSF, AVI, ZAV, PS)
- Frame extraction and reassemble from the damaged video file
- Video frame recovery with the codec information of local codec file or local video file
- Partial recovery for the specific time range of OCR time or time data
- Recovery of time from the meta-data file
- Audio file recovery for SILK format

#### Video Analysis

- Object detection
- · AI-based object detection
- Detected objects categorization
- Deduplication of same objects det
- Color and Area Filter for objects
- Time Filter (Provides time offset setting for viewing the detected objects in the desired time zone)
- Object Filter (Provides filter for the user to view only relevant objects)
- Video summarization
- Video display quality enhancement
- Restoration of vehicle numberplate

#### Image Enhancement

- Image editing and adjustment
- Crop, zoom, rotate/reverse, filter, color/brightness/contrast, super resolution, motion deblur, perspective transform, lens distortion correction, deinterlacing, focus correction, image overlay

#### File Exportation and Reporting

- Export original and converted file
- Format converter
- JPG and PNG format
- AVI and MP4 format
- MP3 and AMR format

   Summarized scene is saved as playable video file
- Assurance of evidence data integrity
- Supports report formats (PDF, Excel)

#### Hardware Acceleration

– Multi-core CPU/GPU support for video analysis acceleration

\*Contact us for more detailed product spec information





## **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.



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



#### **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.



#### 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.



#### 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.



#### 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.



#### **COMMUNICATION AND SOCIAL MEDIA ACTIVITY**

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

#### **ALL MAJOR BRANDS SUPPORTED**

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

## MOBILedit Smartwatch Kit

Essential hardware for smartwatch forensic analysis



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

#### SAMSUNG GALAXY WATCH READERS

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



#### **ALL-IN-ONE READER FOR APPLE WATCHES**

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

#### **GARMIN WATCH CABLES**

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

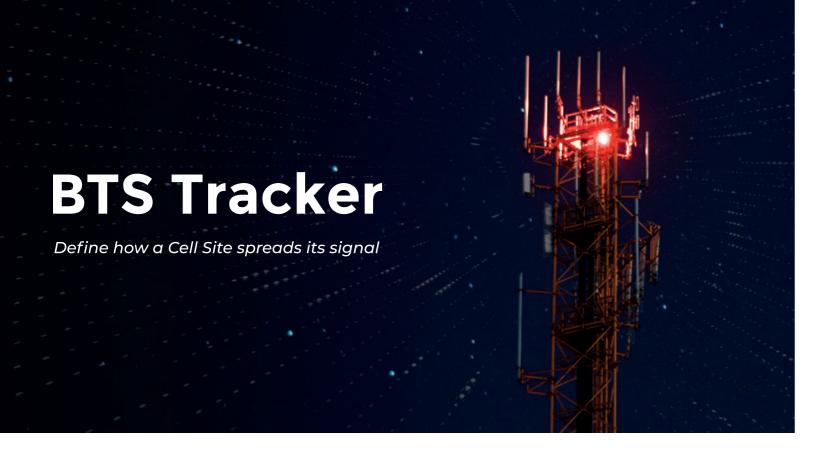
The kit also includes several adapters for various Samsung Galaxy Watch models, tools for smartwatch handling, accessories for smartwatch connection, and both USB-C and Lightning cables.

## MOBILedit Dive Kit

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







#### **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.

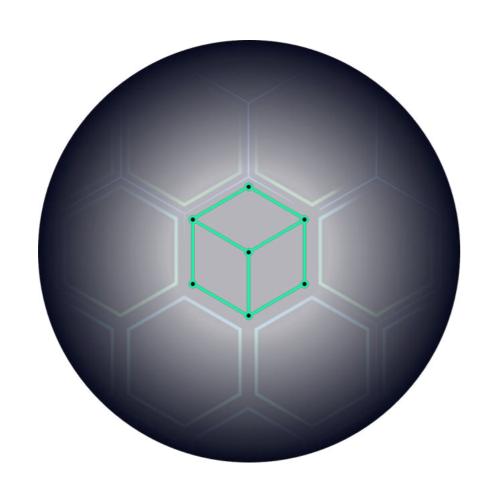








## Cyber Security

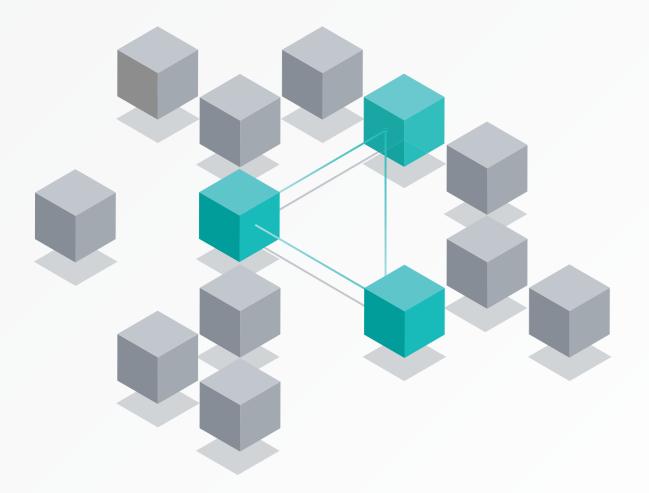






## IBM Security ReaQta

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

9

remote kill

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

Provides heuristic, signature

and behavioral techniques

in its multilayered defense

Makes remediation available

with automated or single-click

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

#### 6

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

#### 10

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

#### 2

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

#### 7

Simplifies and speeds response through guided or autonomous remediation

#### 1

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

#### 8

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

IBM Security ReaQta



## Degausser





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



Model: DEA-MW15000X

**Simultaneous Erasing Capacity** 

HDD

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

Charging time

17 seconds

**Magnetic Field Generated** 

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

## MagWiper MW-25X Degausser

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



Model: DEA-MW25000X

Simultaneous Erasing Capacity

HDD

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

Charging time

20 seconds

Magnetic Field Generated

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

## Features



#### 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.







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)

## 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.



NSA EPL listed compact, lightweight and efficient instant degausser.



Model: DEA-MW1B



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**



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



Only need to insert the target in the chamber, push the "Erase" button, and remove the target.



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



A cooling fan operates as required during the operation.

The chamber door locks on closure to



prevent operator hand insertion, or target ejection.



Meets PCI DSS, Data Security Standard, NIST Guidelines, NIST SP 800-36, NIST SP



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



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



**Operating** Indicator

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



The LCD shows total number of erasures and magnetic field intensity used for



Permits preparation of next load during















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	×	×	×	<b>✓</b>	
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 K.			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/10A, 220V/3A 100V/13A, 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

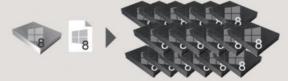


## DiskClon DC6000 Series

Disk Duplicator & Wiper

#### Why DiskClon Needed?





#### 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









#### Plug & Wipe

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









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







#### Specification

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.)			

<sup>\*</sup>For the improvement of product quality, the specification of hardware is subject to change without prior notice.

#### CLONIX Co., Ltd.

Backup / Restore / Cloning Solution Provider

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

Recruitment of Partner Company & Dealers



Contact sales@clonix.com



## **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



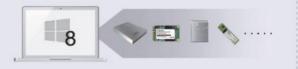
## **NetClon NC1000 Series**

Network-based Disk Duplicator & Wiper

#### Why NetClon Needed?

 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



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.



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



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

	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.)			

<sup>\*</sup>For the improvement of product quality, the specification of hardware is subject to change without prior notice.

#### CLONIX Co., Ltd.

Backup / Restore / Cloning Solution Provider

8F KyungDong Bldg. 4, SunaeRo 46 BeonGil BunDangGu, SeongNamSi GyeonGiDo, Korea

Tel. +82 70 7090 8280 Fax. +82 70 7016 2380 www.clonix.com

Recruitment of Partner Company & Dealers



Contact sales@clonix.com



## Blancco Drive Eraser for ITAD

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



#### Why Blancco

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

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

**View Our Certifications** 

#### Request Your Free Trial

**Get Started Today** 

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

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

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

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

#### **Key Benefits**

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



#### **Technical Specifications**

ERASURE	MINIMUM SYSTEM REQUIREMENTS
Locally or remotely controlled data erasure via the Blancco Management Console High-speed, simultaneous erasure of multiple drives, including the ability to customize drive batch sizes and drive speed thresholds RAID dismantling and direct access to the underlying physical drives SSD detection and secure erasure with Blancco's patented SSD method Automated detection and unlocking of freeze locked drives Detection, notification and erasure of hidden areas (DCO, HPA) and remapped sectors Support for internal drive erasure commands, including cryptographic erasure and TCG feature set on self-encrypting drives Ability to reformat SATA and SAS drives after erasure	1 GB RAM memory in most cases (2 GB for PXE booting)     Local erasure:     CD/DVD drive or USB port for booting the software     SVGA display and VESA compatible video card     USB port for saving reports      Remote erasure (requires Blancco Management Console):     Ethernet NIC     DHCP Server running on local network for PXE booting, remote erasure and report collection

USABILITY	REPORTING
Accelerated NIST Purge erasure  Multi-tasking to allow the hardware diagnostics and updating the report during the erasure time  Screensaver displaying the erasure progress to monitor the process remotely  Resume an erasure that has been interrupted without consuming extra licenses  Dedicated interface for loose drive erasure  Support for LAN and WLAN networks, including 802.1x authentication	Digitally-signed Certificate of Erasure Choose between asset level or drive-level reports Save reports locally or send them through the network to the Blancco Management Console Detailed reports enabled by enhanced hardware detection Extensive erasure information, including HDD details for seamless audit procedures User extendable report (with option to add "custom fields")

DEPLOYMENT	HARDWARE DETECTION & DIAGNOSTICS	CONFIGURABILITY & AUTOMATION
Blancco Drive Eraser is platform independent Local control with HASP dongles, standalone images, or centralized control through the Blancco Management Console or Blancco Cloud Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)	<ul> <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 Blancco products (BDECT, BMC, BUSBC)</li> </ul>	Customize erasure software to fit specific needs  Customize input fields in erasure reports  4 levels of process automation: workflow, manual, semi-automatic, automatic  Ability to communicate back and forth with an Asset Management System or other external system (IBR workflows) on asset and drive level  Fine-tune erasure process (speed/time limit, configurable conditions, etc.)  Execute customized workflows defined on the Blancco Management Console or Blancco Cloud, locally or remotely; automate the processing across all company assets

HARDWARE SUPPORT	AUDITING	LANGUAGE SUPPORT
Erase data securely from PCs, laptops, servers and storage environments based in x86 and x86-64 architectures BIOS & UEFI machines including Intelbased Macs, Apple T2 and Secure Boot IDE/ATA, SATA, SCSI, SAS, USB, Fibre Channel, FireWire hard disk drives of any size/blocksize SATA and SAS solid state drives of any size/blocksize AMMC drives of any size/blocksize NVMe drives of any size/blocksize SAS, SCSI, ATA and NVMe self-encrypting drives	Verification algorithms to automatically check the overwritten patterns Hexviewer provides fast visual verification of the erasure for compliance Reports offer tamper-proof reporting and can include a customized digital signature Embed reports in the drives for a fast erasure audit Search and export reports via APIs	English, German, Japanese, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian     Up to 20 different keyboard layouts supported

Copyright © 2022 Blancco Technology Group. All Rights Reserved.

## 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

## 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.





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

See more in the back

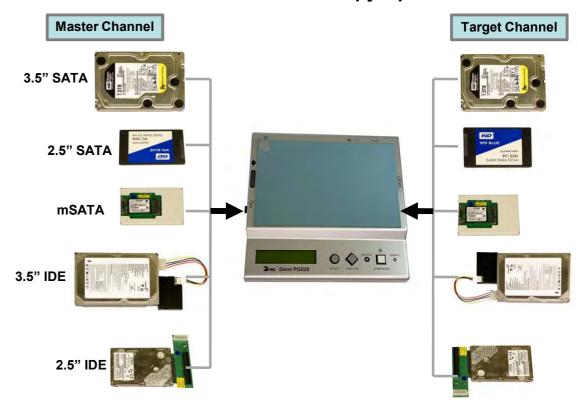
For more information, please visit www.yecglobalsolutions.com or call (657) 298-3276.

### DEMI PG520

#### **FEATURES**

- **DUPLICATION** All copy, All copy & compare, All compare, Error skip copy, File system copy & compare, File system copy, File system copy
- **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

#### 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

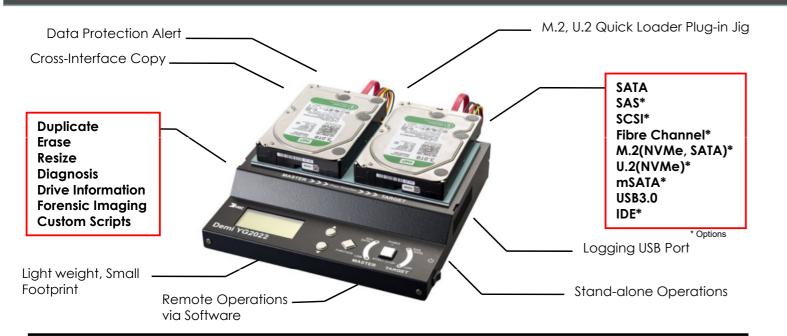
**Developed and Manufactured** YEC Co. Ltd.,

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

#### Latest M.2 and U.2 SSD Support

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

#### **NIST 800.88 Standards Compliant**

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

#### **Cross-Interface Copy**

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

#### **Safeguarding Data Against Unintended Overwrite**

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

#### More Than A Duplicator

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

#### File System and Mapping Copy modes make copy fast

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

#### **Data Recovery Copy Modes**

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

#### **Use Device As External Drive**

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

#### **Increase Power With Software**

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

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

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

### DEMI YG2022

#### **FEATURES**

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

**Target Drive** 

■ **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
SATA	0	0	0	0	0	0	0	0	0
SAS	0	0			0	0	0		
SCSI	0		0		0	0	0		
FC	0			0	0	0	0		
USB3.0	0				0	0	0	0	0
mSATA	0	0	0	0	0	0	0	0	0
IDE	0	0	0	0	0	0	0	0	0
M.2	0				0	0	0	0	
U.2	0				0	0	0		0

OPTIONS
SAS Kit
SCSI Kit
Fibre Channel Kit
mSATA Adapter
IDE Kit

M.2 NVMe/SATA U.2 NVMe Software

#### **SPECIFICATIONS**

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

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

#### www.yecglobalsolutions.com

Global Sales and Support

#### YEC Global Solutions, Inc.

10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A. T: 657-298-3276 sales@yecglobalsolutions.com

#### www.kk-yec.co.jp

**Developed and Manufactured** 

#### YEC Co. Ltd.,

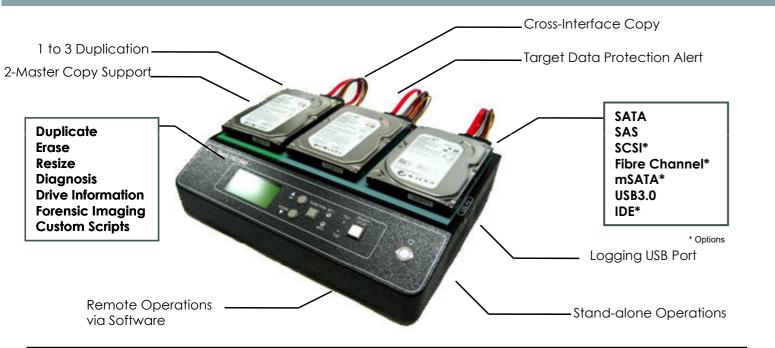
3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan

T:+81-42-796-8511 F:+81-42-796-2367

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

## Demi YG2040

## Dependable, Versatile Duplicator



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

#### A Wide Range of Interface Support

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

#### **Dual Master Drive Configuration Copy**

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

#### **Cross-Interface Copy**

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

## Proactive Data Protection from Unintended Overwrite

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



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

#### More Than A Duplicator

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

## File System and Mapping Copy modes make copy fast

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

#### **Data Recovery Copy Modes**

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

#### **Use Device As External Drive**

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

#### **Increase Power With Software**

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

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

### DEMI YG2040

#### **FEATURES**

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

#### **CROSS-INTERFACE CONNECTIONS MATRIX**

Master Drive mSATA 0 0 0 0  $\bigcirc$ 0 0 0  $\bigcirc$ 0 0 0 0 0 0 SCSI 0 0 0 0 0 FC 0 0 0 USB3.0  $\bigcirc$ 0 0 0 0 0 0 mSATA 0 0 0 0 0 0 0 0 0  $\circ$ 

**OPTIONS**SCSI Kit
Fibre Channel Kit
USB Kit (Target)

mSATA Adapter IDE Kit Terminal Software

#### **SPECIFICATIONS**

**Target Drive** 

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

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

#### 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

Developed and Manufactured

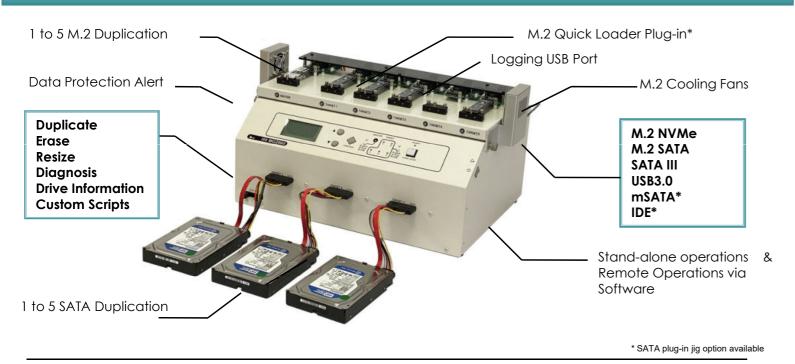
YEC Co. Ltd.,

3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan

T:+81-42-796-8511 F:+81-42-796-2367

## **HIT MG2060**

## PCIe M.2 & SATA **Duplicator**



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

#### M.2 and SATA Interface Support

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

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

#### Slow Drive Elimination – Reliable Performance

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

#### **Proactive Data Protection from Unintended Overwrite**

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

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

#### Reporting

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

#### More Than A Duplicator

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

#### **NIST 800.88 Standards Compliant**

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

#### File System and Mapping Copy modes make copy fast

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

#### **Low Maintenance**

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

#### **Increase Power With Software**

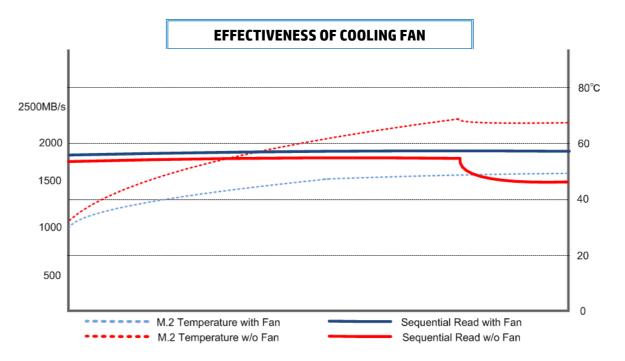
Optional software adds advantages furthermore in using HIT MG2060. It executes a script remotely, creates log files, work reports and CSV database and saves them in PC. Sold separately.

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

### **HIT MG2060**

#### **FEATURES**

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



#### **SPECIFICATIONS**

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

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

#### 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

**Developed and Manufactured** 

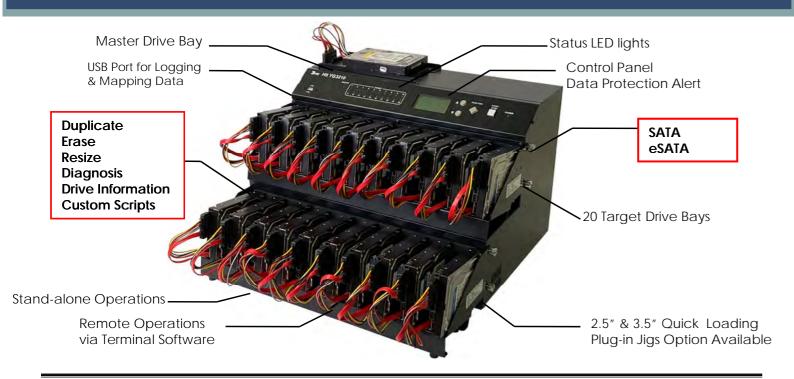
#### YEC Co. Ltd.,

3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan

T:+81-42-796-8511 F:+81-42-796-2367

## **HIT YG3210**

## Industrial Grade SATA Duplicator



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

#### Industrial Grade Duplicator

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

## Slow Drive Elimination – Keeping Copy Speed Fast User can set minimum transfer speed in the Configuration Management. When

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

#### 18 Duplication Scenarios

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

#### Proactive Data Protection from Unintended Overwrite

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

#### More Than A Duplicator

Mass target duplication is not the only advantage HIT YG3210 offers. As ar 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 event efficiently.

#### Increase Power with Software\*

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

\*Varies by device model

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

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

### **HIT YG3210**

#### **FEATURES**

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



Status Indicator LED



Detachable Plug-in Jig Option

#### **SPECIFICATIONS**

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

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

#### www.yecglobalsolutions.com

Global Sales and Support

#### **YEC Global Solutions, Inc.**

10541 Calle Lee Suite 121, Los Alamitos, CA 90720 U.S.A. T: 657-298-3276 sales@yecglobalsolutions.com

#### www.kk-yec.co.jp

Developed and Manufactured YEC Co. Ltd.,

3-44-45 Minamimachida, Machida, Tokyo 194-0005 Japan

T:+81-42-796-8511 F:+81-42-796-2367

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

# Media Shredder & Destroyer





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



### **Advantages**

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

#### **Shredding size**

#### **Electrical cabinet**





**Shredding blade** 





### **Specifications**

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





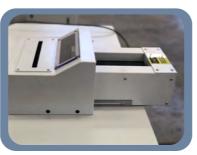
Shredder with double feeding ports designed for iPads and HDDs with H4 level.



### **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.

### **Feeding Ports**



Shredding blade





**Shredding size** 





Control panel



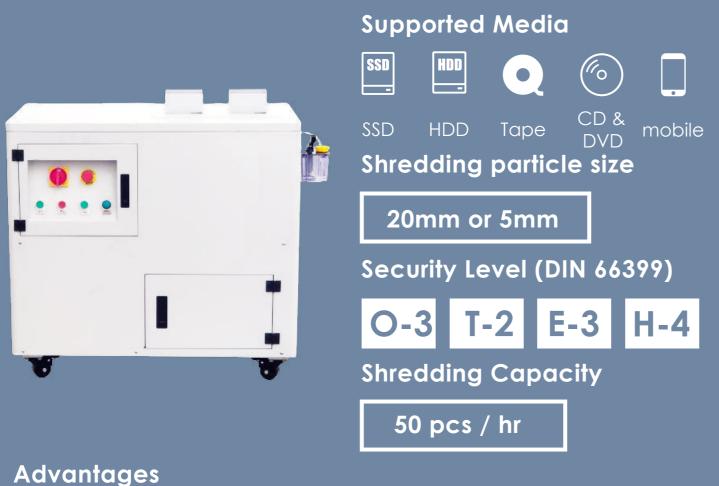
**Specifications** 

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





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



- 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** 





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





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



### **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





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

4

### **Supported Media**









Tape

mobile Floppy

Shredding particle size

More than 80% in 9\*9mm

Security Level (DIN 66399)

**Shredding Capacity** 

Approx in 320mm<sup>2</sup>

### Advantages

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

### **Shredding blade**





Shredding size





•	
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







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



### **Other Advantages**

- Combo blades with 4mm and 2mm with three step shredding construction.
- Specifically design for office environments.
- Solid hardened steel knifes which can shred the hard drives including the data diskes.
- 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	





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

# Supported Media







SSD Chip Memory chip

ID Card





Sim Card

CD & DVD

### **Shredding Particle Size**

### **Optional**

A. 0.5\*0.5 mm<sup>2</sup>

B. 1\*1 mm<sup>2</sup>

C. 2\*2 mm<sup>2</sup>

### **Shredding Capacity**

5 - 10kg / hr

## **Advantages**

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









**Electrical cabinet** 

Screen mesh



Filter system



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







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











small appliance disposal

HDD Computer printer PCB

Shredding particle size

20mm \* random or customized

**Shredding Capacity** 

500 kg / hr

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

### **Front view**







Side view

Shredding blade



**Back view** 

**Control panel** 







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





# Expert Server Hard Disk Shredder

### Powerful server hard disk and desktop shredder.



### Other Advantages

- Special Hardened Cutting Mechanism Door Safety Auto Sensor System
- Auto-Sensor Stop
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning

- Auto Control Reverse System
- Manual Function
- Safety Circuit Breaker
- High Quality Geared Motor

### **Optional Recording System**



**Shredding size** 



Waste collection Bin



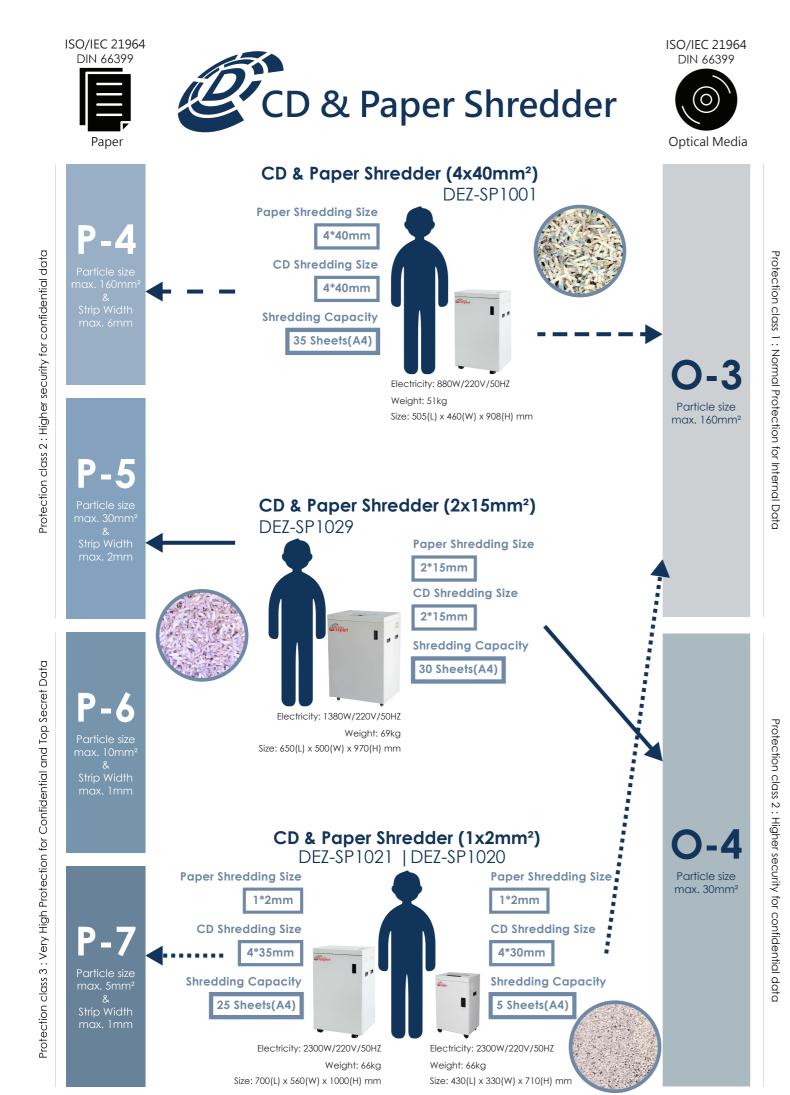
**Feeding Conveyor** 



Model: DED-SHS

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





## **Features**





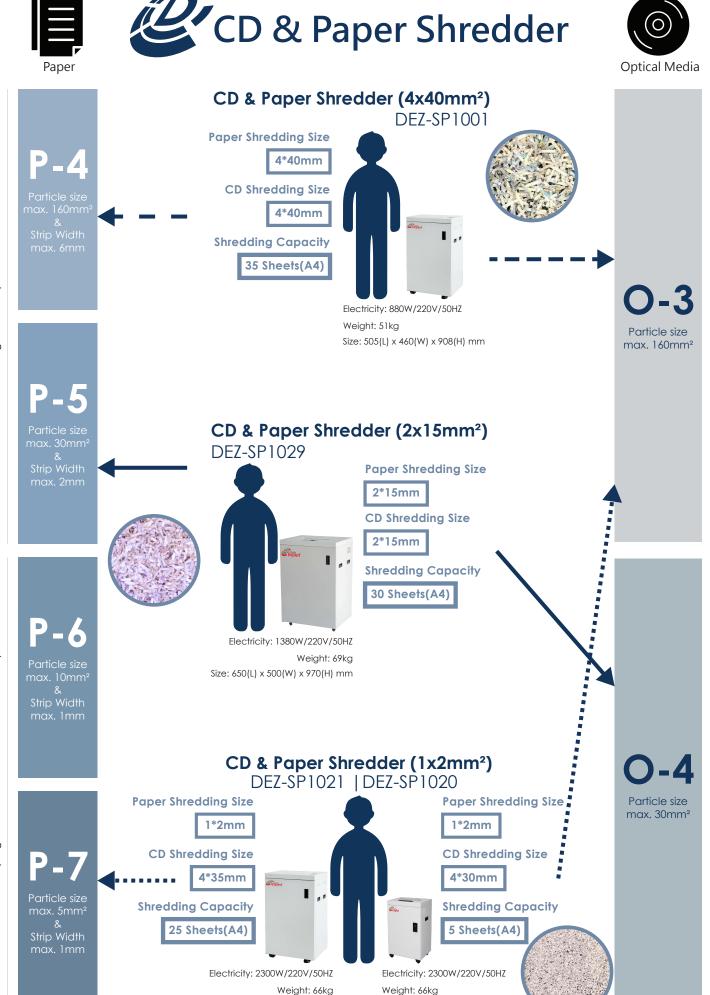




**Z** Sleep mode for saving energy

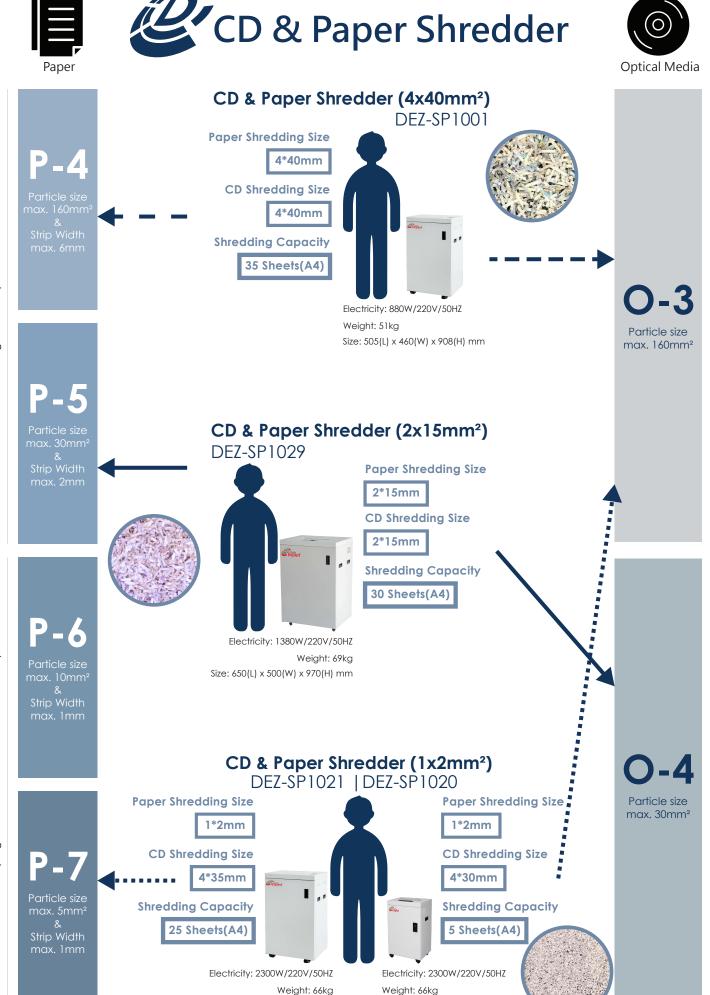


Model	SP1020	SP1021	SP1029	SP1001
Paper Shredding Size	1*2mm	1*2mm	2*15mm	4*40mm
CD Shredding Size	4*30mm	4*35mm	2*15mm	4*40mm
Security Level DIN 66399	P-7 /O-5	P-7 /O-3	P-5 / O-4	P-4 /O-3 /F-1
Shredding Capacity (70g/m²)	5 sheets(A4)	15 Sheets (A4)	30 Sheets (A4)	35 Sheets(A4)
Shredding Speed	2.2m /minute	2.2m /minute	2.2m/minutes	2.5m/minutes
Insertion Width	240mm	310mm	310mm	240mm
Bin Capacity	50L	100L	165L	90L
Power / Voltage / Frequency	550W/220V/50HZ	2300W/220V/50HZ	1380W/220V/50HZ	880W/220V/50HZ
Confinue 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



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

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



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

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

# **Features**



Durable shredding blade system



Auto reverse function for jamming paper



Full bin indicator



Motor overheat indicator



Z Sleep mode for saving energy



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



## 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)

**Shredding Capacity** 

1000 pcs / hr

# **Advantages**

- Special Hardened Cutting Mechanism
   Door Safety Auto Sensor System
- Auto-Sensor Stop
- Auto-Start by Micom System
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning

- Optical Sensor Sensitivity Recovery
- Auto Control Reverse System
- Manual Function
- Safety Circuit Breaker
- Oiler System
- High Quality Geared Motor

### Model: DED-CDS2

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







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

# 1919

### **Application**





CD & DVD

Paper

# **Shredding Particle Size**

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

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

## Security Level (DIN 66399)



# **Shredding Capacity**

600 pcs / hr

4,800 pcs / hr

### **Advantages**

- Special Hardened Cutting Mechanism
   High Quality Geared Motor
- Auto-Sensor Stop
- Auto-Start by Micom System
- Auto-Stop by Micom System
- Auto-Stop for Cutter Revolution
- Self-Diagnosis System
- Auto Cleaning
- Optical Sensor Sensitivity Recovery

- Manual Function
- Auto Control Reverse System
- Safety Circuit Breaker
- Oiler System
- Auto Oiling Alarm
- Door Safety Auto Sensor System

# **Model: DED-CDPS**

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







# **HDD Crusher**

# **Level H-3 Hard Drive Crusher Listed on NSA/CSS EPL for**



**End-of-Life Solutions for Over 50 Years** 

**Hard Disk Destruction Devices** 

Model No.: DED-HDC01





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

**Security Engineered Machinery** 

©2021 Security Engineered Machinery | All rights reserved

Extended warranty

### **Specifications:**

8 seconds per cycle
204 drives per hour
1 HDD up to 1.85" thick
4 standard notebook HDDs or 6 ultra-thin HDDs
Up to 5.625"W x 1.85"H x 9"D
115/1/60 International voltage available
7 Amps @120V / 1/3 HP – single phase
22" x 10" x 19"
115 lbs.
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

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

# **HDD Crusher**

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



### **CONFIGURATIONS**



### **0101-SSDKIT**

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



### 0101-DEP

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

31"H x 15.5"W x 24"D Dimensions:

64 lbs. Weight (empty): Weight (with 0101): 184 lbs.



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

# DED-OMS01

### **Level O-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:**

$\boxtimes$	
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) Weight	40 in. x 21.5 in. x 23.35 in. 231 lbs.
Electrical	120/1/60 or 220/1/50
	Requires dedicated line
Power	1HP
Warranty	1 year non-wear parts/90 days labor



- NSA EPL listed for CD destruction
- Waste bin full/door open indicator with auto stop
- Energy savings mode shuts off power when
- 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

0201-DEP

• Anti-static waste bin and anti-static bags\*

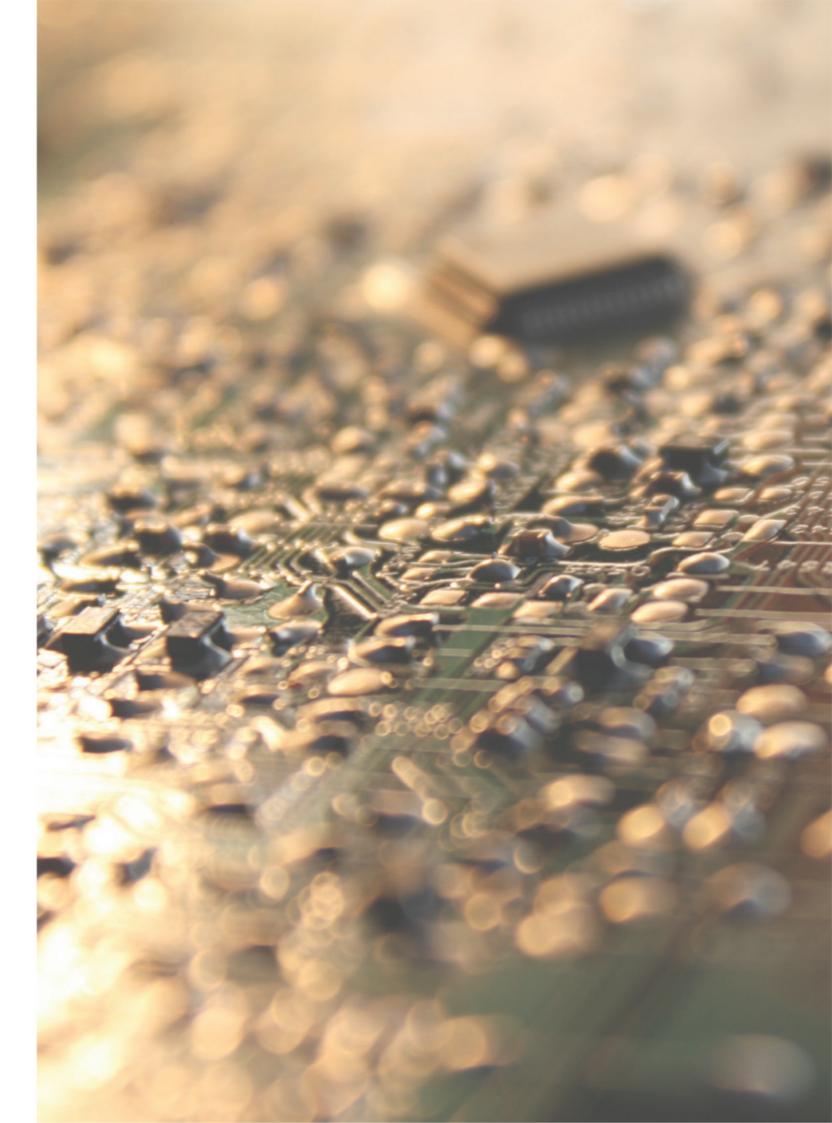
### **Options and Accessories:**

- Anti-static collection bags
- Oil packs



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.



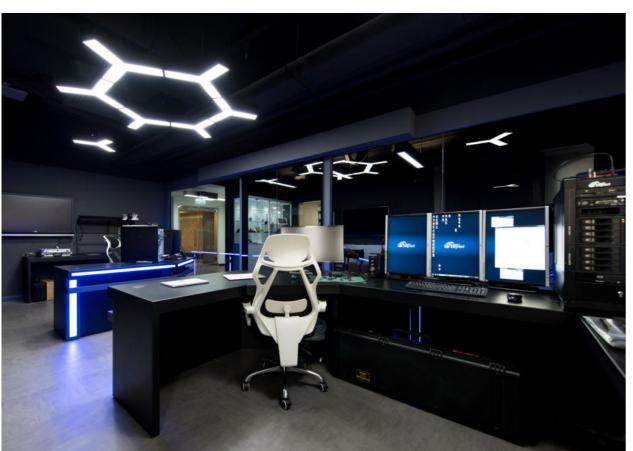


<sup>\*</sup>Unique to SEM









# **Technology Makes Possibility**

# Follow us



Website



Facebook



YouTube



LinkedIn