uWiPeR

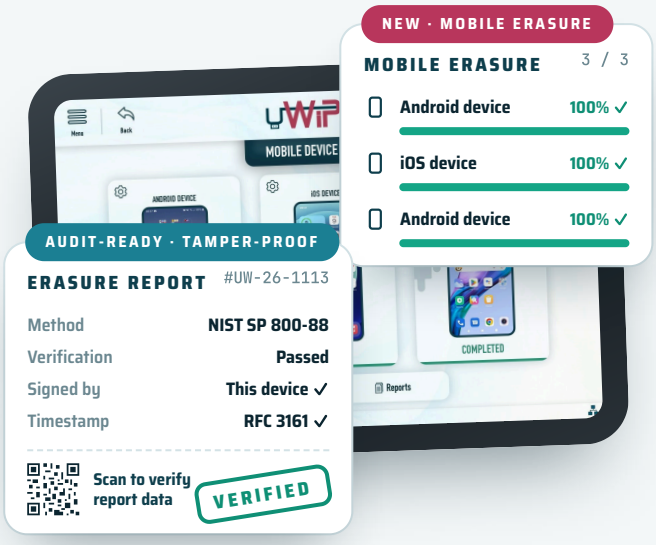
NEW Mobile erasure & hardware diagnostics

ONE TOUCH TO ERASE · VERIFY · REPORT

Erase everything. With a single device.

uWiPeR erases disks, SSDs, USB drives **and now Android & iOS phones** to international standards, verifies the result, tests phone hardware and hands you an audit-ready report for every single job.

- Standalone: no PC, no installation, no training
- Built-in verification on every job
- Hardware-signed, tamper-proof report with a verification QR code



4
Drives erased at the same time

13+
International erasure standards

9
Interface languages

0 PC
No computer or software installation needed

THE REAL PROBLEM

The real challenge isn't erasing data. It's proving the data is actually gone.

A deleted file is a missing signpost, not missing data. Auditors, regulators and courts don't ask whether someone pressed delete; they ask for evidence. **uWiPeR turns every erasure into a record you can show.**

Delete — file table only

Removes the entry in the file table. Every byte stays on the disk.

~~A4~~	~~E2~~	~~56~~	~~46~~	~~2A~~	~~FA~~	~~A1~~	~~15~~
78	6C	73	78	20	49	42	41
4E	20	54	52	31	32	20	30

Recoverable with any tools — Yes
Verified — No
Evidence for the auditor — None

Quick format — new file system

Rebuilds the file system and leaves the data underneath. Nothing is logged.

00	00	00	00	00	00	00	00
78	6C	73	78	20	49	42	41
4E	20	54	52	31	32	20	30

Recoverable with any tools — Yes
Verified — No
Evidence for the auditor — None

uWiPeR — every sector

Overwrites to the chosen standard, reads it back, then issues a tamper-proof report.

00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00

Recoverable with any tools — No
Verified — Read back
Evidence for the auditor — QR-verifiable report

Full disk

Bit-by-bit overwrite of the whole drive, hidden HPA/DCO areas removed on request.

Files & folders

Erase only what must go and keep the drive in service. The report lists every item.

Partition

Erase one partition to standard while the other partitions stay intact.

Mobile device NEW

Android and iOS phones, several side by side, with eSIM erasure and hardware tests.

GDPR · ISO/IEC 27001 · NIST SP 800-88

ERASE · VERIFY · REPORT

MOBILE DEVICE ERASURE

NEW Phones carry the most personal data. Now they get the same proof.

01 Connect and detect
Each phone appears with its make, model and battery level. Add more devices with one touch.

02 Pre-checks
uWiPeR warns you about a linked account, a low battery or a missing authorisation before you press start.

03 Erase
All phones are erased in parallel, Android and iOS side by side, including eSIM profiles and memory cards.

04 Completed and reported
Every phone gets its own report with the erasure and diagnostic results.



Not just erased. Tested and reported.

uWiPeR also tests the phone's hardware, from the touchscreen and cameras to the microphone, sensors and more. The results go into the device report, so every phone leaves both clean and graded for reuse, resale or return.

Touchscreen	PASS	Cameras	PASS
Microphone	PASS	Sensors	PASS

COMPLIANCE

Regulators don't ask whether you deleted it. They ask you to prove it.

GDPR · EU General Data Protection Regulation

`Art. 17` **Right to erasure.** Erase the media that holds the data to a recognised standard, disks and phones alike.

`Art. 5(2)` **Accountability.** Every job ends with a hardware-signed report: ID, timestamp, device, method and verification result.

`Art. 32` **Security of processing.** Verified overwrite before disposal, resale or reuse.

ISO/IEC 27001 & international standards

`A.8.10` **Information deletion.** Repeatable erasure jobs with records an ISMS auditor can sample.

`A.7.14` **Secure disposal or reuse of equipment.** Built-in verification, written into every report.

`NIST · PCI DSS · HIPAA` **Recognised methods.** NIST SP 800-88 Rev. 2 Clear and Purge plus 11 more standards, or your own pattern.

Tamper-proof reports. Proof anyone can check.

1 Signed in hardware
Signed offline by its own hardware, proving the report came from that very uWiPeR.

2 RFC 3161 timestamp
Whenever a connection is available, the signature gets a trusted timestamp.

3 One QR code
Even if the original file is lost, scanning the QR code verifies the information on the report.

What every report proves: Report ID · Make & model · Serial number · Capacity · Erasure standard · Pattern & passes · Verification result · Start & end time · Erased files & folders · Diagnostic results · Verification QR code · Thermal label

ERASURE STANDARDS

13 international standards. Or your own pattern.

- NIST SP 800-88 Rev. 2 Clear
- NIST SP 800-88 Clear
- NATO Standard
- British HMG IS5 Enhanced
- NAVSO P-5239-26
- Air Force SSI 5020
- OPNAVINST 5239.1A
- NIST SP 800-88 Rev. 2 Purge
- US DoD 5220.22-M
- British HMG IS5 Baseline
- CSEC ITSG-06
- GOST R 50739-95
- NSA 130-1
- Custom: your own pattern

- ✓ Quick, smart or full verification
- ✓ Format after erasure
- ✓ Remove HPA / DCO areas
- ✓ Adjustable block size

TECHNICAL SPECIFICATIONS

Simultaneous erasure	Up to 4 drives: HDD, SSD, USB · Android & iOS phones
Ports	2 × USB 3.2 · 1 × USB 3.0 · 1 × SATA III · Ethernet
Screen	10.1″ touchscreen · 9 interface languages
Body	Aluminium, fanless & silent · 248 × 167 × 20.5 mm · 850 g
Power	AC 100–240 V · DC 12 V 5 A
Label printing	Thermal label printers supported
Network	Ethernet, automatic or static IP · NTP time sync
In the box	Device, carrying case, power adapter, SATA cable, USB-to-SATA and NVMe-to-USB adapters

Erase it. Verify it. Report it.

info@difose.com
uwiper.com

DIFOSE
DIGITAL FORENSICS & SECURITY