Involatile

Recovering disk-encryption keys from volatile memory

The Problem

A forensics investigator seizes an encrypted machine.

Full-disk encryption works exactly as it should. There is no way around it.

Power it down

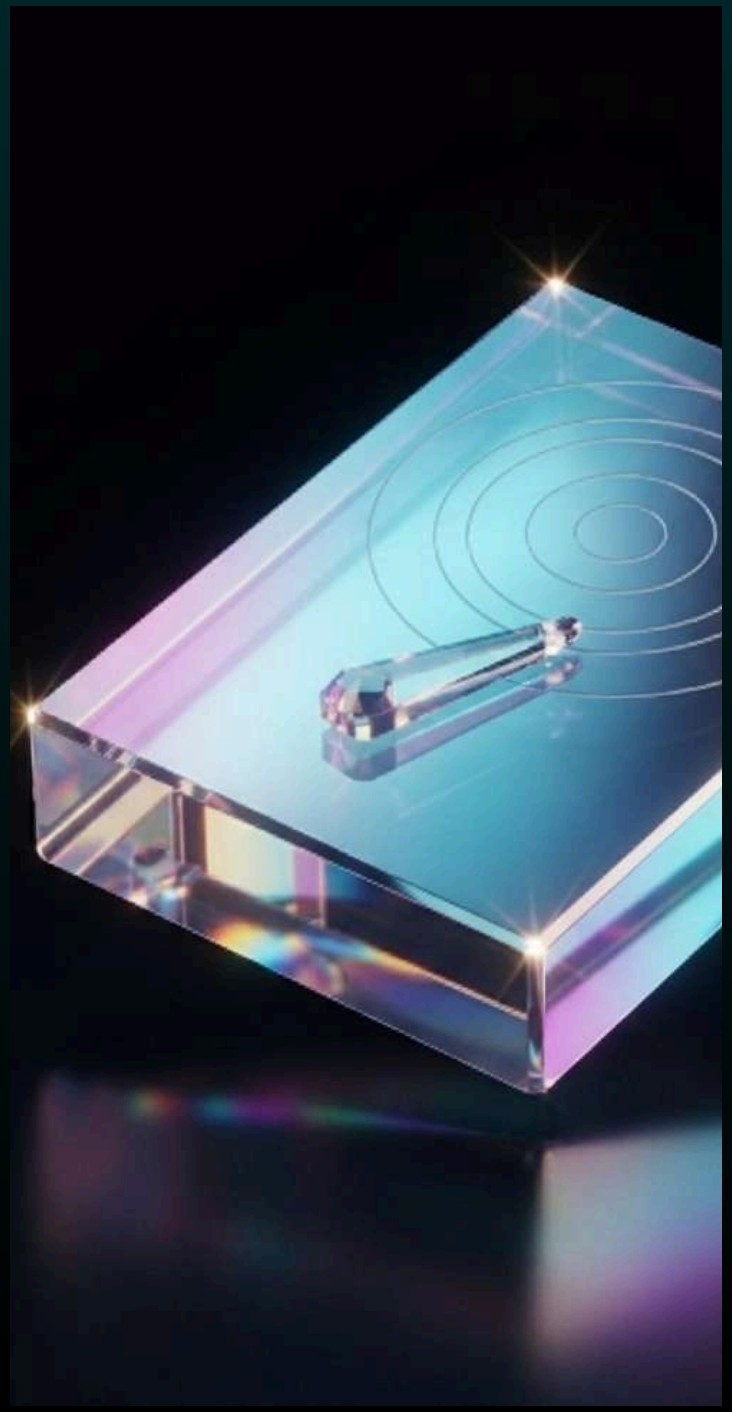
The decryption key may be gone forever. Evidence is lost.

Keep the machine running

The decryption key is in RAM, but RAM is volatile and power loss will erase everything.

The dilemma

Standard forensics procedure says don't pull the plug. So how do we get in?



The key insight

The lock on the screen and the lock on the disk are not the same lock.

To reach the OS login screen the machine has already decrypted the disk at boot, so the key is resident in memory regardless of whether a user is logged in or not

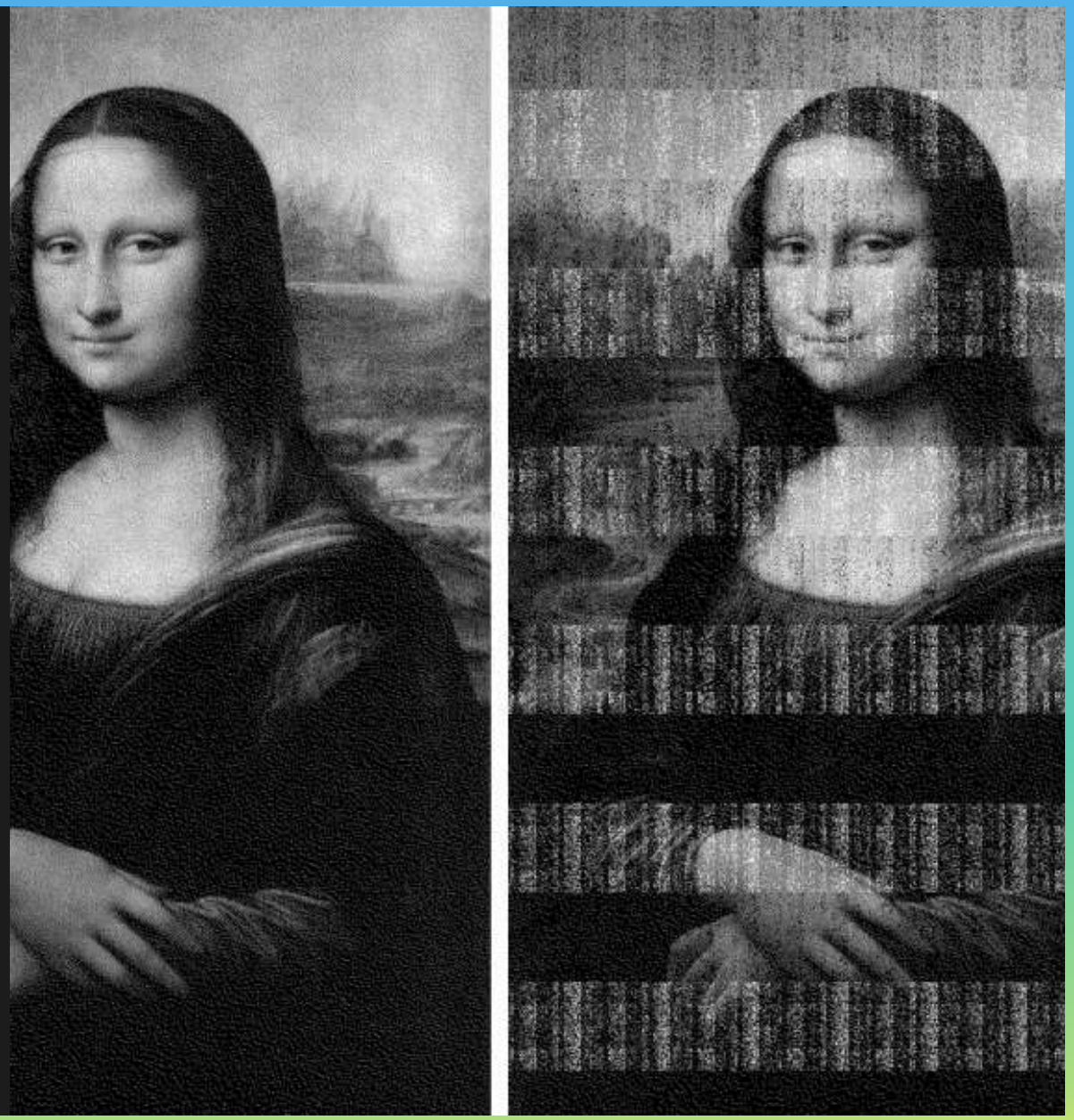
Involatile is a forensically sound tool that recovers disk-encryption keys from a memory image

How it works

1. **Find**
   Detect cryptographic keys by the structure of its key schedule

2. **Recover**
   Reconstruct keys even from partially degraded memory

3. **Report**
   Sound and reproducible evidence output an investigator can use



How does one obtain the memory images?

Live capture/VM snapshot

Software reads RAM on the running machine. Simplest way. Need privileged access on the target machine.

DMA attack

A peripheral pretends to be a DMA device and reads the RAM directly bypassing the OS.

Hibernation file

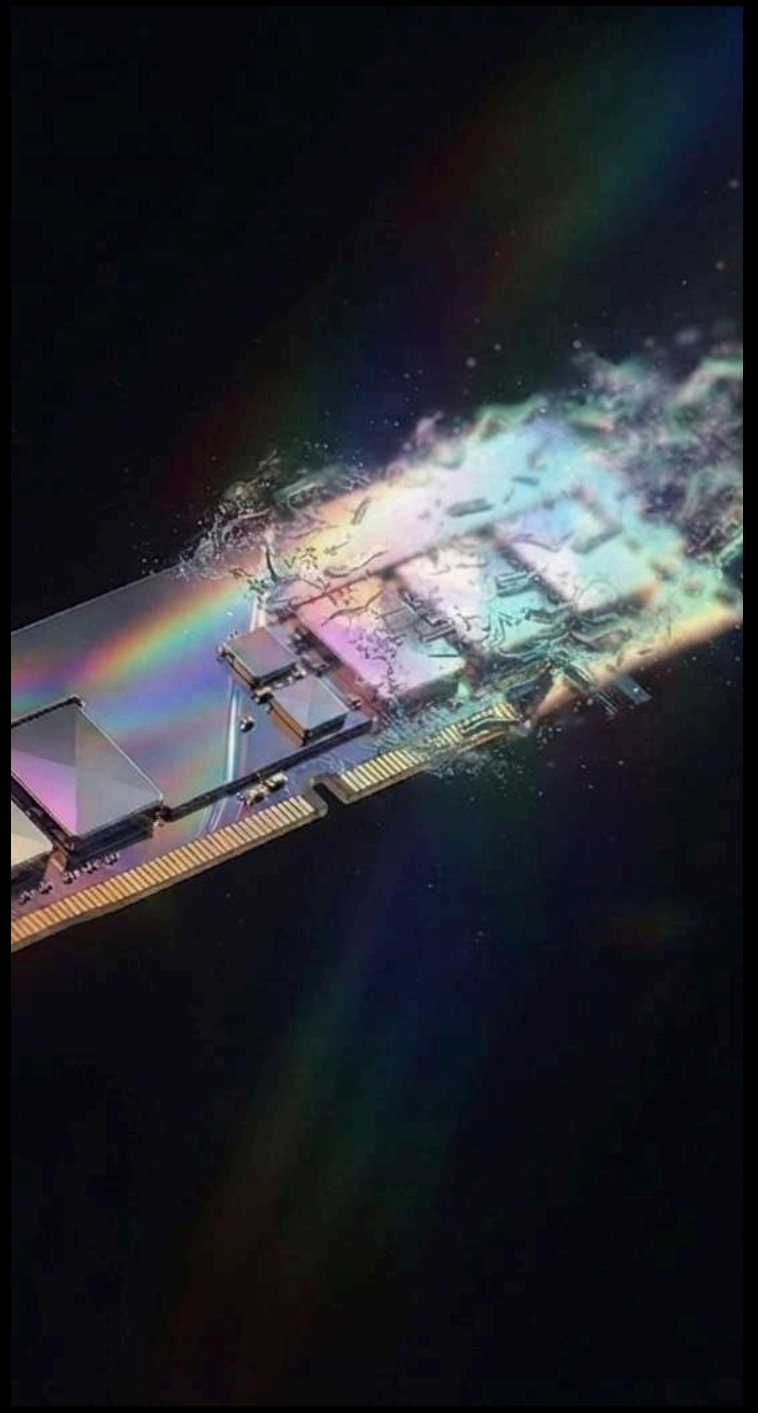
The OS writes all of RAM to disk on hibernate. If the disk only has encrypted partitions we can use the hibernation file to get the keys.

Cold boot attack

Physically chill the DRAM chips to slow the decay and then dump the contents. Can be done by booting into a minimal dumper or by transplanting the memory into another machine.

Recovering keys from decayed memory images

- Images obtained via the cold boot method will be decayed to a certain extent
- Decay is one-directional, so we know which bits to trust
- The key schedule's redundancy lets us rebuild the key from what survives



Forensic Soundness

Never alter the evidence

Read-only handling

Neither the memory image or the evidence drive is ever modified

SHA-256 integrity

Hash on ingest and re-hash after. Unchanged hash proves nothing was altered

Chain of custody

An append-only audit log records every operation, with timestamps.

- **Integrity is proven**
  Image will not change after acquisition
- **Authenticity is supported**
  Live capture is never a perfect snapshot,so the method is documented

Proving it works

Success is measured against known ground truth

- We will generate our own memory images with known keys, so we can check the tools output with the correct answer
- We will measure recovery rates against both clean and decayed memory images
- We will show how much decay the tool can handle before it fails

Live Demo

Locked

An encrypted volume. Inaccessible. Contents sealed.

Recover

Run the tool on an obtained memory image. Key is recovered.

Mounted

Use the key to mount the drive and obtain access to files.

The Scope

In Scope

- AES-128/256 key recovery
- Multi-format image ingest
- Soundness, reporting and evaluation
- Decay tolerant reconstruction

Out of scope

- Not a general memory-forensics suite
- Defeating hardware memory encryption
- Raw/ECC key recovery

Limitations and Defenses

Hardware memory encryption

RAM itself is encrypted. Only used on enterprise machines.

Secure boot

Unsigned OSs will refuse to boot. Makes getting the memory image difficult.

IOMMU/Kernel DMA Protection

Restricts what a peripheral device can read, blocks DMA attacks.

TPM (Trusted Platform Module)

Guards the key at rest. Not while in the RAM.

Thank you.

Jaindu Charindith 230102V

Nemith Kaluarachchi 230311K

Thimalka Wijepala 230717K