



FIND. DECRYPT. OPEN.



Toni Pärn
Director of Sales



Passware **Kit Forensic**

Passware Kit Forensic



390 file types

Full Disk Encryption

Memory Analysis

Batch Recovery

New Network-Distributed Password Recovery Engine



Tools Help

Recover Password

Items
Passwords Found
Resource Manager
Performance
Attacks
Log
Network Log

ITEM NAME	STATUS	PASSWORDS FOUND	SPEED	PASSWORDS CHECKED	TIME
myr-owerpoint.ppt	password not found				
MyOldWord.doc	Password found	Open-Password: jjj Modify-	—	—	—
MyAcronisBackup.tib	Password found	Open-Password: 1234	—	—	—
My... > ap.alexander.peresvet@gmail...	Password not found		—	—	—
MyExcelTable.xlsx	Password found	Open-Password: MyPasswor	—	—	—
a9-two pwds.pdf	Password not found		—	—	—
AcronisBackup-AES256.tib	Password found	Open-Password: 1234	—	—	—
CUSTOM RECOVERY #3 Skip group					
a7-full-encrypted-speed.pdf	Password found	Open-Password: speed	—	—	—
Western Digital My Passport 2626	Password not found		—	—	—
wallet.dat-Test12345	Item skipped	Resume			
MyAppleDMG.dmg	<div style="width: 20%; height: 10px; background: linear-gradient(to right, green, white); border: 1px solid #ccc;"></div>	Skip	251 p/sec	884	4 seconds
MyAppleNotes.sqlite > iCloud	Waiting	Skip	—	—	—
MyApple... .sqlite > My very secret note	Waiting	Skip	—	—	—
MyDriveCrypt.dcv	Waiting	Skip	—	—	—

PASSWORDS FOUND
22

PASSWORDS CHECKED
22,357,857

TIME ELAPSED
9 minutes, 43 seconds

SEARCH SPEED
295 p/sec

PROCESSING ITEMS 2 OF 37

MyDriveCrypt.dcv

MyAppleDMG.dmg

CURRENT ATTACKS (285 PLANNED)

243. Brute-force attack

244. Xieve attack

245. Brute-force attack

CURRENT PASSWORD
wi

LENGTH
2

Manage Attacks
Manage Items
PAUSE
STOP

Support for hashcat rules



Attack S

BASIC ATTACKS

- Dictionary
- Xieve
- Brute-force
- Mask
- Known Passwords/Part
- Previous Passwords

GROUPS

- Join Attacks
- Append Attacks

ADVANCED

- Apply Rules**

New Apply Rules Attack

The Apply Rules attack functions like a programming language specifically designed for generation password candidates. It includes function to modify, trim, or extend words, along with conditional operators to filter results. [Learn more...](#)

SETTINGS

Rules file

Comment

Sample passwords [↻](#)

Passwords to check 0



Hardware Benchmark

The benchmark data is provided by Passware customers.
GPU speeds may vary depending on the CPU and the version of Passware Kit.

Check our [hardware recommendations](#) and how to use the [Hardware Benchmark](#) feature in Passware Kit.

Graphics processing units (GPU)

Central processing units (CPU)

Graphics processing units (GPU) Benchmarks

Show additional GPU info

Search



GPU	↑↓	Cores	↑↓	MSRP \$	↑↓	MS Office 2010	↑↓	MS Office 2013-2019	↑↓	APFS (encrypted)	↑↓	FileVault Non-system	↑↓	iTunes Backup 10.2	↑↓	RAR 5.0
NVIDIA GeForce RTX 5090		21,760		1,999		488,082		85,727		189,138		141,883		867		33%
NVIDIA RTX 6000		18,176		6,799		303,502		50,304		120,245		88,729		684		20%
NVIDIA GeForce RTX 4090		16,384		1,599		296,522		48,581		117,395		85,859		831		20%
AMD Radeon Instinct MI250		13,312		12,000		136,558		N/A		53,243		39,770		N/A		9%
NVIDIA GeForce RTX 5080		10,752		999		261,022		44,984		97,938		73,272		523		17%
AMD Radeon RX 7900 XTX		12,288		999		256,293		34,545		92,904		71,400		379		

Password list export



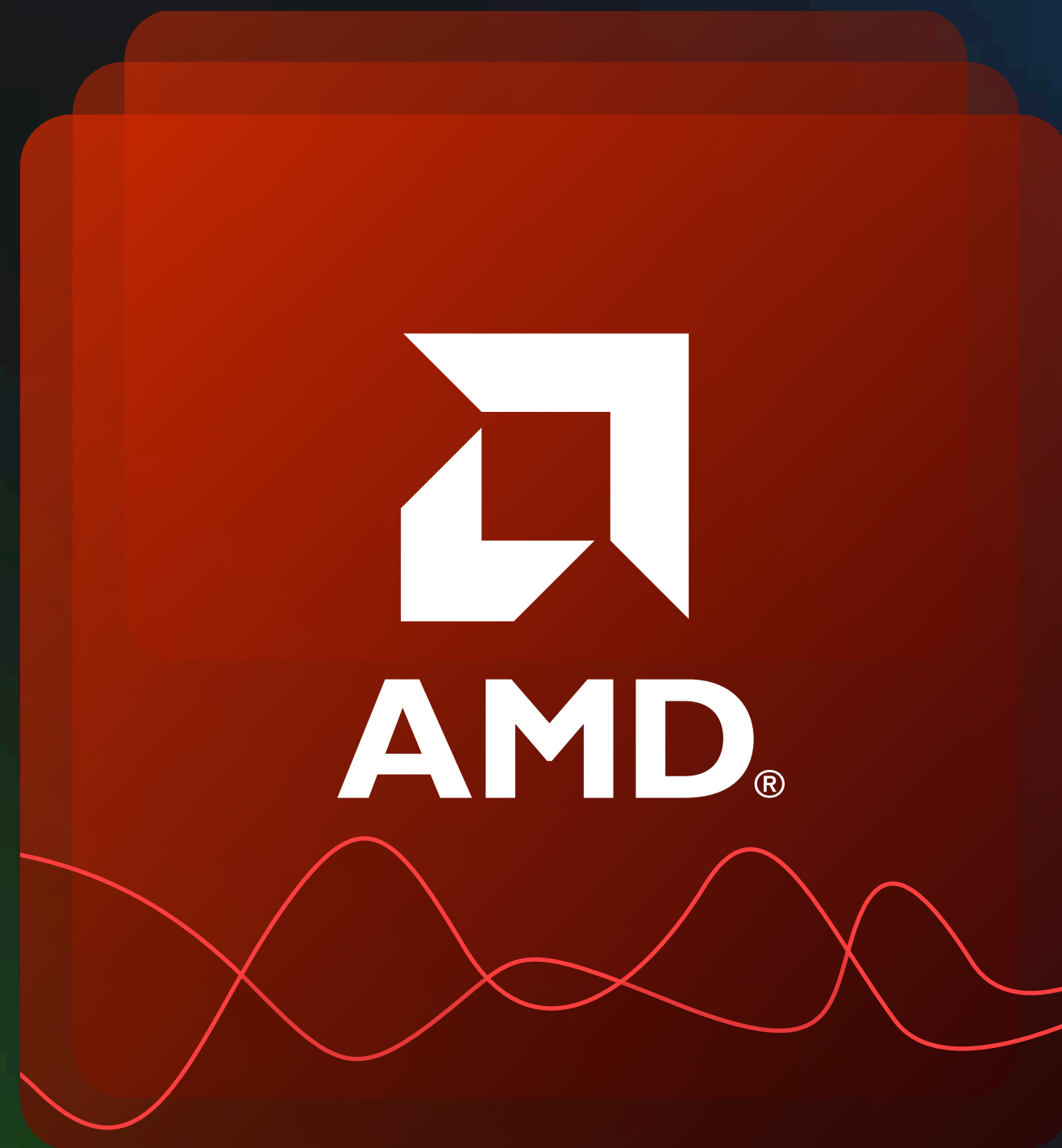
Attack Settings

ATTACK	LANGUAGE	LENGTH	SETTINGS	PASSWORDS ...	COMPLEXITY	COMMENT
Apply Rules	—	—	—	211,048,200	●●●●●	
Join Attacks	—	—	Trim from 5 to 6 chars	4,138,200	●●●●●	
1 1. Dictionary	Passware Dictionary Small	1 – 128	Known parts: e*	14,871	●●●●●	
2. Brute-force	English	1 – 4	Numbers	11,110	●●●●●	
3. Mask	English	3 – 3	Mask: ?s?d?s	10,890	●●●●●	
<input type="button" value="+"/>						

1 ITEM SELECTED

- Cut
- Copy
- Paste
- Move Up
- Move Down
- Move To Top
- Move To Bottom
- Export passwords list**
- Remove

Support for all major GPU vendors





Passware **Kit Mobile**

Passware Kit Mobile



30,000+

Extractions

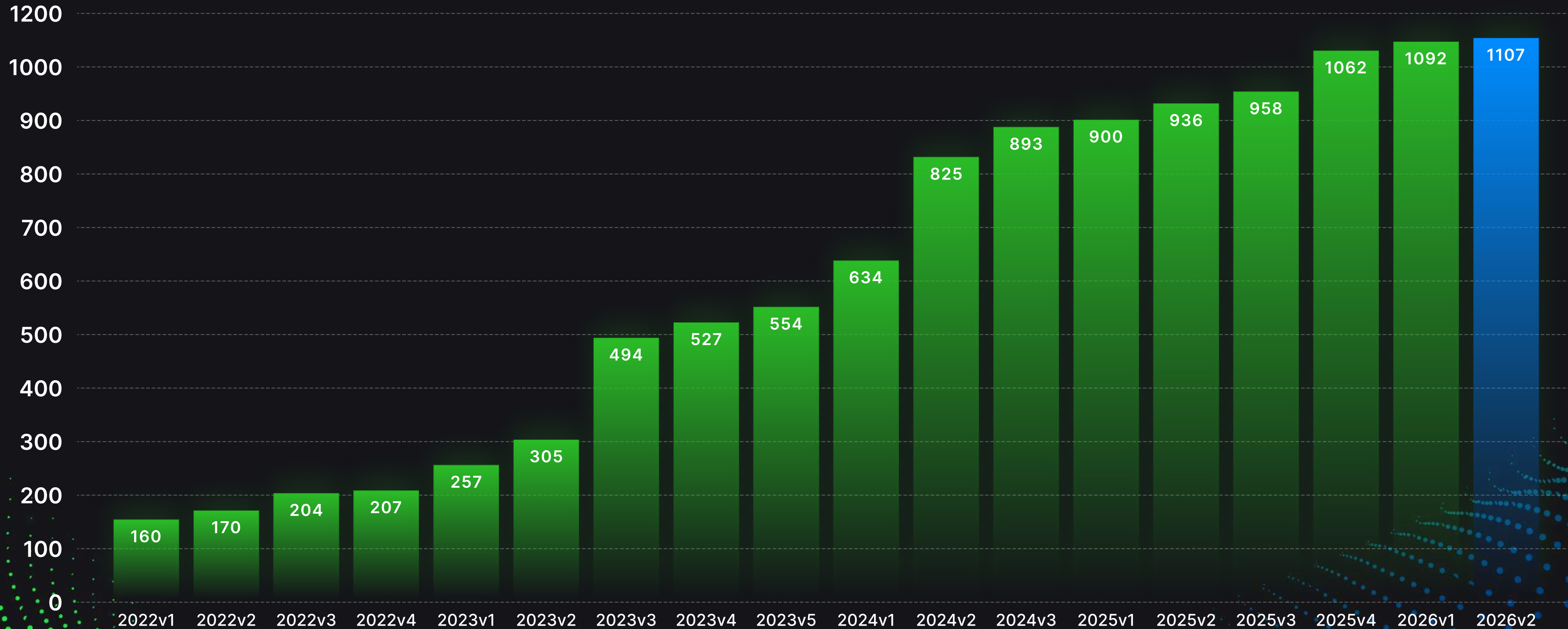
675+

Customers

85

Countries

Supported Devices: 1,100+ in 2026 v2



Huawei Decryption



Home navigation icons: Home, Back, Forward, Refresh


Tools Help [Smiley Face] [Minimize] [Maximize] [Close]

Huawei P20

Folder: Huawei P20

CPU	DATA	ENCRYPTION	PASSWORD RECOVERY	PASSWORD TYPE	LENGTH	CHARACTERS
HiSilicon KIRIN970	111.45 GB	File-Based	Accelerated, On Workstation	Pin	Unknown	Digits Only

Items Passwords Found Resource Manager Performance Attacks Log Network Log



Huawei Device

Folder: E: \ Passware \ PKM \ Huawei P20

Item Type: Huawei Kirin Device — Numerical Passcode, Partial decryption possible, Hardware acceleration possible

Device: Huawei P20 (EML-AL00)

Complexity: ●●●● Brute-force - Medium

Userdata MD5: 9577D3F31FB4C0CB74414575E61C1DDE

Some passwords or encryption keys were not found.
There is an alternative method of partial data decryption without recovering the password.

[TRY PARTIAL DECRYPTION](#)

Password: Huawei device password **Not found**

Extracted data: **E: \ Passware \ PKM \ Huawei P20 \ unprotected**

MD5 hashes for files: **E: \ Passware \ PKM \ Huawei P20 \ unprotected \ Md5Hashes.txt**

PASSWORDS FOUND	TIME ELAPSED
0	3 minutes, 20 seconds
PASSWORDS CHECKED	
10,000	

Print

[RESUME ATTACKS](#) [SAVE REPORT](#) [DONE](#)



Hi Dimitry,

Yes, I ran it over the weekend, it didn't get the recovery keys or the pin as expected but I did get a partial decryption which has recovered a lot of media which has been very helpful.

It's the only tool that was able to get anything from the phone, im a big fan of the tool


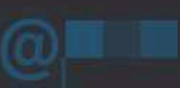



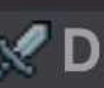






Thank you







Digital Forensics Investigator



FIB Digital Forensics Unit Syndicate 1. | Team 1


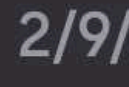
























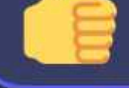












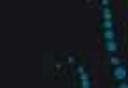

 7/11/25, 1:59 PM
 Passware Kit Mobile has support for the 4S if you have access to that


 1 

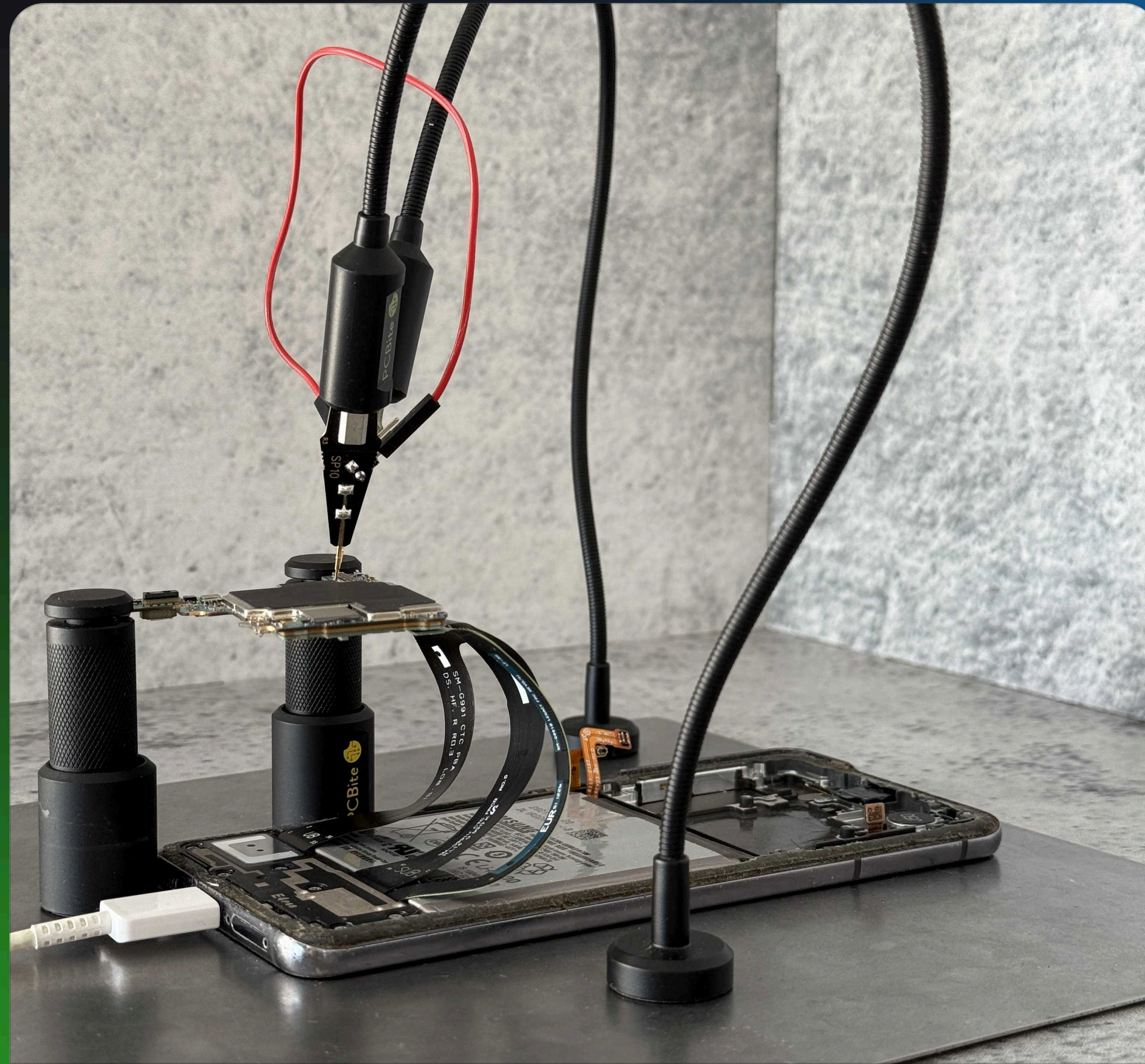

 2/9/25, 9:22 PM
 Passware Kit Mobile is what you need 👍

 4 

 7/2/25, 11:37 AM
 Good decryption and support for many smaller android manufacturers - and their support will also help in individual cases with custom builds for individual troublesome models

Samsung S20/21





Device Decryption **Add-On**

Device-Decryption Add-On



**Macs with Apple T2
Security Chips**

Western Digital Disks

Lenovo ThinkPad Laptops

Seagate and LaCie Drives



Tools

Help



Device with TPM and PXE

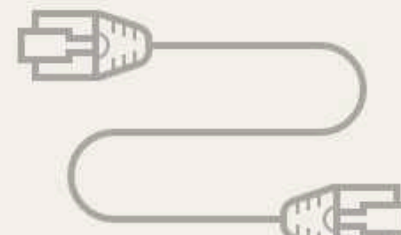
Check if Device is Supported › Prepare Bootable Server USB › **Extract Keys** › Decrypt Disk Image



Prepare target device



Prepare secondary computer



Turn on and boot the computers to the appropriate modes



Save the VMK HEX file to the Passware Bootable Analyzer USB (Disk 1)



Extract the encryption keys

Connect the bootable USB Disk 1 to this computer and **browse for the dump.bin file**

G: \ dump.bin

Browse...

The encryption keys have been extracted. You can now restore the original device firmware and decrypt the disk image.

VMK Key **SeH/fv8nCaU70Sqo6rShtic8NoCnTWedzjYuqBwhLSk=**

VMK Key File **E: \ Encrypted Laptop \ ... \ vmk.txt**

Recovery Key **717750-008470-287298-033044-132880-432300-581680-524403**

PREVIOUS STEP

NEXT

Transcend SSD



BitLocker PIN recovery



Tools Help

Desktop with AMD Zen fTPM

Check if Device is Supported > Patch Firmware > Extract Keys > Restore Device > Recover PIN and Decrypt Disk


Create Passware Bootable Analyzer USB

Boot the target device from USB

Check if the device is supported

Connect the bootable USB disk to this computer and browse for the **Passware_Bootable_Analyzer_Results.bin** file

F: > Passware_Bootable_Analyzer_Results.bin



The device is supported

The computer is protected with TPM and BitLocker PIN.
Before decrypting the disk image, Passware Kit recovers the BitLocker PIN.
Recovery process can be time-consuming.



Passware **Kit Ultimate**



7/22/25, 12:22 PM
 Good news about Bitlocker with TPM 😊 https://youtu.be/v4AFKRvUHbo?si=oG_BL4UAiEJad2yr (edited)

YouTube

Passware

What's New in Passware Kit 2025 v3

DFIR 🇨🇦 12/2/24, 6:45 PM

Anyone have experience with the **@Passware Support** Device Decryption function? Wondering if the unlocking feature for Western Digital My Passport drives is an instant unlock, or brute force procedure.

DFIR Anyone have experience with the **@Passware Su...**

DFIR 🇬🇧 12/2/24, 10:14 PM

As long as it's a supported model it gives you the option to temporarily instant unlock and mount the drive to get data access (you can then acquire it using something like FTK imager) when the drive power cycles it is locked again, or you can try and crack the password, speeds were really fast (closer to NTLM speeds). We've used both methods with great success!

👍 1

From reading the readme, is this only ...

DFIR 🇬🇧 10/18/24, 8:24 AM

Yes. Pre T2 only. If you want to crack T2 Macs you will need Passware device decryption addon. Very useful, we've had countless successes with it 😊

📧 1 **this** 2

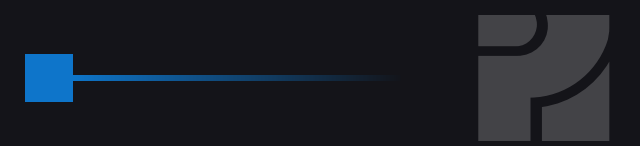
Good news about Bitlocker with TPM 😊 h...

DFIR 🇬🇧 7/25/25, 12:47 PM

Just to give a shoutout to **@Passware Support** about this. I've used BitPixie exploit loads of times with success, but today had a complete POS HP device which just wasn't playing ball with BitPixie exploit, had no pcie slots for DMA attacks either. Tried the new Passware implementation for TPM and it worked first time 🥳, key extracted and data decrypted!

🥳 5 🥳 8

What Makes Passware Unique?



Comprehensive Device and File Support



Exclusive solutions

for BitLocker-encrypted devices, Lenovo ThinkPads, Macs with T2 chips, Seagate disks, select Huawei mobiles, and other devices.



Network-distributed

agent that runs on Windows, Linux, and in the cloud, offering hardware-accelerated password recovery with linear scalability, and remote management.



Custom software versions

tailored to help with high-profile cases.



Live Demo



Future **Roadmap**

Passware Kit Forensic Roadmap



BitLocker Autopilot

Steganos containers V22

LastPass IndexedDB support

Cache checked passwords for
slow attacks

Bitlocker Magic Stick

Passware Kit Mobile Roadmap



Rockchip tablets

DPR+ for Android

Exynos 1280 - Samsung A53 and more

Exynos 9611 - Samsung A50/51 and more

Exynos 850 - Samsung A12/13 and more

Cache checked passwords for slow attacks



Q&A



Thank You!