

A quick guide to our device extraction methods.



Locked Android devices



Huawei Kirin

Support for devices based on 710, 710F, 810, 659, 960, 970, 980, 985, 990, and 990 5G Kirin chipsets, having File-Based Encryption and running Android OS 9 and 10.



Huawei Qualcomm EDL

Support for devices based on MSM8917, MSM8937, MSM8940, and SDM450 Qualcomm chipsets and having File-Based Encryption. Passcode brute force is available.



Samsung Exynos

Support for devices based on Exynos chipsets, having Full-Disk Encryption and running Android OS 7, 8 and 9 or upgraded to Android OS 10 - 11.
Support for devices based on Exynos chipsets, having File-Based Encryption and running pre-installed Android OS 9 and 10 or updated to Android OS 11. Passcode brute force is available.



MTK Android

Support for devices based on MT6737, MT6739, MT6580, and MT6753 chipsets and having Full-Disk Encryption. Support for devices based on MT6765, MT6768, MT6785, MT6761, MT6893, MT685, MT6771, MT6873, MT6781, MT6877 and MT6833 chipsets and having File-Based Encryption. Support for Samsung devices with the Helio G80 chipset and Huawei devices with MT6765 chipset. Passcode brute force is available.



MTK Android via boot modification

Support for MTK devices with an unlocked bootloader and having Full-Disk Encryption.



Sony Android

Support for MTK-based Sony XA1, Sony L1, Sony L2, and Sony L3 devices having Full-Disk Encryption. Passcode brute force is available.



Spreadtrum Android

Support for devices based on Spreadtrum chipsets and having Full-Disk Encryption. Decryption support for SC7731E, SC9832E, SC9863, and SC9850 chipsets. Passcode brute force is available.

Support for devices based on the UNISOC T610/T618/T700/T310/T606/T612/T616/SC9863A chipsets, running Android OS 10 - 13 and having File-Based Encryption (FBE).



LG Qualcomm LAF

Support for LG devices with Android OS 6 - 7 and based on MSM8917, MSM8937, MSM8940, and MSM8953 Qualcomm chipsets.



Qualcomm EDL

Support for devices having Full-Disk Encryption (FDE) and based on MSM8909, MSM8916, MSM8939, MSM8952, MSM8917, MSM8937, MSM8940, and MSM8953 Qualcomm chipsets. Support for Qualcomm Snapdragon 845/710. Passcode brute force is available.



Unlocked Android devices



Android full file system

File system extraction of Android OS 10 devices with File-Based Encryption as well as Android OS 7 - 10 devices based on Qualcomm chipsets with Security Patch Level no later than October 2022.



Android physical

Temporary rooting of Android devices running Android OS 4.0 - 10.0. The Security Patch Level date must not exceed October 2019.



Android Agent

Logical data extraction via USB and Wi-Fi of Android devices running Android OS 4.1 - 14.0. Manual extraction of selected apps is available as well as automated screenshots/screen recordings of device data.



APK Downgrade

The Android app downgrade method covers 45 most popular apps and is compatible with Android OS versions 5.0 - 13.0.

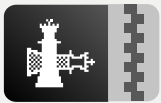


Android backup

Logical data extraction via ADB backup of Android devices running Android OS 4.0 - 11.0.



Locked iOS devices



iOS full logical checkm8

Partial file system extraction in BFU mode. Supported devices include Apple's A7 to A11 SoC, which includes iPhone 5s through iPhone X and running iOS up to 15.8.2.



Unlocked iOS devices



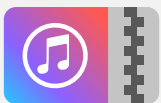
iOS full logical checkm8

Full file system and keychain extraction in DFU mode. Supported devices include Apple's A7 to A11 SoC, which includes iPhone 5s through iPhone X and running iOS up to 15.8.2.



iOS full logical via SSH

Full file system and keychain extraction of devices already jailbroken with various jailbreaks including checkra1n and unc0ver.



iTunes backup

Logical extraction via the iTunes backup procedure of Apple devices running iOS 8.0 - 17.0.



iOS Agent

Full file system extraction via iOS Agent from Apple devices running iOS versions 14.0 - 14.3, 14.4 - 14.5.1, 14.6 - 14.8.1, 15.6 - 15.7.1 and 16.0 - 16.5.1.
Full file system and keychain from iPads based on the A8 - A15, M1, and M2 chipsets and running iPadOS 15.0 - 15.7.3, and 16.1 - 16.5.