



A quick guide to our device extraction methods

A locked Android device

1. Huawei Android Dump

Extraction and decryption of devices based on 710, 710F, 810, 659, 960, 970, 980, 990, 990 5G Kirin chipsets, having File Based Encryption and running Android OS 9 and 10.

Passcode brute force is built-in.

2. Samsung Exynos Dump

Extraction and decryption of devices based on Exynos chipsets, having Full Disk Encryption and running Android OS 7, 8 and 9.

Passcode brute force is available.

3. Qualcomm EDL Dump

Extraction of devices based on Qualcomm chipsets and having Full Disk Encryption. Decryption support for MSM8909, MSM8916, MSM8939, MSM8952, MSM8917, MSM8937, MSM8940, MSM8953 chipsets.

Passcode brute force is available

4. Physical MTK Image

Extraction and decryption of devices based on MT 6737, MT 6739 and MT 6580 chipsets and having Full Disk Encryption.

Passcode brute force is available

Bootloader exploitation

Extraction and decryption of MTK devices with an unlocked bootloader and having Full Disk Encryption.

Passcode brute force is available.

An unlocked Android device

1. Android physical via ADB

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

2. Android backup via ADB

Logical data extraction via ADB backup of Android devices running Android OS 4.0-10.0

3. Logical extraction via OxyAgent

Logical data extraction via USB and Wi-Fi of Android devices running Android OS 4.0-10.0.

WhatsApp and Signal data extraction is available as well as automated screenshots of inaccessible device data.



5 Spreadtrum (SPD) Android Dump

Extraction of devices based on Spreadtrum chipsets and having Full Disk Encryption.

Decryption support for SC7731E, SC9832E, SC9863, SC9850 chipsets. Passcode brute force is available.

A locked Apple iOS device

1. Partial file system via checkm8 vulnerability

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 14.2.

An unlocked Apple iOS device

1. Full file system via checkm8 vulnerability

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 14.2.

2. Full file system of jailbroken devices

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

3. Logical extraction via iTunes backup

Logical extraction via iTunes backup procedure of Apple devices running iOS 8.0-14.2.

4. File structure extraction

Files available via PTP protocol can be extracted. Supported Apple iOS versions are 8.0-14.2.