Approach to the Hidden Data in 'Samsung Secure Folder' with MD-NEXT

Why forensic investigators must keep their eye on the Samsung Secure Folder? Like the word 'Secure Folder', Samsung Secure Folder is separated from the normal storage space and encrypted based on Samsung's security technology 'Knox'. PIN/pattern/password or biometric verification is required to access the secure folder. The data in the secure folder is not accessible from outside and is not visible even when the device is connected to the PC. This means, personal or confidential data can be stored in Samsung Secure Folder, and this can be the core data for your forensic investigation. Today we introduce how MD-NEXT can help you to approach Samsung Secure Folder with various methods by models, MD-NEXT will support Android version 11 soon, and you'll get more meaningful data!

**'The 'Knox' space manages the entire space variably just like many apps manage data in their DB. And when data is deleted from the Knox, it is returned to the non-allocated area of the basic storage space, therefore, 'Logical Extraction' is carried out in file unit.*

MD-NEXT Extraction methods by Models

✓ ***Galaxy A5/S7/S8/S9/Note8/Note9 Series (Exynos & Qualcomm)***

If the Android security patch level is before August 2019, you can obtain the security folder using the ADB Pro T4 method. The USERDATA partition is acquired as a physical image, and additionally, the files stored in the secure folder are decrypted and acquired as a separate logical image.

✓ ***Galaxy A6/A7/S9/J6/Note9 Series (Exynos)***

If the Android OS version is 10, you can obtain the secure folder using the Bootloader Pro method. Like the ADB Pro T4 method, the USERDATA partition is acquired as a physical image, and additionally, the files stored in the secure folder are decrypted and acquired as a separate logical image.

✓ ***Galaxy A30/A40/A50/S10/Note10 Series + Galaxy Tab A 10.1 Series (Exynos)***

Samsung Galaxy S10 and Note 10 series of devices and some A series of devices, you can obtain a secure folder by using the Full Filesystem (Bootloader Pro2) method (Supports both Android 9,10 and 11). When acquiring the active files of the USERDATA partition, the files stored in the secure folder are decrypted and acquired as a single logical image.

How to Review Data?

The data in the secure folder is acquired as a separate logical image from the physical image of the USERDATA partition. The file naming scheme for logical images has been changed in MD-NEXT version 1.89.5(Released date Jul.15, 2020), so the file name may differ depending on the version. Information on the file name and extension of the acquired images can be checked in the acquisition report.

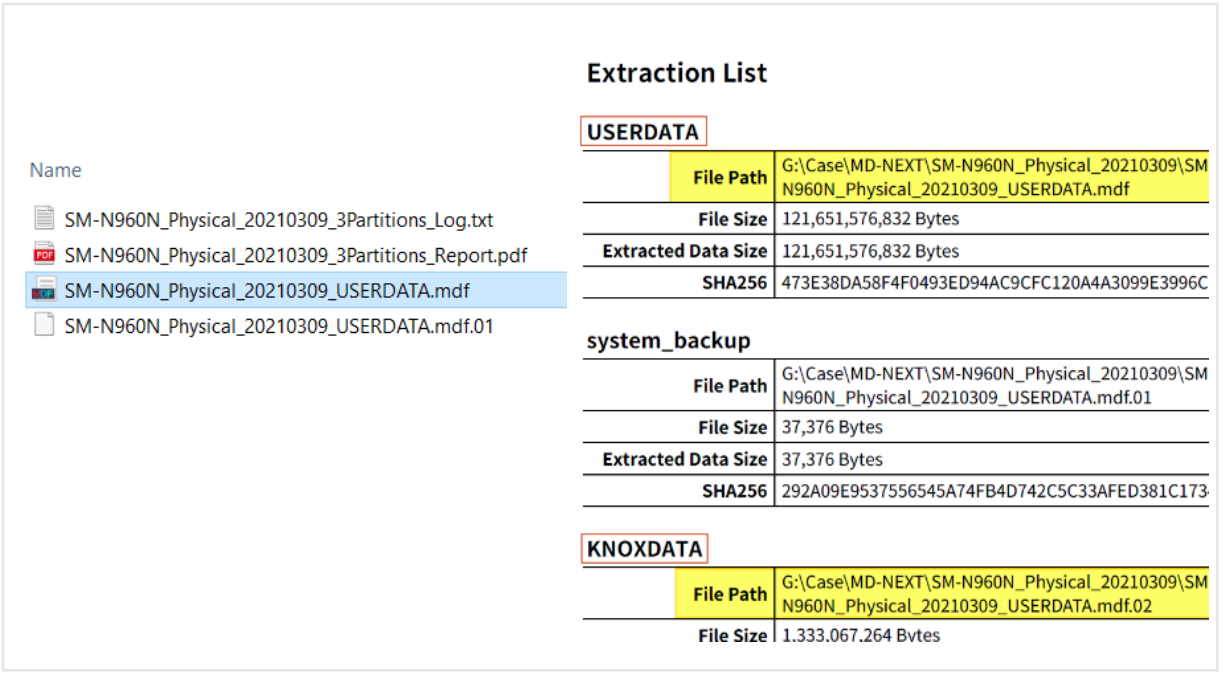

Image 1. Extraction result of Galaxy S7~S9/Note8~9 series

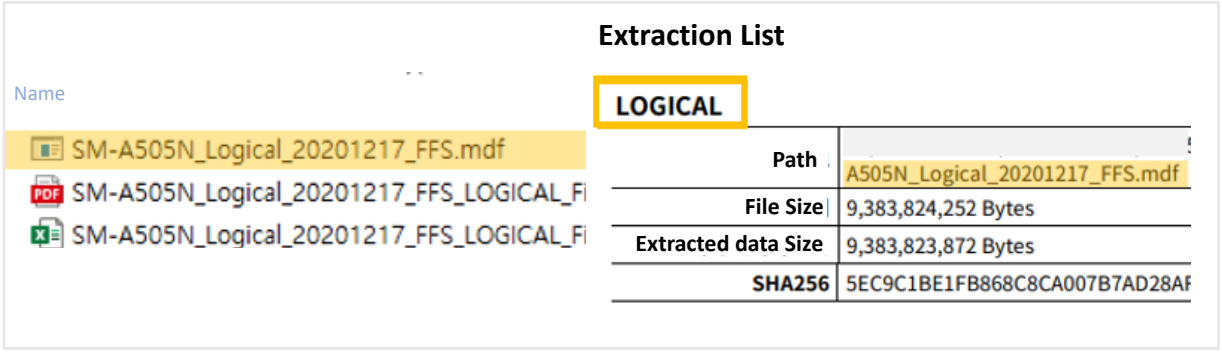

Image 2. Extraction result of Galaxy S10/Note 10 series