Whitepaper

# Samsung Secure Folder

This whitepaper deals with data extraction and analysis of Samsung Secure Folder. Learn the extraction methods of Samsung Secure Folder which varies with the model, OS version, and security patch level by MD-NEXT. Find out how you can discover meaningful data from the analyzed result by MD-RED.

## ►►► Contents ◄◄◄

# 01 What is Samsung Secure Folder?

Secure Folder is a separate storage space within the device, protected by 'Knox'—a security technology of Samsung. By keeping sensitive data or personal contents and apps in Secure Folder, users can protect one's personal data from being unintentionally exposed by external factors(e.g., attacks from malicious apps).

Data in Secure Folder are inaccessible from the outside, even when the mobile device is connected to PC. Unlike the previous Private Mode function, Secure Folder not only supports the file hiding function but also allows apps to be installed and run-on Secure Folder.

(Private Mode : A function that hides data by file units. It is supported by Samsung Galaxy S7 or below)

Secure Folder holds a separate encrypted storage space based on 'Knox'(Security technology of Samsung). Access to Secure Folder requires an authentication process through a PIN, pattern, password, or biometric identification. In addition, Secure Folder includes a function that hides an app icon from home or apps screen, while its own name/icon could be modified as well.

★ Secure Folder is only available to user joined in Samsung Accounts.

Secure Folder

※ **Reference Site**

https://www.samsung.com/uk/support/mobile-devices/what-is-the-secure-folder-and-how-do-i-use-it

## Galaxy S7 / S8 / Note 8 Series

ADB Pro T4
(Security Patch Level
~2019-08)

- **ADB PRO T4** method can extract Secure Folder in Samsung Galaxy S7/S8/Note 8 series with **Android security patch levels** of **2019**-**08 or above**.
- At first, ADB PRO T4 extracts the USERDATA partition as a Physical image. After that, ADB PRO T4 decrypts the Secure Folder file before extracting it as a Logical image.

※ Please be reminded before the extraction :

- Proceed with extraction while the device is booted in a normal mode.
- User should allow USB Debugging. (Refer to 'How to enable developer mode by manufacturer' manual)
- Check the security patch level before proceeding with extraction.
  (Settings > About phone > Software information > Android security patch level)
- Screen unlock is required.

## Galaxy S9 / Note 9 Series

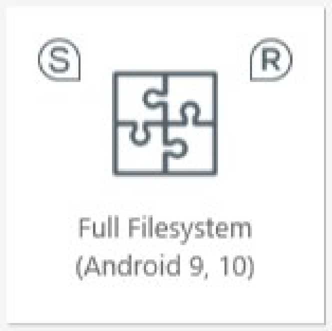
BootLoader Pro
(Android 10)

- **Bootloader Pro** method can extract Secure Folder in Samsung Galaxy S9/Note 9 series with **Android OS version of 10**.
- Just as the ADB Pro T4 method, Bootloader Pro extracts the USERDATA partition as a Physical image. After that, Bootloader Pro decrypts the Secure Folder file before extracting it as a Logical image.

※ Please check the boot status

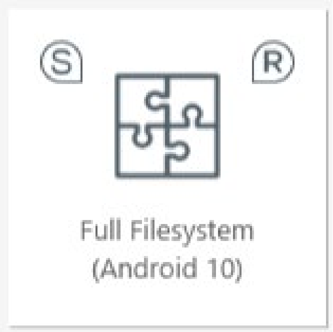
- Start the extraction in a download mode.
- Device reboots to normal mode when the extraction is underway. After the booting has been completed, data are extracted with the screen turned off.
- Although the extraction does not require a screen unlock, 'Secure startup' mode should be turned off if it has been activated.

## Galaxy S10 / Note10 Series + Galaxy A Series



- **Full Filesystem**(Bootloader Pro2) method can extract the Secure Folder in Samsung Galaxy S10/Note 10 series/several A series. (**Android 9, 10, 11 are all supported**)
- When extracting an active file in the USERDATA partition, Bootloader Pro2 decrypts the Secure Folder file before extracting it as a Logical image.

## Galaxy S20 Series



- **Full Filesystem**(Bootloader Pro2) method can extract the Secure Folder in Samsung Galaxy S20 series. (**Android 10, 11 are all supported**)
- When extracting an active file in the USERDATA partition, Bootloader Pro2 decrypts the Secure Folder file before extracting it as a Logical image.

## Galaxy S21 Series

- **Full Filesystem**(Bootloader Pro2) method can extract the Secure Folder in Samsung Galaxy S21 series. (**Android 11**)
- When extracting an active file in the USERDATA partition, Bootloader Pro2 decrypts the Secure Folder file before extracting it as a Logical image.

※ What is Full Filesystem Extraction?

- Full Filesystem Extraction extracts all the active files stored in the USERDATA partition. This extraction method brings the same result as Physical extraction, except for the unallocated area.

※ Please check the boot status

- Start the extraction in a download mode.
- Device reboots to normal mode when the extraction begins, and it remains booted while data are extracted.
- Screen unlock is required.

## ►►► Q & A ◄◄◄

**Q** Can we extract Secure Folder through Android Live method?

**A** Since AndroidLive only operates in a normal mode, it has no authority to access to Secure Folder. This is identical in other spaces such as Dual Messenger or KT Two Phone service. (See Appendix)

**Q** Can we extract Secure Folder through Physical method?

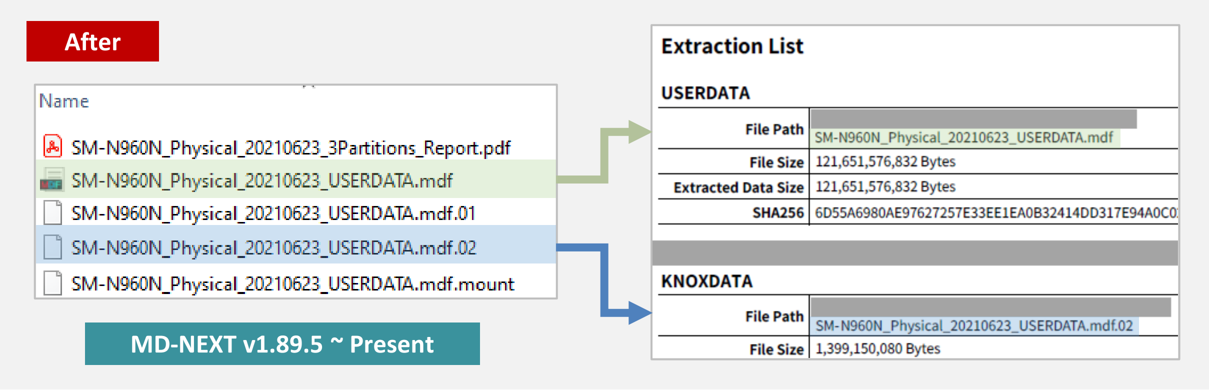
**A** Subfiles of Knox(Secure Folder) are extra encrypted, and each file cannot be decrypted after the extraction. For this reason, Secure Folder cannot be analyzed even after going through Physical extraction.

## Galaxy S7~S9 / Note 8, 9 Series Extraction Results

- Secure Folder data are separately extracted as Logical images, apart from the Physical image of USERDATA partition.
- The file naming system of Logical images has been modified in MD-NEXT version 1.89.5, so the names of files may vary by versions.
- Information on the file name, extension, etc., is notified in the analysis report.

| MD - NEXT Version | File Name |
|---|---|
| V1.89.5 ~ present | File name _USERDATA.mdf.(01~05) |
| v1.88.0 ~ v1.89.4 | File name _KNOXDATA.mdf |

Names of Secure Folder Image Files by versions



After

Name

SM-N960N_Physical_20210623_3Partitions_Report.pdf
SM-N960N_Physical_20210623_USERDATA.mdf
SM-N960N_Physical_20210623_USERDATA.mdf.01
SM-N960N_Physical_20210623_USERDATA.mdf.02
SM-N960N_Physical_20210623_USERDATA.mdf.mount

MD-NEXT v1.89.5 ~ Present

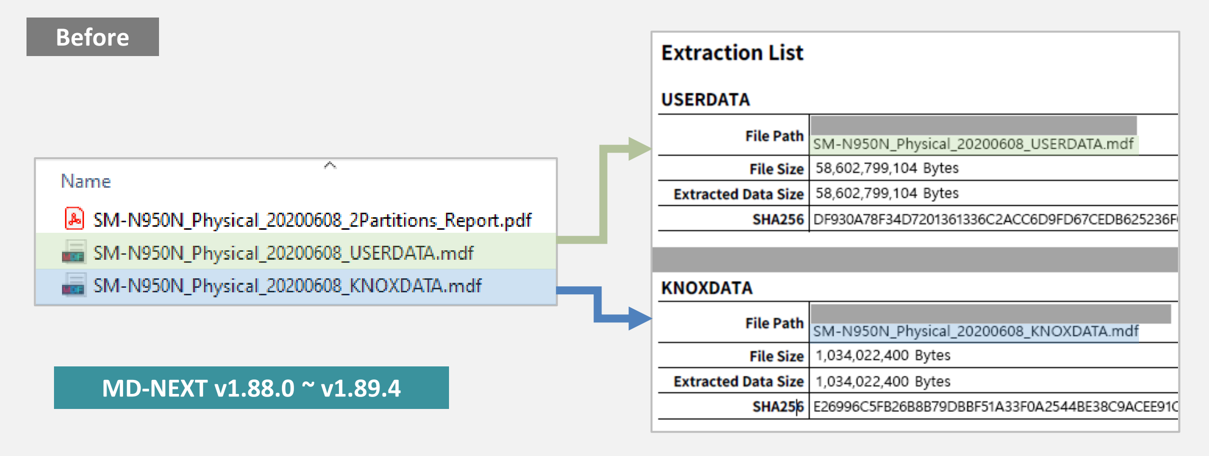
**Extraction List**

**USERDATA**

| | |
|---|---|
| **File Path** | [redacted]<br>SM-N960N_Physical_20210623_USERDATA.mdf |
| **File Size** | 121,651,576,832 Bytes |
| **Extracted Data Size** | 121,651,576,832 Bytes |
| **SHA256** | 6D55A6980AE97627257E33EE1EA0B32414DD317E94A0C0 |

**KNOXDATA**

| | |
|---|---|
| **File Path** | [redacted]<br>SM-N960N_Physical_20210623_USERDATA.mdf.02 |
| **File Size** | 1,399,150,080 Bytes |



Before

Name

SM-N950N_Physical_20200608_2Partitions_Report.pdf
SM-N950N_Physical_20200608_USERDATA.mdf
SM-N950N_Physical_20200608_KNOXDATA.mdf

MD-NEXT v1.88.0 ~ v1.89.4

**Extraction List**

**USERDATA**

| | |
|---|---|
| **File Path** | [redacted]<br>SM-N950N_Physical_20200608_USERDATA.mdf |
| **File Size** | 58,602,799,104 Bytes |
| **Extracted Data Size** | 58,602,799,104 Bytes |
| **SHA256** | DF930A78F34D7201361336C2ACC6D9FD67CEDB625236F |

**KNOXDATA**

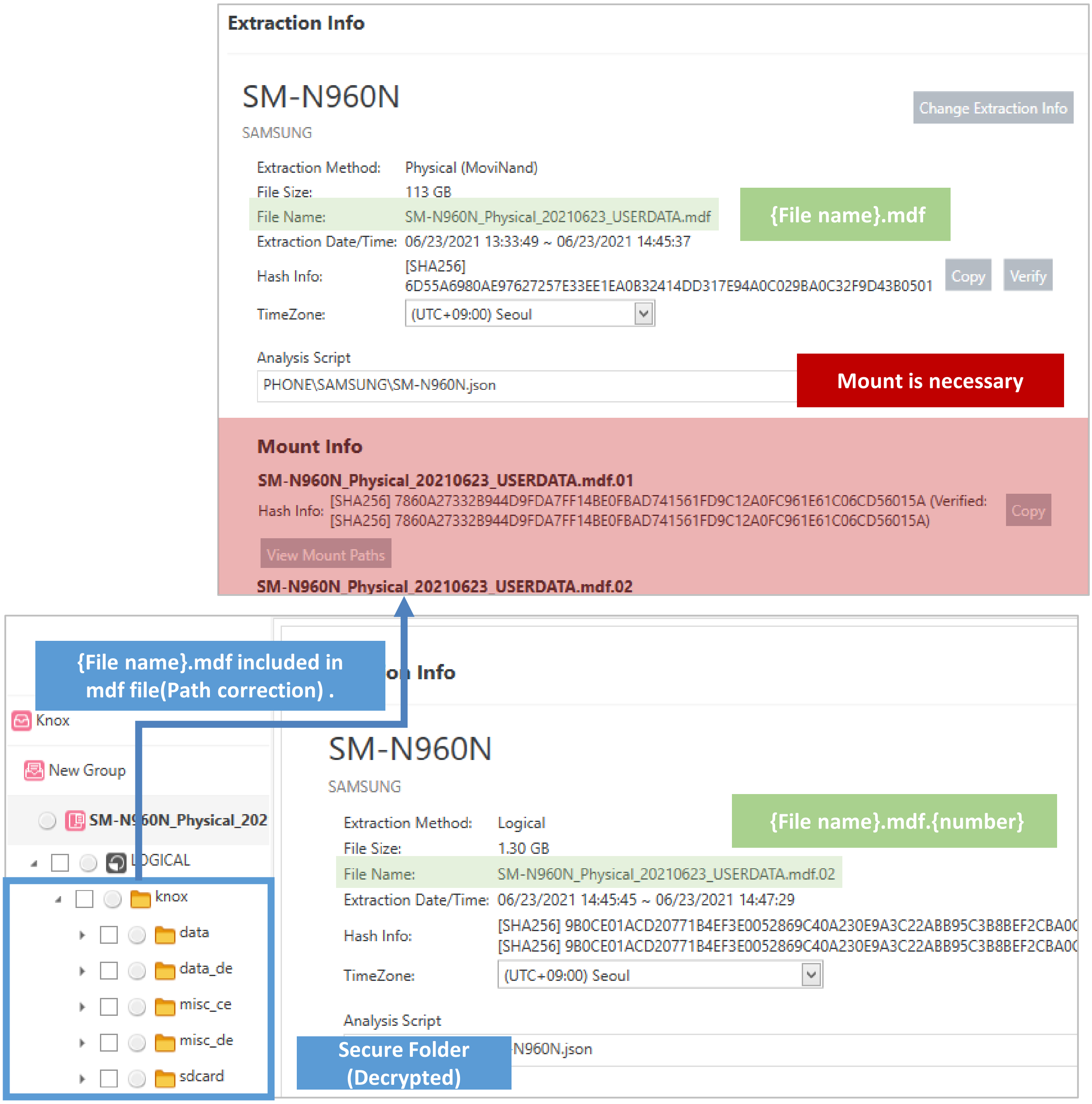
| | |
|---|---|
| **File Path** | [redacted]<br>SM-N950N_Physical_20200608_KNOXDATA.mdf |
| **File Size** | 1,034,022,400 Bytes |
| **Extracted Data Size** | 1,034,022,400 Bytes |
| **SHA256** | E26996C5FB26B8B79DBBF51A33F0A2544BE38C9ACEE91C |

Extracted image

Extraction report (_Report.pdf)

## Galaxy S7~S9 / Note 8, 9 Series Extraction Results

- MD-RED provides the 'Mount' function in order to create an integrated analysis result on USERDATA and Secure Folder.
- The 'Mount' function rearranges Secure Folder-related files—which are stored in a Logical Image—into the Filesystem structure of USERDATA Image. Through this procedure, the two images are integrated and are analyzed as a singular Filesystem.



Extraction Info

SM-N960N
SAMSUNG

Extraction Method: Physical (MoviNand)
File Size: 113 GB
File Name: SM-N960N_Physical_20210623_USERDATA.mdf
Extraction Date/Time: 06/23/2021 13:33:49 ~ 06/23/2021 14:45:37
Hash Info: [SHA256] 6D55A6980AE97627257E33EE1EA0B32414DD317E94A0C029BA0C32F9D43B0501
TimeZone: (UTC+09:00) Seoul

Analysis Script
PHONE\SAMSUNG\SM-N960N.json

Mount Info

SM-N960N_Physical_20210623_USERDATA.mdf.01
Hash Info: [SHA256] 7860A27332B944D9FDA7FF14BE0FBAD741561FD9C12A0FC961E61C06CD56015A (Verified: [SHA256] 7860A27332B944D9FDA7FF14BE0FBAD741561FD9C12A0FC961E61C06CD56015A)

SM-N960N_Physical_20210623_USERDATA.mdf.02

{File name}.mdf

Mount is necessary

{File name}.mdf included in mdf file(Path correction) .

SM-N960N

SAMSUNG

Extraction Method: Logical
File Size: 1.30 GB
File Name: SM-N960N_Physical_20210623_USERDATA.mdf.02
Extraction Date/Time: 06/23/2021 14:45:45 ~ 06/23/2021 14:47:29
Hash Info: [SHA256] 9B0CE01ACD20771B4EF3E0052869C40A230E9A3C22ABB95C3B8BEF2CBA0C
[SHA256] 9B0CE01ACD20771B4EF3E0052869C40A230E9A3C22ABB95C3B8BEF2CBA0C
TimeZone: (UTC+09:00) Seoul

Analysis Script
N960N.json

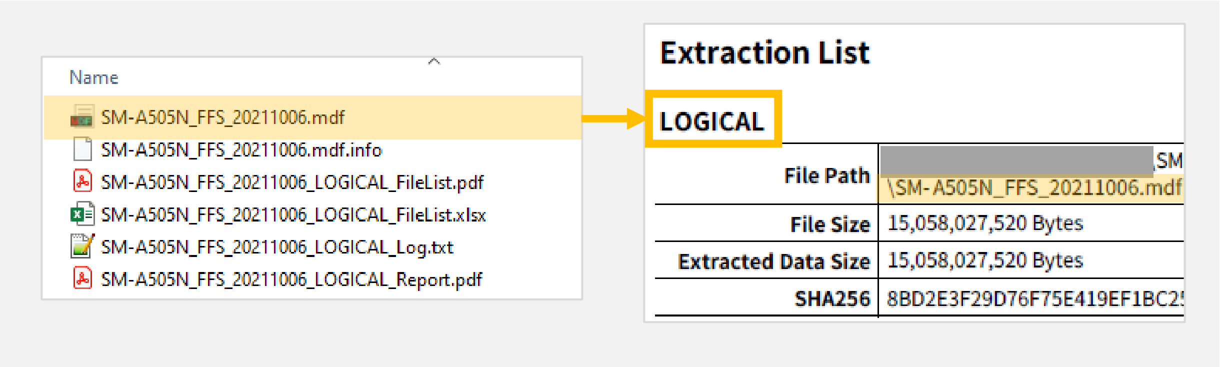
{File name}.mdf.{number}

Secure Folder (Decrypted)

ADB Pro T4, Bootloader Pro Info. on Extracted Image (Applied 'Mount' feature)

## Galaxy S10, S20, S21 / Note 10 Series Extraction Results

- Data stored in Secure Folder and all the active files within the USERDATA partition are extracted as one Logical image. (Full Filesystem Extraction)
- Already extracted as a singular image, a Full Filesystem Image does not require a 'Mount' process.



Name

- SM-A505N_FFS_20211006.mdf
- SM-A505N_FFS_20211006.mdf.info
- SM-A505N_FFS_20211006_LOGICAL_FileList.pdf
- SM-A505N_FFS_20211006_LOGICAL_FileList.xlsx
- SM-A505N_FFS_20211006_LOGICAL_Log.txt
- SM-A505N_FFS_20211006_LOGICAL_Report.pdf

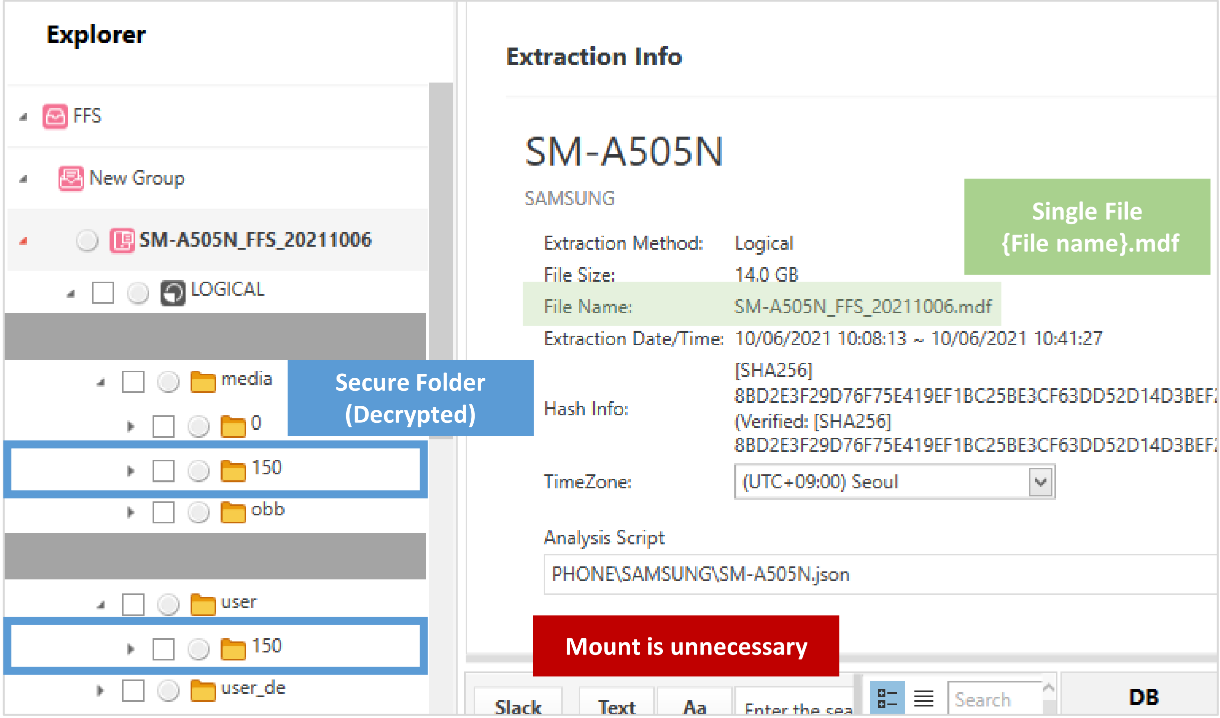
**Extraction List**

**LOGICAL**

| | |
|---|---|
| **File Path** | [redacted]\SM<br>\SM-A505N_FFS_20211006.mdf |
| **File Size** | 15,058,027,520 Bytes |
| **Extracted Data Size** | 15,058,027,520 Bytes |
| **SHA256** | 8BD2E3F29D76F75E419EF1BC2 |

Extracted image

Extraction report (_Report.pdf)



**Explorer**

- FFS
  - New Group
    - SM-A505N_FFS_20211006
      - □ LOGICAL
        - [redacted]
          - □ media
            - □ 0
            - □ 150
            - □ obb
        - [redacted]
          - □ user
            - □ 150
          - □ user_de

Secure Folder (Decrypted)

**Extraction Info**

SM-A505N

SAMSUNG

| | |
|---|---|
| Extraction Method: | Logical |
| File Size: | 14.0 GB |
| File Name: | SM-A505N_FFS_20211006.mdf |
| Extraction Date/Time: | 10/06/2021 10:08:13 ~ 10/06/2021 10:41:27 |
| Hash Info: | [SHA256]<br>8BD2E3F29D76F75E419EF1BC25BE3CF63DD52D14D3BEF<br>(Verified: [SHA256]<br>8BD2E3F29D76F75E419EF1BC25BE3CF63DD52D14D3BEF |
| TimeZone: | (UTC+09:00) Seoul |

Analysis Script

PHONE\SAMSUNG\SM-A505N.json

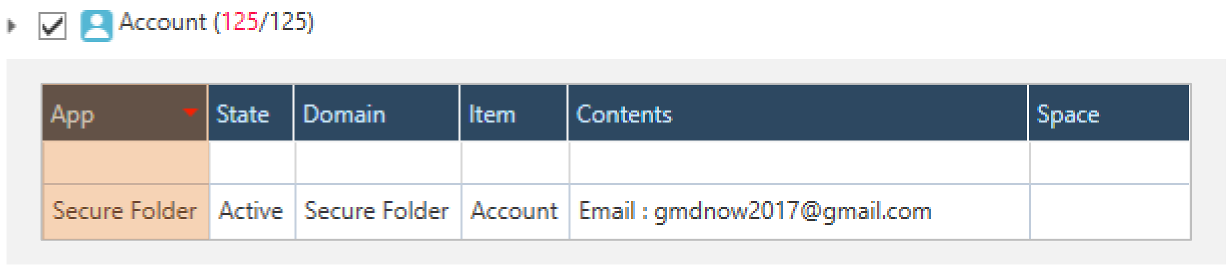
Single File
{File name}.mdf

Mount is unnecessary

Info. of an Image Extracted by Full Filesystem Extraction

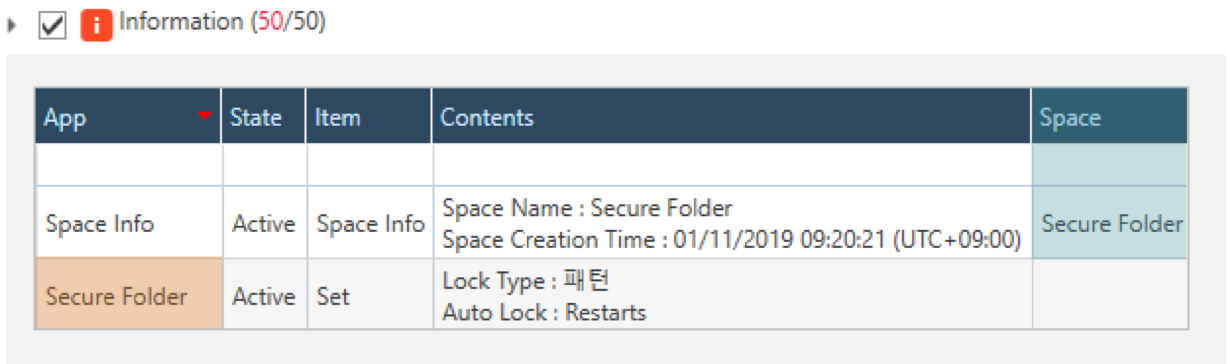
## Secure Folder Information

- Secure Folder info. is shown at the Accounts/Information/Etc artifacts. (The analysis results may vary by device environments.)
- **Each analysis result on Secure Folder is** marked as **'Secure Folder' in the 'App' or the 'Space' field**.
    - Account – Samsung Account Using Secure Folder
    - Information – Lock scheme or Auto Lock of Secure Folder / Creation time
    - Etc– Package names of the applications installed on Secure Folder



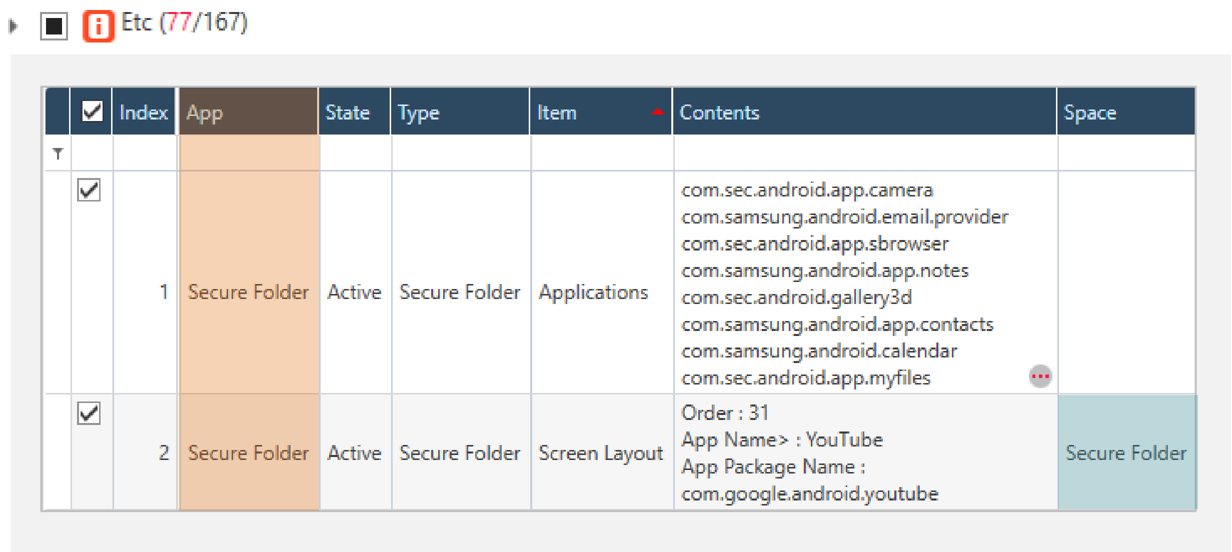
☑ Account (125/125)

| App | State | Domain | Item | Contents | Space |
|---|---|---|---|---|---|
| | | | | | |
| Secure Folder | Active | Secure Folder | Account | Email : gmdnow2017@gmail.com | |



☑ Information (50/50)

| App | State | Item | Contents | Space |
|---|---|---|---|---|
| | | | | |
| Space Info | Active | Space Info | Space Name : Secure Folder<br>Space Creation Time : 01/11/2019 09:20:21 (UTC+09:00) | Secure Folder |
| Secure Folder | Active | Set | Lock Type : 패턴<br>Auto Lock : Restarts | |

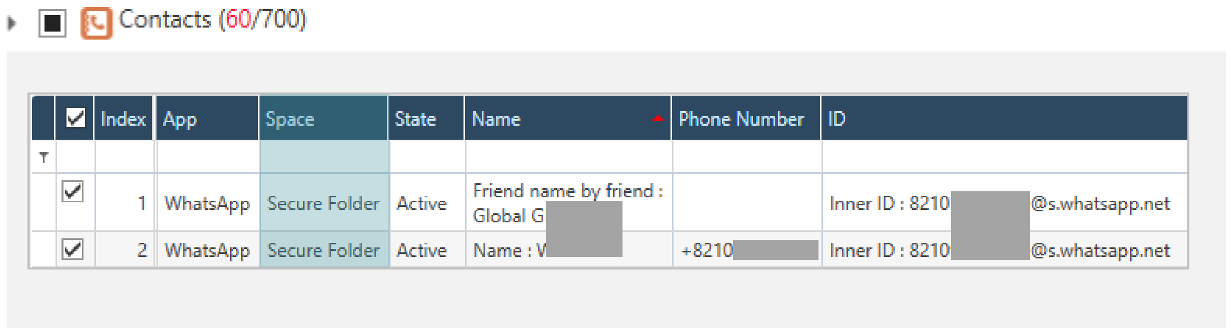


■ Etc (77/167)

| | ☑ | Index | App | State | Type | Item | Contents | Space |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | ☑ | 1 | Secure Folder | Active | Secure Folder | Applications | com.sec.android.app.camera<br>com.samsung.android.email.provider<br>com.sec.android.app.sbrowser<br>com.samsung.android.app.notes<br>com.sec.android.gallery3d<br>com.samsung.android.app.contacts<br>com.samsung.android.calendar<br>com.sec.android.app.myfiles | |
| | ☑ | 2 | Secure Folder | Active | Secure Folder | Screen Layout | Order : 31<br>App Name> : YouTube<br>App Package Name :<br>com.google.android.youtube | Secure Folder |

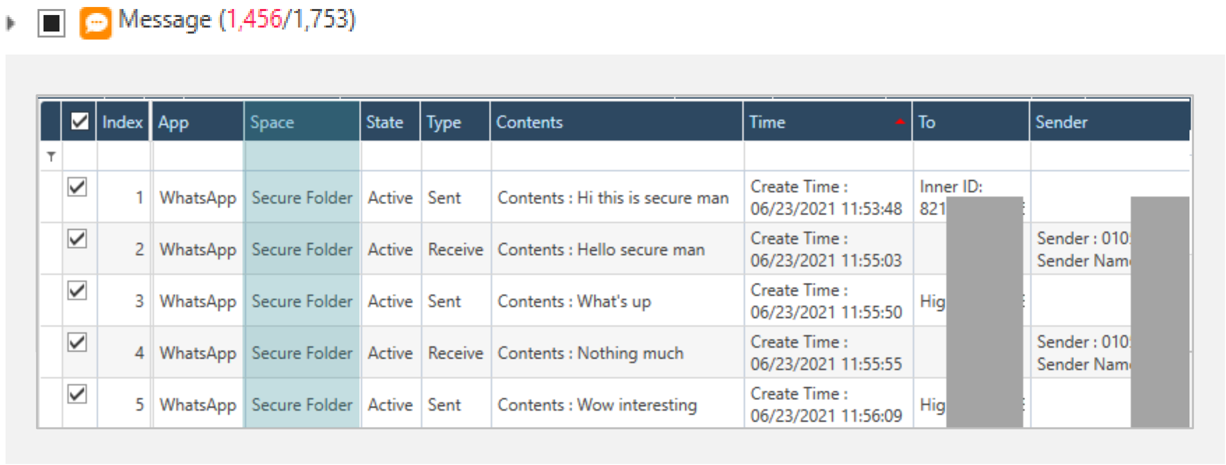
## App Data

- Data analysis results on apps stored in Secure Folder are marked as **'Secure Folder'** in the **'Space'** field.



▪ ☎ Contacts (60/700)

| ☑ | Index | App | Space | State | Name | Phone Number | ID |
|---|---|---|---|---|---|---|---|
| ☑ | 1 | WhatsApp | Secure Folder | Active | Friend name by friend : Global G[redacted] | | Inner ID : 8210[redacted]@s.whatsapp.net |
| ☑ | 2 | WhatsApp | Secure Folder | Active | Name : W[redacted] | +8210[redacted] | Inner ID : 8210[redacted]@s.whatsapp.net |



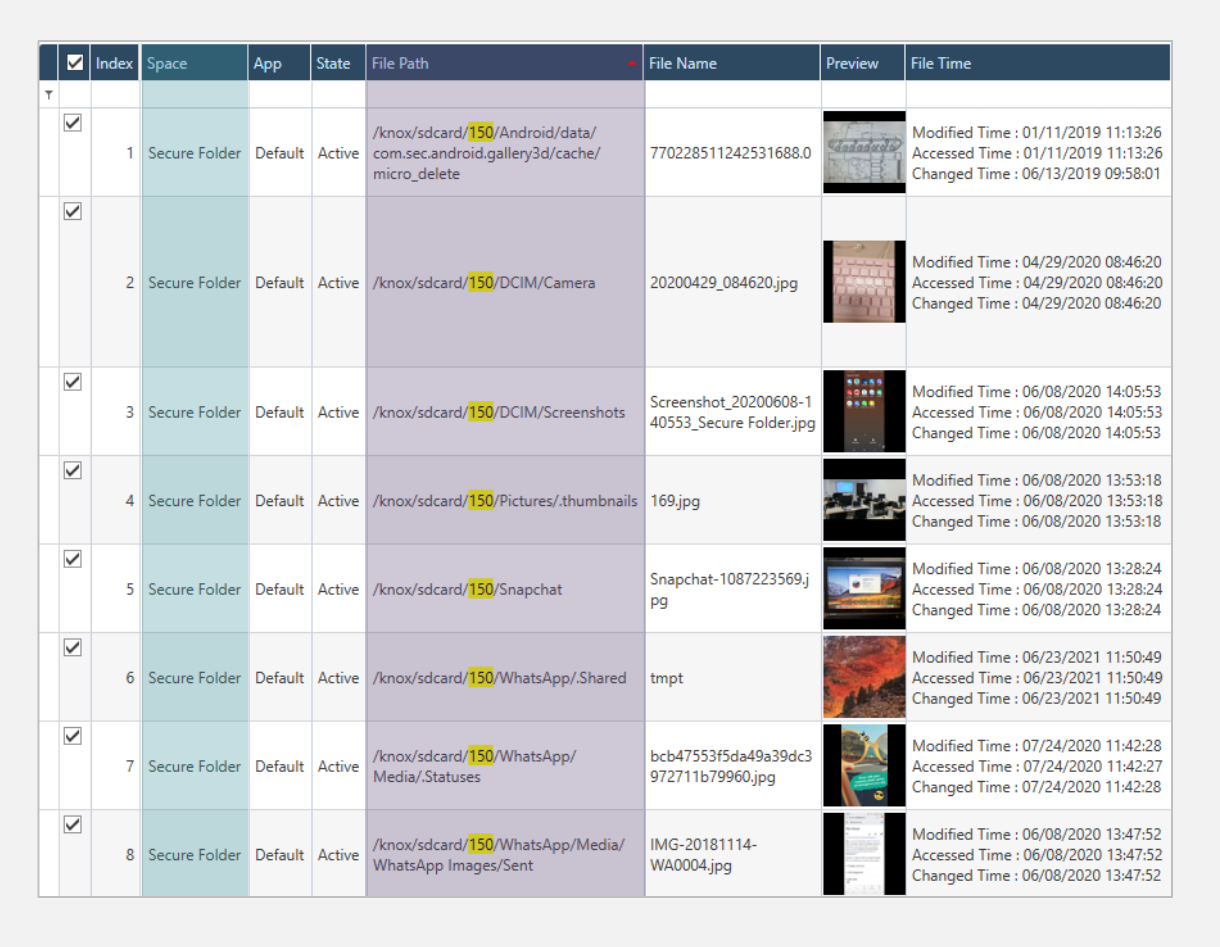
▪ Message (1,456/1,753)

| ☑ | Index | App | Space | State | Type | Contents | Time | To | Sender |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | WhatsApp | Secure Folder | Active | Sent | Contents : Hi this is secure man | Create Time :<br>06/23/2021 11:53:48 | Inner ID:<br>821[redacted] | [redacted] |
| ☑ | 2 | WhatsApp | Secure Folder | Active | Receive | Contents : Hello secure man | Create Time :<br>06/23/2021 11:55:03 | [redacted] | Sender : 010[redacted]<br>Sender Nam[redacted] |
| ☑ | 3 | WhatsApp | Secure Folder | Active | Sent | Contents : What's up | Create Time :<br>06/23/2021 11:55:50 | Hig[redacted] | [redacted] |
| ☑ | 4 | WhatsApp | Secure Folder | Active | Receive | Contents : Nothing much | Create Time :<br>06/23/2021 11:55:55 | [redacted] | Sender : 010[redacted]<br>Sender Nam[redacted] |
| ☑ | 5 | WhatsApp | Secure Folder | Active | Sent | Contents : Wow interesting | Create Time :<br>06/23/2021 11:56:09 | Hig[redacted] | [redacted] |

## Multimedia

- Multimedia files of Secure Folder can be identified **through their file paths** shown in Multimedia analysis result. (For further descriptions on file paths, refer to the "Appendix".)
- As in App Data analysis result, each Multimedia analysis result would henceforth be marked as 'Secure Folder' in the 'Space' field.

■ Multimedia (12,147/17,452)



| ☑ | Index | Space | App | State | File Path | File Name | Preview | File Time |
|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | Secure Folder | Default | Active | /knox/sdcard/150/Android/data/com.sec.android.gallery3d/cache/micro_delete | 770228511242531688.0 | | Modified Time : 01/11/2019 11:13:26<br>Accessed Time : 01/11/2019 11:13:26<br>Changed Time : 06/13/2019 09:58:01 |
| ☑ | 2 | Secure Folder | Default | Active | /knox/sdcard/150/DCIM/Camera | 20200429_084620.jpg | | Modified Time : 04/29/2020 08:46:20<br>Accessed Time : 04/29/2020 08:46:20<br>Changed Time : 04/29/2020 08:46:20 |
| ☑ | 3 | Secure Folder | Default | Active | /knox/sdcard/150/DCIM/Screenshots | Screenshot_20200608-140553_Secure Folder.jpg | | Modified Time : 06/08/2020 14:05:53<br>Accessed Time : 06/08/2020 14:05:53<br>Changed Time : 06/08/2020 14:05:53 |
| ☑ | 4 | Secure Folder | Default | Active | /knox/sdcard/150/Pictures/.thumbnails | 169.jpg | | Modified Time : 06/08/2020 13:53:18<br>Accessed Time : 06/08/2020 13:53:18<br>Changed Time : 06/08/2020 13:53:18 |
| ☑ | 5 | Secure Folder | Default | Active | /knox/sdcard/150/Snapchat | Snapchat-1087223569.jpg | | Modified Time : 06/08/2020 13:28:24<br>Accessed Time : 06/08/2020 13:28:24<br>Changed Time : 06/08/2020 13:28:24 |
| ☑ | 6 | Secure Folder | Default | Active | /knox/sdcard/150/WhatsApp/.Shared | tmpt | | Modified Time : 06/23/2021 11:50:49<br>Accessed Time : 06/23/2021 11:50:49<br>Changed Time : 06/23/2021 11:50:49 |
| ☑ | 7 | Secure Folder | Default | Active | /knox/sdcard/150/WhatsApp/Media/.Statuses | bcb47553f5da49a39dc3972711b79960.jpg | | Modified Time : 07/24/2020 11:42:28<br>Accessed Time : 07/24/2020 11:42:27<br>Changed Time : 07/24/2020 11:42:28 |
| ☑ | 8 | Secure Folder | Default | Active | /knox/sdcard/150/WhatsApp/Media/WhatsApp Images/Sent | IMG-20181114-WA0004.jpg | | Modified Time : 06/08/2020 13:47:52<br>Accessed Time : 06/08/2020 13:47:52<br>Changed Time : 06/08/2020 13:47:52 |

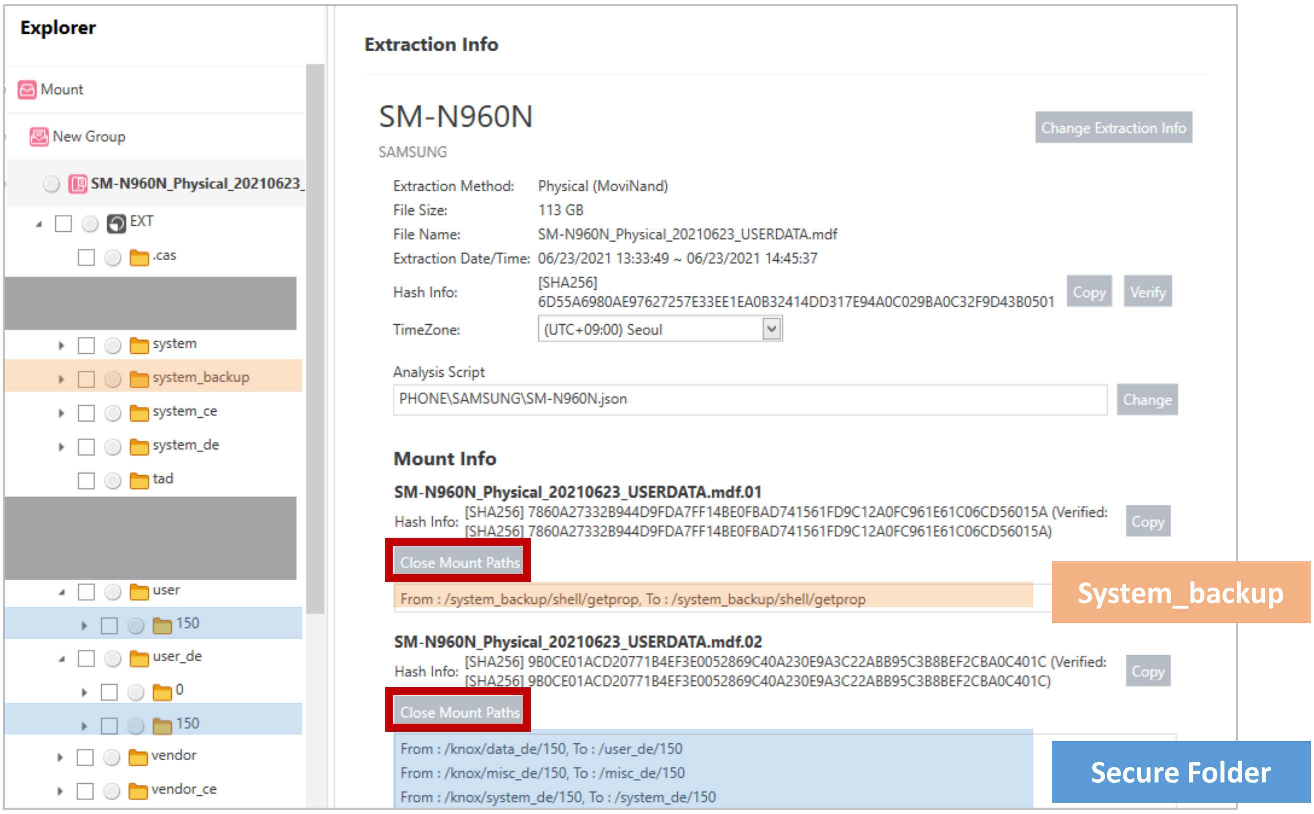
※ Applied from MD-NEXT version 1.89.5 / MD-RED version 3.6.10 or above

## Mount Function

- Mount function integrates a USERDATA partition image and a separately extracted Logical image into one filesystem by revising the paths in MD-RED.
- The Secure Folder, encrypted SD cards, and the extracted images of system_backup accord with this case.
- If an app with data-encrypting function has been installed on Secure Folder,
    - Several data cannot be analyzed since the extracted Secure Folder image does not contain the decryption key. (e.g., Wickr Me – Messages, Daum mail – Body, etc.)
    - Data in secure folder can be decrypted and be analyzed only after the 'Mount' function has reconstructed the data into a single filesystem.

### ※ How to Use

- When an additional .mdf image is added to a case of MD-RED, file paths of other Logical images(.mdf.01~05) are revised. After that, a case analysis is provided altogether.
- Information on revised paths is indicated in the {file name}.mount file(created alongside with .mdf files during the extraction). Check it out from the 'Extraction Info.' in MD-RED→'Mount Info.'.



Extraction Info

SM-N960N
SAMSUNG

Extraction Method: Physical (MoviNand)
File Size: 113 GB
File Name: SM-N960N_Physical_20210623_USERDATA.mdf
Extraction Date/Time: 06/23/2021 13:33:49 ~ 06/23/2021 14:45:37
Hash Info: [SHA256] 6D55A6980AE97627257E33EE1EA0B32414DD317E94A0C029BA0C32F9D43B0501
TimeZone: (UTC+09:00) Seoul

Analysis Script
PHONE\SAMSUNG\SM-N960N.json

Mount Info

SM-N960N_Physical_20210623_USERDATA.mdf.01
Hash Info: [SHA256] 7860A27332B944D9FDA7FF14BE0FBAD741561FD9C12A0FC961E61C06CD56015A (Verified: [SHA256] 7860A27332B944D9FDA7FF14BE0FBAD741561FD9C12A0FC961E61C06CD56015A)

From : /system_backup/shell/getprop, To : /system_backup/shell/getprop

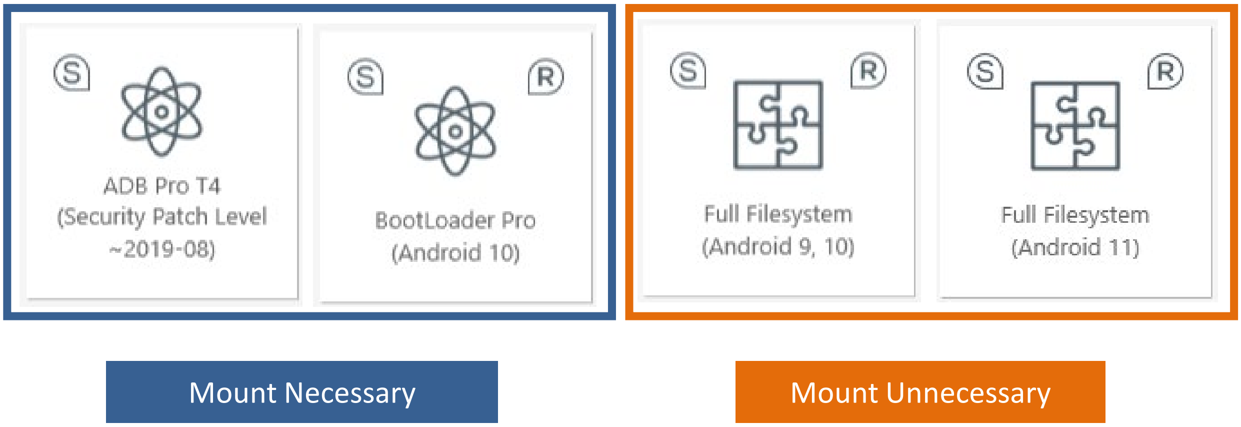
SM-N960N_Physical_20210623_USERDATA.mdf.02
Hash Info: [SHA256] 9B0CE01ACD20771B4EF3E0052869C40A230E9A3C22ABB95C3B8BEF2CBA0C401C (Verified: [SHA256] 9B0CE01ACD20771B4EF3E0052869C40A230E9A3C22ABB95C3B8BEF2CBA0C401C)

From : /knox/data_de/150, To : /user_de/150
From : /knox/misc_de/150, To : /misc_de/150
From : /knox/system_de/150, To : /system_de/150

MD-RED Mount Info.

## Comparison Between Physical & Full Filesystem Extraction

- When Physical (ADB Pro 4, Bootloader Pro) and Full Filesystem extraction takes place, Secure Folder-related files in the extracted images have various paths depending on whether the Mount function has been executed or not.
- In Physical Extractions,
  - If a Logical image has not been mounted, the image should be analyzed separately. In this case, decrypted files follow a /knox path—the file path of encrypted files.
  - If a Secure Folder image has been mounted, file paths of the Logical image are revised.
- In Full Filesystem Extractions,
  - After being decrypted, Secure Folder files are saved within the extracted image by using the revised paths.
  - For this reason, the Mount function is not necessary in this case.



Mount Necessary

Mount Unnecessary

| Classification | Physical | | Full Filesystem |
|---|---|---|---|
| | Single File – Before | Mount Applied – After | |
| App Data | /knox/data/(150~160) | /user/(150~160) | /user/(150~160) |
| Multimedia | /knox/sdcard/(150~160) | /knox/sdcard/(150~160) | /media/(150~160) |
| Other | /knox/system_de/(150 ~160) … | /system_de/(150~160)<br>… | /system_de/(150~160)<br>… |

Secure Folder Path

## Multiple User IDs support

- Android OS provides separate workspaces so that different apps and settings could be supported for each user on a single device.
- Since every user space is separated, a user cannot access the data of another. User data of an individual are stored under a distinct folder sorted by the User ID.
- If user reactivates(creation) a workspace after inactivating(deletion) it, another User ID might be given. (e.g., Secure Folder recreated after being deleted : 150 -> 151, Once again recreated after being deleted : 151 -> 150)

| User ID | Descriptions | Space name (MD-RED) |
|---|---|---|
| 0 | Default app | - |
| 150 ~ 160 | Samsung Secure Folder | Secure Folder |
| 95,  96 | Dual Messenger (Samsung) | Dual Messenger |
| 97, 98, 99 | Dual Messenger (LG) | Dual Messenger |
| 10, 11 | KT Two Phone Service ,<br>Work spaces(Workplace Profile), etc. | Non-default space |

Primary User ID

| Classification | Path |
|---|---|
| App Data | /user/{Users ID}/Package Name(ApplicationID) |
| Multimedia | /media/{User ID} |
| System Configuration/Status | /system/users/{User ID} |
| User ID Info. | /system/users/{User ID}.xml  (File) |

User Path

※ Reference Site

https://source.android.com/devices/tech/admin/multi-user

https://source.android.com/devices/tech/admin/multi-user-testing

HancomWITH | www.hancomgmd.com
HancomWITH, Room 215,2nd Floor, H Square N-dong, 235, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea