

<Watch - 포렌식>











































문제는 다음과 같았다.

사이버 범죄자 김소리의 스마트워치를 압수했다.
김소리를 파헤쳐보자!

1. 어플리케이션 개수
2. 3번째 리마인더 작성 시간(HH:MM:SS)
3. 음악 파일명(@@@.mp3)
4. 김소리의 거주지(countryName cityName)
5. 1695650088에 뉴스를 발행한 author

3S{1_2_3_4_5}

파일을 다운 받아서 열어봤더니 전체 폴더가 다음과 같았다.

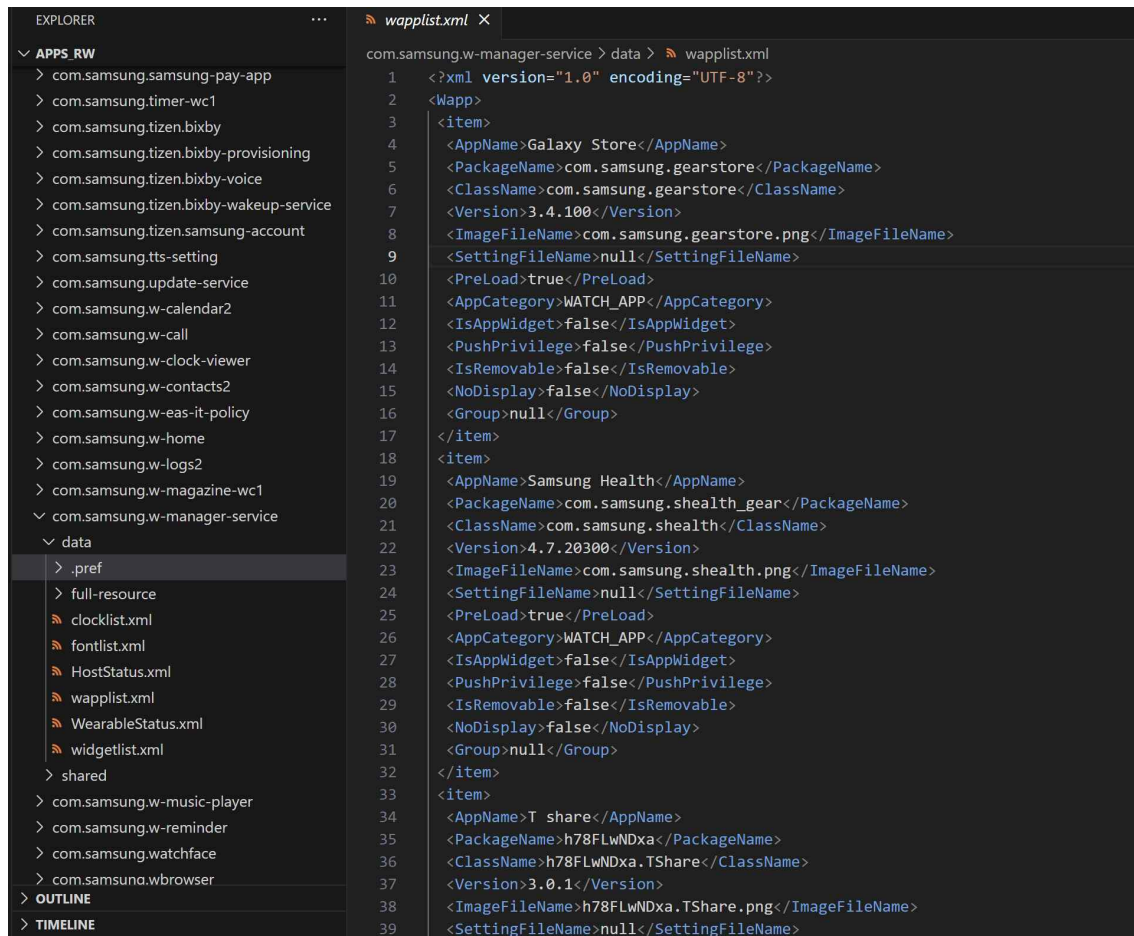
 com.holofactory.breakout		2023-10-31 오후 8:45	파일 폴더
 com.samsung.alarm-solis		2024-07-26 오전 8:00	파일 폴더
 com.samsung.alti-barometer		2024-07-26 오전 7:59	파일 폴더
 com.samsung.app-widget		2024-07-26 오전 7:59	파일 폴더
 com.samsung.b2-setup-wizard		2024-07-26 오전 7:59	파일 폴더
 com.samsung.clocksetting		2024-07-26 오전 7:59	파일 폴더
 com.samsung.daily-briefing		2024-07-26 오전 7:59	파일 폴더
 com.samsung.dqagent		2024-07-26 오전 7:59	파일 폴더
 com.samsung.fmg		2024-07-26 오전 7:59	파일 폴더
 com.samsung.gearstore		2024-07-26 오전 7:58	파일 폴더
 com.samsung.idle-service		2024-07-26 오전 7:59	파일 폴더
 com.samsung.ime-companion-service		2024-07-26 오전 7:58	파일 폴더
 com.samsung.iot-resource-service		2024-07-26 오전 7:58	파일 폴더
 com.samsung.message		2024-07-26 오전 7:31	파일 폴더
 com.samsung.runestone-core		2024-07-26 오전 7:56	파일 폴더
 com.samsung.samsung-pay-app		2024-07-26 오전 7:56	파일 폴더
 com.samsung.timer-wc1		2024-07-26 오전 7:55	파일 폴더
 com.samsung.tizen.bixby		2024-07-26 오전 7:55	파일 폴더
 com.samsung.tizen.bixby-provisioning		2024-07-26 오전 7:55	파일 폴더
 com.samsung.tizen.bixby-voice		2024-07-26 오전 7:55	파일 폴더
 com.samsung.tizen.bixby-wakeup-service		2023-10-31 오후 8:45	파일 폴더

문제 해결을 위해서 폴더 전체를 visual code로 열어 보았다.

▼ APPS_RW

- > com.holofactory.breakout
- > com.samsung.alarm-solis
- > com.samsung.alti-barometer
- > com.samsung.app-widget
- > com.samsung.b2-setup-wizard
- > com.samsung.clocksetting
- > com.samsung.daily-briefing
- > com.samsung.dqagent
- > com.samsung.fmg
- > com.samsung.gearstore
- > com.samsung.idle-service
- > com.samsung.ime-companion-service
- > com.samsung.iot-resource-service
- > com.samsung.message
- > com.samsung.runestone-core
- > com.samsung.samsung-pay-app
- > com.samsung.timer-wc1
- > com.samsung.tizen.bixby
- > com.samsung.tizen.bixby-provisioning
- > com.samsung.tizen.bixby-voice
- > com.samsung.tizen.bixby-wakeup-ser...
- > com.samsung.tizen.samsung-account
- > com.samsung.tts-setting
- > com.samsung.update-service
- > com.samsung.w-calendar2
- > com.samsung.w-call
- > com.samsung.w-clock-viewer
- > com.samsung.w-contacts2
- > com.samsung.w-eas-it-policy
- > com.samsung.w-home
- > com.samsung.w-logs2

첫 번째 문제를 풀기 위해서 manager-service를 타고 wapplist.xml에 들어갔다.



중간 중간에 AppName으로 다운 받아진 앱들이 나열되어 있다.

단축키를 통해서 단어 검색을 돌려보니까 21개의 앱들이 있다는 것 확인했다. 확인하는 김에 목록들을 정리해보았다.

Galaxy store, samsung health, T share, 갤러리, 고도-기압계, 날씨, 내 폰 찾기, 네이버 지도, 뉴스 브리핑, 리마인더, 메시지, 뮤직, 빅스비, 설정, 세계시각, 스타벅스, 알람, 연락처, 전화, 캘린더, 타이머

자 이제 3번째 리마인더 작성 시간을 찾아보자.

reminder counter log에 들어가서 로그를 확인해봤다.

```
EXPLORER
└─ APPS_RW
  └─ com.samsung.w-eas-ic-policy
    └─ com.samsung.w-home
      └─ com.samsung.w-logs2
        └─ com.samsung.w-magazine-wc1
          └─ com.samsung.w-manager-service
            └─ data
              └─ .pref
                └─ full-resource
                  └─ clocklist.xml
                    └─ fontlist.xml
                      └─ HostStatus.xml
                        └─ wapplist.xml
                          └─ WearableStatus.xml
                            └─ widgetlist.xml
                              └─ shared
                                └─ com.samsung.w-music-player
                                  └─ com.samsung.w-reminder\data
                                    └─ .pref
                                      └─ reminder.db
                                        └─ reminder.db-journal
                                          └─ reminderConsumerLog
                                            └─ com.samsung.watchface
                                              └─ com.samsung.wbrowser
                                                └─ com.samsung.weather
                                                  └─ com.samsung.windicator
                                                    └─ GJebuFc12C
                                                      └─ h78FLwNDxa
                                                        └─ istarbucks
                                                          └─ scrOUeIM1o
                                                            └─ sfWDXU4bMc
                                                              └─ UOlvk2Ahmu
                                                                └─ OUTLINE
                                                                  └─ TIMELINE

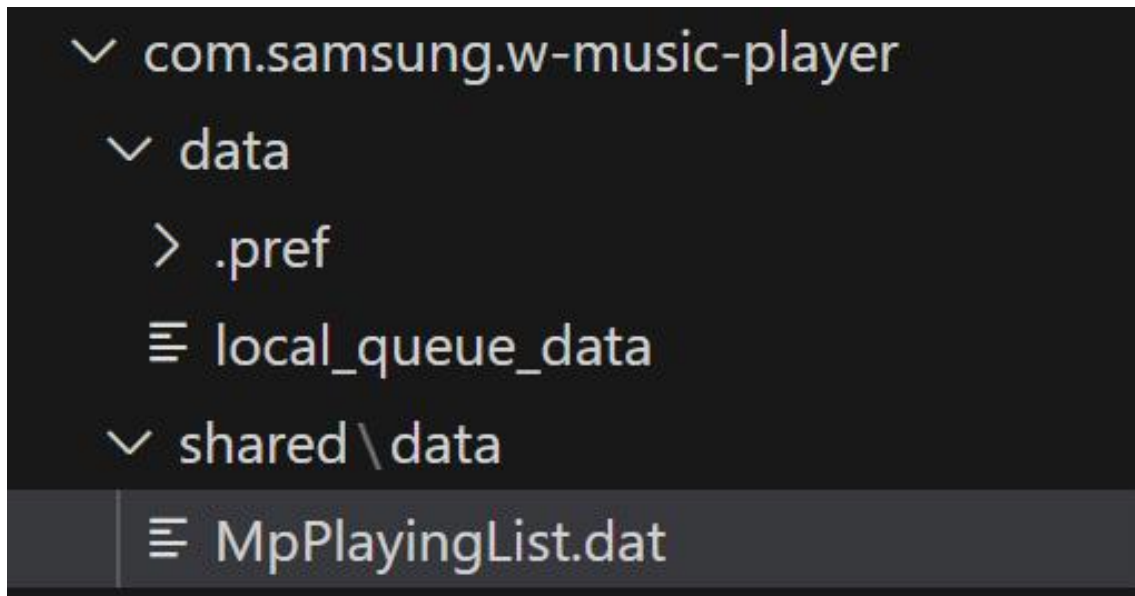
reminderConsumerLog
com.samsung.w-reminder > data > reminderConsumerLog
1 2023/10/29 22:38:18:371 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-appc
2 2023/10/29 22:38:18:371 start
3 2023/10/29 22:38:18:400 __onStartWipicAgent
4 2023/10/29 22:38:18:400 __stopAfterNSeconds
5 2023/10/29 22:38:18:401 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-appc
6 2023/10/29 22:38:18:401 __onReceiveBtOffGearChangeRequest
7 2023/10/29 22:38:18:401 __sendUpdateInd
8 2023/10/29 22:38:18:447 __stopAfterNSeconds
9 2023/10/29 22:38:18:447 setRequest Send response for com.samsung.w-reminder-appcontrol-add
10 2023/10/29 22:38:25:339 __onStopWorker
11 2023/10/29 22:38:25:397 __checkAppVersion version=1.6.31, updateVersion=1.6.31
12 2023/10/29 22:38:25:525 __unsetTimerForGearNotiAck
13 2023/10/29 22:38:25:525 __unsetTimerForUpdateGearAck
14 2023/10/29 22:45:39:581 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-widg
15 2023/10/29 22:45:39:581 start
16 2023/10/29 22:45:39:594 __onStartWipicAgent
17 2023/10/29 22:45:39:594 __stopAfterNSeconds
18 2023/10/29 22:45:39:594 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-widg
19 2023/10/29 22:45:39:595 __onReceiveBtOffGearChangeRequest
20 2023/10/29 22:45:39:595 __sendUpdateInd
21 2023/10/29 22:45:39:618 __stopAfterNSeconds
22 2023/10/29 22:45:39:618 setRequest Send response for com.samsung.w-reminder-widget
23 2023/10/29 22:45:47:332 __onStopWorker
24 2023/10/29 22:45:47:383 __checkAppVersion version=1.6.31, updateVersion=1.6.31
25 2023/10/29 22:45:47:494 __unsetTimerForGearNotiAck
26 2023/10/29 22:45:47:495 __unsetTimerForUpdateGearAck
27 2023/10/29 22:45:48:764 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-appc
28 2023/10/29 22:45:48:764 start
29 2023/10/29 22:45:48:888 __onStartWipicAgent
30 2023/10/29 22:45:48:888 __stopAfterNSeconds
31 2023/10/29 22:45:48:888 getOriginOfLaunchingFromCurrentRequestBT off gear change request from com.samsung.w-reminder-appc
32 2023/10/29 22:45:48:888 __onReceiveBtOffGearChangeRequest
33 2023/10/29 22:45:48:889 __sendUpdateInd
34 2023/10/29 22:45:48:965 __stopAfterNSeconds
35 2023/10/29 22:45:48:965 setRequest Send response for com.samsung.w-reminder-appcontrol-add
36 2023/10/29 22:45:56:332 __onStopWorker
37 2023/10/29 22:45:56:397 __checkAppVersion version=1.6.31, updateVersion=1.6.31
38 2023/10/29 22:45:56:521 __unsetTimerForGearNotiAck
39 2023/10/29 22:45:56:521 __unsetTimerForUpdateGearAck
```

세 번째 start를 보니 시간을 확인할 수 있었다.

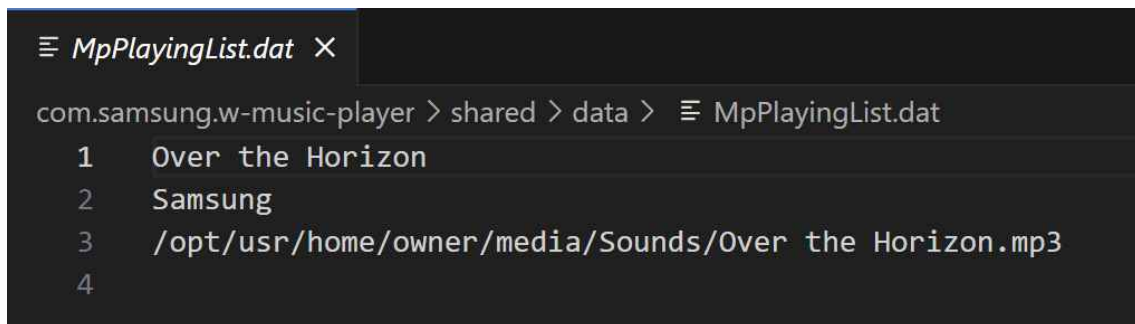


음악 파일명을 찾아보자.

music player을 타고 들어가서 playinglist를 확인해봤다.

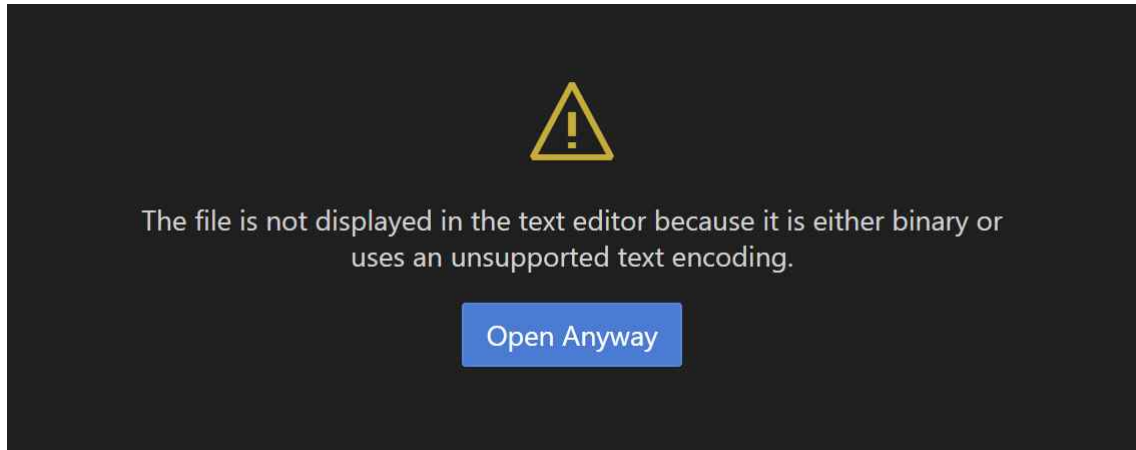


눌러보니 over the horizen 이라는 곡을 들었다는 것을 확인할 수 있었다.



김소리의 거주지를 찾아보자.

이것저것 찾아봤는데 지원되지 않는 파일이라고 떠서 여기서 더 이상 하지 못했다.



데이터베이스 사용하는 법을 공부해야 할 것 같다.