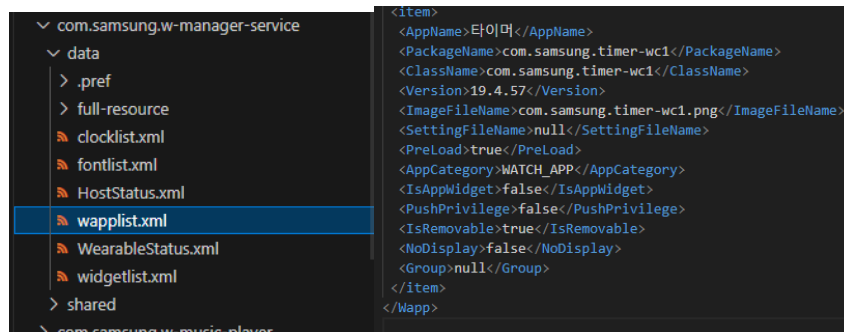


# 3S CTF

## Forensic-Wat ch??

SWING 32 기 한재희

다운받은 파일을 비주얼코드로 열어봤다. 그래야 보기 편할 것 같아서 열어보았다.  
우선 앱 개수를 먼저 세야 하기 때문에 이것 저것 눌러보다가 manager-service 폴더가  
있길래 거기에 waplist 가 있어서 살펴봤다.

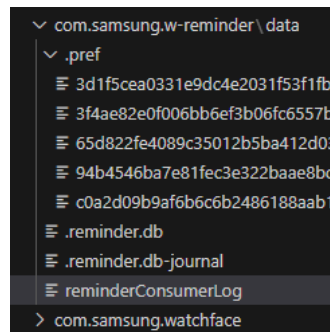


보니까 이렇게 한 묶음씩 앱 별로 묶여 있는 듯한 모양이어서



이렇게 옆에 타임라인 처럼 뜨길래 묶음을 세어보니 총 21 개 였다.

그리고 3 번째 리마인드 시간을 찾기 위해 보다가 폴더에 reminder 이름이 있어서 거기에  
있는 log 로그 폴더를 봤다.



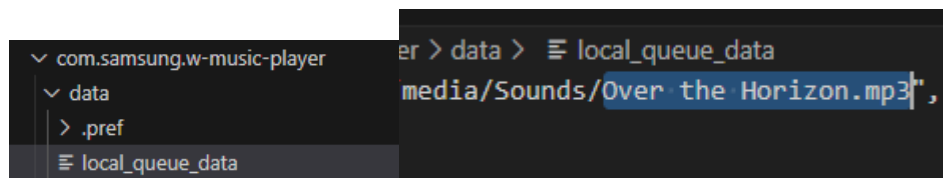
```

1 2023/10/29 22:38:18:371 getOrigin
2 2023/10/29 22:38:18:371 start
3 2023/10/29 22:38:18:400 __onStart
4 2023/10/29 22:38:18:400 __stopAft
5 2023/10/29 22:38:18:401 getOrigin
6 2023/10/29 22:38:18:401 __onRecei
7 2023/10/29 22:38:18:401 __sendUpd
8 2023/10/29 22:38:18:447 __stopAft
9 2023/10/29 22:38:18:447 setReques
10 2023/10/29 22:38:25:339 __onStopWo
11 2023/10/29 22:38:25:397 __checkApp
12 2023/10/29 22:38:25:525 __unsetTi
13 2023/10/29 22:38:25:525 __unsetTi
14 2023/10/29 22:45:39:581 getOrigin
15 2023/10/29 22:45:39:581 start
16 2023/10/29 22:45:39:594 __onStart
17 2023/10/29 22:45:39:594 __stopAft
18 2023/10/29 22:45:39:594 getOrigin
19 2023/10/29 22:45:39:595 __onRecei
20 2023/10/29 22:45:39:595 __sendUpd
21 2023/10/29 22:45:39:618 __stopAft
22 2023/10/29 22:45:39:618 setReques
23 2023/10/29 22:45:47:332 __onStopWo
24 2023/10/29 22:45:47:383 __checkApp
25 2023/10/29 22:45:47:494 __unsetTi
26 2023/10/29 22:45:47:495 __unsetTi
27 2023/10/29 22:45:48:764 getOrigin
28 2023/10/29 22:45:48:764 start

```

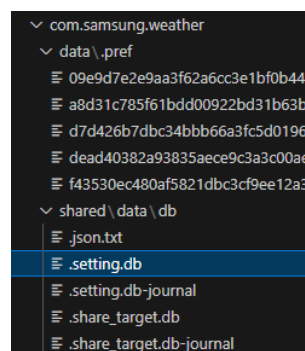
Start 를 보니 세번째 스타트가 22:45:48 이라는 걸 알 수 있었다.

음악 파일명을 찾기 위해 또 보다가 바로 밑에 music-player 폴더가 있어서 그 안에 있는 data 를 봤다.



보니까 Over the Horizon.mp3 하나만 있는걸 확인할 수 있었다.

사는 곳을 찾기 위해 찾아보다가 날씨가 밑에 있길래 봤다.



근데 거의 다 .db 로 끝나길래 데이터베이스를 깔아서 확인해봤다.

이름	타입	스키마
▼ 테이블 (8)		
▼ CITY_TABLE		CREATE TABLE CITY_TABL
PK_ID	INTEGER	"PK_ID" INTEGER NOT NULL
pageIndex	INTEGER	"pageIndex" INTEGER
locationId	TEXT	"locationId" TEXT
cityName	TEXT	"cityName" TEXT
cityNameEng	TEXT	"cityNameEng" TEXT
countryName	TEXT	"countryName" TEXT
countryNameEng	TEXT	"countryNameEng" TEXT
stateName	TEXT	"stateName" TEXT
stateNameEng	TEXT	"stateNameEng" TEXT

찾다가 여기에 도시 이름 칸이 있는데 내용이 나오지 않아서 여긴 막혔다.  
막혔다고 생각했는데 이것저것 눌러보다가 데이터 탐색칸을 누르니까 딱 뚫다.

PK_ID	pageIndex	locationId	cityName	cityNameEng	countryName	countryNameEng
필터	필터	필터	필터	필터	필터	필터
1	1	0 4145000000:CurrentCity	하남시	Hanam	대한민국	9999

하남시에 사는 것 같다.  
뉴스를 찾기 위해 가장 연관 있어보이는 magazine 을 열어봤다.

테이블(T):	stories
meta	meta
sqlite_sequence	sqlite_sequence
stories	stories
topics	topics

테이블을 바꾸다가 stories 에 뉴스들이 모여 있는 것 같아서 필터링으로 1695650088  
검색해봤다.

_id	topicName	topicId	type	storyId	author	url
...	필터	필터	필터	필터	필터	필터
1	52 스포츠	sports	NULL	sports-1695650088-1629315401	세계일보	http://c

세계일보가 뉴스를 낸 걸 확인할 수 있다.

3S{21\_22:45:48\_Over the Horizon.mp3\_대한민국 하남시\_세계일보}