📖

Wat ch??

Wat ch??

500

Forensic SWING

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

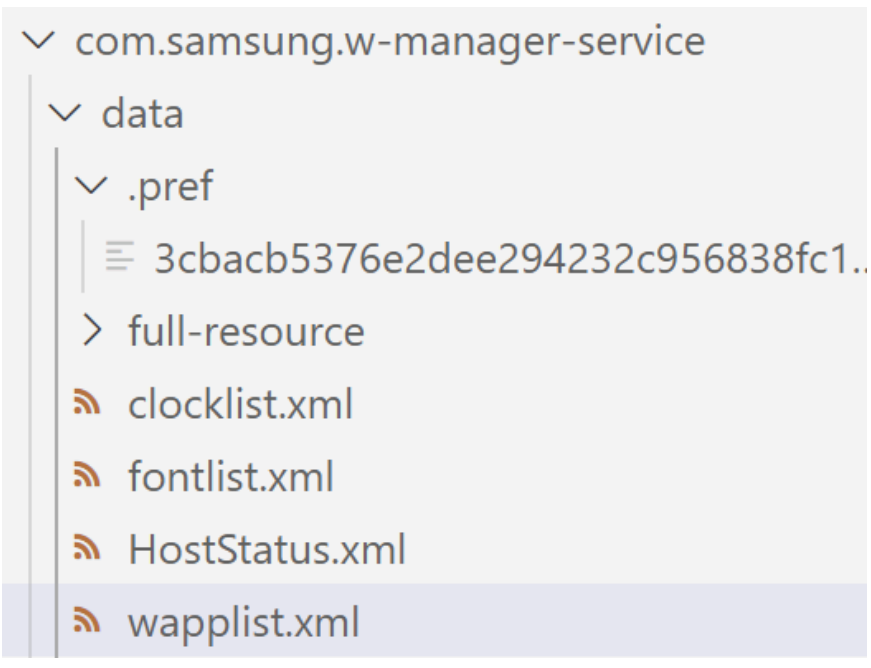
flag 형식: 3S{1_2_3_4_5}

wat_ch_.zip

플래그 제출

문제의 파일을 Visual Studio Code와 DB로 열어 살펴봤다.

1. 어플리케이션 개수



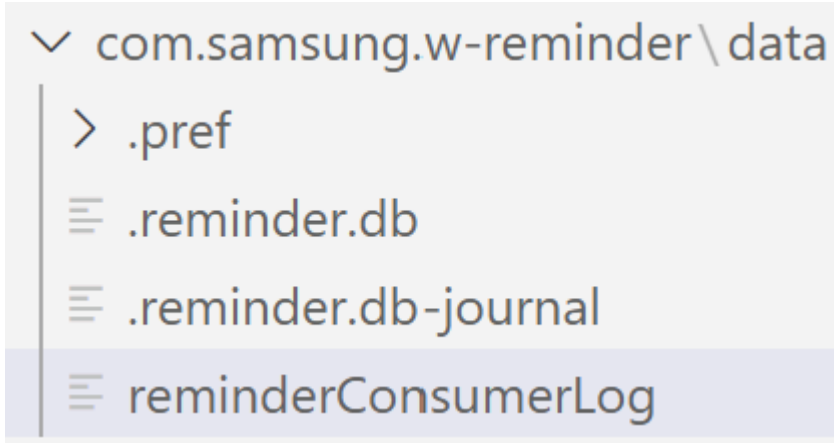
모든 앱 리스트를 살펴본 결과

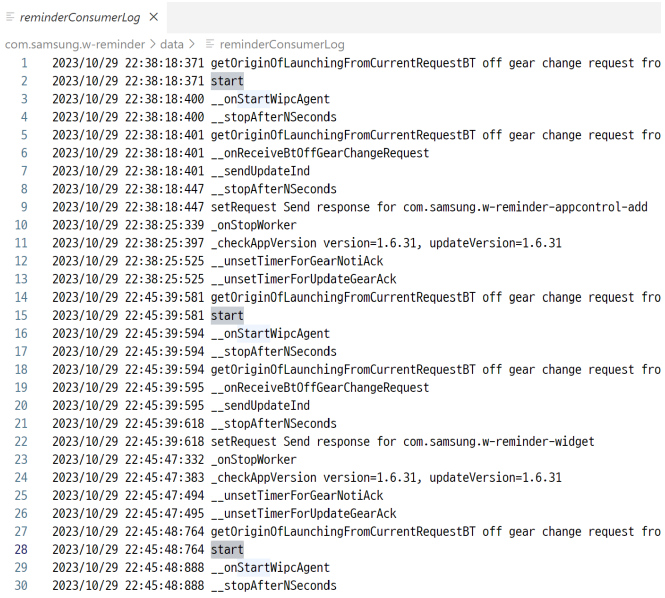
Galaxy Store
Samsung Health
T share
갤러리
고도-기압계
날씨
내 폰 찾기
네이버 지도
뉴스 브리핑

리마인더
메시지
뮤직
빅스비
설정
세계시각
스타벅스
알람
연락처
전화
캘린더
타이머

로 총 `21`개인 것을 알 수 있다.

2. 3번째 리마인더 작성 시간(HH:MM:SS)





리마인더 로그를 살펴보니 세번째 start 시간을 보아 `22:45:48`인 것으로 보인다.

3. 음악 파일명(@@@.mp3)

뮤직 플레이어 데이터를 보니 mp3 음악이 `Over the Horizon.mp3` 하나만 남아있는 것을 볼 수 있다.

4. 김소리의 거주지(countryName cityName)

테이블(T): USERINFO0 — 모든 열에서 필터링

	KEY	VALUE	EXTRA1	EXTRA2	EXTRA3
	필터	필터	필터	필터	필터
1	TNC	UPf8T/···	NULL	NULL	NULL
2	Name	UPf8T/···	NULL	NULL	NULL
3	Email	UPf8T/···	NULL	NULL	NULL
4	UserID	VLUZCv6xazV2XNIce···	NULL	NULL	NULL
5	UserAuthToken	ArKc8ls61YT0oxkMI···	NULL	NULL	NULL
6	LoginID	dkMw6DkAmdRwhM···	NULL	NULL	NULL
7	APIURL	7rvgU7lcRt17n4yaQ···	NULL	NULL	NULL
8	AUTHURL	7rvgU7lcRt17n4yaQ···	NULL	NULL	NULL
9	Time	Xoj4/···	NULL	NULL	NULL
10	SignInMCC	FKoLYSZlmQ9lgzph···	NULL	NULL	NULL
11	DeviceID	CiInzVBm5/YmpcAk/···	NULL	NULL	NULL
12	CustomizedService	yroiRiB4SUbXel+nge···	NULL	NULL	NULL
13	MCC	FKoLYSZlmQ9lgzph···	NULL	NULL	NULL
14	RCC	4NzEKtZbFngecDKY···	NULL	NULL	NULL

테이블(T): USERPROFILE0 — 모든 열에서 필터링

	KEY	VALUE	EXTRA1	EXTRA2	EXTRA3
	필터	필터	필터	필터	필터
1	birthdays:date:day	sntOM5pq6t1sJcAtj···	NULL	NULL	NULL
2	birthdays:date:month	7T/···	NULL	NULL	NULL
3	birthdays:date:year	e0qDKuEEz2FFFnljO···	NULL	NULL	NULL
4	birthdays:metadata:source:type	QDHAPm2qaOO6Im···	NULL	NULL	NULL
5	etag	99iRYR5s7/···	NULL	NULL	NULL
6	locales:metadata:source:type	QDHAPm2qaOO6Im···	NULL	NULL	NULL
7	locales:value	4NzEKtZbFngecDKY···	NULL	NULL	NULL
8	names:familyName	HCpkQ+c37BetM8QI···	NULL	NULL	NULL
9	names:givenName	Pu32dtWwbMJA20+···	NULL	NULL	NULL
10	names:metadata:source:type	QDHAPm2qaOO6Im···	NULL	NULL	NULL
11	birthdays	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
12	emailAddresses	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
13	events	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
14	genders	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
15	healths	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
16	messengerAccounts	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
17	names	h6cOIZdZ57RT9Ggli···	NULL	NULL	NULL
18	nicknames	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
19	notes	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
20	organizations	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
21	phoneNumbers	jMmv75qotUtg30kVQ···	NULL	NULL	NULL
22	photos	6aqSgQ3xnWqCLTV···	NULL	NULL	NULL
23	statusMessages	h6cOIZdZ57RT9Ggli···	NULL	NULL	NULL
24	userId	VLUZCv6xazV2XNIce···	NULL	NULL	NULL
25	webAddresses	jMmv75qotUtg30kVQ···	NULL	NULL	NULL

여러 코드와 DB를 살펴봤지만 정확한 거주지는 알지 못했다.

다만 countryCode KR이고 언어 설정도 한국어 이기에 Korea 쯤으로 추측.. 할 수 있다.

5. 1695650088에 뉴스를 발행한 author

매거진의 DB를 열어 살펴봤다.

DB Browser for SQLite - C:\Users\lucy4\Downloads\wat_ch_\apps_rw\com.samsung.w-magazine-wc1\data\service\db\.magazine.db

파일(F) 편집(E) 보기(V) 도구(T) 도움말(H)

새 데이터베이스(N) | 데이터베이스 열기(O) | 변경사항 저장하기(W) | 변경사항 취소하기(R) | 프로젝트 열기(P) | 프로젝트 저장하기(V) | 데이터베이스

데이터베이스 구조 | 데이터 보기 | Pragma 수정 | SQL 실행

테이블(T): stories — 모든 열에서 필터링

	gePath	authorImageWidth	authorImageHeight	title	body	body_full	imestamp	image	imagePa
		필터	필터	필터	필터	필터	5650088	필터	필터
1		NULL	NULL	[아시안게임] 단일팀···	얼어붙은 한반도 정세···	NULL	1695650088	https://ic-···	NULL

DB Browser for SQLite - C:\Users\lucy4\Downloads\wat_ch_\apps_rw\com.samsung.w-magazine-wc1\data\service\db\.magazine.db

파일(F) 편집(E) 보기(V) 도구(T) 도움말(H)

새 데이터베이스(N) | 데이터베이스 열기(O) | 변경사항 저장하기(W) | 변경사항 취소하기(R) | 프로젝트 열기(P) | 프로젝트 저장하기(V) | 데이터베이스

데이터베이스 구조 | 데이터 보기 | Pragma 수정 | SQL 실행

테이블(T): stories — 모든 열에서 필터링

	d	type	storyId	author	authorImage	authorImagePath	authorImageWidth	authorImageHeight	title
		필터	필터	필터	필터	필터	필터	필터	필터
1		NULL	sports-1695650088···	세계일보	http://···	NULL	NULL	NULL	[아시안게임] 단일팀·

stories 테이블로 이동하여 타임스탬프에 1695650088을 검색했더니, 해당 매거진의 author 정보를 알 수 있다.

세계일보

이를 다 조합하면 FLAG는 다음과 같다.

3S{21_22:45:48_Over the Horizon.mp3_Korea_세계일보}