

Digital Evidence from Android-based Smartwatch

Jae-ki Kim

Jack2

jack2@korea.ac.kr

jack2yo@gmail.com

<http://jack2.codebreaking.org>





1. Target Device

2. Method & Process

3. Digital Evidence

4. Conclusion

Target Device

- Smart Watch – Galaxy Gear (SAMSUNG)





- Smart Watch – Galaxy Gear (SAMSUNG)

속성	정보
프로세서	삼성 엑시노스 4212 SoC. ARM Cortex-A9 MP2 800 MHz CPU, ARM Mali-400 MP4 440 MHz GPU
메모리	512 MB LPDDR1 SDRAM, 4 GB 내장 메모리
디스플레이	1.63인치 320 x 320 S-Stripe RGB 서브픽셀 방식의 삼성D Super AMOLED 정전식 터치스크린
네트워크	블루투스 4.0+BLE
카메라	190만 화소 AF
배터리	Li-Ion 315 mAh, 사용 시간 25시간, 대기 시간 150시간
운영체제	안드로이드 기반 웨어러블 커스텀 OS

Method & Process

For Collecting Digital Evidence

from Android-based Smartwatch



0. Warming-Up

- Access to a Galaxy Gear



0. Warming-Up

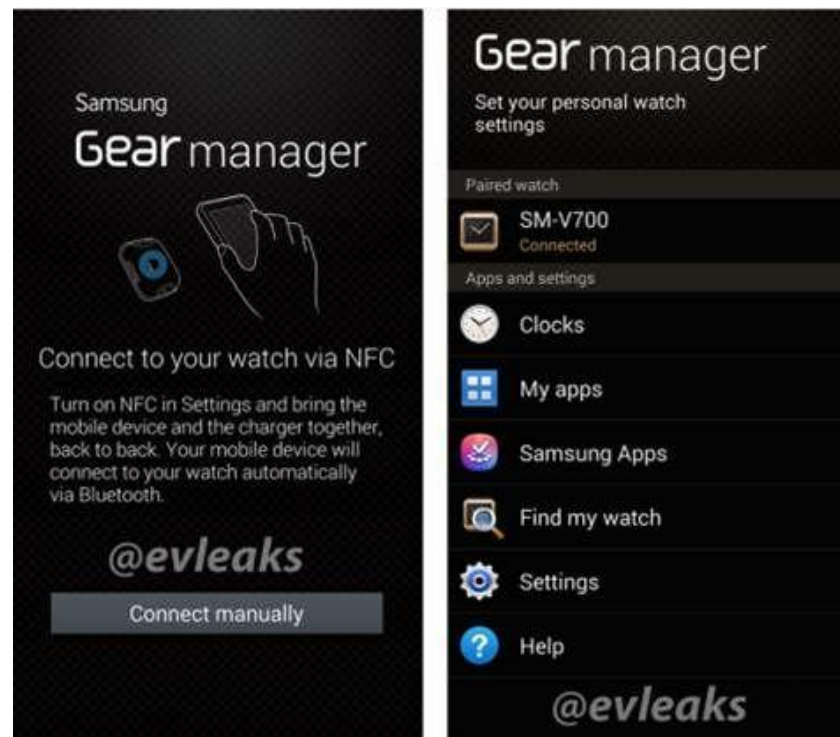
- Access to a Galaxy Gear
 - ✓ Need to **approved device** (ex. Galaxy S III or later)





0. Warming-Up

- Access to a Galaxy Gear
 - ✓ Need to approved device (ex. Galaxy S III or later)
 - ✓ **Install 'Gear Manger' Application (only SAMSUNG Apps)**





0. Warming-Up

- Access to a Galaxy Gear
 - ✓ Need to approved device (ex. Galaxy S III or later)
 - ✓ Install 'Gear Manger' Application (only SAMSUNG Apps)
- **Synchronization (For the 1st time)**
 - ✓ NFC
 - ✓ Bluetooth



0. Warming-Up

- Access to a Galaxy Gear
 - ✓ Need to approved device (ex. Galaxy S III or later)
 - ✓ Install 'Gear Manger' Application (only SAMSUNG Apps)
- Synchronization (For the 1st time)
 - ✓ NFC
 - ✓ Bluetooth
- **Hold the Galaxy Gear Charging Dock**
 - ✓ Connect with USB

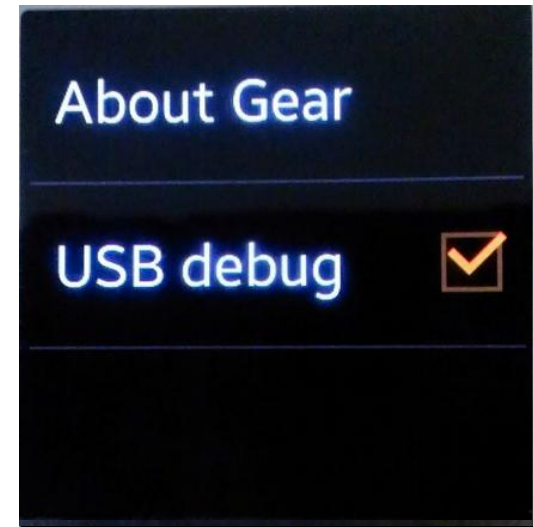




1. Rooting

▪ Previous work

- ✓ Install [Samsung USB Drivers](#)
- ✓ Settings > Gear Info > Tap Software Version 10 times
- ✓ Enable USB Debugging on the Galaxy Gear
- ✓ Plug in the Galaxy Gear via USB



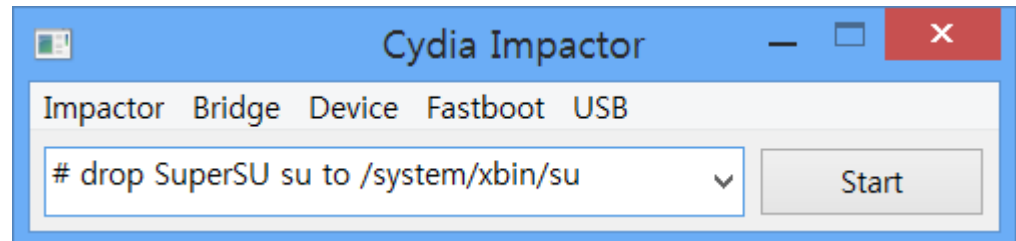


1. Rooting

- Previous work
 - ✓ Install Samsung USB Drivers
 - ✓ Settings > Gear Info > Tap Software Version 10 times
 - ✓ Enable USB Debugging on the Galaxy Gear
 - ✓ Plug in the Galaxy Gear via USB

- **Root the Galaxy Gear**

- ✓ Download [Cydia impactor](#)
- ✓ Start
- ✓ Install [Busybox](#)



```
C:\Users\Jaeki>adb devices
List of devices attached
4101874456a8b0a9    device
```

```
C:\Users\Jaeki>adb shell
shell@android:/ $ su
su
root@android:/ #
```




2. Imaging

▪ Limitations

- ✓ Only 4GB Built-In Memory
- ✓ No Network Interface (Wi-Fi, 3G/4G)

▪ Remote Dump with nc

[FORENSIC INSIGHT](#) | [멤버](#) | [이벤트](#) | [사진](#) | [파일](#)



김재기
3월 22일 · 수정됨

덤프 관련해서 질문있습니다~
Android 레퍼런스 폰인 Nexus 시리즈에는 외장 sdcard 를 사용하지 못합니다.
그래서 adb shell 상에서 dd if=[대상] of=/sdcard/image.img 와 같은 식으로 이
미징을 하는데 용량 한계가 있어서 용량한계로 종료되는 현상이 발생합니다.
이러한 경우 어떤 방법으로 이미지를 뜯 수 있을지 포렌식 인사이트 그룹 멤버님
들의 노하우가 궁금합니다. 😊



2. Imaging

▪ Limitations

- ✓ Only 4GB Built-In Memory
- ✓ No Network Interface (Wi-Fi, 3G/4G)

▪ Remote Dump with nc

- ✓ C:\Users\Jack2> adb forward tcp:8787 tcp:8787
- ✓ root@android:/ # ./busybox nc -l -p 8787 -e dd if=/dev/block/mmcblk0p21

```
/dev/block/mmcblk0p21 /data ext4 rw,nosuid,nodev,noatime,barrier=1 ....
```

- ✓ C:\Users\Jack2> nc 127.0.0.1 8787 > jack2.img

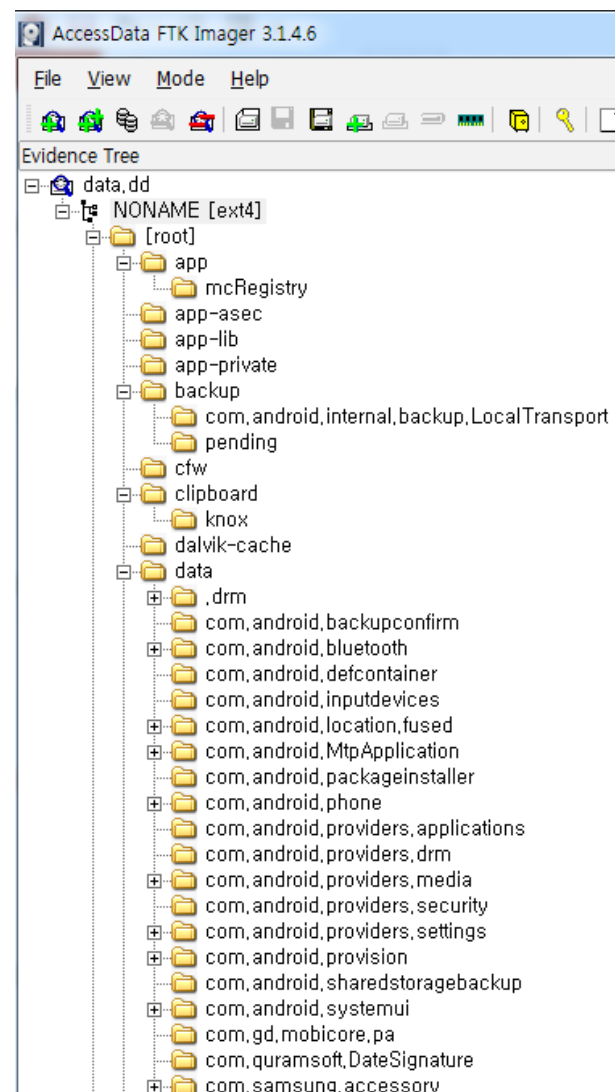
Digital Evidence



Use FTK Imager

Very large amounts of data -- ::

Select useful 4 digital evidences ^^





bt_config.xml

- **Path**

- ✓ /data/misc/bluetooth/

- **Info**

- ✓ Specific information synchronized smartphone (Device name , Bluetooth address ...)

```
<N2 Tag="Remote">
  <N1 Tag="04:1b:ba:26:59:ae">
    <N1 Tag="Manufacturer" Type="int">15</N1>
    <N2 Tag="LmpVer" Type="int">6</N2>
    <N3 Tag="LmpSubVer" Type="int">16646</N3>
    <N4 Tag="Name" Type="string">Jack2 (SHV-E330L)</N4>
    <N5 Tag="DevClass" Type="int">5898764</N5>
    <N6 Tag="DevType" Type="int">1</N6>
    <N7 Tag="LinkKeyType" Type="int">5</N7>
    <N8 Tag="PinLength" Type="int">0</N8>
    <N9 Tag="LinkKey" Type="binary">98f3e3929ea9de4da66ec59e3e2f1476</N9>
    <N10 Tag="Service" Type="string">0000110a-0000-1000-8000-00805f9b34fb 00001105-0000-1000-8000-00805f9b34fb
  </N1>
</N2>
</Bluetooth>
```

If you fail to obtain a smartphone,
Identify the synchronized device



NotificationSync.db

▪ Path

✓ /data/data/com.samsung.appcessory.NotiConsumerService/databases/

▪ Info

✓ SMS/MMS, Hangout Message, Gmail information synchronized smartphone

mPackage	mMsgType	mID	mNotiID	mDateTime	mMainText	mTitle	mPhoneNumber	mTextMessage
Click here to define a filter								
message	sms	35	123	1397636511000	8246		8246	[인증번호:8246] 카카오톡에서 보낸 인증번호입니다.
googlemail		-1	-1778170201	1397637853150	Jack2	Jack2		Notice Test -- ----- Jack2's Blog : http://jack2.codebreaking.org jack2.gear@gmail.com
message	sms	37	123	1397639388000	발신자 정보 없음			[LG U+] 개인정보보호를 위해 작성하신 휴대폰 가입청서 및 구비서류를 꼭 챙겨가세요!
message	sms	39	123	1397696544000	메시지			[LG U+] 신청하신 LG 유플러스 멤버십 카드가 우체국에 접수되었습니다. 7일 이내 배
googletalk		-1	0	1397696661503	Jaeki Kim	Jaeki Kim		행아웃에서 메시지를 보냈습니다.

Though deleted messages from your smartphone,
Check original message used by Synchronized information



watch.xml

- **Path**

- ✓ /data/data/com.samsung.accessory.FindMyPhone/ConsumerService/shared_prefs/

- **Info**

- ✓ Find a synchronized smartphone

```
root@android:/data/data # cat ./com.samsung.accessory.FindMyPhoneConsumerService/shared_prefs/watch.xml
y.FindMyPhoneConsumerService/shared_prefs/watch.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="attached" value="false" />
</map>
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
root@android:/data/data # ls -l ./com.samsung.accessory.FindMyPhoneConsumerService/shared_prefs/
-rw-rw---- u0_a12 u0_a12 306 2014-04-14 17:39 AccessoryPreferences.xml
-rw-rw---- u0_a12 u0_a12 112 2014-04-17 10:09 watch.xml
```

Guessing Activity Time

Ex) Put smartphone in the car and Visit Crime scene



WeatherClock

▪ Path

- ✓ /data/data/com.sec.android.widgetapp.ap.hero.accuweather.consumer.widget/databases/

▪ Info

- ✓ Check the local weather used Synchronized smartphone

The screenshot shows a database viewer interface. On the left, a tree view displays the database structure: WeatherClock (parent), android_metadata (child), MY_WEATHER_INFO (selected child), and MY_WEATHER_SETTING_INFO (child). The main area shows the 'Data' tab selected, displaying a table with the following columns: RecNo, NAME, NAME_ENG, STATE, STATE_ENG, LOCATION, TIMEZONE, and SU. The table contains two records. The first record (RecNo 1) has NAME '성북구' (Seongbuk-gu), NAME_ENG 'Seongbuk-gu', STATE '(null)', STATE_ENG '(null)', LOCATION 'cityId:current', TIMEZONE 'GMT+9', and SU '0'. The second record (RecNo 2) has NAME '서울' (Seoul), NAME_ENG 'Seoul', STATE '(null)', STATE_ENG '(null)', LOCATION '10000', TIMEZONE 'GMT+9', and SU '0'. The first record is highlighted with a red box around the NAME and NAME_ENG columns.

RecNo	NAME	NAME_ENG	STATE	STATE_ENG	LOCATION	TIMEZONE	SU
1	성북구	Seongbuk-gu	(null)	(null)	cityId:current	GMT+9	0
2	서울	Seoul	(null)	(null)	10000	GMT+9	0

Although Galaxy Gear is no GPS,

Check recently visited local information

Conclusion

Next Target Issue

Smart Watch – Galaxy Gear2 (SAMSUNG)

속성	정보
프로세서	1.0 GHz 듀얼 코어 프로세서
메모리	512 MB LPDDR1 SDRAM, 4 GB 내장 메모리
디스플레이	1.63인치 320 x 320 S-Stripe RGB 서브픽셀 방식의 삼성D 슈퍼 아몰레드 정전식 터치
네트워크	블루투스 v4.0 LE
센서	가속 센서, 자이로스코프, 심박 센서 , 방수/방진
카메라	200만 화소 AF
배터리	Li-Ion 300 mAh, 사용 시간 2~3일, 대기 시간 6 일
운영체제	타이젠 기반 웨어러블 플랫폼





- <http://theunlockr.com/2013/11/20/root-samsung-galaxy-gear-video/>
- <https://www.facebook.com/groups/212473532271572/permalink/247282375457354/>

