DFRWS USA 2016 – Presentations Ⅰ

A practical approach to analyze smartphone backup data as a digital evidence

Jaehyeok Han and Sangjin Lee

* Keywords : Backup and Restore, encryption

2016. 08. 08

Digital Forensic Research Center (DFRC)

Center for Information Security Technologies(CIST)

Korea University

Contents

- **Introduction**
- **Process to create backup files & approach**
  - Android
    - adb protocol – common for android devices
    - Kies/Smart switch - Samsung smartphone backup files
    - LG PC suit - LG smartphone backup files
  - iOS
    - iTunes, Backup protocols
- **Case study**
- **Conclusion**

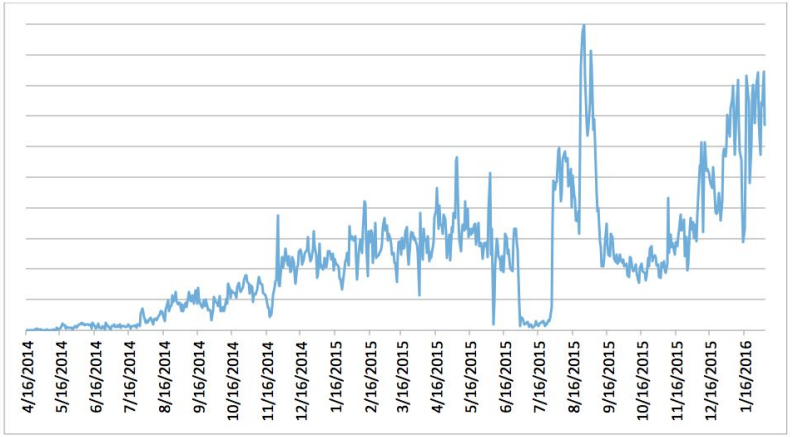
Introduction

Importance of backup data

- **Backup preserves user data including personal information**
  - device damage or loss could cause the disclosure of private information
  - frequent update of OS and apps could cause many errors

  → **Many people used to backup and restore their data**

- **The growing amount of ransomware attack requires more interest of the backup**
  - The best way against ransomware is backup of your data regularly



[Android Ransomware Trend]

Introduction

Valuable Backup for user data

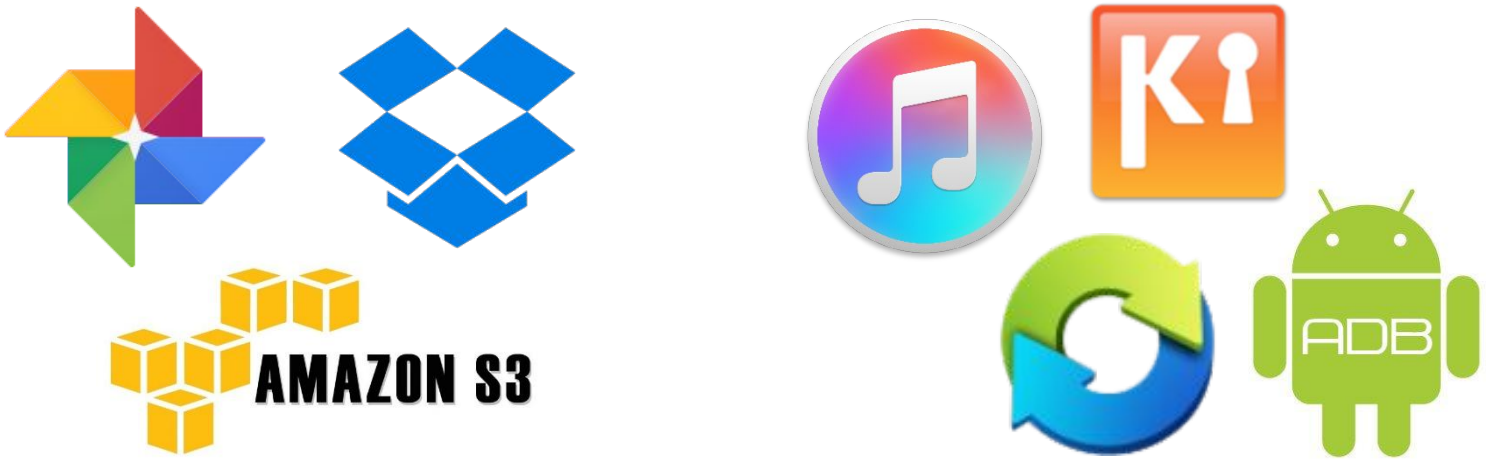
- **Backup files represent data in the devices at the moment**
  - Not just copied files – recover deleted data?
  - But it’s hard to recover deleted,
    because backup file is created using allocated data

- **The types of plaintext or can be decrypted**
  - Compression, Encryption, Encoding

Introduction

Backup data from smartphone

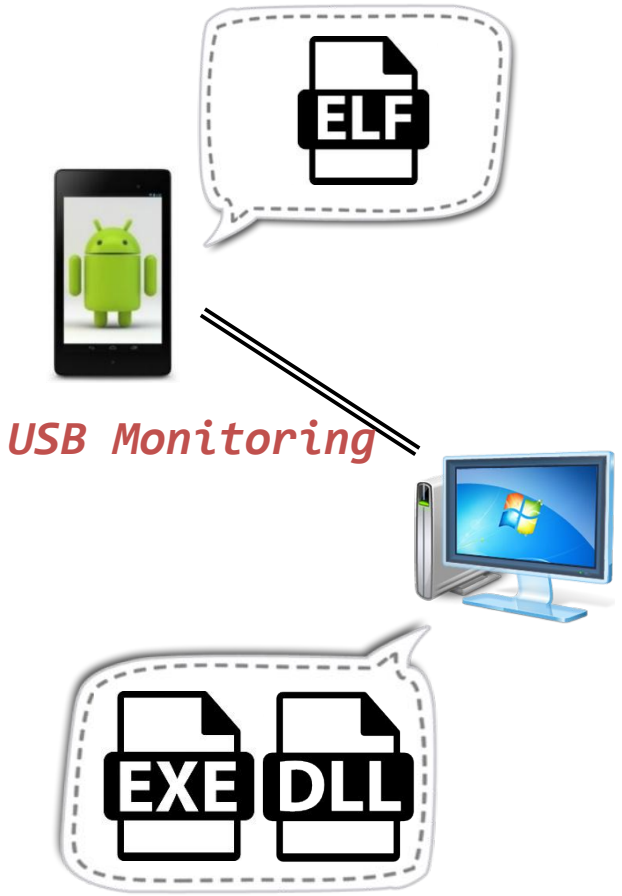
- **Smartphone is necessary, like a PC or laptop**
  - Use a cloud service (google, amazon, dropbox)
    → cloud storage
  - Use a synchronization program or commands(iTunes, Kies, adb)
    → local storage(hard disk, SD card, etc)



Process to create backup files

Method to figure out the process

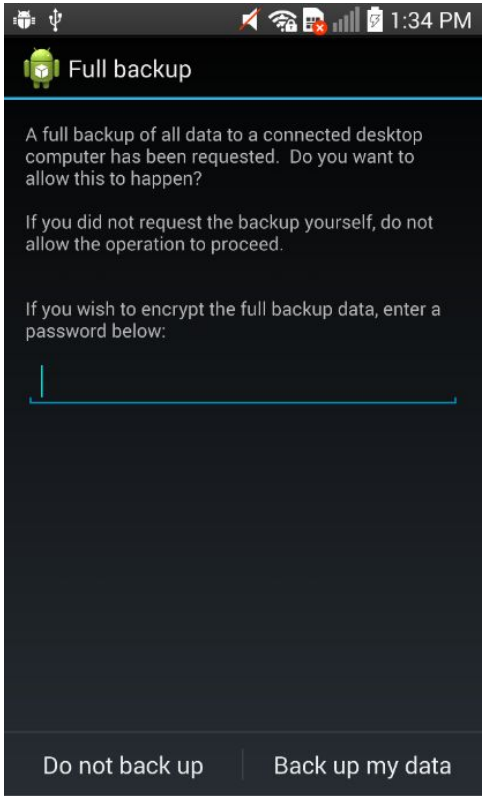
- **USB Monitoring**
  - Check the location of creating backup files
    - smartphone(android) : ELF files, demon
    - PC(windows) : .exe, .dll of the application
- **Source code(AOSP) analysis**

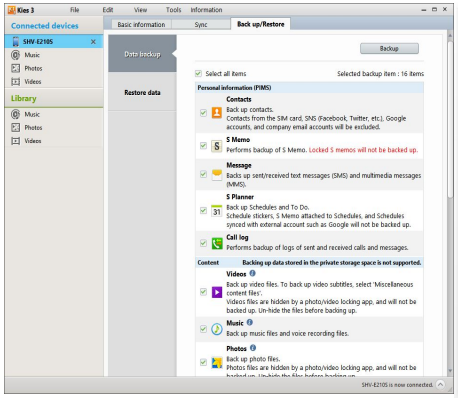


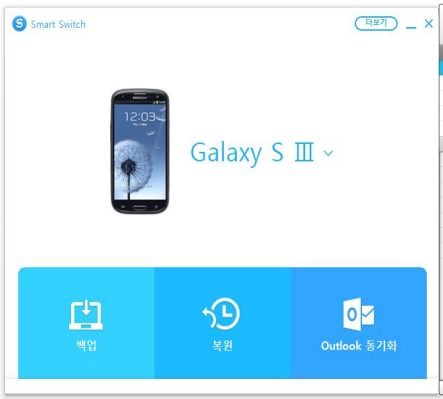
Process to create backup files

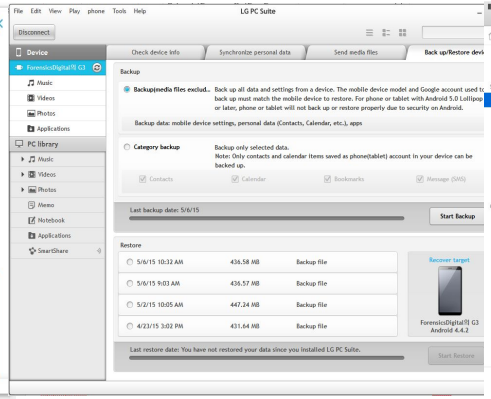
Ways to make backup files

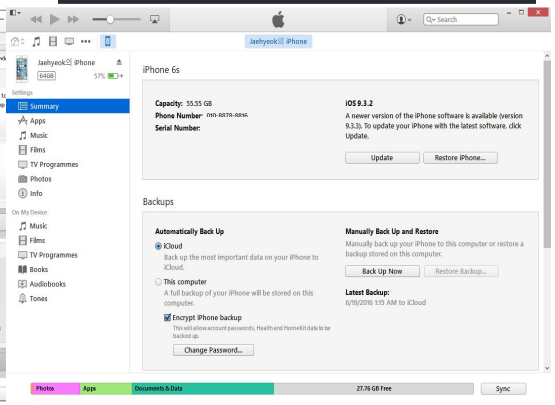
- **Android OS**
  - adb backup -all –f backup.ab
  - Samsung Galaxy series – Kies / Smart switch
  - LG Optimus,G series – LG PC Suite, LG Bridge
- **iOS**
  - iTunes











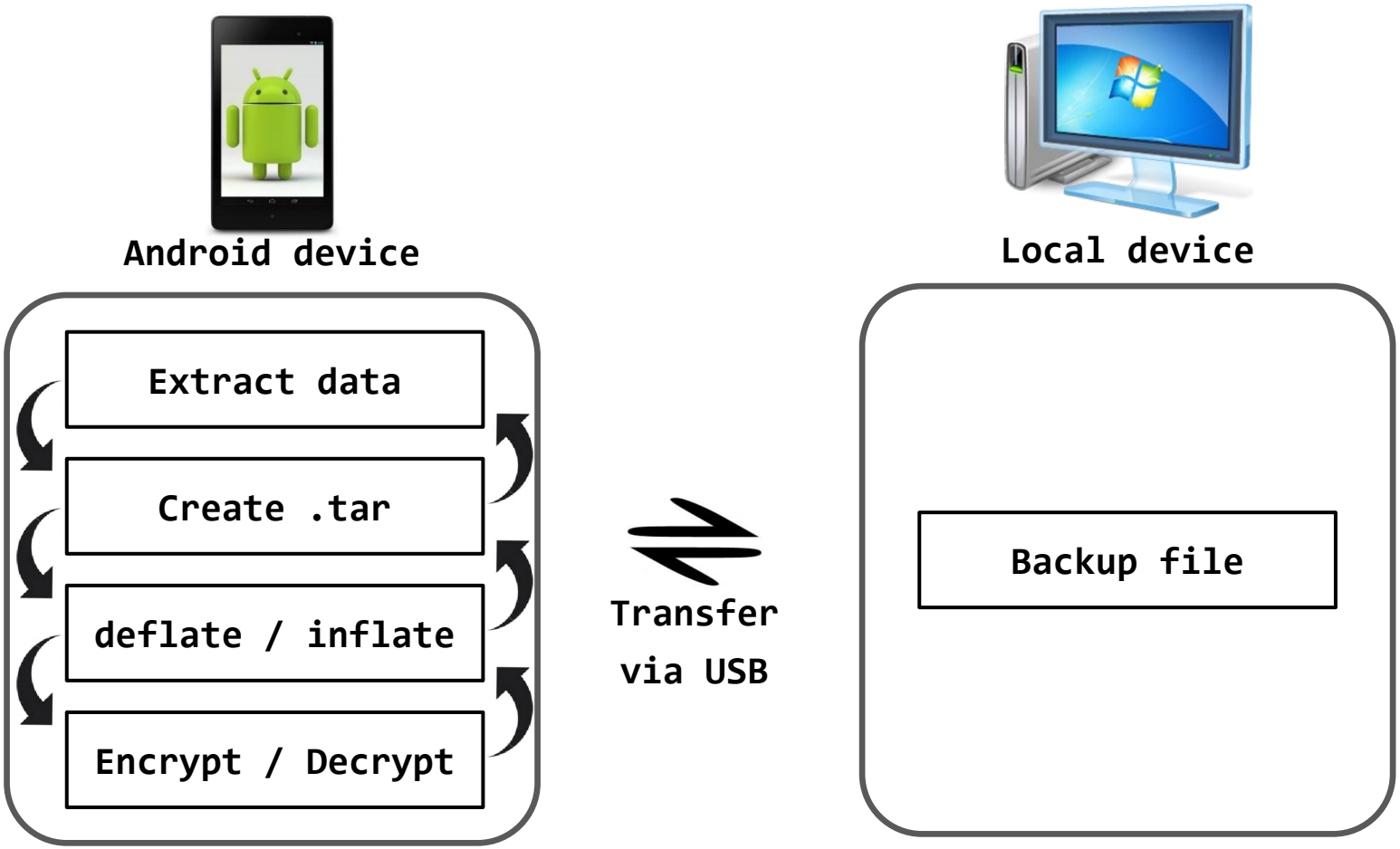
Process to create backup files

Backup items

- **Personal information (PIMS) - encrypted**
  - Contacts, message, call log, calendar, memo, and so on.
- **Account information and settings - encrypted**
  - email account, wifi, alarm, home screen, lock screen, and other configurations
- **Contents – without encryption**
  - Videos, Music, Photos, documents, Application, etc.

adb backup

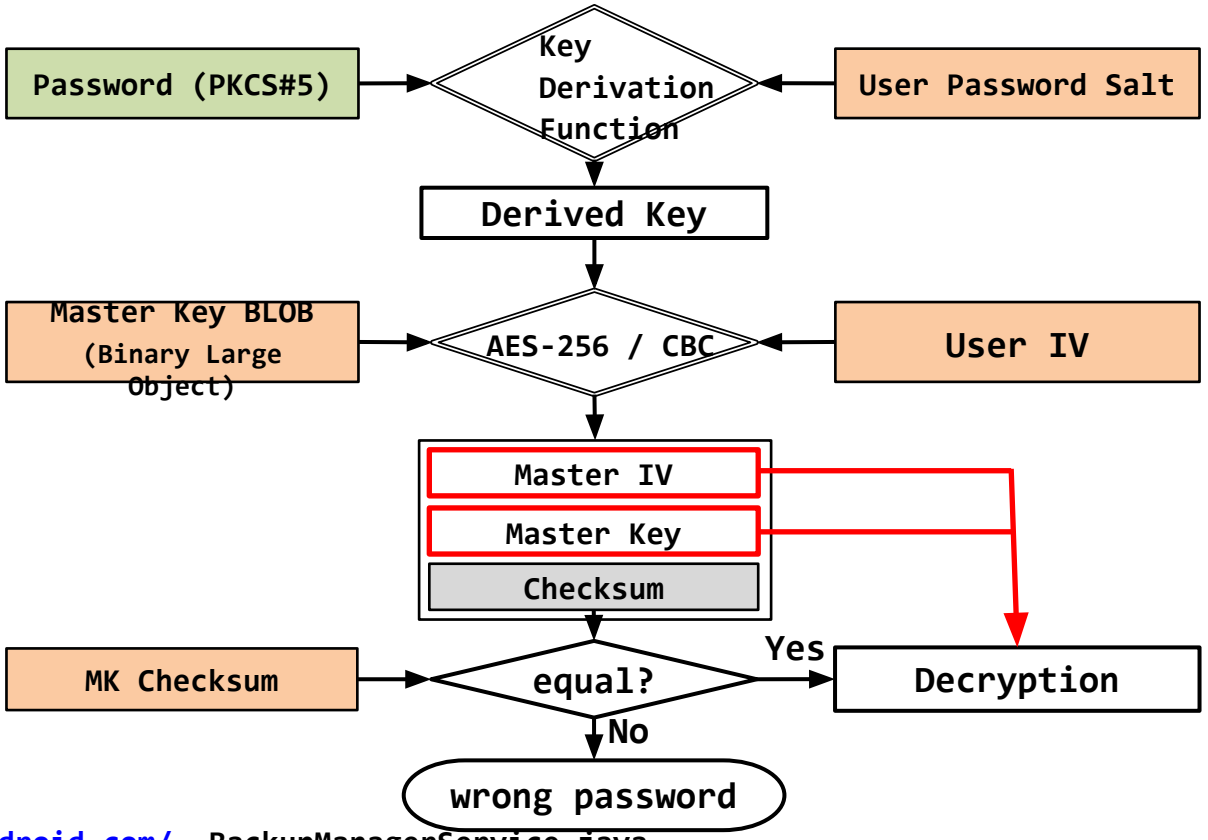
Process to generate adb backup file



adb backup

Android open source code from AOSP

- **Restore adb backup files**



https://source.android.com/, BackupManagerService.java

Android Encryption System, Teufl P. et al., Privacy and Security in Mobile Systems, IEEE, 2014.

adb backup

adb restore / Android Backup Extractor(abe)

- **adb restore backup.ab**
  - It can be extracted only the needed data from the backup manually

- **Utility to extract and repack Android backups**
  - Largely based on BackupManagerService.java from AOSP
    - unpack : abe unpack <backup.ab> <backup.tar> [pasward]
    - pack   : abe pack   <backup.tar> <backup.ab> [pasward]

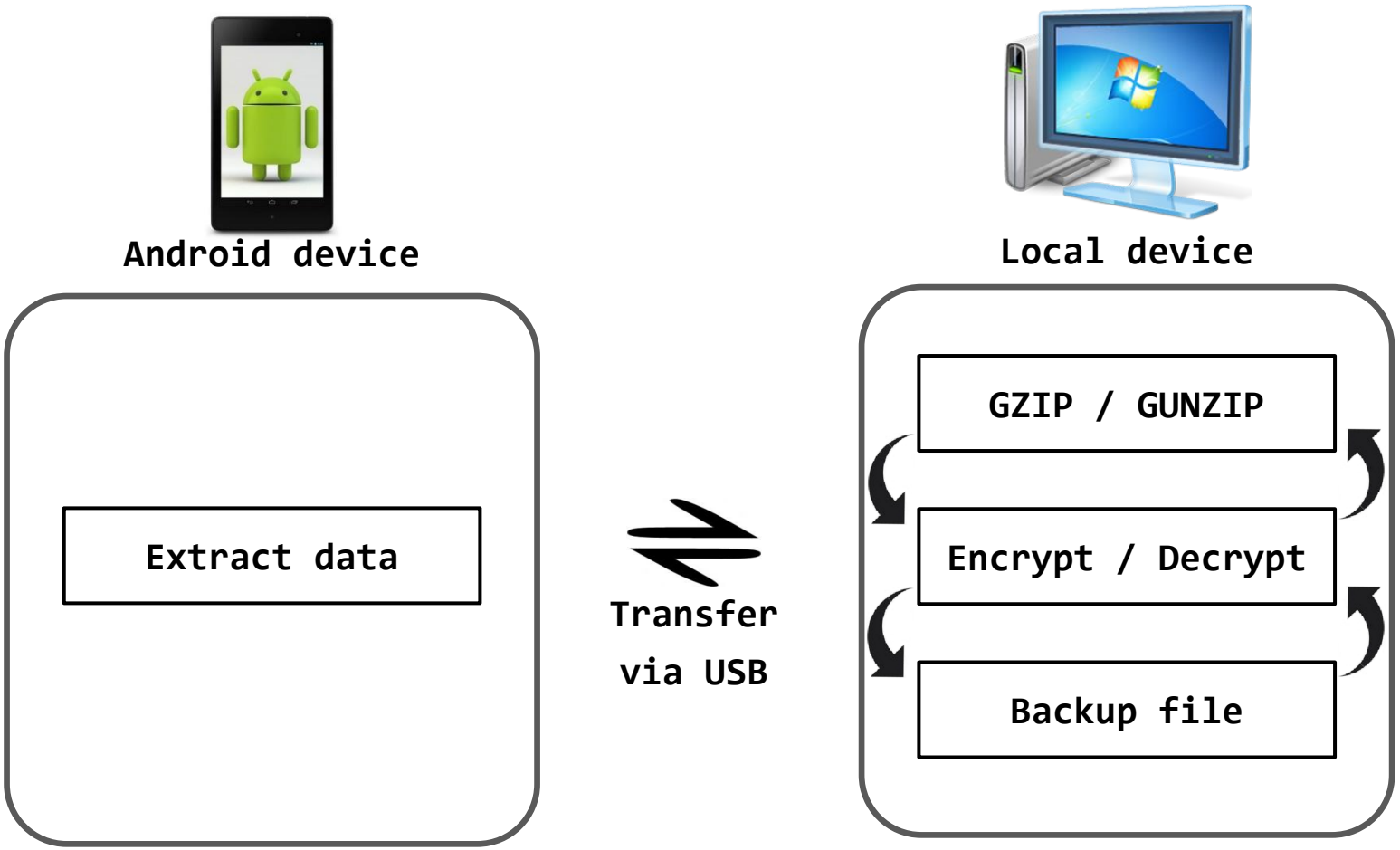
http://sourceforge.net/projects/adbextractor

https://github.com/nelenkov/android-backup-extractor (Nikolay Enlenkov)

Samsung smartphone backup data

Process to generate Samsung backup file

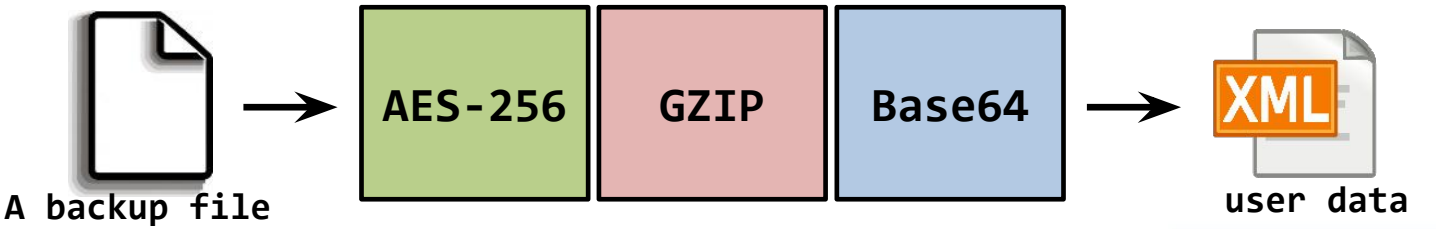
- KIES, Smart Switch



Samsung smartphone backup data

Restore Samsung backup files

- Decryption : AES-256
- Decompression : GZIP / Base64 decode



SMS, MMS

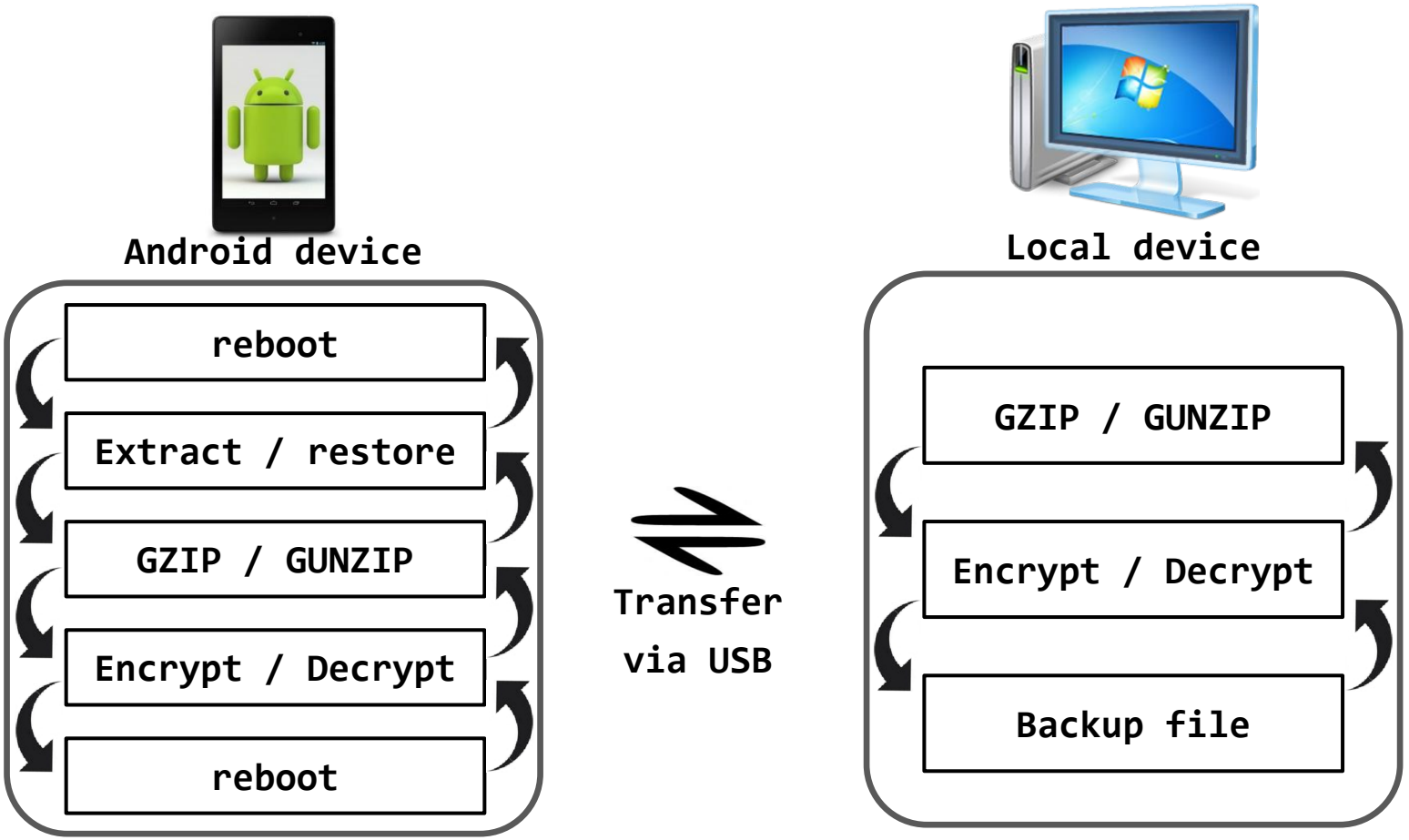
CreateDate	Sender	Receivers	MsgState	Decoded Message
2016-02-12T00:49:25			Read	
2016-02-12T01:45:01			Read	
2016-02-12T02:33:20			Read	
2016-02-12T07:55:30			Read	
2016-02-12T07:55:47			Read	
2016-02-12T16:26:16			Read	
2016-02-12T18:16:09			Read	
2016-02-12T18:16:45			Read	
2016-02-12T18:28:10			Read	

transformed to csv file format

LG smartphone backup data

Process to generate LG backup file

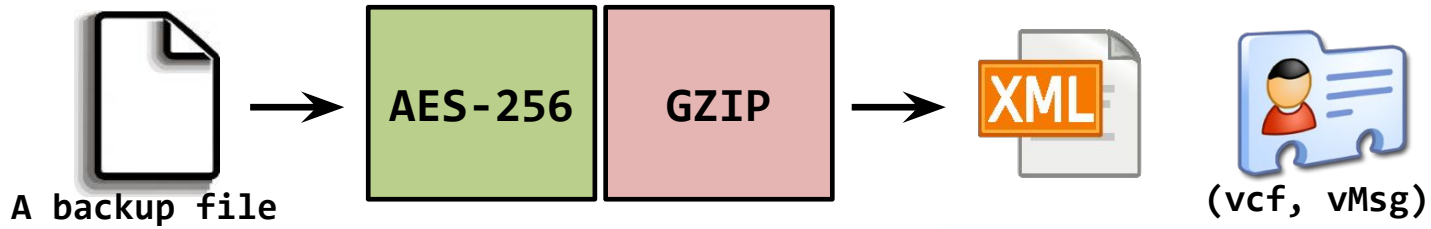
- LG PC Suite (Backup mode / Category backup mode)



LG smartphone backup data

Restore LG backup files

- Decryption : AES-256
- Decompression : GZIP



Contacts >

Name	PHONE	WORK	EMAIL	GROUP

bookmarks ⌄

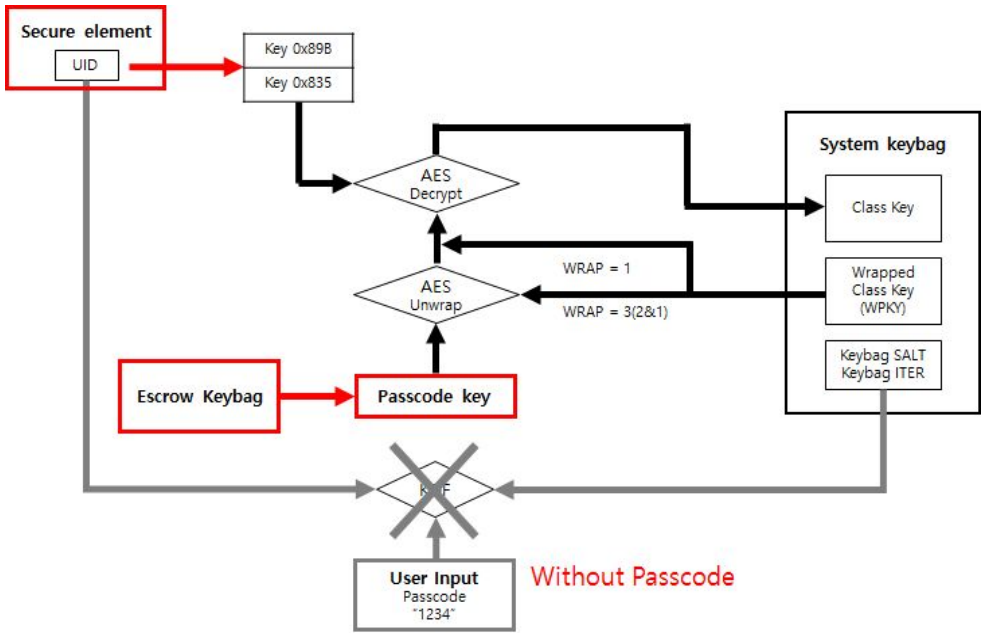
Title	URL
Google	http://www.google.co.kr/
LG mobile	http://www.lgapps.co.kr/
Naver	http://www.naver.com/
Facebook	http://www.facebook.com/

transformed to csv file format

iPhone backup data

- **Ways to backup iPhone data**
  - iTunes : Automatically backup on this computer / Manually backup
  - other utilities or use backup protocols.

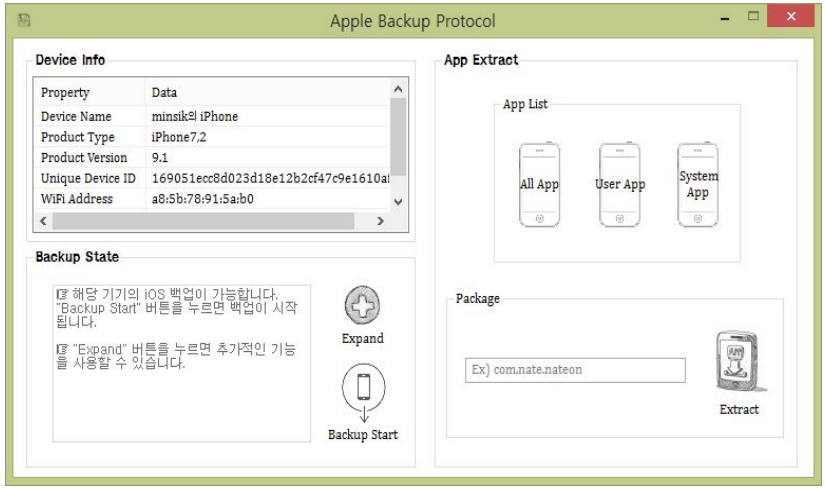
- **Use Lockdown files for pairing without passcode.**
  - DeviceCertificate, *EscrowBag*, HostCertificate, HostID, RootCertificate, SystemBUID



iPhone backup data

- **Extract backup data : protocols**
  - Mobile Backup2, AFC - media, File Relay – log, sms
  - Installation proxy – installed app list, House arrest – app data

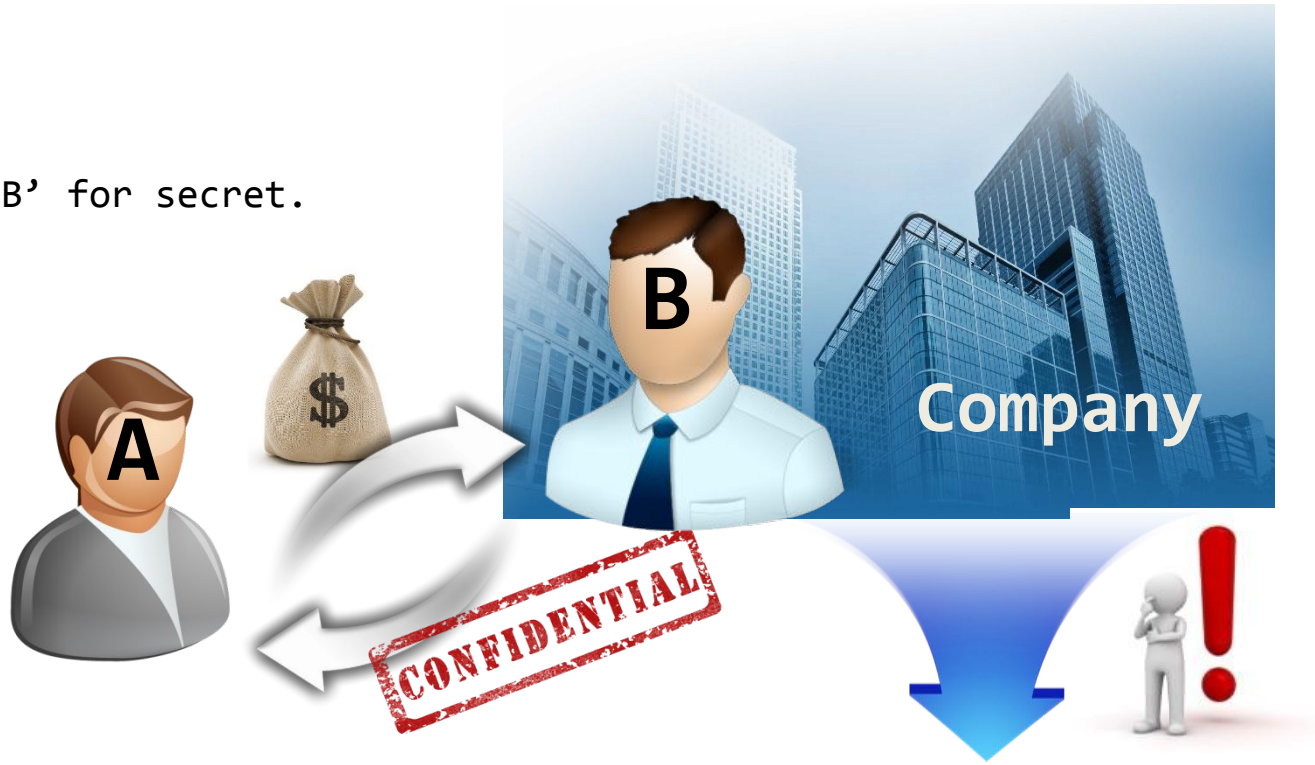
- **Restore and investigate the backup data using utilities**
  - iPhone backup browser, iFunBox, iTools, iBackupBot, iPhone backup browser



Case study

Leakage of Company's secret

- **Situation**
  - 'A' gave money to 'B' for secret.



- **Backup files were circumstantial evidence.**
  - PC and smartphone were properties of company(policy)
  - Smartphone was initialized by factory reset and anti-forensic tools were used on the PC.

Conclusion

- **Backup data of smartphone have valuable and important things.**
  - Data for the user's activity → a possibility as a digital evidence

- **The Backup data is one of the artifacts.**
  - It should be collected from PC – the past data
  - It would be extracted from smartphone – the current data

    (An alternative of selective imaging)

  → **User data can collect from smartphone's backup data.**

Thank you for listening

one01h@korea.ac.kr, sangjin@korea.ac.kr

KOREA UNIVERSITY

Korea University 정보보호대학원 CIST Center for Information Security Technologies