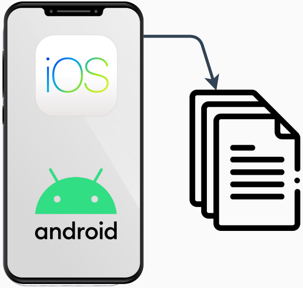
Systematic Evaluation of Forensic Data Acquisition using Smartphone Local Backup

DFRWS 23 Presentation

Julian Geus Jenny Ottmann Felix Freiling

Chair of IT Security Infrastructures
Friedrich-Alexander-Universität Erlangen-Nürnberg

Introduction



analysis

analysis

conviction

Smartphone Data Analysis

Black-Box tools: Software- or hardware tools from forensic service providers used to acquire data from mobile devices

Cellebrite

Belkasoft
forensics made easier

MSAB

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

OXYGEN
FORENSICS

Smartphone Data Analysis

Black-Box tools: Software- or hardware tools from forensic service providers used to acquire data from mobile devices

Cellebrite

Belkasoft
forensics made easier

MSAB

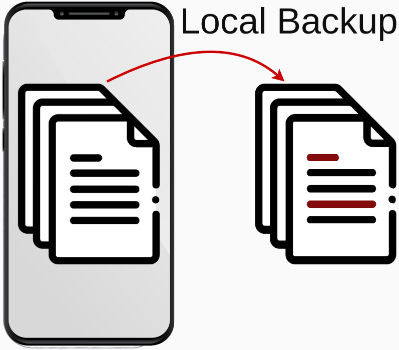
ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

OXYGEN
FORENSICS

Forensic Requirements

In forensics, it is of particular importance that the data's **provenance is explainable** and that the acquisition method is **verifiable and transparent**[a].

[a] Rodney McKemmish. *When is digital evidence forensically sound?* Springer, 2008.



Local Backup

The evidence is invalid!

???
The evidence is invalid!

Outline

Local Backup Basics

1. Why do we **care** about the local backup process in forensics?
2. Which **kind** of backup processes exist?

Evaluation Methodology

3. How can we **evaluate** the backup process?

Practical Execution

4. What is the **outcome** of an exemplary evaluation?

Local Backup

Different Kinds of Backup

Local Backup

- OS-Specific
- Third-Party

Cloud Backup

Different Kinds of Backup

Local Backup

- OS-Specific
- Third-Party

Cloud Backup

Research Idea

Why should anyone care about the local backup mechanism of mobile phones?

- **generic** - all Android and iOS devices supported
- can reliably acquire data **beyond the user's privileges**
- commonly used by **forensic service providers**

⇒ hardly any research on the implications

Research Idea

Why should anyone care about the local backup mechanism of mobile phones?

- **generic** - all Android and iOS devices supported
- can reliably acquire data **beyond the user's privileges**
- commonly used by **forensic service providers**

  ⇒ hardly any research on the implications

Research Idea

Are files acquired with the backup method of iOS or Android **forensically sound**?

Android Backup

The Android Debug Bridge (ADB) offers a local backup mechanism.

- by default all apps are included (before Android 12)
- apps can **opt-out** of local backup data
- Google apps, WhatsApp, Facebook, and more don’t participate

Android Backup

The Android Debug Bridge (ADB) offers a local backup mechanism.

- by default all apps are included (before Android 12)
- apps can **opt-out** of local backup data
- Google apps, WhatsApp, Facebook, and more don't participate

  Solution: **app downgrading**

Android Backup

The Android Debug Bridge (ADB) offers a local backup mechanism.

- by default all apps are included (before Android 12)
- apps can **opt-out** of local backup data
- Google apps, WhatsApp, Facebook, and more don’t participate

  Solution: **app downgrading**

ADB backup is **deprecated since 2019** and might be removed in future versions.

iOS Backup

iOS has an extensive local backup mechanism, natively supported on macOS and Windows with iTunes.

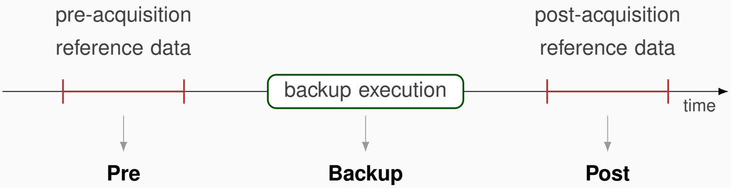
- for forensics: *libimobiledevice* [1]
- apps can **disable the backup** of their files
- can be encrypted using a user defined password: includes **more data**

  ⇒ health data, website- and call history, Wi-Fi settings, saved passwords

[1] `https://libimobiledevice.org/`

Methodology

Evaluation Methodology

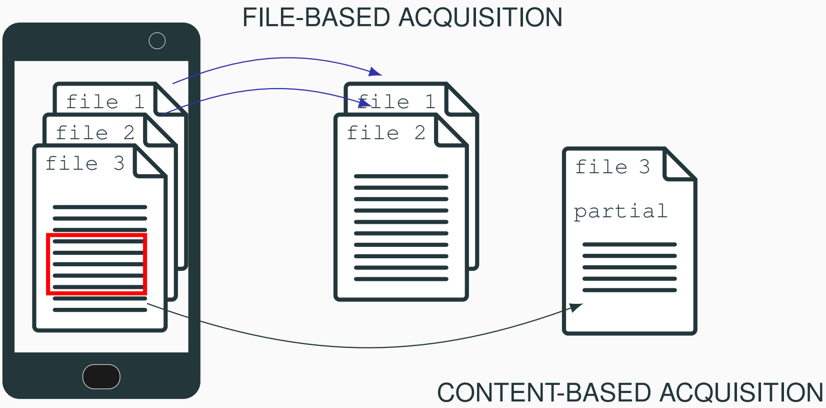


Pre: **reference data** before the acquisition to check for consistency errors

Backup: actual **local backup data**

Post: **post acquisition reference data** for a more detailed analysis

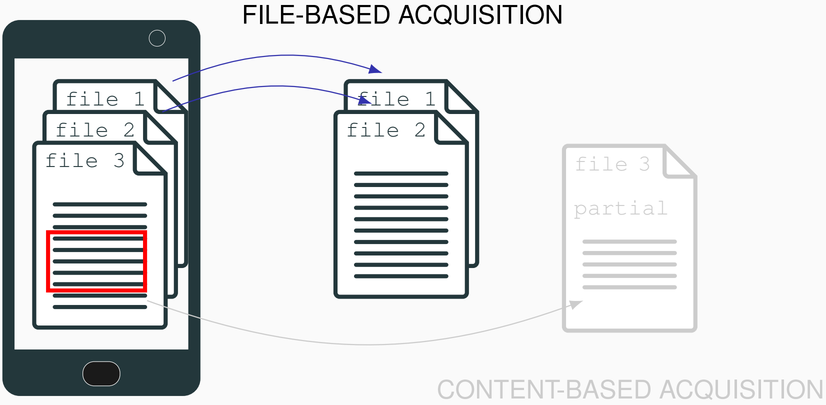
Different Types of Data



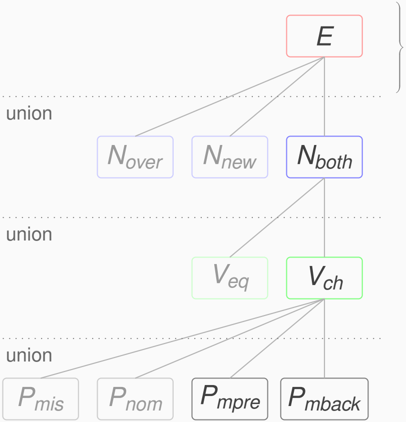
FILE-BASED ACQUISITION

CONTENT-BASED ACQUISITION

Different Types of Data



Data Classification



E

union

N_{over} N_{new} N_{both}

union

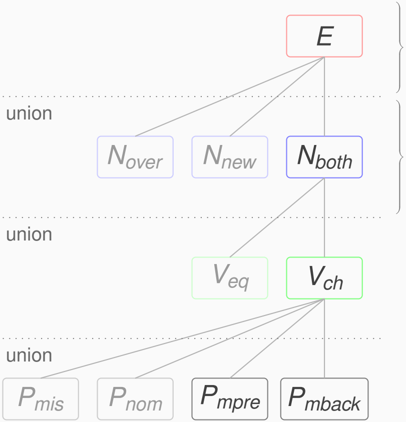
V_{eq} V_{ch}

union

P_{mis} P_{nom} P_{mpre} P_{mback}

Acquisition Experiment (union of *Pre* and *Backup*)

Data Classification



E

union

N_{over} N_{new} N_{both}

union

V_{eq} V_{ch}

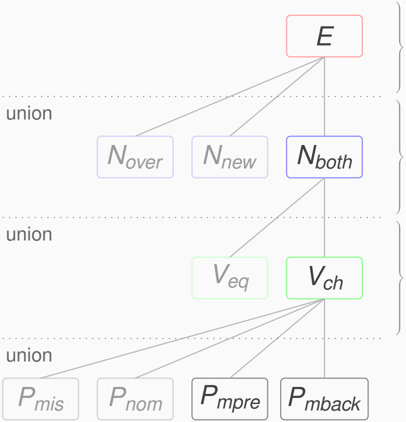
union

P_{mis} P_{nom} P_{mpre} P_{mback}

Acquisition Experiment (union of *Pre* and *Backup*)

Filename Comparison (between *Pre* and *Backup*)

Data Classification

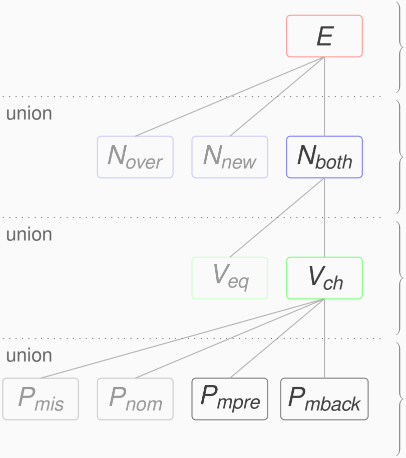


Acquisition Experiment (union of *Pre* and *Backup*)

Filename Comparison (between *Pre* and *Backup*)

Value Comparison (between *Pre* and *Backup*)

Data Classification



Acquisition Experiment (union of *Pre* and *Backup*)

Filename Comparison (between *Pre* and *Backup*)

Value Comparison (between *Pre* and *Backup*)

Mismatch Classification (using *Post* data)

Practical Execution

Practical Execution

Android Evaluation

Google Pixel 2

- Android 11
- rooted with Magisk

ADB Local Backup Evaluation

- ADB’s full backup functionality
- app downgrading for various apps

Practical Execution

Android Evaluation

Google Pixel 2

- Android 11
- rooted with Magisk

ADB Local Backup Evaluation

- ADB’s full backup functionality
- app downgrading for various apps

iOS Evaluation

Apple iPhone 8

- iOS 14.6
- checkra1n jailbreak

iOS Local Backup Evaluation

- created with libimobiledevice
- encrypted and unencrypted backups

Android Local Backup Results

Android full backup and app downgrading evaluation for various apps

	⊘ **File Count**			
	Pre	*Backup*	⊘ N_{both}	⊘ $\boldsymbol{V_{ch}}$
Full Backup	**10853**	**1365**	1365	0
AD Telegram	**374**	**157**	157	0

1: Average result of **20 full backup** and **Telegram downgrading** runs.

iOS Local Backup Results

iOS unencrypted and encrypted local backup evaluation

⌀ **File Count**				
Pre	*Backup*	⌀ N_{both}	⌀ $\boldsymbol{P_{mback}}$	⌀ $\boldsymbol{P_{mpre}}$
39401	**715**	715	1	84

2: Average result of **20 encrypted** evaluation runs.

iOS Local Backup Results

iOS unencrypted and encrypted local backup evaluation

⌀ **File Count**				
Pre	*Backup*	⌀ N_{both}	⌀ $\boldsymbol{P_{mback}}$	⌀ $\boldsymbol{P_{mpre}}$
39401	**715**	715	1	84

2: Average result of **20 encrypted** evaluation runs.

$\boldsymbol{P_{mpre}}$: merging of sqlite **WAL** data (only to the backup file copies)

Conclusion

The evidence is invalid!

No, it is not!
The evidence is invalid!

Conclusion and Conributions

- The practical execution provides a **better understanding** of the **implications** of local backups for forensics.

  ⇒ observed changes have to be considered

- Our evaluation methodology can be **easily replicated** under different conditions.

  ⇒ must be redone under different conditions

Conclusion and Conributions

- The practical execution provides a **better understanding** of the **implications** of local backups for forensics.

  ⇒ observed changes have to be considered

- Our evaluation methodology can be **easily replicated** under different conditions.

  ⇒ must be redone under different conditions

Thank you for your attention!

Any questions or comments?

Image Attributions

- https://app.leonardo.ai/
- https://www.flaticon.com/ - Freepik
- https://www.pexels.com/ - Ron Lach