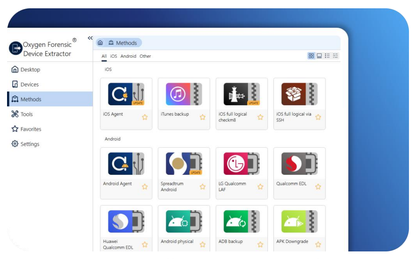
Friedrich-Alexander-Universität
Erlangen-Nürnberg

YAFED - Yet Another (Mobile) Forensic Extraction Device

Julian Geus

Do We Need Another Acquisition Framework?

Source: https://cellebrite.com/
Accessed: 31.01.25



Source: https://www.oxygenforensics.com/
Accessed: 31.01.25

Source: https://github.com/AvillaDaniel/AvillaForensics
Accessed: 31.01.25

...

Source: https://www.msab.com/
Accessed: 31.01.25

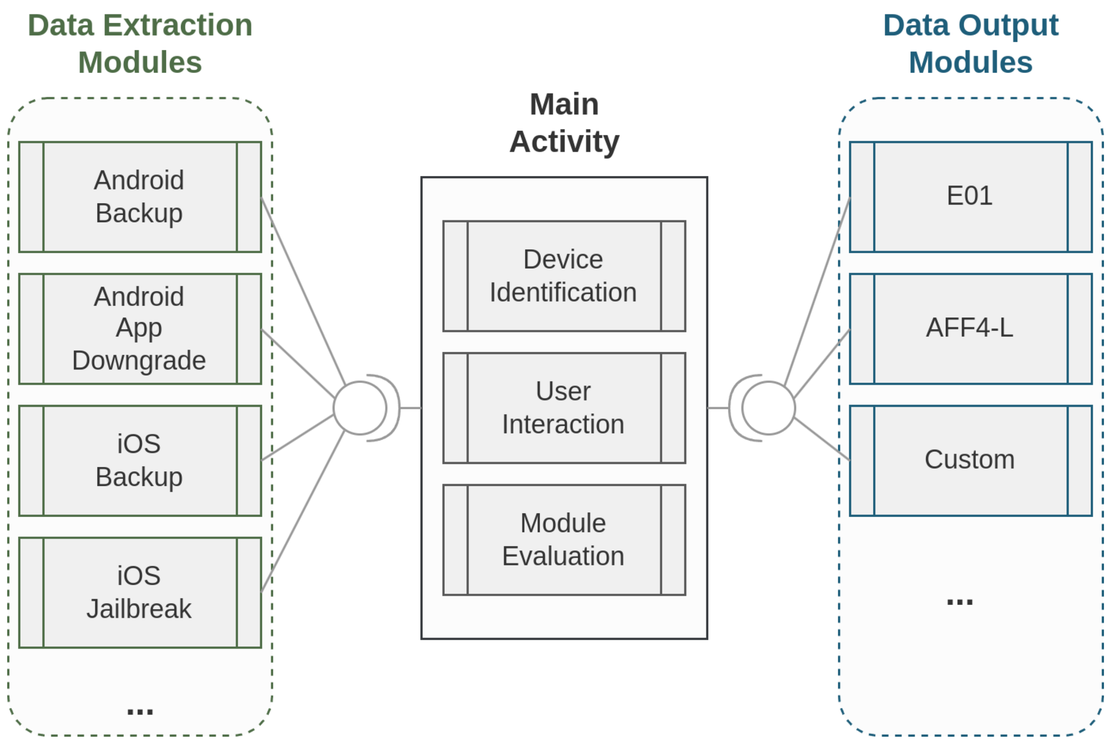
Main Goals

- **Extendibility**: We strive to build a framework, that can be arbitrarily extended by further data acquisition and output modules and thus does not only capture the current trend of data acquisition but can also easily be tailored to future challenges.
- **Usability**: To compete with the current landscape of black-box tools from forensic providers, a self-explanatory user-interface as well as support for advanced scripting features will be provided.
- **Verifiability**: Data provenance and integrity are two major goals in digital forensics. Those will be tackled by:
  → **publicly available source code** for full transparency and an **evaluation feature** to ensure the data integrity of the modules

Framework Overview

Data Extraction Modules
The extraction is executed by numerous modules. Each module targets a specified subset of mobile devices.

- Predefined interface (supported devices, preconditions)
- Easily extendable with the latest acquisition techniques
- Evaluation possible (data integrity and repeatability)



Data Output Modules
The user can choose or implement their preferred output format.

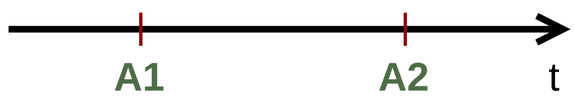
Main Activity
Guides through the extraction process.

- Gathers device information
- Scripting interface
- Displays applicable modules
- Logs all events
- Outputs the data, including metadata

Evaluation of Acquisition Procedures

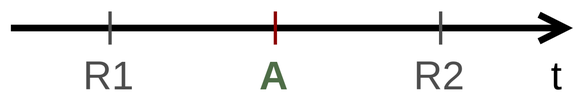
How to ensure the acquisition modules work correctly and do not alter data?
→ Implement an evaluation mode!

Verify the **Repeatability** of any acquisition module



We acquire two datasets *A1* and *A2* with the same acquisition module and compare their contents.

Verify the **Integrity** and **Correctness** of any acquisition module



We acquire two reference data sets *R1* and *R2*, before and after the actual acquisition *A*. For data correctness we check if *A* matches *R1* and for data integrity we check if *R2* changed compared to *R1*.

Acknowledgements

This is a joint project together with: Felix Freiling, Birgit Dohr-Recktenwald and Jenny Ottmann

Feedback and Collaboration

Please connect with us (julian.geus@fau.de) to:

- give feedback on our general idea,
- propose further improvements/modules.