Selective Imaging of File System Data on Live Systems

By:
Fabian Faust, Aurélien Thierry, Tilo Müller and Felix Freiling

From the proceedings of
The Digital Forensic Research Conference
DFRWS EU 2021
March 29 - April 1, 2021

Selective Imaging of File System Data on Live Systems

Extended abstract

Authors: Fabian Faust, Aurélien Thierry, Tilo Müller, Felix Freiling

DFRWS 2021 VIRTUAL EUROPE

Selective imaging on live systems

- Forensic imaging that only includes selected data objects
- Performed live using system that contains evidence
- Useful in situations where 1:1 imaging isn’t feasible such as when system needs to remain fully operational or time is especially critical

What is the problem?

- Not well defined and understood yet, most research focused on post-mortem selective imaging
- Live environment can be unreliable, manipulated and include malicious software
- How to perform reliably in challenging live environment?

→ Development of a modular framework for live selective imaging with focus on forensic soundness

DFRWS 2021 VIRTUAL EUROPE

Framework functionality and design

- Live selective imaging functionality
- File system level
- Windows operating system
- Simple to modify and expand
- Open source

Forensic soundness

Defining concrete requirements for maximizing forensic soundness on live systems:

- Minimize source corruption
- Ensure evidence data authenticity and integrity
- Provide extensive documentation
- Ensure digital reliability and security
- Ensure physical reliability and security

SIT – (Live) Selective Imaging Tool

- Based on DFIR ORC framework for forensic data acquisition on live systems
- Creation of a single, pre-configured, portable binary
- Execution from an external flash drive using console
- Usage of AFF4 format for resulting image
- SIT is available on GitLab

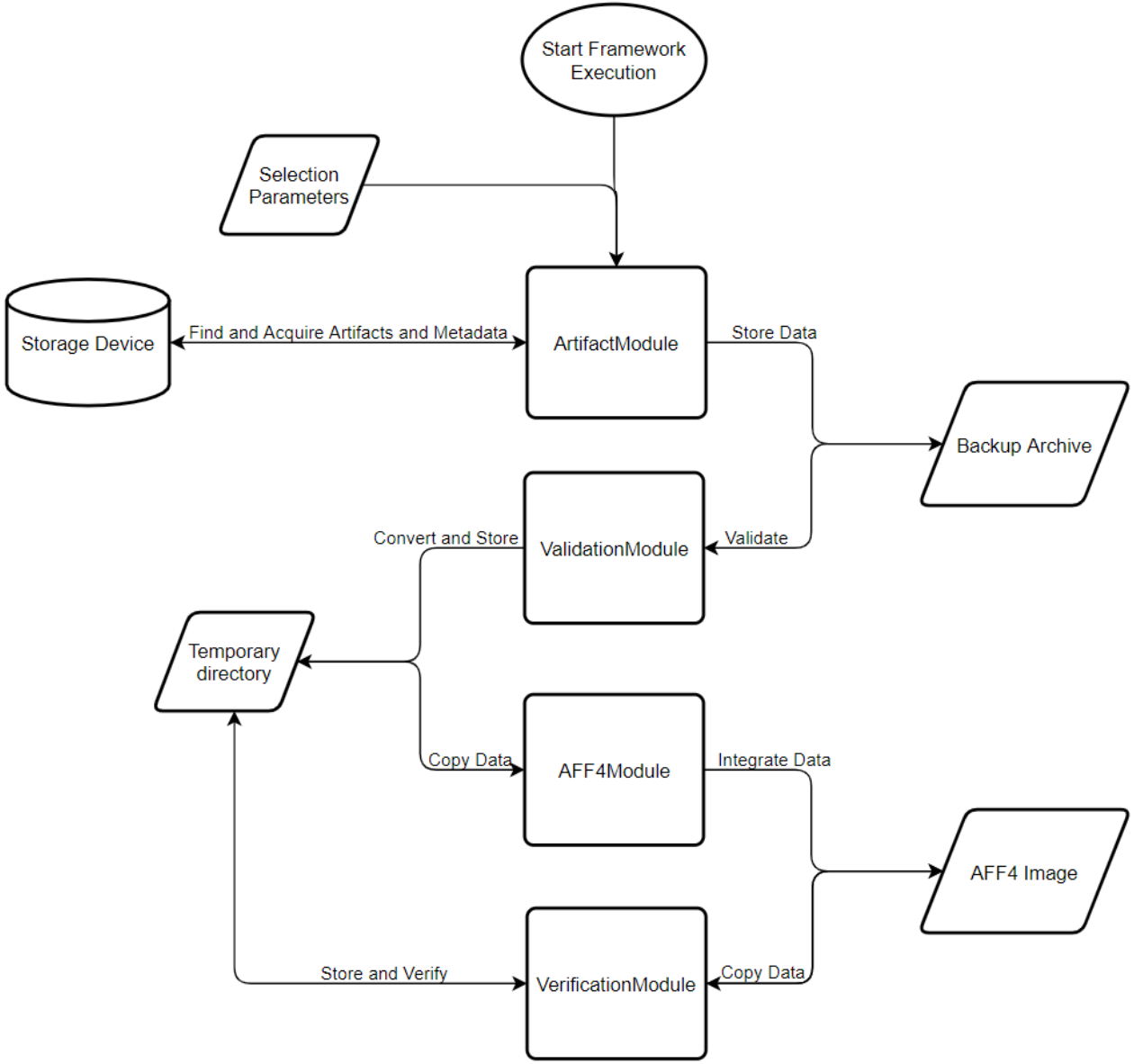
Forensic soundness measures

- **Minimize source corruption**: Execution from external flash drive using custom temporary directory, file access using MFT parser by DFIR ORC
- **Ensure evidence data authenticity and integrity**: Extensive verification for all acquired data objects
- **Provide extensive documentation**: Extensive logging and feedback during execution

DFRWS 2021
VIRTUAL EUROPE

Forensic soundness measures

- **Ensure digital reliability and security**: Validation step to detect unexpected or obviously manipulated results, reliable error handling
- **Ensure physical reliability and security**: Should be handled separately from software implementation



SIT execution

- Four modules, executed sequentially
- Working with output of previous module
- Each module can be disabled, restarted or stopped

Discussion

- **Strengths**: Portable, customizable, extensive steps to check authenticity and integrity, minimal source corruption.
- **Weaknesses**: Malware manipulation still possible, configuration on separate system, image not encrypted.
- **Forensic soundness**: High level of forensic soundness for live system environment but not perfect

Questions?

DFRWS 2021
VIRTUAL EUROPE

Thanks for your attention!

DFRWS 2021
VIRTUAL EUROPE