AMSL
Advanced Multimedia and Security Lab

A Common Scheme for Evaluation of Forensic Software

Mario Hildebrandt, Stefan Kiltz, Jana Dittmann

Research Group on Multimedia and Security

Dept. of Computer Science, Otto-von-Guericke University

PO Box 4120, 39016 Magdeburg, Germany

Email: {hildebrandt, kiltz, dittmann}@iti.cs.uni-magdeburg.de

The work in this paper has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Programme under Contract No. FKZ: 13N10818.

AMSL
Advanced Multimedia and Security Lab

Outline

- Motivation
- State of the Art
- Selected threats for forensic software
- Common evaluation scheme for forensic software (COSEFOS)
- Results of the evaluation with COSEFOS
- Derived framework for the development of forensic software (libopenforensic)
- Conclusions

AMSL
Advanced Multimedia and Security Lab

Motivation

- Software is widely used in IT-forensics and traditional forensic disciplines (e.g. Dactyloscopy) gradually convert to software-based solutions (digitised forensics), too
- Technical and legal aspects should be assessed
- No common evaluation scheme for (digital) forensic software exists, yet
- Goal: create a common evaluation scheme to alleviate the selection of an approriate tool and the decision of the judge assessing the Daubert criteria

AMSL
Advanced Multimedia and Security Lab

State of the Art

- NIST Forensic Software Testing Support Tools [1] for the evaluation of forensic duplication tools
- Validation and Verification of safety relevant software using the V-Model from IEC61508 [2]
- Validation and Verification of string searches [3]
- Validation and validation guidelines from the Scientific Working Group on Digital Evidence [4]
- Common criteria for information technology security evaluation [5]

[1] National Institute of Standards and Technology, FS-TST: Forensic Software Testing Support Tools - Requirements, Design Notes and User Manual, 2005.
[2] G. Klotz-Engmann, “Funktionale Sicherheit- Integraler Bestandteil der Betriebssicherheit, Schutzeinrichtungen nach IEC 61508/61511, Funktionale Sicherheit und SIL,” 2007. [Online]. Available: http://www.sdv-ev.de/fileadmin/pdf/Klotz-Engmann.pdf
[3] Y. Guo, J. Slay, and J. Beckett, “Validation and verification of computer forensic software tools - Searching Function,” Digital Forensic Research Workshop, 2009.
[4] Scientific Working Group on Digital Evidence, “SWGDE Recommended Guidelines for Validation Testing Version 1.1,” 2009. [Online]. Available: http://www.swgde.org/documents/current-documents/2009-01-15%20SWGDE%20Recommendations%20for%20Validation%20Testing%20Version%20v1.1.pdf
[5] “Common Criteria for Information Technology Security Evaluation,” 2009, version 3.1, Revision 3, Final. [Online]. Available: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

AMSL
Advanced Multimedia and Security Lab

State of the Art – legal fundamentals

- Federal Rules of Evidence [1]
  - Set of rules for the admission of evidence in court proceedings
  - Rule 901: requirement for authentication or identification of evidence; part b, clause 9: automatic autentication (only in a few other countries)
  - Rule 702: qualification of an expert witness
  - Best Evidence Rules (1001-1008)
- Daubert Challenge [2]
  - Judge has the role of a gatekeeper for scientific evidence
  - Several criteria can be addressed during a Daubert hearing

[1] Federal Evidence Review, “Federal Rules of Evidence 2011,” 2011. [Online]. Available: http://federalevidence.com/downloads/rules.of.evidence.pdf
[2] L. Dixon and B. Gill, Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases Since the Daubert Decision. RAND Institute
for Civil Justice, 2001, ISBN: 0-8330-3088-4.

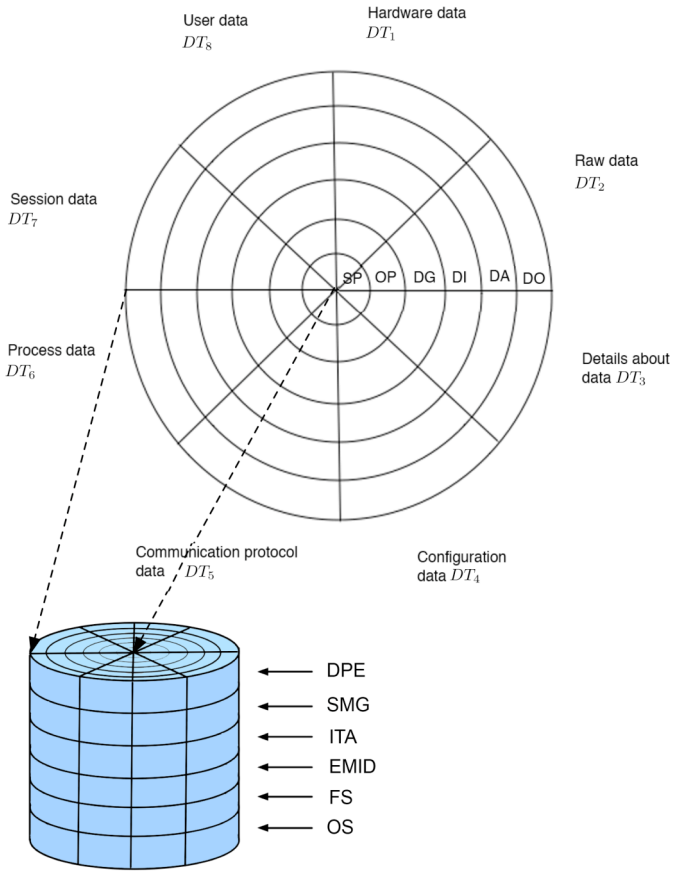
AMSL
Advanced Multimedia and Security Lab

State of the Art – legal fundamentals

- Daubert criteria
  - whether it can be (and has been) tested
  - whether it has been subjected to peer review and publication
  - its known or potential rate of error
  - the existence and maintenance of standards controlling the particular technique's operation
  - whether it is generally accepted in the scientific community.

[1] L. Dixon and B. Gill, Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases Since the Daubert Decision. RAND Institute
for Civil Justice, 2001, ISBN: 0-8330-3088-4.

State of the Art – Model of the forensic process



- Phases:
  - used to model sequence details during a forensic investigation
- Classes of methods:
  - classify forensic capabilities of software, not only dedicated forensic suites gather forensically relevant data
- Forensic datatypes:
  - layered approach similar to ISO/OSI model (not mutual exclusive)
  - used to determine input and output data of forensic tools/methods

AMSL
Advanced Multimedia and Security Lab

Exemplary threats for forensic software

- Possible attacks on forensic software (violating forensic soundness)
  - Anti-forensics [1]
  - Exploits for vulnerabilities of forensic software [2]
- Attacker model for forensic software
- Based on the Incident-/CERT Taxonomy [3]
  - Corruption of data (Alteration and data hiding)
  - Stealing of data (Gathering of confidential data)
  - Corruption of processes (Exploits for forensic software, interruption of the investigation)

[1] S. Garfinkel, “Anti-Forensics: Techniques, Detection and Countermeasures,” 2007.
[2] T. Newsham, C. Palmer, A. Stamos, and J. Burns, “Breaking Forensics Software: Weaknesses in Critical Evidence Collection,” 2007.
[3] J. D. Howard and T. A. Longstaff, “A common language for computer security incidents (sand98-8667),” Sandia National Laboratories, Tech. Rep. ISBN 0-201-63346-9, 1998.

AMSL
Advanced Multimedia and Security Lab

Common evaluation scheme for forensic software (COSEFOS)

- The common evaluation scheme for forensic software is divided into Hard-Criteria and Soft-Criteria
- Hard-Criteria are diveded into:
  - *Must-Criteria*: Criteria that must be fulfilled by the evaluated forensic application
  - *Should-Criteria*: Criteria that should be fulfilled by the forensic application; otherwise they must be provided externally
  - *Can-Criteria*: Criteria that might be fulfilled

AMSL
Advanced Multimedia and Security Lab

Common evaluation scheme for forensic software (COSEFOS)

Hard-Criteria	Soft-Criteria
Must-Criteria	
- Core functionality CF	- General acceptance within the expert community GA - Publication of the method PM - Standards for the usage of the application SU - Intention of the investigation II - Personal familiarity with the application PF
Should-Criteria	
- Logging LF - Protection of the integrity of the gathered data IP - Protection of the authenticity of the gathered data AP - Protection of the confidentiality of the gathered data CP - Access restriction for the gathered data AR - Protection of the integrity of the source data SP	
Can-Criteri a	
- System heterogeneity SH - Minimality of required system rights MR - Open Source O S	

AMSL
Advanced Multimedia and Security Lab

COSEFOS: Formalisation

f=({PP, CM, DT}, {CF, FL, IP, AP, CP, AR, SP, SH, MR, OS}, {GA, PM, SU, II, PF})

- {PP, CM, DT} classification of the application according to the model of the forensic process to group software with similar functionality
- Evaluation using hard-critera and soft-criteria
- Hard-criteria (Must-, Should- and Can-Criteria) {CF, FL, IP, AP, CP, AR, SP, SH, MR, OS}
- Soft-criteria {AE, PM, SU, II, PF}

→ Can be used to evaluate exisiting applications and to support the development of new software

AMSL
Advanced Multimedia and Security Lab

Exemplary evaluation with COSEFOS

Results for dcfldd 1.3.4-1

- Core functionality (CF): When using Linux Kernel <=2.4: Last sector is not acquired if number of sectors is odd; additional sectors around defective sectors might be marked as defect, too; HPA/DCO are not recognised automatically
- Logging (LF): partially: logging of errors and hash values
- Integrity protection (IP) for the gathered data: various hash algorithms
- Authenticity/Confidentiality protection (AP), access restriction: none

AMSL
Advanced Multimedia and Security Lab

Exemplary evaluation with COSEFOS

Results for dcfldd 1.3.4-1 (cont'd)

- Integrity Protection of the source data (SP): partially (dcfldd does not write to the source disk if it is not told to)
- System heterogeneity (SH): various operating systems and platform architectures are supported
- Required system rights (MR): read access to source disk, write access to destination
- Open source software (OS)
- Soft criteria: is generally accepted (GA), method has been published (PM), no particular standards for the usage (SU) exist (only best practices), no intention for the investigation (II) could be determined from dcfldd

AMSL
Advanced Multimedia and Security Lab

Exemplary evaluation with COSEFOS
Results for EnCase Forensic 6.1.0.17

- Core functionality (CF): some particular circumstances cause errors during the data gathering
- Logging (FL): limited process accompanying documentation; report generator for the final documentation; some meta-data: timestamps, case-id, name of the investigator, notes
- Integrity protection for the gathered data (IP): MD5 for the gathered data and CRC-Checksums for each block within the evidence file
- Authenticity protection (AP): none in EnCase Forensic, might be provided by EnCase SAFE Module

AMSL
Advanced Multimedia and Security Lab

Exemplary evaluation with COSEFOS

Results for EnCase Forensic 6.1.0.17 (cont'd)

- Confidentiality protection/access restriction (CP): limited (password in evidence file header, no encryption)
- Integrity protection for the source data (SP): FastBloc SE software write blocker during the investigation
- System heterogeneity (SH): none (Windows only)
- Required system rights (MR): Administrator privileges needed to acquire forensic duplicates from storage media
- Availability of the source code (OS): no, proprietary closed source software
- Soft criteria: EnCase is generally accepted, the Software can be bought and tested (GA), exisiting standards and certifications for the usage of Encase (SU), no particular intention for the investigation is enforced (II)

AMSL
Advanced Multimedia and Security Lab

COSEFOS-derived framework for the development of forensic software

- Libopenforensic: a demonstrator designed to fulfill as much Hard-Criteria of COSEFOS as possible
- The Criteria are used to define requirements for forensic software
- Libopenforensic is intended to enforce a forensic sound proceeding
- Currently relies on the Advanced Forensic Format for storing the gathered data

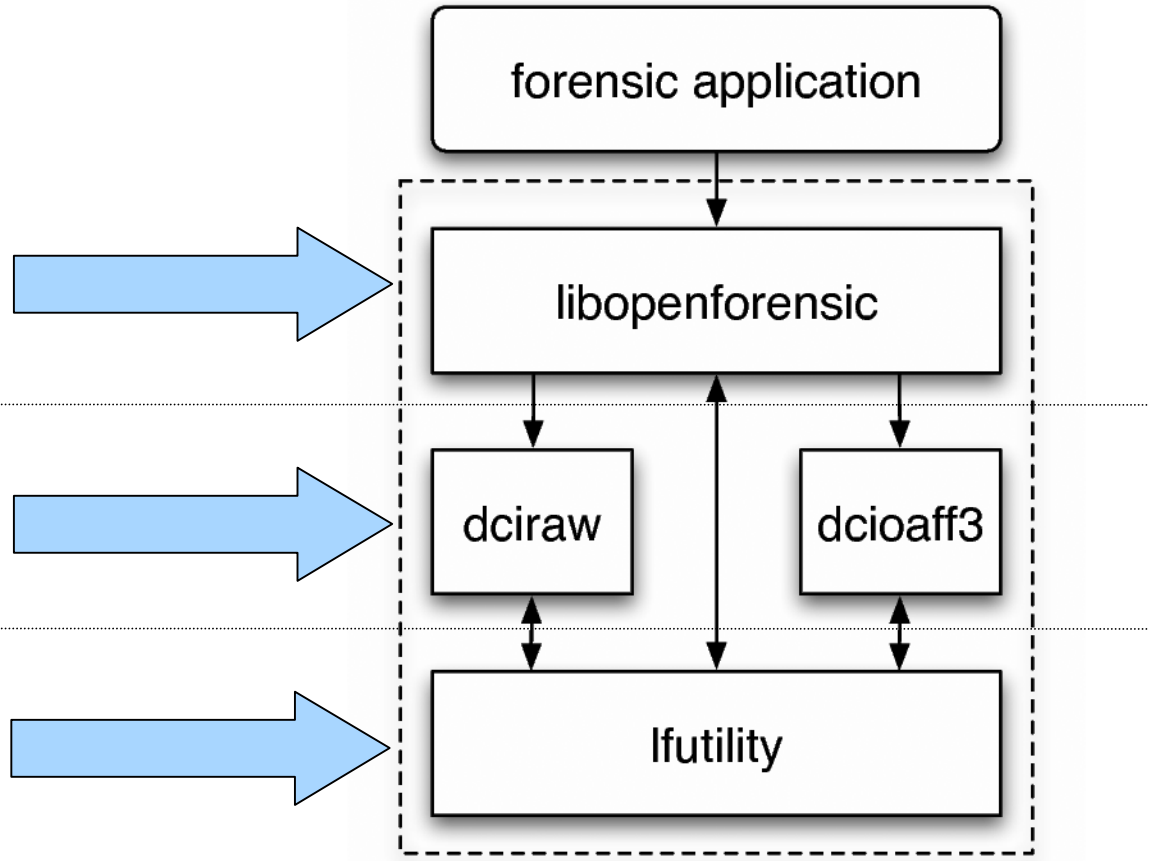
AMSL
Advanced Multimedia and Security Lab

Derived framework for the development of forensic software (libopenforensic)

Interface for the forensic application (abstraction of the data modules)

Data access modules (conventional raw, aff)

Internal service routines (e.g. hash generation and logging for data modules)



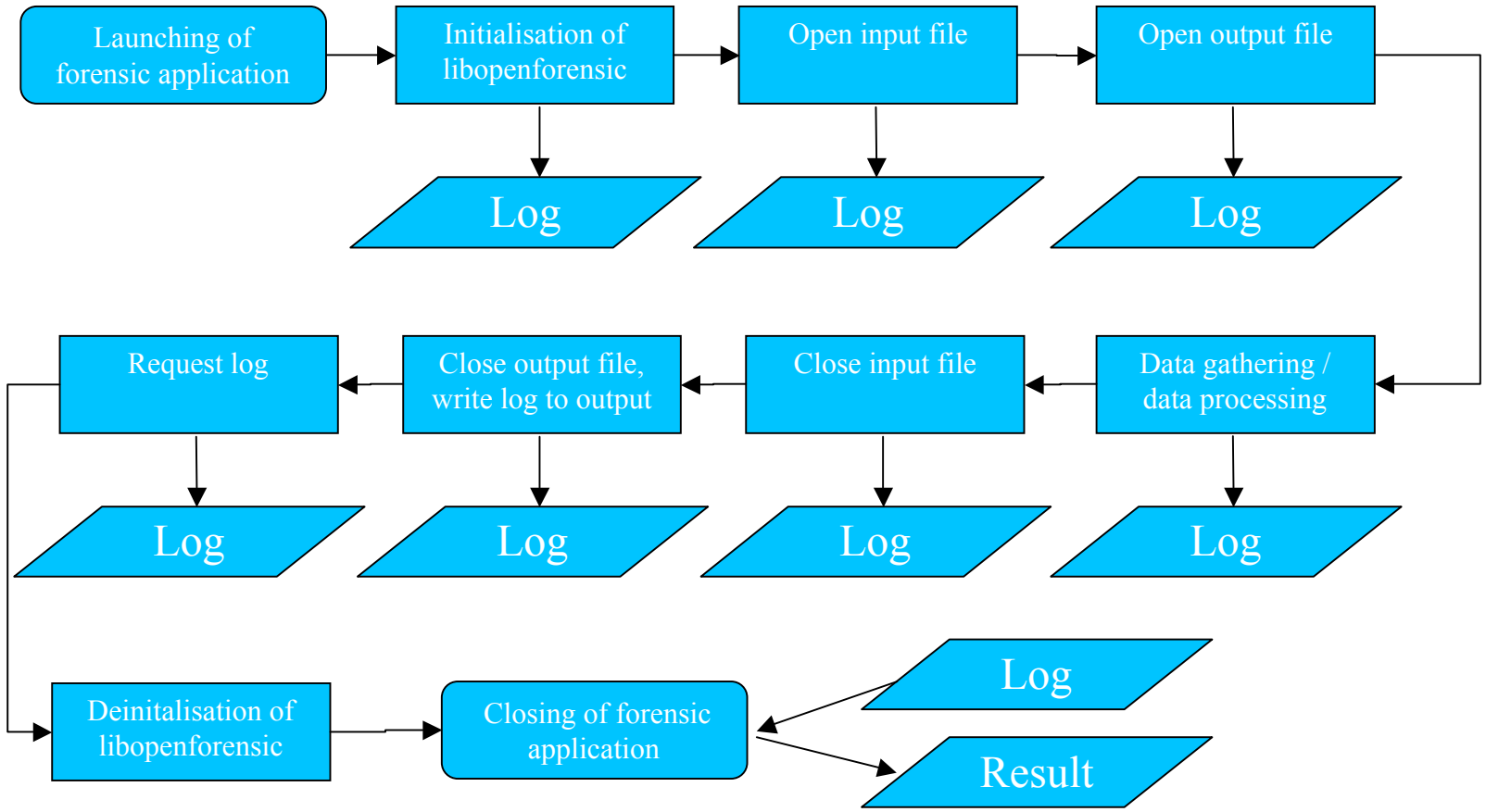
AMSL
Advanced Multimedia and Security Lab

Derived framework for the development of forensic software (libopenforensic)

- Logged data (always with timestamp):
  - initialization: application with full path, commandline with all parameters, system user name and group, libopenforensic version and compile date, aff version, program sha256 hash, hostname with operating system information
  - open input file: filename and path, access rights, owner/group, filesize, access time, creation time, modification time, file hash (sha256 default)
  - open output file: filename and path
  - data processing: amount of copied data (if full file contents: source and destination file)
  - close input file: filename and path
  - close output file: filename and path
  - Deinitialization: Log must be requested first!

AMSL
Advanced Multimedia and Security Lab

Derived framework for the development of forensic software (libopenforensic)



AMSL
Advanced Multimedia and Security Lab

Conclusions

- Introduction of a common evaluation scheme for forensic software (COSEFOS) using legal aspects of U.S. Jurisdiction to show tendencies for other countries
- Several unmet requirements for forensic soundness in exemplarily evaluated tools
- COSEFOS also suitable to enhance the development of forensic software, shown exemplarily on framework libopenforensic
- Future work includes the extension of the formalisation with an evaluation scale for potential use in the benchmarking of forensic software

AMSL
Advanced Multimedia and Security Lab

Thank you very much for your attention!