Unifying Metadata-Based Storage Reconstruction and Carving with LAYR

By:

Janine Schneider (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)), Hans-Peter Deifel (FAU), Stefan Milius (FAU), and Felix Freiling (FAU)

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2020 USA

Virtual -- July 20-24

Unifying Metadata-Based Storage Reconstruction and Carving with LAYR

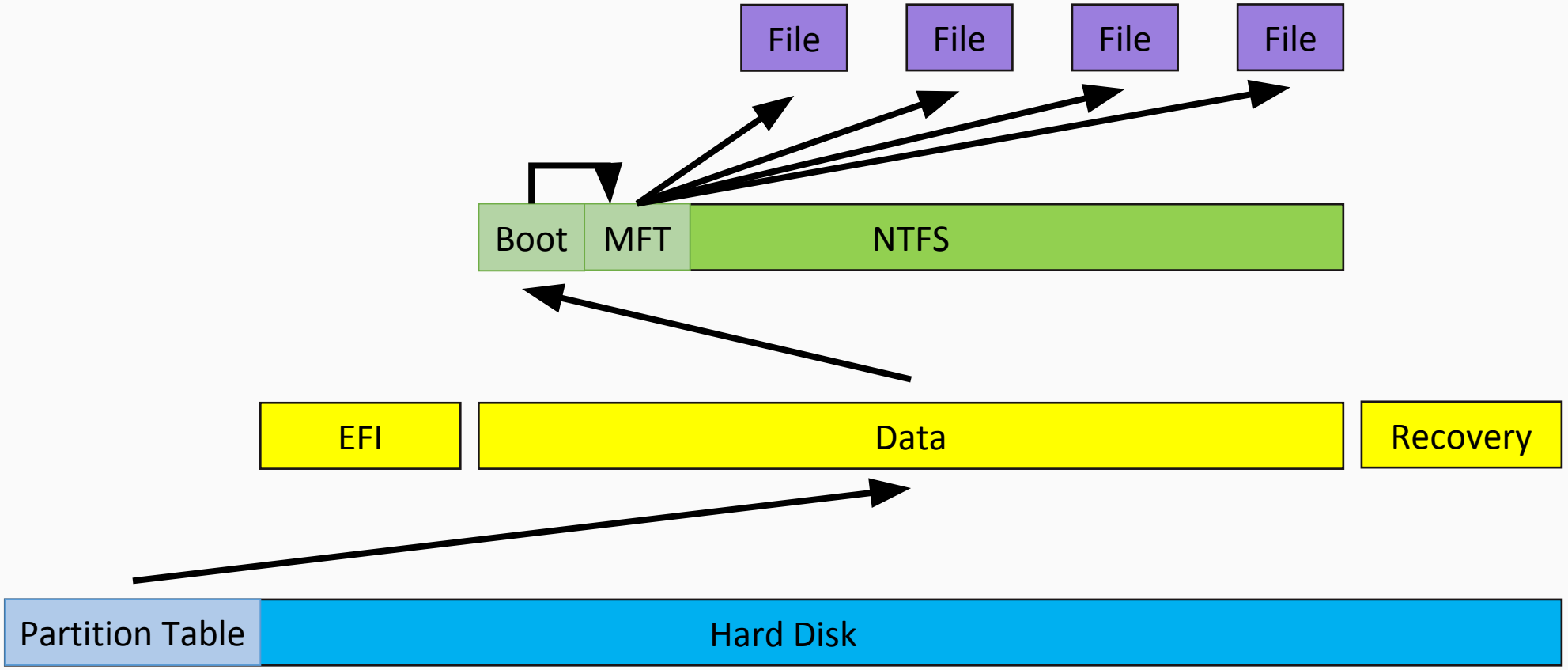
Janine Schneider, Hans-Peter Deifel, Stefan Milius, Felix Freiling

July 21, 2020

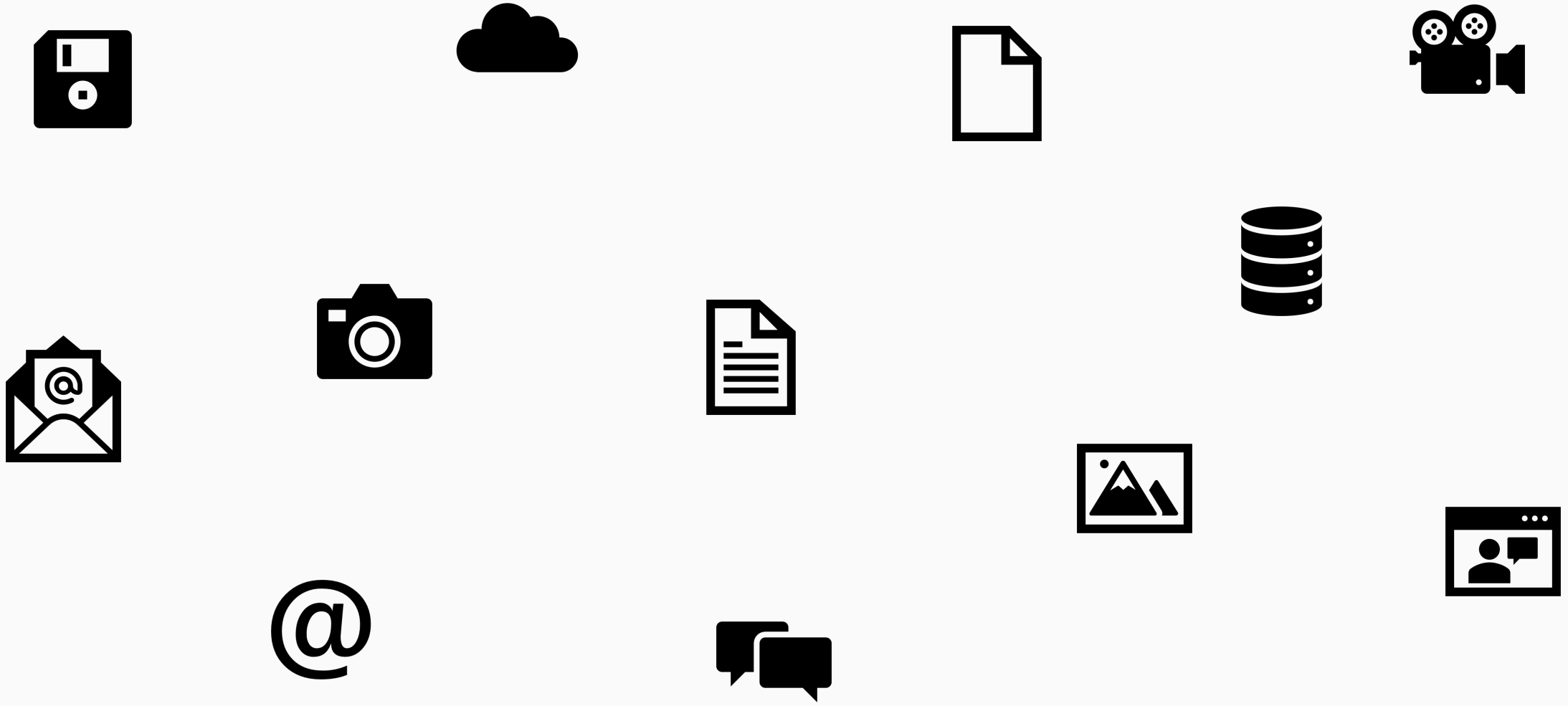
IT Security Infrastructures Lab
Department of Computer Science
Friedrich-Alexander University Erlangen-Nürnberg (FAU)

Digital Evidence

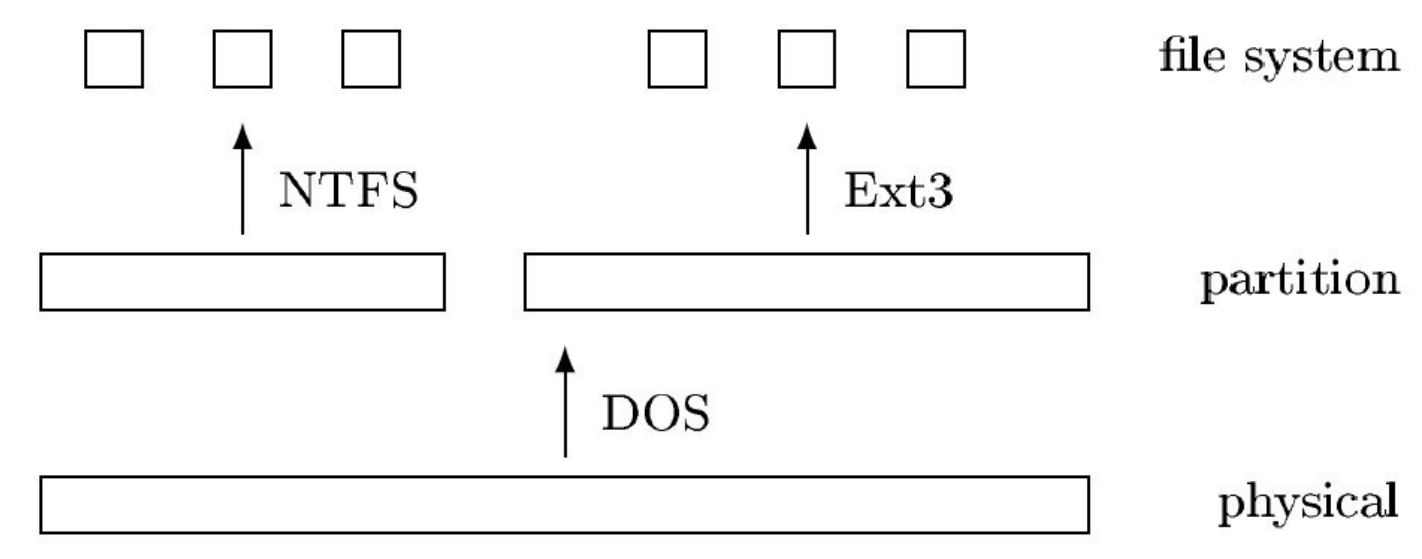
Data reconstruction



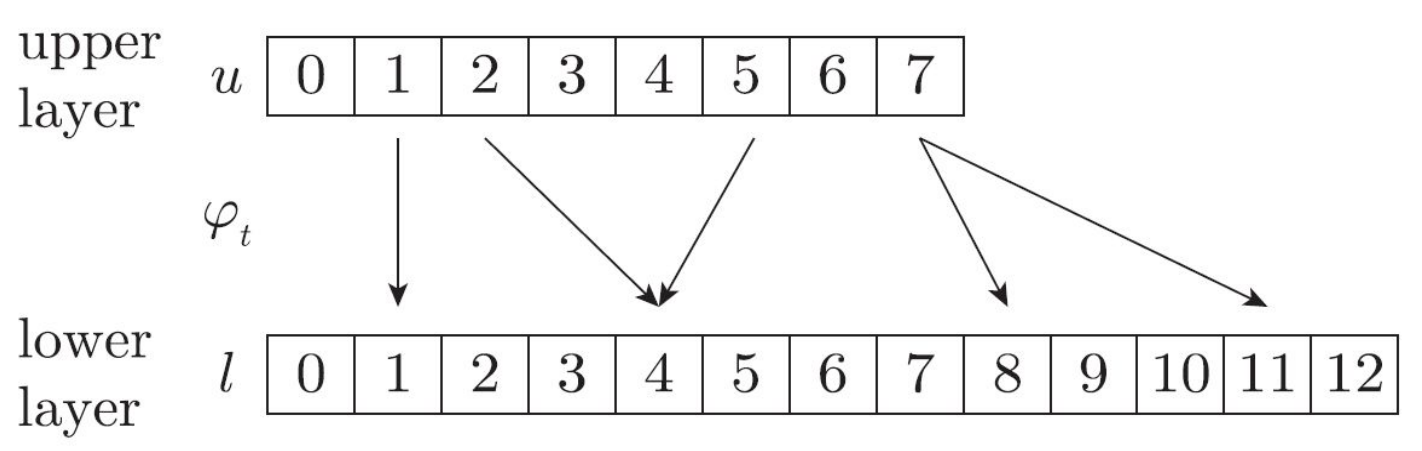
Digital Evidence



Model basis

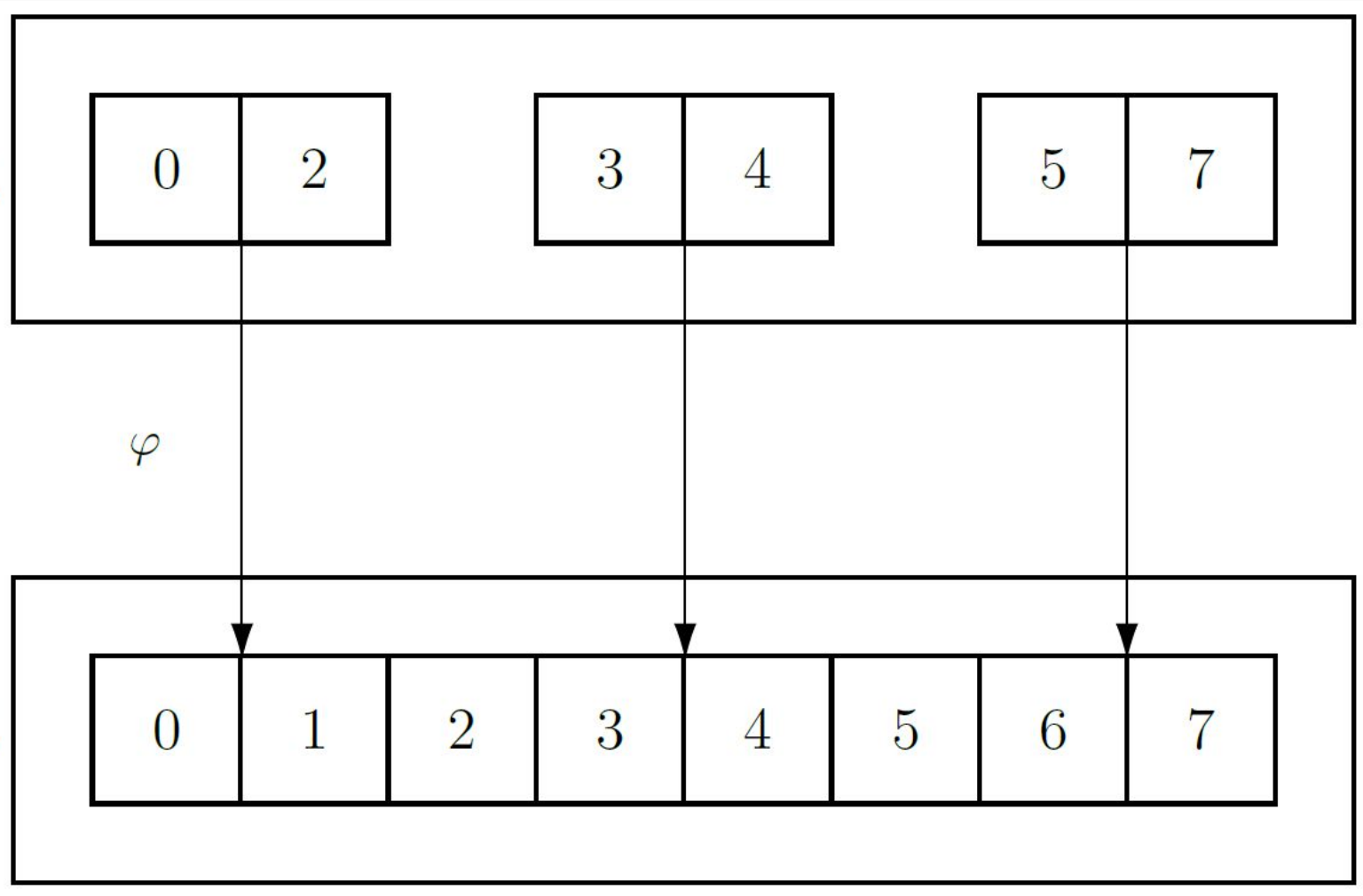


B. Carrier, File System Forensic Analysis

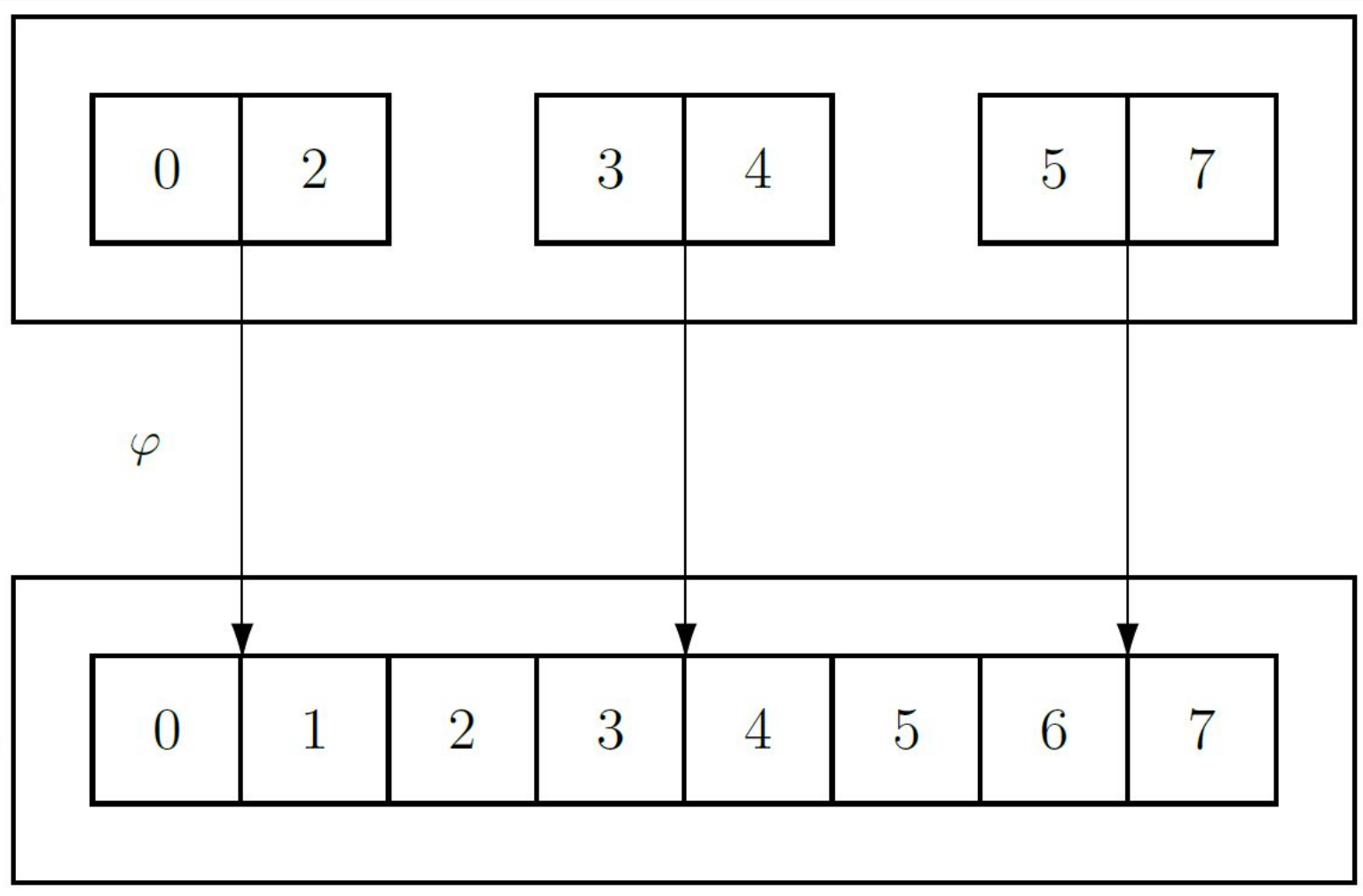


F. Freiling, T. Glanzmann, H. P. Reiser, Characterizing loss of digital evidence due to abstraction layers

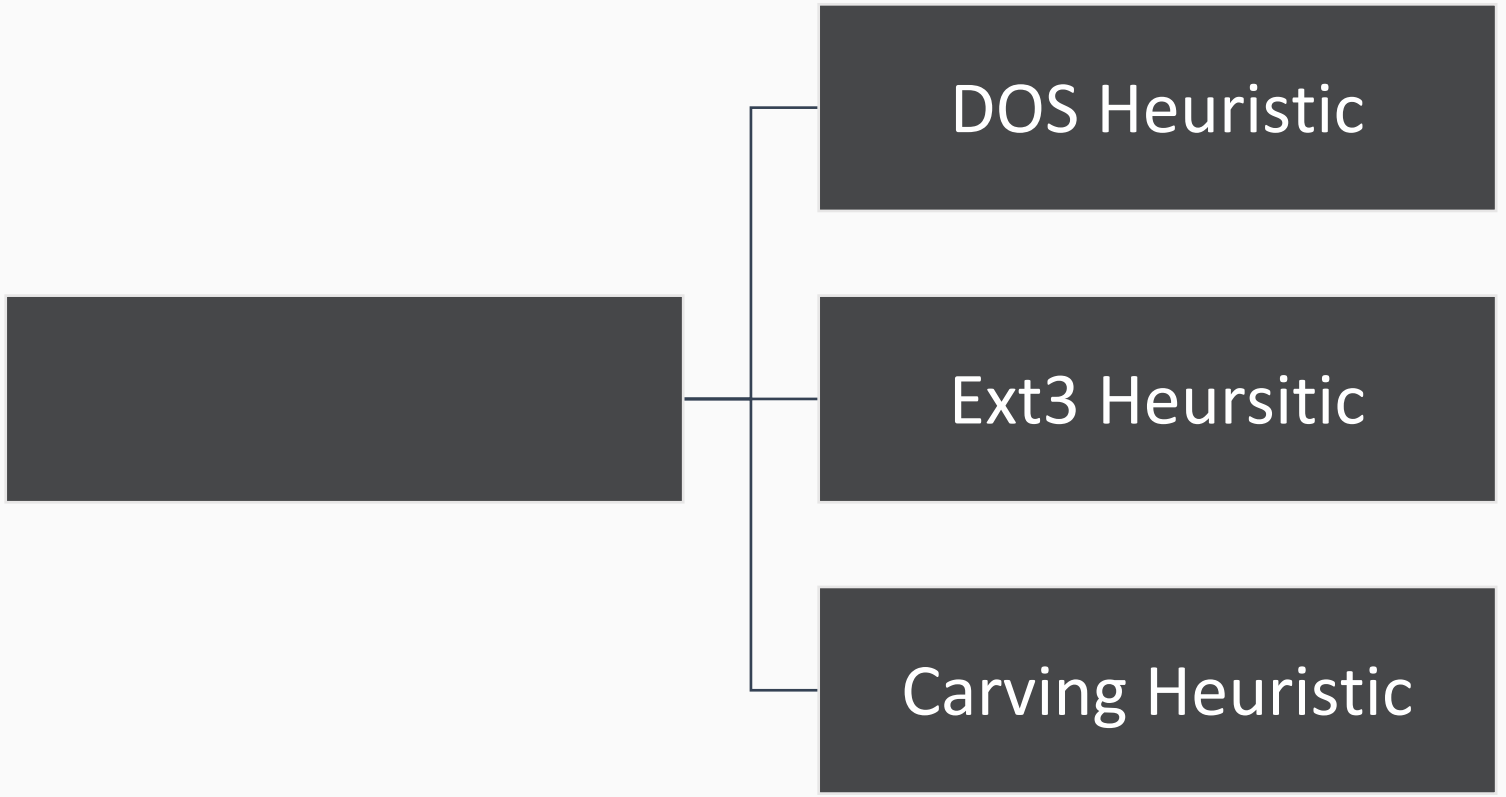
Abstract model

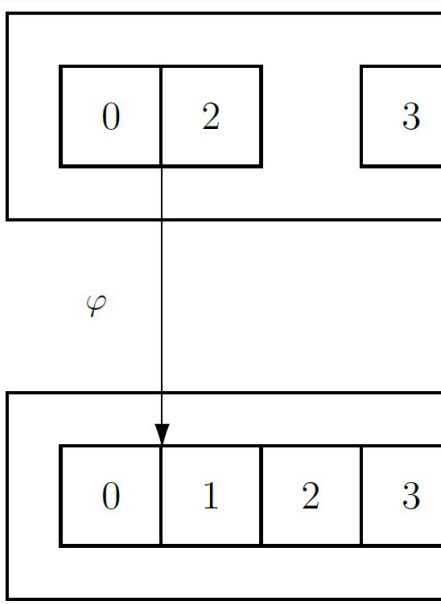


Heuristics



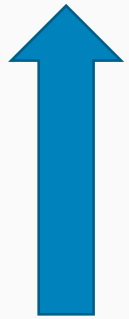
Heuristics





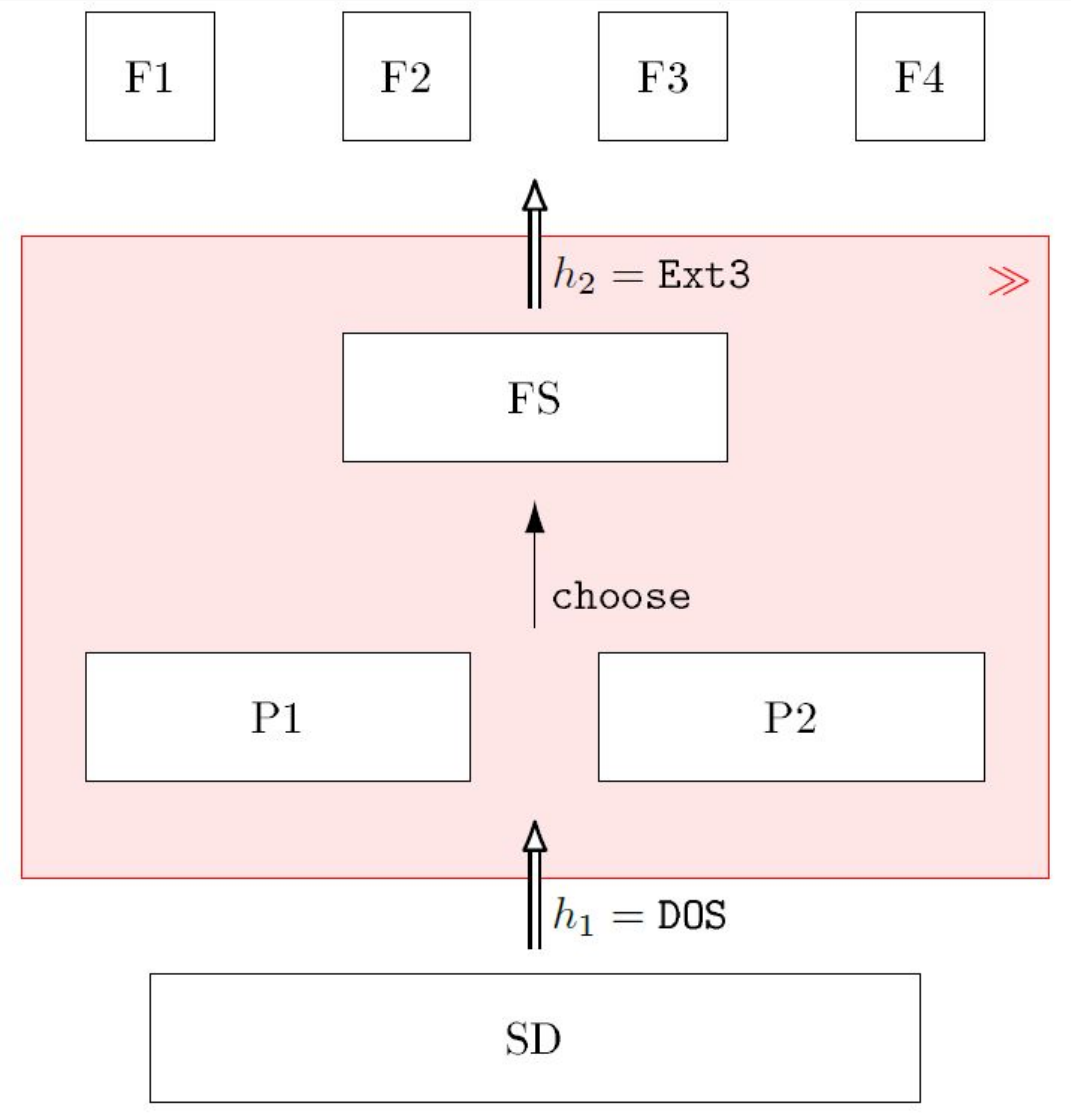
Operators

- Sequential operators execute a heuristic, inspect the result, and then execute further heuristics based on that.

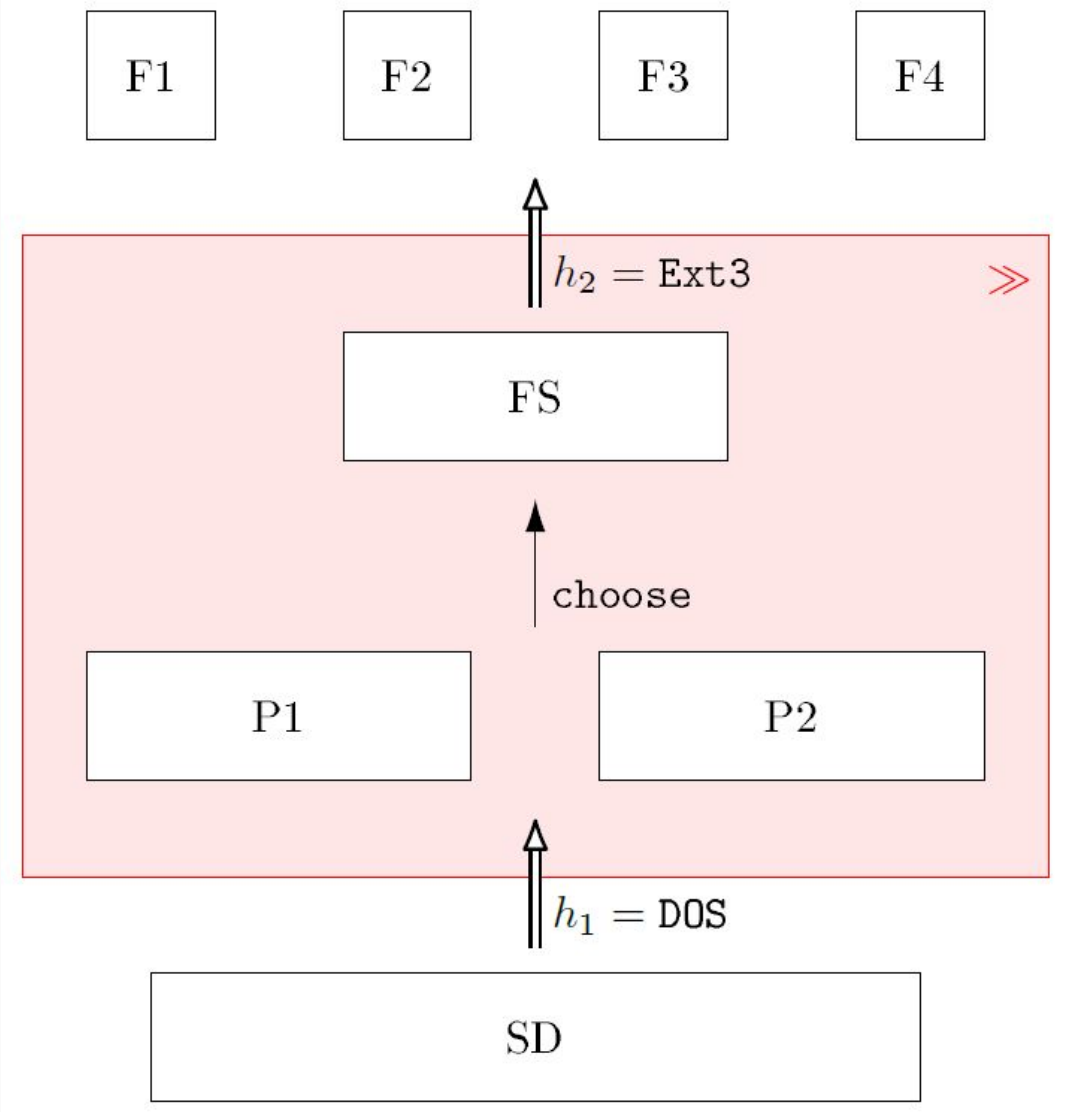


- Parallel operators execute two (or more) heuristics independently from each other and combine the results of both.

Sequential Composition

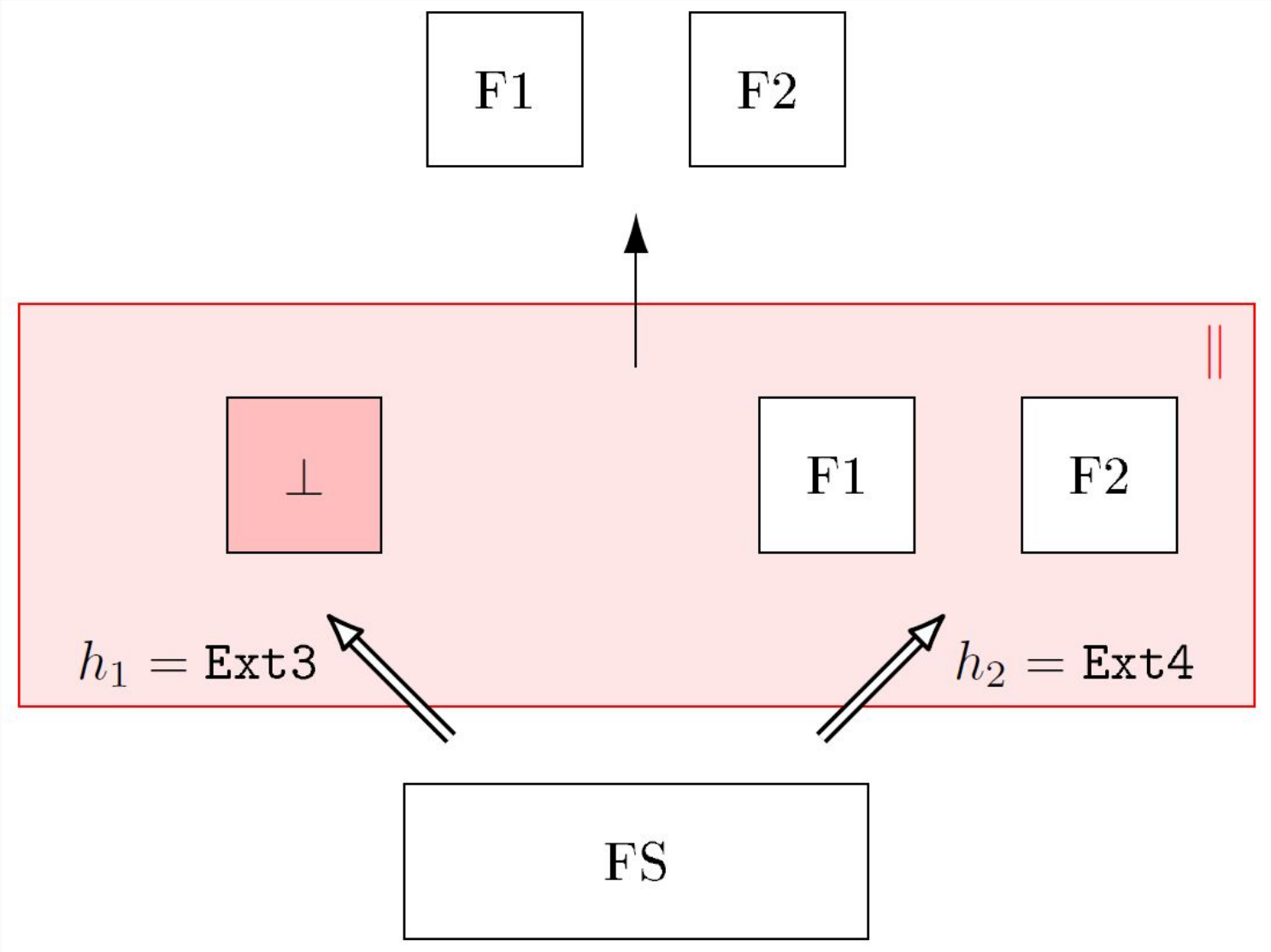


Sequential Composition

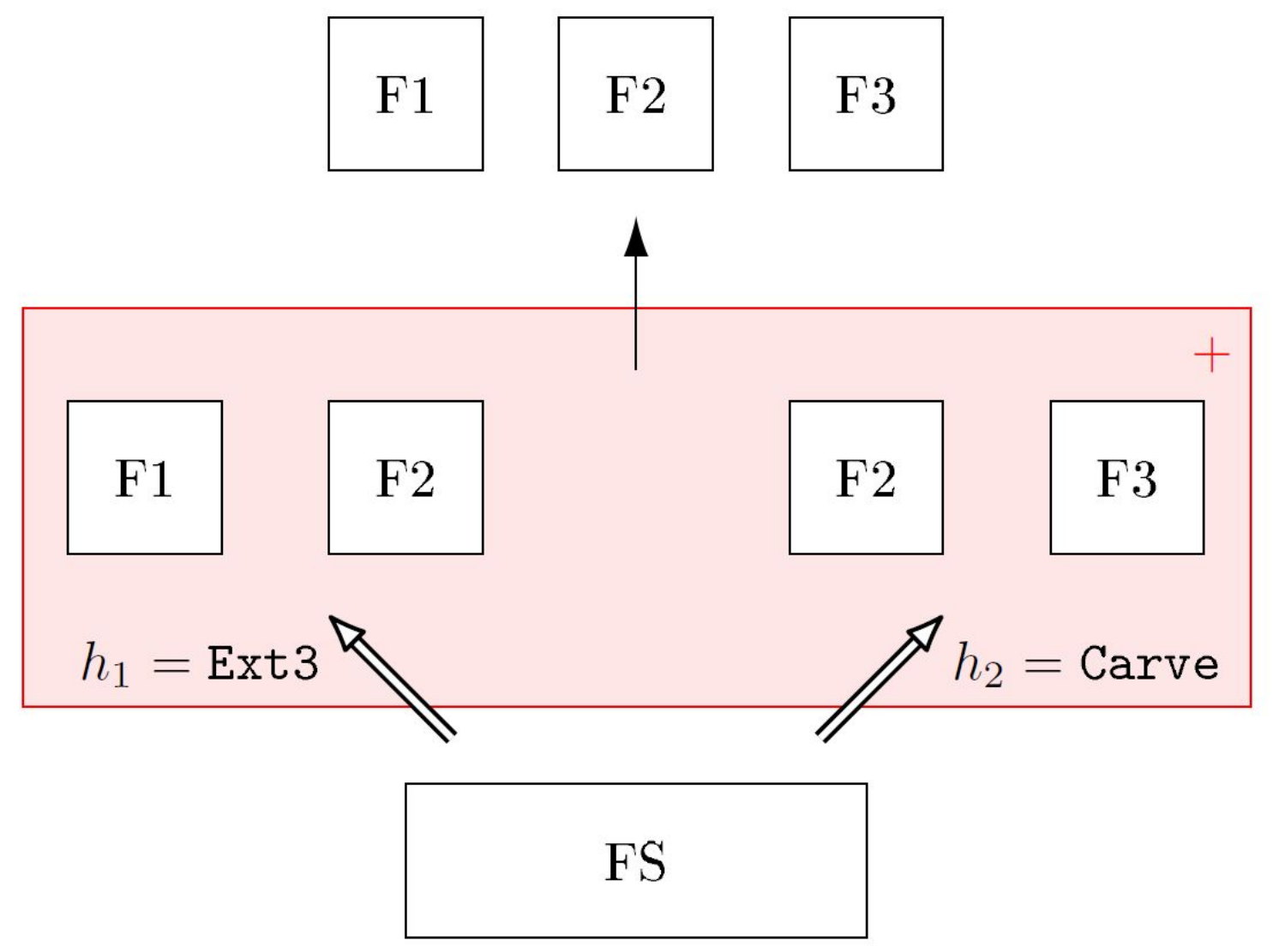


$$h_1 \gg h_2$$

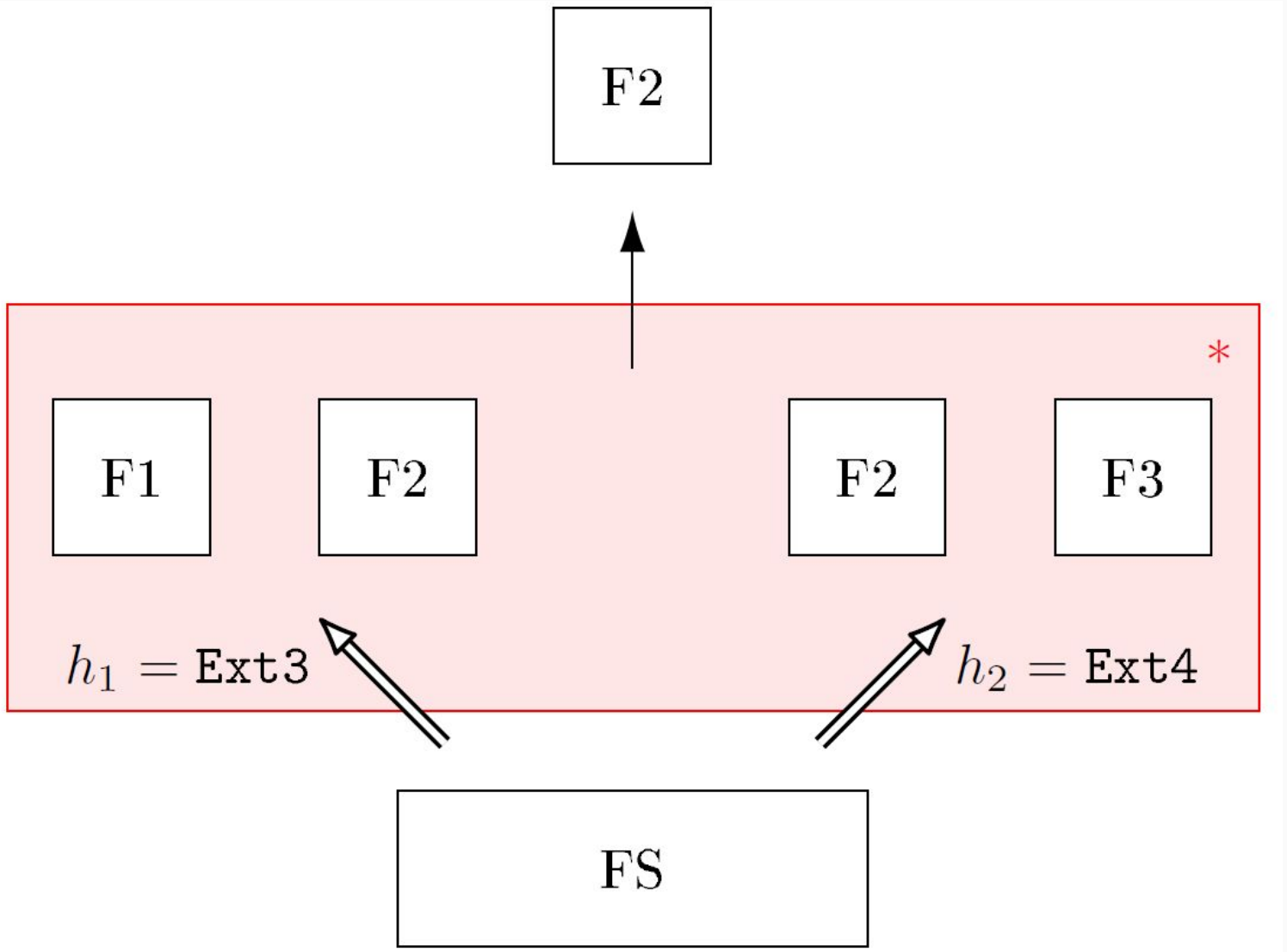
Or



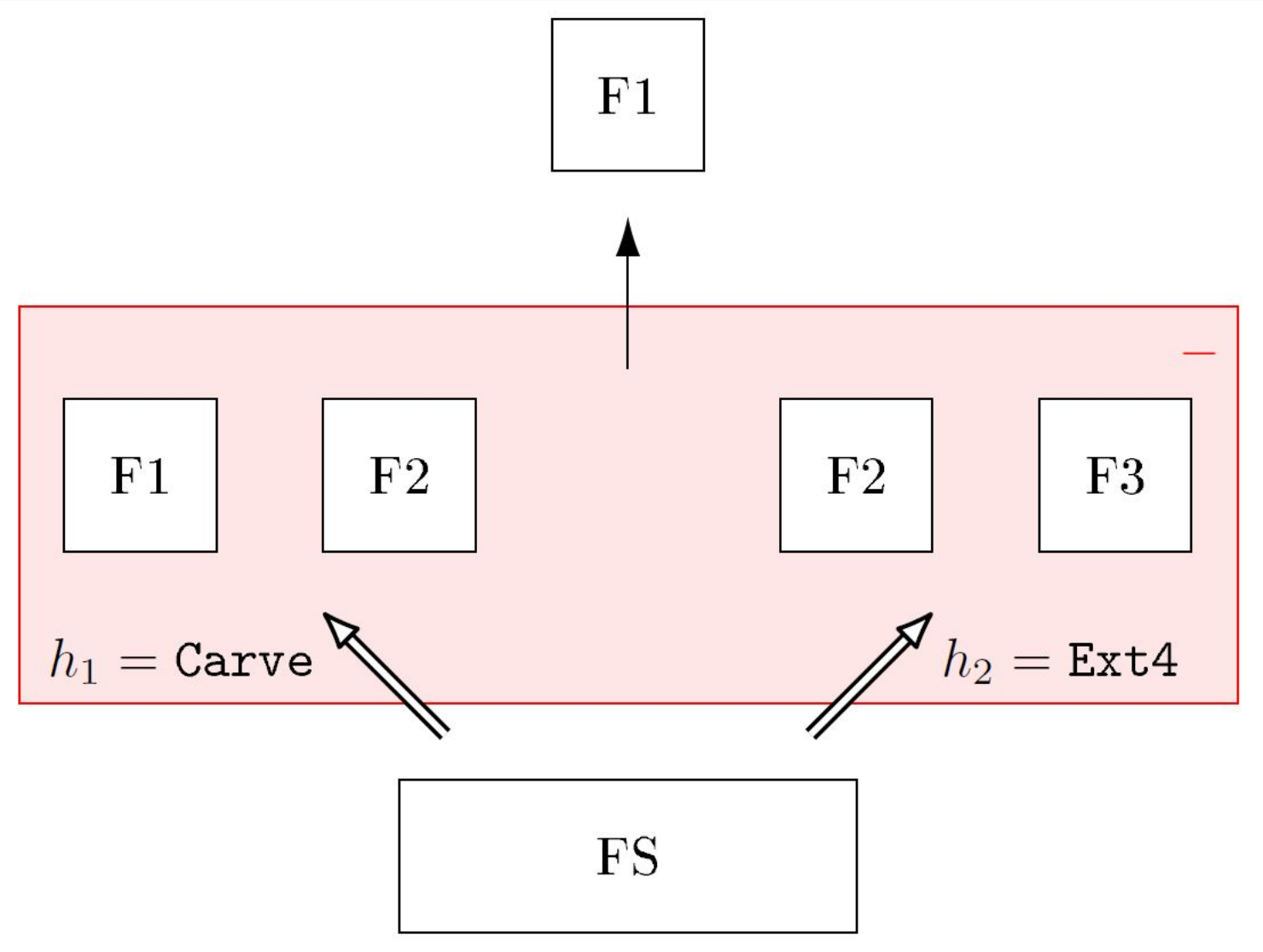
Union



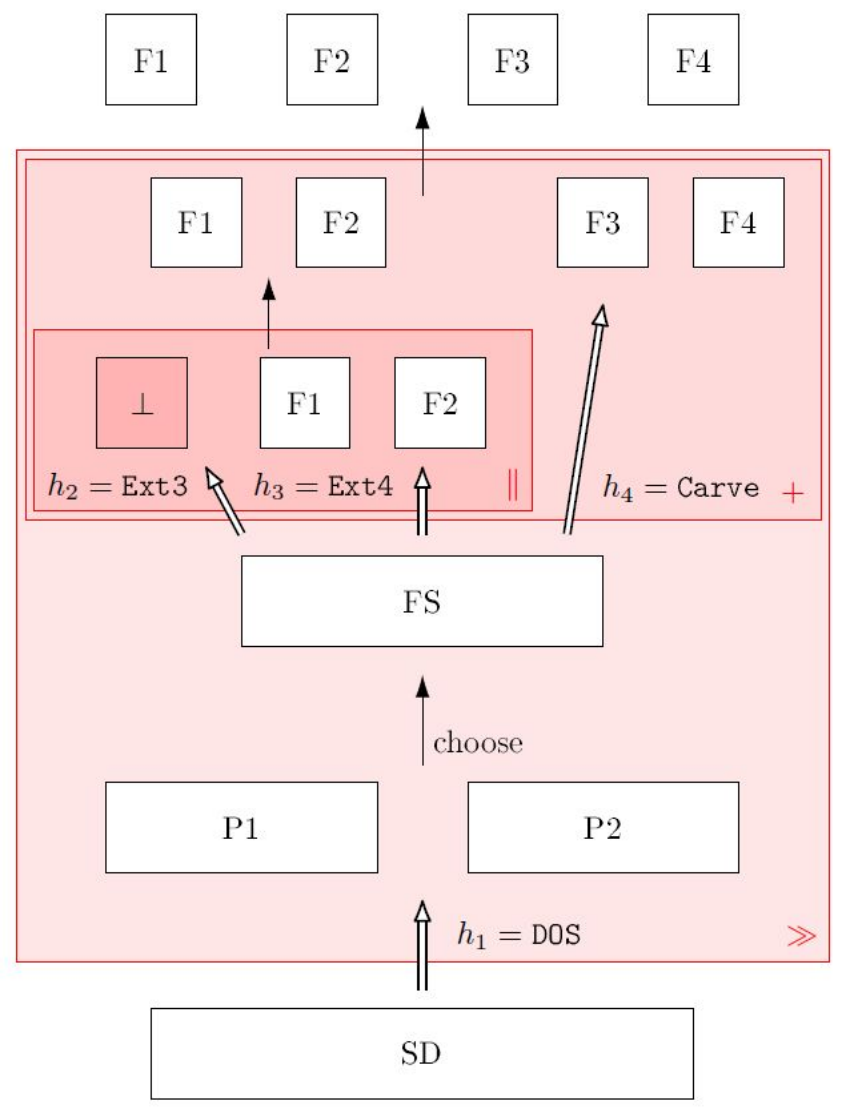
Intersection



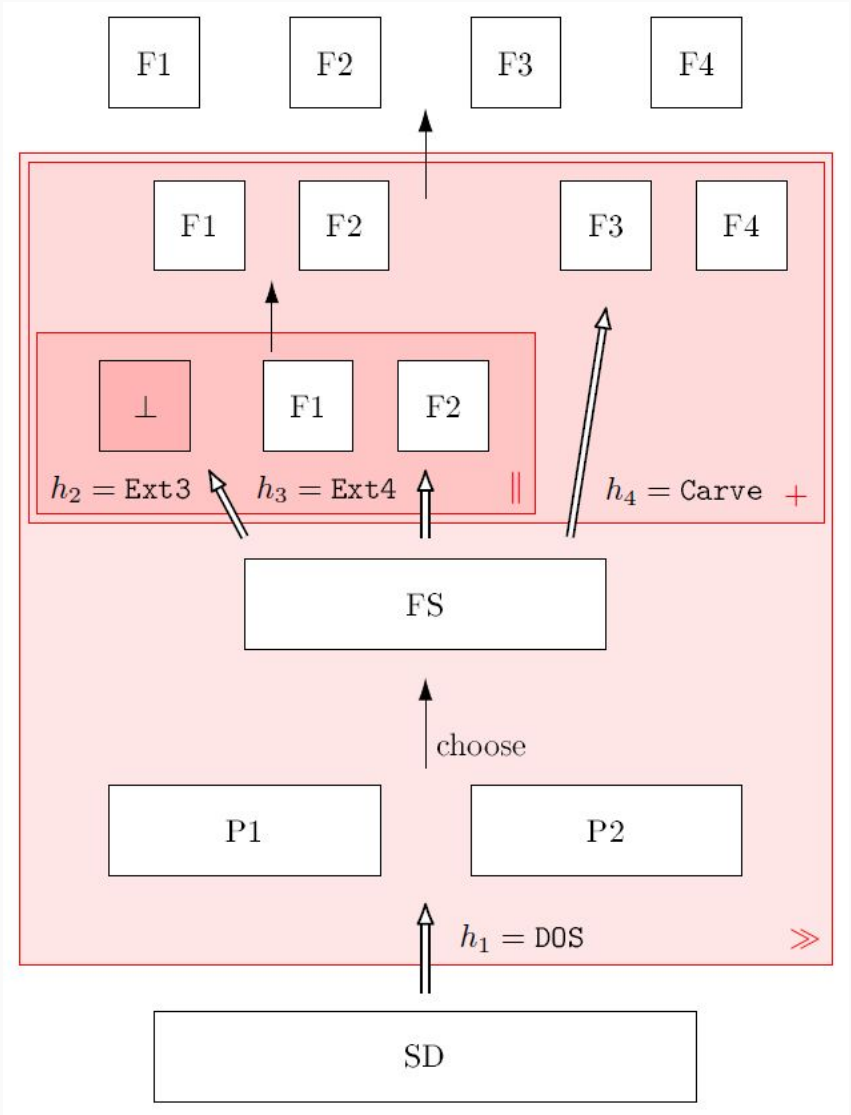
Minus



Operator Nesting



Operator Nesting



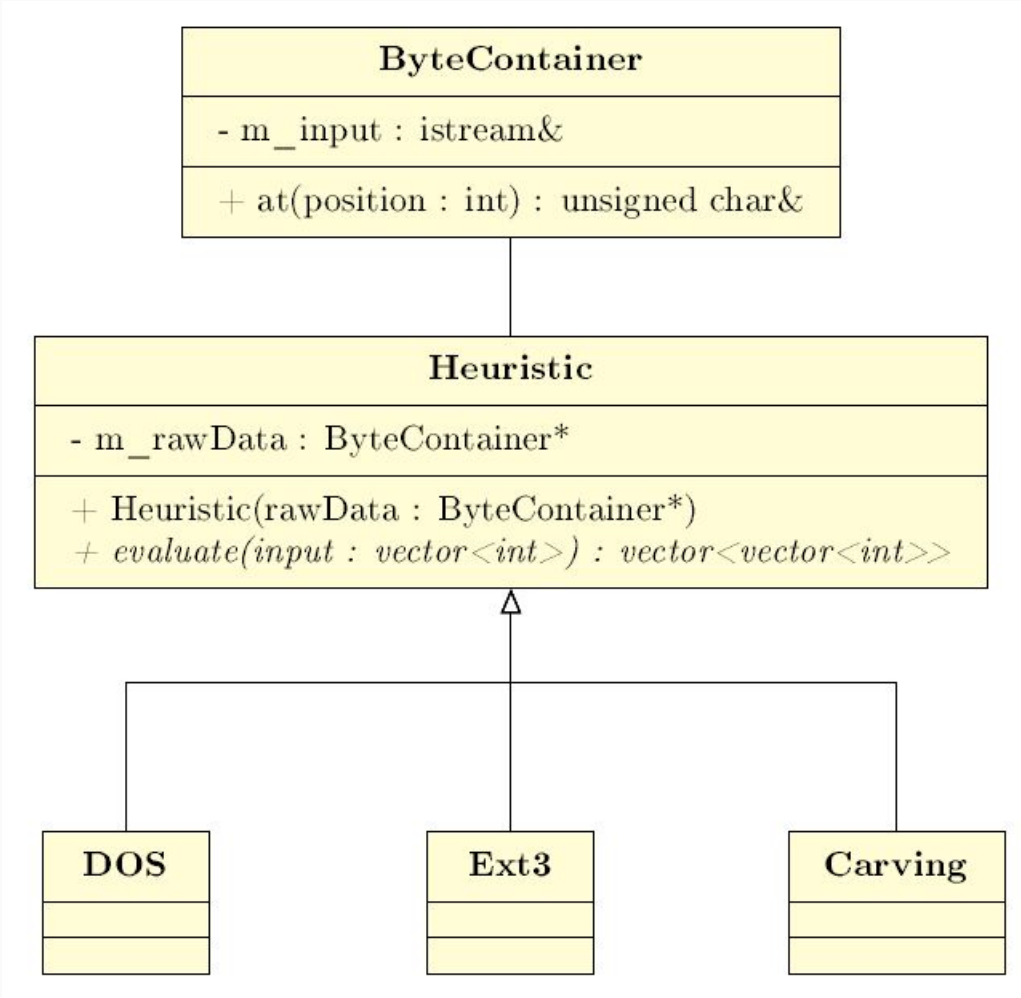
$$DOS \gg ((Ext3 \,||\, Ext4) + Carve)$$

Software Design

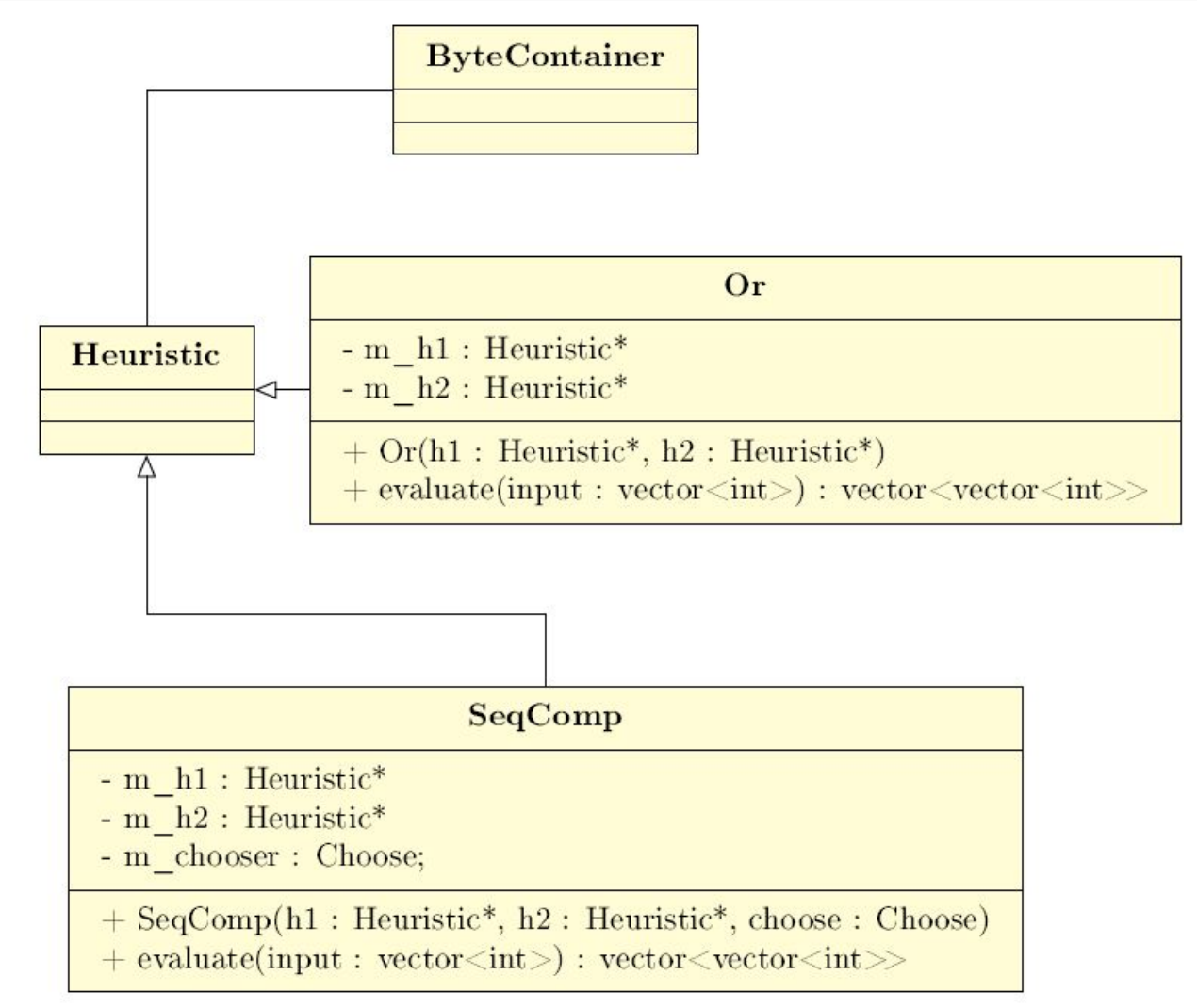
LAYR:

- Forensic reconstruction and analysis tool
- LAYR classes directly derived from formal definitions
- Modular design
- C++

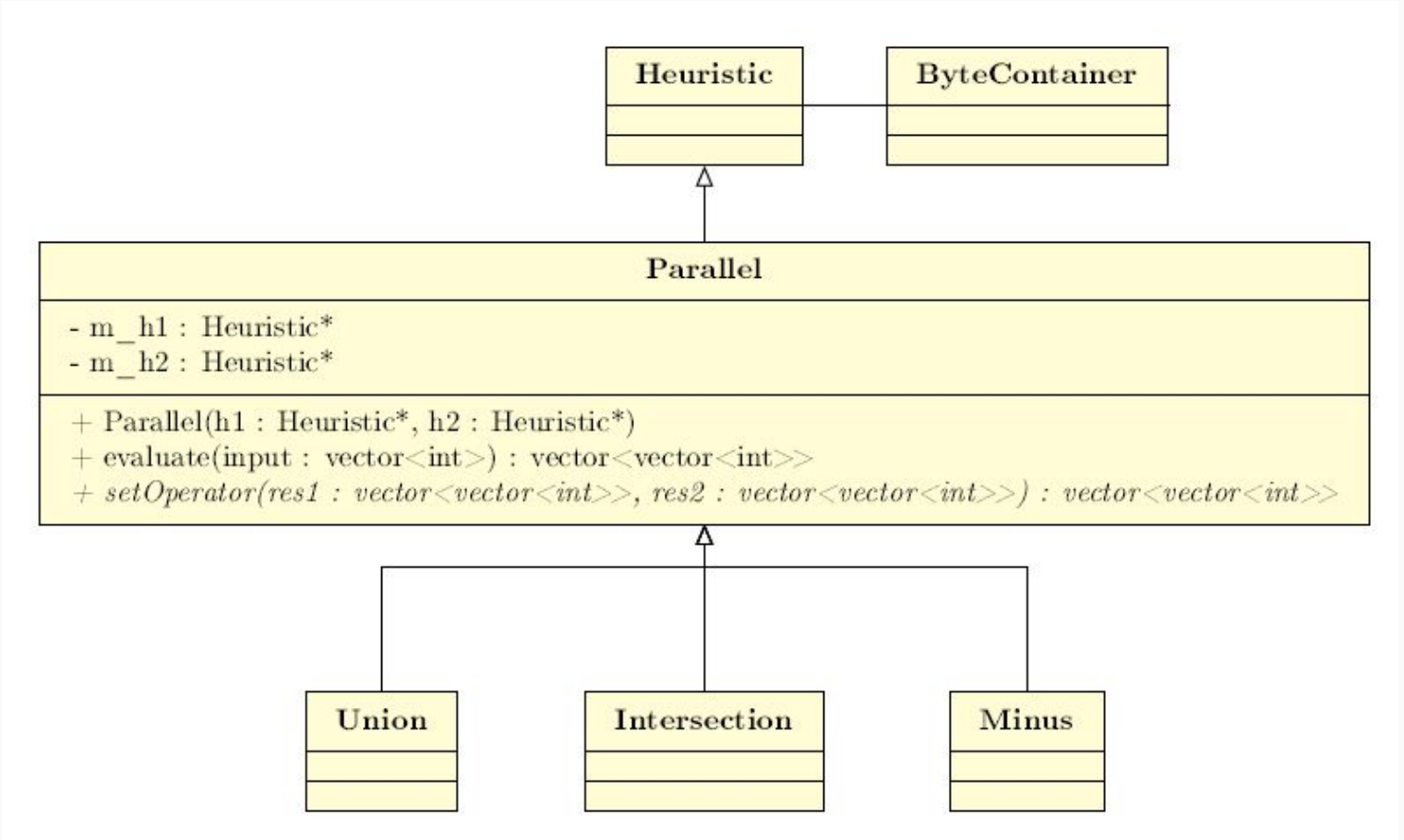
Class Layout



Class Layout



Class Layout



Evaluation

Heuristic Evaluation:

- Comparison with expected output
- Verification of the decoding process

Evaluated heuristic	TSK tool	Used image	Additional heuristics	Test result
DOS	mmls	DFTT Extended DOS Partition Test		passed
Ext3	istat	DFTT EXT3FS Keyword Search #1		passed

Evaluation

Composition Evaluation:

- Composition verification through combination with test heuristics

Evaluated module	TSK tool	Used image	Additional heuristics	Test result
SeqComp	istat	DFTT EXT3FS Keyword Search #1	Ext3 + Input	passed
Or	istat	DFTT EXT3FS Keyword Search #1	Ext3 + Failure	passed
Union	istat	DFTT EXT3FS Keyword Search #1	Ext3 + AddResult	passed
Intersection	istat	DFTT EXT3FS Keyword Search #1	Ext3 + AddResult	passed
Minus	istat	DFTT EXT3FS Keyword Search #1	Ext3 + AddResult	passed

Conclusion

- Current heuristics operate on one single storage object as input
- No user interface
- Equal block size not practical
- No metadata

Conclusion

- Current heuristics operate on one single storage object as input
- No user interface
- ~~Equal block size not practical~~ ✔
- ~~No metadata~~ ✔

Conclusion

- Complex reconstruction tasks possible
- Combination of different reconstruction approaches and techniques
- Framework easily extendable

Thank you!

Formulas

- $H \coloneqq [B] \to (\mathcal{P}([B]) + \{\bot\})$
- $(\gg): H \times H \to H$

  $h_1 \gg h_2 \coloneqq h_1 \gg\!= choose \gg\!= h_2$
- $(||): H \times H \to H$
- $(h_1 \,||\, h_2)(x) \coloneqq if\ h_1(x) = \bot\ then\ h_2(x)\ else\ h_1(x)$
- $(op): \big(\mathcal{P}([B]) \times \mathcal{P}([B]) \to \mathcal{P}([B])\big) \to (H \times H \to H)$

  $h_1 + h_2 \coloneqq h_1\ op(\cup)\ h_2$

  $h_1 * h_2 \coloneqq h_1\ op(\cap)\ h_2$

  $h_1 - h_2 \coloneqq h_1\ op(\setminus)\ h_2$