SUPERVISOR'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	Explainability of malware classsifiers
Author's name:	Bc. Ondřej Vereš
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	computer science
Thesis supervisor:	prof. Ing. Václav Šmídl, Ph.D.
Supervisor's department:	computer science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment — **ordinarily challenging**

Evaluation of thesis difficulty of assignment.

The assignment was motivated by an existing software explaining malware classifiers. The challenge was to extend existing method using an approach missing in the existing toolbox.

Satisfaction of assignment — **fulfilled**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The assignment was fulfilled, the author define TreeLime as adaptation of the LIME explainer to Tree data. The proposed method was adequately analyzed and studied.

Activity and independence when creating final thesis — **A - excellent.**

Assess that student had positive approach, time limits were met, conception was regularly consulted and was well prepared for consultations. Assess student's ability to work independently.

The student worked independently, learned the existing software by studying its source with only minor help from the original authors. He also studied the LIME theory and proposed all the versions reported in the thesis.

Technical level — **B - very good.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The main focus of the author was on the implementation and analysis of the explainers. He studied in detail behavior of the method, performed a lot of sensitivity studies and studied internal processes within the method.

Formal and language level, scope of thesis — **C - good.**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

The thesis is written is a bit terse form, with relatively short introductory and theoretical parts. The broader scope of the thesis is a bit neglected. This is related to the lack of time invested in the text, the author tried to improve his TreeLime until the last moment.

Selection of sources, citation correctness — **B - very good.**

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.

All relevant sources have been used and properly cited. I would appreciate a wider scope of the theoretical survey.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

The student worked independently on analysis of a software package that was not very stable and had to struggle with implementation issues. His experimental work was very good.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation.

The student actively worked on the goal of explaining malware samples. He have learned the existing software and contributed a new method based on the LIME approach. The modification of the LIME to tree structures, denoted TreeLime, is an original contribution of the author. It is a valuable contribution, in spite of the fact that it did not outperform existing methods. However, the textual part of the thesis is rather terse and could benefit from more time invested in its polishing.

I evaluate handed thesis with classification grade B - very good.

Date: **3.6.2024** Signature: