

# Review report of a final thesis

Czech Technical University in Prague

Faculty of Information Technology

**Student:** Jan Vojtěšek  
**Reviewer:** Ing. Tomáš Zahradnický, Ph.D.  
**Thesis title:** Analysis of the Rescue File of BestCrypt Volume Encryption  
**Branch of the study:** Information Technology

**Date:** 14. 6. 2017

<i>Evaluation criterion:</i>	<i>The evaluation scale: 1 to 5.</i>
<b>1. Difficulty and other comments on the assignment</b>	<b>1 = extremely challenging assignment, 2 = rather difficult assignment, 3 = assignment of average difficulty, 4 = easier, but still sufficient assignment, 5 = insufficient assignment</b>
<i>Criteria description:</i> Characterize this final thesis in detail and its relationships to previous or current projects. Comment what is difficult about this thesis (in case of a more difficult thesis, you may overlook some shortcomings that you would not in case of an easy assignment, and on the contrary, with an easy assignment those shortcomings should be evaluated more strictly.)	
<i>Comments:</i> I find this assignment an extremely challenging assignment, as the reverse engineering course is taught in the master's study programme. The student had to study and master a lot of technologies and techniques in order to be able to successfully complete this thesis.	
<i>Evaluation criterion:</i>	<i>The evaluation scale: 1 to 4.</i>
<b>2. Fulfilment of the assignment</b>	<b>1 = assignment fulfilled, 2 = assignment fulfilled with minor objections, 3 = assignment fulfilled with major objections, 4 = assignment not fulfilled</b>
<i>Criteria description:</i> Assess whether the thesis meets the assignment statement. In Comments indicate parts of the assignment that have not been fulfilled, completely or partially, or extensions of the thesis beyond the original assignment. If the assignment was not completely fulfilled, try to assess the importance, impact, and possibly also the reason of the insufficiencies.	
<i>Comments:</i> I find the assignment fulfilled.	
<i>Evaluation criterion:</i>	<i>The evaluation scale: 1 to 4.</i>
<b>3. Size of the main written part</b>	<b>1 = meets the criteria, 2 = meets the criteria with minor objections, 3 = meets the criteria with major objections, 4 = does not meet the criteria</b>
<i>Criteria description:</i> Evaluate the adequacy of the extent of the final thesis, considering its content and the size of the written part, i.e. that all parts of the thesis are rich on information and the text does not contain unnecessary parts.	
<i>Comments:</i> Size of the thesis exceeds criteria laid upon the bachelor thesis.	
<i>Evaluation criterion:</i>	<i>The evaluation scale: 0 to 100 points (grade A to F).</i>
<b>4. Factual and logical level of the thesis</b>	<b>95 (A)</b>
<i>Criteria description:</i> Assess whether the thesis is correct as to the facts or if there are factual errors and inaccuracies. Evaluate further the logical structure of the thesis, links among the chapters, and the comprehensibility of the text for a reader.	
<i>Comments:</i> Factual view. I find most of the facts in the thesis accurate except for few statements. As an example, the student says on page 38: "an adversary also needs administrator privileges in order to be able to read its memory". This statement is incorrect. A user with sufficient privileges does not need to be an administrator in order to read process memory.  Logical view. The thesis is organized logically.	
<i>Evaluation criterion:</i>	<i>The evaluation scale: 0 to 100 points (grade A to F).</i>
<b>5. Formal level of the thesis</b>	<b>100 (A)</b>
<i>Criteria description:</i> Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspects, see Dean's Directive No. 14/2015, Article 3.	

*Comments:*

I find the level of formalism used in the thesis as adequate and accurate.

Language. I find no significant English mistakes, except for few missing articles.

Typography. I have no objections to the typography of the thesis.

*Evaluation criterion:*

*The evaluation scale: 0 to 100 points (grade A to F).*

**6. Bibliography**

100 (A)

*Criteria description:*

Evaluate the student's activity in acquisition and use of studying materials in his thesis. Characterize the choice of the sources. Discuss whether the student used all relevant sources, or whether he tried to solve problems that were already solved. Verify that all elements taken from other sources are properly differentiated from his own results and contributions. Comment if there was a possible violation of the citation ethics and if the bibliographical references are complete and in compliance with citation standards.

*Comments:*

The thesis refers to 41 references composed of web sources, books, and journal papers. I find this number adequate and the composition balanced.

*Evaluation criterion:*

*The evaluation scale: 0 to 100 points (grade A to F).*

**7. Evaluation of results, publication outputs and awards**

100 (A)

*Criteria description:*

Comment on the achieved level of major results of the thesis and indicate whether the main results of the thesis extend published state-of-the-art results and/or bring completely new findings. Assess the quality and functionality of hardware or software solutions. Alternatively, evaluate whether the software or source code that was not created by the student himself was used in accordance with the license terms and copyright. Comment on possible publication output or awards related to the thesis.

*Comments:*

The student put a lot of effort into examining BestCrypt and did even more work than the assignment commanded. In addition to what he had to do he also analyzed the boot loader and created two utilities, namely bcve\_otfe and rsc\_dumper.

*Evaluation criterion:*

*No evaluation scale.*

**8. Applicability of the results**

*Criteria description:*

Indicate the potential of using the results of the thesis in practice.

*Comments:*

I find the thesis results applicable, as it provides an independent 3rd party review of a commercial encryption tool.

*Evaluation criterion:*

*No evaluation scale.*

**9. Questions for the defence**

*Criteria description:*

Formulate any question(s) that the student should answer to the committee during the defence (use a bullet list).

*Questions:*

1. How could a regular user read process memory without being an administrator?

*Evaluation criterion:*

*The evaluation scale: 0 to 100 points (grade A to F).*

**10. The overall evaluation**

100 (A)

*Criteria description:*

Summarize the parts of the thesis that had major impact on your evaluation. The overall evaluation **does not** have to be the arithmetic mean or any other formula with the values from the previous evaluation criteria 1 to 9.

*Comments:*

I find this thesis an exceptional bachelor thesis. The student must have put a lot of effort into learning reverse engineering yet before master's study. This thesis could have been a diploma thesis and for this reason I do recommend it to be awarded by the dean as an exceptional bachelor's thesis. I do recommend Mr. Jan Vojtěšek's bachelor thesis for defense and grade it with A (excellent).

Signature of the reviewer: