*Review of a Doctoral Thesis at FIT BUT*

**Doctoral thesis** (title of the thesis): ***METHODS FOR INTELLIGENT NETWORK FORENSICS***

**Name of the doctoral student** (name and surname): ***Jan Pluskal***

---

**Name and institution of the reviewer** (full name of the reviewer, full name and country of the institution):

***Professor Jill Slay, SmartSat Chair of Cyber Security, University of South Australia, Mawson Lakes, SA5095. Australia.***

---

Please state your opinion on the following aspects of (I) the candidate's doctoral thesis and (II) the candidate's overall achievements, and (III) state your conclusion (a minimum of approx. 300 characters for each item? point below is recommended):

## I. Doctoral Thesis

Appropriateness and Relevance

Is the area addressed by the thesis appropriate to the particular scientific discipline of the doctoral thesis and does the thesis address relevant problems within the chosen area?

***This thesis develops the history and future direction of a discipline that the candidate and I both acknowledge as a special kind of Network Forensics. This specific approach, which is not shared by many theoreticians , is a pragmatic one designed to support the Law Enforcement community in its work in understanding the nature of criminal activity in this domain.***

A summary of the Contributions of the Thesis

From your point of view, please summarize what the goal of the thesis is, what the main contributions of the thesis are, and whether the thesis has achieved the chosen goal.

***The thesis and the written dissertation are very clearly expressing the goal of***

- ***"Revisiting methods used in network forensics tools to improve their capabilities of processing captured network communication and extraction of evidence in order to relax requirements on the technical expertise of LEA investigators."***

***This is a really important and very necessary goal since the problems faced by the Law Enforcement community are unique. Criminals are not governed by law, regulation and ethics and develop a set of unique illegal and unethical skills. Law Enforcement officers operate in a highly regulated environment and often, even though we try our best, with undeveloped technical skills. Thus, the role of the researcher in this field is to try to compensate for the lack of technical skills while maintaining a stance that they must produce reliable intelligence or electronic evidence for the courts.***

***Through the series of published papers and summary, the thesis develops a set of refined tools and/or techniques to develop Law Enforcement approaches to the investigation of various networks, architectures and protocols to achieve the goal above. I believe it achieves this goal very well.***

*Review of a Doctoral Thesis at FIT BUT*

Please indicate also specific contributions of the doctoral student.

Novelty and Significance:

Please assess the level of novelty of the results and their significance for the given scientific area, for its further development, and if applicable for possible applications in practice.

***The novelty of the results is the development and application of a unique contextualised tool. It is very strong and very focused applied work which has direct impact in its immediate area. The wider impact is perhaps the development of a methodology (and I identify totally with this work since I see myself as a similar researcher located in Australia) that other researchers, in other cultures, can recognise and apply with modifications. To me the kind of research outputs produced are practical ones and published in journals that Law Enforcement will actually read.***

Evaluation of the Formal Aspects of the Thesis:

Please evaluate formal qualities of the doctoral thesis and its language level.

***The thesis and papers are well written in formal style and require no correction. I am a native speaker of English and have no criticism of the candidate's use of English, his grammar, his presentation style, his diagrams, or his referencing. This is definitely presented as university academic level writing, analysis, synthesis and critique. It is also technically well grounded.***

Quality of Publications

Has the core of the thesis been published at an appropriate level? Please judge the quantity and quality of the publications. When judging the quality, please take into account internationally recognized standards (WoS/Scopus quartiles, CORE ranks, specific knowledge of flagship publication channels of a given community, etc.) in a way appropriate for the given area of the thesis.

***While there is often great concern expressed around whether publications are able to be accepted in ranked and Q1 publications, this work, like my own in the same field, is highly applied and designed for Law Enforcement. The candidate and supervisors have chosen, in my opinion, the appropriate journals and conferences and relate well to the professional/ academic community in this field.***

## II. Candidate's Overall Achievements

Overall R&D Activities Evaluation:

Does the student's doctoral thesis, the results included into it, and possible other scientific achievements listed in the list of scientific activities indicate that he/she is a person with scientific erudition and creative abilities?

***I believe that the candidate has demonstrated creativity, scientific ability, and a deep understanding of the issues that arise for Law Enforcement in solving 'wicked problems' in cybercrime, cyber war, cyber terrorism and other similar contexts. The development of tools and techniques to simplify complex technical processes is very difficult and the candidate has done this exceedingly well.***

Assessment of Other Candidate Characteristics (optional):

More characteristics of the doctoral student may be added here in a separate paragraph (e.g., awards, grant participation, international collaboration, etc.).

***The candidate is well-linked internationally and should be encouraged to extend his work.***

---

## III. Conclusion

The conclusion should contain an explicit statement saying whether, in your opinion, the doctoral thesis and the student´s achievements until now meet the generally accepted requirements for the award of an academic degree (in accordance with Section 47 of Act No. 111/1998 Coll., on higher education institution).*

* Short overview of both the Act and corresponding internal BUT regulations is enclosed.

***The student should be awarded the PhD degree with no corrections needed.***

***Adelaide, Australia: 22nd March 2023.***

Signature of the reviewer: