

## Homework 6

In this homework we make a break from coding and do literature research. Your task is to pick one paper from a list of publications related to Bayesian Networks and Belief Propagation, read and understand it and write a short summary in up to 2 pages of text. Show that you have understood well the motivation, methodology, results and the contribution of the paper to the set of malware detection techniques.

List of papers:

1) Polonium: Tera-Scale Graph Mining for Malware Detection

<https://www.ml.cmu.edu/research/dap-papers/dap-chau.pdf>

2) Detecting Malware Based on DNS Graph Mining

<http://www.hindawi.com/journals/ijdsn/2015/102687/>

3) Detecting Malicious Domains via Graph Inference

[http://link.springer.com/chapter/10.1007%2F978-3-319-11203-9\\_1#page-1](http://link.springer.com/chapter/10.1007%2F978-3-319-11203-9_1#page-1)

To access this paper, you must login through Shibboleth to TUMOnline using your TUM credentials. Ask for more instructions if you cannot figure it out.

4) Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data

<http://arxiv.org/pdf/1411.5005.pdf> (Arxiv Preprint, but still interesting)

Have fun!