**Ph.D. Thesis Defense “Imaging and Evaluating The Memory Access for Malware”**

**Abstract:** Malware analysis is a forensic process. After infection and the damage represented itself with the full scale, then the analysis of the attack, the structure of the executable, and the aim of the malware can be discovered. These discoveries are converted into analysis reports and malware signatures and shared among antivirus databases and threat intelligence exchange platforms. This highly valuable information is then utilized in the detection mechanisms in order to prevent further dissemination and infections of malware. The types of analysis of the malware sample in this process can be grouped into two categories: static analysis and dynamic analysis. In static analysis, the executable file is reverted to the source code through disassemblers and reverse engineering software and analyzed whereas dynamic analysis includes running the sample in an isolated environment and analyzing its behavior. Both static and dynamic analysis have limitations such as packing, obfuscation, dead code insertion, sandbox detection, and anti-debugging techniques. Memory operations, on the other hand, are not possible to hide by these limitations and inevitable for any software since the inventions of the computational models. Therefore, in this research, memory operations and access patterns for the malicious acts are examined, and a contribution of a novel approach for extracting of memory access images is presented. In addition to extraction, methods of how these images can be used for detection and comparison is introduced through an image comparison technique.

**Key Words:** Malware Analysis, Malware Imaging, Memory Analysis, Dynamical Binary Analysis, Memory Operations Analysis.

**Short Bio:**

Çağatay Yücel is a Ph.D. candidate at the Computer Engineering Department at Yaşar University. His research interests are Reverse Engineering, Malware Analysis, Cyber Threat Intelligence, and Computer Forensics.