Abstrak

Analisis *malware* membutuhkan keterampilan khusus untuk melakukan pendeteksian dan memahami cara kerja dari *malware* tersebut. Program berbahaya atau *malware* menjadi sebuah ancaman atau masalah yang sulit bagi para peneliti, tidak ada *platform* komputasi atau lingkungan yang kebal terhadap ancaman tersebut. Kompleksitas yang meningkat membuat para peneliti harus bekerja keras dan membutuhkan waktu untuk memahami cara kerja *malware*

Terdapat dua teknik dasar yang sering digunakan untuk melakukan analisis *malware* yaitu statis dan dinamis analisis, dan penelitian *malware* yang dilakukan selama ini masih berfokus pada analisis perilaku yang keberhasilan metode tersebut tergantung pada model *malware*. Penggunaan teknik *signature based* sangat tergantung pada perilaku *malware* yang dianalisis, analisis menjadi sulit ketika ditemukan *malware* baru yang menggunakan suatu teknik untuk menyulitkan sistem analisis.

Berdasarkan uraian fakta yang disampaikan, dianggap perlu dibangun sebuah ontologi dalam melakukan analisis terhadap *malware* sehingga dapat digunakan sebagai pengembangan, pemetaan pengetahuan serta mengindetifikasi cara kerja *malware*. Pada penelitian ini metode yang diusulkan adalah pengembangan dari metode *Malware Analysis Body of Knowledge*, dimana metode ini bekerja pada domain tertentu untuk memetakan karakteristik dan mengklasifikasi jenis *malware* yang akan dibahas. Pada penelitian ini berfokus kepada ontologi sebagai *knowledge base* dan pembahasannya lebih kepada memetakan karakteristik dan pengklasifikasian jenis *malware*, dengan memanfaatkan *protégé* sebagai tools untuk merancang model ontologi *malware*

Kata kunci

Malware, Forensika Digital, Ontologi, Pengembangan, Karakteristik, Klasifikasi *Malware*

Abstract

Malware analysis requires special skills to make the detection and understand the workings of the malware. Malicious programs or malware becomes a threat or a problem that is difficult for researchers, there is no computing platform or environment that is immune to the threat. The increased complexity makes the researchers have to work hard and take time to understand how the malware

There are two basic techniques that are often used to perform analysis of malware is static and dynamic analysis, and research conducted during the malware is still focused on the analysis of the behavior of the success of the method depends on the model of the malware. The use of signature-based technique is highly dependent on the behavior of malware that were analyzed, the analysis becomes difficult when it was discovered a new malware that uses a technique to complicate analysis system.

Based on the description of the facts presented, it is necessary to build an ontology in the analysis of malware that can be used as a development, knowledge mapping as well as identifyingQ malware. In this study, the proposed method is the development of methods of Malware Analysis Body of Knowledge, where this method works on a specific domain to map and classify the characteristics of a type of malware that will be discussed. In this study focuses on the ontology as a knowledge base and more discussion to map the characteristics and classification of malware, by using protégé as tools for modeling ontology malware

Keywords

Malware, Digital Forensics, Ontology, Development, Characteristics, Classification