

Lembar Pengesahan Pembimbing

**Metode Klasifikasi Dan Analisis Karakteristik Malware
Menggunakan Konsep Ontologi**

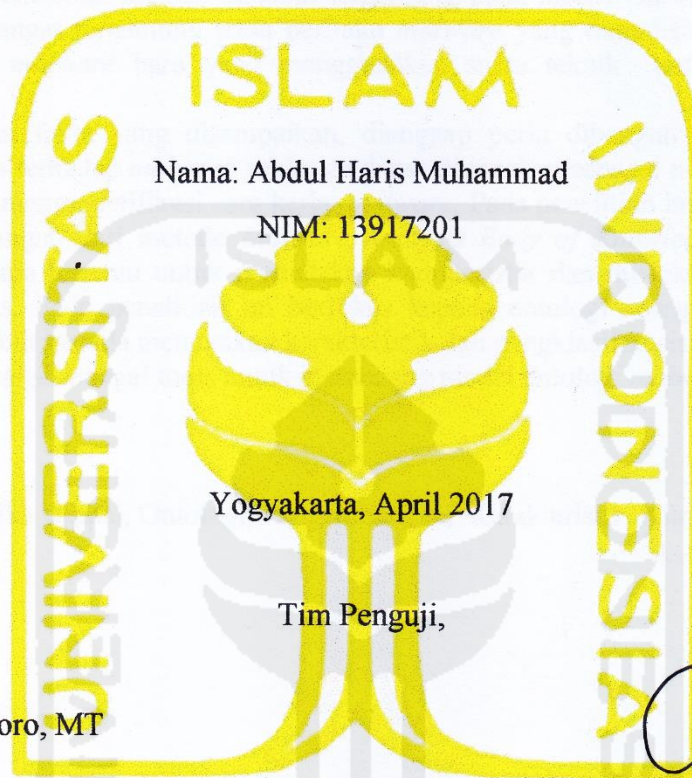


Pembimbing I

Dr. Bambang Sugiantoro, MT

Lembar Pengesahan Penguji

**Metode Klasifikasi Dan Analisis Karakteristik Malware
Menggunakan Konsep Ontologi**



Nama: Abdul Haris Muhammad

NIM: 13917201

Yogyakarta, April 2017

Tim Penguji,

Dr. Bambang Sugiantoro, MT
Ketua

Yudi Prayudi, S.Si, M.Kom
Anggota I

Dr. Imam Riadi, M.Kom
Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST.,M.Sc

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 mengidentifikasi 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

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, April 2017

METERAI
TEMPEL

2E9EDAEE084480781

6000
ENAM RIBURUPIAH

Abdul Haris Muhammad

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis



Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain



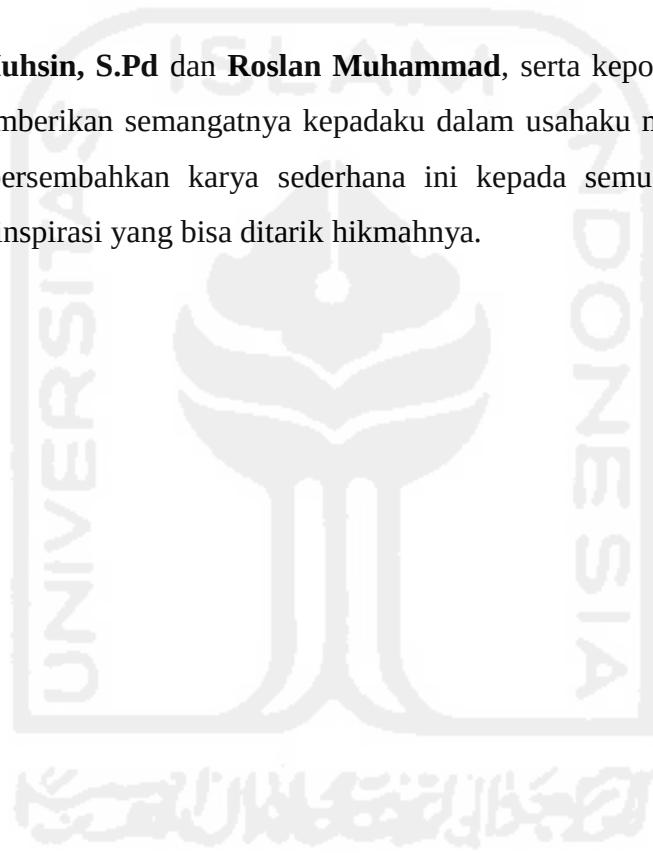
Halaman Persembahan



Karya ini saya persembahkan kepada:

Ayahanda **Ade Muhammad S.Pd** dan **Ibunda Ramla Usaman S.Pd**, yang senantiasa menjadi orang tua yang hebat karena tidak pernah menyerah dalam usaha membesarkan dan menghebatkan anak-anaknya.

Kakakku **Rahma A Muhsin, S.Pd** dan **Roslan Muhammad**, serta keponakanku **Muhammad Al Fatih** yang selalu memberikan semangatnya kepadaku dalam usahaku menuntut ilmu selama ini. Pada akhirnya saya persembahkan karya sederhana ini kepada semua pembaca, untuk dapat ditelusuri dan menjadi inspirasi yang bisa ditarik hikmahnya.



Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbil 'alamin, puji syukur penulis haturkan kehadiran Allah SWT, karena atas limpahan rahmat, hidayah dan inayah-Nya sehingga penelitian yang berjudul **“Metode Klasifikasi dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi”** ini dapat terselesaikan. Dan tak lupa shalawat serta salam kepada baginda Rasulullah Muhammad Sallallah' Alaihi Wasallam selalu penulis curahkan.

Penelitian ini merupakan salah satu syarat untuk mencapai gelar Magister Komputer pada program Pasca Sarjana Universitas Islam Indonesia.

Selama penelitian ini, penulis menyadari bahwa sepenuhnya telah mendapatkan begitu banyak bantuan dari berbagai pihak, sehingga tidak lupa penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

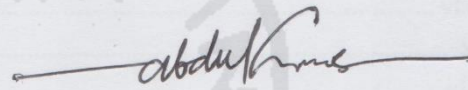
1. Bapak Dr. Ir. Harsoyo, M.Sc sebagai Rektor UII, bapak Dr. Ing. Ilya Fajar Maharika, MA., IAI sebagai Wakil Rektor I, bapak Dr. Nur Feriyanto, M.Si sebagai Wakil Rektor II, dan bapak Dr. Abdul Jamil, SH, MH sebagai Wakil Rektor III.
2. Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc. sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Bapak Dr. Bambang Sugiantoro, M.T. selaku pembimbing I yang telah meluangkan waktunya dalam membimbing dan membantu serta memudahkan penulis selama penulisan tesis ini.
4. Bapak Ahmad Luthfi, S.Kom., M.Kom selaku pembimbing II yang telah meluangkan waktunya dalam membimbing dan membantu serta memudahkan penulisa selama penulisan tesis ini.
5. Bapak Yudi Prayudi, S.Si., M.Kom selaku Ketua Jurusan Forensika Digital FTI UII sekaligus sebagai penguji III yang telah meluangkan waktunya dalam membimbing dan membantu serta memudahkan penulis selama penulisan tesis ini.
6. Bapak Dr. Imam Riadi, M. Kom selaku penguji IV yang telah memberikan masukan, saran, dan kritikan kepada penulis sebagai perbaikan untuk menjadi lebih baik.
7. Segenap Dosen dan Staf UII Yogyakarta yang telah memberikan bantuan, motivasi, dan bimbingan serta waktu luangnya dalam berdiskusi dengan penuh kesabaran dan keikhlasan.
8. Rekan-rekan mahasiswa MTI angkatan IX yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.

9. Kedua Orang Tua tercinta, Ayahanda Ade Muhammad A.Ma., S.Pd., dan Ibunda Ramla Usman, A.Ma.,S.Pd., Serta kakak, Roslan Muhammad, dan Rahma A. Muhsin., S.Pd yang tiada henti-hentinya memberikan segala bentuk dukungan, do'a, dan semangat, serta terus menjadi motivasi bagi penulis agar penelitian ini segera terselesaikan.

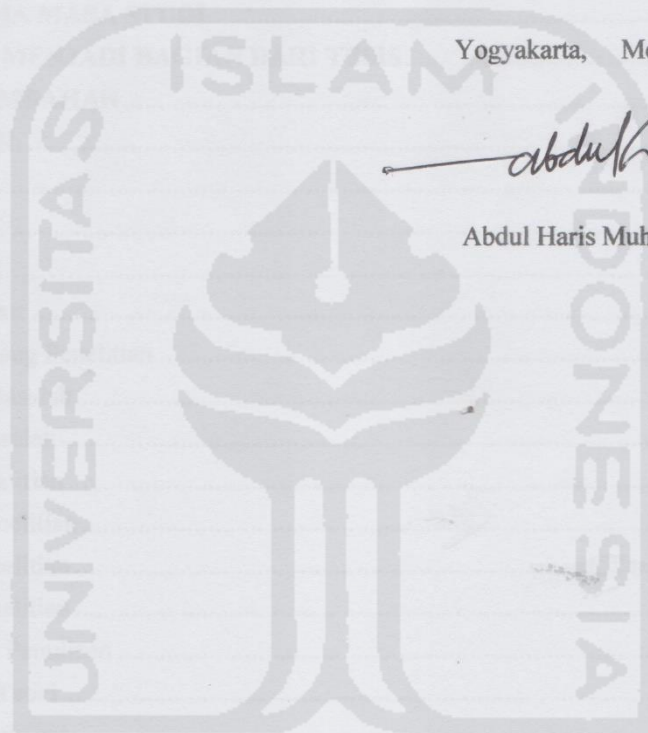
Penulis menyadari isi maupun cara penyampaian dalam laporan penelitian ini masih jauh dari sempurna, untuk itu kami mengharapkan saran dan kritik yang bersifat membangun dari para pembaca. Dan semoga apa yang didapatkan dari penelitian ini dapat menjadi manfaat bagi diri pembaca sendiri dan orang lain.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Yogyakarta, Mei 2017



Abdul Haris Muhammad



وَالْحَمْدُ لِلّٰهِ رَبِّ الْعَالَمِينَ