



**ANALISA SAMPLE MALWARE PADA SISTEM OPERASI WINDOWS 10
DENGAN TOOLS *CUCKOO SANDBOXX***

SKRIPSI

**Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Program Studi Informatika**

Oleh :

Muhammad Rifki Adiyatma

2022110055P

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI
2025**



**ANALISA SAMPLE MALWARE PADA SISTEM OPERASI
WINDOWS 10 DENGAN TOOLS CUCKOO SANDBOXX**

SKRIPSI

**Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Program Studi Informatika**

Oleh :

**Muhammad Rifki Adiyatma
2022110055P**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI
2025**

LEMBAR PENGESAHAN SKRIPSI

**Analisa Sampel Malware Pada Sistem Operasi Windows
Menggunakan Cuckoo Sandbox**

Oleh

Muhammad Rifki Adiyatma

NPM : 2022.11.0055P

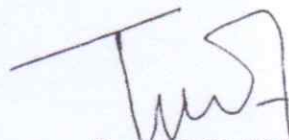
Palembang 25 Maret , 2025

Pembimbing I



**Dr. Herri Setiawan, S.Kom., M.Kom.
NIK : 2003.01.0060**

Pembimbing II



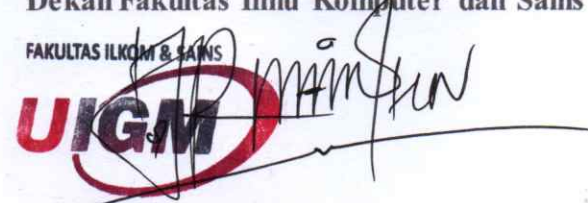
**Tasmi, S.Si., M.Kom
NIK: 2017.01.0230**

Mengetahui,

Dekan Fakultas Ilmu Komputer dan Sains

FAKULTAS ILMU KOMPUTER DAN SAINS

UIGN



**Rudi Heriansyah, S.T., M.Eng. Ph.D.
NIK: 2022.01.0315**

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari Selasa tanggal 11 Februari 2025 telah dilaksanakan ujian sidang skripsi :

Nama : Muhammad Rifki Adiyatma

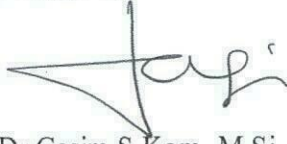
NPM : 2022.11.0055P

Judul : Analisa sampel malware pada sistem operasi windows menggunakan *cuckoo sandbox*

Oleh Prodi Teknik Informatika Fakultas Ilmu Komputer dan Sains Universitas Indo Global Mandiri Palembang

Palembang, 24 Maret 2025

Penguji 1,



Dr. Gasim, S.Kom., M.Si

NIK: 2023.01.0340

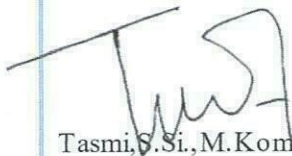
Penguji 2,



Dr. Shinta Puspasari, S.Si., M.Kom

NIK: 2015.01.0132

Penguji 3,



Tasmi, S.Si., M.Kom

NIK: 2017.01.0230

Menyetujui,

Ka. Prodi Teknik Informatika



Zaid Romegar Mai, S.T., M.Cs

NIK: 2021.01.0307



SURAT KETERANGAN REVISI SKRIPSI
PROGRAM STUDI TEKNIK INFORMATIKA (SI)
FASILKOM DAN SAINS UNIVERSITAS INDO GLOBAL MANDIRI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa :

Nama : Muhammad Rifki Adiyatma

NPM : 2022.11.0055P

Judul : Analisa sampel malware pada system operasi windows
menggunakan cuckoo sandbox

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan SKRIPSI

Palembang, 24 Maret 2025

Penguji 1,

Dr. Gasim, S.Kom., M.Si

NIK: 2023.01.0340

Penguji 2,

Dr. Shinta Puspasari, S.Si., M.Kom

NIK: 2015.01.0132

Penguji 3,

Tasmi, S.Si., M.Kom.

NIK: 2017.01.0230

Menyetujui,

Ka. Prodi Teknik Informatika

Zaid Romegar Mair, S.T., M.Cs

NIK: 2021.01.0307

Analisa Malware Pada Sistem Operasi Windows Menggunakan

Cuckoo Sandboox

ABSTRAK

Analisis malware merupakan langkah penting dalam mendeteksi, memahami, dan mengurangi dampak dari perangkat lunak berbahaya pada sistem komputer. Penelitian ini berfokus pada analisis sampel malware pada sistem operasi Windows menggunakan *Cuckoo Sandbox*, sebuah platform *open-source* yang dirancang khusus untuk menganalisis perilaku malware secara otomatis. Proses analisis dilakukan dengan mengisolasi sampel dalam lingkungan virtual yang dikendalikan, sehingga dapat memonitor aktivitas berbahaya tanpa risiko terhadap sistem host. Penelitian ini melibatkan beberapa tahap, mulai dari pengumpulan sampel malware, konfigurasi *Cuckoo Sandbox*, hingga eksekusi dan analisis hasil. *Cuckoo Sandbox* mengamati berbagai parameter, termasuk file yang dimodifikasi, registri yang diakses, koneksi jaringan yang dibuka, serta proses yang dijalankan oleh malware. Data yang dikumpulkan kemudian dianalisis untuk mengidentifikasi pola dan teknik yang digunakan oleh malware .

Kata Kunci : Sistem Operasi Windows 10, *Cuckoo Sandbox* ,Analisa
Dinamis,Sample Malware

***Analysis Of Malware Samples On The Windows Operating System
Using Cuckoo Sandbox***

ABSTRACT

Malware analysis is a critical step in detecting, understanding, and mitigating the impact of malicious software on computer systems. This study focuses on analyzing malware samples on the Windows operating system using Cuckoo Sandbox, an open-source platform specifically designed to automatically analyze malware behavior. The analysis process involves isolating the sample in a controlled virtual environment, allowing for the monitoring of harmful activities without risking the host system. The research includes several stages, from malware sample collection and Cuckoo Sandbox configuration to execution and result analysis. Cuckoo Sandbox observes various parameters, including modified files, accessed registry keys, opened network connections, and processes executed by the malware. The collected data is then analyzed to identify patterns and techniques used by the malware

Kata Kunci : *Windows Operating System 10, Cuckoo Sandbox, Analysis
Dynamic, Sample Malware*

KATA PENGANTAR

Puji dan Syukur Penulis persembahkan kehadiran Allah SWT berkat Rahmat dan Hidayah-Nya lah akhirnya penelitian ini dapat diselesaikan dengan baik tepat pada waktunya, tidak lupa shalawat serta salam selalu dilimpahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga sahabat para pengikut dan insyaallah kita semua hingga akhir zaman.

Skripsi yang penulis buat dengan judul “Analisa Sample Malware Pada Sistem Operasi Windows Menggunakan *Cuckoo Sandbox*” disusun guna memenuhi syarat kelulusan dalam memperoleh gelar Sarjana (S1) pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri (UIGM) Palembang. Tidak lupa Penulis mengucapkan terima kasih atas bantuan yang diberikan selama penyusunan skripsi ini kepada :

1. Dr. Marzuki Alie, SE., MM selaku Rektor Universitas Indo Global Mandiri (UIGM).
2. Rudi Heriansyah, S.T., M.Eng., Ph.D sebagai Dekan Fakultas Ilmu Komputer Universitas Indo Global Mandiri (UIGM).
3. Evi Yulianti, S.Kom., M.SI sebagai Dosen Pembimbing Akademik
4. Zaid Romegar Mair, S.T., M.Cs sebagai Ketua Prodi Teknik Informatika Universitas Indo Global Mandiri (UIGM).
5. Dr. Herri Setiawan, M.Kom sebagai Dosen Pembimbing I.
6. Tasmi, S.Si., M.Kom. Sebagai Dosen Pembimbing II.
7. Keluarga saya, Istri dan Anak tersayang yang selalu mendukung dan mendoakan saya.
8. Bapak/Ibu Dosen Fakultas Ilmu Komputer dan Karyawan/Karyawati Universitas Indo Global Mandiri (UIGM).

Penulis menyadari bahwa penyusunan skripsi ini masih memiliki banyak kekurangan, karenanya Penulis mengharapkan saran dan kritik yang sifatnya membangun agar

dapat digunakan demi perbaikan skripsi ini nantinya. Penulis juga berharap agar skripsi ini akan memberikan banyak manfaat bagi semua pihak yang memerlukannya.

Palembang, 05 Desember 2024

Penulis,

Muhammad Rifki Adiyatma

NPM : 2022110055P

DAFTAR ISI

HALAMAN JUDUL LUAR.....	i
HALAMAN JUDUL DALAM.....	ii
LEMBAR PENGESAHAN SKRIPSI.....	iii
LEMBAR PERSETUJUAN DEWAN PENGUJI.....	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGHANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan.....	5
BAB I PENDAHULUAN.....	4
BAB II LANDASAN TEORI.....	4
BAB III METODOLOGI PENELITIAN.....	6
BAB IV HASIL DAN PEMBAHASAN.....	6
BAB V KESIMPULAN DAN SARAN.....	6
BAB II LANDASAN TEORI.....	7
2.1 Pengertian Malware.....	7
2.2 Jenis-Jenis Malware.....	7
2.3 Hash.....	9
2.4 Malware Analysis.....	10
2.5 Metode Analisis Malware.....	10
2.5.1 Analisis Malware Dinamis.....	10

2.6 Spesifikasi Perangkat lunak dan perangkat keras.....	11
2.6.1 Cuckoo Sandbox.....	11
2.6.2 Virus Total.....	11
2.7 Sistem Operasi Windows.....	11
2.8 Penyebab Kerentanan Sistem Operasi Windows Terhadap Malware.....	13
2.9 Strategi Perlindungan Dan pencegahan.....	13
2.10 Perencanaan Sistem Analisis.....	14
2.11 Trojan.....	15
2.12 Ransomware Wannacry.....	16
2.12.1 Cara Kerja Ransomware Wannacry.....	17
BAB III METODE PENELITIAN.....	21
3.1 Metode Penelitian Dinamis Analisis.....	21
3.2 Analisis Malware Dinamis.....	22
3.2.1 Sistem Keamanan.....	24
3.3 Aplikasi Yang Dibutuhkan Dalam Metode Penelitian.....	26
3.4 Rencana Pengerjaan.....	26
3.4.1 Proses Upload Sampel Malware.....	26
3.5 Analisis Perilaku Malware.....	28
3.6 Analisis Malware Manual.....	28
3.7 Data Penelitian.....	28
3.8 Pengumpulan Data.....	29
3.9 Diagram Alur Analisis Malware.....	30
3.10 Hasil Analisa Malware.....	30
3.10.1 Cara Analisa Malware.....	31
3.11 Sampel Malware.....	32
3.12 Summary Result.....	32
BAB IV HASIL DAN PEMBAHASAN.....	32
4.1 Definisi Masalah.....	32
4.2 Study Literature	32
4.3 Analisis.....	32
4.4 Testing.....	33

4.4.1 Analisis Dinamis	33
4.4.2 Pengujian Malware Pada Tools Cuckoo Sanbdoox.....	34
4.4.3 Persiapan lingkungan Pengujian	34
4.4.4 Analisa Identifikasi Malware.....	33
4.4.5 Tampilan File Malware.....	35
4.4.6 Pemilihan Sampel Malware.....	36
4.4.7 Analisa Hasil Pengujian Sampel Malware.....	36
4.4.8 Aktivitas Registry.....	36
4.4.9 Efek Dari Keamanan.....	38
4.5 Analisa Malware Ramsorware.....	39
4.5.1 Analisa Signature.....	39
4.5.2 Static Analysis.....	44
4.5.3 String Analysis.....	46
4.5.4 Hasil Analisis Ancaman Siber.....	47
4.5.5 Ramsorware Downloader.....	48
4.6 Perbandingan Antara Sistem Operasi Windows Dan Virtual Mesin (VM).....	51
4.7 Metode Analisis Yang Digunakan.....	53
4.8 Menjalankan Malware Untuk Observasi.....	54
4.9 Kinerja & Efisiensi.....	55
4.10 Analisa Lalu Lintas Jaringan.....	56
4.10.1 Spesifikasi Keamanan Windows Dan Virtual Machine (VM).....	56
4.11 Summary Result.....	57
4.11.1 Identifikasi File.....	57
BAB V KESIMPULAN DAN SARAN.....	59
5.1 Kesimpulan dan Saran.....	59
DAFTAR PUSTAKA.....	59

DAFTAR TABEL

Table 2.1 Spesifikasi Hardware.....	10
Tabel 2.2 Spesifikasi software.....	10
Table 3.1 Tools metode penelitian.....	25
Tabel 3.2 Sampel malware.....	30
Tabel 4.1 Identitas malware.....	34
Tabel 4.2 Aktivitas Registry.....	36
Tabel 4.3 Aktivitas Registry Pada Ramsorware Wannacry.....	40
Tabel 4.4 Jaringan.....	42
Tabel 4.5 Aktivitas Virtual Memory.....	47
Tabel 4.6 Log Aktivitas Jaringan.....	48
Tabel 4.7 Hasil Check HASH Pada Virus Total.....	50
Tabel 4.8 Perbandingan Windows dan Virtual Machine.....	51
Tabel 4.9 Metode Analisis.....	52
Tabel 4.10 Observasi.....	53
Tabel 4.11 Kinerja & Efisiensi.....	54
Tabel 4.12 Lalu Lintas Jaringan.....	55
Tabel 4.13 Windows & Virtual Machine.....	55

DAFTAR GAMBAR

Gambar 2.1 Rancangan Sistem	13
Gambar 2.2 Jenis trojan.....	14
Gambar 2.3 Cara kerja Ransomware.....	16
Gambar 3.1 Tahap Penelitian.....	20
Gambar 3.2 Cara kerja Cuckoo Sandboox.....	21
Gambar 3.3 Cuckoo Sandbox.....	26
Gambar 3.4 Proses Download Sample Malware.....	26
Gambar 3.5 Hasil Download Sample Malware.....	26
Gambar 3.6 Proses upload sample Malware.....	26
Gambar 3.7 Hasil sample Malware.....	27
Gambar 3.8 Data Penelitian.....	28
Gambar 3.9 Sample Malware.....	28
Gambar 3.10 Diagram alur analisa malware.....	29
Gambar 4.1 halaman dashboard cuckoo sandboox.....	33
Gambar 4.2 Tampilan file sample malware setelah di upload.....	34
Gambar 4.3 Sampel Malware.....	35
Gambar 4.4 Grafik Aktivitas Malware.....	37
Gambar 4.5 File Terdeteksi Malware.....	38
Gambar 4.6 Hasil Check Pada Virus Total.....	39
Gambar 4.7 Section.....	43
Gambar 4.10 Data Resources.....	44
Gambar 4.11 String Analysis Malware.....	46
Gambar 4.12 Deteksi Rule Yara.....	48
Gambar 4.13 Crowdsourced IDS Rules.....	49