

**ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE  
MENGUNAKAN METODE STATIC ANALYSIS**

**SKRIPSI**



Disusun oleh:

**Rio Saputra  
17.83.0051**

**PROGRAM SARJANA  
PROGRAM STUDI TEKNIK KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2021**

**ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE  
MENGUNAKAN METODE STATIC ANALYSIS**

**SKRIPSI**

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta untuk  
memenuhi salah satu syarat memperoleh gelar Sarjana Komputer  
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

**Rio Saputra**  
**17.83.0051**

**PROGRAM SARJANA  
PROGRAM STUDI TEKNIK KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2021**

# HALAMAN PERSETUJUAN

## SKRIPSI

### ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGUNAKAN METODE STATIC ANALYSIS

yang dipersiapkan dan disusun oleh

**Rio Saputra**

**17.83.0051**

Telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal <08 februari 2021>

**Dosen Pembimbing**

**DONY ARIYUS, M.KOM**

**NIK. 190302128**

## HALAMAN PENGESAHAN

### SKRIPSI

#### ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGUNAKAN METODE STATIC ANALYSIS

yang dipersiapkan dan disusun oleh

**Rio Saputra**

**17.83.0051**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal <22 februari 2021>

#### Susunan Dewan Penguji

**Nama Penguji**

**Tanda Tangan**

**Uyock Anggoro Saputro, M.Kom**  
**NIK. 190302419**

**Nila Feby Puspitasari, S.Kom, M.Cs**  
**NIK. 190302161**

**Dony Ariyus, M.Kom**  
**NIK. 190302128**

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal < 22 februari 2021 >

**DEKAN FAKULTAS ILMU KOMPUTER**

**Krisnawati, S.Si, M.T.**  
**NIK. 190302038**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Rio Saputra**  
**NIM : 17.83.0051**

Menyatakan bahwa Skripsi dengan judul berikut:

### **Analisis Dan Deteksi File PDF Yang Terinfeksi Malware Menggunakan Metode Static Analysis**

Dosen Pembimbing : DONY ARIYUS, M.KOM

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, <22 februari 2021>

Yang Menyatakan,



Rio Saputra

## HALAMAN MOTTO

“**Kunci sukses** itu ada tiga, yang pertama itu **jangan ambisi** saat sudah nyampai step yang di inginkan, yang kedua **jangan syrik/iri** kepada orang lain, Dan yang ketiga **jangan lupa untuk bersedekah** karena sebagian harta kita itu milik orang lain juga.”

**(H. Bolot)**

“Anda ingin mengetahui siapa diri Anda? Jangan bertanya. Beraksilah!”

**(Thomas Jefferson)**

“Pekerjaan-pekerjaan kecil yg selesai dilakukan lebih baik daripada rencana-rencana besar yang hanya didiskusikan.”

**(Peter Marshall)**

"Beberapa orang memimpikan kesuksesan, sementara yang lain bangun setiap pagi untuk mewujudkannya."

**(Wayne Huizenga)**

## HALAMAN PERSEMBAHAN

Puji syukur kepada Allah SWT atas segala nikmat, hidayah, dan kesempatan menimba ilmu, sehingga penulis dapat menyelesaikan laporan ini. Dalam penyusunan laporan ini penulis banyak dibantu, dibimbing, dan didukung oleh berbagai pihak. Laporan ini penulis persembahkan kepada :

1. Kedua orang tua, Bapak Basuki dan Ibu Listiana yang selalu mendo'akan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing saya yang telah membantu dalam penyusunan skripsi ini.
3. Kepada keluarga besar Bapak Mujiono yang telah memberikan semangat dan dukungan, baik secara material atau secara visual.
4. Kepada Sahabat dan teman-teman yang ada di saat suka maupun duka selama masa perkuliahan.
5. Semua pihak yang mendukung saya secara langsung ataupun tidak langsung.

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa atas karunia. Yang telah melimpahkan kasih dan sayang-Nya kepada kita semua, sehingga penulis bisa menyelesaikan skripsi dengan tepat waktu, yang diberi judul “*Analisis Dan Deteksi File PDF Yang Terinfeksi Malware Menggunakan Metode Static Analysis*” .

Tujuan dari penyusunan skripsi ini guna memenuhi syarat memperoleh gelar Sarjana pada program studi S1 Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Didalam pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu disini penulis sampaikan rasa terimakasih sedalam-dalamnya kepada:

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta, dan sekaligus selaku Dosen pembimbing yang telah bersedia memberikan pengarahan dan masukan dalam menyelesaikan Skripsi saya.
4. Bapak Joko Dwi Santoso, M.kom. selaku Dosen yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.



7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.



Yogyakarta, 22 februari 2021

Penulis

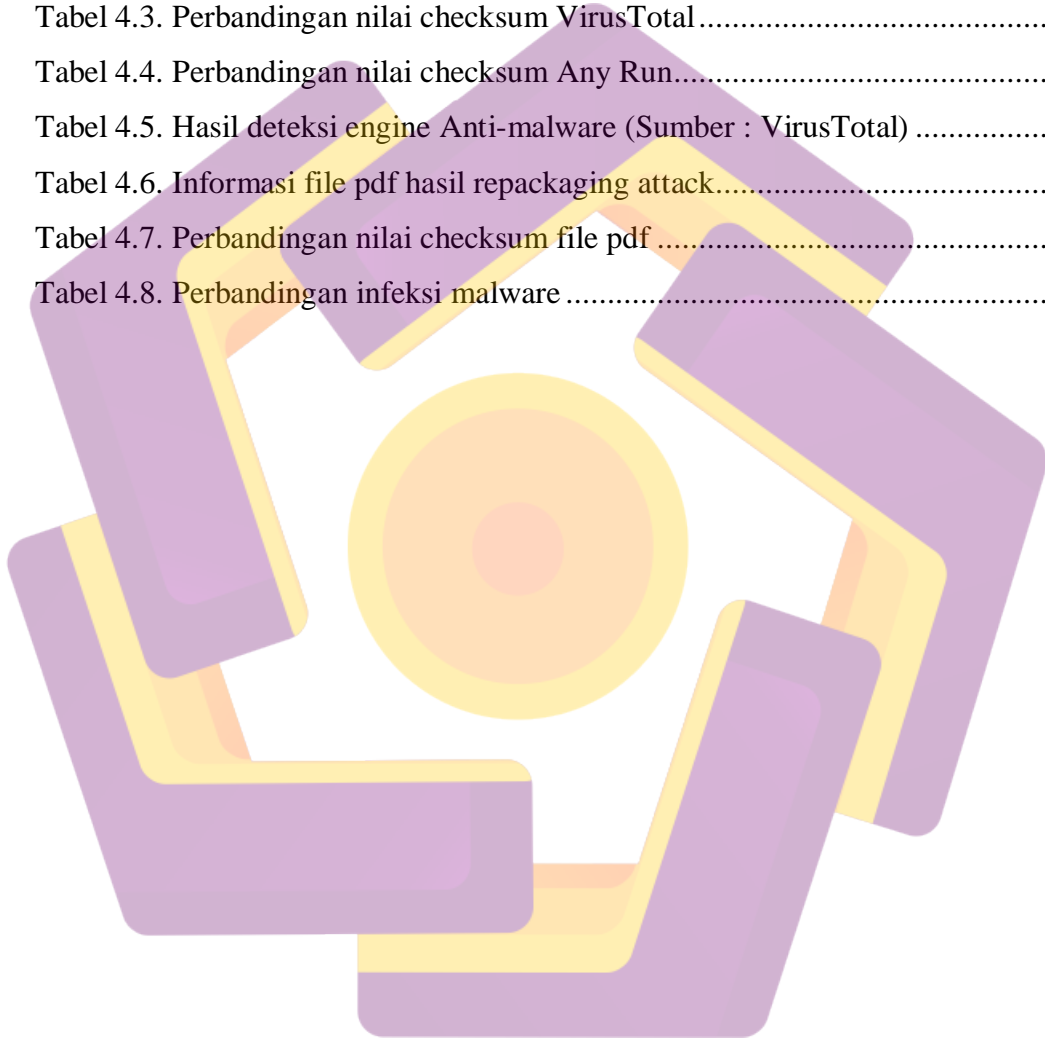
## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>HALAMAN PERSETUJUAN</b> .....	ii
<b>HALAMAN PENGESAHAN</b> .....	iii
<b>HALAMAN PERNYATAAN KEASLIAN SKRIPSI</b> .....	iv
<b>HALAMAN MOTTO</b> .....	v
<b>HALAMAN PERSEMBAHAN</b> .....	vi
<b>KATA PENGANTAR</b> .....	vii
<b>DAFTAR ISI</b> .....	ix
<b>DAFTAR TABEL</b> .....	xi
<b>DAFTAR GAMBAR</b> .....	xii
<b>INTISARI</b> .....	xiii
<b>ABSTRACT</b> .....	xiv
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Maksud dan Tujuan Penelitian.....	2
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
<b>BAB II LANDASAN TEORI</b> .....	5
2.1 Tinjauan Pustaka.....	5
2.2 Malware.....	9
2.2.1 Virus .....	9
2.2.2 Worm.....	9
2.2.3 Spyware.....	9
2.2.4 Trojan.....	10
2.2.5 Adware.....	10
2.2.6 Keylogger.....	10
2.2.7 Ransomware.....	10
2.2.8 Malicious Cyptominers.....	10
2.2.9 Rootkit .....	11
2.2.10 Backdoor.....	11
2.3 Anti-Malware.....	11
2.3.1 Anomaly-based Detection.....	11

2.3.2 Specification-based Detection.....	11
2.3.3 Signature-based Detection .....	12
2.4 File PDF.....	12
2.5 Static Analisis .....	13
2.6 Virus Total.....	14
2.7 App Any Run .....	14
2.8 MSFvenom .....	14
2.9 Virtual Machine .....	15
2.10 Payload.....	15
2.11 Kali Linux.....	16
2.12 Framework Metasploit .....	16
2.13 Meterpreter.....	17
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>18</b>
3.1 Gambaran Umum.....	18
3.2 Alur Penelitian Virus Total.....	20
3.3 Alur Penelitian Any Run .....	20
3.4 Alur Implementasi MSFvenom.....	21
3.5 Alat dan Bahan Penelitian .....	23
3.6 Metode Penelitian.....	23
3.6.1 Metode Pre-Experimental Design .....	23
3.6.1.1 Metode One Group Pretest Posttest Design.....	24
3.7 Metode Analisis .....	24
3.7.1 Analisis Static.....	24
<b>BAB IV PEMBAHASAN.....</b>	<b>25</b>
4.1 Implementasi Sistem .....	25
4.2 Implementasi Malware .....	25
4.3 Analisis File.PDF Sebelum Terinfeksi Malware .....	28
4.4 Implementasi Virus Total .....	30
4.5 Implementasi Any Run.....	33
4.6 Hasil Dan Pembahasan.....	36
4.6.1 Hasil Analisis File.PDF Setelah Terinfeksi Malware.....	36
<b>BAB V PENUTUP .....</b>	<b>42</b>
5.1 Kesimpulan.....	42
5.2 Saran.....	42
<b>DAFTAR PUSTAKA .....</b>	<b>44</b>
<b>LAMPIRAN .....</b>	<b>46</b>

## DAFTAR TABEL

Tabel 2.1. Perbandingan dengan beberapa penelitian sebelumnya .....	7
Tabel 4.1. Informasi File PDF (Sumber: VirusTotal).....	28
Tabel 4.2. Perbandingan nilai checksum antara VirusTotal dan Any Run .....	29
Tabel 4.3. Perbandingan nilai checksum VirusTotal .....	32
Tabel 4.4. Perbandingan nilai checksum Any Run.....	35
Tabel 4.5. Hasil deteksi engine Anti-malware (Sumber : VirusTotal) .....	36
Tabel 4.6. Informasi file pdf hasil repackaging attack.....	39
Tabel 4.7. Perbandingan nilai checksum file pdf .....	40
Tabel 4.8. Perbandingan infeksi malware .....	41



## DAFTAR GAMBAR

Gambar 3.1. Diagram Alur Metode Penelitian.....	19
Gambar 3.2. Alur Penelitian VirusTotal .....	20
Gambar 3.3. Alur Penelitian App Any Run .....	21
Gambar 3.4. Alur Implementasi MSFvenom .....	22
Gambar 3.5. Desain Penelitian One Group Pretest Posttest Design.....	24
Gambar 4.1. Metasploit.....	25
Gambar 4.2. Skema Jaringan.....	26
Gambar 4.3. Ip Public .....	26
Gambar 4.4. Payload.....	27
Gambar 4.5. Hasil Payload.....	28
Gambar 4.6. Informasi File pdf menggunakan Any Run.....	29
Gambar 4.7. Scan VirusTotal Sebelum infeksi Malware.....	30
Gambar 4.8. Detail VirusTotal sebelum terinfeksi Malware .....	31
Gambar 4.9. Scan VirusTotal sesudah terinfeksi Malware .....	31
Gambar 4.10. Detail VirusTotal sesudah terinfeksi Malware .....	32
Gambar 4.11. Scan Any Run sebelum terinfeksi malware .....	33
Gambar 4.12. Details Scan Any run sebelum terinfeksi Malware .....	34
Gambar 4.13. Scan Any Run sesudah terinfeksi malware .....	34
Gambar 4.14. Details Scan Any run sesudah terinfeksi Malware .....	35
Gambar 4.15. Informasi File pdf melalui Any Run.....	40

## INTISARI

*Portable Document Format* (disingkat *PDF*) adalah sebuah format berkas yang dibuat oleh Adobe Systems pada tahun 1993 untuk keperluan pertukaran dokumen digital. Format *PDF* digunakan untuk merepresentasikan dokumen dua dimensi yang meliputi teks, huruf, citra dan grafik vektor dua dimensi. Pada Acrobat 3-D, kemampuan *PDF* juga meliputi pembacaan dokumen tiga dimensi. Sekitar bulan september 2007, file *PDF* mulai dimanfaatkan oleh pembuat *virus* untuk menyertakan kode-kode tertentu dalam dokumen tersebut. Biasanya berupa *trojan*. Seperti juga diberitakan Avira tanggal 6 Mei 2008, kelemahan *PDF* dimanfaatkan untuk menyisipkan kode virus, sehingga ketika *PDF* dijalankan *virus* yang berupa *trojan* tersebut bisa menginstall dirinya ke komputer. Untuk mengetahui bagaimana *malware* dapat melakukan infeksi pada *File PDF* maka dari itu di perlukan analisis.

Analisis dilakukan dengan melakukan implementasi penyusupan *malware* pada sampel *File PDF* yang terjangkit *malware*. Penyusupan *malware* pada sampel *File* menggunakan *tools MSFvenom*. Dalam melakukan scanning, file akan dilakukan injeksi dengan tujuan menyusupkan *malware* yang diciptakan menggunakan *MSFvenom*.

Hasil implementasi yaitu *file PDF* yang berhasil diinfeksi *malware*. Selanjutnya dilakukan analisis statis guna mengetahui dampak dari hasil infeksi *malware*. Analisis statis menggunakan tool *VirusTotal* dan *App Any Run*. selanjutnya ditemukan perbedaan ukuran *file* dari sebelum infeksi *malware*.

**Kata kunci:** File PDF, Malware, Analisis Malware, Analisis Static.

## **ABSTRACT**

*Portable Document Format (abbreviated as PDF) is a file format created by Adobe Systems in 1993 for the purpose of exchanging digital documents. The PDF format is used to represent two-dimensional documents which include text, letters, images and two-dimensional vector graphics. In Acrobat 3-D, PDF capabilities also include reading three-dimensional documents. Around September 2007, PDF files began to be used by virus authors to include certain codes in the document. Usually a trojan. As Avira also reported on May 6, 2008, PDF weaknesses were used to insert virus code, so that when the PDF was run the virus in the form of a trojan could install itself on the computer. To find out how malware can infect PDF files, analysis is needed.*

*The analysis was carried out by implementing malware infiltration on a sample PDF file which was infected by malware. Infiltration of malware in the sample file using MSFvenom tools. In scanning, the file will be injected with the aim of infiltrating the malware created using MSFvenom.*

*The result of the implementation is a PDF file that was successfully infected with malware. Furthermore, a static analysis is carried out to determine the impact of the malware infection results. Static analysis using VirusTotal and App Any Run tools. furthermore found differences in file size from before malware infection.*

**Keyword:** File PDF, Malware, Malware Analysis, Analysis Static.