

DAFTAR ISI

TUGAS AKHIR.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
DAFTAR SINGKATAN	xiii
DAFTAR LAMPIRAN	xiv
ABSTRAK	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Pertanyaan Penelitian	3
1.4 Batasan Masalah.....	3
1.5 Tujuan Penelitian.....	4
1.6 Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terkait.....	5
2.2. Landasan Teori	12
2.2.1. Malware	12
2.2.2. Hybrid Analysis	13
2.2.3. Reverse Engineering	14

2.2.4.	VirusTotal	14
2.2.5.	APKTool	14
2.2.6.	JADX	15
2.2.7.	Phishing	15
2.2.8.	Telegram	16
2.2.9.	Mobile Security Framework (MobSF)	16
2.2.10.	Whatsapp	17
BAB III METODOLOGI PENELITIAN.....		18
3.1.	Objek dan Subjek Penelitian	18
3.2.	Alat dan Bahan Penelitian	18
3.3.	Diagram Alur Penelitian.....	19
3.3.1.	Identifikasi Masalah.....	20
3.3.2.	Studi Literatur	20
3.3.3.	Mencari Sampel Malware	21
3.3.4.	Analisis Statis	21
3.3.5.	Modifikasi Source Code	22
3.3.6.	Analisis Dinamis.....	23
3.3.7.	Dokumentasi	23
BAB IV HASIL DAN PEMBAHASAN		24
4.1.	Hasil Pemindaian VirusTotal	24
4.2.	Hasil Analisis Statis JADX	25
4.2.1.	Analisis Permission.....	25
4.2.2.	Analisis Source Code.....	27
4.2.3.	META-INF	33
4.3.	Hasil Analisis Statis Menggunakan MobSF	33

4.3.1.	<i>Security Score</i>	33
4.3.2.	<i>Analisis Permission</i>	34
4.3.3.	<i>Analisis Source Code</i>	35
4.4.	Perbandingan Analisis Manual dan Otomatis	36
4.5.	Modifikasi <i>Source Code</i>	37
4.6.	Hasil Analisis Dinamis Pada Perangkat Android	40
4.6.1.	Instalasi pada perangkat android	40
4.6.2.	Aktivitas saat aplikasi dijalankan	41
4.6.3.	Percobaan serangan akun korban	43
4.6.4.	Cara Mengatasi Infeksi <i>Malware</i> pada <i>Smartphone</i> Android	46
BAB V KESIMPULAN DAN SARAN		49
5.1.	Kesimpulan	49
5.2.	Saran	49
DAFTAR PUSTAKA		51
LAMPIRAN		54