

## DAFTAR ISI

LEMBAR PENGESAHAN .....	ii
LEMBAR ORISINALITAS .....	iii
ABSTRAK.....	iv
ABSTRACT.....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
DAFTAR SINGKATAN .....	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN.....	14
1.1. Latar Belakang.....	14
1.2. Rumusan Masalah .....	16
1.3. Pertanyaan Penelitian .....	16
1.4. Tujuan Penelitian.....	17
1.5. Batasan Masalah.....	17
1.6. Manfaat Penelitian.....	17
BAB II TINJAUAN PUSTAKA .....	18
2.1. Tinjauan Pustaka .....	18
2.2. Dasar Teori.....	25
2.2.1. Pengertian Analisis.....	25
2.2.2. Reverse Engineering .....	25
2.2.3. Smartphone .....	25
2.2.4. Android .....	26
2.2.5. Whatsapp GB .....	27
2.2.6. Malware.....	27
2.2.7. AhMyth .....	28
2.2.8. JADX.....	28
2.2.9. Linux .....	29
2.2.10. Kali Linux.....	29
2.2.11. Sistem Operasi .....	30
2.2.12. Backdoor.....	31

2.2.13.    Mobile Security Framework (MobSF).....	31
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>32</b>
3.1.    Subjek dan Objek Penelitian.....	32
3.2.    Alat dan Bahan Penelitian .....	32
3.3.    Diagram Alir Penelitian.....	34
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>41</b>
4.1    Hasil Instalasi Pada Android .....	41
4.2    Hasil Exploit.....	42
4.3    Hasil Analisis Otomatis Menggunakan MobSF (Analisis Statis).....	50
4.3.1    Security Score .....	50
4.3.2    Analisis Permission.....	52
4.3.3    Code Analysis .....	55
4.4    Hasil Analisis Manual .....	57
4.4.1    Analisis Permission.....	57
4.4.1    META-INF.....	59
4.4.2    Resources .....	60
4.4.3    Classes.dex .....	61
4.4.4    Assets .....	63
4.4.5    Lib .....	64
4.4.6    Res.....	65
4.4.7    Analisis Source Code .....	66
4.5    Perbandingan Analisis Otomatis (MobSF) dan Manual.....	110
<b>BAB V KESIMPULAN DAN SARAN.....</b>	<b>112</b>
5.1    KESIMPULAN .....	112
5.2    SARAN.....	113
<b>DAFTAR PUSTAKA .....</b>	<b>115</b>
<b>LAMPIRAN.....</b>	<b>118</b>