

**ANALISIS KESADARAN PENGGUNA APLIKASI TELEGRAM
MOD TERHADAP KEAMANAN INFORMASI MENGGUNAKAN
METODE *STATIC ANALYSIS* DAN KUANTITATIF**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Teknik Komputer



disusun oleh

ALI AKBAR MASNOROI

19.83.0442

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS KESADARAN PENGGUNA APLIKASI TELEGRAM
MOD TERHADAP KEAMANAN INFORMASI MENGGUNAKAN
METODE *STATIC ANALYSIS* DAN KUANTITATIF**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Teknik Komputer



disusun oleh

ALI AKBAR MASNOROI

19.83.0442

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS KESADARAN PENGGUNA APLIKASI TELEGRAM MOD
TERHADAP KEAMANAN INFORMASI MENGGUNAKAN METODE
STATIC ANALYSIS DAN KUANTITATIF**

yang disusun dan diajukan oleh

Ali Akbar Masnoroi

19.83.0442

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 18 Agustus 2023

Dosen Pembimbing,

Jeki Kuswanto, M.Kom

NIK. 190302456

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS KESADARAN PENGGUNA APLIKASI TELEGRAM MOD
TERHADAP KEAMANAN INFORMASI MENGGUNAKAN METODE
STATIC ANALYSIS DAN KUANTITATIF**

yang disusun dan diajukan oleh

Ali Akbar Masnoroi

19.83.0442

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.Kom
NIK. 190302181

Senie Destya, M.Kom
NIK. 190302312

Jeki Kuswanto, M.Kom
NIK. 190302456



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ali Akbar Masnoroi
NIM : 19.83.0442

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS KESADARAN PENGGUNA APLIKASI TELEGRAM MOD
TERHADAP KEAMANAN INFORMASI MENGGUNAKAN METODE
STATIC ANALYSIS DAN KUANTITATIF**

Dosen Pembimbing : Jeki Kuswanto, 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.

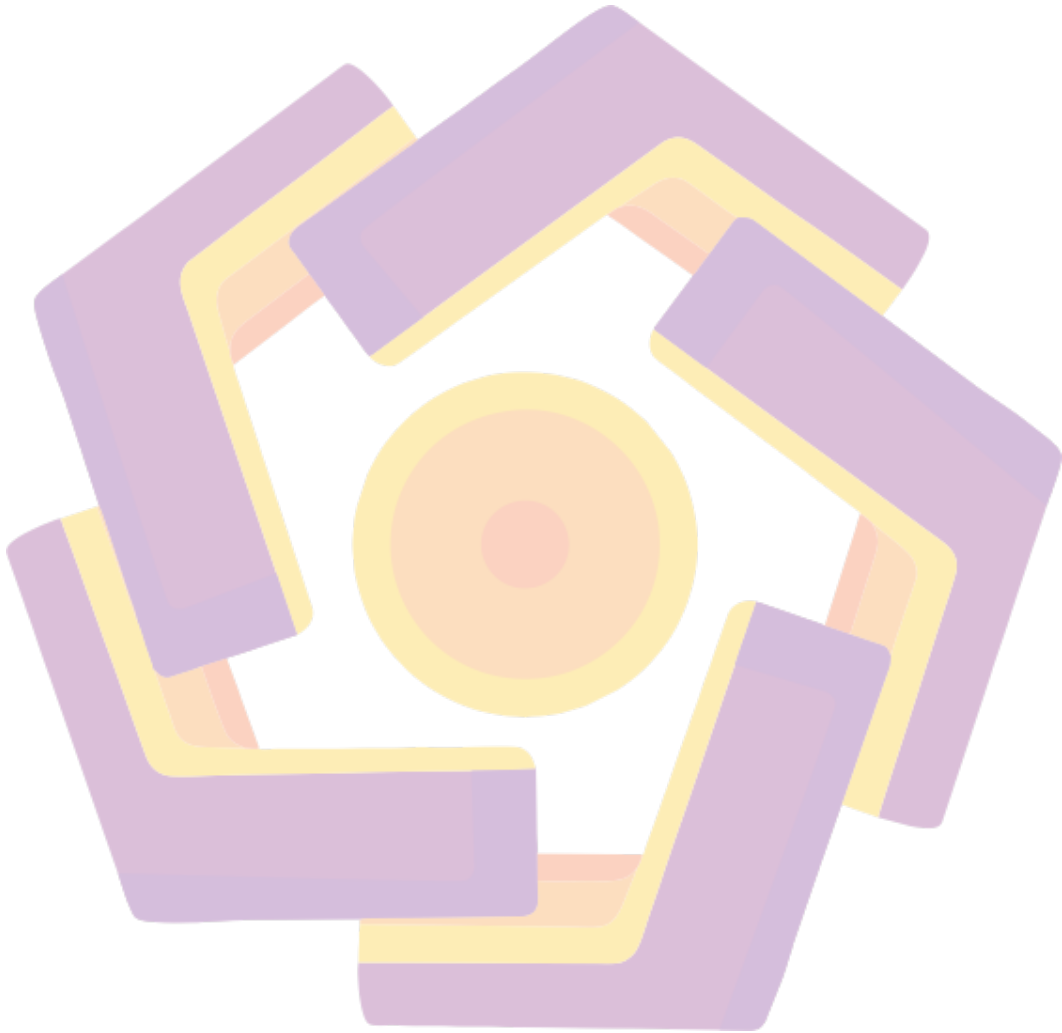
Yogyakarta, 18 Agustus 2023

Yang Menyatakan,



Ali Akbar Masnoroi

HALAMAN PERSEMBAHAN



KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, taufik dan hidayahnya kepada penulis sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan judul: “Analisis Kesadaran Pengguna Aplikasi Telegram Mod Terhadap Keamanan Informasi Menggunakan Metode *Static Analysis* dan Kuantitatif” dengan baik. Sholawat serta salam senantiasa kita curahkan kehadirah rosulullah Muhammad SAW yang senantiasa kita harapkan syafa’atnya di hari akhir kelak.

Penulis pada kesempatan kali ini menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya khususnya kepada Bapak dan Ibu yang telah mendukung dan mendoakan anaknya sehingga dapat menyelesaikan kuliah S1 ini. Ucapan terima kasih juga penulis sampaikan kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku rektor Universitas AMIKOM Yogyakarta.
2. Bapak Dony Ariyus, M.Kom. selaku ketua program studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Wahid Miftahul Ashari, S.Kom., M.T. sebagai dosen wali yang memberikan arahan dari awal hingga akhir semester terhadap penulis.
4. Bapak Jeki Kuswanto, M.Kom. sebagai dosen pembimbing yang telah memberikan banyak arahan serta dukungan terhadap penulis.
5. Rekan-rekan mahasiswa kelas Teknik Komputer 02 angkatan 2019 yang memberikan semangat serta dukungan terhadap penulis.

Akhirnya dengan kerendahan hati penulis menyadari bahwa penulisan skripsi ini masih banyak kekurangan, sehingga kritik dan saran yang bersifat membangun sangat penulis harapkan. Harapannya skripsi ini nantinya dapat memberikan manfaat bagi pendidikan di sektor bidang cybersecurity. Sekian terima kasih penulis ucapkan

Yogyakarta, 8 Agustus 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN.....	xi
DAFTAR LAMBANG DAN SINGKATAN	xii
DAFTAR ISTILAH	xiii
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1 Studi Literatur	6
2.2 Dasar Teori	15
2.2.1. Cyber Security	15
2.2.2. Keamanan Informasi	15
2.2.3. Android	17
2.2.4. Mobile Security Framework	17
2.2.5. Yaazhini	17
2.2.6. Telegram	18
2.2.7. SPSS Statistics	18
2.2.8. Malicious software	18
2.2.9. Analisis statis	21
2.2.10. Java Development Kit (JDK).....	22
2.2.11. Python	22
2.2.12. Git	22
2.2.13. Microsoft Visual C++ Build Tools	22
2.2.14. OpenSSL	22
2.2.15. Wkhtmlpdf	22
BAB III METODE PENELITIAN	23
3.1. Objek Penelitian.....	23
3.1.1. Telegram Mod Premium	24
3.1.2. Telegram Plus Messenger	24

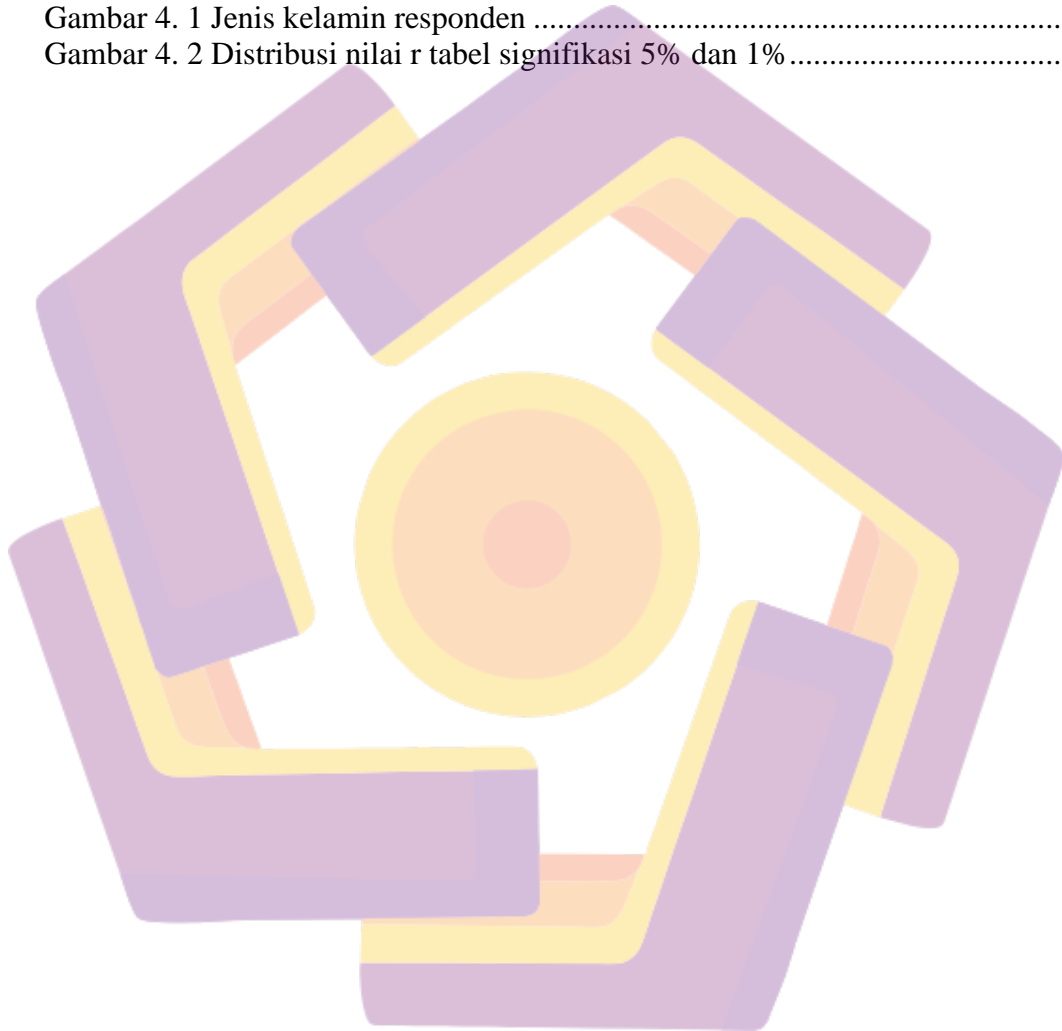
3.1.3.	Telegram X	25
3.2.	Alur Penelitian	25
3.2.1.	Alur Proses Analisis Statis	27
3.2.2.	Alur Proses Metode Kuantitatif	27
3.3.	Metodologi Penelitian.....	28
3.3.1.	Metode Pengumpulan Data.....	28
3.3.2.	Metode Kuesioner atau Angket.....	28
3.3.3.	Simple Random Sampling	29
3.3.4.	Metode Analisis Data.....	29
3.4.	Analisis Permasalahan	29
3.5.	Solusi Yang Ditawarkan	30
3.6.	Alat dan Bahan.....	31
3.4.1.	Alat.....	31
3.4.2.	Bahan	31
BAB IV	HASIL DAN PEMBAHASAN	33
4.1.	Analisis Aplikasi Telegram Mod Menggunakan Mobile Security Framework.....	33
4.1.1.	Analisis Perizinan Aplikasi.....	33
4.1.2.	Analisis Manifest	39
4.1.3.	Analisis Kode.....	47
4.1.4.	Analisis NIAP	53
4.2.	Analisis Aplikasi Telegram Mod Menggunakan Yaazhini.....	58
4.2.1.	Analisis Celah Kerentanan.....	59
4.3.	Hasil Penelitian	64
4.3.1.	Jenis Kelamin.....	64
4.3.2.	Usia	64
4.4.	Deskripsi Jawaban Responden.....	65
4.4.1.	Variabel A	68
4.4.2.	Variabel B	68
4.4.3.	Variabel C	69
4.4.4.	Variabel D	70
4.5.	Analisis Data.....	70
4.5.1.	Uji Validitas	70
4.5.2.	Uji Reliabilitas	72
4.5.3.	Uji Normalitas.....	73
4.6.	Hasil Analisis.....	75
4.6.1.	Persentase Variabel A	75
4.6.2.	Persentase Variabel B	77
4.6.3.	Persentase Variabel C	78
4.6.4.	Persentase Variabel D	80
BAB V	PENUTUP	82
5.1.	Kesimpulan	82
5.2.	Saran	83
REFERENSI	84
LAMPIRAN	87

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	9
Tabel 3. 1 Masalah pada objek penelitian.....	29
Tabel 3. 2 Daftar solusi	30
Tabel 3. 3 Alat penelitian.....	31
Tabel 3. 4 Bahan penelitian.....	31
Tabel 4. 1 Hasil analisis perizinan aplikasi pada MobSF	33
Tabel 4. 2 Keterangan <i>permission</i> pada analisis perizinan aplikasi.....	35
Tabel 4. 3 Hasil analisis Manifest pada MobSF	39
Tabel 4. 4 Keterangan <i>issue</i> pada analisis Manifest	42
Tabel 4. 5 Hasil analisis kode pada MobSF.....	47
Tabel 4. 6 Hasil analisis NIAP pada MobSF	53
Tabel 4. 7 Keterangan pengidentifikasi pada analisis NIAP	55
Tabel 4. 8 Hasil analisis kerentanan pada Yaazhini	59
Tabel 4. 9 Keterangan nama kerentanan pada Yaazhini.....	60
Tabel 4. 10 Usia responden.....	64
Tabel 4. 11 Nilai hasil jawaban responden	65
Tabel 4. 12 Rata-rata variabel A	68
Tabel 4. 13 Rata-rata variabel B	68
Tabel 4. 14 Rata-rata variabel C	69
Tabel 4. 15 Rata-rata variabel D	70
Tabel 4. 16 Hasil uji validitas	72
Tabel 4. 17 Hasil uji reliabilitas	73
Tabel 4. 18 Hasil uji normalitas	74
Tabel 4. 19 Skor jawaban variabel A	76
Tabel 4. 20 skor jawaban variabel B.....	77
Tabel 4. 21 Skor jawaban variabel C	79
Tabel 4. 22 Skor jawaban variabel D.....	80

DAFTAR GAMBAR

Gambar 1. 1 Statistika aplikasi perpesanan paling populer.	1
Gambar 3. 1 Ikon Telegram	23
Gambar 3. 2 Halaman web Plus Messenger pada situs apkpure.com.....	24
Gambar 3. 3 Halaman web Telegram X pada situs apkloo.com.....	25
Gambar 3. 4 Alur penelitian.....	26
Gambar 4. 1 Jenis kelamin responden	64
Gambar 4. 2 Distribusi nilai r tabel signifikansi 5% dan 1%.....	71



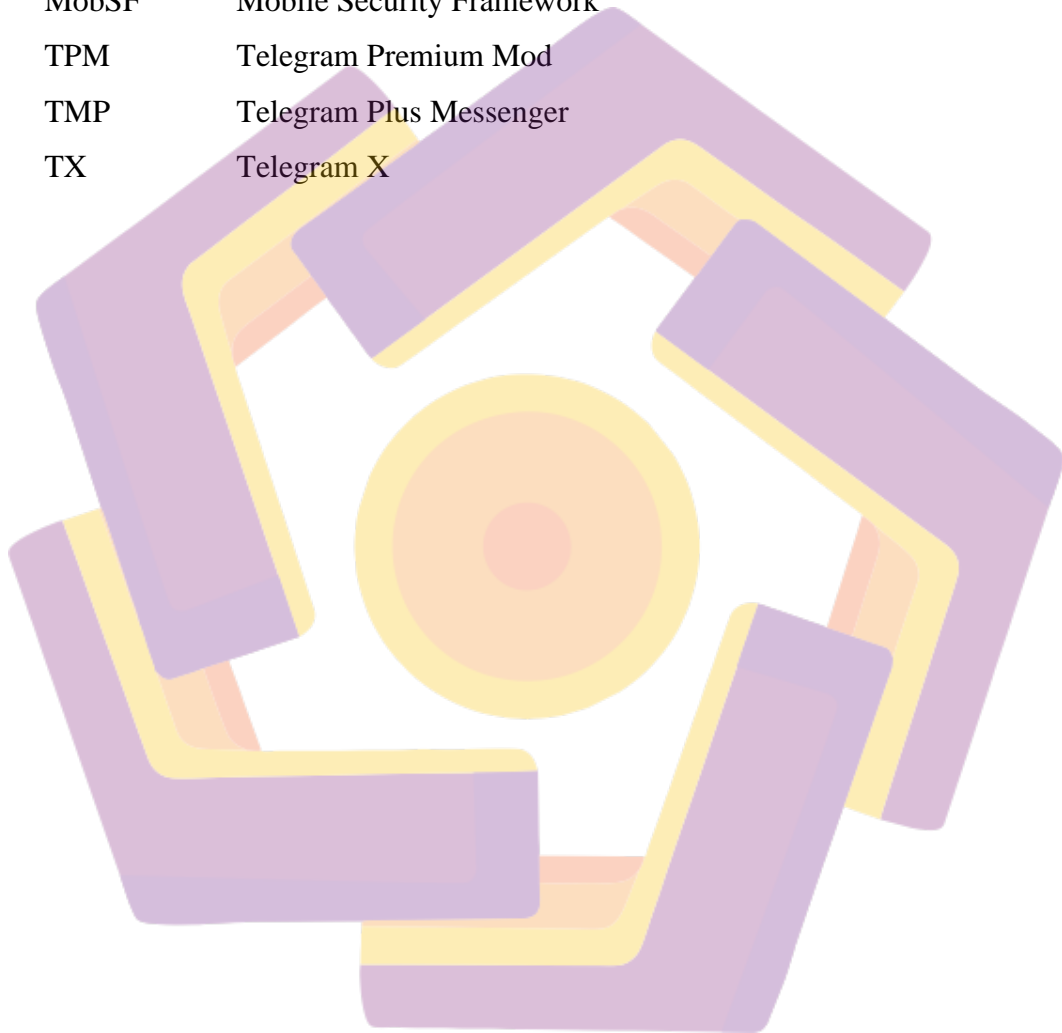
DAFTAR LAMPIRAN

Lampiran 1 Pertanyaan kuesioner penelitian	87
Lampiran 2 Respons kuesioner penelitian	92
Lampiran 3 <i>Dataset</i> hasil kuesioner penelitian.....	98
Lampiran 4 Log <i>output</i> hasil uji validitas	101
Lampiran 5 Log <i>output</i> hasil uji reliabilitas.....	103
Lampiran 6 Log <i>output</i> hasil uji normalitas.....	107
Lampiran 7 Laporan analisis statis Telegram Mod Premium - MobSF.....	108
Lampiran 8 Laporan analisis statis Telegram Plus Messenger - MobSF.....	124
Lampiran 9 Laporan analisis statis Telegram X - MobSF.....	142
Lampiran 10 Laporan analisis statis Telegram Mod Premium - Yaazhini	154
Lampiran 11 Laporan analisis statis Telegram Plus Messenger - Yaazhini	160
Lampiran 12 Laporan analisis statis Telegram X - Yaazhini.....	167



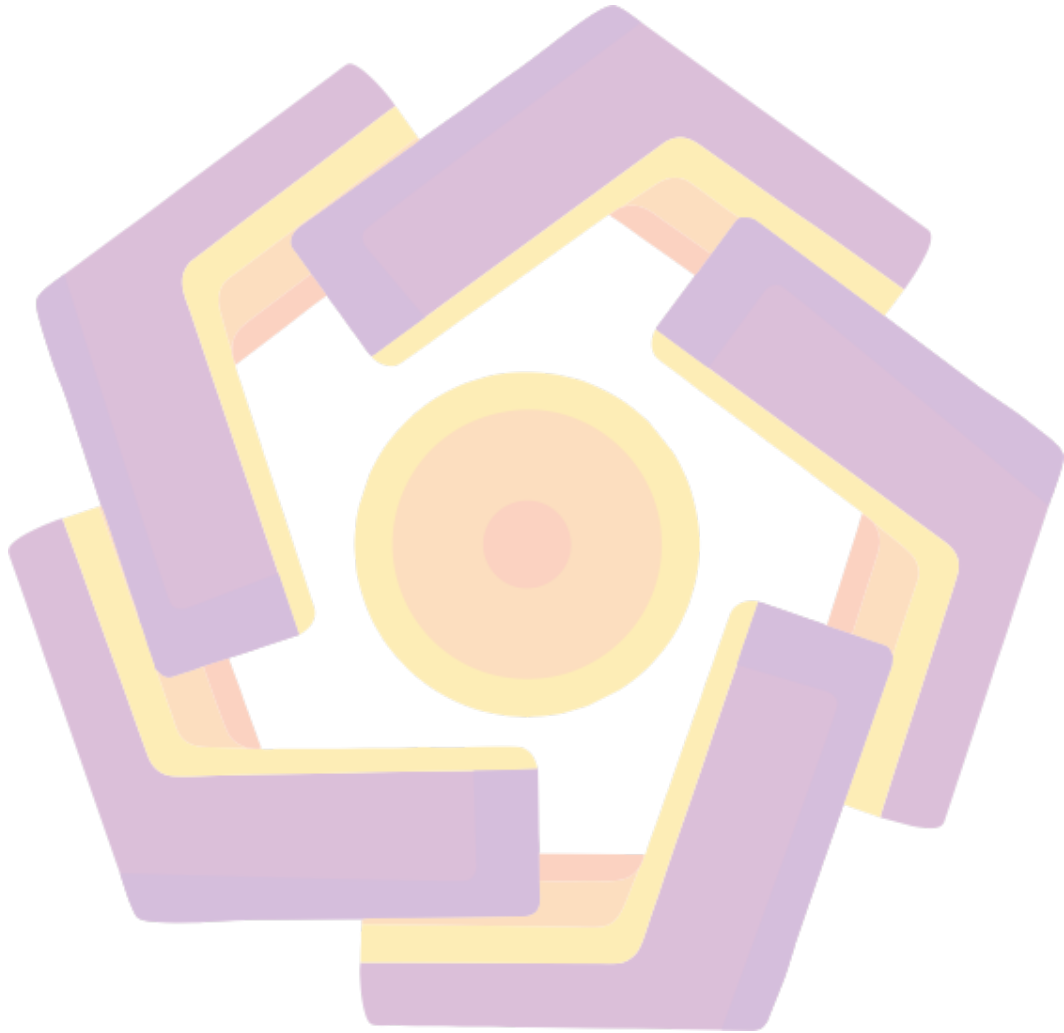
DAFTAR LAMBANG DAN SINGKATAN

Σsk	Nilai kriterium
$\Sigma variabel$	Jumlah item pertanyaan pada setiap variabel
ΣN	Jumlah responden yang ada
MobSF	Mobile Security Framework
TPM	Telegram Premium Mod
TMP	Telegram Plus Messenger
TX	Telegram X



DAFTAR ISTILAH

Modder Seseorang yang melakukan modifikasi pada sebuah aplikasi



INTISARI

Semakin pesat perkembangan teknologi membuat pengguna teknologi semakin meningkat pula dan dampak dari teknologi tersebut akan lebih cepat tersebar. Keamanan teknologi informasi yang ada ini dapat tersebar dan diakses oleh orang yang tidak bertanggung jawab dengan memanfaatkan celah keamanan pada setiap media informasi, salah satunya adalah aplikasi yang ada di perangkat *mobile*. Android merupakan salah satu dari sekian banyak sistem operasi yang paling banyak digunakan perangkat *mobile* dengan fitur dan dukungan berbagai aplikasi untuk memudahkan aktivitas pada kehidupan manusia. Salah satu celah yang memungkinkan terjadinya *cybercrime* ialah dengan memanfaatkan aplikasi Android yang tidak resmi di mana aplikasi tersebut memiliki fitur yang lebih baik yang tidak ditawarkan oleh pengembang resmi sehingga pengguna akan lebih tertarik menggunakannya. Peneliti akan mengambil contoh aplikasi Telegram mod sebagai objek penelitian dikarenakan aplikasi tersebut memiliki versi premium namun bisa diunduh secara *free* di internet. Tujuan penelitian ini adalah bagaimana kesimpulan terkait kesadaran pengguna aplikasi mod terhadap keamanan informasi serta penggunaan Mobile Security Framework (MobSF) dan Yaazhini sebagai metode analisis statis pada beberapa aplikasi Telegram Mod. Sampel aplikasi akan diambil melalui internet dan dianalisis, kemudian *output* analisis akan dibuat menjadi sebuah *report*. Hasil analisis statis pada penelitian ini, beberapa Telegram mod terdapat beberapa *permission* yang memiliki status *dangerous* pada analisis menggunakan Mobile Security Framework serta terdeteksi beberapa celah keamanan seperti *insecure communication*, *Android backup vulnerability*, *Weak hash - SHA-1*, dan lain-lain pada analisis Yaazhini.

Kata kunci: Android, Mobile Security Framework, Yaazhini, Analisis statis, Telegram

ABSTRACT

The faster the development of technology makes the users of technology also increase and the impact of this technology will spread more quickly. The security of existing information technology can be spread and accessed by irresponsible people by exploiting security holes in any information media, one of which is an application on a mobile device. Android is one of the most widely used operating systems for mobile devices with features and support for various applications to facilitate activities in human life. One of the loopholes that allows cybercrime to occur is by utilizing unofficial Android applications where these applications have better features that are not offered by official developers so that users will be more interested in using them. Researchers will take the example of the Telegram mod application as an object of research because the application has a premium version but can be downloaded for free on the internet. The purpose of this study is to draw conclusions regarding the awareness of mod application users towards information security and the use of the Mobile Security Framework (MobSF) and Yaazhini as static analysis methods in several Telegram Mod applications. Application samples will be taken via the internet and analyzed, then the analysis output will be made into a report. The results of the static analysis in this study, some Telegram mods have several permissions that have dangerous status on analysis using the Mobile Security Framework and several security holes have been detected such as insecure communication, Android backup vulnerability, Weak hash - SHA-1, etc. on Yaazhini's analysis.

Keyword: *Android, Mobile Security Framework, Yaazhini, Static analysis, Telegram*