

TUGAS AKHIR

**ANALISIS *MALWARE* KWETZA MENGGUNAKAN
METODE *REVERSE ENGINEERING***



KHUSNUL FAUZIAH

20102001

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024**

TUGAS AKHIR

**ANALISIS *MALWARE* KWETZA MENGGUNAKAN
METODE *REVERSE ENGINEERING***

***ANALYSIS OF KWETZA MALWARE USING THE
REVERSE ENGINEERING METHOD***

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer



KHUSNUL FAUZIAH

20102001

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024**

LEMBAR PERSETUJUAN PEMBIMBING

**ANALISIS *MALWARE* KWETZA MENGGUNAKAN
METODE *REVERSE ENGINEERING***

***ANALYSIS OF KWETZA MALWARE USING THE
REVERSE ENGINEERING METHOD***

Dipersiapkan dan Disusun Oleh

KHUSNUL FAUZIAH

20102001

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 1 April 2024

Pembimbing Utama,



(Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom)

NIDN. 0613038503

LEMBAR PENGESAHAN TUGAS AKHIR

**ANALISIS *MALWARE* KWETZA MENGGUNAKAN
METODE *REVERSE ENGINEERING***

***ANALYSIS OF KWETZA MALWARE USING THE
REVERSE ENGINEERING METHOD***

Disusun Oleh

KHUSNUL FAUZIAH

20102001

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir
Pada Hari Rabu, 24 April 2024

Penguji I,



Trihastuti Yuniati, S.Kom., M.T.

NIDN. 0602068902

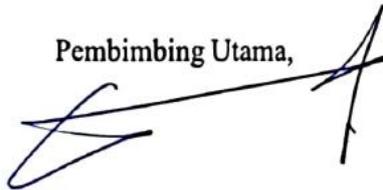
Penguji II,



Gunawan Wibisono, S.Kom, M.Kom.

NIDN. 0601018601

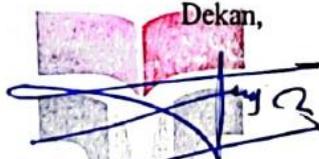
Pembimbing Utama,



Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom.

NIDN. 0613038503

Dekan,



Auliya Burhanuddin, S.Si., M.Kom.

NIK. 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Khusnul Fauziah
NIM : 20102001
Program Studi : S1 Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:

ANALISIS *MALWARE* KWETZA MENGGUNAKAN METODE *REVERSE ENGINEERING*

Dosen Pembimbing Utama : Wahyu Adi Prabowo, S.Kom., M.B.A.,
M.Kom

Dosen Pembimbing Pendamping : -

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim 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 tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian 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.

Purwokerto, 1 April 2024,

Yang Menyatakan


C133FALX042943229
(Khusnul Fauziah)

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadiran Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga peneliti dapat menyelesaikan penyusunan skripsi dengan judul “Analisis *Malware* Kwetza Menggunakan Metode *Reverse Engineering*” sebagai salah satu persyaratan yang harus dipenuhi untuk menyelesaikan Pendidikan tingkat Sarjana Komputer pada Fakultas Informatika Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, tidak terlepas dari dukungan dan bantuan dari berbagai pihak selama ini. Oleh karena itu, pada kesempatan ini peneliti mengucapkan terimakasih kepada:

1. Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan dengan baik;
2. Kedua orang tua peneliti, Bapak Fahrudin dan Ibu Suci Purwaningsih yang telah memberikan do'a, dukungan dan motivasi secara terus-menerus sehingga peneliti mampu menyelesaikan studinya sampai sarjana;
3. Dr. Tenia Wahyuningrum, S.Kom., M.T selaku Rektor Institut Teknologi Telkom Purwokerto;
4. Auliya Burhanuddin, S.Si., M.Kom selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto;
5. Amalia Belandinna Arifa, S.Pd., M.Cs selaku Ketua Program Studi S1 Informatika;
6. Wahyu Adi Prabowo, S.Kom.,M.B.A.,M.Kom selaku dosen pembimbing pertama yang senantiasa memberikan pengarahan dan dukungan dalam menyelesaikan tugas akhir ini;
7. Seluruh dosen dan karyawan Institut Teknologi Telkom Purwokerto yang telah memberikan banyak kesempatan, tempat dan waktu pada peneliti dalam menyelesaikan studi di Institut Teknologi Telkom Purwokerto;
8. Kedua adik peneliti, Dilla Safira dan Irham Aris Arhama yang telah memberikan semangat dan menjadi *mood booster* peneliti;

9. Seluruh Keluarga Besar yang telah memberikan doa dan dukungannya;
10. Afa Salsabila Nahrowi yang telah menjadi rekan seperjuangan dalam penyusunan skripsi dan memberikan motivasi serta dukungan;
11. Ramadan Muhammad Wildan yang selalu mendukung, mendoakan dan memberikan semangat serta selalu menemani dalam penyusunan laporan penelitian;
12. Teman – teman peneliti, terutama Niken Pratiwi, Alyssa Diva Risana Fauziah, Atifah Herawati yang telah memberikan dukungan dan semangat.

Peneliti menyadari bahwa masih banyak kekurangan dalam penyusunan skripsi ini, sehingga kritik dan saran yang membangun sangat diharapkan. Akhir kata, peneliti berharap semoga skripsi ini dapat bermanfaat dan membantu menambah pengetahuan bagi yang membutuhkan.

Purwokerto, 1 April 2024



Khusnul Fauziah

DAFTAR ISI

TUGAS AKHIR.....	ii
LEMBAR PERSETUJUAN PEMBIMBING.....	iii
LEMBAR PENGESAHAN TUGAS AKHIR.....	iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR SINGKATAN.....	xii
DAFTAR LAMPIRAN.....	xiii
ABSTRAK.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	4
1.3. Pertanyaan Penelitian.....	4
1.4. Tujuan Penelitian.....	4
1.5. Batasan Masalah.....	4
1.6. Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA.....	6
2.1. Penelitian Terkait.....	6
2.2. Dasar Teori.....	14
2.2.1. <i>Malware</i>	14
2.2.2. <i>Kwetza</i>	15
2.2.3. <i>Reverse Engineering</i>	15
2.2.4. <i>Mobile Security Framework (MobSF)</i>	16
2.2.5. <i>Metasploit</i>	16
2.2.6. <i>Exploit</i>	18
2.2.7. <i>Backdoor</i>	18
2.2.8. <i>Payload</i>	19
2.2.9. <i>Meterpreter</i>	19

2.2.10. Signal Messenger	20
2.2.11. Kali Linux	20
2.2.12. JADX	21
BAB III METODOLOGI PENELITIAN.....	23
3.1. Objek dan Subjek Penelitian	23
3.2. Alat dan Bahan Penelitian	23
3.3. Diagram Alur Penelitian.....	24
3.3.1. Identifikasi Masalah	25
3.3.2. Studi Literatur	25
3.3.3. Tahap Pengujian.....	26
3.3.4. Tahap Pengujian.....	33
BAB IV HASIL DAN PEMBAHASAN	35
4.1. Hasil Instalasi Pada Versi Android	35
4.1.1. Hasil Instalasi Pada Android Versi 12 Dengan MIUI 13.0.5.....	35
4.1.2. Hasil Instalasi Pada Android Versi 10 Dengan MIUI 12.5.3.....	36
4.2. Hasil <i>Exploit</i>	36
4.3. Hasil Analisis Statis Menggunakan MobSF.....	38
4.3.1. <i>Security Score</i>	38
4.3.2. <i>Analisis Permission</i>	39
4.3.3. <i>Analisis Source Code</i>	43
4.4. Hasil Analisis Manual Menggunakan JADX	45
4.4.1. <i>Analisis Permission</i>	46
4.4.2. META-INF.....	48
4.4.3. <i>Analisis Source Code</i>	49
4.5. Perbandingan Analisis Manual dan Analisis Otomatis	56
BAB V.....	59
KESIMPULAN DAN SARAN.....	59
5.1. Kesimpulan.....	59
5.2. Saran	60
DAFTAR PUSTAKA	61
LAMPIRAN.....	65

DAFTAR GAMBAR

Gambar 1. 1 Data Pengguna Versi Android Menurut StatCounter.....	1
Gambar 1. 2 Jumlah Sampel Malware Yang Terdeteksi Menurut Data Kaspersky Security Network	2
Gambar 3. 1 Diagram Alur Penelitian.....	25
Gambar 3. 2 Menyisipkan Malware.....	27
Gambar 3. 3 Exploit.....	28
Gambar 3. 4 Tahap Reverse Engineering	34
Gambar 4. 1 Instalasi Pada Android Versi 12 Dengan MIUI 13.0.5.	35
Gambar 4. 2 Instalasi Pada Android Versi 10 Dengan MIUI 12.5.3	36
Gambar 4. 3 <i>Security Score</i> Pada Aplikasi Sebelum Disusupi <i>Malware</i>	39
Gambar 4. 4 <i>Security Score</i> Pada Aplikasi Sesudah Disusupi <i>Malware</i>	39
Gambar 4. 5 Sampel <i>Permission</i> MobSF Sebelum Disusupi <i>Malware</i>	40
Gambar 4. 6 Sampel <i>Permission</i> MobSF Sesudah Disusupi <i>Malware</i>	41
Gambar 4. 7 Sebelum Disusupi <i>Malware</i>	44
Gambar 4. 8 Penambahan File <i>SaveAttachmentUtil.java</i> Sesudah Disusupi <i>Malware</i>	44
Gambar 4. 9 Sebelum Disusupi <i>Malware</i>	44
Gambar 4. 10 Penambahan Kode Pada <i>Class QrCameraView.java</i> Sesudah Disusupi <i>Malware</i>	44
Gambar 4. 11 Penambahan Kode Pada <i>Class Camera1Controller.java</i> Sesudah Disusupi <i>Malware</i>	45
Gambar 4. 12 Sampel <i>Permission</i> Manual Sebelum Disusupi <i>Malware</i>	46
Gambar 4. 13 Sampel <i>Permission</i> Manual Sesudah Disusupi <i>Malware</i>	47
Gambar 4. 14 Penambahan <i>Class</i> Pada Aplikasi Yang Sudah Disusupi <i>Malware</i>	49
Gambar 4. 15 Fungsi Pertama Pada <i>Class AssistActivity</i>	50
Gambar 4. 16 Fungsi Kedua Pada <i>Class AssistActivity</i>	50
Gambar 4. 17 Fungsi Ketiga Pada <i>Class AssistActivity</i>	51
Gambar 4. 18 Fungsi Keempat Pada <i>Class AssistActivity</i>	51
Gambar 4. 19 Fungsi Kelima Pada <i>Class AssistActivity</i>	51
Gambar 4. 20 Fungsi Keenam Pada <i>Class AssistActivity</i>	52
Gambar 4. 21 Fungsi Ketujuh Pada <i>Class AssistActivity</i>	53
Gambar 4. 22 Fungsi Pada <i>Class AssistActivity1</i>	54
Gambar 4. 23 Penambahan Kode Pertama Pada <i>Class MainActivity</i>	55
Gambar 4. 24 Penambahan Kode Kedua Pada <i>Class MainActivity</i>	56

DAFTAR TABEL

Tabel 2.1. Penelitian Terkait	10
Tabel 3. 1 Kebutuhan Perangkat Keras	23
Tabel 3. 2 Kebutuhan Perangkat Lunak	24
Tabel 3. 3 Command Menu	29
Tabel 3. 4 <i>File System Commands</i>	30
Tabel 3. 5 Networking Commands	30
Tabel 3. 6 System Commands	31
Tabel 3. 7 User Interface Commands	31
Tabel 3. 8 Webcam Commands	32
Tabel 3. 9 Audio Output Commands	32
Tabel 3. 10 Android Commands	32
Tabel 3. 11 Application Controller Commands	33
Tabel 4. 1 Sampel <i>Android Commands</i> Yang Telah Diuji Coba	36
Tabel 4. 2 Penambahan Permission Sesudah Disusupi Malware Pada MobSF	41
Tabel 4. 3 Penambahan Permission Manual Sesudah Disusupi Malware	47
Tabel 4. 4 Perubahan META-INF	48
Tabel 4. 5 Perbandingan Hasil Analisis	56

DAFTAR SINGKATAN

<i>MOBSF</i>	= <i>Mobile Security Framework</i>
<i>APK</i>	= <i>Android Package Kit</i>
<i>RAT</i>	= <i>Remote Access Trojan</i>
<i>TCP</i>	= <i>Transmission Control Protocol</i>
<i>HTML</i>	= <i>HyperText Markup Language</i>
<i>XML</i>	= <i>Extensible Markup Language</i>
<i>API</i>	= <i>Application Programming Interface</i>
<i>KB</i>	= <i>Kilobyte</i>

DAFTAR LAMPIRAN

Lampiran 1 Instalasi dan Konfigurasi Sistem	65
Lampiran 2 Menyisipkan Malware	65
Lampiran 3 File kwetza.py.....	67
Lampiran 4 Proses Exploit.....	77
Lampiran 5 Hasil Exploit.....	77
Lampiran 6 Permission yang Didapatkan Pada Analisis Manual Sebelum Disusupi Malware.....	81
Lampiran 7 Permission yang Didapatkan Pada Analisis Manual Sesudah Disusupi Malware.....	83
Lampiran 8 Permission yang Didapatkan Pada MobSF Sebelum Disusupi Malware.....	85
Lampiran 9 Permission yang Didapatkan Pada MobSF Sesudah Disusupi Malware	87
Lampiran 10 Penambahan Class AssistActivity Pada Analisis Manual Sesudah Disusupi Malware	89
Lampiran 11 Penambahan Class AssistActivity1 Pada Analisis Manual Sesudah Disusupi <i>Malware</i>	91
Lampiran 12 Penambahan Kode Pertama Pada Class MainActivity Sesudah Disusupi Malware	92
Lampiran 13 Penambahan Kode Kedua Pada Class MainActivity Sesudah Disusupi Malware	93
Lampiran 14 Penambahan Kode Pada MobSF Sesudah Disusupi Malware.....	94
Lampiran 15 Cek Plagiarisme	103