BAB V
KESIMPULAN DAN SARAN

1.1. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dijelaskan pada BAB sebelumnya, maka dapat disimpulkan bahwa:

1. Perilaku *malware* kwetza setelah terpasang pada aplikasi adalah sebagai berikut:
   a. Aplikasi yang sudah disusupi *malware* kwetza tidak bisa terpasang pada Android versi 12, tetapi bisa terpasang pada Android versi 10.
   b. Setelah terpasang, aplikasi yang sudah disusupi *malware* kwetza dapat melakukan berbagai perintah seperti *check_root, dump_sms, dump_calllog, dump_contacts, geolocate* dan *hide_app_icon.*
   c. Kemampuan *malware* kwetza adalah dapat membuka aplikasi sendiri atau beralih antara aplikasi tanpa interaksi langsung dari pengguna. Hal ini bisa menjadi pertanda atau gejala yang jelas bahwa sesuatu yang tidak wajar terjadi pada perangkat.
2. Terjadi perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware* yaitu sebagai berikut:
   a. Pada analisis manual bagian META-INF terdapat perubahan penandatanganan dari CERTIFIC.SF menjadi ALIAS_NA.SF.
   b. *Permission* yang diperoleh pada pengujian secara manual dan otomatis menggunakan MobSF memiliki kesamaan dengan penambahan tiga *permission* yaitu *WRITE_SETTINGS, READ_CALL_LOG*, dan *ACCESS_COURSE LOCATION.*
   c. Pada analisis secara manual terdapat penambahan *class* pada folder *classes4.dex* dengan nama AssistActivity dan AssistActivity1. Kode pada *class* tersebut digunakan untuk melakukan komunikasi jarak jauh dengan perangkat, termasuk pembacaan dan penulisan file,

d. koneksi jaringan TCP, serta untuk memuat dan menjalankan *class* dinamis pada saat *runtime.*
e. Pada analisis menggunakan MobSF ditemukan penambahan kode yang melibatkan objek kamera, namun MobSF tidak dapat mendeteksi *class* AssistActivity dan AssistActivity1 yang berisi *malware*.

1.2. Saran

1. Untuk penelitian selanjutnya dapat menggunakan *tools* selain Kwetza, untuk melakukan penyisipan *malware*.
2. Pada penelitian berikutnya melakukan pengujian menggunakan aplikasi selain Signal Messenger.