BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Hasil riset dan pembahasan sebelumnya telah dijabarkan. Berikut hasil kesimpulan dari penelitian ini:

1. Terdapat perubahan kode sebelum dan sesudah disisipi *malware* yaitu telah melakukan analisis otomatis dan menemukan file perubahan pada *CameraView* yang berfungsi untuk memberikan akses diluar kamera setelah disisipi *malware*. Ketika melakukan analisis JADX secara manual terdapat penambahan *class* sesudah disisipi *malware* berkaitan dengan classes.dex yaitu a, b, c, d, e, f, g, *MainBroadcastReceiver*, *MainService* dan *Payload* yang merupakan bagian dari *backdoor*. Terdapat 3 *class* inti yaitu *MainBroadcastReceiver, MainService* dan *Payload.* Kode yang berfungsi untuk tetap terjaga saat mengontrol aplikasi saat melakukan komunikasi jarak jauh dengan perangkat, termasuk pembacaan dan penulisan *file*, koneksi jaringan dan menonaktifkan *launcher activity.*
2. MobSF dapat mengidentifikasi dari perizinan yang didapatkan melalui uji coba manual dan otomatis terdapat kesamaan 7 penambahan *permissions* yaitu SEND_SMS, RECEIVE_SMS, READ_SMS, WRITTE_SETTINGS, SET_WALLPAPER, WRITE_CALL_LOG, dan RECORD_AUDIO. MobSF menemukan 2 penambahan *file* yaitu file f dan *payload* terdapat pada *folder* org/telegram/messenger/stage yang berkaitan dengan *malware* tetapi MobSF tidak dapat menemukan keseluruhan penambahan *file* yang berkaitan dengan *malware* setelah di *scanning.*

5.2 Saran

1. Penelitian berikutnya, beberapa *tools* lainnya dapat digunakan untuk menyisipkan *malicious software*.
2. Dapat melaksanakan uji coba dengan Android versi terbaru.
3. Dapat menggunakan *tools* versi terbaru.
4. Dapat menggunakan jaringan yang berbeda.
5. Mendapatkan notifikasi/*pop up* ketika telegram dibuka oleh *user*.