# BAB 6

# KESIMPULAN DAN SARAN

## 6.1 Kesimpulan

Berikut adalah beberapa kesimpulan yang didapat setelah melakukan penelitian :

1. Perangkat lunak untuk mendeteksi *malware* menggunakan pendekatan *Grayscale Image* dan *Entropy Graph* berhasil dibangun dengan nilai batasan yang optimal adalah 60 yang didapat dari hasil pengujian beberapa dataset menggunakan variasi jumlah data dan nilai batas yang berbeda.
2. Setelah melakukan berbagai macam pengujian, ternyata didapatkan bahwa jika ukuran file yang digunakan untuk pembanding dan juga file yang diunggah jika memiliki selisih ukuran yang besar, akan mungkin terjadi kesalahan saat penentuan hasil akhir dan juga persentase kemiripan.
3. Pada hasil dari pengujian, keseluruhan dari perangkat lunak berjalan sesuai keinginan dan tidak ada bug.

## 6.2 Saran

Setelah menyelesaikan pengembangan perangkat lunak dan juga penelitian, ada beberapa saran untuk pengembangan perangkat lunak selanjutnya yaitu :

1. Jumlah dari file pembanding yang disediakan pada bank *malware* sebisa mungkin sama rasionya, seperti jika terdapat 50 buah file *malware*, harus ada juga 50 buah file non-*malware* dan juga sebisa mungkin diperbanyak agar akurasi semakin akurat.
2. Sebisa mungkin ukuran data dalam bank *malware* dan juga non *malware* memiliki distribusi yang rata.
3. Perhitungan *similarity* hanya berdasarkan pada *Entropy Graph* dan *Grayscale Image*, mungkin akan lebih baik jika proses perhitungan *similarity* digabungkan dengan proses pendeteksian *malware* dengan menggunakan pendekatan yang lain.

# DAFTAR REFERENSI


[1] Elisan, C. C. (2012) *Malware, Rootkits & Botnets A Beginner's Guide*. McGraw Hill Professional, Atlanta, Georgia.

[2] Mohanta, A. dan Saldanha, A. (2020) *Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware*. Apress Berkeley, CA, New York, USA.

[3] Gholizadeh, S. (2022) Top popular python libraries in research. *Authorea Preprints*, **3**, 142–145.

[4] Landage, J. dan Wankhade, M. (2013) Malware and malware detection techniques: A survey. *International Journal of Engineering Research*, **2**, 61–68.

[5] Aycock, J. (2006) *Computer Viruses and Malware*. Springer New York, NY, Calgary, Canada.

[6] Chun, W. (2001) *Core python programming*. Prentice Hall Professional, Upper saddle river, New Jersey.

[7] Nataraj, L., Karthikeyan, S., Jacob, G., dan Manjunath, B. S. (2011) Malware images: Visualization and automatic classification. *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, New York, NY, USA, 20 July VizSec '11, pp. 1–7. Association for Computing Machinery.

[8] Han, K. S., Lim, J. H., Kang, B., dan Im, E. G. (2015) Malware analysis using visualized images and entropy graphs. *International Journal of Information Security*, **14**, 1–14.

[9] Lahitani, A. R., Permanasari, A. E., dan Setiawan, N. A. (2016) Cosine similarity to determine similarity measure: Study case in online essay assessment. *2016 4th International Conference on Cyber and IT Service Management*, Bandung, Indonesia, 26-27 April, pp. 1–6. 2016 4th International Conference on Cyber and IT Service Management.