BAB 1
Pendahuluan

1.1 Latar Belakang

Malware merupakan program yang sengaja dibuat untuk membahayakan dan merugikan sistem operasi atau data pada komputer (Siddiqui, 2008). Langkah untuk deteksi terhadap serangan malware telah dilakukan dengan menerapkan metode-motode terkini yang dirasa mampu untuk deteksi malware masuk dan merusak sistem, salah satu metode tersebut adalah *behavior based detection*.

Pendeteksian malware berbasis *behaviour based detection* adalah metode deteksi malware berdasarkan pengamatan secara terus-menerus terhadap perilaku aplikasi untuk menentukan apakah perilaku itu berbahaya atau tidak (Alqurashi & Batarfi, 2016), dalam metode ini perilaku malware dan program biasa dipelajari dan dilakukan pemantauan serta analisis, setelah itu hasil analisis dapat dijadikan acuan bahwa suatu program dapat dikategorikan sebagai malware jika memiliki perilaku yang meyimpang dari perilaku normal program pada umumnya.

Metode pendeteksian malware yang umum digunakan saat ini adalah *signature based*, metode ini digunakan pada *tools* anti virus saat ini, dalam metode ini terdapat dua teknik yang biasa digunakan yaitu *byte pattern* dan file *checksum* atau nilai *hash.*

Secara umum metode pendeteksian malware dibagi menjadi dua yaitu, *Signature-Based* dan *Behavior-Based* menurut (Deylami, Muniyandi, Ardekani, & Sarrafzadeh, 2016), dan sebagian besar *tools* keamanan khususnya *tool* anti malware saat ini masih menggunakan metode pendeteksian berbasis *signature-based* (Preda, Christodorescu, Jha, & Debray, 2008). Selain kedua metode tersebut terdapat satu metode lainnya yang dapat digunakan untuk mendeteksi malware yaitu *Statistical Based Detection,* hal ini sebagaimana disampaikan oleh (Damodaran, 2015).

Tabel 1. 1 Kelebihan dan kekurangan signature dan behavior

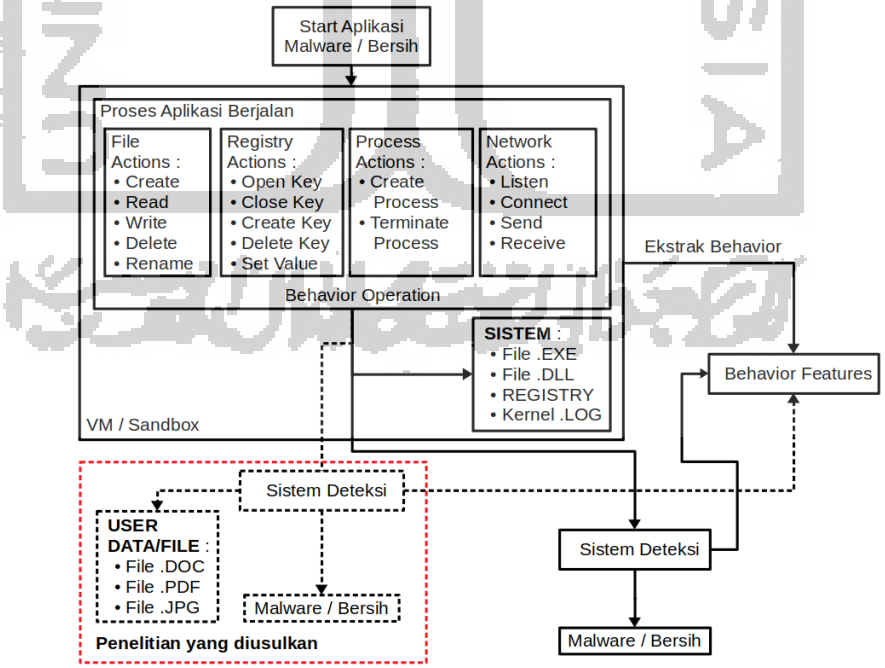
No	*Signature Detection Method*		*Behavior Detection Method*	
	Kelebihan	**Kekurangan**	**Kelebihan**	**Kekurangan**
1.	Mudah dijalankan	Gagal untuk mendeteksi polimorfik malware	Dapat mendeteksi polimorfik malware	Kompleksitas penyimpanan untuk pola *behavior*

Tabel 1. 2 Kelebihan dan kekurangan signature dan behavior (Lanjutan)

No	*Signature Detection Method*		*Behavior Detection Method*	
	Kelebihan	**Kekurangan**	**Kelebihan**	**Kekurangan**
2.	Cepat indentifikasi	Informasi disimpan dalam database yang sangat besar	Dapat mendeteksi jenis serangan malware yang tak dipahami	Kompleksitas waktu
3.	Dapat diakses secara luas		Dapat mendeteksi ketergantungan aliran-data	

(Souri & Hosseini, 2018)

Dalam sistem operasi Windows, proses merupakan dasar dari sebuah unit eksekusi dan juga inisiator dari suatu *behavior*. Dalam penjelasannya (Liu, Ren, Liu, & Duan, 2011) menyebutkan bahwa *behavior operations* merupakan operasi dasar yang menyebabkan adanya perubahan pada status sistem oleh sebuah perangkat lunak, seperti membuat file, mengubah registry, membuat proses, dan sebagainya. Selain *behavior operations* hal lain yang menjadi bagian dari proses adalah *target behavior operations*, yaitu target operasi seperti file sistem, registry, port jaringan dan sebagainya, sistem merupakan target operasi pada umumnya. Gambar 1 dibawah menjelaska 4 (empat) *behavior operations* yang menjadi acuan untuk meng-ekstrak *behavior features* yaitu data *behavior* yang digunakan untuk deteksi malware berdasarkan kesamaan *features*, dan juga menjelaskan beberapa penelitian yang sudah ada dan yang akan diusulkan pada penelitan ini.



Gambar 1.1 Gambaran penelitian yang sudah ada dan yang akan diusulkan.

(Liu et al., 2011), (Veeramani & Rai, 2012)

Penelitian yang berkembang saat ini lebih fokus pada *behavior operation* dimana sistem sebagai *target behavior operations*, contoh penelitian yang dilakukan oleh (Kheir, 2013), penelitian ini membahas tentang klasifikasi dan deteksi malware berdasarkan perilaku tidak normal pada *header user agent* yang melakukan *reques* ke server pada trafik jaringan. Dalam penelitian ini *target behavior operation* adalah system dengan *behavior features* yang diekstrak lebih pada bagian *network action* dari *behavior operations*. Penelitian lainnya yang dilakukan oleh (Berlin, Slater, & Saxe, 2015) adalah deteksi malware *behavior* dengan menggunakan fasilitas bawaan pada sistem operasi Windows yaitu *Windows Audit Logs*, sama halnya dengan penelitian sebelumnya, sistem merupakan *target behavior operations* dan *behavior features* diekstrak dari *behavior operations* melalui analisis menggunakan *virtual sandbox* yang telah dikonfigurasi sedemikian rupa, sehingga informasi yang ditemukan pada *audit logs* menurut peneliti ini cukup untuk deteksi malware.

Namun sayangnya penelitian berbasis *behavior approach* untuk deteksi malware yang ada saat ini dan dari penelitan-penelitian yang disampaikan diatas tidak membahas secara spesifik tentang data user seperti file .docx, .pdf dan .jpeg sebagain *target behavior operations* padahal, beberapa tahun belakangan malware yang menjadi topik utama dalam dunia keamanan komputer adalah malware yang manargetkan data user sebagai sasaran seperti ransomware. Oleh sebab itu diperlukan sebuah penelitian yang membahas secara spesifik deteksi malware berbasi *behavior approach* dimana perilaku aplikasi terhadap data dalam hal ini sebagai *target behavior operations* dapat digunakan sebagai cara deteksi malware.

Dalam penelitian ini *dynamic* analisis digunakan sebagai tahapan pertama dari dua tahapan utama, *dynamic* analisis merupakan proses mengamati aktivitas malware pada sebuah *virtual machine* sebagaimana disampaikan oleh (Yusirwan, Prayudi, & Riadi, 2015), tahapan ini juga untuk meng-ekstrak *behavior features*. Tahapan kedua yaitu merancang skema deteksi berdasarkan hasil pada tahapan pertama. Harapannya penelitian ini nantinya dapat memberikan kontribusi berupa teknik baru dalam bidang keamanan computer khususnya dalam ruang lingkup metode deteksi malware berbasis *behavior approach*.

1.2 Rumusan Masalah

Merujuk kepada latar belakang yang telah dipaparkan sebelumnya, maka dapat diambil rumusan masalah di dalam penelitian ini, yaitu :

a. Bagaimanakah penerapan metode *behavior approach* untuk deteksi malware berdasarkan perilaku aplikasi terhadap data ?
b. Bagaimanakah kinerja *behavior approach* dalam mendeteksi malware berdasarkan perilaku aplikasi terhadap data ?

1.3 Batasan Maslah

Beberapa batasan masalah yang ditetapkan di dalam penelitian ini adalah sebagai berikut:

a. Penelitian ini hanya mengambil satu sampel dari malware ransomware yaitu ransom.locky. Malware ransom.locky dipilih untuk dijadikan sampel karena malware ini merupakan tipe malware yang menjadikan data user berupa file dokumen sebagai target dengan cara di enkripsi, selain itu malware ini merupakan malware dengan jumlah korban yang cukup banyak untuk tahun 2016 versi mcAfee.
b. Data yang menjadi sampel objek penelitian hanya file dokumen ber-ekstensi .DOC/X, .XLS/X, .PPT/X, .OD*, .PDF serta file image ber-ekstensi .JPG, .JPEG, dan .PNG. File dokumen dengan ekstensi tersebut dipilih karena merupakan file dokumen yang umum digunakan atau yang umumnya ada di dalam setiap komputer.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, dapat ditentukan tujuan penelitian. Adapun tujuan dari penelitian ini adalah:

a. Menerapkan metode *behavior approach* untuk deteksi malware berdasarkan perilaku aplikasi terhadap data.
b. Mengukur kinerja dari penerapan metode *behavior approach* untuk deteksi malware berdasarkan perilaku aplikasi terhadap data.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini untuk memberikan kontribusi berupa teknik baru dalam hal pendeteksian malware berbasis *behavior detection,* dan diharapkan menjadi masukkan baru bagi peneliti yang akan melakukan penelitian dalam hal deteksi malware, dan bagi developer dibidang keamana komputer khususnya developer *tool* anti malware

diharapkan menjadi sumbangan teknik baru yang dapat dimanfaatkan untuk mendeteksi dan mengatasi malware.

1.6 *Review* Penelitian

Berikut ini akan dibahas ulasan tentang penelitian yang telah dilakukan sebelumnya berkaitan dengan pendeteksian malware, dalam tulisannya (Mujumdar, Masiwal, & Meshram, 2013) yang berjudul *Analysis of Signatue Based and Behavior Based Anti Malware Approaches* memaparkan tentang sistem anti malware yang ada saat ini, bahwa mayoritas sistem keamanan khususnya anti malware masih menerapkan sistem atau metode pendeteksian yang berbasis pada *signature detection*, hal itu menurut para peneliti ini tidak cukup untuk mencegah bahaya kemanan serta ancaman malware yang datang saat ini, penelitian ini juga membahas tentang dua metode pendeteksian malware yang ada saat ini yaitu melalui pendekatan *signature based* dan melalui pendekatan *behavior based,* kemudian para penulis menutup dengan kesimpulan bahwa masing-masing metode baik *signature based* dan *behavior based* memiliki kelebihan dan kekurangan.

Sedangkan penelitian yang dilakukan oleh (Liu et al., (2011) dengan judul *Behavior-Based Malware Analysis And Detection* membahas tentang bagaimana mendeteksi malware berdasarkan pada fitur-fitur yang diekstrak dari malware, penelitian ini menjelaskan bahwa setiap jenis malware akan memiliki banyak *signature* hasil dari perubahan sedikit untuk malware yang sama akan menghasilkan malware yang berbeda tetapi pada prinsipnya setiap malware tersebut pada level tertentu memiliki kesamaan fitur jika diekstrak *behaviornya*, dan untuk mengetahuinya penelitian ini melakukan investigasi dan mengeksplorasi teknik untuk melakukan ekstrak malware *behavior* dimana hal itu dijadikan dasar untuk deteksi malware. Adapun (Veeramani & Rai, 2012) dalam penelitiannya *Windows API based Malware Detection and Framework Analysis* menjelaskan bahwa untuk Mendeteksi malware *zero day* adalah tantangan bagi para peneliti untuk waktu yang cukup lama, mengandalkan system deteksi malware berbasis *signature* sudah tidak dapat mengatasi malware-malware baru yang akan dating terutama malware seperti *zero day malware.*

Penelitian dengan judul *From Malware Signatures to Anti Virus Assisted Attacks* adalah penelitian yang ditulis oleh (Wressnegger, Freeman, Yamaguchi, & Rieck, 2016), penelitian ini membahas tentang kelemahan yang terdapat pada metode pendeteksian malware berbasis *signature*, setelah menjelaskan tentang mekanisme pendeteksian malware menggunakan metode *signature* itu sangat simpel dan cepat tapi, jika penanganan

signature tidak dilakukan dengan hati-hati hal itu akan menjadi masalah, berbalik dari mekanisme pertahanan menjadi instrumen serangan, para penulis juga menyajikan sebuah metode yang secara otomatis dapat menangani masalah tersebut.

Penelitian lain yang mencoba memberikan sebuah alternatif untuk pendeteksian malware berbasis *signature* ditulis oleh (Siddiqui, 2008), mengangkat tema *Data Mining Methods For Malware Detection,* peneliti ini ingin memberikan alternatif pendeteksian malware menggunakan *data mining,* alasan penulis karena sistem pendeteksian berbasis *signature* tidak dapat mendeteksi malware jenis baru, dalam mendukung penelitiannya penulis melakukan pengumpulan dan menganalisa ribuan file baik malware maupun program bersih untuk dibuatkan sebuah model yang akam mengklasifikasi program atau file berdasarkan kelasnya yaitu kelas malware atau kelas file/program bersih. Penulis mengklaim dari hasil eksperimen yang dilakukan, tingkat keberhasilan mendeteksi malware baru mencapai 98.4% dan dengan tingkat kesalahan atau *false positive* hanya 1.9% untuk pendeteksian.

Mengangkat tema *Malicious Behavior Detectinon using Windows Audit Logs,* (Berlin et al., 2015) melakukan penelitian tentang bagaimana mendeteksi malware menggunakan fasilitas bawaan pada sistem operasi Windows yaitu *audit log,* menurut para peneliti, *audit log* pada Windows memberikan informasi yang cukup untuk bisa mendeteksi adanya perilaku buruk sehingga dapat digunakan untuk mendeteksi adanya malware, dalam pengunjian yang dilakukan pada sejumlah sampel malware didapatkan hasil 83% dengan tingkat *false positive* hanya 0.1%.

Penelitian yang dilakukan oleh (Kheir, 2013) dengan judul *Behavioral Classification and detection of malware through HTTP user agent anomalies,* membahas tentang tantangan mendeteksi malware di lalu-lintas jaringan, berbagai teknik dilakukan oleh *Bootmaster* untuk menyembunyikan aktivitasnya di tengah lalu-lintas jaringan yang sangat besar, meskipun banyak aktivitas tidak normal pada bagian header *user-agent* HTTP namu hanya sedikit yang terdeteksi, olehnya itu peneliti melakukan penelitian untuk menganalisa perilaku tidak normar dalam lalu-lintas malware pada *HTTP user agent header.* Peneliti melakukan taksonomi dari malware untuk perilaku menyimpang pada *headerHTTP user agen* dan mengusulkan taksonomi ini sebagai mekanisme untuk pendeteksian malware. Hasil yang didapatkan dari pengujian menggunakan mekanisme yang diusulkan yaitu berupa rendahnya angka *false positives.*

Tabel 1. 3 Literatur Review Penelitian

No.	Paper	Masalah	Solusi	*Behavior Approach*
1.	Liu et al., (2011)	Malware memiliki banyak sekali tanda-tanda unik yang terdapat didalamnya, dan setiap tanda unik memiliki perilaku-prilaku yang dapat digunakan untuk mendeteksi malware secara lebih tepat.	Melakukan investigasi terhadap teknik untuk melakukan ekstrak malware *behavior feature* dengan melakukan klasifikasi dari formal *behavior* dan merancang sistem untuk mendeteksi malware jenis baru.	Eksplorasi terhadap *behavior* dari malware dan membuat klasifikasi *behavior,* target *operation behavior* adalah sistem
2.	Berlin, K., Slater, D., & Saxe, J. (2015)	Sistem keamanan jaringan dan antivirus yang menggunakan metode *signature based detection* terbukti tidak cukup untuk mendeteksi ancaman tipe polimorfik malware pada komputer.	Melakukan pencegahan dengan pendekatan *behavior based detection* dengan memanfaatkan *audit logs* yang menjadi *standard build-in* pada sistem operasi Windows.	Melakukan eksplorasi beberapa fitur malware *behavior* yang terekam pada log untuk semua kategori *behavior operation,* dengan target *operation behavior* adalah sistem.
3.	Alazab, Layton, Venkatara man, & Watters, (2010)	Menawarkan lima langkah untuk bagaimana mendeteksi malware yang samar dengan melakukan invertigasi terhadap	Menawarkan sistem otomatis yang membongkar dan melakukan ekstak terhadap API *calls features* secara efektif	Mengumpulkan fitur-fitur *behavior* dari malware pada semua kategori *behavior*

Tabel 1. 4 Literatur Review Penelitian (Lanjutan)

No.	Paper	Masalah	Solusi	*Behavior Approach*
		structural dan *behavioral features* dari API *calls.*	dari sebuah aplikasi eksekutabel menggunakan metode analisis perhitungan *n-gram.*	*operation,* dengan target *operation behavior* adalah sistem.
4.	Veeramani & Rai, (2012)	Mendeteksi malware *zero day* adalah tantangan bagi para peneliti untuk waktu yang cukup lama, mengandalkan system deteksi malware berbasis *signature* sudah tidak dapat mengatasi malware-malware baru yang akan dating terutama malware seperti *zero day malware.*	Menawarkan metode deteksi malware berbasi ektraksi *behaviror* atau perilaku yang berkaitan dengan malware dalam *application programming interface (API) call.* Melakukan klasifikasi malware berdasarkan pada kesamaan penggunaan *API call* pada semua kategori malware.	Melakukan eksplorasi malware *behavior* berdasarkan *API call* yang yang dilakukan malware, dengan target *operation behavior* adalah sistem.
5.	Nizar Kheir, (2013)	Masalah pada deteksi anomali *botnet* pada lalu-lintas jaringan yang digunakan *bootmaster* untuk berkomunikasi dengan menyembunyikan aktivitas ditengah lalu-lintas jaringan yang sangat besar.	Menggunakan taksonomi dari anomali malware *user agent* untuk mekanisme pendeteksian malware, berbasis pada *behavior detections based*	Eksplorasi beberapa fitur *behavior operation* fokus pada *network operation* karena untuk menemukan anomali data pada jaringan,

Tabel 1. 5 Literatur Review Penelitian (Lanjutan)

No.	Paper	Masalah	Solusi	*Behavior Approach*
				dengan sistem sebagai target *behavior operation.*
6.	Siddiqui, (2008)	Malware baru dengan varian yang sama tidak dapat dideteksi dengan metode *signature based*, type polimorfik malware merupakan tantangan untuk metode baru untuk dapat mendeteksi tipe malware jenis virus yang dapat menghindari antivirus yaitu jenis virus polimorfik.	Memperkenalkan data mining sebagai framework deteksi malware, menggunakan data mining untuk mengoleksi dan klasifikasi *behavior* malware dan *benign* program dengan pendekatan *statistical based detection*.	Mengumpulkan fitur-fitur yang dipilih dari ribuan malware dan *benign* aplikasi *behavior operation* dan diklasifikasikan, dengan target *operation behavior* adalah sistem.
7.	Singhal & Raul, (2012)	Malware dapat datang dari media seperti *local network*, internet, ataupun *device* yang dipasang, pengguna komputer rumahan dapat menggunakan anti virus yang dapat selalu diupdate, tapi bagi sebuah perusahaan menjadi sangat riskan	Membangun sebuah antivirus yang dapat memeriksa file yang milintas pada jaringan dan juga dapat memriksa file yang berpotensi sebagai virus berdasarkan pada pengetahuan yang dibagnun dengan menggunakan metode	Mengumpulkan fitur-fitur *behavior* dari file virus dan file yang terinfeksi virus pada semua kategori *behavior operation*, dengan target *operation*

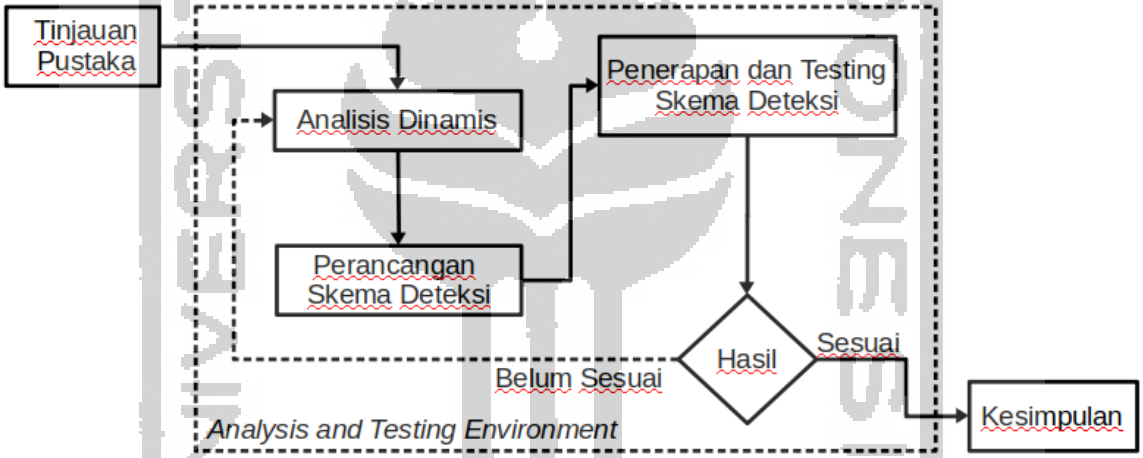
Tabel 1. 6 Literatur Review Penelitian (Lanjutan)

No.	Paper	Masalah	Solusi	*Behavior Approach*
		ketika virus baru dapat masuk dan menyerang semua komputer yang terhubung jaringan perusahaan.	*machine learning* dengan mengumpulkan *system API calls* yang dibuat oleh virus dan file yang diinfeksi oleh virus.	*behavior* adalah sistem.
8.	Penelitian yang diusulkan	Penelitian dalam hal deteksi malware dengan metode *behavior approach* yang ada saat ini tidak secara spesifik membahas perilaku aplikasi terhadap data dimana malware termasuk didalamnya, hal ini yang menjadi masalah beberapa tahun terakhir seperti malware ransomware contohnya yang secara spesifik dirancang untuk menargetkan data pengguna komputer.	diperlukan sebuah penelitian yang membahas secara spesifik deteksi malware berbasi *behavior approach* dimana perilaku aplikasi terhadap data dalam hal ini sebagai *target behavior operations* dapat digunakan sebagai cara deteksi malware.	Eksplorasi *behavior operation* fokus pada *file operation* dan *proses operation* karena untuk menemukan anomali pada data user, dengan user data sebagai target *behavior operation.*

1.7 Metodologi Penelitian

Agar penelitian ini terarah dan mendapatkan hasil yang maksimal, maka penelitian ini menggunakan beberapa tahapan metode penelitian sebagaimana dibawah ini:

a. Tinjauan Pustaka
b. Pendeteksian
    1. Analisis dinamis
    2. Perancangan skema untuk mendeteksi malware
    3. Penerapan skema pendeteksian dan melakukan testing
    4. Hasil, kembali ke poin 1 (analisis) jika hasil belum sesuai dan jika hasil telah sesui lanjut ke kesimpulan.
c. Kesimpulan.



Gambar 1.2 Alur Metode Penelitian.

Gambar 1.2 diatas merupakan alur dan tahapan-tahapan yang dilakukan dalam metode penelitian ini. Tahapan tinjauan pustaka dilakukan sebagai tahapan awal untuk memberikan dasar bagi arah penelitian, tahapan kedua merupakan bagian utama dari penelitian ini yang terdiri dari *dynamic* analisis, perancangan skema deteksi, penerapan dan testing skema serta evaluasi hasil, jika hasil belum sesuia maka proses kembali ke tahapan analisis, selanjutnya jika hasil sesuai maka tahapan terakhir yaitu menarik kesimpulan.

1.8 Sistematika Penulisan

Laporan penelitian ini disusun dengan sistematika penulisan yang dapat mempermudah proses pembahasan penelitian. Adapun sistematika penulisan yang dimaksud adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Bab ini memuat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, *literature review*, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini memuat teori-teori penunjang yang digunakan sebagai dasar penelitian pendeteksian malware dan mitigasi data.

BAB 3 METODOLOGI PENELITIAN

Bab ini membahas tentang langlah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB 4 HASIL PENELITIAN DAN PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat, evaluasi dan hasil.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil penelitian serta saran dan rekomendasi untuk penelitian selanjutnya.