Bab I PENDAHULUAN

I.1 Latar Belakang

Dalam era ini internet sudah menjadi sebuah hal yang sangat lumrah bagi manusia dikarenakan dapat membantu manusia dalam melakukan berbagai aktifitas. Banyak sekali komputer saling terhubung dengan komputer lainnya menggunakan internet. Internet memiliki banyak sekali hal positif yang dapat diambil dalam era ini tetapi internet juga memiliki hal yang negatif seperti *cyber crime*. *Cycber crime* adalah sebuah penyalahgunaan menggunakan internet untuk mendapatkan keuntungan ataupun menyebarkan *malware* menggunakan internet (Saini, Rao, 2012).

Malware adalah sebuah kode yang berada pada perangkat lunak yang dapat menyebabkan kerusakan pada fungsi sistem (McGraw, Morrisett, 2000). *Malware* tetap menjadi ancaman yang berbahaya dan kemunculannya dapat menyebabkan masalah pada korban yang terkena *malware*. Dikarenakan hal tersebut keamanan internet merupakan hal yang penting dalam era internet ini untuk menjaga semua aktifitas yang kita lakukan di internet.

Keamanan internet pada era ini telah berubah sebelumnya selalu berfokus pada perangkat yang ada pada komputer menjadi perangkat yang berada *mobile* (Milosevic, Malek, Ferrante, 2016). Perangkat *mobile* pada era ini merupakan perangkat yang terlemah sehingga dapat terjangkit *malware* khusus dengan mudah yaitu *mobile malware* (Symantec Corporation, 2015). *Mobile malware* terus naik dan mencapai 6 juta sample yang terdeteksi pada tahun 2014, naik 14% pada tahun yang sama (Mcaffe Labs, 2015).

Malware analysis merupakan sebuah cara untuk mendapatkan informasi dari malware untuk mengatasi serangan terhadap korban yang terinfeksi (Gutmann, 2007). Dari informasi yang didapat, infeksi *malware* bisa dikenali lewat signature dan dapat menggambarkan bagaimana cara sebuah malware itu bekerja. Ada dua cara untuk melakukan analisis *malware* yaitu *static analisis* dan *dynamic analisis*. Static analisis dapat digunakan untuk melakukan investigasi terhadap *static features* seperti *Permission-Based*. Biasanya static analisis digunakan pada perangkat lunak yang memiliki sumber daya yang minimal. Dynamic analisis juga merupakan sebuah pendekatan yang sangat efektif dengan

melakukan percobaan pada malware yang akan diidentifikasi. Dynamic analisis pada mobile malware menggunakan cpu dan juga memory. Dalam menggunakan cpu dan memory pada dynamic analisis akan dimonitor *cpu usage* dan *virtual memory* untuk melakukan pendeteksian *malware.*

Selain itu, aka nada kasus dimana malware akan benar-benar diinjeksikan kedalam android. Analisis malware didalam perangkat android dilakukan dengan melakukan akuisisi terhadap memory dari android, kemudian hasil akuisisi memory akan dianalisis dengan menggunakan tools voloatility. Dalam hasil analisis ini bisa dibuktikan adanya kegiatan malware pada memory milik perangkat yang terjangkit. Diharapkan dengan adanya penelitian tentang malware pada smartphone ini, dapat memberikan informasi dan edukasi kepada pengguna bahwa terdapat ancaman pada perangkat android dengan cara malware melakukan injeksi terhadap memory pada android.

Memory Forensics adalah sebuah cara untuk mendapatkan bukti proses untuk mendapatkan suatu kejanggalan yang ada pada proses. Kelebihan dari *memory forensics* ini yaitu dapat mengetahui *malware* yang terhubung langsung dengan proses yang berada pada *memory*. Setelah mendapatkan proses yang mencurigakan akan dilakukan *reverse engineering* untuk mendapatkan API yang ada pada suatu proses.

API adalah beberapa kumpulan dari sebuah perintah untuk melakukan program aplikasi. Dalam API bisa digunakan untuk mendapatkan malicious activity dari suatu malware dan dalam melakukan analisis API adalah cara yang sangat efektif untuk mendapatkan bagaimana cara kerja malware (Alquraishi, Batarfi, 2017). Dengan menggunakan API bisa dilakukan analisis *malicious activity* dengan beberapa API yang didapatkan.

Berdasarkan data yang telah dianalisis tersebut maka hasil dari penelitian ini adalah dampak dari sample malware menggunakan API yang didapatkan sebelumnya dengan menggunakan *reverse engineering* dan bagaimana proses berjalan dalam suatu *environtment* yang ada. Dampak tersebut berdasarkan *malicious activity* dan proses menggunakan plugin *psxview* dan plugin *malfind.*

I.2 Perumusan Masalah

Pada tugas akhir ini, rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana cara melakukan analisis *malware* pada android dengan mengunakan static analisis.
2. Bagaimana melakukan analisis terhadap RAM perangkat android yang telah diakuisisi.
3. Bagaimana cara mengidentifikasi *malware* dengan analisis memory menggunakan *reverse enginering.*

I.3 Tujuan Penelitian

Pada tugas akhir ini, tujuan yang ingin dicapai adalah sebagai berikut:

1. Dapat melakukan analisis malware pada android dan mendapatkan informasi tentang malware menggunakan static analisis
2. Melakukan analisis terhadap RAM perangkat android menggunakan tools Volatility dengan memanfaatkan plugin yang tersedia
3. Melakukan analisis terhadap API dari aplikasi perangkat android menggunakan tools APKtools untuk mengetahui *malicious activity* yang terdapat pada perangkat android

I.4 Manfaat Penelitian

Manfaat dari tugas akhir ini adalah sebagai berikut:

1. Mengetahui adanya aktifitas malware malware pada RAM Android
2. Mengetahui cara kerja malware dari proses analisis melalui sandbox dan RAM yang diakuisisi dari perangkat android yang terjangkit malware
3. Mengetahui cara kerja malware menggunakan perilaku yang didapatkan menggunakan API

I.5 Batasan Masalah

Batasan masalah untuk penelitian ini adalah sebagai berikut :

1. Tidak menangani network traffic analisis
2. Hanya membahas *memory forensics.*
3. Tidak membahas kode *assembly* yang telah diinjeksikan terhadap *memory.*

4. Dampak didapat hanya berdasarkan API
5. Menggunakan 10 sample malware

I.6 Ruang Lingkup

Ruang lingkup untuk penelitian ini adalah sebagai berikut :

1. Tools yang digunakan untuk melakukan analisis terhadap RAM yang telah diakuisisi adalah Volatility
2. Menggunakan Android SDK Manager untuk membuat emulator
3. Menggunakan sistem operasi android 4.4.2 (API 19).
4. Tools yang digunakan untuk melakukan akuisisi RAM dari perangkat android adalah LiME (Linux Memory Extractor).
5. Menggunakan static analysis
6. Menggunakan enviroment yang telah dibuat untuk menjalankan malware

I.7 Sistematika Penulisan

Penulisan ini akan dijabarkan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan memberikan uraian latar belakang, rumusan masalah, tujuan penelitan, manfaat penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan literature yang relevan dengan permasalahan yang dihadapi. Menjelaskan setiap teori yang digunakan berdasarkan referensi yang telah didapatkan.

BAB III METODOLOGI PENELITIAN

Bab ini akan menjelaskan tentang langkah-langkah penelitian secara rinci, mulai dari tahap awal, tahap analisis, tahap desain, tahap pengujian dan tahap akhir dari penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang pembahasan hasil setelah proses eksekusi dari *malware* pada sandbox dilakukan dan dianalisis menggunakan volatility dan APKtools. Pembahasan berisi tentang temuan dari rangkaian analisis kedua tools tersebut.

BAB V Kesimpulan dan Saran

Pada bab ini berisi kesimpulan yang menjelaskan tujuan penelitian dapat tercapai serta menjelaskan kelebihan dan kekurangan dari penelitian ini. Sedangkan saran, berisi halhal yang dapat dilakukan sebagai kontribusi terhadap penelitian ini dikemudian hari.