1. Pendahuluan

Latar Belakang

Pada kasus tindak kriminal, dibutuhkan *digital forensic* yang bertugas melakukan penyelidikan terhadap bukti *digital*. Bukti *digital* tersebut salah satunya didapatkan dari komputer yang nantinya akan dilakukan proses akuisisi memori [1]. Tiap komputer memiliki sistem operasi yang berbeda serta sistem keamanan yang berbeda. Terkait dengan sistem keamanan pada komputer, pada perangkat berbasis Windows, Microsoft menerapkan sistem Virtual Secure Mode (VSM). VSM merupakan fitur pada Windows 10 yang digunakan untuk mengamankan sistem operasi. VSM juga merupakan *secure environment* yang berfungsi untuk melindungi sistem operasi dari target serangan [2]. Pada kondisi ini, user akan memasuki tahap IUM (*Isolated User Mode*) yang mana akan mengisolasi user ke dalam lingkungan terpisah dari Windows.

IUM bekerja langsung dengan fitur lain di Windows 10, Credential Guard, dan Device Guard. Credential guard menggunakan IUM sebagai pertahanan terhadap serangan hash [3]. IUM mengandalkan kernel yang aman untuk menangani pekerjaan sistem operasi dasar. Saat *secure kernel* menangani ini, kernel di Windows adalah yang menangani operasi utama yang berjalan di perangkat. Keuntungan utama menggunakan kernel terpisah untuk menangani IUM adalah kernel yang aman tidak berisi modul *third party*. Ini memungkinkan kernel yang aman untuk beroperasi tanpa risiko gangguan dari *third party codes*. Untuk mencapai IUM, *safe kernel* bergantung pada hypervisor Windows, Hyper-V, untuk mengelola kernel Windows dan *safe kernel*. Dengan kata lain, hypervisor dapat mengatur izin memori yang berbeda untuk kedua kernel, sehingga kernel normal tidak mungkin mengakses memori kernel yang aman. Hyper-V memegang partisi root. Pada partisi ini terdapat dua kernel dan dua tipe user mode. Isolasi ini diimplementasikan oleh Hyper-V sebagai entitas dasar yang mengatur eksekusi lingkungan dalam VSM [2].

Salah satu kegiatan forensik digital yang sering dilakukan adalah memperoleh bukti digital dari suatu perangkat. Kegiatan tersebut memerlukan beberapa *tools* untuk memulihkan memori yang telah dihapus, yaitu *tools* akuisisi memori. Ada beberapa *tools* akuisisi memori yang dapat digunakan oleh forensik digital. Biasanya, alat-alat ini dijalankan pada *normal kernel*, bukan pada *secure kernel*. Berdasarkan penjelasan di atas, secure mode berjalan pada kernel berbeda yang terpisah dari kernel utama pada Windows. Hal inilah yang melatarbelakangi dilakukannya penelitian ini. Studi ini membantu kegiatan forensik digital untuk mencegah adanya masalah yang muncul saat melakukan proses akuisisi memori di kegiatan mendatang. Studi ini akan mencari tahu apakah ada perbedaan saat melakukan proses akuisisi memori pada *secure mode* dan *normal mode*, atau tidak. Tujuan lainnya yaitu untuk mencari tahu apa yang menjadi penyebab dari perbedaan tersebut. Studi ini dilakukan dengan analisis kode statis, setelah dilakukan percobaan pada lingkungan Windows yang berbeda.

Analisis kode statis adalah salah satu proses *reverse engineering* untuk memverifikasi file yang dapat dieksekusi atau biasanya dikenal sebagai file .exe untuk melihat semua instruksi dari program. Salah satu keuntungan metode ini yaitu dapat memberikan informasi tentang fungsi penting dari program, dan dalam beberapa kasus dapat mengungkapkan apakah file memiliki masalah atau tidak. Metode ini dapat mengevaluasi seluruh *source code* dalam waktu yang lebih efisien menggunakan beberapa *tools*, tidak seperti analisis kode secara manual. Selain itu, metode ini dapat dilakukan tanpa perlu berada dalam jaringan *online* [4], [5]. Analisis kode statis dapat dilakukan dengan beberapa metode, beberapa di antaranya adalah pemindaian *antivirus*, pencarian string, analisis *runtime system*, *disassembly*, dan sebagainya. Analisis kode statis dapat dilakukan dengan beberapa *tools* forensik. Salah satu *tools* yang terkenal adalah *Interactive Disassembler* (IDA). *Tools* ini digunakan untuk melakukan kegiatan forensic karena tidak hanya sekedar melakukan disassembling, namun dapat melakukan hal lain seperti mengidentifikasi error, menemukan koneksi antar beberapa *function*, dan juga menganalisis kerentanan.

Berdasarkan latar belakang di atas, penelitian ini bereksperimen pada proses akuisisi memori yang dijalankan pada lingkungan Windows yang berbeda, yaitu secure mode dan normal mode. *Tools* akuisisi memori yang digunakan dalam penelitian ini adalah FTK Imager dan Autopsy. Dalam kasus ini, *tools* akuisisi memori akan dites dengan dan tanpa VSM yang berjalan pada sistem operasi Windows 10. Setelah mendapatkan hasil percobaan dan menemukan beberapa masalah saat menjalankan alat, selanjutnya akan dilakukan analisis kode statis terhadap *tools* akuisisi memori menggunakan metode *search string* dengan bantuan *Interactive Disassembler* (IDA) dan menggunakan metode analisis *runtime system* secara langsung pada sistem operasi Windows itu sendiri.

Penelitian terkait dilakukan oleh Niken [6]. Hasil penelitian tersebut menunjukkan bahwa FTK Imager tidak dapat berjalan dengan baik pada perangkat yang digunakan. Dari penelitian oleh Niken, menunjukkan bahwa peneliti menyarankan untuk melakukan studi lebih lanjut tentang masalah terkait tetapi mengujinya dengan berbagai variabel lain, untuk mendapatkan hasil yang lebih jelas. Studi ini melanjutkan penelitian sebelumnya untuk menemukan variabel baru yang muncul saat memperoleh memori dalam *secure mode* dengan beberapa perbedaan. Perbedaannya, studi ini menjelaskan cara memasuki VSM secara detail, penelitian ini juga akan menguji *tools* yang sama yaitu FTK Imager, namun dengan perangkat berbeda yang memiliki spesifikasi berbeda di dalamnya. Selain itu, penelitian ini

menambahkan *tools* yang berbeda dari penelitian sebelumnya yaitu Autopsy. Tujuan menggunakan *tools* yang berbeda adalah untuk mengidentifikasi apakah *tools* ini terpengaruh oleh *secure mode* atau tidak.

Kejadian pada perangkat yang digunakan akan menjadi titik awal untuk penelitian ini. Masalah yang muncul adalah alasan untuk menganalisis *tools* akuisisi memori apakah *source code* dari *tools* tersebut memiliki masalah yang tidak mendukung aplikasi untuk berjalan pada *secure mode*, atau sistem pada Windows yang menyebabkan gangguan pada kinerja *tools* akuisisi memori. Hasil akhir dari penelitian ini adalah mengetahui apakah *secure mode* memengaruhi proses akuisisi memori atau tidak, dan apa yang menyebabkan *secure mode* memengaruhi prosesnya.

Topik dan Batasannya

Topik dan batasan masalah yang digunakan dalam penelitian tugas akhir ini mencakup bagaimana cara mengetahui faktor yang menyebabkan sistem pada *tools* akuisisi memori mengalami *crash* ataupun *error* saat VSM dalam kondisi aktif, serta bagaimana cara menganalisis sistem dengan kondisi VSM aktif dan apa pengaruhnya pada *tools* akuisisi memori dengan menggunakan metode analisis kode statis. Kode yang akan dianalisis dalam penelitian ini hanya kode statis. *Tools* yang akan dianalisis pada penelitian ini hanya yang merupakan *tools* akusisi memori, yaitu:

Tabel 1. List *tools* akuisisi yang dianalisis

Tools	Version	Download Source
FTK Imager	4.5.0.3	https://accessdata.com/product-download/ftk-imager-version-4-5
FTK Imager	4.3.0.18	https://accessdata.com/product-download/ftk-imager-version-4-3-0
Autopsy	4.19.3	https://www.autopsy.com/download/
Autopsy	4.7.0	https://github.com/sleuthkit/autopsy/releases?page=2

Tujuan

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah untuk mengetahui faktor apa saja yang menyebabkan sistem pada *tools* akuisisi memori mengalami *crash* ataupun *error* saat VSM dalam kondisi aktif, serta dampak yang ditimbulkan oleh VSM pada *tools* akuisisi memori dengan menggunakan metode analisis kode statis.

Organisasi Tulisan

Pada bab 2 dibahas studi terkait penelitian yang dilakukan, bab 3 dibahas sistem yang dibangun, bab 4 dibahas evaluasi dari model, dan bab 5 dibahas kesimpulan dari penelitian yang dilakukan.