BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet telah mengubah gaya hidup masyarakat, baik dari sosial, pendidikan, kesehatan dan bahkan pemerintahan Selain mengubah pola hidup masyarakat *internet* juga menciptakan masalah baru yang merupakan kejahatan dunia maya, khususnya pada aktivitas setiap transaksi atau proses di *Internet* yang menggunakan perangkat lunak *web browser* [1]. Kemudahan pada sebuah akses juga menjadi ancaman dan kejahatan langsung pada *web server* suatu lembaga sehingga memberikan potensi kerugian yang sangat besar [2]. *Web browser* dirancang untuk menyimpan semua aktivitas dan informasi yang dilakukan seseorang pada saat menjelajahi *internet* seperti *Uniform Resource Locator* (URL), kata kunci pencarian, Cap Waktu, kata sandi dan lain-lain [3]. Namun, untuk keamanan pengguna, beberapa informasi mereka tidak disimpan dalam sistem komputer, para pengembang *web browser* saat ini juga masih berlomba- lomba membuat agar setelah ketika aktivitas *browsing* selesai informasi dan semua aktivitas yang dilakukan sebelumnya dapat terhapus, saat ini disebut dengan mode penjelajahan pribadi [4]. Fitur keamanan ini membuat *web browser* digunakan oleh individu untuk melakukan kejahatan, dengan metode anti-forensik lainnya seperti menggunakan *web browser portable* dengan mode *private* yang dirancang agar tidak meninggalkan jejak bukti digital pada komputer [5] dan penghapusan atau perubahan *registry* ketika sedang berselancar didunia maya. *Portable web browser* mampu dijalankan tanpa ada dipasang di komputer, jadi hanya disimpan di penyimpanan *eksternal* media agar tidak meninggalkan file dalam program komputer [4]

Menurut *Chivers* (2013) ketika seseorang menggunakan mode *private browsing* saat beraktivitas di internet dapat mampu pencegahan dalam analisa forensik digital. Hal ini dikarenakan pada saat menggunakan *web browser* dengan mode *private*, *browsing* jejak digital seperti *history* dan bukti digital lainnya tidak terekam oleh *web browser*, padahal *web browser* didesain untuk menyimpan

setiap informasi seperti file *history*, URL, pencarian dan *password* yang berkaitan dengan aktivitas pengguna *web browser* tersebut (*Dharan* 2014).

Namun sayangnya, keunggulan dari fitur mode *private* ini sering di salah gunakan untuk melakukan kejahatan apalagi dengan ditambah teknik anti forensik seperti *portable web browser* dan penghapusan *registry* pada sistem operasi yang mampu mengurangi interaksi *browsing* dengan *disk* komputer yang sangat efektif dalam menghilangkan jejak dan menambah keamanan ketika sedang bertransaksi dalam *internet* [5].

Penyelidikan pada *web browser* komputer juga dikenal sebagai digital forensik. Secara umum, digital forensik dibagi menjadi dua teknik, *live forensic* dan statis forensik. Metode *live forensic* adalah metode yang membutuhkan suatu kondisi dimana komputer tetap hidup dan masih berjalan begitu juga semua datanya yang melewati *Random Access Memory* (RAM). Data yang berjalan di komputer adalah data yang mudah menguap karena saat komputer menyala disaat itu juga *ram* beroperasi untuk menulis dan menghapus data [13]. Kualitas data yang dikumpulkan sangat berdampak pada proses investigasi dan kualitas data yang disalin harus mengandung informasi yang lengkap seperti akses informasi dan waktu [14].

Beberapa informasi yang dapat ditemukan pada RAM juga tergantung pada sistem operasi yang digunakan [15]. Informasi yang dapat ditemukan pada RAM seperti proses yang sedang berjalan, informasi tentang *file* yang dapat dieksekusi, kunci registri, informasi tentang aktivitas jaringan, *driver* yang digunakan, *login* pengguna, kata sandi dan kunci kriptografi, tersembunyi proses dan data, *malware*, data sementara, aplikasi *portable* Aplikasi yang tidak diinstal pada komputer itu sendiri tetapi dengan kondisi berjalan, dan banyak informasi penting lainnya [18].

Beberapa peneliti telah mengembangkan dan mengusulkan kerangka kerja baru untuk mengidentifikasi suatu kegiatan dan meningkatkan langkah penyelidikan forensik dengan tujuan menemukan bukti digital [22] dengan Pendekatan yang terstruktur dan model yang bertujuan untuk mengidentifikasi kegiatan diharapkan dapat membantu meningkatkan proses inkuiri. Setiap model

yang berbeda memiliki fase yang berbeda. Model baru ini juga telah dibandingkan dengan *Systematic Digital Forensic Investigation Model* (SDFIM), *Integrated Digital Investigation Process* (IDIP), dan lain lain. Model baru ini membagi proses penyelidikan menjadi empat tingkat berdasarkan fase yaitu pengumpulan, pemeriksaan, analisis dan pelaporan yang saat ini disebut *National Institute of Standards and Technology* (NIST) [23].

Penelitian ini bertujuan untuk mengkaji *portable web browser* dengan *mode private tor* pada *browser Brave* menggunakan metode *live forensics*. Metode *live forensic* yang diusulkan merupakan pengembangan dari investigasi NIST. Metode ini menangkap memori secara langsung setelah sesi penjelajahan pada *web browser* dan kemudian menganalisis memori yang telah diakuisisi dengan tujuan untuk mencari artefak dalam memori. Eksperimen dilakukan di pada *browser web*, dengan studi mengungkap kejahatan distribusi sekaligus transaksi jual beli narkoba di indonesia.

1.1 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang akan di teliti oleh peneliti yaitu semakin beragamnya metode *anti-forensic* khususnya pada aktivitas *browsing* dalam kegiatan ilegal. Maka dari itu diperlukan juga sebuah teknik dengan standar tertentu untuk menginvestigasi sebuah kasus aktivitas ilegal yang di lakukan pada *browser*. Dari masalah yang diuraikan diatas maka digunakanlah teknik *live forensic* dengan metode *National Institute of Standards and Technology* (NIST) untuk menganalisis sebuah kasus akvitas ilegal saat *browsing* dengan skenario yang telah ditetapkan.

1.2 Batasan Masalah

Dalam melakukan penelitian ini adapun batasan masalah yang di tetapkan adalah sebagai berikut:

1. Sistem yang digunakan pada Skenario adalah sebuah sistem komputer yang terhubung dengan USB *driver* yang digunakan oleh tersangka untuk *browsing*, dan pada skenario penelitian terbatas pada *virtual machine* dengan sistem operasi *windows 7*.
2. Proses pengumpulan data pada *live forensic* dilakukan hanya ketika kondisi sistem dalam keadaan hidup, tidak bisa dilakukan ketika sistem dalam kondisi mati
3. Dalam penelitian ini hanya membahas mengenai investigasi dari aplikasi *portable brave browser* dengan connectivitas *tor* menggunakan metode live *forensic* dari awal hingga proses analisis selesai.
4. Ada beberapa bukti potensial yang bisa dianalisa pada live forensic seperti *hibernation file* dan *pagefile*, namun analisa *live forensic* penelitian ini berfokus menganalisis barang bukti memori RAM dengan teknik analisa *file carving* dan *string analisis* pada RAM
5. Penelitian menggunakan skenario aktivitas *surfing* seperti *browsing* dengan kata kunci terkait narkotika dan aktivitas jual-beli narkotika via *whatsapp* yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian serangan.
6. Sistem operasi yang digunakan pada lab penelitian adalah *windows 7*, dalam hal ini dijadikan sebagai barang bukti komputer yang dipakai tersangka.
7. Aplikasi yang digunakan untuk melakukan perbandingan *file* akuisisi RAM dan hasil dari duplikat adalah *MD5 Checker*.
8. Tools yang digunakan dalam proses analisis yaitu *volatility, bulk-extractor, foremost*

1.3 Tujuan Penelitian

Tujuan yang ingin di capai peneliti dalam penelitian ini yaitu :

1. Merancang model scenario live forensic dengan kasus interaksi atau transaksi antara penjual dan pembeli dengan konteks jual beli obat terlarang secara online
2. Menganalisis bukti digital dari computer tersangka (pembeli) dengan teknik file carving dan string analisis
3. Mendapatkan bukti bukti digital serta mampu menemukan artefak artefak yang berguna untuk dilakukan pemeriksaan lebih lanjut

1.4 Manfaat Penelitian

Berdasarkan paparan uraian latar belakang masalah, rumusan masalah, batasan masalah dan tujuan penelitian di atas, maka manfaat yang diharapkan dalam penelitian ini adalah sebagai berikut:

1. Sebagai pendalaman materi dalam bidang digital forensik khususnya pada *live forensic* dengan Metode NIST dan studi kasus aktivitas *surfing* pada *portable web browser brave* dengan *mode private*.
2. Memperinci dan melengkapi penelitian sebelumnya terkait proses investigasi digital forensic khususnya *live forensic* dan investigasi *portable private web browser* yang biasa digunakan sebagai anti forensik.
3. Memberikan panduan dalam proses investigasi pada *portable private web browser brave* menggunakan teknik *live forensic*. Penelitian ini diharapkan dapat membantu para investigator dalam menemukan bukti kejahatan berdasarkan bukti memori RAM *image*.

1.5 Sistematika Penulisan

Sistematika penulisan ini disusun guna memberikan gambaran secara umum mengenai isi dari penelitian yang dilakukan, dalam sistematika ini terbagi menjadi beberapa bab yaitu:

Bab I Pendahuluan, Bab ini memuat tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, Pada bab ini menjelaskan mengenai teori-teori yang terkait untuk memecahkan masalah serta menjelaskan tools yang digunakan pada saat melakukan analisis.

Bab III Metodologi Penelitian, Bab ini berisi tentang langkah-langkah untuk mempersiapkan skenario kasus dan gambaran umum dalam menyelesaikan kasus tersebut, serta mempersiapkan penyusunan kerangka investigasi forensic.

Bab IV Hasil dan Pembahasan, Bab ini membahas mengenai persiapan lingkungan penelitian, implementasi skenario, akuisisi memori ram kemudian analisa data berdasarkan temuan yang telah didapatkan pada saat melakukan investigasi bukti digital sesuai prosedur yang telah diuraikan pada Bab III.

Bab V Kesimpulan dan Saran, Bab ini berisi tentang kesimpulan dari hasil penelitian serta saran dan rekomendasi untuk penelitian selanjutnya.