

Bab I

Pendahuluan

1.1 Latar belakang

Internet saat ini sudah menjadi kebutuhan manusia karena internet sangat membantu manusia dalam berbagai aspek, mulai dari sumber informasi, bersosialisasi hingga berbisnis bisa dilakukan melalui internet. Salah satu alat untuk mengakses internet adalah dengan menggunakan web browser. Web browser merupakan salah satu program aplikasi untuk mengakses layanan yang tersedia pada situs web[1]. Pengguna dapat melakukan banyak aktivitas di internet melalui browser seperti mencari suatu informasi dari web, mengakses sosial media, mengunduh *file* dan sebagainya. Saat ini banyak sekali browser internet yang dirilis dengan berbagai nama seperti Google Chrome, Mozilla Firefox, Opera, Brave, dan lain-lain.

Selain itu web browser menyediakan berbagai fitur untuk menjaga keamanan penggunaannya ketika menjelajahi internet, seperti mode *private* atau *incognito*, pencegahan pelacakan, anti *phishing*, pembersihan data, dan lain – lain. Namun fitur tersebut juga bisa dimanfaatkan oleh pengguna yang melakukan tindakan kriminal di internet dan melakukan kegiatan anti forensik untuk meminimalkan atau menghilangkan jejak digital. Salah satunya fitur mode *private* atau *incognito*, pada mode normal semua aktivitas yang dilakukan pengguna di dalam browser direkam dan disimpan disistem browser. Aktivitas yang telah dilakukan tersebut dapat dilihat pada riwayat penelusuran atau riwayat unduhan jika pengguna mengunduh suatu *file*. Sedangkan untuk mode *private*, aktivitas yang dilakukan pengguna di dalam browser tidak disimpan sehingga fitur ini memungkinkan pengguna untuk menjelajahi internet tanpa menyimpan informasi apa pun di dalam browser[2]. Pencarian bukti digital dari aktivitas *browsing* merupakan komponen penting dari penyelidikan digital forensik[3]. Sehingga diperlukan suatu metode penyidikan untuk mendapatkan data atau bukti digital dari web browser.

Mahlous dan Mahlous (2020) melakukan penelitian pada mode *private* dari web browser Brave dengan mempelajari *private browsing mode*, memeriksa penjagaan privasi data dan akuisisi data forensik, serta menguraikan lokasi direktori dan jenis bukti yang tersedia melalui analisis *live* dan *post-mortem*. Dalam penelitian ini dilakukan pengambilan data dari RAM (Random Access Memory) dan *hard disk* dengan memanfaatkan *tools* seperti FTK

Imager, WinHex, Internet Evidence Finder (IEF), dan Autopsy. Kesimpulan dari penelitian ini adalah *live memory analysis* dari memori RAM lebih efektif karena beberapa jenis artefak seperti URL, email, dan gambar dapat ditemukan. Sebaliknya, *post-mortem analysis* membawa ke jalan buntu bagi peneliti karena Brave berhasil menghapus semua data dan informasi terkait *private browsing sessions* dari *hard disk*[4].

Pada tugas akhir ini membahas tentang analisis terhadap data artefak yang didapatkan dari tiga mode keamanan web browser dengan menerapkan teknik akuisisi memori *live forensics* yang melibatkan beberapa *tools* forensik. Penerapan teknik akuisisi *live forensics* ini dipilih karena teknik ini dinilai paling sesuai untuk kasus yang diuji. Lalu pada simulasi kasus melibatkan dua web browser yaitu Brave, dan Opera GX. Brave merupakan salah satu *secure* browser populer yang mengutamakan privasi dan keamanan penggunanya. Statistik pengguna aktif bulanan Brave browser pada bulan Januari 2024 mencapai 67,18 juta pengguna[5]. Selain itu Brave browser juga terus melakukan pengembangan fiturnya hingga saat ini. Dan Opera GX adalah varian khusus dari browser Opera yang dikhususkan untuk *gamers*. Browser ini juga dilengkapi dengan fitur privasi yang saat ini belum diteliti sampai mendalam. Pada simulasi, kedua browser tersebut disimpan pada *internal storage (hard disk)* komputer. Selanjutnya hasil akuisisi data dari simulasi tersebut dilakukan analisis untuk mengetahui seberapa banyak data bukti digital yang bisa didapatkan serta untuk menguji efektivitas dari metode yang dijalankan dalam tugas akhir ini.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dibuat, rumusan masalah tugas akhir ini adalah untuk mencari tahu sejauh mana pengaturan mode keamanan browser memengaruhi kelengkapan data forensik yang didapatkan serta bagaimana metode *live forensics* bisa mengakuisisi data forensik tersebut seperti data histori penelusuran internet dan akun untuk melakukan *login*.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah melakukan analisis terhadap hasil akuisisi data seperti data histori penelusuran dan akun yang digunakan untuk *login* untuk mengetahui dampak dari pengaturan mode keamanan pada browser terhadap informasi jejak digital yang bisa didapatkan.

1.4 Batasan Masalah

Batasan masalah dari tugas akhir ini adalah sebagai berikut:

1. Uji coba pada tugas akhir ini melibatkan dua browser yaitu Brave yang merupakan salah satu *secure* browser populer, dan Opera GX yang juga merupakan *secure* browser yang saat ini belum diteliti secara mendalam.
2. Percobaan dilakukan di dalam lingkungan yang terkontrol, semua perangkat yang digunakan disediakan oleh penulis.