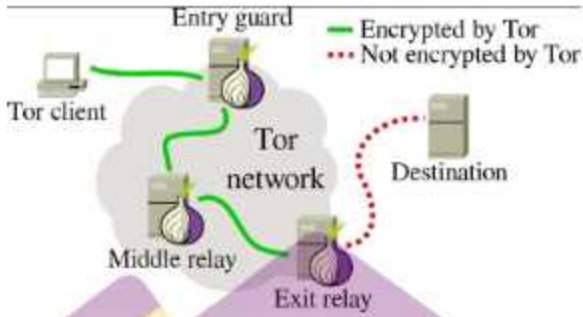
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Live forensic merupakan salah satu bidang ilmu forensik digital yang tumbuh sangat cepat untuk membantu penyidik dalam menyelidiki dan menemukan bukti penting yang diambil dari *volatile memory* barang bukti [1] [2]. *Live Forensics* pada dasarnya memiliki kesamaan pada teknik forensik tradisional dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja *live forensics* merupakan respon dari kekurangan teknik forensik tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan (*real time activity*), seperti aktivitas program, swap file, *running system*, *network connections*, *unencrypted file contents*, *cryptographic keys/password* dan informasi sensitive lainnya, sehingga menjadi kelebihan dari teknik live forensic [3] [4] [5] [6].

Proses akuisisi *live forensic* dilakukan ketika kondisi sistem dalam keadaan hidup, karena hampir keseluruhan penggunaan aktif sistem tersimpan pada RAM. [7] [8]. *Live forensic* memang memerlukan ketelitian dan prosedur khusus agar tidak berdampak pada integritas barang bukti atau bahkan mengganggu *service* yang berjalan pada target sistem [9]. Selain itu penanganan data dan informasi pada RAM harus dilakukan dengan hati-hati karena data dan informasi tersebut bisa hilang jika sistem mati [10] [11] [12] [13].

The Onion Router atau biasa disebut TOR, merupakan arsitektur jaringan yang populer karena kemampuan enkripsi berlapis-lapis (*complex layers*) dalam transmisi data yang mampu menyembunyikan identitas dan lokasi user. Sejak awal rilisnya tahun 2002, TOR banyak digunakan oleh komunitas yang sangat mendukung kebebasan privasi, jurnalis, pemerintah dan pelaku *cybercrime* [14]. Mayoritas penggunaan Tor digunakan untuk mengakses dark web secara anonym, *dark web* juga menjadi tempat banyak aksi pelaku *cybercrime* dan teroris.



Gambar 1.1 Cara Kerja TOR Network [18]

Segala jenis kejahatan dengan transaksi rahasia, seperti narkoba, pencucian uang, pasar gelap atau bahkan manusia, dapat dilakukan di *Dark Web* [15] [16]. Berikut adalah beberapa contoh kejahatan dark web yang umum [17]:

Tabel 1.1 Aktivitas dan Layanan Ilegal di Dark Web

Aktivitas Ilegal	**Deskripsi**
Violent content	Terorisme, human experiments, gore, *self-destruction*, propaganda teroris
Black market	Penjualan ilegal narkoba, film bajakan, kartu kredit, akun bank dan informasi sensitif lainnya
Malware-as-a-Service	Jasa layanan dan penjualan malware kit, 0day exploit, dan bahkan ransomware.

Penggunaan jaringan TOR memanglah aman, namun tidak dengan Tor Browser sebagai media aksesnya. Tor Browser Bundle (TBB) didevelop menggunakan browser open source Mozilla Firefox dengan tambahan fitur anonim protokol tor-nya. Sama halnya dengan browser lain, TBB memiliki riwayat pencarian, aktifitas download, *cache* dan *cookie* yang tersimpan pada SQLite database dalam bentuk clear text. Sehingga hal inilah yang bisa dimanfaatkan penyidik dalam mengumpulkan barang bukti berupa browser forensik.

Berdasarkan permasalahan dan latar belakang di atas, penelitian ini berfokus pada analisis bukti digital yang terdapat pada RAM menggunakan

metode *National Institute of Standards Technology* (NIST), dengan studi kasus mengungkap bukti kejahatan terorisme pada objek TOR browser.

1.2 Rumusan Masalah

Dari latar belakang masalah tersebut, maka dapat ditentukan beberapa rumusan masalah, diantaranya sebagai berikut :

1. Bagaimana langkah dalam melakukan akuisisi bukti digital pada Tor Browser menggunakan metode Live Forensic?
2. Bagaimana teknik yang bisa diterapkan pada analisis data digital pada RAM?
3. Bagaimana perbandingan hasil analisis teknik analisa data memori ram yang telah di lakukan pada proses penelitian berlangsung?
4. Bagaimana karakteristik bukti digital pada Tor browser?

1.3 Batasan Masalah

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

1. Skenario *suspect* sistem yang digunakan oleh pelaku pada skenario penelitian terbatas pada virtual machine.
2. Proses akuisisi *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 tor Browser 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.
5. Penelitian menggunakan skenario aktivitas surfing seperti browsing kata kunci terkait terorisme yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian jejak digital.
6. Teknik analisa memori ram image yang digunakan adalah file carving dan string *filtering*.

7. Sistem operasi yang digunakan pada lab penelitian adalah Windows 7, dalam hal ini dijadikan sebagai barang bukti komputer yang dipakai pelaku.
8. Skenario surfing yang dilakukan oleh pelaku terbatas hanya mengakses *service* TOR browser tanpa membuka aplikasi lain.
9. Aplikasi yang digunakan untuk melakukan perbandingan file akuisisi RAM dan hasil dari file duplikat adalah MD5 Checker.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya maka tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Melakukan tahapan analisis live forensic untuk mencari informasi barang bukti digital pada Tor Browser. Penelitian ini memperlihatkan secara rinci proses investigasi mulai dari akuisisi barang bukti.
2. Melakukan akuisisi data dan analisis pada RAM.
3. Mengetahui karakteristik bukti digital pada teknik live forensik.
4. Mengimplementasikan teknik *file carving* dan *string filtering* dalam menganalisa barang bukti memori ram image.

1.5 Manfaat Penelitian

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.