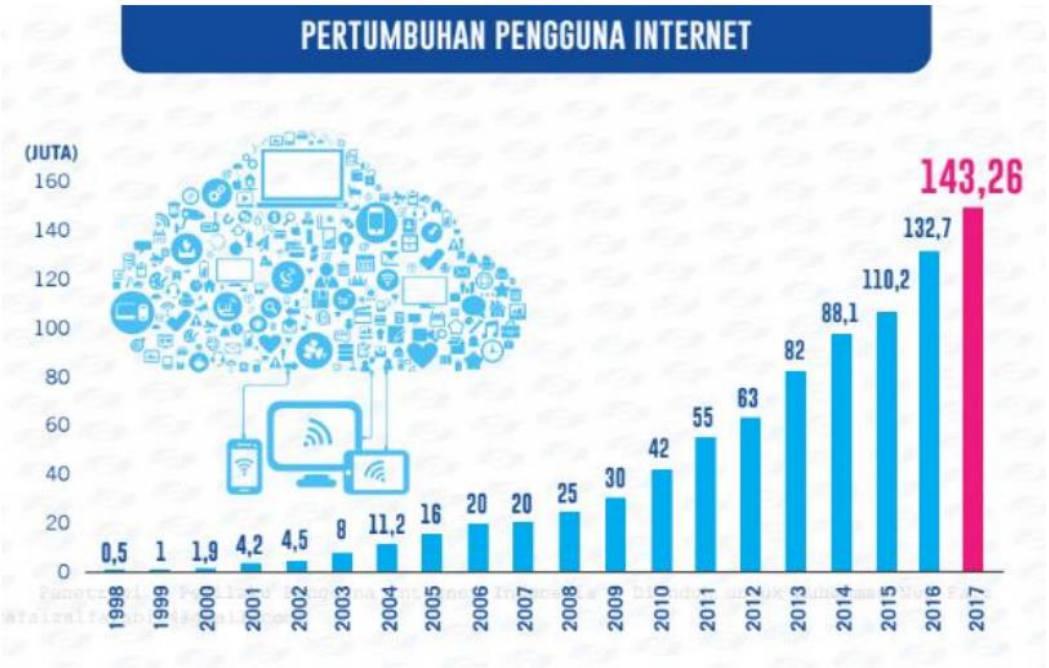
# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

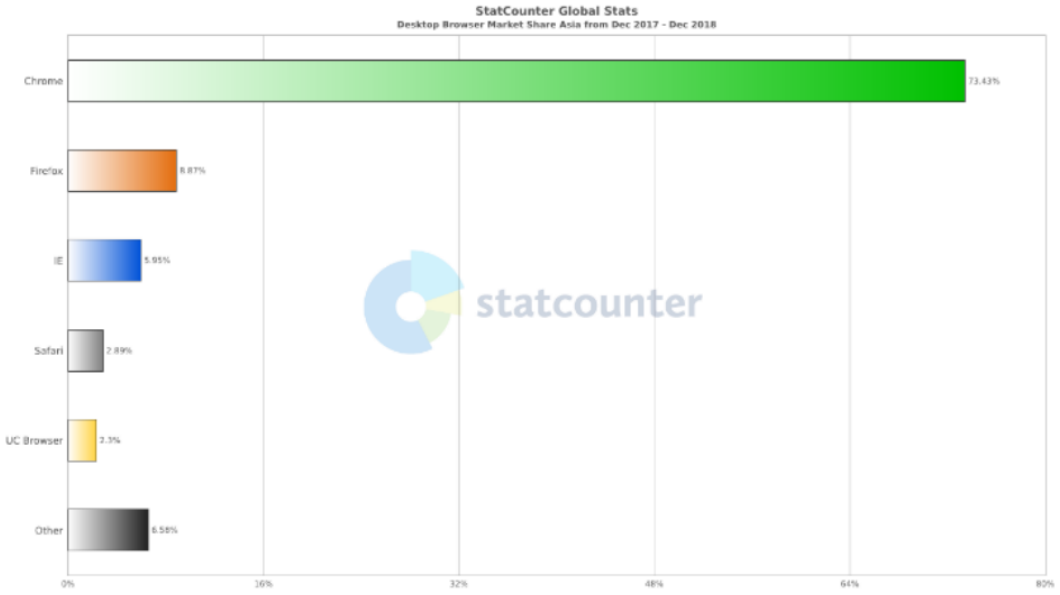
Pada prinsipnya manusia memiliki kebutuhan untuk komunikasi ataupun berinteraksi dengan manusia satu sama lainnya, selanjutnya interaksi ini berbentuk kelompok. Sifat berkelompok ini didasari pada kemampuan dalam berkomunikasi, mengungkapkan rasa dan kemampuan saling bekerja sama. Globalisasi saat ini menjadi penggerak lahirnya era penggunaan teknologi informasi yang mempengaruhi kemudahan kepada manusia dalam hal komunikasi. Selain memberikan dampak positif, perkembangan teknologi informasi dan telekomunikasi juga memberikan dampak negative yaitu banyaknya kejahatan yang berkaitan dengan aplikasi *internet*. Semakin meningkat kejahatan dunia maya diikuti dengan pertumbuhan pengguna *internet* seperti gambar 1. [1]




Data sumber: [2]

Gambar 1. 1 Pertumbuhan Pengguna *Internet* di Indonesia[3]

*Cybercrime* adalah istilah nya dari kejahatan di dunia *internet* atau juga di dunia maya. Dari tahun ke tahun selalu bertambah baik dari sisi jumlahnya maupun variasi kejahatannya. *Internet* pada awal nya hanya untuk mengirimkan pesan singkat atau *e-mail* saja, akan tetapi sekarang *internet* telah digunakan diberbagai aktivitas pekerjaan dan kehidupan manusia setiap hari nya seperti mengirim gambar, video, data yang dikirimkan dengan sangat mudah dan cepat. [2]Berdasarkan data dari Direktorat Tindak Pidana Kejahatan siber (Dit Tipidsiber) Bareskrim Polri Tahun 2017 menangani kasus *cybercrime* sebanyak 5.061, angka itu naik 3% dibandingkan tahun 2016, yang berjumlah 4.931 kasus. Berdasarkan gambar 1.1 tentang Pertumbuhan Pengguna *Internet* di Indonesia, maka diperlukan suatu tindakan berupa prosedur untuk menangani kejahatan pada dunia siber, yaitu salah satunya menggunakan *digital forensics*.




Data sumber : Statcounter, December 2017 – December 2018

Gambar 1. 2Pasar *Web Browser* Desktop di Asia[3]

*Web browser* yang digunakan oleh penggunanya di beberapa wilayah Asia periode Desember 2017 - Desmber 2018. Pengguna *web browser* jenis *Chrome* paling banyak sampai 73,43% dari jumlah pengguna *web browser* di Asia. Pada peringkat berikutnya ada *Firefox* dengan 8,87%, lalu *Internet Explorer* 5,95%, *Safari*, *UC Browser* dan lain-lain. Penggunaan *web browser* yang terus meningkat sehingga dibutuhkan cara untuk menanggulangi jika ada suatu kasus yang melibatkan *web browser*. Ada beberapa yang dapat dijadikan bukti digital yaitu kata kunci, *username,* kunjungan *website*, lokasi penyimpanan, format waktu .yang digunakan dan juga beberapa tools yang digunakan penyidik dalam mencari bukti digital pada *web browser* yaitu *Google Chrome, Mozilla Firefox, Internet Explorer, Safari,* dan *Opera*.[3]

Dari data pertama di atas Direktorat Tindak Pidana Kejahatan siber (Dit Tipedsiber) Bareskrim Polri Tahun 2017 telah menangani kasus *cybercrime* sebanyak 5.061 angka itu naik 3% dibandingkan tahun 2016 yang jumlah 4.931 kasus. Pertumbuhan Pengguna di dunia *Internet* di Indonesia, maka diperlukan suatu tindakan lebih lanjut, dengan salah satu cara yaitu dengan menggunakan *digital forensics*. Pada data kedua dapat disimpulkan bahwa dimana akan ada tindakan kejahatan di dunia maya yang harus ada penanggulangan nya, banyak pengguna *internet* yang menggunakan *web browser* seperti *Google Chrome, Mozilla Firefox, Internet Explorer, Safari*, dan Opera. Dimana *Google Chrome* sebagai *web browser* sering digunakan oleh penggunanya. Ada beberapa yang dapat dijadikan bukti digital seperti kata kunci, *username*, kunjungan *website*, lokasi penyimapanan, dan yang terakhir format waktu.

Terdapat sebuah kasus pada situs *website* cbcindonesia.com pada tahun 2019 yang mengatakan bahwa permohonan dari *browser* chrome dan firefox untuk menyimpan nomor kartu kredit atau kartu debit setelah melakukan transaksi pada platform, alamat penagihan, nama dan nomor paspor di situs travel, karena data tersebut dapat disalahgunakan oleh pelaku kejahatan di dunia maya. Sebagian pengguna dari *internet* banyak

sekali menjalankan autofill di *browser*. Alasannya demi kemudahan dan tidak khawatir lupa kata sandi (password). Akan tetapi ini bisa menjadi jalan bagi pelaku kejahatan didunia maya yang telah memasang malware pada perangkat korban. Lembaga riset kemanan siber *Kapersky* menemukan scenario ini menjadi semakin popular dikalangan *scammers online*. Pada paruh pertama tahun ini saja, produk kemanan *Kapersky* mendeteksi lebih dari 940.000 aksi pencurian.

Dengan banyak nya aktivitas dan informasi yang dilakukan menggunakan *web browser* semua aktivitas itu direkam dalam database *web browser* tersebut. Informasi aktivitas ini seperti daftar kunjungan URL, kata kunci pencarian, hal ini dijadikan bukti yang akan berpotensi mengungkap kejahatan oleh para ahli digital *forensics*. Penggunaan berbagai *web browser* juga dapat dianalisis untuk mengetahui alur dari pengguna *web* tersebut. Dengan *web browser* yang digunakan sebagai penelitian ini ialah *google chrome*, *opera*, *mozilla firefox*, *uc browser*, *microsoft edge*. *Tool* yang digunakan oleh peneliti ialah *The Sleuthkit* (*Autopsy*), *EnCase*, *FTK Imager*. [3]

Beberapa penelitian yang telah dilakukan terkait dengan bukti digital pada *web browser forensics* diantaranya dengan penelitian yang diteliti [3] bahwa setiap aktivitas pada web ialah data yang akan diungkapkan dalam suatu pikiran dan niat pengguna seperti kata pencarian, kunjungan *web*, *file* yang diunduh. Dengan yang diteliti ialah aktivitas *web browser* harus diperiksa secara rinci.

*Dead forensic* merupakan suatu metode yang membutuhkan data sistem yang telah tersalin tanpa bantuan sistem operasi tersangka, Secara histori penggunaan computer, istilah dead forensic yang tertuju panda suatu kondisi hanya sistem operasi, data tersebut tersimpan secara permanen dalam perangkat media penyimpanan umumnya hardisk dan flasdisk.[2]

*Autopsy* merupakan sebuah *software* yang digunakan untuk melihat kembali data yang disimpan dan juga memberikan informasi mengenai *hex*, *strings*, *file*, *file metadata*, *results*, maupun *indexted text*.[3] Dengan ada nya *autopsy* ini yang akan melihat data-data penting pada browser seperti Mozilla Firefox, Internet Explorer (Versi 4,0-9,0), Google Chorme, UCBrowser dan Opera. Aplikasi ini digunakan untuk me*recover* di website, termasuk situs web popular seperti Yahoo, Gmail, Facebook, Google, dll.

Penggunaan dead forensic pada pencarian data yang berada di *browser*, penelitian ini dikarenakan pada penelitian sebelumnya menggunakan bukti digital pada freeze ssd(Solid State Drive). Lalu akan dikembangkan lagi untuk mencari data-data lainnya. Dimana data tersembunyi meninggalkan jejak atau masih berada di suatu *browser* yang telah digunakan. Informasi yang didapatkan pada suatu *browser* yang akan di uji coba yaitu *Google Chrome*, *Mozilla Firefox*, *Microsoft Edge*, *UCBrowser*, dan *Opera* dimana *browser-browser* dan tambahan software tersebut sebagai pembuktian hasil bukti digital.[4]

Dari Latar belakang permasalahan tersebut, penulis bermaksud untuk menganalisa *browser* menggunakan metode *dead forensik* pada suatu komputer yang telah terinstall *browser Google Chrome*, *Mozilla Firefox*, *Microsoft Edge*, *UCBrowser*, dan Opera, yang mana akan menganalisa dari suatu kejahatan yang terdapat di *browser* tersebut dengan bantuan *Autopsy*, *EnCase* dan juga *FTK Imager* sebagai perbandingan.

## 1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah pada penelitian ini, Bagaimana menerapkan analisis *browser* yang berada di komputer dalam kasus transaksi untuk mendapatkan bukti digital?

## 1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang ada maka dapat diketahui tujuan dari penelitian ini, Mendapatkan hasil bukti digital melalui konsep analisis bukti digital berupa *cache* yang berada di *browser* telah tersimpan di *harddisk* pada komputer dalam kasus transaksi *illegal* dengan *dead forensik.*

## 1.4. Manfaat Penelitian

Dari penelitian ini, manfaat yang dapat diambil yaitu :

1. Menambahkan pengetahuan dan juga dapat menarapkan ilmu digital *forensic*.
2. Mengetahui proses akuisisi dan juga analisis *harddisk* komputer.
3. Mendapatkan informasi sebuah data yang ada pada harddisk komputer sebagai barang bukti digital.

## 1.5. Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan- batasan masalah penelitian sebagai berikut :

1. *Dead* Forensic sebagai analisis *forensic*, yang dianalisa pada penelitian ini adalah *browser* yang sering digunakan atau banyak digunakan oleh *user Google Chrome, Mozilla Firefox, Microsoft Edge,* dan *Opera*
2. *Tools* yang digunakan adalah *FTK Imager,* dan *Autopsy*.
3. Studi kasus yang dianalisa *Facebook, Instagram, Twitter, Linkedin, Whatsapp,* dan *Pinterest*.
4. Penelitian ini tidak menggunakan *incognito* atau samaran.

## 1.6. Sistematika Penelitian

Struktur penulisan yang digunakan untuk menjelaskan jawaban dari pertanyaan yang diajukan untuk tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bagian ini berisi mengenai latar belakang pengambilan1 suatu persoalan, identifikasi masalah dari persoalan tersebut, tujuan yang akan dicapai , rumusan masalah yang muncul dari tujuan yang diinginkan, batasan masalah yang digunakan, dan sistematika penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan penjelasan secara singkat mengenai penelitian yang telah dilakukan sebelumnya serta teori yang digunakan dalam tugas akhir ini, dimulai dari penjelasan tentang dasar teori yang digunakan, dan juga *tools* yang digunakan apa saja.

BAB III METODE PENELITIAN

Pada bab ini dijelaskan mengenai simulasi yang digunakan serta skenario uji yang dilakukan.

BAB IV ANALISIS DAN PEMBAHASAN

Pada bab ini dijelaskan hasil pengujian dari simulasi yang telah dilakukan. *Tools* yang digunakan adalah *autopsy* dan *ftk imager* akan digunakan sebagai parameter uji dari simulasi tugas akhir ini.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang mengacu pada tujuan yang ingin dicapai dan saran untuk penelitian selanjutnya.