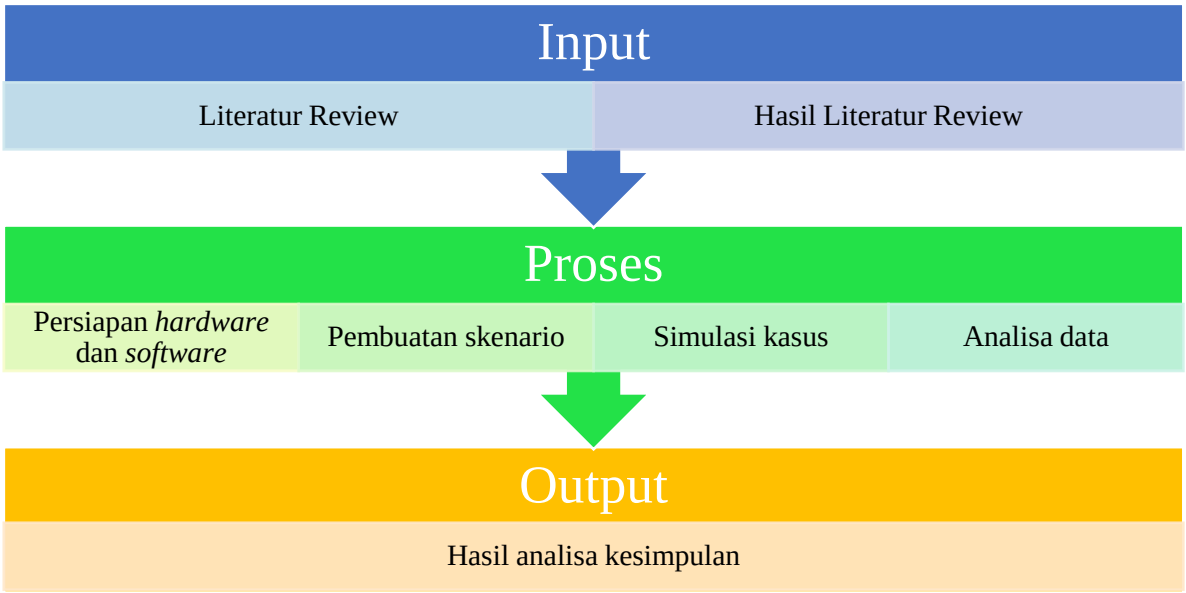
BAB 3
Metodologi Penelitian

Dalam penelitian ini dijabarkan tahapan penelitian, sehingga dapat diketahui urutan langkah –langkah penelitian sebagai pedoman yang jelas dan mudah dalam menyelesaikan penelitian. Urutan langkah-langkah penelitian dapat dilihat pada gambar 3.1.



Gambar 3.1 Alur Metodologi Penelitian

3.1 Studi Pustaka

Studi pustaka merupakan aktivitas kegiatan mempelajari *literature review* mengenai uraian dari teori-teori, temuan, maupun rangkuman dari penelitian-penelitian yang telah dilakukan sebelumnya sebagai landasan dan acuan dalam melakukan penelitian.

Sumber *literature review* yang digunakan dalam penelitian ini diambil dari jurnal, artikel, *paper*, buku, *website*, dan sumber lainnya yang membahas tentang Jumplist, Windows forensik, aplikasi *recovery file*, dan aplikasi untuk analisa isi jumplist.

3.2 Kebutuhan Perangkat Keras

Perangkat keras yang digunakan dalam mendukung implementasi penelitian ini adalah satu buah komputer desktop merk Lenovo seri ThinkCentre Edge 72dengan spesifikasi sebagai berikut :

Tabel 3.1 Spesifikasi Komputer Desktop

Tipe desktop	Tower
Merk/Model	Lenovo/Thinkcentre Edge71
Processor	Intel(R)Core(TM) i7 -2600K @ 3.40 GHz
Memory	4 GB DDR3 665MHz
Storage	SATA 500 GB
Graphics	Intel Standard VGA Graphics Adapter
Optical Drives	TSSTcorp DVD-RW SH-216AB

3.3 Kebutuhan Perangkat Lunak

Adapun kebutuhan perangkat lunak / *software*yang digunakan dalam proses analisa adalah sebagai berikut :

1. OS Windows 10
2. Linux Santoku
3. JumpListExt
4. Belkasoft Evidence Center

3.4 Skenario dan simulasi kasus

Dalam penelitian ini disusun sebuah skenario dan simulasi kasus sebagai berikut:

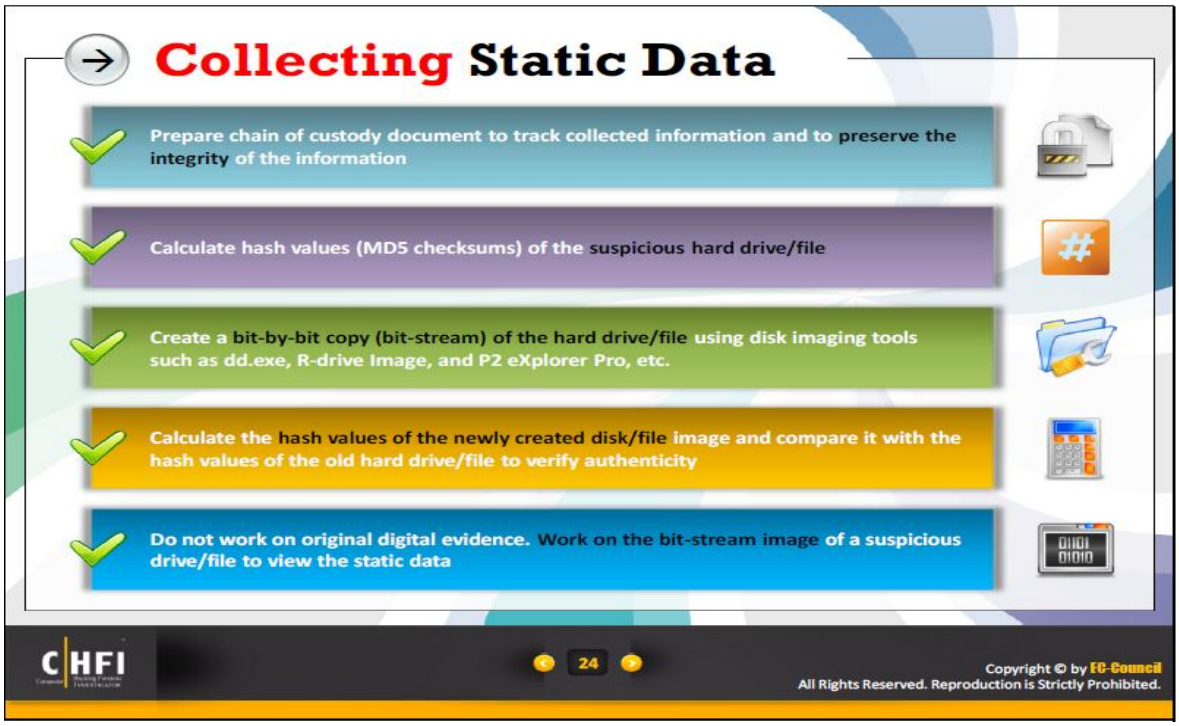
Dalam penelitian ini, disimulasikan sebuah kasus dimana seorang karyawan A mengambil data transaksi keuangan berupa pembayaran gaji dari komputer atasannya dengan maksud menaikkan gaji yang diterimanya. Karyawan A mengcopy ke dalam flashdisk sebuah file dengan nama file “2. Oktober 2018” yang mana file tersebut berisi rincian gaji masing-masing karyawan yang akan dibayarkan di bulan November. Karyawan A kemudian mengedit isi file tersebut menggunakan komputernya dengan menaikkan penerimaan gajinya dan beberapa karyawan yang lain serta menurunkan gaji pada karyawan lainnya lagi tanpa merubah nominal total pembayaran gaji di bulan November tersebut untuk menghindari kecurigaan. Selanjutnya karyawan A tersebut mengembalikan file tersebut ke komputer atasannya dan menghapus riwayat akses file

komputernya sebagai upaya menghilangkan jejak dengan cara menghapus riwayat akses pada komputernya dengan cara menghapus file Jump Lists melalui direktori Windows explorer pada direktori *AutomaticDestinations*.

3.5 Akuisisi dan analisa data

Tahap akuisisi data pada penelitian ini dilakukan secara statik forensik.Proses akuisisi sendiri terbagi menjadi 3 jenis yaitu akuisisi pada perangkat menyala, akuisisi pada perangkat yang tidak menyala, dan partial akuisisi(Sudyana, Sugiantoro, & Luthfi, 2016). Penentuan akuisisi didasarkan pada hasil identifikasi barang bukti. Pada akuisisi dengan perangkat yang tidak menyala, dilakukan dengan prosedur statik akuisisi dengan melakukan *imaging bit stream copy* terhadap media penyimpanan data.

Menurut (Ramadhan, Prayudi, & Sugiantoro, 2017) fokus dari statik forensik adalah pemeriksaan hasil *imaging* untuk menganalisis isi dari bukti barang digital , seperti *file* yang dihapus, *history web browsing*, berkas fragmen, koneksi jaringan, *file* yang diakses, *history login user*, dan lain-lain untuk membuat *timeline* ringkasan kegiatan pada bukti digital sewaktu digunakan.Gambar 3.3 menunjukkan tahapan mendapatkan data bukti barang digital secara statik forensik.



Gambar 3.2Tahapan mendapatkan data statik

(Sumber : modul 09 CHFI)

3.5.1 Sumber data

Sumber data penelitian ini didapatkan pada perangkat komputer desktop dengan sistem operasi Windows 10 dari *history* Jump Lists, yang berada di *drive* C dengan kondisi *entries* Jumplist sebelum dihapus dan setelah dihapus. Studi kasus yang akan diterapkan dalam penelitian menggunakan metode statik forensik,dimana data diperoleh dari perangkat komputer desktop yang tidak menyala. Dari skenario yang telah dibuat data tersebut adalah riwayat akses sebuah file excel dengan nama file 2. Oktober 2018.xlsx sebagai bukti dalam kasus pencurian data transaksi keuangan berupa pembayaran gaji.

3.5.2 Proses mendapatkan data

Proses mendapatkan data dalam penelitian ini diperoleh dengan menggunakan metode statik forensik. Akuisisi dilakukan menggunakan *tools* Linux Santoku pada *drive* C dengan langkah awal membuat *hashing,* yang kemudian dilakukan *imaging bit stream copy* untuk mendapatkan file *image.dd.* Langkah berikutnya adalah melakukan penghapusan catatan yang berada di Jump Lists, selanjutnya dilakukan akuisisi lagi pada *drive* C hingga didapatkan file *image.dd* yang kedua, dan kemudian dilakukan analisa terhadap kedua file tersebut.

3.5.3 Target hasil penelitian

Berdasarkan skenario yang telah dibuat, analisa dilakukan terhadap data-data yang didapatkan melalui *tools* yang sudah ditentukan, yaitu JumpListEx.dan Belkasoft Evidence Center. Dari analisa pada kedua file *image.dd* tersebut hasil yang diharapkan adalah mendapatkan gambaran yang jelas catatan informasi *entries* di Jump Lists sebelum dan setelah terhapus, baik berupa tipe file, lokasi file, *create date, accessdate*, *last modified* terutama pada riwayat akses file excel dengan nama file 2. Oktober 2018.xlsx sebagai bukti dalam kasus pencurian data transaksi keuangan.