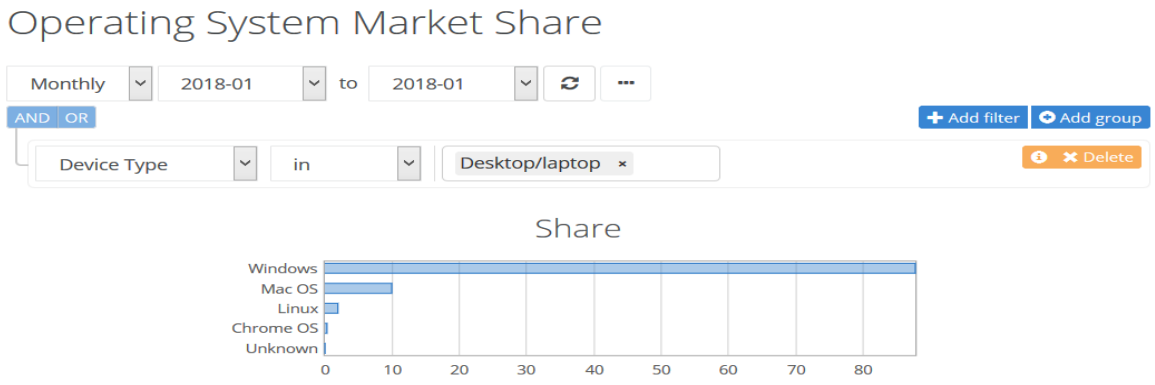
BAB 1
Pendahuluan

1.1 Latar Belakang

Windows 10 adalah sistem operasi dari Microsoft Corporation untuk server, PC desktop, laptop, tablet, ponsel, dan perangkat terkait lainnya yaitu Internet of Things (Staff, 2016) dan dirilis di seluruh dunia pada 29 Juli tahun 2015. Sejak dirilis Windows 10 sudah terpasang di 75 juta PC dan mengalami kenaikan pada minggu ke-10 menjadi 110 juta perangkat. Pada bulan November 2017 sistem operasi Windows 10 telah terpasang di 600 juta perangkat, angka tersebut meliputi perangkat PC, tablet, konsol game Xbox One, *headset mixed reality* HoloLens dan papan tulis pintar *Surface Hub* (Rizal, 2017). Faktor percepatan penggunaan Windows 10 dikarenakan beberapa hal, seperti tawaran *upgrade* secara gratis dari Windows 7 dan Windows 8.1 serta peningkatan jumlah pemilik perangkat komputer baru yang memerlukan sistem operasi.

Menurut laporan perusahaan riset (NetMarketShare, 2018) menunjukkan bahwa pada bulan Januari 2018 Sistem operasi window memiliki *marketshare* tertinggi dengan persentasi 87,79%. Sedangkan posisi kedua ditempati Mac OS sebanyak 9,95%, Linux sebanyak 1,93% dan chrome OS dengan *marketshare* 0,31%.

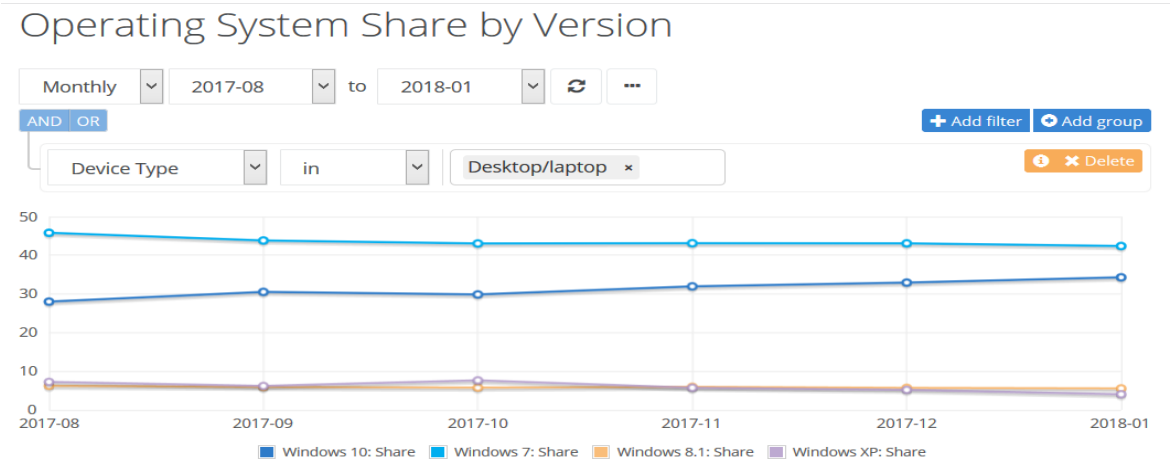


Gambar 1.1 *Marketshare* Sistem Operasi

(https://netmarketshare.com/operating-system-market-share.aspx)

Berdasarkan versi dari sistem operasi Windows, pada rentang bulan Juli 2017 sampai dengan Bulan Januari 2018 pengguna Windows 10 mengalami tren peningkatan jumlah pengguna sebanyak 6,28% dari 28,01% di bulan Agustus 2017 dan pada bulan Januari 2018 mengalami kenaikan menjadi 34,29%. Hal tersebut berbanding terbalik dengan Windows 7,

walaupun masih memiliki *marketshare* tertinggi di bulan Januari 2018 sebanyak 42,39%, namun dalam periode yang sama mengalami penurunan sebanyak 3.42%. Dengan perkembangan tersebut menunjukkan bahwa sebagian pengguna operasi Windows telah beralih ke sistem operasi Windows 10.



Gambar 1.2 Pengguna OS Windows (Agustus 2017 - Januari 2018)

(https://netmarketshare.com/operating-system-market-share.aspx)

Pada Windows 10 memiliki beberapa fitur baru, yang diantaranya adalah Jump Lists. Fitur Jump Lists mulai diperkenalkan pada Windows 7 hingga saat ini versi Windows 10. Jump Lists menyediakan informasi aktifitas pengguna pada perangkat komputer berupa *interface* berisi daftar file yang sebelumnya telah diakses, file yang sedang diakses, serta link halaman web yang baru dikunjungi. Definisi Jumplist menurut peneliti terdahulu dapat diuraikan sebagai berikut :

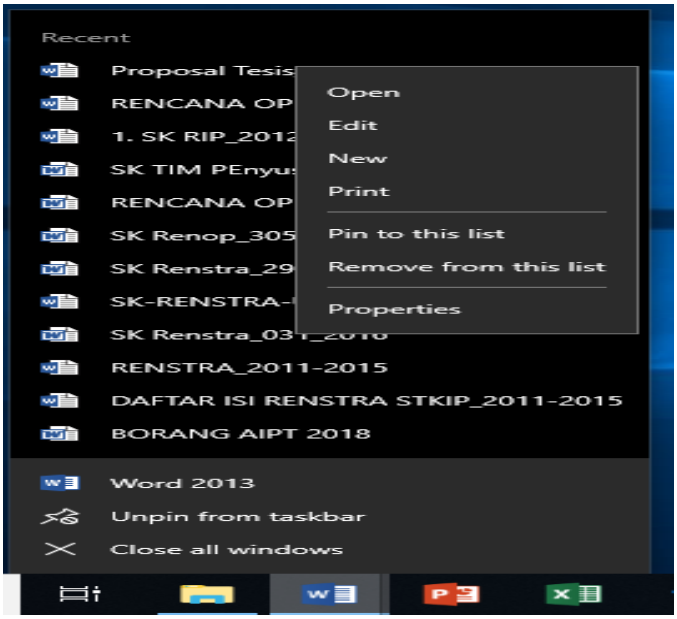
1. Jump Lists adalah fitur baru dari sistem operasi Windows yang menunjukkan file dan tugas-tugas yang paling baru atau yang paling sering digunakan oleh pengguna (Ghafarian, 2015).
2. Jumplist adalah antarmuka grafis yang terkait dengan setiap aplikasi yang diinstal yang berisi daftar file-file yang sebelumnya telah diakses oleh aplikasi tersebut (lynes 2012)
3. Jumplist adalah jalan pintas untuk item baru atau yang sering diakses terkait dengan program atau situs web (lalli)
4. Jumplist adalah catatan aktivitas pengguna baru pada komputer (Stevenson)

Dari keempat definisi di atas, pengertian atau definisi jumplist dapat disimpulkan "Catatan aktifitas penggunaan pada komputer berupa file-file yang paling baru atau paling sering digunakan per basis aplikasi".

Jumplist berfungsi untuk mempermudah pengguna komputer seperti membuka file yang baru dikerjakan, melakukan pin pada file tertentu, terutama jika mengerjakan file yang sama setiap hari.

Terdapat beberapa cara atau metode yang dapat digunakan untuk menghapus entri jumplist diantaranya adalah:

1. Secara manual dengan cara memilih setiap entri yang terdapat di *Taskbar* melalui klik kanan dengan *mouse* dan pilih "*Remove from this list".*



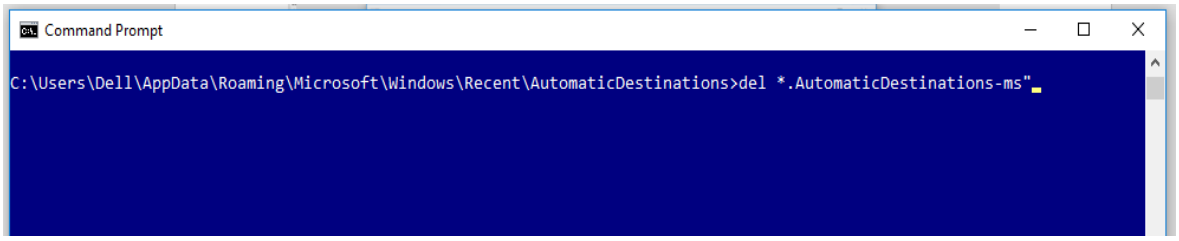
Gambar 1.3 Menghapus Jumplist Melalui Taskbar

Pada metode penghapusan ini, akan menghapus daftar jumplist yang terdapat pada aplikasi di *taskbar*, namun demikian tidak menghilangkan file jumplist yang berada di direktori "*AutomaticDestinations".* Daftar Jumplist yang dapat dihapus hanya pada file yang tidak diberi tanda "Pinned".

2. Melalui Start menu dengan melakukan klik kanan pada aplikasi yang dipilih selanjutnya klik kanan pada file yang akan dihapus dari daftar jumplist. Pada metode penghapusan ini memiliki dampak yang sama dengan metode penghapusan melalui *taskbar*.

Gambar 1.4 Menghapus Jumplist melalui Start menu

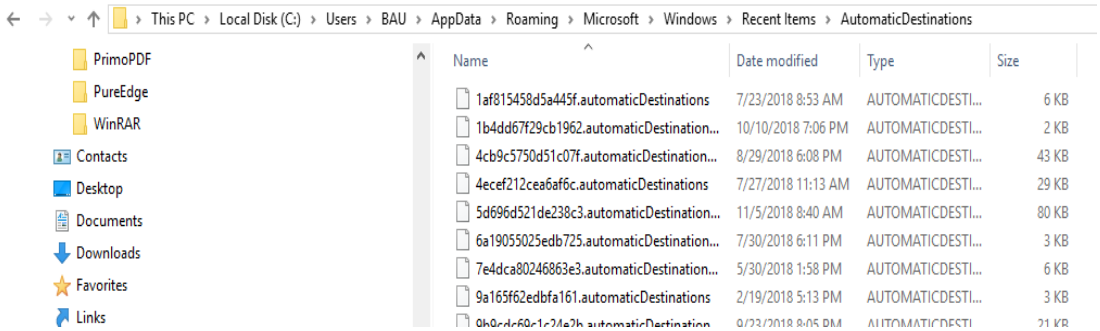
3. Penghapusan melalui Command prompt



Gambar 1.5 Menghapus Jumplist melalui CommandPrompt

Pada metode penghapusan ini, akan menghilangkan file-file jumplist pada direktori "*AutomaticDestinations-MS*, namun demikian tidak menghapus file yang berada di direktori *Recent*. Cara penghapusan menggunakan *command prompt* digunakan untuk menghapus secara paksa dan File-file yang terhapus melalui command prompt tidak masuk ke Recycle bin.

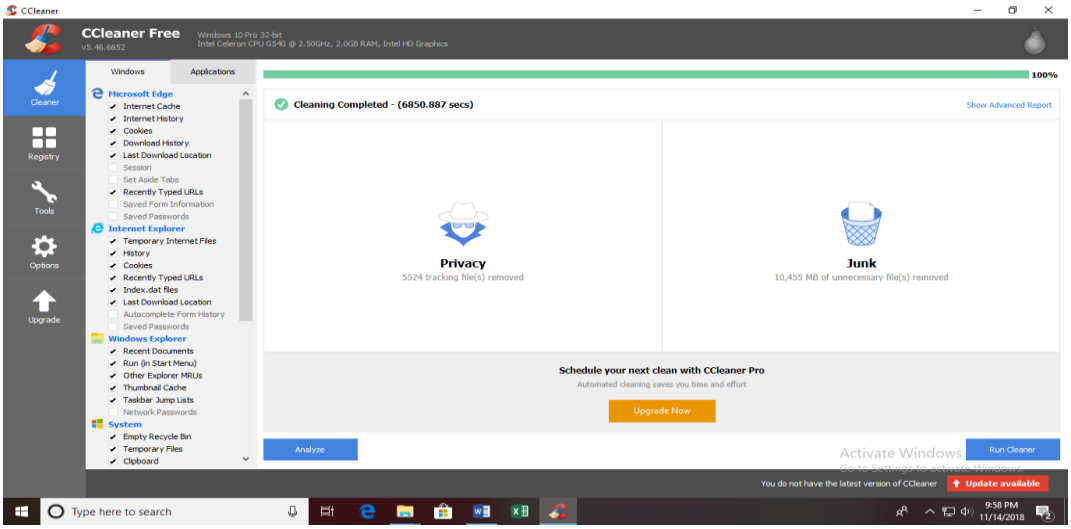
4. Penghapusan melalui direktori windows explorer pada direktori *AutomaticDestinations*



Gambar 1.6 Menghapus Jumplist melalui direktori *AutomaticDestination*

Pada metode penghapusan ini file yang terhapus akan masuk ke *recycle bin*. Metode ini juga akan menghilangkan file pada direktori *Recent*.

5. Penghapusan melalui Aplikasi



Gambar 1.7 Menghapus Jumplist melalui Aplikasi

Pada metode penghapusan menggunakan aplikasi seperti CCleaner yang terjadi adalah menghapus file jumplist pada taskbar, start menu maupun direktori "*Recent*". Akan tetapi pada direktori "*AutomaticDestinations*" masih terdapat *AppIds* dari file-file jumplist yang terhapus.

Jumplist berpotensi menjadi sumber bukti berharga yang dapat mengarahkan secara langsung interaksi pengguna dengan komputer (Team, 2017). Jump Lists memiliki dua jenis, *custom destinations* dan *automatic destinations.* Pada *custom destinations* dibuat saat pengguna melakukan '*pins'* atau memasangkan file ke *Start Menu*atau *Task bar*. Lokasi *custom destinations* terletak di :

C:\Users\<UserProfile>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Sedangkan *automatic destinations* dibuat secara otomatis saat pengguna berinteraksi dengan sistem yang melakukan tindakan seperti membuka aplikasi atau mengakses file. Lokasi *automatic destinations* terletak di :

C:\Users\<UserProfile>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Penelitian-penelitian mengenai Jump Lists pernah dilakukan diantaranya oleh (Singh & Singh, 2016) dalam penelitiannya tentang Jump Lists menyebutkan bahwa Jump Lists memiliki potensi untuk menyediakan sumber bukti tentang aktifitas pengguna ke penyidik. Penelitian tersebut berhasil mengurai struktur Jump Lists pada Windows 10 dan upaya anti forensik yang dilakukan pada Jump Lists.

(Stevenson Smith, 2013) dalam penelitiannya mengungkapkan jejak lengkap penipu dalam menciptakan dokumen palsu atau kegiatan ilegal lainnya ketika menggunakan komputer serta metode yang dapat digunakan untuk mengidentifikasi artifak yang berada di Jump Lists dan potensi untuk digunakan sebagai bukti forensik dalam kasus penipuan keuangan.

Keberdaan Jump list sendiri masih sedikit dikenal oleh pelaku kejahatan, namun demikian tidak menutup kemungkinan dihilangkannya catatan *entries* Jump Lists tersebut. Dengan keberadaan catatan yang terdapat di Jump Lists, menyebabkan tindakan-tindakan atau upaya yang dilakukan dalam menghilangkan bukti digital, termasuk di dalamnya menghapus catatan *entries* Jump Lists.Kondisi tersebut mengakibatkan diperlukannya metode dalam menangani tindakan menghilangkan bukti digital. Walaupun telah dihapus, seharusnya catatan yang berada dalam *entries* Jump Lists tetap dapat ditelusuri.Hasil yang diharapkan dari analisa yang dilakukan adalah mendapatkan catatan informasi artifak digital dari *entries* Jump Lists.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka dibuat rumusan masalah sebagai berikut:

Informasi artefak digital apa saja yang terdapat pada pada *entries* Jump Lists sebelum dan sesudah terhapus?

1.3 Batasan Masalah

Sesuai latar belakang dan rumusan masalah yang telah dijelaskan di atas, maka peneliti memberikan batasan masalah sebagai berikut :

1. Perangkat yang digunakan dalam penelitian ini adalah komputer desktop dengan operasi sistem Windows 10.
2. Kegiatan akuisisi hanya dilakukan pada *entries* Jump Lists
3. Analisa dilakukan hanya pada metode penghapusan melalui Windows Explorer pada direktori *Automatic Destinations.*

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah mendapatkan gambaran yang jelas catatan informasi artifak digital yang terdapat pada *entries* Jump Lists sebelum dan sesudah terhapus.

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai dalam penelitian ini adalah :

1. Untuk penulis diharapkan dapat meningkatkan wawasan baik secara teori maupun praktek dalam pengembangan kualitas akademis dan non akademis.
2. Untuk pengembangan keilmuan diharapkan dapat sebagai alternatif bahan pertimbangan dalam penanganan investigasi forensik operasi sistem Windows 10 pada perangkat desktop.

1.6 Review Penelitian

Pada bagian ini akan dibahas ulasan tentang penelitian yang relevan dan telah dilakukan sebelumnya berkaitan dengan penelitian mengenai Jump Lists.

Pada penelitian yang dilakukan (Singh & Singh, 2016) mengidentifikasi struktur Jump Lists di Windows 10 dan membandingkannya dengan Windows 7/8. Selanjutnya struktur Jump Lists tersebut diuraikan menggunakan *tool* JumpListExt. Selain itu, artifak yang dicatat dari empat web browser juga diuraikan dan ditunjukkan dalam aktifitas waktu selama periode waktu menggunakan Jump Lists.

Penelitian sebelumnya yang dilakukan oleh (Ghafarian, 2015) menyelidiki nilai-nilai forensik Jump List data dengan menggunakan beberapa *tools* untuk melihat data pada mesin virtual. Dalam penelitian ini juga menyajikan analisis komparatif kinerja *tools*.

(Stevenson Smith, 2013) dalam penelitiannya mengungkapkan jejak lengkap penipu dalam menciptakan dokumen palsu atau kegiatan ilegal lainnya ketika menggunakan komputer serta metode yang dapat digunakan untuk mengidentifikasi artifak yang berada di Jump Lists dan potensi untuk digunakan sebagai bukti forensik dalam kasus penipuan keuangan.

Pada penelitian lain yang dilakukan oleh (Barnett, 2012) memberikan gambaran tentang fungsi dan perilaku dari Jump Lists dan juga memeriksa struktur Jump Lists dengan maksud mengusulkan penelitian lebih lanjut untuk dimanfaatkan dalam kapasitas forensik.

Penelitian mengenai Jump List juga dilakukan oleh (Lallie, Harjinder S. and Bains, 2012) dengan menganalisis struktur dari konfigurasi file di Jump Lists dan khususnya rekaman dari konfigurasi file serta beberapa *entries* penting di dalamnya.

(Lyness, 2012) membahas tentang jenis dan tingkat informasi yang dicatat oleh fitur Jump Lists untuk aplikasi yang berbeda seperti Notepad, Microsoft Word, dan lain-lain serta struktur catatan-catatan dan tindakan pengguna yang menyebabkan diperbarui.

Tabel 1.1 Literatur Review

No	Paper Utama	Jump Lists	Versi Windows		Yang diuji		Metode	Fokus penelitian
			7	10	App. Windows dan Office	Web Browser		
1	(Singh & Singh, 2016)	√	-	√	-	√	Deteksi upaya anti forensik pada Jump Lists	Konsistensi struktur Jump Lists
2	(Ghafarian, 2015)	√	√	-	√	√	Analisis komparatif kenerja *tools* untuk melihat data Jump Lists	Melihat isi folder tersembunyi
3	(Stevenson Smith, 2013)	√	√	-	√	√	Deteksi dokumen palsu melalui *timeline* dokumen	Identifikasi artifak dokumen palsu atau kegiatan ilegal dalam kasus penipuan keuangan berdasarkan *timeline* penciptaan dokumen
4	(Barnett, 2012)	√	√	-	-	√	Melakukan download dan upload gambar dari beberapa web browser kemudian informasi yang disimpan di Jump Lists dibandingkan secara manual untuk web yang berbeda	Gambaran fungsi dan perilaku dari Jump List dengan melakukan *download* dan *upload* melalui web browser serta struktur file
5	(Lallie, Harjinder S. and Bains, 2012)	√	√	-	√	√	Instalasi Microsoft Windows 7 dengan memasukkan sejumlah file, URL, dan program yang diakses untuk membuat *entri* Jump Lists. Dilakukan pencatatan waktu/tanggal untuk mengkorelasikan file dengan *entri* dalam Jump List	Analisa struktur dari file konfigurasi dan catatan file konfigurasi dari Jump Lists

No	Paper Utama	Jump Lists	Versi Windows		Yang diuji		Metode	Fokus penelitian
			7	10	App. Windows dan Office	Web Browser		
6	(Lyness, 2012)	√	√	-	√		Instalasi VMWare dan Windows 7, selanjutnya melakukan modifikasi konfigurasi di kotak dialog 'Customize Start Menu' berikutnya membuka sejumlah file sampel, dan melakukan 'pin' satu entri masing-masing dari Jump Lists, melakukan instalasi aplikasi dan setelah membuka 2 file aplikasi tersebut di *uninstal.* Langkah selanjutnya menyelidiki seberapa sering file diakses, apakah tanggal/waktu akses file dicatat, menghapus, memindah dan mengganti nama file.	Analisa informasi yang dicatat oleh fitur Jump Lists, struktur catatan-catatan dan tindakan yang mengakibatkan terjadinya update yang dilakukan oleh pengguna
Usulan Penelitian		Peneliti akan melakukan akuisisi pada *entries*Jump Lists pada OS Windows 10 di perangkat desktop					Fokus dari penelitian ini adalah menguji *entries* di Jump Lists sebelum terhapus dan setelah dilakukan penghapusan untuk mengetahui apakah terdapat perbedaan informasi pada *entries* Jump Lists tersebut.	

Paparan singkat mengenai penelitian ini tertulis pada tabel 1.2 Penelitian yang diusulkan

Tabel 1.2 Penelitian yang diusulkan

Judul	Uraian singkat masalah penelitian	Solusi	Hasil yang diharapkan
Analisis Forensik *deleted entries*Jump Lists Windows 10 pada Perangkat Komputer Desktop	Penelitian ini membahas tentang *entries* yang berada di Jump Lists Windows 10 di perangkat komputer desktop untuk mengetahui catatan informasi pada saat sebelum dan setelah terhapus. Skenario dan studi kasus dalam penelitian ini adalah pencurian data transaksi keuangan berupa pembayaran gaji. Pelaku tindak kejahatan dalam rangka menghilangkan jejaknya, menghapus riwayat akses pada komputernya dengan cara menghapus file Jump Lists melalui direktori Windows explorer pada direktori *AutomaticDestinations*.	Melakukan akuisisi *deleted entries* Jump Lists menggunakan JumplistExt dan Belkasoft Evidence Center untuk mengetahui informasi sebelum dan sesudah terhapus.	Memberikan gambaran yang jelas catatan informasi *entries* di Jump Lists sebelum dan setelah terhapus.

1.7 Metodologi Penelitian

Dalam melakukan penelitian, perlu disusun langkah-langkah metodologi dalam menyelesaikan penelitian. Adapun langkah-langkah yang ditepuh selama melakukan penelitian ini adalah sebagai berikut:

1. Studi pustaka

   Langkah pertama dalam penelitian ini dimulai dengan melakukan studi kepustakaan dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik berupa artikel, jurnal, makalah, paper, maupun situs internet yang menunjang dalam pelaksanaan penelitian.

2. Persiapan alat dan bahan

   Kebutuhan alat dan bahan dalam penelitian ini adalah perangkat komputer dengan operasi sistem Windows 10 serta *tools* yang akan digunakan dalam melakukan analisa.

3. Skenario kasus, akuisisi dan analisa

   Pada bagian ini dilakukan skenario kasus dimanaseorang 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*.

   Langkah beikutnya dilakukan analisa untuk mendapatkan gambaran yang jelas catatan informasi*entries* Jump Listssebelum dan setelahterhapus.

4. Laporan

   Laporan adalah bagian terakhir penelitian dengan membuat tulisan selama proses penelitian.

1.8 Sistematika penulisan

Sistematika penulisan dalam penelitian ini, terbagi dalam beberapa BAB yaitu :

BAB I Pendahuluan

Pada BAB ini merupakan pengantar terhadap permasalahan yang akan dibahas. Dalam BAB ini memberikan gambaran tentang penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, review penelitian, metodologi penelitian dan sistematika penulisan.

BAB II Tinjauan pustaka

Pada BAB ini menjelaskan tentang teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini.

BAB III Metodologi Penelitian

Pada BAB ini berisi tentang gambaran secara umum proses akuisisi pada *deleted entries* Jumplists Windows 10 diperangkat komputer desktop.

BAB IV Hasil dan Pembahasan

Pada BAB ini membahasa tentang hasil implementasi dari proses akuisisi pada *deleted entries* Jumplists Windows 10 diperangkat komputer desktop.

BAB V Kesimpulan dan Saran

Kesimpulan dan saran merupakan tahapan akhir dari peneliti yang berisi dari uraian pada setiap bab sebelumnya serta saran berdasarkan temuan selama penelitian, serta rekomendasi untuk pengembangan penelitian selanjutnya.