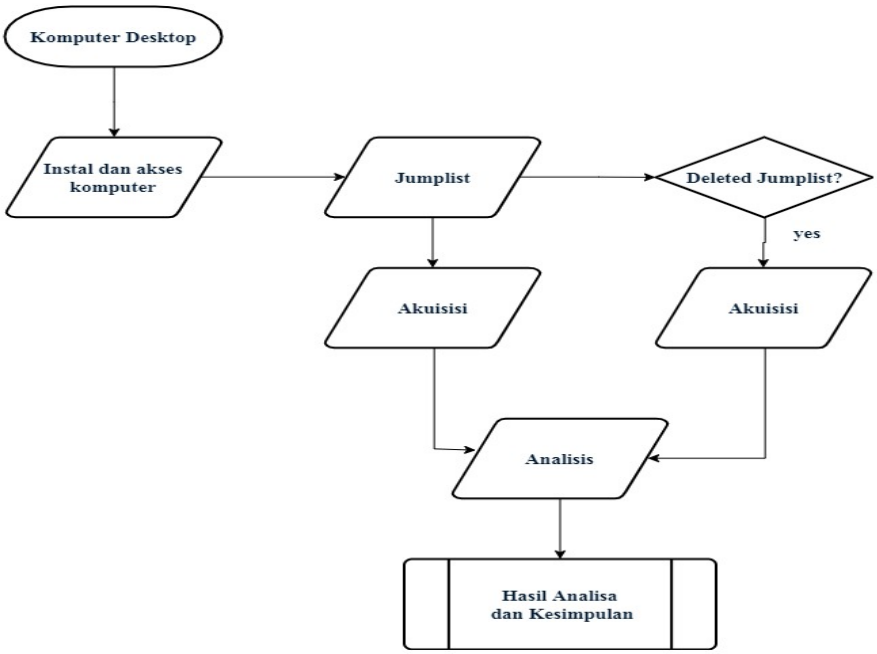
BAB IV
Hasil dan Pembahasan

4.1 Skenario dan Simulasi Kasus

Skenario kasus dalam penelitian ini adalah sebagai berikut :

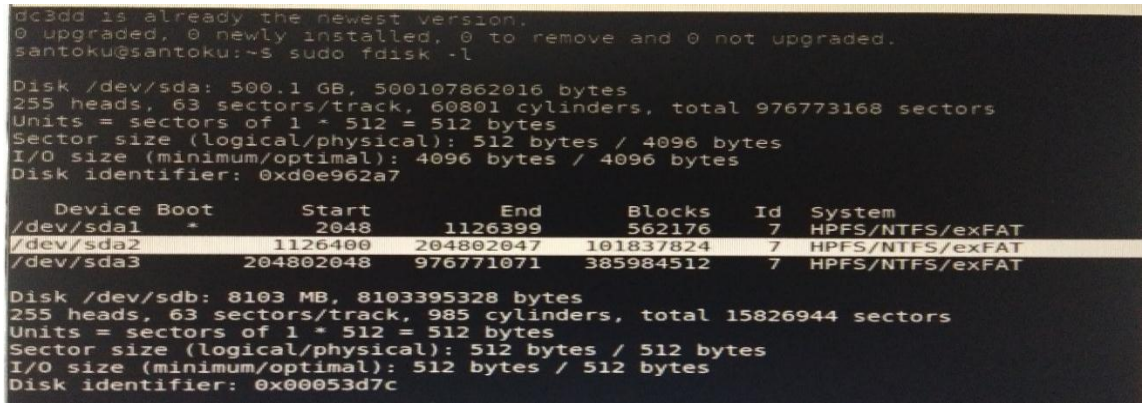
Dalam penelitian ini, disimulasikan sebuah kasus dimana seorang karyawan A mengambil data transaksi keuangan berupa pembayaran gaji dari komputer atasannya dengan maksud menaikkan gaji yang diterimanya. Karyawan A mengcopy ke dalam flashdisk sebuah file dengan nama file "2. Oktober 2018" yang mana file 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*. Skenario kasus yang diuraikan di atas, dijelaskan pada gambar 4-1 berikut:



Gambar 4.1 *Flowchart* skenario kasus

4.2 Cara Memperoleh Data

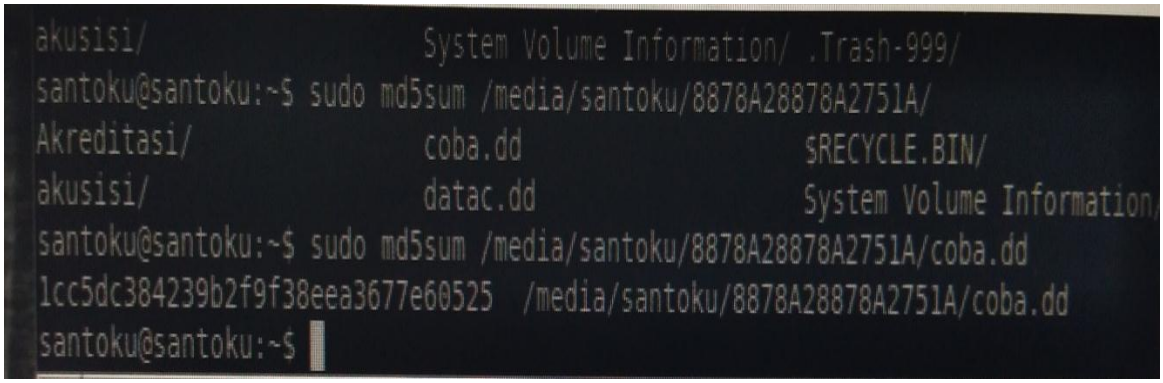
Setelah semua skenario dan sumulasi kasus selesai dibuat, dilakukan akuisisi sebanyak 2 kali dimana akuisisi yang pertama kondisi catatan jumplist belum dihapus dan yang kedua saat catatan jumplist telah dihapus. Akuisisi dilakukan dengan menggunakan *tools* Linux Santoku pada *drive* C dengan langkah awal mencari lokasi drive C pada partisi komputer dengan perintah *sudo fdisk –l* seperti pada gambar 4.2.



Gambar 4.2 Partisi Drive

Setelah partisi drive C diketahui, kemudian langkah berikutnya adalah membuat *hashing,* dan cek hasil MD5sum sebagimana pada gambar 4.3. Langkah selanjutnya dilakukan *imaging* untuk mendapatkan file *image.dd,* dan yang terakhir dari file **dd* tersebut dilakukan ekstraksi agar bisa dilakukan analisis.

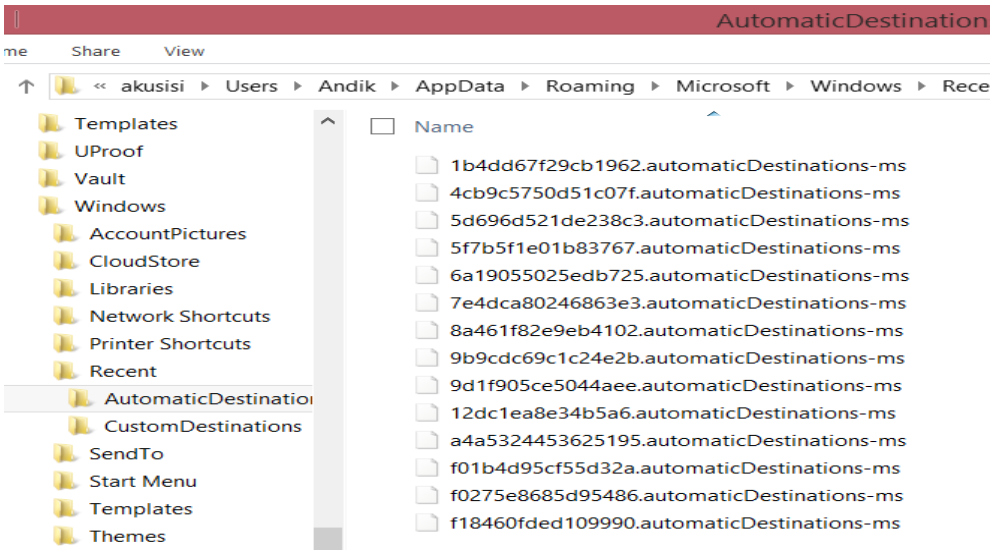
Pada akuisisi yang kedua, dilakukan proses *recovvery* dan akuisisi dengan menggunakan *tool* Belkasoft.



Gambar 4.3 Hasil MD5sum

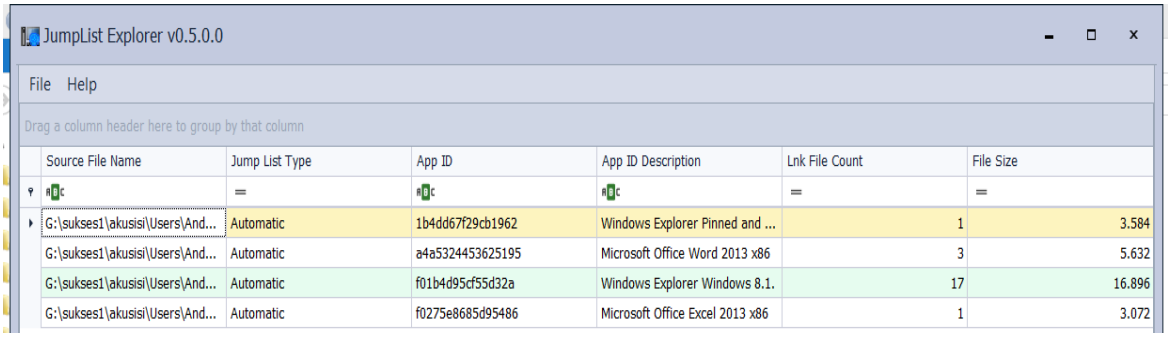
4.3 Analisis JumpList sebelum dilakukan penghapusan

Proses analisis dilakukan setelah mendapatkan ektraksi dari file **.dd.* Analisis dilakukan pada direktori *AutomaticDestinations*sebagaimana disajikan dalam gambar 4.4 berikut



Gambar 4.4 Direktori *AutomaticDestinations* hasil ekstraksi

Dari direktori *AutomaticDestinations* tersebut didapatkan sebanyak 14 file. Masing-masing file memiliki *AppIDs* yang merujuk kepada aplikasi atau aktifitas yang pernah diakses. File kemudian dianalis menggunakan aplikasi JumpListExt sebagimana gambar 4.4.



Source File Name	Jump List Type	App ID	App ID Description	Lnk File Count	File Size
G:\sukses1\akusisi\Users\And...	Automatic	1b4dd67f29cb1962	Windows Explorer Pinned and ...	1	3.584
G:\sukses1\akusisi\Users\And...	Automatic	a4a5324453625195	Microsoft Office Word 2013 x86	3	5.632
G:\sukses1\akusisi\Users\And...	Automatic	f01b4d95cf55d32a	Windows Explorer Windows 8.1.	17	16.896
G:\sukses1\akusisi\Users\And...	Automatic	f0275e8685d95486	Microsoft Office Excel 2013 x86	1	3.072

Gambar 4.5 Analisis menggunakan JumpListExt

Dari gambar 4.5 di atas kemudian dapat diuraikan *Entries Jumplist* berdasarkan *AppID Description, LNK File Count,* serta *File Size* dari masing-masing *AppID* seperti disajikan pada tabel 4.1 berikut.

Tabel 4.1 *Entries* Jumplist pada *AutomaticDestinations*

No	Jump List Type	AppID	AppID Description	Lnk File Count	File Size
1	Automatic	1b4dd67f29cb1962	Windows Explorerand Pinned	1	3.584
2	Automatic	4cb9c5750d51c07f	Movies and TV (Windows Store App)	1	3.584
3	Automatic	5d696d521de238c3	Chrome	0	1.536
4	Automatic	5f7b5f1e01b83767	Quick Acces	11	14.336
5	Automatic	6a19055025edb725	Unknown AppID	1	3.072
6	Automatic	7e4dca80246863e3	Control Panel	3	5.120
7	Automatic	8a461f82e9eb4102	Foxit Reader 7.2.0.722	2	4.096
8	Automatic	9b9cdc69c1c24e2b	Notepad (64 bit)	1	3.072
9	Automatic	9d1f905ce5044aee	Edge Browser	2	4.096
10	Automatic	12dc1ea8e34b5a6	Microsoft Paint	1	3.584
11	Automatic	a4a5324453625195	Microsoft Office Word 2013 x86	3	5.632
12	Automatic	f01b4d95cf55d32a	Windows Explorer	17	16.896
13	Automatic	f0275e8685d95486	Microsoft Office Excel 2013 x86	1	3.072
14	Automatic	f18460fded109990	Unknown AppID	2	3.072

Dari Tabel 4.1 di atas dapat diketahui Deskripsi dari masing-masing AppID, ukuran file AppID beserta jumlah aliran data. Berdasarkan AppID dan jumlah aliran datanya didapatkan hasil sebagaimana tabel 4.2.

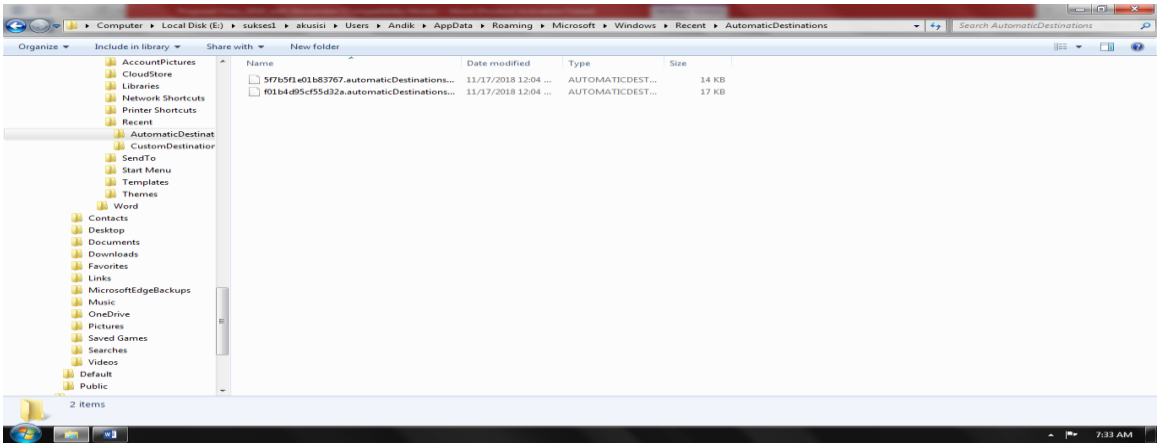
Tabel 4.2 Catatan Aktifitas pengguna komputer

No	Last Modified	Aplications	File Name	Location
1	2018-10-30 ; 15:12:11	Movies and TV (Windows Store App)	DBH-05-360p-SAMEHADAKU.TV.mp4	My Computer\C:\Users\Andik\Downloads
2	2018-10-30 ; 16:00:22	Microsoft Paint	Triump Daytona 675.jfif	My Computer\C:\Users\Andik\Downloads
3	2018-10-30 ; 16:04:57	Microsoft Office Word 2013 x86	1. Cover kepegawaian.docx	My Computer\D:\Akreditasi
4	2018-10-30 ; 16:05:27	Microsoft Office Word 2013 x86	1. Cover kepegawaian.docx	My Computer\G:\2
5	2018-10-30 ; 16:07:20	Edge Browser	SK Pemberhentian Bu Siti Aisyah.pdf	My Computer\D:\Akreditasi
6	2018-10-30 ; 16:09:22	Edge Browser	SK Dosen Tetap_Lita Erdiana.pdf	My Computer\D:\Akreditasi
7	2018-10-31 ; 13:14:56	Notepad 64 bit)	serial office 2013.txt	My Computer\G:\18 Okt
8	2018-10-31 ; 13:57:22	Microsoft Office Excel 2013 x86	2. Oktober 2018.xlsx	G:\\Keuangan\TA_2018_2019
9	2018-10-31 ; 14:01:42	Microsoft Office Word 2013 x86	Proposal Tesis_2018_Edit.docx	My Computer\D:\TESIS ANDIK

Dari tabel 4.2 dapat diketahui bahwa pada komputer tersebut pernah melakukan akses file dengan nama file *"2.Oktober 2018.xlsx"* pada tanggal 31 Oktober 2018 dari sebuah thumb drive dengan AppID f0275e8685d95486 yang merujuk ke Microsoft Office excel 2013 x86.

4.4 Analisis Jumplist setelah dilakukan penghapusan

Analisis dilakukan setelah penghapusan *AppID* pada direktori *AutomaticDestinations*. Namun demikian tidak semua *AppID* tersebut bisa dihapus, sehingga dari direktori *AutomaticDestinations* tersebut masih terdapat 2 (dua) *AppID* yang merujuk kepada aplikasi atau aktifitas yang pernah diakses sebagaimana gambar 4-6.



Gambar 4.6 Direktori *AutomaticDestinations* setelah dilakukan penghapusan

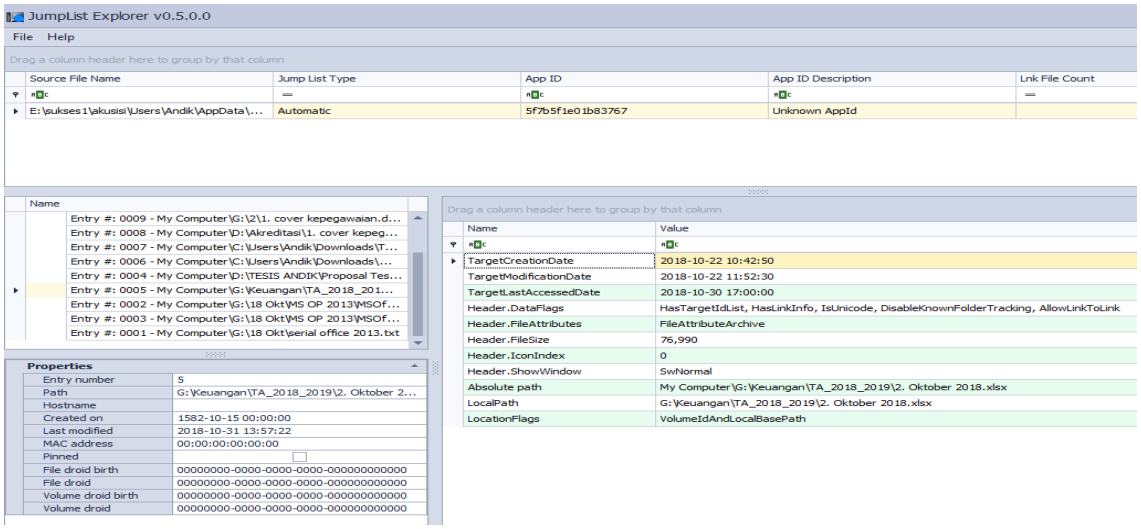
Dari gambar 4-6 di atas terdapat 2 (dua) *AppID* yang tidak bisa dihapus yaitu 5f7b5f1e01b83767 yang merujuk pada Quick Acces dan f01b4d95cf55d32a yang merujuk pada Windows Explorer, dimana dari kedua *AppID* tersebut juga masih menyimpan *history* penggunaan komputer tersebut.

Tabel 4.3 *Entries* Jumplist pada *AutomaticDestinations* yang tidak bisa dihapus

No	Jump List Type	AppID	AppID Description	Lnk File Count	File Size
1	Automatic	5f7b5f1e01b83767	Quick Acces	9	13.652
2	Automatic	f01b4d95cf55d32a	Windows Explorer	17	16.896

Berdasarkan tabel 4.3 di atas, 2 (dua) *AppID* tersebut kemudian dianalisis menggunakan *tools* JumplistExt dan Belkasoft untuk menguraikan aliran data yang masih tersimpan, dalam konteks penelitian ini terkait dengan aktifitas akses pada *file* dengan nama *file "2.Oktober 2018.xlsx"*oleh karyawan A.

Dengan menggunakan *tool* JumplistExt dapat ditelusuri bahwa pada AppID 5f7b5f1e01b83767 juga didapatkan jejak aktifitas penggunaan komputer tersebut dimana telah mengakses file dengan nama file *"2.Oktober 2018.xlsx"* yang diakses pada tanggal 31 Oktober 2018 pukul 13:57:22 seperti pada gambar 4-6.



Gambar 4.7 Jejak akses file 2. Oktober 2018 melalui *tool* JumplistExt

Pada analisa menggunakan *tool* Belkasoft Evidence Center juga ditemukan jejak aktifitas pada komputer tersebut saat mengakses file dengan nama file *"2.Oktober 2018.xlsx"*pada tanggal 31 Oktober 2018 pukul 13 :57:22 sebagaimana pada gambar 4.7.

Gambar 4.8 Jejak akses file 2. Oktober 2018 melalui *tool* Belkasoft Evidence Center

4.5 Analisa perbandingan data

Berdasarkan skenario dan simulasi kasus yang telah dilakukan dalam penelitian ini, berikut adalah perbandingan data dalam penelitian ini seperti pada tabel 4.5 :

Tabel 4.4 Perbandingan data Jump Lists

Tool/skenario	Sebelum dihapus		Setelah dihapus	
	Σ AppID	Ketersediaan data	Σ AppID	Ketersediaan data
JumplistExt	14	Ada	2	Ada
Belkasoft Evidence Center	14	Ada	2	Ada

Tabel 4.4 menunjukkan bahwa sebelum dihapus terdapat 14 (empat belas) *AppID* dengan dengan ketersediaan data sejumlah 46 (empat puluh enam) LNK *File* (tabel IV-1), berikutnya setelah dilakukan penghapusan masih terdapat 2 (dua) *AppID* dengan ketersediaan data sejumlah 26 (dua puluh enam) LNK *File* (tabel IV-3) atau masih terdapat aliran data LNK *File* sebanyak 56% dari kondisi sebelum dilakukan penghapusan.

Dari skenario dan simulasi kasus serta analisa yang telah dilakukan baik sebelum *AppID* pada drektori *AutomaticDestinations* dihapus atau sesudah dihapus didapatkan hasil bahwa pada saat dilakukan penghapusan *AppID* terdapat 2 (dua) *AppID* yang tidak bisa dihapus yaitu 5f7b5f1e01b83767 yang merujuk pada Quick Acces dan f01b4d95cf55d32a yang merujuk pada Windows Explorer.

AppID 5f7b5f1e01b83767 (Quick Acces) terdapat perbedaan jumlah data dimana sebelum dihapus memiliki aliran data sejumlah 11 (sebelas) LNK *File*, sedangkan pada kondisi setelah dilakukan penghapusan menjadi 7 (tujuh) LNK *File*, namun demikian dari 7 (tujuh) LNK *File* tersebut juga memiliki aliran data dari *AppID* yang lain dimana dalam penelitian ini *AppID* 5f7b5f1e01b83767 (Quick Acces) juga memiliki aliran data dari 5 (lima) *AppID* lain yaitu:

1. 8a461f82e9eb4102 (Foxit Reader 7.2.0.722)
2. 9d1f905ce5044aee (Edge Browser)
3. 12dc1ea8e34b5a6 (Microsoft Paint)
4. a4a5324453625195 (Microsoft Office Word 2013 x86)
5. f0275e8685d95486 (Microsoft Office Excel 2013 x86)

AppID f01b4d95cf55d32a (Windows Explorer) tidak memiliki perbedaan aliran data LNK *File* baik sebelum maupun setelah dilakukan penghapusan.

Tindakan atau upaya dalam menghilangkan bukti digital dalam tindak kejahatan, berkaitan dengan tingkat pengetahuan komputer dari pelaku kejahatan. Pengguna komputer dengan kemampuan dasar secara umumnya akan melakukan aktifitas menghapus pada *file* yang diinginkan dan selanjutnya mengkosongkan pada *Recycle Bin*. Di samping itu, terdapat pengguna komputer dengan tingkat pengetahuan *advance* dalam bidang komputer yang dinilai lebih ahli dengan memaksimalkan pengetahuan dasarnya dalam bidang komputer sebagaimana yang telah dilakukan oleh karyawan A sebagai pelaku tindak kejahatan. Karyawan A, dalam upaya menghilangkan jejak aktivitasnya, menghapus riwayat akses pada komputernya melalui cara yang berbeda, yaitu dengan menghapus melalui Windows Explorer pada direktori *AutomaticDestinations*. Sementara itu, pengguna komputer dengan kemampuan tingkat pengetahuan *expert,* memiliki pengetahuan dalam bidang komputer yang lebih tinggi seperti pengembang (*developer)* penemu (*founder)* ataupun *hacking (hacker).*

Karyawan A dalam tindak kejahatannya, walaupun telah melakukan penghapusan, pada *AppID* yang merujuk Quick Acces masih memiliki informasi yang menunjukkan catatan aktifitas komputer yang masih tersimpan sebagaimana terdapat pada aliran data dari *AppID* yang lain. Berkaitan dengan *AppID* yang tidak dapat dipulihkan, masih dapat diketahui bahwa *AppID* tersebut pernah tercatat dalam aktifitas penggunaan komputer sebelum dilakukan penghapusan dengan melihat *extensi* nama *file* yang berada di *AppID* 5f7b5f1e01b83767 (Quick Acces). Setiap *AppID* memiliki identitas yang berbeda-beda sesuai dengan aplikasi *file* tersebut, dalam hal penelitian ini *AppID* telah terhapus, sehingga memerlukan waktu lama untuk menemukan *file* yang dicari karena tercampur *file-file* lain dengan *ekstensi* yang berbeda-beda pada *AppID* 5f7b5f1e01b83767. Meskipun demikian, berkaitan dengan aktifitas akses *file* dengan nama *file "2.Oktober 2018.xlsx"* yang seharusnya berada di *AppID* f0275e8685d95486 yang merujuk ke Microsoft Office excel 2013 x86, masih dapat ditelusuri melalui *AppID* 5f7b5f1e01b83767 (Quick Acces).