BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Penelitian terdahulu mengenai Jump List dilakukan oleh(Singh & Singh, 2016) dimana 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.

Sementara itu, 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*.

Lebih jauh, (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.

Jauh sebelumnya, penelitian mengenai Jump List 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.

Pada penelitian lain 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.

Pertama kali penelitian mengenai Jump List dikemukakan oleh (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.

2.2 Komputer

Komputer berasal dari kata “Computare” yang berarti memperhitungkan atau menggabungkan bersama-sama. Dalam Bahasa Inggris “to Compute” yang berarti menghitung (Manis, 2017).

Menurut Kamus Besar Bahasa Indonesia (KBBI) komputer adalah alat elekronik otomatis yang dapat menghitung atau mengolah data secara cermat menurut instruksi, dan memberikan hasil pengolahan, serta dapat menjalankan sistem multimedia (film, musik, televisi, faksimile, dan sebagainya), biasanya terdiri atas unit masukan, unti pengeluaran, unti penyimpanan, serta unit pengontrolan (Indonesia, n.d.).

Dikarenakan bidang komputer yang sangat luas, dalam penelusurannya sangat banyak ahli yang mendefinisikan pengertian komputersecara berbeda-beda diantaranya adalah :

1. Menurut (Fouri, 1981) Komputer adalah suatu alat pemroses data yang mampu melakukan perhitungan dengan jumlah besar secara cepat, termasuk perhitungan aritmatika dan operasi logika, tanpa campur tangan dari manusia.
2. Menurut (Blissmer, 1985) Komputer adalah suatu alat elektronik yang mampu melakukan beberapa tugas antara lain menerima input, memproses input tadi sesuai dengan programnya, menyimpan perintah-perintah dan hasil dari pengolahan dan menyediakan output dalam bentuk informasi.
3. Menurut (V. Carl Hamacher Zvonko G. Vranesic, 2001) Komputer adalah mesin penghitung elektronik yang cepat dapat menerima informasi input digital, memprosesnya sesuai dengan suatu program yang tersimpan di memorinya dan menghasilkan output informasi.

Berdasarkan definisi dari beberapa sumber referensi dapat disimpulkan bahwa komputer adalah sebuah mesin elektronik yang dapat menerima input digital, melakukan proses pengolahan dan penyimpanan serta menghasilkan output berupa informasi secara cepat.

2.3 Komputer Desktop

Desktop dari bahasanya berasal dari *desk* yang berarti meja dan *top* yang berarti atas, sehingga pengertian dari desktop adalah komputer yang penggunaanya di atas meja (Interogator, 2017). Komputer desktop juga sering disebut sebagai *Personal Computer* (PC) yang dalam penggunaannya berada dalam satu tempat dan bersifat semi permanen.

Gambar 2.1 Komputer Desktop

Komputer desktop memiliki bermacam-macam bagian yang diantaranya monitor, CPU, *keyboard* dan *mouse* yang terpisah dan dihubungkan melalui kabel maupun usb. Masing-masing bagian dari komputer desktop berukuran cukup besar yang dirancang untuk diletakkan dan digunakan di atas meja.

2.4 Windows 10

Windows 10 adalahsistemoperasidari Microsoft Corporation untuk server, PC desktop, laptop, tablet, ponsel, danperangkatterkaitlainnyayaitu Internet of Things(Staff, 2016).Windows 10 merupakan sistem operasi generasi baru dari Windows yang dirancang untuk memasuki era kumputasi yang lebih personal di dunia *mobile-first, cloud first* (Alam, 2015), dimana teknologi menghilang dan orang-orang yang menjadi pusatnya. Pada era ini mobilitas pengalaman adalah hal yang penting, bukan mobilitas perangkat.

Sistem Operasi dari Windows 10 memiliki 4 versi yaitu Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise, dan Windows 10 Education. Microsoft merancang setiap tipe dengan tujuan yang spesifik. Menurut (Wijaya, 2016)Windows 10 berdasarkan tujuan dan target penggunanya adalah :

1. Windows 10 Home, dirancang untuk kebutuhan harian di rumah. Pada sistem operasi ini sudah memiliki fitur unggulan dari microsoft walaupun tidak lengkap seperti versi Pro, Enterprise, dan Education.
2. Windows 10 Pro, memiliki kemampuan enskripsi yang membuat data-data aman pada saat terhubung ke *network public.*

3. Windows 10 Enterprise, versi ini tepat digunakan bagi level perusahaan atau kantor karena dilengkapi kemampuan manajemen dan keamanan yang memuaskan.
4. Windows 10 Education, sesuai nama versinya sistem operasi ini ditujukan bagi pendidikan seperti sekolah dan universitas.

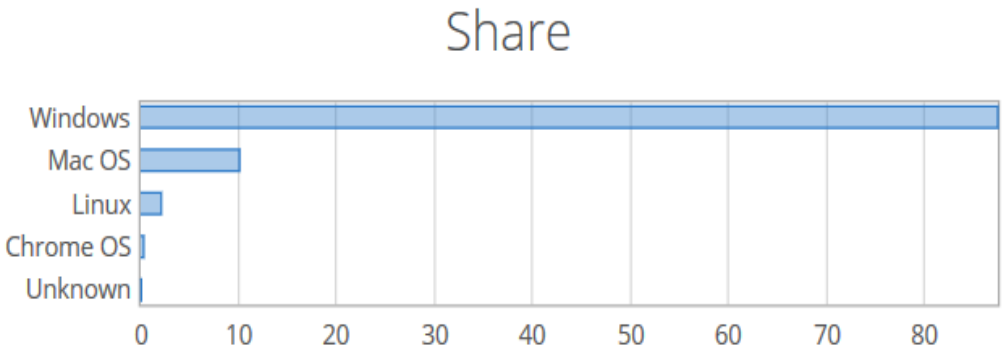
Kebutuhan *hardware* yang duperlukan dalam instalasi Windows 10 pada perangkat komputer desktop minimal memiliki Prosesor 1 Ghz, RAM 1 GB untuk Windows 10 versi 32 bit dan 2 GB versi 64 bit, Hard disk space 16 GB untuk Windows 10 versi 32 bit dan 20 GB versi 64 bit.Kartu grafis DirectX 9 atau lebih tinggi dan Dislpay 800x600(Microsoft, n.d.).

Tabel 2.1 Kebutuhan minimal *hardware* untuk Windows 10

Komponen	32 bit	64 bit
Processor	1 GHz or faster processor or SoC	
RAM	1 GB	2 GB
Hard Disk Space	16 GB	20 GB
Graphics Card	DirectX 9 or later with WDDM 1.0 driver	
Display	800x600	

2.5 Windows Forensik

Windows sebagai sistem operasi keluaran dari microsoft memiliki persentase pengguna yang sangat tinggi di dunia. Berdasarkan statistik yang dikeluarkan oleh Netmarketshare pengguna sistem operasi Windows pada bulan Februari 2018 sebesar 87.44%, jauh di atas sistem operasi yang lain seperti Mac OS (10.09%), Linux (2.10%), Chrome OS (0.31%), Unknown (0.06%), dan BSD (0.00%) sebagaimana ditunjukkan pada gambar 2.2.



Gambar 2.2 Statistik pengguna OS pada bulan Februari 2018

Berdasarkan data di atas, maka sistem operasi yang memiliki kemungkinan paling banyak ditemukan ketika mendapatkan barang bukti berupa komputer adalah Windows. Inti forensik yang dilakukan pada pada barang bukti berupa komputer berhubungan dengan penyelamatan dan analisis barang bukti berupa file-file di dalam harddisk komputer(Prayudi & Afrianto, 2007).

Dari sistem operasi Windows, diantaranya yang dapat dijadikan sebagai barang bukti berupa*shortcut file*. *Shortcut file* adalah file dengan ekstensi .lnk yang dibuat dan di akses oleh pengguna komputer dengan sistem operasi Windows. Lokasi dari *shortcut file* dibuat di sistem operasi pada folder *recent*.Isi dari *shortcut file* berupa informasi tentang *files* atau *network* yang diakses oleh pengguna.

2.6 Recovery File

File recovery adalah file-file yang dicari sesuai dengan maksud investigasi dan dicoba untuk diangkat kembali (Nuh Al-Azhar, 2012). Dengan adanya file yang berhasil ditemukan dan diangkat, maka analis forensik atau investigator dapat mengembangkan investigasinya dengan baik serta dapat membuktikan keterlibatan pelaku dalam kejahatan tersebut.

File recovery memiliki peranan yang penting dalam digital forensik dikarenakan menjadi dasar dari permintaan investigasi. Peranan tersebut adalah upaya pengembangan investigasi suatu kasus *computer crime* dan/atau *computer-related crime* serta upaya penyelamatan data terhadap isi dari suatu media penyimpanan yang hilang secara tidak sengaja atau sengaja (Nuh Al-Azhar, 2012).

Menurut (Nuh Al-Azhar, 2012) berdasarkan tipe *file* yang akan dicari dan dingkat, *file recovery* terdiri dari :

1. *Logical Files Recovery*

   Logical file adalah *file-file* yang maih ada dan tercatat di *file system* yang sedang yang berjalan (*running*) di suatu partisi dari media penyimpanan seperti *harddisk, flashdisk,* dan *memory card.* Dalam artian posisi *cluster* dan sektor untuk penyimpanan *file* masih tercatat dengan baik di pada *file system*.

   File-file logical bisa berupa aplikasi (memiliki ekstensi *.exe), *library* (*.dll), *office* (berupa *.doc/docx, presentasi *.ppt/pptx, *spreadsheet* *.xls/xlsx), logs (*.log/txt), multi media (audio *.mp3/amr, video *.mp4/avi/mpeg, gambar *.jpg/bmp/png) dan

lain-lain. Untuk memudahkan pencarian terhadap *file* yang diinginkan, maka *logical recovery files* dibagi menjadi 3 yaitu berdasarkan nama *file,* ekstensi dan isinya.

2. *Deleted Files Recovery*

   Deleted files adalah *file-file* yang sudah terhapus namun masih tercatat di *file system.* Dikarenakan sudah terhapus, *cluster-cluster* yang ditempati oleh *deleted files* tersebut ditandai sebagai *unallocated cluster* yang merujuk kepada *cluster* yang sudah tidak teralokasi lagi untuk *file-file* tersebut dan dapat digunakan lagi untuk penyimpanan *file-file* baru.Dalam artian *deleted files* masih tersimpan pada *cluster* atau sektor pada penyimpananya sampai terjadi *overwriten* oleh *file-file* baru.

   Pada kondisi *deleted files* tersebut belum tertimpa, maka sangat memungkinkan dilakukan proses *recovery* secara utuh terhadap *file* tersebut. Adapun jika telah terjadi *overwritten* pada sebagian *cluster* dan sektor dari *deleted files* maka sisa sektor dari *deleted files* tersebut dikenal dengan istilah *file slack* (area diantara *end of sector* hingga *end of cluster*).

   Proses *recovery* terhadap *deleted files* dengan melakukan analisa *root directory* dari *fle system* FAT12/16 dan FAT32, atau $MFT (*Master File Table)* dari *file system* NTFS.Pada *filesystem* NTFS ketika satu *file* dihapus, maka MFT *entry* untuk *file* tersebut masih berada pada $MFT. Namun demikian MFT *entry* dari*deleted file* tersebut dapat ditimpa oleh MFT *entry* dari *file* baru sehingga tidak tercatat lagi di $MFT. *Deleted files* yang sudah tidak tercatat lagi di $MFT (*lost file*) dapat dilakukan metode penelusuran keberadaan *files* di *file* metadata $LogFile.

   Dalam melakukan proses *recovery* banyak dikembangkan aplikasi-aplikasi dengan tujuan mendapatkan *deleted file recovery.* Beberapa aplikasi forensik yang berbasis Windows untuk *deleted file recovery* diantaranya adalah EnCase, FTK, WinHex, dan Recover My Files.

3. *Lost Files Recovery*

   Lost file merupakan file yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari partisi suatu media penyimpanan seperti *harddisk, flashdisk,* dan *memory card,* namun *file* tersebut masih berada di *cluster* dan sektor –sektor penyimpanannya. Misalnya proses *re-format* sehingga menghapus *file system* lama dan menghasilkan *file system* yang baru. Walaupun *lost file* masih berada di *cluster* dan sektor penyimpanannya, *file system* yang seddang berjalan tidak memiliki catatan apapun tentang *lost file* tersebut. Sehingga proses *recovery* yang

memungkinkan dilakukan adalah dengan didasarkan pada *signature* dari *header* maupun *footer* dari jenis format *lost file.*

File signature adalah beberapa *byte* pertama (dari *header*) atau terakhir (*footer*) dari suatu format/ekstensi *file.File signature* dikembangkan oleh Gary Kessler dan biasa dinyatakan dalam bilangan heksadesimal. Masing-masing ekstensi/format *file* memiliki *signature* yang berbeda-beda antara yang satu dengan yang lain.Berikut adalah tabel *file signature* yang sering digunakan dalam analisis forensik oleh investigator(Nuh Al-Azhar, 2012).

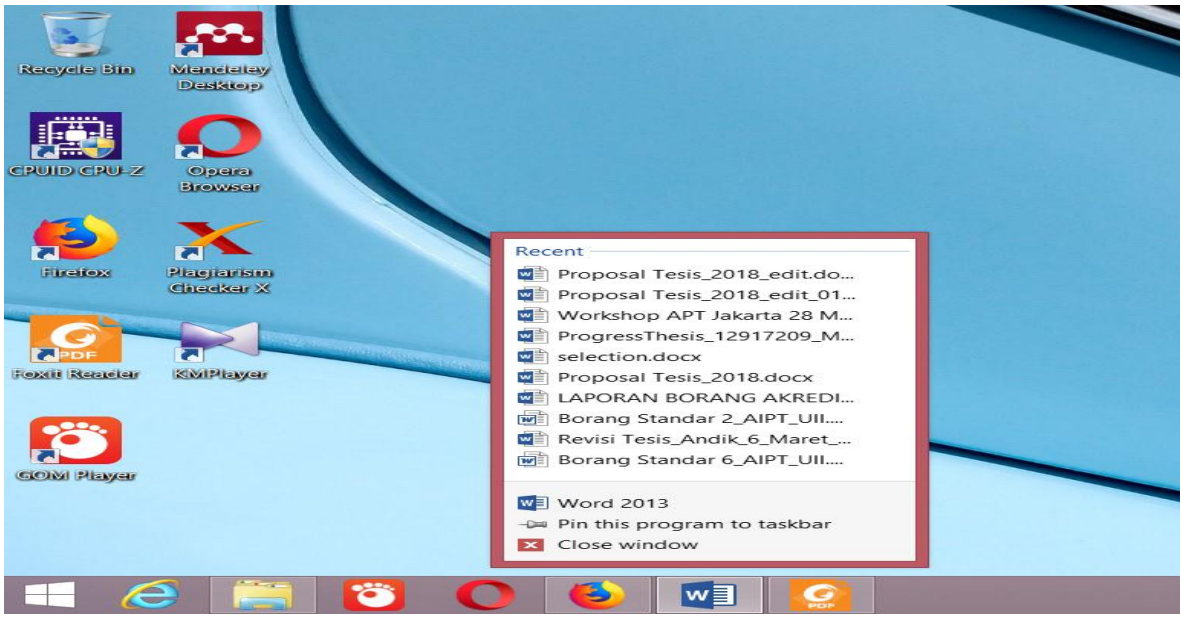
Tabel 2.2 Tabel *File Signature*

Tipe Ekstensi *File*	***Signature***
***File-file* Gambar Digital**	
*.bmp (*Bitmap Image*)	0x42 4d
*.jpg(*File*grafikJPEG/JFIF) *.jpg (JPG dari *digital camera* yang menggunakan EXIF (*Exchangeable Image File Format*) *.jpg (JPG dengan SPIFF (*Still Picture Interchange File Format*)	0xffd8ffe0xxxx4a46494600 0xffd8ffe1xxxx4578696600 0xff d8 ff e8 xx xx 53 50 49 46 46 00
*.png (*file Portable Network Graphics*)	0x89 50 4e 47 0d 0a
***File-file* Video**	
*.avi(*file*AudioVideo*Interleave*dariWindows)	0x41 56 49 20 4c 49
*.wmv/wma (*file* Windows Media Audio/Video)	0x30 26 b2 75 8e 66 cf 11
*.mp4 (*file* video MPEG-4)	0x00 00 00 14 66 74
*.flv (*file* video *flash*)	0x46 4c 56 01
*.mpeg/mpg (*file* video) *.mpg/vob (*file* video dvd atau mpeg2)	0x000001bx 0x000001ba
***File-file* Audio**	
*.wav (*file* audio Windows)	0x52494646xxxxxxxx57415645666d7420
*.mp3/mpeg/mpg (*file* audio mpeg) *.mp3 (*file* audio mpeg-1 audio layer 3)	0xff fx 0x49 44 33
*.amr (*file* audio Adaptive Multi-Rate, sering ditemukan sebagai format audio di *handphone*GSM)	0x23 21 41 4d 52

Tipe Ekstensi *File*	*Signature*
***File-file* Office**	
*.pdf (*file Portable Document Format*)	0x25 50 44 46
*.odt/odp (*file* OpenDocument untuk dokumen dan presentasi) *.kwd (*file* dokumen KWord) *.sxc, sxi, sxw (*file* OpenOfficeuntuk*spreadsheet*, presentasi dan dokumen)	0x50 4b 03 04
*.zip (*file* arsip PKZIP)	
*.zip (*file* arsip kompresi WinZip)	0x57 69 6e 5a 69 70
*.doc/ppt/xls (file Microsoft Office 2003 untuk dokumen, presentasi dan *spreadsheet*) *.db (*file* database MSWorks)	0xd0 cf 11 e0 a1 b1 1a e1
*.docx/pptx/xlsx (*file* Microsoft Office 2007untuk dokumen, presentasi dan *spreadsheet*)	0x50 4b 03 04 14 00 06 00
*.doc (*file* dokumen Perfect Office)	0xcf 11 e0 a1 b1 1a e1 00
*.doc (*file* dokumen DeskMate)	0x0d 44 4f 43
*.rtf (file dokumen Rich Text Format)	0x7b 5c 72 74 66 31
*.ws (*file* dokumen Wordstar 5.0/6.0)	0x1d 7d
*.ws2 (*file* dokumen Wordstar 2)	0x57 53 32 30 30 30
*.dbx (*file* untuk *folder email* Outlook Express)	0xcf ad 12 fe
*.pst (*file* untuk *personal* Microsoft Outlook)	0x21 42 44 4e

2.7 JumpLists

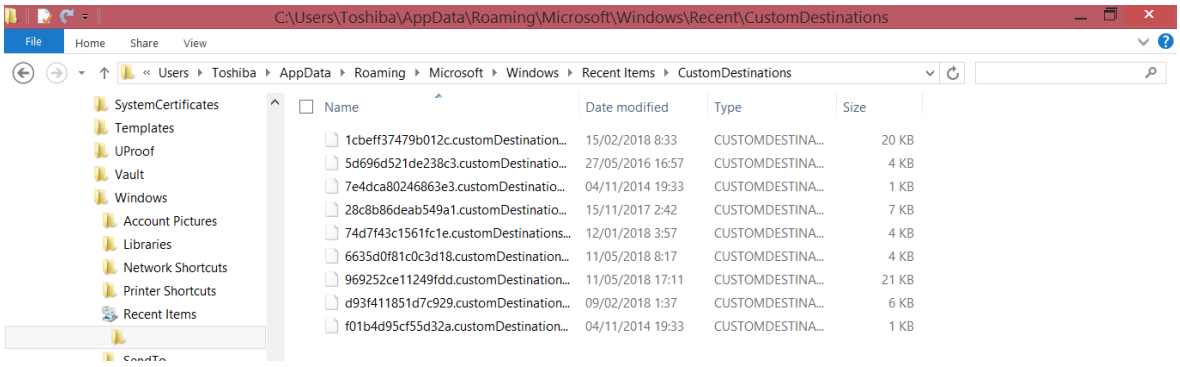
Jump Listsadalah fiturbarudarisistemoperasi Windows yang menunjukkan file dantugas-tugas yang paling baruatau yang paling sering digunakan oleh pengguna (Ghafarian, 2015). Mulai diperkenalkan pada Windows 7, yang berfungsi memberikan akses cepat ke tujuan yang sering digunakan seperti *file, folder,* maupun tautan. Jumplists dapat diakses dengan melakukan klik kanan pada tombol *taskbar* atau klik tanda panah pada program atau aplikasi di *start menu*.Jika pengguna sering mengakses *file, folder,* maupun tautan, yang baru-baru ini digunakan, maka Jumplists sangat membantu dalam mempercepat akses (Gates, 2018).



Gambar 2.3 Jumplist pada MS Word

Jump Lists memiliki 2 jenis, yaitu *custom Destinations* dan *Automatic Destinations*. Lokasi keberadaan Jump Lists tersembunyi, dan tidak dapat ditemukan melalui *Windows Explorer*, sehingga untuk dapat melihatnya harus diketikkan secara manual melalui *Address Bar*. Pada *custom destinations* dibuat saat pengguna melakukan '*pins'* atau memasangkan file ke *Start Menu* atau *Task bar*. Lokasi *custom destinations* terletak di :

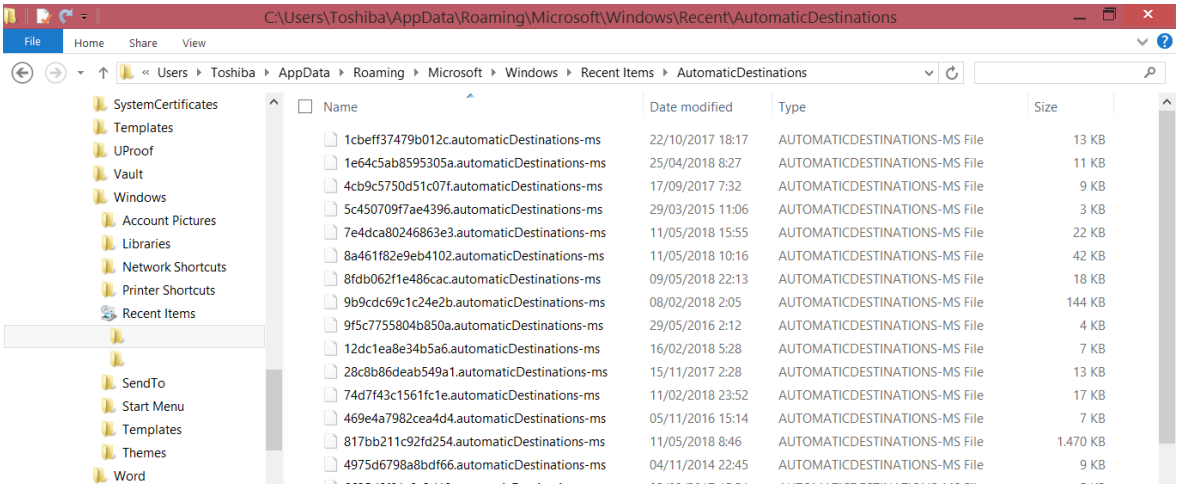
C:\Users\<UserProfile>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations



Gambar 2.4 Lokasi *custom Destinations*

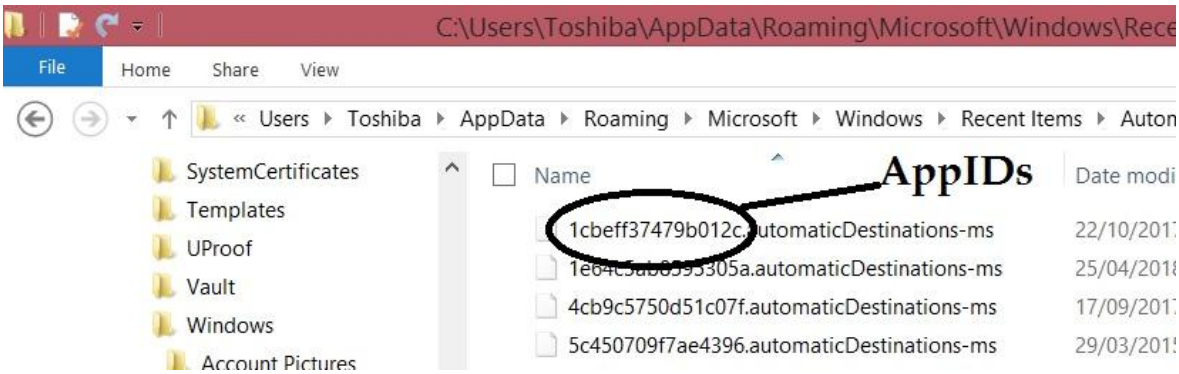
Sedangkan *automatic destinations* dibuat secara otomatis saat pengguna berinteraksi dengan sistem yang melakukan tindakan seperti membuka aplikasi atau mengakses file. Lokasi *automatic destinations* terletak di :

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



Gambar 2.5 Lokasi *Automatic Destinations*

Pada kedua jenis Jump Lists terdapat 16 digit alphanumerik yang menunjukkan identitas dari aplikasi *file* tersebut. Digit alphanumerik di Jump Lists dikenal juga dengan sebutan AppIDs.



Gambar 2.6 AppIDs Jump Lists

Masing-masing *file* yang terdapat dalam Jump Lists berbeda-beda, sesuai dengan aplikasi dari *file* tersebut.Daftar AppIDs dapat ditemukan pada beberapa situs website diantaranya situs websiteGithub. Berikut adalah tabel daftar AppIDs yang kemungkinan ditemukan dari Jump Lists dengan mengacu yang dibuat(Pullega, 2017).

Tabel 2.3 Daftar AppIDs dan dapat diakses di website Github

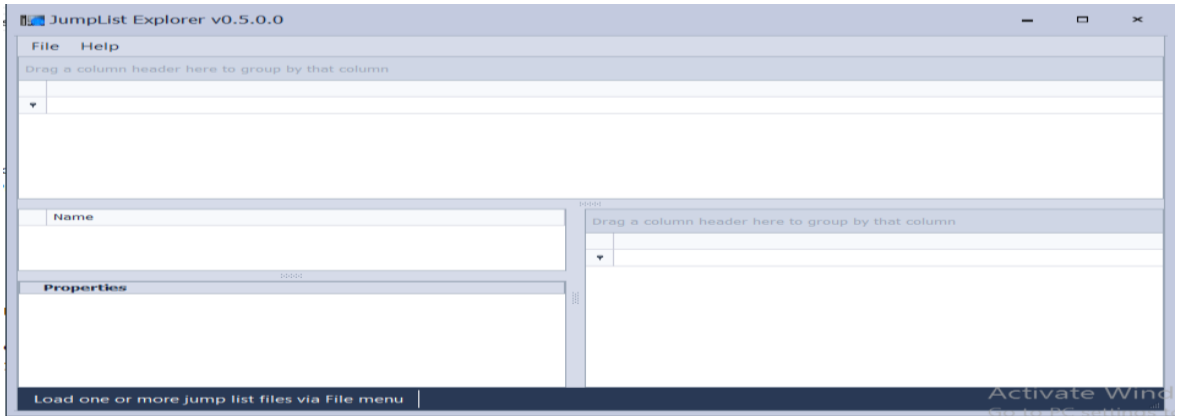
AppID	Deskripsi Aplikasi
Aplikasi	
7e4dca80246863e3	Control panel

AppID	Deskripsi Aplikasi
cdf30b95c55fd785	Microsoft Office Excel 2007
9839aec31243a928	Microsoft Office Excel 2010 x86
6e855c85de07bc6a	Microsoft Office Excel 2010 x64
f0275e8685d95486	Microsoft Office Excel 2013 x86
b8ab77100df80ab2	Microsoft Office Excel x64
5d6f13ed567aa2da	Microsoft Office Outlook 2010 x64
6d2bac8f1edf6668	Microsoft Office Outlook 365
f5ac5390b9115fdb	Microsoft Office PowerPoint 2007
9c7cc110ff56d1bd	Microsoft Office PowerPoint 2010 x86
5f6e7bc0fb699772	Microsoft Office PowerPoint 2010 x64
d00655d2aa12ff6d	Microsoft Office PowerPoint x64
a7bd71699cd38d1c	Microsoft Office Word 2010 x86
44a3621b32122d64	Microsoft Office Word 2010 x64
a4a5324453625195	Microsoft Office Word 2013 x86
fb3b0dbfee58fac8	Microsoft Office Word 365 x86
a18df73203b0340e	Microsoft Word 2016
Gambar /Melihat Dokumen	
de48a32edcbe79e4	Acrobat Reader 15.x
3594aab44bca414b	Windows Photo Viewer
b3f13480c2785ae	Paint 6.1 (build 7601: SP1)
Internet browser	
5c450709f7ae4396	Firefox 1.0/2.0/3.0
1461132e553e2e6c	Firefox 6.0
28c8b86deab549a1	Internet Explorer 8/9/10 (32bit)
5d696d521de238c3	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116
d1f905ce5044aee	Edge Browser
a0d6b1b874c6e9d2	TOR Browser 6.0.2
Berbagi File	
5fb817cd5a8cad21	Google Drive
7b7f65aaeca20a8c	Dropbox App 5.4.24

AppID	Deskripsi Aplikasi
caea34d2e74f5c8	uTorrent 3.4.7
Media Player	
817bb211c92fd254	GOM Player 2.0.12.3375 / 2.1.28.5039
4d8bdacf5265a04f	The KMPlayer 2.9.4.1434
74d7f43c1561fc1e	Windows Media Player 12.0.7601.17514
faef7def55a1d4b	VLC 2.2.6 (64bit)

2.8 JumpList Extractor

JumpListExt (Jump List Extractor) adalah alat *Graphical User Interface* (GUI) untuk mengurai Jump Lists pada Windows 10 baik secara individual maupun secara kolektif. JumpListExt berfokus pada penguraian dan menampilkan data yang diurai pada antarmuka pengguna. Data yang diurai dapat diekspor menjadi database SQLite. Fitur yang terdapat pada JumpListEx adalah mengurai Jumplists, membuat daftar data yang diuraikan pada antarmuka pengguna, dan mengekspor data yang diurai.



Gambar 2.7 JumpListExt

2.9 Belkasoft Evidence Center

Belkasoft adalah software forensik yang digunakan untuk mengumpulkan dan menganalisis bukti digital dari perangkat seluler dan komputer(Belkasoft, 2019). Didirikan pada tahun 2002 di California yang berfokus dibidang digital forensik, pemulihan data dan rekayasa balik. Pemanfaatan Belkasoft untuk memerangi pembunuhan, penipuan, kebocoran data, perdagangan narkoba, kejahatan terhadap anak-anak, serta kejahatan online dan offline lainnya.