Abstrak

ANALISIS FORENSIK *DELETED ENTRIES* JUMP LISTS WINDOWS 10 PADA PERANGKAT KOMPUTER DESKTOP

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. Keberdaan Jump list sendiri masih sedikit dikenal oleh pelaku kejahatan, namun demikian tidak menutup kemungkinan dihilangkannya catatan *entries* Jump Lists tersebut. Tindakan atau upaya dalam menghilangkan bukti digital, termasuk di dalamnya menghapus catatan *entries* Jump Lists mengakibatkan diperlukannya metode dalam menangani tindakan menghilangkan bukti digital. catatan yang berada dalam *entries* Jump Lists, walaupun telah dihapus seharusnya tetap dapat ditelusuri. Dalam penelitian ini dilakukan percobaan pada sebuah perangkat komputer dengan sistem operasi Windows 10 dengan skenario dan simulasi kasus pencurian data transaksi keuangan berupa pembayaran gaji. Pelaku tindak kejahatan dalam rangka menghilangkan jejaknya, menghapus riwayat akses pada komputernya dengan cara menghapus file jumplist melalui direktori Windows explorer pada direktori *AutomaticDestinations*. Akuisisi dilakukan pada kondisi file Jump Lists pada direktori *AutomaticDestinations* sebelum dan setelah dilakukan penghapusan. Dari kedua data akuisisi tersebut kemudian dilakukan analisa untuk mendapatkan informasi artifak digital yang terdapat pada *entries* Jump Lists baik sebelum dan sesudah terhapus. Dari analisa yang telah dilakukan didapatkan hasil bahwa tidak semua *AppID* bisa dihapus dimana masih tersimpan catatan informasi nama file, lokasi file, *create date, accessdate*, maupun *last modified.* Jumplist sebelum dilakukan penghapusan terdapat 14 *AppID* dengan jumlah data sebanyak 46 LNK File, sedangkan saat dilakukan penghapusan masih terdapat 2 *AppID* dengan jumlah data 26 LNK File atau 56% dari kondisi sebelum dilakukan penghapusan. *AppID* yang tidak bisa dihapus yaitu 5f7b5f1e01b83767 dan f01b4d95cf55d32a, dalam hal penelitian ini *AppID* 5f7b5f1e01b83767 yang merujuk pada Quick Acces juga menyimpan catatan informasi dari file *"2.Oktober 2018.xlsx"* dengan *AppID* f0275e8685d95486 yang merujuk pada Microsoft Office excel 2013 x86.

Kata kunci

Jump Lists, AppID, Windows 10 forensik, Bukti Digital

Abstract

ANALYSIS FORENSICS *DELETED ENTIRES* JUMP LISTS WINDOWS 10 ON DEVICE COMPUTER DESKTOP

Windows 10 has some new features in which one of them is Jump Lists. The Jump Lists has been launched firstly on Windows 7 until Windows 10.Jump Lists provides information of user activities on the computer as the interfacecontaining the list of files which has been accessed, files which are being searched, and the webpage which has been recently visited. The existence of Jump Lists is still rarely known by most criminals; however it is quite possible for them to delete the the entire data of the entries of Jump Lists. The actions and efforts of eliminating the digital evidence including the actions of deleting the entire data of the entries of Jump Lists effects on the need of essential method to handle any action and effort of deleting the digital evidence. By having such kind of method, the digital data still can be traced although it has been deleted. This research conducted the experiment on the computer with its operational system of Windows 10 in which it had a scenario and simulation of criminal case on stealing the data of money transaction of wages payment. To vanish their tracks, the digital criminal deleted all of the historical accesses on the computer through removing the Jump Lists files from the directory of Windows explorer on the Automatic Destination directory. The acquisition was done on the Jump Lists file of a directory on the Automatic Destination before and after the deleting processes. From the two acquisition data, the analysis was carried out to obtain the digital information on the entries Jump Lists before and after they were deleted. From all of the analysis, it was found that not all of the AppID could be erased since the Jump List still kept some essential information of the file name, file location, create date, access date, and the last modified. Jump list before removal there were 14 AppIDs with a total of 46 LNK Files, while at the time of deletion there were still 2 AppIDs with a total of 26 LNK Files or 56% of the conditions before deletion. AppIDs that cannot be deleted are 5f7b5f1e01b83767 and f01b4d95cf55d32a, in this case AppID 5f7b5f1e01b83767 which refers to Quick Access also stores information records from the file "2.October 2018.xlsx" with AppID f0275e8685d95486 which refers to Microsoft Office excel 2013 x86.

Key Words:
Jump Lists, AppID, Windows 10 forensics, Digital Evidence