



Prefetch Data Extractor v1.0.4

© 2013 -2015 Andrew Smith, Orion Investigations Co Ltd



Introduction

The prefetch file is a system generated file with the file extension “.pf” and is found in the following location: "C:\Windows\Prefetch". The Windows operating system uses the contents of the prefetch folder as a way to speed up the loading of applications. It does this by storing data required by the program during the first ten seconds of use in the prefetch file.

The prefetch file contains useful information for the forensic investigator including the number of times that an application has run (from the creation date of the prefetch file) and the last run date of the application. For most operation systems only one last run date is available. For Windows 8 there are 8 last run dates. PDE will display details of files that have been accessed by the application. This information can prove useful when conducting malware investigations or identifying files that have been directly accessed by a user.

The screenshot shows the Prefetch Data Extractor v1.0.3 application window. It features a menu bar with 'File', 'Export to csv', 'Options', and 'Help'. Below the menu is a toolbar with icons for file operations and a search icon. The main area contains a table with the following columns: Select, File Name, File Size (Bytes), File Created Time, File Modified Time, Last Run Time, Run Count, Process Name, and Process Path. The table lists several applications, including ATBROKER.EXE, AUDIODG.EXE, BTHSAMPALSER..., BTHSSECURITYM..., BTPLAYERCTRL.E..., and CHROME.EXE. Below the main table is a section titled 'Files Accessed' which contains a sub-table with columns for Select, File Name, and Files Accessed. This sub-table lists files accessed by ATBROKER.EXE, such as NTDLL.DLL, KERNEL32.DLL, APISETSCHEMA.DLL, KERNELBASE.DLL, and LOCALE.NLS.

Select	File Name	File Size (Bytes)	File Created Time	File Modified Time	Last Run Time	Run Count	Process Name	Process Path
<input type="checkbox"/>	ATBROKER.EXE-2...	8604	2015-07-19_1...	2015-07-19_1...	2015-07-19_16-54	1	ATBROKER.EXE	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\A...
<input type="checkbox"/>	AUDIODG.EXE-BD...	37348	2014-10-31_1...	2015-07-19_2...	2015-07-19_20-28	3568	AUDIODG.EXE	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\A...
<input type="checkbox"/>	BTHSAMPALSER...	59762	2015-07-18_0...	2015-07-19_1...	2015-07-19_16-53	5	BTHSAMPALSER...	DEVICE\HARDDISKVOLUME2\PROGRAM FILES\INTEL\...
<input type="checkbox"/>	BTHSSECURITYM...	37200	2015-07-18_0...	2015-07-19_1...	2015-07-19_16-53	5	BTHSSECURITYM...	DEVICE\HARDDISKVOLUME2\PROGRAM FILES\INTEL\...
<input type="checkbox"/>	BTPLAYERCTRL.E...	24842	2015-07-18_0...	2015-07-18_0...	2015-07-18_09-58	1	BTPLAYERCTRL.E...	DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\IN...
<input type="checkbox"/>	CHROME.EXE-D99...	139724	2014-10-31_1...	2015-07-19_1...	2015-07-19_19-06	1974	CHROME.EXE	DEVICE\HARDDISKVOLUME2\PROGRAM FILES (X86)\G...

Select	File Name	Files Accessed
<input type="checkbox"/>	ATBROKER.EXE-2E15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
<input type="checkbox"/>	ATBROKER.EXE-2E15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
<input type="checkbox"/>	ATBROKER.EXE-2E15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
<input type="checkbox"/>	ATBROKER.EXE-2E15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
<input type="checkbox"/>	ATBROKER.EXE-2E15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
<input type="checkbox"/>	ATBROKER.EXE-2F15A492.pf	DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\ATBROKER.FXF

Key Points

- 1) From the “Options” menu the user can select either local time or UTC. By default PDE will display local time.
- 2) The search function will only search the contents of the “Files Accessed” window. It does not search the main window.
- 3) The “Reload” button will reload the contents of the “Files Accessed” window.



Prefetch Data Extractor v1.0.4

© 2013 -2015 Andrew Smith, Orion Investigations Co Ltd



-
- 4) The user has the following options for exporting data to CSV:
- a. Export all results from the main window
 - b. Export selected results from the main window
 - c. Export selected search results from the “Files Accessed” window
 - d. From the “Help” menu the user can check for updates.

Version Changes

V1.0.4 - 20-07-2015

Added an App config file to ensure PDE will run correctly on OS with Net Framework 3.5,4 and 4.5 installed.