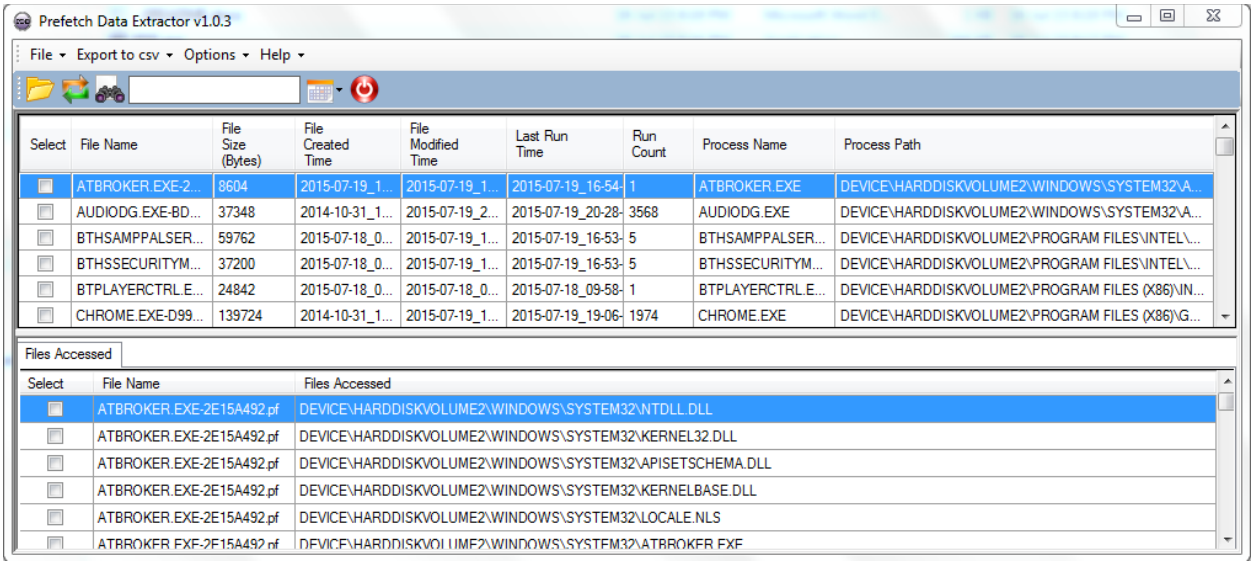
Prefetch Data Extractor v1.0.4

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.



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.

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.