PCFerret
Technology Solutions

PCFerret Pro and PCFerret Pro Portable

Award-Winning Windows® Tools for finding hidden data on computers

© Copyright PCFerret Technology Solutions 2002-2018, all rights reserved.

Table of Contents

A Brief Introduction To PCFerret 2

Utility Tabs

Quick System Details Tab 3
Full System Details Tab 4
Reboot Operations Tab 6
ADS Tab 9
Find Files By Type Tab 13
Browser Media Tab 18
Cached URLs Tab 22
Options 27

Tools

Generate Password 30
Hash Generator 32
Windows Error and Warning Event Viewer 35
Analyze File 38
Detect Tor Browser 39
Clean Uninstall 41

Integrated Features

View File Option 42
View ADS File Option 43
File Analysis Report 45

Updates and Support

Updates 46
Support 47

Technical Reference

What is an Alternate Data Stream (ADS)? 48
What is a Reboot Operation? 50

A Brief Introduction to PCFerret

PCFerret has been designed to find things on a PC which may be difficult to find, undesirable or intentionally hidden. PCFerret is an ideal tool for parents, schools and businesses alike. It's easy to use and the award-winning user interface makes it suitable for both the computer novice and the IT professional.

PCFerret's functionality is described in detail within the remainder of this document and on our website Features page.

Quick System Details Tab

The *Quick System Details* Tab is PCFerret's launch page. This replaces the previous Welcome launch page.

Quick System Details

User Name:	David
Computer Name:	DEVELOPMENT
Local IP Address(es):	192.168.56.1, 192.168.0.8
Operating System:	Windows 8.1 Professional (x64) Build: 9600 Service Pack: No Service Packs installed
Total Physical Memory:	7.99 Gigabytes
Available Physical Memory:	3.49 Gigabytes
Computer Manufacturer:	ZT Systems.
Motherboard:	Manufacturer: Intel Corporation Model: Base Board Product: DP55WB Version: AAE64798-206 Serial Number: AZWB00300

Figure 1. An example of the Quick System Details screen.

This tab has been designed to provide the user with basic details relating to the PC on which it is run. This is useful if you just wish to discover which operating system the PC is running or how much RAM is installed, without running the Full System Details report. As soon as you run PCFerret, this basic system information will be displayed.

Full System Details Tab

The *System Details* tab has been designed with the computer professional in mind. This feature gives the user the ability to collate technical information relating to the PC, such as operating system and hardware details, and have it presented to them in a single page report format, without the need to launch other utilities. It also allows technical support departments to request details from users without having to talk the user through what may be seen as complex procedures.

The report can be printed for the user's records or for transmission via fax. The report can also be saved in HTML, RTF and plain text format and sent as an attachment via email.

To refresh the report, click or tap on the Refresh icon or right-click and select *Refresh*.

The report details:

- User Name
- Computer Name
- Computer Workgroup
- Local IP Address
- Public IP Address
- Operating System Details
- Motherboard
- CPU
- Memory (RAM) size and configuration
- .NET Version(s)
- Video Card
- Storage Devices
- Storage Media Hardware Serial numbers
- Installed Browsers
- Default Browser
- Page File details
- Every user's Screen Saver details
- Monitor resolution and refresh rates
- Network Adapter(s)
- USB Controllers
- User Accounts
- And much more ...

For a quick glance at the PC's basic configuration, you can use the Quick System Details tab.

If the Last Accessed date of the *Page File* is followed by the * character, this means that the File Last Accessed feature is currently switched-off in the operating system and the Last Access time / date is not being recorded. This feature is often switched-off in order to increase hard disk access speed. As this feature can be switched on and off, its value should not be relied upon.

Reboot Operation Tab

For an explanation of *Reboot Operations*, click here.

When the Reboot Operations tab is clicked, the following windows Dialog Box will appear containing details of all the reboot operations, if any.

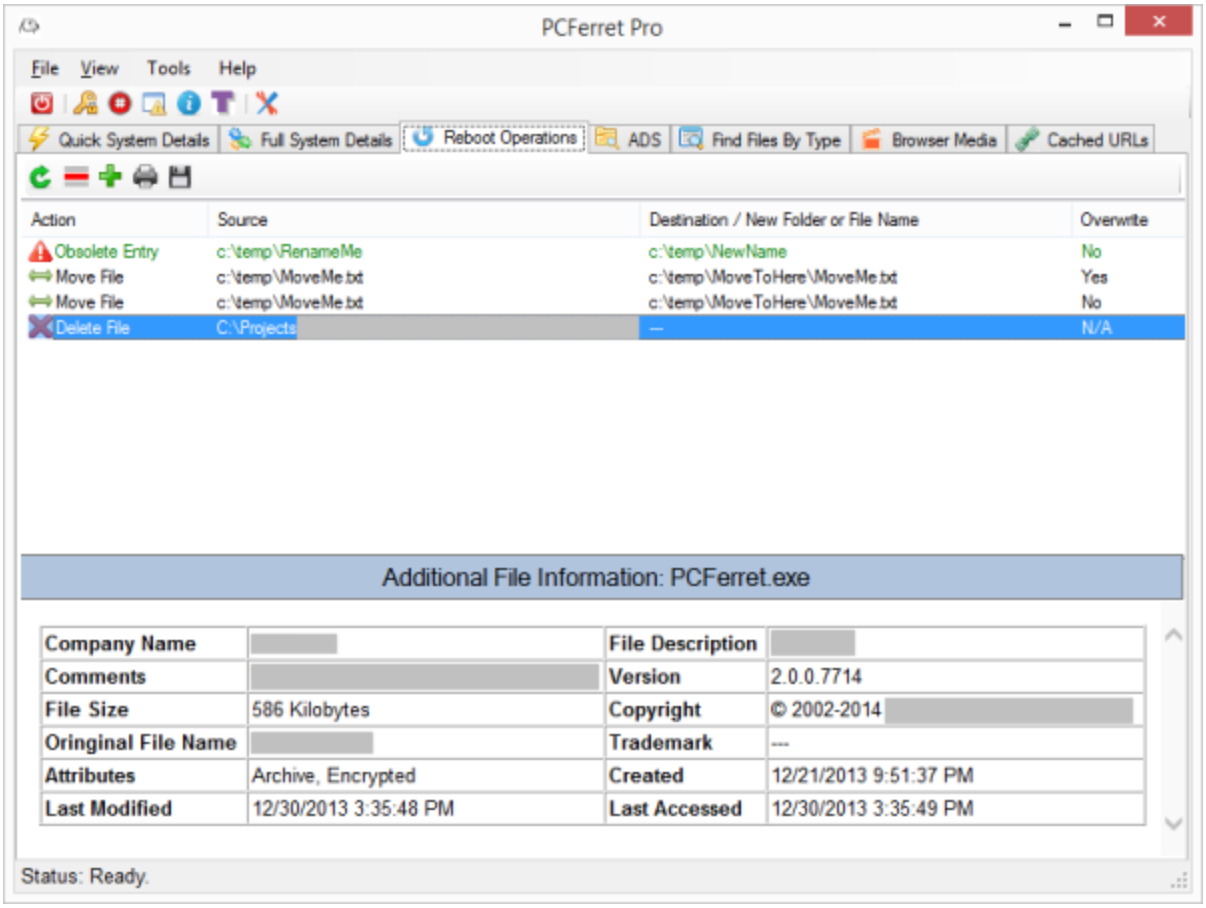


Figure 1. The Reboot Operations display. Reduced to 75% of actual size.

Columns Explained

Action: This can be one of the following values:

- Delete File
- Delete Folder
- Move File
- Move Folder
- Rename File
- Rename Folder
- Obsolete Entry

Obsolete Entry refers to an invalid action such as a file to be deleted which does not exist. please note that

while an entry may be obsolete at a given time, it does not mean that it will be obsolete at the time the computer is rebooted.

Source: The file / folder to perform the action on.

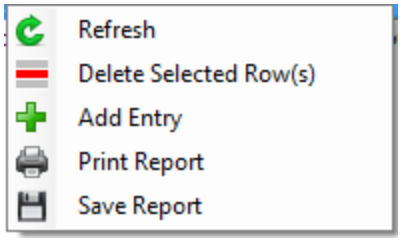
Destination / New Folder or File Name: The result of the action. I.e. in the case of a file rename operation, the name of the new file / folder. In this case of a delete operation, Destination does not apply.

Overwrite: Should the destination file be overwritten if it already exists; Yes / No. Overwrite does not apply to all operations and will show the value of "N/A" when this is the case.

Additional File Information Section

This shows additional information relating to the selected file. The information contained in the report may vary depending on the type of file selected.

Context (right-click) Menu Explained



The Reboot Operations Context Menu.

Refresh: Refresh the display.

Delete Selected Row(s): This option will delete the selected entries. A confirmation will be required in order to complete this action. This action cannot be undone.

Add Entry: This is used to add your own Reboot Operation. See figure 2 below.

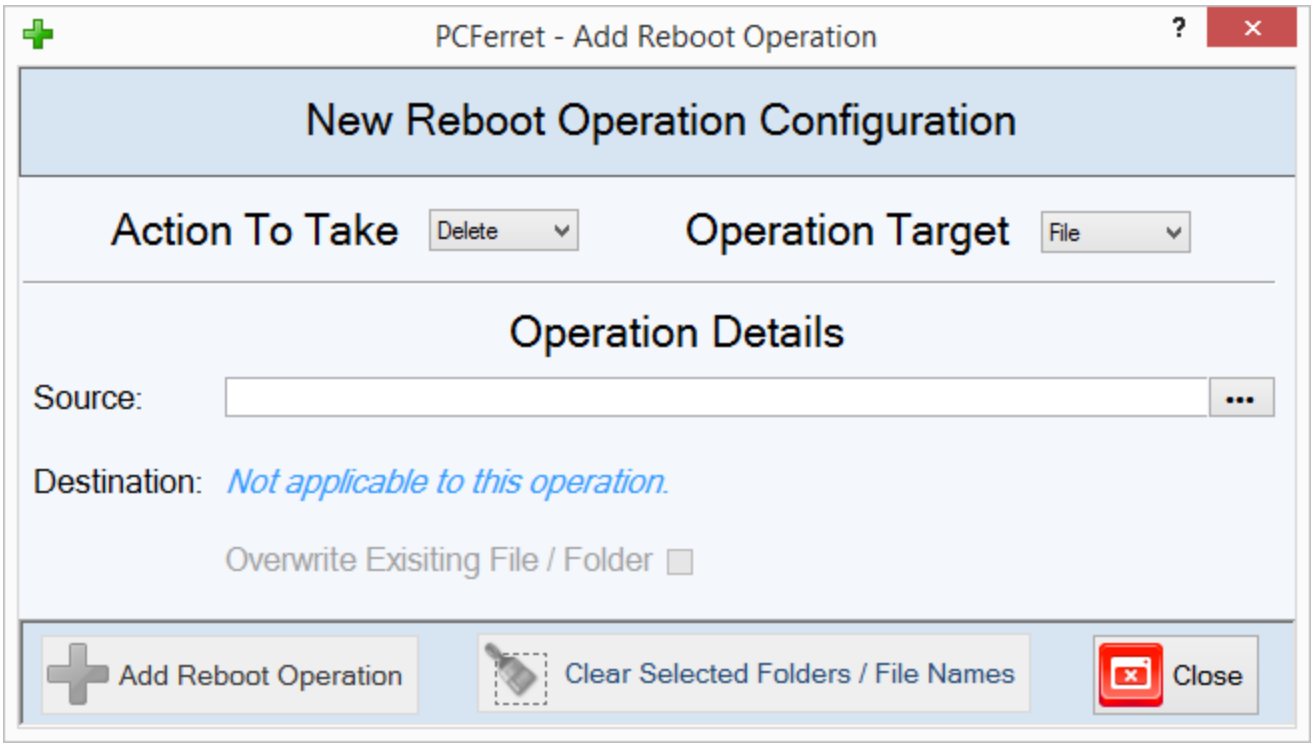


Figure 2. The Add Reboot Operation entry window.

To add an entry:

- Select the Action To Take. This can be one of three values: Delete, Move or Rename
- Select the Operation Target. This is either File or Folder
- Select the Source File or Folder
- Depending on how the previous operations are set, you may need to select a Destination
- Click or tap the Add Reboot Operation button

The operation will now appear in the list of reboot operations.

Print Report: This option will format and print a report of all the listed reboot operation(s).

Save Report: This option will format and allow you to save to disk or other media, a report of all the listed reboot operation(s).

ADS Tab

For an explanation of *Alternate Data Streams*, click here.

When the ADS tab is clicked, the following Dialog Box will appear:

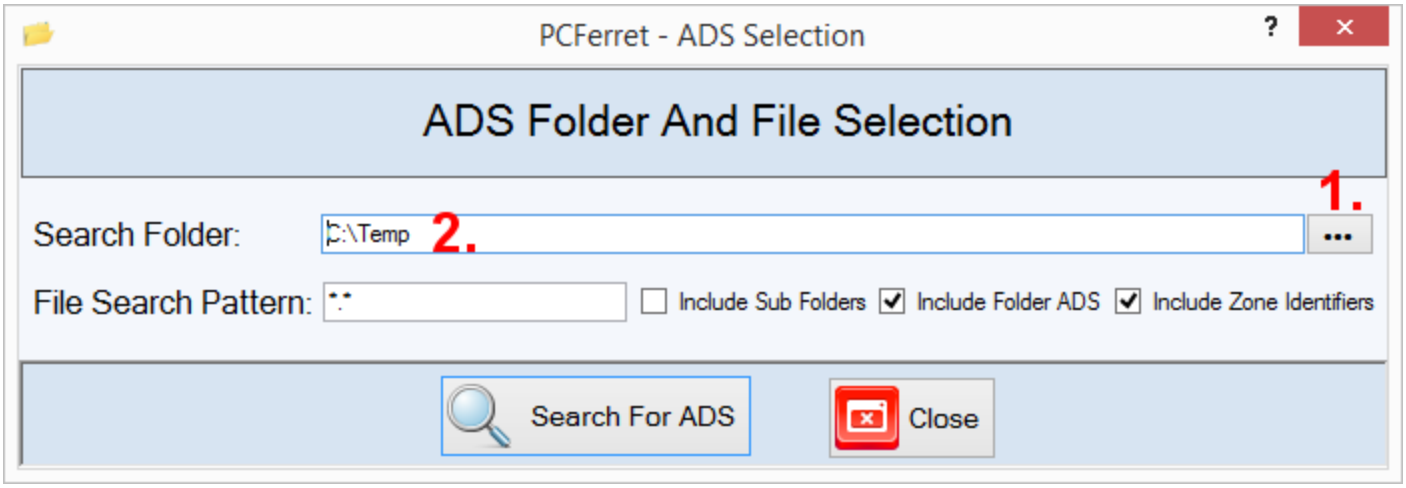


Figure 1. The ADS Folder and File Selection dialog box.

If the Cancel button is selected, or the search has completed, the search dialog can be redisplayed by pressing / tapping the Start Search button on the menu bar as illustrated below.

The ADS Folder and File Selection Menu Bar. The Start Search button is the one circled in red.

Using the ADS Folder and File Selection dialog box

Select the folder

In order to select the folder you wish to search, click on the icon numbered as 1 in figure 1 and select the folder from the resultant Browse For Folder dialog box. Clicking in the area where the folder is displayed (2), will have the same effect.

Determine the file search pattern

Enter the file search pattern you wish to use. The default is all files (*.*). This input field uses the standard Windows wildcard operators, ***** and **?**.

Select the required options

Include Sub Folders: This option instructs PCFerret to search folders recursively.

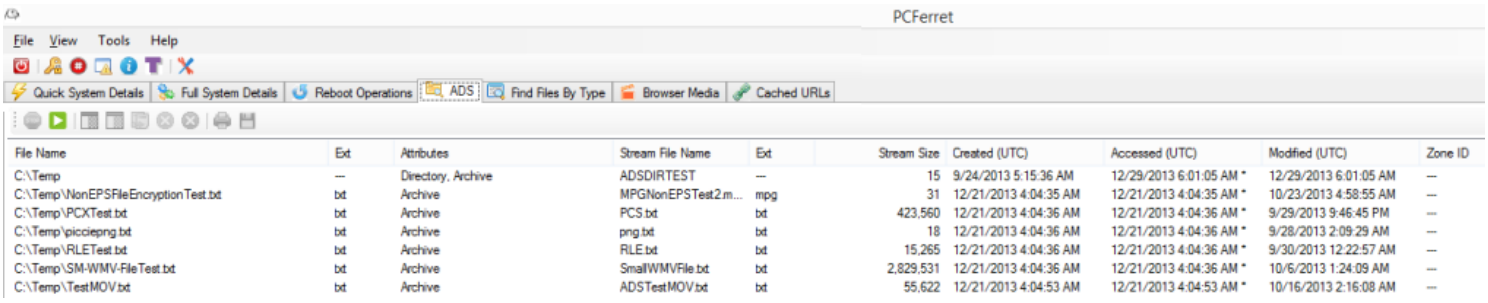
Include Folder ADS: Folders themselves can contain Alternate Data Streams, not just files. This option instructs PCFerret to include folders in the search.

Include Zone Identifiers: Include Alternate Data Streams in the search which contain Zone Identifiers. Read about Zone Identifiers here, in the section entitled: So what are they used for?

Click / tap the Search For ADS button.

Viewing the results

Figure 2 below, shows a reduced size image (75%) of the ADS search results window. Each column is explained below.



File Name	Ext	Attributes	Stream File Name	Ext	Stream Size	Created (UTC)	Accessed (UTC)	Modified (UTC)	Zone ID
C:\Temp	---	Directory, Archive	ADSDIRTEST	---	15	9/24/2013 5:15:36 AM	12/29/2013 6:01:05 AM *	12/29/2013 6:01:05 AM	---
C:\Temp\NonEPSFileEncryptionTest.txt	txt	Archive	MPGNonEPSTest2.m...	mpg	31	12/21/2013 4:04:35 AM	12/21/2013 4:04:35 AM *	10/23/2013 4:58:55 AM	---
C:\Temp\PCXTest.txt	txt	Archive	PCS.txt	txt	423,560	12/21/2013 4:04:36 AM	12/21/2013 4:04:36 AM *	9/29/2013 9:46:45 PM	---
C:\Temp\picciepng.txt	txt	Archive	png.txt	txt	18	12/21/2013 4:04:36 AM	12/21/2013 4:04:36 AM *	9/28/2013 2:09:29 AM	---
C:\Temp\RLETest.txt	txt	Archive	RLE.txt	txt	15,265	12/21/2013 4:04:36 AM	12/21/2013 4:04:36 AM *	9/30/2013 12:22:57 AM	---
C:\Temp\SM-WMV-FileTest.txt	txt	Archive	SmallWMVFile.txt	txt	2,829,531	12/21/2013 4:04:36 AM	12/21/2013 4:04:36 AM *	10/6/2013 1:24:09 AM	---
C:\Temp\TestMOV.txt	txt	Archive	ADSTestMOV.txt	txt	55,622	12/21/2013 4:04:53 AM	12/21/2013 4:04:53 AM *	10/16/2013 2:16:08 AM	---

Figure 2. ADS Search Results Windows.

Columns Explained

File Name: The path and file name of the file containing the Alternate Data Stream.

Ext (Extension): The file extension (if any) of the file containing the Alternate Data Stream.

Attributes: The attributes of the file containing the Alternate Data Stream. I.e. Directory / Archive / Read Only / System / Hidden.

Stream File Name: The file name of the Alternate Data Stream.

Ext (Extension): The file extension (if any) of the Alternate Data Stream.

Stream Size: The file size of the Alternate Data Stream.

Created (UTC): The creation date of the file (not the Alternate Data Stream).

Accessed (UTC): The last accessed date of the file (not the Alternate Data Stream). If the date is followed by the * character, this means that the File Last Accessed feature is currently switched-off in the operating

system and the Last Access time / date is not being recorded. This feature is often switched-off in order to increase hard disk access speed. As this feature can be switched on and off, its value should not be relied upon.

Modified (UTC): The last modified date of the file (not the Alternate Data Stream).

Zone ID: The Zone Identifier of the Alternate Data Stream. E.g. "Internet". Read about Zone Identifiers here in the section entitled: So what are they used for?

ADS Options

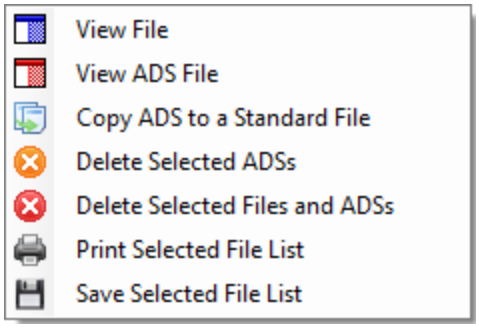


Figure 3. The context (right-click) menu available in the ADS Search Result Windows.

View File: Includes details of the File Analysis Report

View ADS: File Includes details of the File Analysis Report

Copy ADS To A Standard File

This option copies an ADS to a standard file so that in can be accessed and manipulated in the same ways as any other file.

Selecting this option will cause a Save File dialog to appear. Choose the folder and file name you wish to save the ADS under then click / tap the Save button. A confirmation will be displayed if the save was successful. This action does not delete the ADS from the file.

Delete Selected ADS(s)

This option will delete the selected ADS(s) from the file. A confirmation will be required in order to complete this action. This action cannot be undone.

Delete Selected File and ADS(s)

This option will delete the selected file(s) and their associated ADS(s). A confirmation will be required in order to complete this action. This action cannot be undone.

Print Selected File List

This option prepares and prints a report containing the details of all selected files. All of the details shown in figure 2 are included.

Save Selected File List

This option prepares and saves a report in HTML format containing the details of all selected files. All of the details shown in figure 2 are included.

Find Files By Type Tab

The *Find Files By Type* tab allows you to search for files based on their content, rather than their file suffix. This allows for the detection of files which may have been renamed in order to hide data by deliberately misleading the searcher or they could have been inadvertently renamed without their file suffix, or an incorrect suffix may have been specified.

If you wish to search for files by their suffix, you may do so by selecting the Search By Ext option as show in figure 1 below. As this form of search is self-explanatory, the rest of this topic will be dedicated to the Search By Type option.

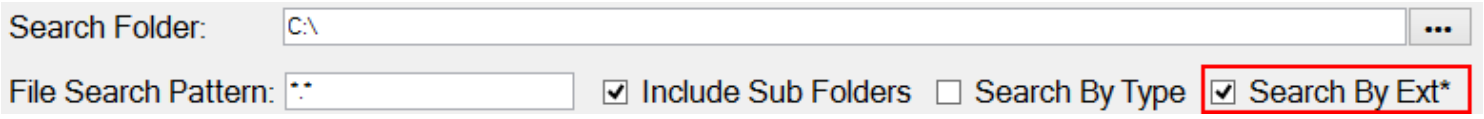


Figure 1. Find Files By Ext (Extension)

Searching By Type

To search for particular types of files, simply check the check boxes adjacent to the type of file you wish to search for. Prior to commencing the search, you may wish to change the default or previously saved options by clicking the Options button at the bottom of the selection window. Doing so will show the Options window as shown below.

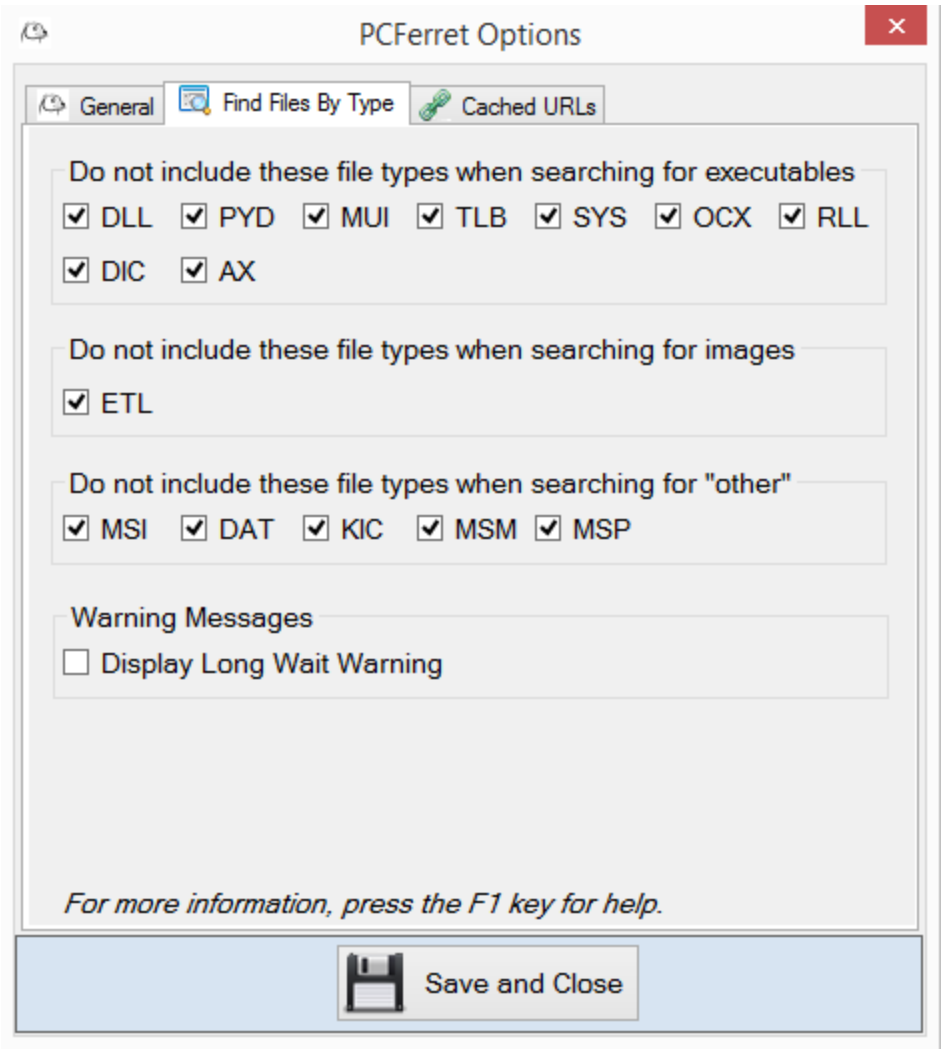


Figure 2. The Options window.

These options are provided to the user in order to Reduce False Positives (reduce the number of files which are reported to be of a certain type, when they are not). This can occur when files unrelated to the search criteria contain the same binary signatures (headers, etc) as the kind of file PCFerret is searching for. Some file types can be indistinguishable from others during analysis, for this reason. These settings are optional as some files may be given a different file extension in order to disguise their true content, or they may have been inadvertently, incorrectly named. The details of such files will be shown with a red highlight on any search results.

The Display Long Wait Warning option is provided so that you may switch off the warning message which is displayed when selecting the Find Files By Type tab. This message is designed to provide additional information to new users.

If you wish to select / deselect all of the files types in a category, simply click the ☑ All or ☐ All image respectively.

How PCFerret Performs A Search

PCFerret searches for the specified files by reading each file and examining its binary data. This can be a simple check of the first few bytes of the file or, depending on the file type PCFerret is searching for, the file may be examined via a complex algorithm. Due to the complexity of such analysis, results cannot be guaranteed to be 100% accurate, however, a substantial amount of research and testing time has gone into PCFerret in order to make it as accurate as possible.

Warnings / Red, Yellow and Orange Highlighting

Red

When a file is highlighted in red as shown below in figure 3, this indicates that the file's content does not match the file's expected file extension. For example, a file may have an extension of .txt where, in reality, analysis has shown that the file is actually a PNG image file. This mismatch could be due to a file naming error or it could be due to someone intentionally obscuring the file's real content. Another possibility is that a program which has created temporary files in a cache, such as the Google Chrome Browser, has named the files using unconventional naming standards. This does not mean that a file's content has been deliberately hidden so a file highlighted by a red line may be quite innocent. If in doubt, there are menu options which can be utilized to provide further details as discussed below.

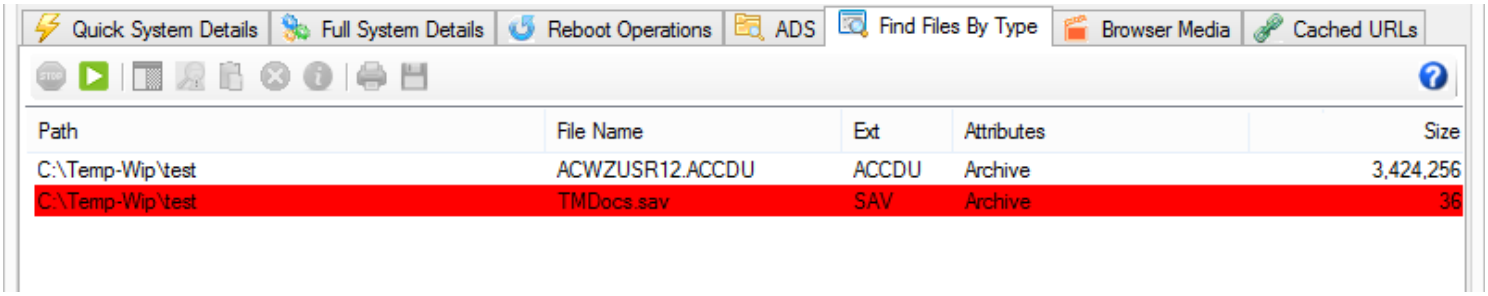


Figure 3. An example of a file content / suffix mismatch.

Yellow

When a file is highlighted in yellow, it indicates that the file may be executable but the analysis of the file's binary content is not conclusive, therefore the file is not marked in red.

Orange

A file highlighted in orange indicates that the file analysis suggests that the file type does not match the file's extension. However, the content of the file is still of the same type as the file's suffix suggests. For example, a file called mypic.jpg may contain an image in the .png format.

Find Files By Type - Sub And Context (right-click) Menus

There are 2 menus available to you when the search has completed. These are the Sub and Context menus as shown below. These menus are functionally identical and which you choose to use is a matter of

personal choice. For simplicity, we will discuss the context menu below.

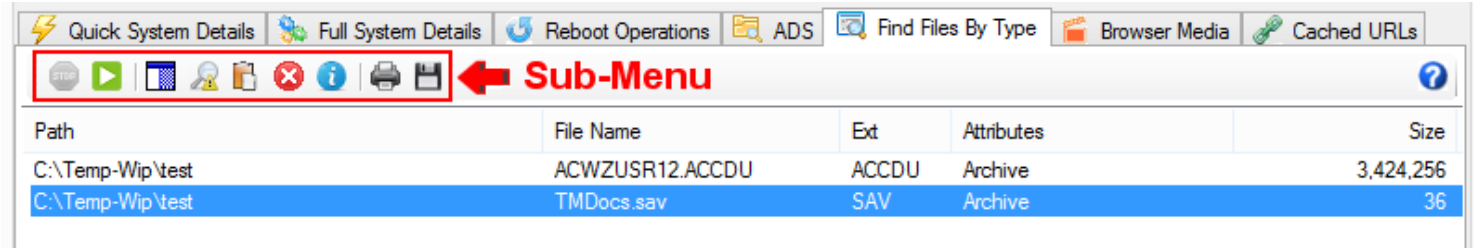


Figure 4. The Sub-Menu

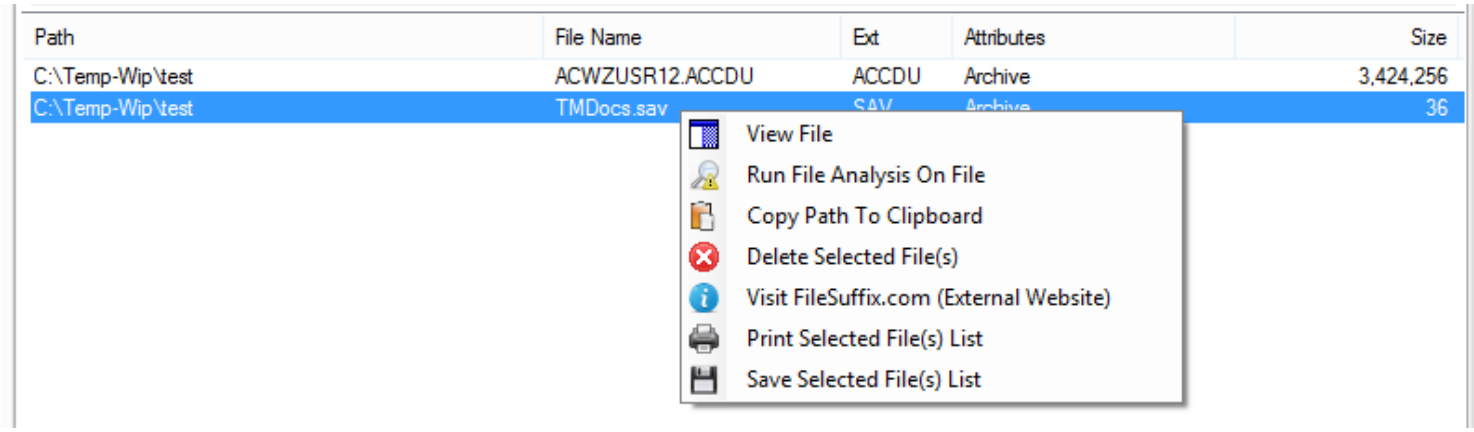


Figure 5. The Context (right-click) menu

The context menu appears when item(s) in the search results list is highlighted and a right-click is made by the user. If the menu items are grayed-out, then no items have been selected. Let's discuss each item on the context menu in turn.

View File

This option activates the View File option. For more information on this subject, click here.

Run File Analysis On File

This option displays the File Analysis Report. For more information on this subject, click here.

Copy Path to Clipboard

This option copies the selected file's fully qualified file name to the Windows clipboard. E.g. c:\windows\system32\afile.sys

Delete Selected File(s)

This option deletes selected file(s).

Visit FileSuffix.com

Selecting this option will cause your default web browser to be launched and you will be taken to the details page for the file suffix of the selected file on the website FileSuffix.com. FileSuffix.com has an extensive database of file suffix descriptions but like all databases of this kind, there may be some file suffixes yet to be added.

Please note that PCFerret does not maintain the website FileSuffix.com and has no commercial interest in the website or the company. PCFerret cannot guarantee the accuracy of any data presented on the FileSuffix.com website.

Print selected File(s) List

This option will print details of any selected files, in a report format.

Save Selected File(s) List

This option will save details of any selected files in a report format, to a file selected by the user.

Media Browser Tab

The *Browser Media* tab has been designed to extract images and movies from the top six most commonly used browsers' cache. The browser names can be seen in figure 1.

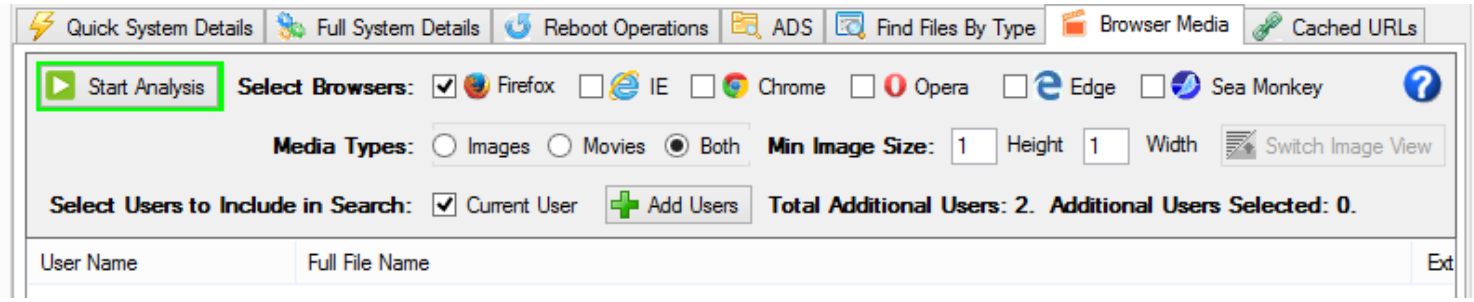


Figure 1. The Browser Media tab.

To view the images and videos (if any) in your browsers' caches, select the browsers you wish to examine and click the Start Analysis button. Only the browsers which are installed on your computer will be selectable.

To view the browser caches of other user accounts (if any) on the computer, select the users from the list produced when the Add Users button (shown above) is clicked. Please note that although a user account may be present on a computer, it does not mean that it will be displayed here. That is due to the fact that although an account is present, no login may have taken place. Additionally, a browser may not have been run on an account since it was created. In either case, no browser caches would be present, so to avoid any potential confusion, PCFerret does not display these accounts.

If the Media Types Images or Both is selected, the Min Image Size functionality will be made available to you. This allows you to specify the minimum size of the images you wish to see reported. Using this, you could for example, exclude icons and other small images. The minimum size is 1 X 1, which is the default. If for any reason the file's dimensions cannot be ascertained, an image size of 1 X 1 will be assumed for search purposes.

There are two views available in which to view the search results, the List View and the Thumb view. The views are selected by the use of the Switch Image View button seen in figure 1, towards the right of the screen shot

The List View

The List View is the default reporting view. As can be seen in figure 2, this shows the details of the files which meet the search criteria. Each entry is prefixed with the logo of the browser whose cache the file was found in.

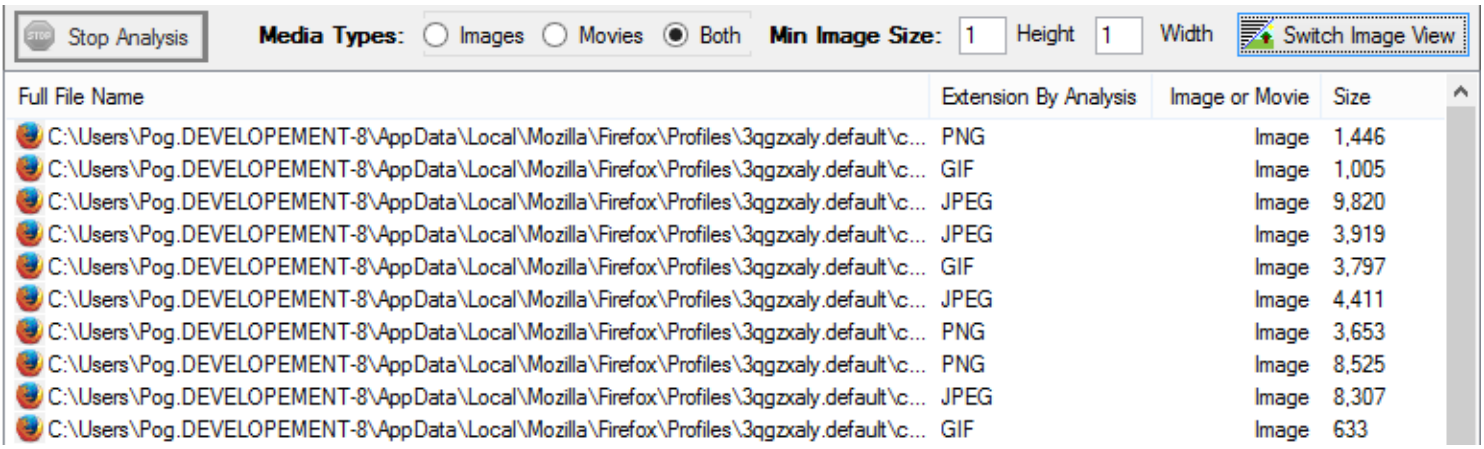


Figure 2. The List View.

Further details on each file can be obtained by using the horizontal scroll bar, or by expanding the window's size. To see other file options, right-click on your chosen file in order to display the List View context menu, as shown in figure 3.

If the Last Accessed date of the file is followed by the * character, this means that the File Last Accessed feature is currently switched-off in the operating system and the Last Access time / date is not being recorded. This feature is often switched-off in order to increase hard disk access speed. As this feature can be switched on and off, its value should not be relied upon.

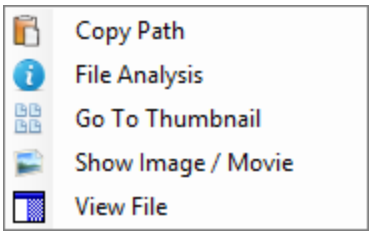


Figure 3. The List View(right-click) Context Menu.

The following is a description of each context menu item:

- Copy Path option copies the full path and file name of the selected file into the Windows Clipboard.
- File Analysis option invokes the File Analysis Report module, giving you additional details in respect to the chosen file.
- Go To Thumbnail option takes you to the selected entry in the Thumbnail View.
- Show Image / Movie option causes the image or movie to be shown in a larger window. In the case of a movie, there is a play movie option for some formats. See figure 5 for an example of this display.
- View File. This invokes the View File option.

The Thumbnail View

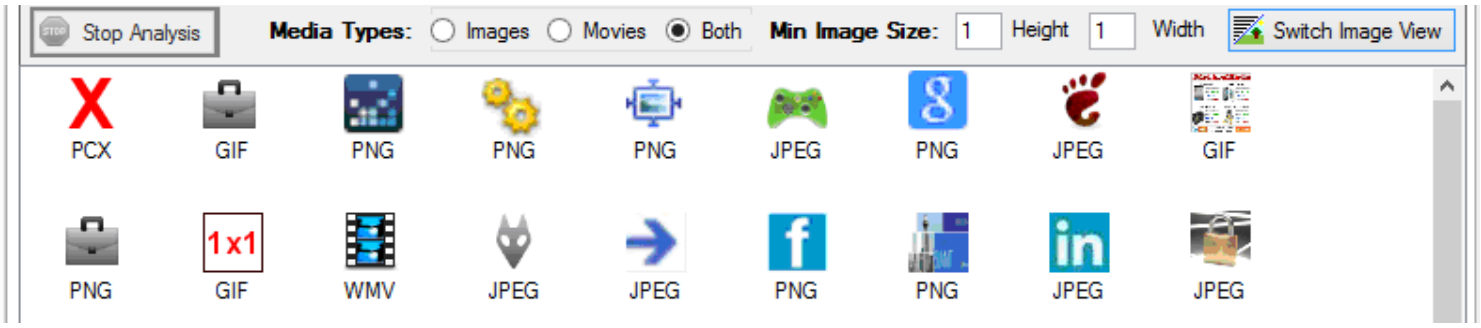


Figure 4. The Thumbnail View.

The Thumbnail View is a viewing alternative to the default List View. This view is particularly useful if you wish to browse through images in the search results.

A Right-click on a result line will bring up a context menu similar to the one shown in figure 3. There is, however, an additional item on this menu titled View List Entry. Selecting this menu item will switch the view mode back to List View, and highlight the entry relevant to the thumbnail image you selected in the Thumbnail View mode.

Not all images may be shown in the Thumbnail View, as an image format may be incompatible with Windows or PCFerret. If PCFerret recognizes such an image, an image featuring a red cross will be shown in its place. Bear in mind, the image may, of course, simply be a red cross. This is what the replacement image would look like:

Images which have the dimensions of 1 x 1 are often used on websites to space other images. As these images are often white, if they were to be displayed directly as a thumbnail, they would be invisible. PCFerret replaces 1 x 1 thumbnails with the graphic shown below. The original file contents are left unchanged.

When a movie is found, the following thumbnail is shown. Using the first or random frame of a video may be misleading as it may appear to the user to be an image.

The Show Image Window

This window shows a larger representation of the chosen result and provides some additional information. If the chosen item is an image, then that image will be shown at actual size, where possible. If the chosen item is a movie, a movie player will be displayed in order for you to watch the movie. Some movie formats are

natively supported by Windows, whereas others may require a suitable Codec to be installed. For more information on Codecs, click on this WikiPedia Link.

The options available on this window are explained in the context menu section here.

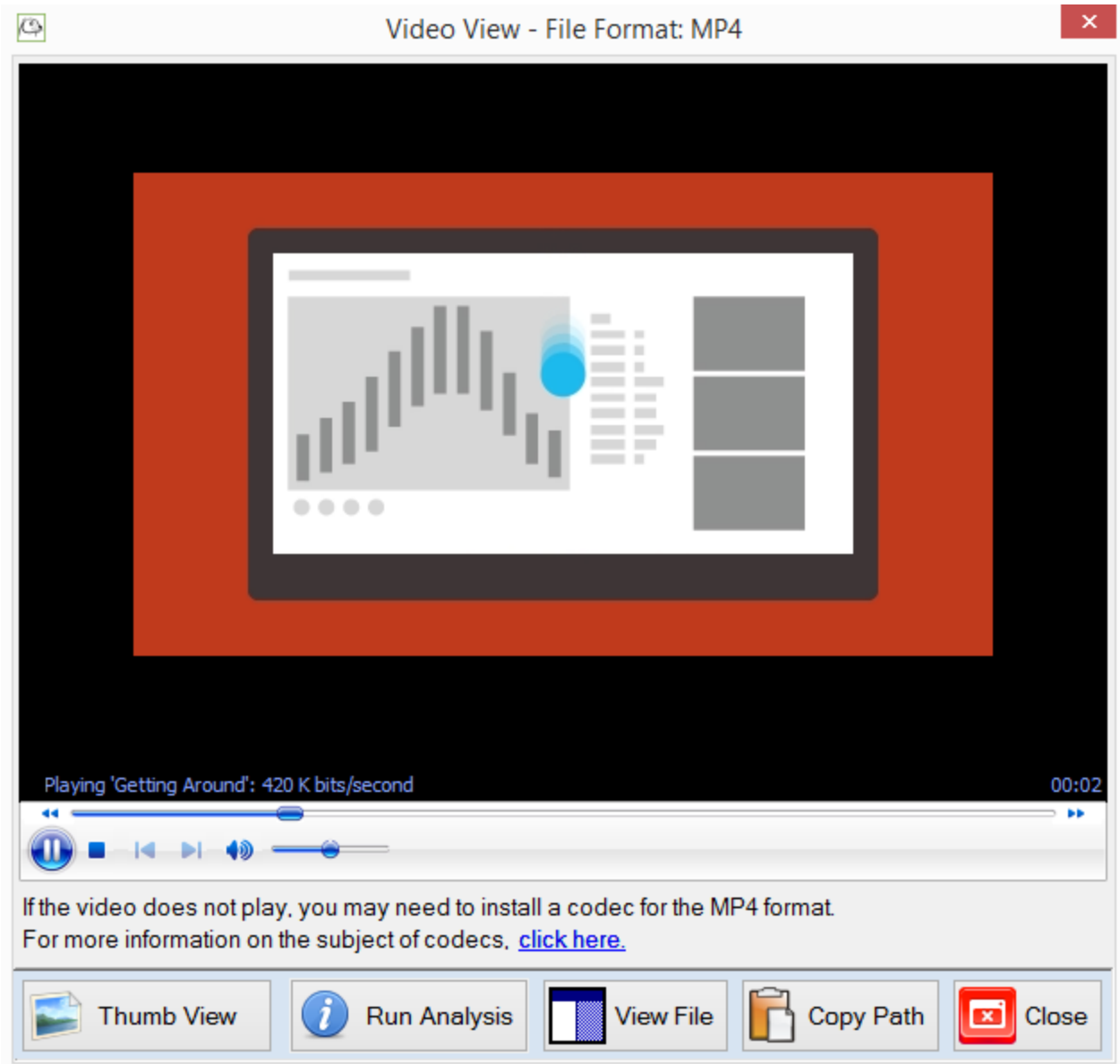


Figure 5. The ShowImage / Movie window.

Important note: PCFerret may detect pornographic, or other movies or images on a computer. Finding such material does not indicate that a computer user is, or should be, aware of its presence or that the user has knowledge of such material being placed there, as It is possible for websites to contain media of this nature of which the user may be unaware. Therefore, undesirable content on a computer does not necessarily indicate that a particular website was visited by the user nor that the user was aware of the link or content.

Cached URLs Tab

The Cached URLs tab has been designed to extract URLs from all files found in the caches of the top six most commonly used browsers' cache. The browser names can be seen in figure 1.

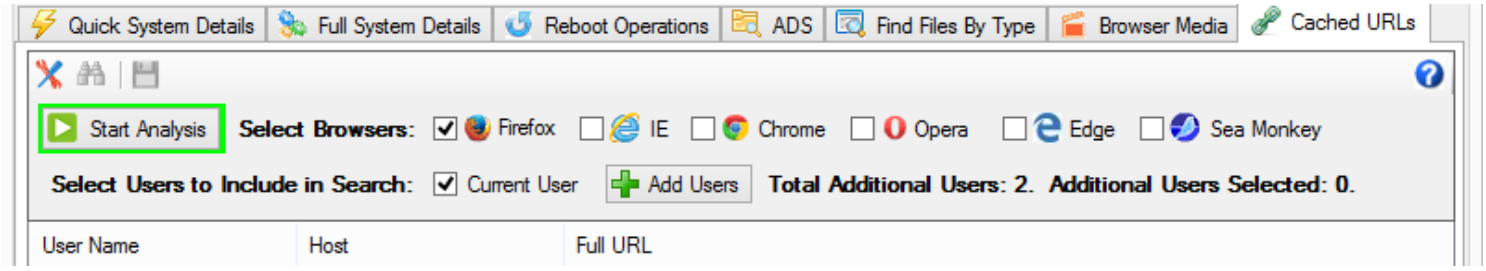


Figure 1. The Cached URLs tab.

To view the URLs (if any) in your browsers' caches, select the browsers you wish to examine and click the Start Analysis button. Only the browsers which are installed on your computer will be selectable.

To view the browser caches of other user accounts (if any) on the computer, select the users from the list produced when the Add Users button (shown above) is clicked. Please note that although a user account may be present on a computer, it does not mean that it will be displayed here. That is due to the fact that although an account is present, no login may have taken place. Additionally, a browser may not have been run on an account since it was created. In either case, no browser caches would be present, so to avoid any potential confusion, PCFerret does not display these accounts.

The Results

During and after the browser's caches have been scanned, a list of URLs which have been found by PCFerret will be displayed. The format of these results can be seen in figure 2. There are additional column headings which are not shown in figure 2. These headings can be viewed either via the horizontal scroll bar or by expanding the view of PCferret.

You can sort the result by clicking on the column headings.

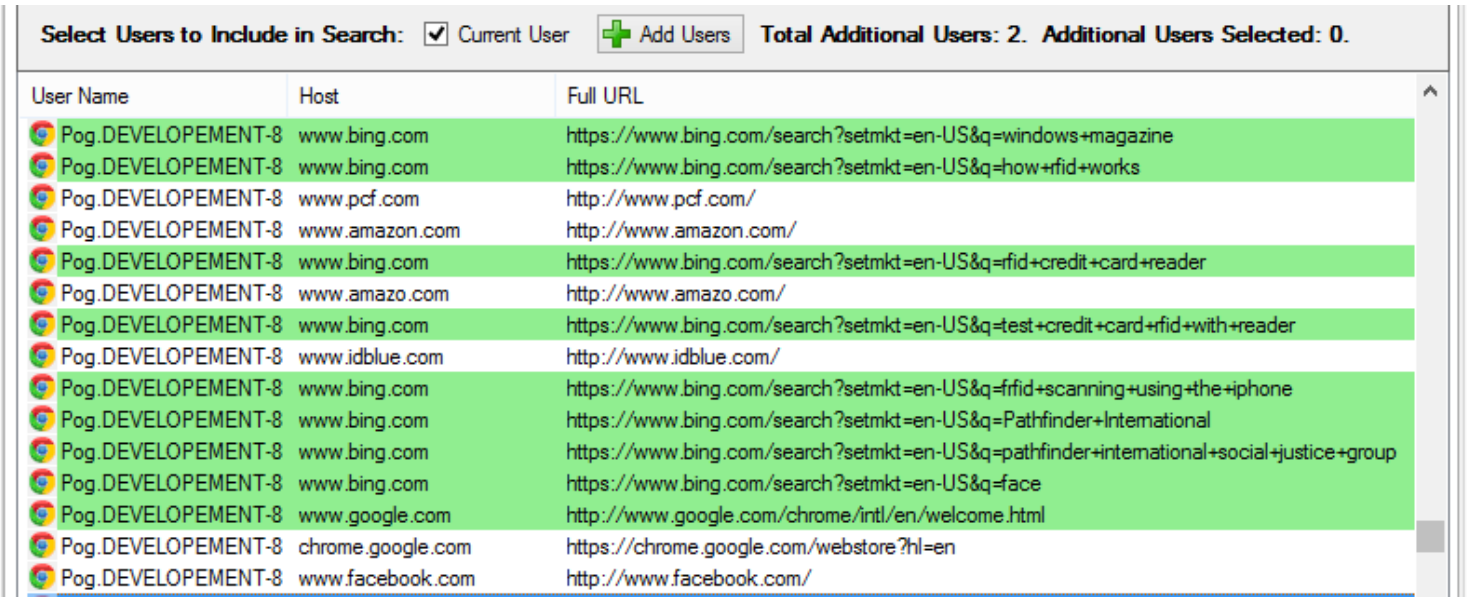


Figure 2. An example of some results.

Key to the Color Coding Of The Results

Notice how the URLs of search engines are shown in **Green**. Other colors which may be displayed are:

Yellow: The highlighted URL is a Level 1 warning.

Red: The highlighted URL is a level 2 warning.

Orange: The highlighted URL is a Level 1 warning and is search engine related.

Purple: The highlighted URL is a Level 2 warning and is search engine related.

This color scheme in no way indicates the true nature of the URLs displayed. They are merely coded in accordance with the words and phrases in PCFerret's database (see below) and by PCFerret's search engine detection algorithm.

The Warning Levels

Level 1 and Level 2 warning levels are defined by the user and, where applicable, the default words and phrases supplied in the default PCFerret Database which was installed along with PCFerret. For a full description of how the database integrates with PCFerret and how the user can change these definitions, please see the Options section of this help file.

Important note: The default PCFerret Words and Phrases Database configuration is designed to reveal links which may point to pornographic websites. The list of words and phrases is by no means exhaustive and serves only to give the user an example of use. Matches on the words and phrases do not necessarily mean that the destination website contains pornographic images as some words or phrases may innocently

form parts of other, larger, words and phrases. These words and phrases can be removed, edited and deleted by the user. It is also possible for links to pornographic websites to be incorporated in other, non pornographic websites. Therefore, a link to a pornographic picture found in a user's browser's cache does not necessarily indicate that the site was visited by the user nor that the user was aware of the link.

For further details on PCFerret's Words and Phrases Database, please see the Options section of this help file.

The Results Context (right mouse click) Menu

Right-clicking on a result will produce the context menu shown in figure 3 below.

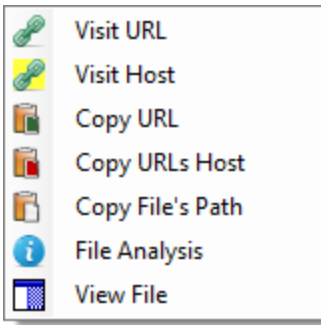


Figure 3. The context (right-click) menu.

Each of the menu items is explained below.

Visit URL

Clicking this will take you to the website destination specified under the Full URL heading.

Visit Host

Clicking this will take you to the website destination specified under the Host heading.

Copy URL

This will copy the FULL URL to the Windows Clipboard.

Copy URLs Host

This will copy the Host to the Windows Clipboard.

Copy File's Path

This will copy the path of the file in which the URL was found. This data can be found under the results

column, File In Which URL Was Found. This is not shown in figure 2.

File Analysis

This will invoke the File Analysis Report module for the above file.

View File

This will invoke the View File module for the above file.

Find

Clicking on the find button or pressing *Ctrl+F*, will display the find dialog as shown in figure 4.

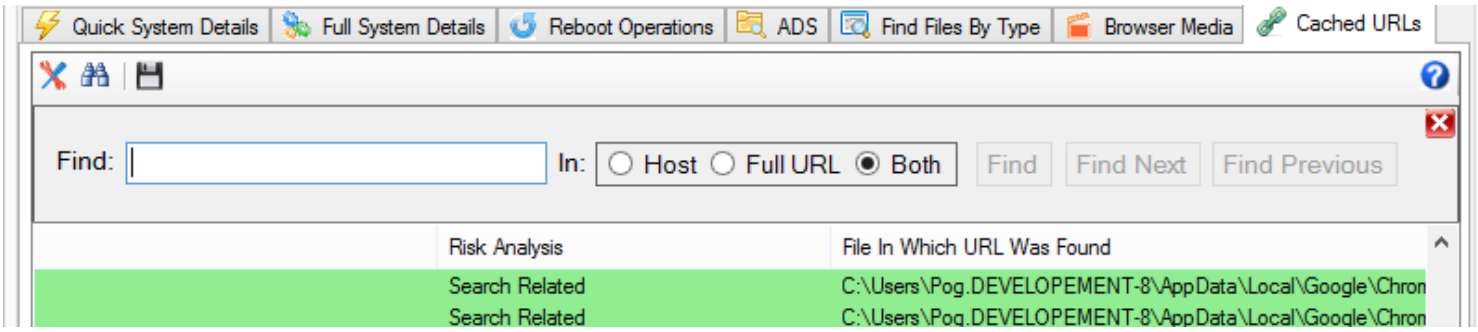


Figure 4. The Find Option.

The find options work the same way as most other find options in Windows programs but with one exception, which is detailed below.

As URLs cannot contain spaces, spaces in URLs are replaced with the text of %20. %20 is the hexadecimal ASCII equivalent of the space character. For example, where you see a URL such as http://example.com/FirstName%20LastName, this is the human writing equivalent of http://example.com/FirstName LastName (notice the space between FirstName and LastName). PCferret is programed to recognize this, so to search for this URL, you would enter in the Find: field, "FirstName Lastname", without the quotation marks. In other words, you would use the space character where you would expect to find a space and not the %20 equivalent.

Save

If you wish to save the results, you can do so by clicking on the Save button. This will save a report in HTML format using your chosen folder and file name. Prior to being prompted for this information, you will see a window containing some options, as shown in figure 5.

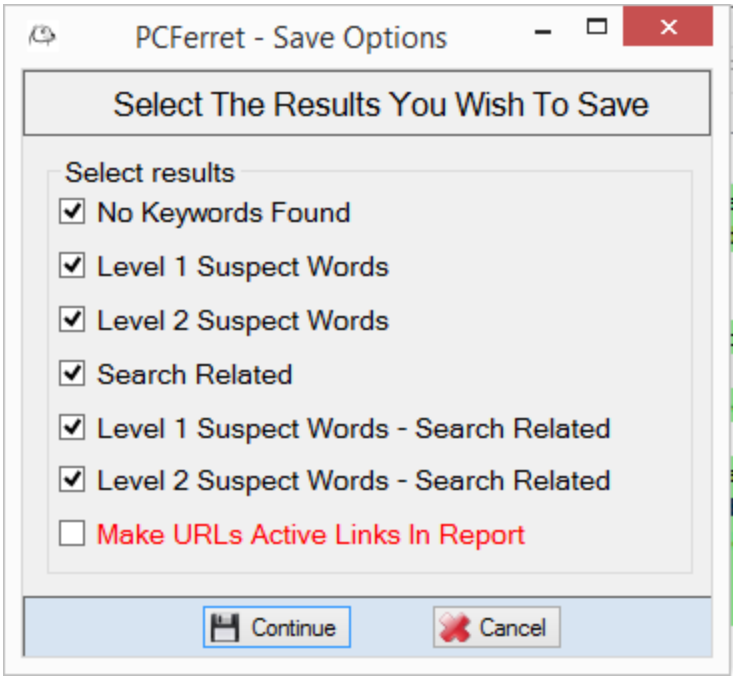


Figure 5. The Save Options.

These options will allow you to save only the options you are interested in. Selecting Make URLs Active Links In Report will make all URLs contained in the report clickable. This will result in anyone viewing the report being able to go straight to any website listed in the report by clicking on the result's respective link. If this option is selected, the following text will appear close to the top of the report:

"VISITING WEBSITES CAN CAUSE YOUR COMPUTER TO BECOME INFECTED WITH A VIRUS OR MALWARE, MAY RESULT IN COMPROMISED OR LOST DATA, OR COMPROMISE YOUR COMPUTER IN OTHER NEFARIOUS WAYS. PLEASE CAREFULLY CONSIDER THIS FACT PRIOR TO VISITING A WEBSITE VIA THE LINKS SHOWN BELOW.

The links shown below may be temporary, or produced by the visited website for other purposes. These links may no longer function as expected or may produce unpredictable results or error messages."

Of course, the report can be printed directly from any of the supported browsers and most likely, many others.

TIP: You can save a report with the entries in an order specified by you, if you sort the results by a column heading prior to saving the report.

Options

The *Options* window enables you to tailor PCFerret's options to suit your individual requirements. The Options are currently divided into three categories, *General*, *Find Files By Type* and *Cached URLs*. Each is explained below.

General

Check For Updates On Startup

By default, if an Internet connection is available, PCFerret checks to see if you are running the latest version. If not, PCFerret will offer to download and install the latest version for you. Unchecking this option will prevent PCFerret from doing so.

You can check for PCFerret updates at any time by selecting Help >> Check For Updates from the main menu.

Find Files By Type

Reduce Positives

These options are provided to the user in order to Reduce False Positives (reduce the number of files which are reported to be of a certain type, when they are not). This can occur when files unrelated to the search criteria contain the same binary signatures (headers, etc) as the kind of file PCFerret is searching for. Some file types can be indistinguishable from others during analysis for this reason.
These settings are optional as some files may be given a different file extension in order to disguise their true content or they may have been inadvertently, incorrectly named. The details of such files will be shown with a red highlight on any search results. More information on this can be found here.

By default, all False Positive options are checked.

Warning Messages

Display Long Wait Warning

A warning message is displayed when selecting the Find Files By Type tab. This is designed to provide additional information to new users.

By default, this option is checked.

For more information on finding files by type, click here.

Cached URLs

Reduce the number of URLs returned, with these options

These options are designed to reduce clutter in your reports by only displaying / saving data that is relevant to your purpose. Each option works independently with the exception of the Show Only Search Engine URLs, which overrides all other options.

Most of these options are self-explanatory, however, I feel that the less experienced computer user may benefit from the following two explanations:

Ignore Local IP Address

Local IP Addresses are IP Addresses which are not outside of your internal network. Therefore, anything bearing a local IP Address may not be of interest to you so you can disable their reporting by checking this option.

Do not show URLs which only point to icon (.ico) files.

When you look at the URLs found by PCFerret, you may notice that a lot of them link to nothing more than an icon file on the website to which it links. This is not uncommon in relation to URLs found in a Browser's Cache. The URLs may contain information which may be valuable to you, depending on what you are looking for. Such a URL will of course, show the website's address. However, if these type of entries are of no value to you, you can prevent them from being displayed by checking this option.

By default, all of these options are unchecked.

Warning Messages

Display Long Wait Warning

A warning message is displayed when selecting the Cached URLs tab. This is designed to provide additional information to new users.

By default, this option is checked.

Display Website Content Warning

A warning message is displayed in order to alert new users to the possible dangers of visiting websites via the links shown by PCFerret.

By default, this option is checked.

Add / Remove Key Words for Level 1 and Level 2 Warnings

This option allows you to add, edit and delete key words or phrases contained in PCFerret's installed database. The database is designed to allow you to customer the warnings given when searching for URLs.

When this button is clicked, a list of key words and phrases which are contained in PCFerret's database is displayed. Using the Add, Edit and Delete buttons, you can customize the Level 1 and Level 2 warnings (see below) which will alert you to words or phrases contained in the database which have been found in URLs displayed by PCFerret.

When such matches are found, the URLs in the Cached URLs section are displayed in the following highlighted colors. All other entries (non matches) are shown with a white background:

Green: The highlighted URL is search engine related.

Yellow: The highlighted URL is a Level 1 warning.

Red: The highlighted URL is a level 2 warning.

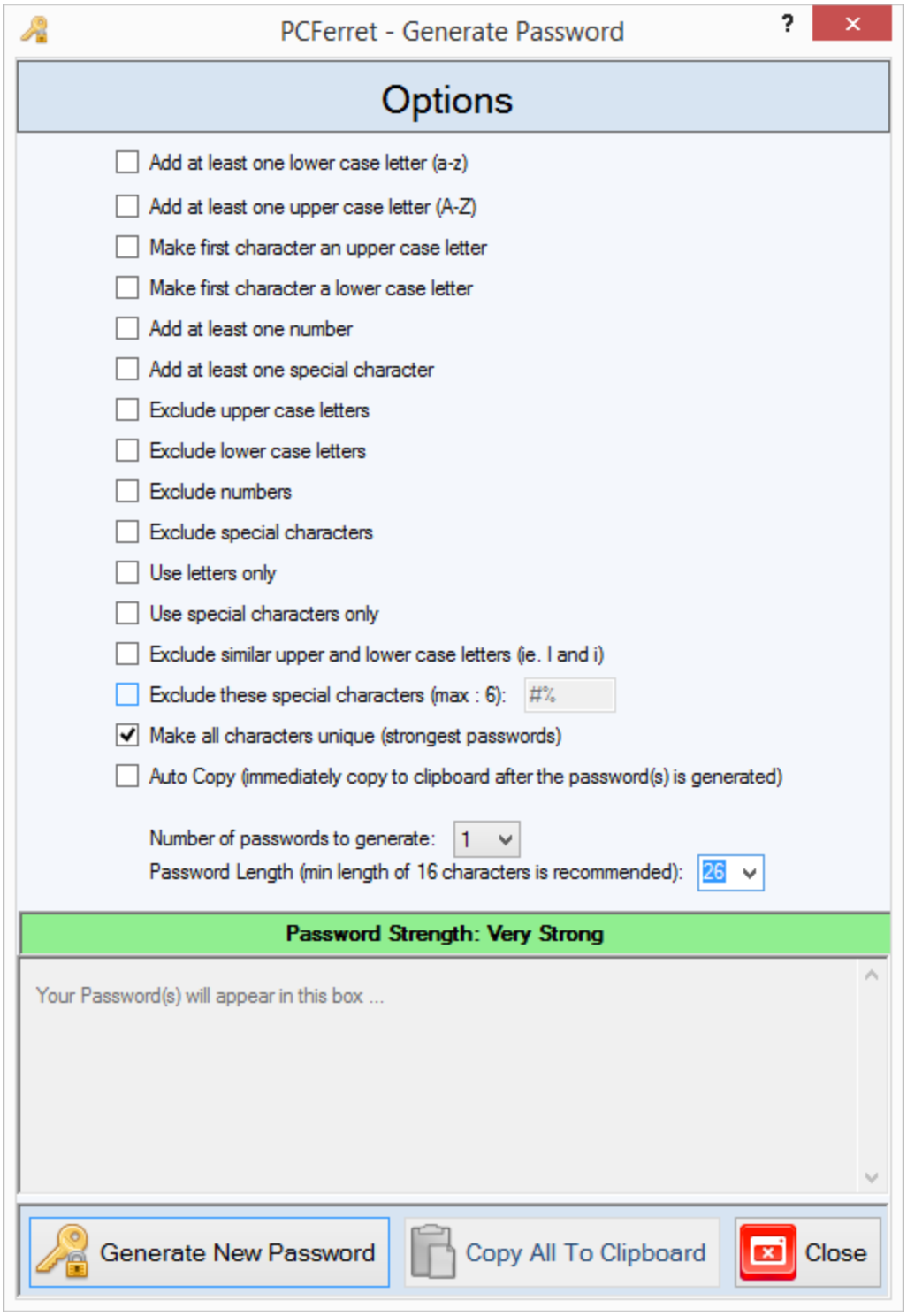
Orange: The highlighted URL is a Level 1 warning and is search engine related.

Purple: The highlighted URL is a Level 2 warning and is search engine related.

This color scheme in no way indicates the true nature of the URLs displayed. There are merely coded in accordance with the words and phrases in PCFerret's database and by PCFerret's search engine detection algorithm.

Generate Password

When you select the *Generate Password* tool, you will be presented with a screen which looks like this:



The options are self-explanatory so we are going to concentrate solely on the use of the Password Generator.

You can use the default options simply by clicking on the *Generate New Password* button.

The password(s) can be copied to the Windows Clipboard by clicking the *Copy All To Clipboard* button. You can copy individual passwords by using the context (right-click) menu item *Copy Selected To Keyboard*.

If the *Auto Copy* option is selected, the password(s) will be copied to the clipboard automatically after creation.

Hash Generator

General

The *Hash Generator* is designed to calculate the Hash value of a file using user selected hash algorithms. The following algorithms are available;

MD5
SHA1
SHA256
SHA384
SHA512

To Calculate a File's Hash Value(s)

1. Select the file you wish to generate the values for by clicking on the Select button or the File field. This will display a file selection dialog.

2. Having chosen the file, check the boxes under the Include heading to select which hash values you wish to generate.

3. Optionally, you can then select a format for the generated hashes under the Add Dashes heading drop down menu. The format of previously generated hash values can also be changed using this control.

4. Optionally, choose if you wish to display the generated values in uppercase. This is the default setting. The format of previously generated hash values can also be changed using this control.

5. Click the Generate Hash Value(s) button. This will save your chosen options as the defaults for later use.

PCFerret will now generate the required hash values and keep you updated as to progress via various status messages. If the file you have chosen is large, you will also see a progress bar to indicate that PCFerret is working on the hash calculations.

Copying The Hash Values

Once the hash values are calculated, they are displayed on the screen. You can copy individual hash values to the Windows Clipboard by clicking the Copy button next to the hash value you wish to copy. Alternatively, you can copy all the hash values by clicking the Copy All button.

If you click the check box for the Exclude Hash Names prior to copying the value, PCFerret will not include the hash's name as part of the copy function. For example;

Normal Copy
MD5: 31B6F5B7388A57A5E085C7CB8C6D20DB

Exclude Hash Name
31B6F5B7388A57A5E085C7CB8C6D20DB

Reporting Options

A report containing the resultant hash values can be either saved to disk or printed by clicking on the Save and Print buttons, respectively. When you click on the Save button, you will be prompted for a location and a file name. The report is saved in the .txt format.

The *Exclude Hash Names* option discussed above performs the same functionality for the report as it does the copy function.

If you wish to exclude PCFerret's Header from your report, select the check box next to the Exclude Header From Report option prior to saving or printing.

Below is an example of how a report is formatted, in this case, with the header present.

PCFerret, version 2.2.0.1114 - File Hash Generation Report

Report Created: 03/01/2015 at 5:52:52 PM

File Name: C:\Temp-Wip\SSDTSetup.exe

MD5:
31B6F5B7388A57A5E085C7CB8C6D20DB

SHA1:
842F2E25D4C8A79B68F25B58760E7B6992FD3A87

SHA256:
2F1FA9C8703A9DB9B3A7F6EAEA6BC2E44B8C3AD146B5EEE17C68F598FAFA9AFA

SHA384:
4CCAC4358E5C96CD5BD36104C0D345CE6D6B0040177C1279E805C5C37A303F56AA98898E5B3548DF3F55F0B58B09BC25

SHA512:
AA41DDFEC19BECD0BB19B1637876DCBE7D4B218DE3773888ECB38E1D4A0EB3013B335F64938D73FCFFC4FB699E4A9657550F73D329B19AE57D11617E3E482292

Windows Error and Warning Event Viewer

The *Windows Error and Warning Event Viewer* is designed specifically to aid the IT Professional in diagnosing Windows issues, without the need to scroll through hundreds or thousands of irrelevant Event Viewer (log) entries.

PCFerret allows you to concentrate your focus on the Errors and Warnings which may appear in the specified Event logs, during a specified time frame. You can choose to view Errors, Warnings or both.

The following event logs can be selected as shown in figure 1 below: Application, Setup, Security, and System.

After clicking the *Get Events* button, a *STOP* button will appear in its place. This button gives you the option to abort the search should you so wish, when the Event Logs are very large and the process is taking too long.

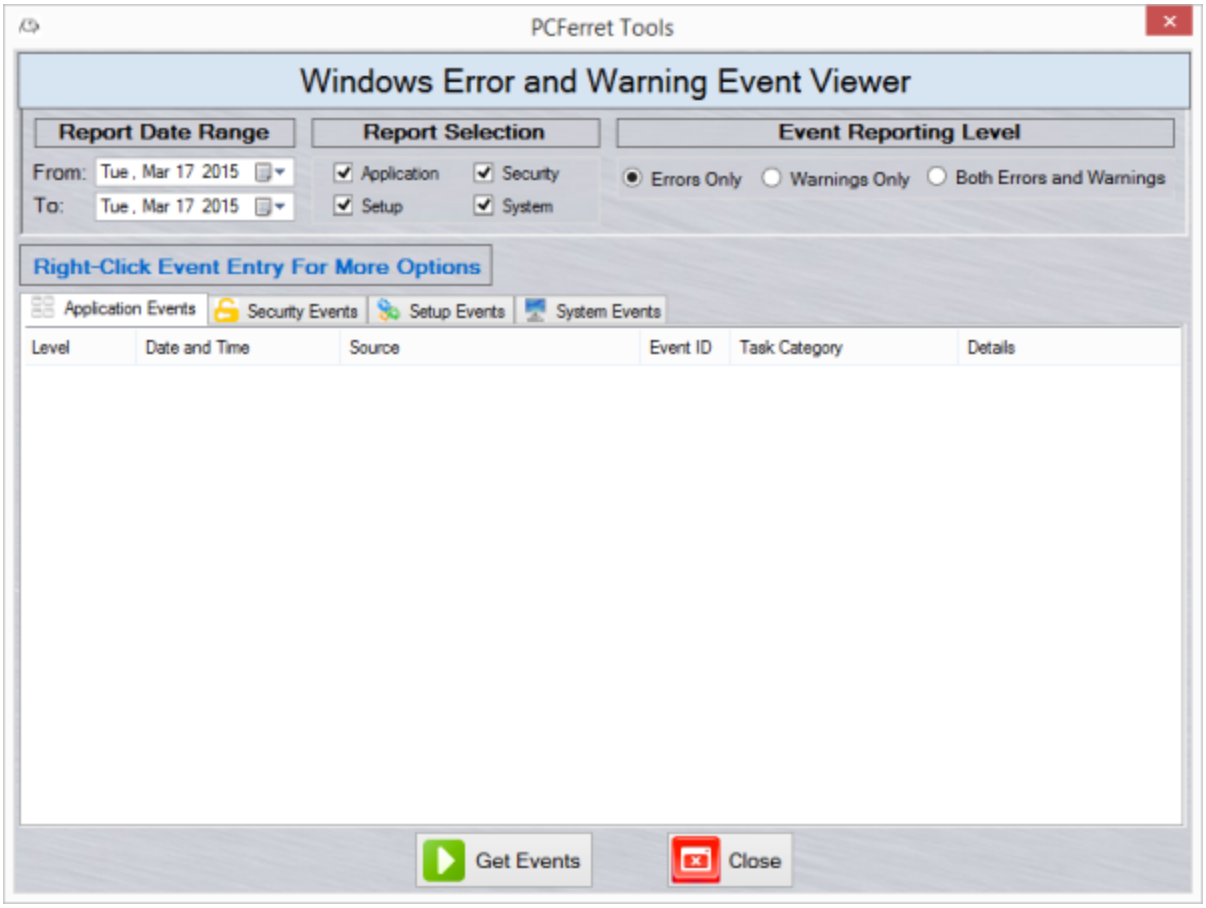


Figure 1. The Windows Error and Warning Event Viewer screen. Shown at 75% of actual size.

A right-click on any listed events will display the Context Menu as illustrated in figure 2 below

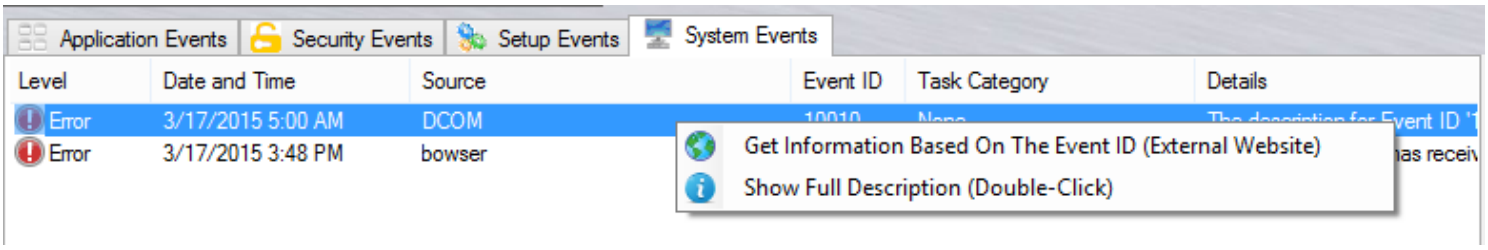


Figure 2. The Context Menu.

Menu Options

Get Information Based on the Event ID (external website): Selecting this will take you to the specific details for this Event ID on the website EventID.net.

Show Full Description (double-click): This option allows you to view the full description of the event in a viewer window. See figure 3 below. Double-clicking an event will also display the full description.

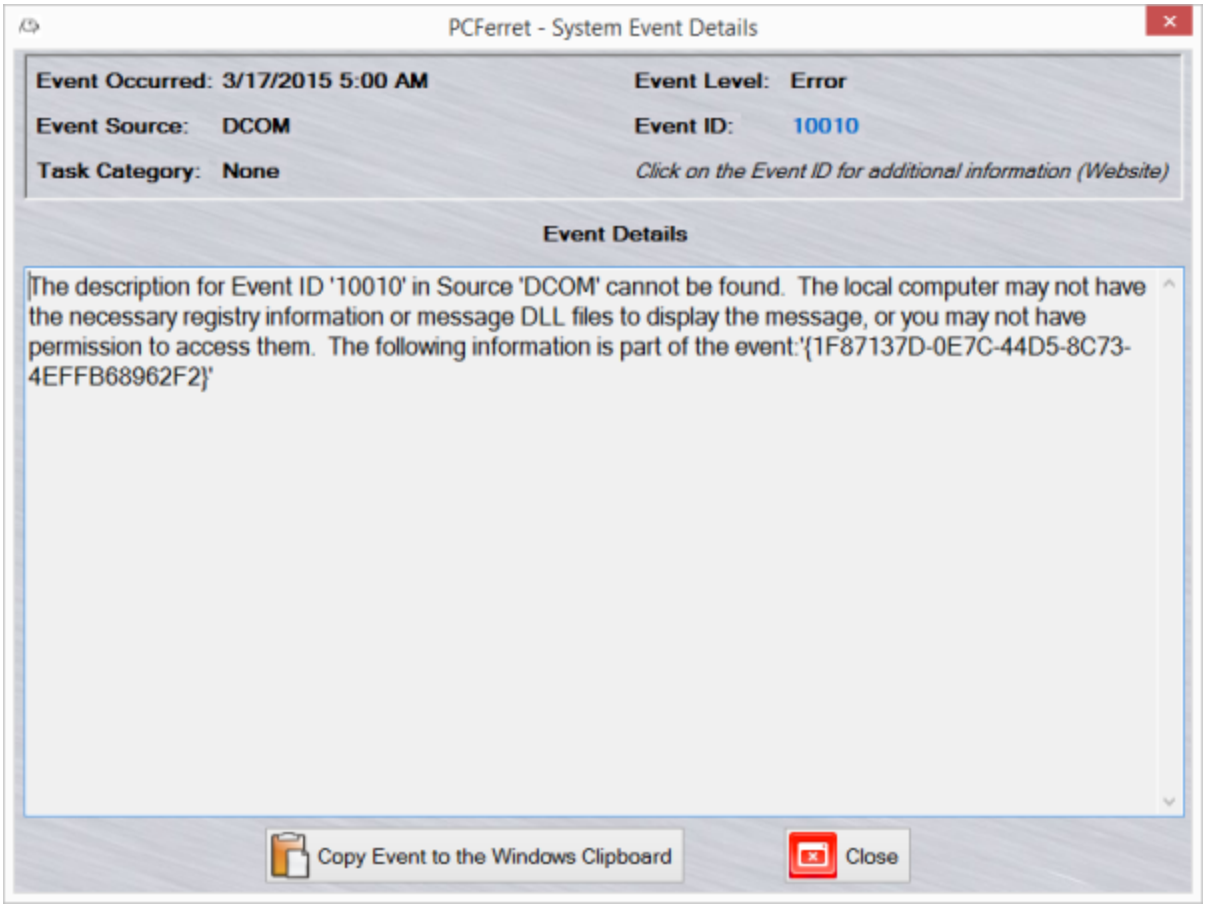


Figure 3. The Event Description Viewer. Shown at 75% of actual size.

Clicking the *Copy Event to the Windows Clipboard* button will instruct PCFerret to copy all of the event details to the Windows Clipboard.

Tip: Copying the Event Occurred date and time from the Windows clipboard makes an excellent search

string for finding the event in the Windows Event Viewer.

Analyze File

The *Analyze File* option is designed to give you as much information as possible about a selected file without having to look in many places. It is the one-stop shop for file information.

For more information and details relating to the generated report, click here.

Detect Tor Browser

The Tor Browser is typically used by people who value their privacy and do not wish for their activities to be tracked on the Web.

The existence of the Tor Browser may, however, be an indication that someone may have something to hide. (For example, inappropriate images or data).

By using this feature, you will be able to detect the presence of the Tor Browser on a PC.

To run this feature, select *Tools >> Detect Tor Browser* from the main menu and you will be presented with the window shown in figure 1.

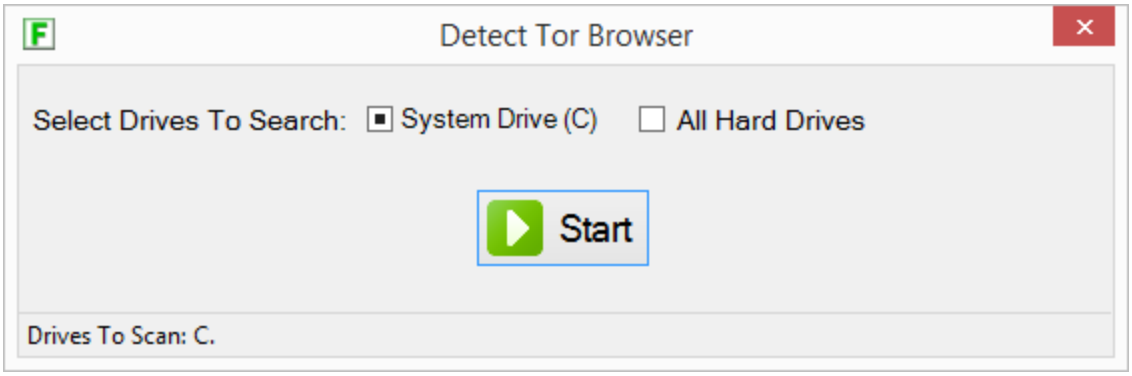


Figure 1. The Detect Tor Browser window.

If you just wish to search your system drive (typically C), just press the Start button. If you wish to search all of your PC's fixed drives, select the *All Hard Drives* option, then press the *Start* button.

During the search, you will be presented with the window shown in figure 2.

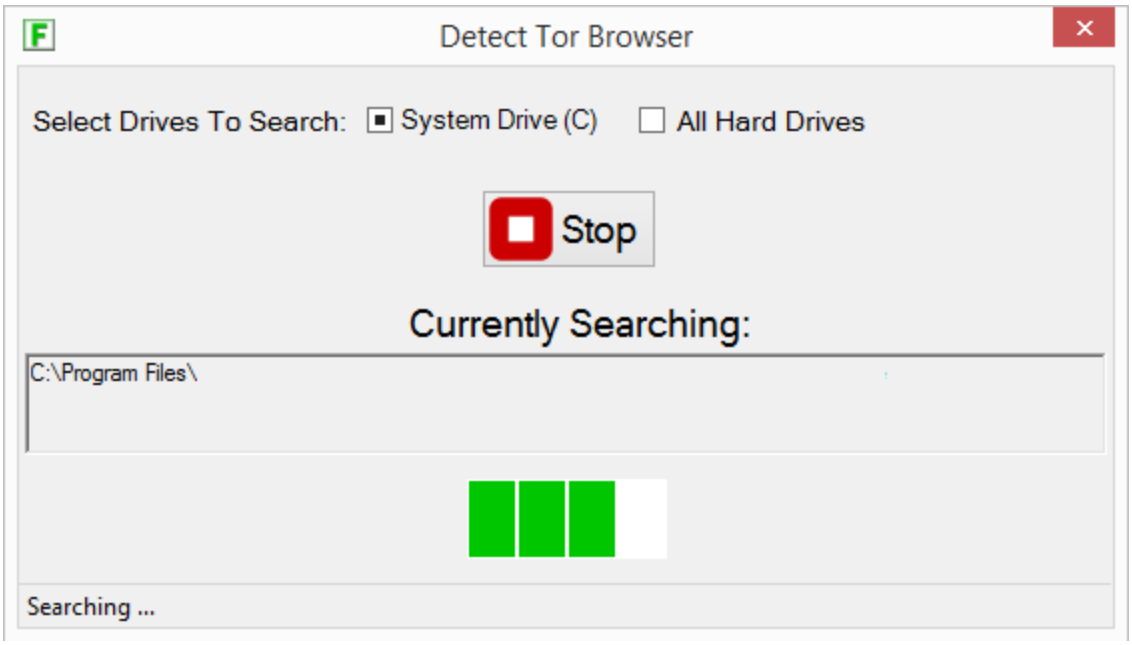


Figure 2. The Tor active search window.

The search can be stopped at any time by pressing the *Stop* button.

Upon completion of the search, PCFerret will let you know if it found the Tor Browser. If PCFerret has found it, you will be given the option to copy the path in which it was found to the Windows Clipboard.

Clean Uninstall

The *Clean Uninstall* tool has been specifically designed to remove all files and registry entries created by PCFerret Pro versions from a computer on which it is installed. This is to assist in a covert analysis of a computer. It is important to note that the *Clean Uninstall* tool may NOT leave a computer forensically free of PCFerret references. This is because the Windows operating system and other programs may create their own references to PCFerret. Removing every single reference ad-hoc could leave a computer unstable. Instead, PCFerret removes all program files (except for the Pro Portable version as the files on the removable device are left intact), data files and Registry entries created by PCFerret.

To help prevent unwanted PCFerret references being left on a computer after a *Clean Uninstall*, it is best to save reports to an external medium, however, if an external medium is used, please be aware that a reference to the device you use, your user name, the device's manufacturer and a date/time stamp may be forensically accessible after the fact. If you save a report to the computer's hard drive, remember to rename it and securely erase it, using a reliable tool such as AxCrypt (http://axantum.com/AxCrypt). While AxCrypt is primarily an encryption program, it also features a reliable data shredder.

After the *Clean Uninstall* has completed, PCFerret will need to reboot (restart) the computer. Some of PCFerret's files may remain on the computer if the reboot is not permitted to take place. It is important that you make sure any unsaved work is saved, prior to rebooting the computer.

Of course, you can also uninstall PCFerret in the usual way by selecting *Uninstall PCFerret* from your program group or by uninstalling it via the Windows Control Panel's *Uninstall a program* option.

View File Option

As can be seen in figure 1 below, the *ViewFile* option shows the plain text contents of the file in the right-hand-side pane and the hexadecimal representation of the file's contents in the left-hand side-pane.

If the file is an image or video file, depending on the format, PCFerret will attempt to display it for you under the *Additional Information* heading. For video display, *Windows Media Player* version 9 or greater must be installed on the computer.

If something suspicious is detected about the file being viewed, a warning message will be displayed under the *Additional Information* heading.

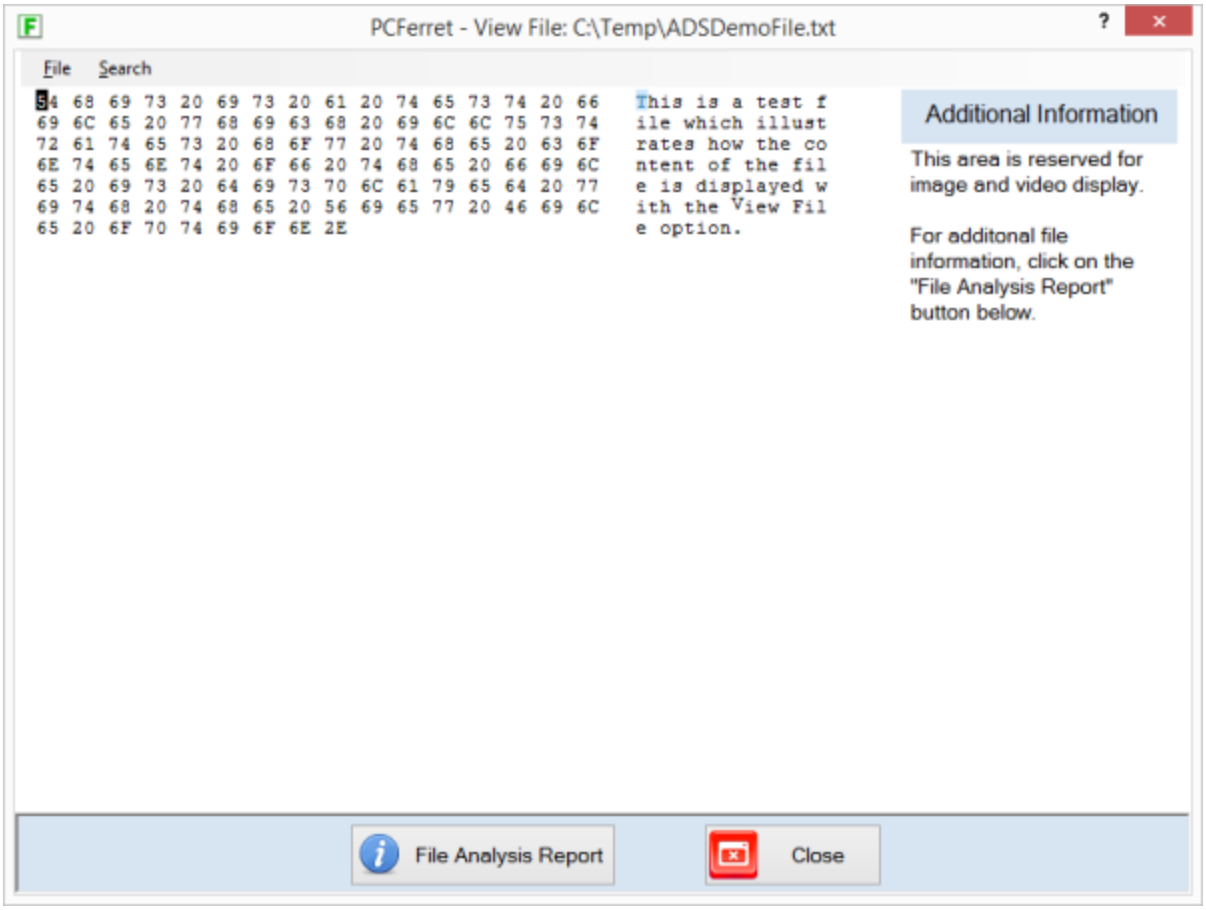


Figure 1. The ViewFile Window. Image reduced to 75%.

For information relating to the File Analysis Report button, click here.

View ADS File Option

As can be seen in Figure 1 below, the View File option shows the plain text contents of the file in the right-hand-side pane and the hexadecimal representation of the file's contents in the left-hand side-pane.

If the file is an image or video file, depending on the format, PCFerret will attempt to display it for you under the *Additional Information* heading. For video display, *Windows Media Player* version 9 or greater must be installed on the computer.

If something suspicious is detected about the file being viewed, a warning message will be displayed under the *Additional Information* heading.

If an executable file (.exe, .com, .pif, .bat, .cmd, .reg, .mst, .msp, .msi, .vb, .vbe, .vbs, .vbscript, .ws, .wsf, .tga) is present in an ADS, you will be alerted by the item being highlighted with a red line and the following text will be displayed, "Warning: This file may be an executable program file. Caution is advised." When this warning is present, care should be taken not to run the suspected executable if it is separated from the main file (see ADS Tab for details) as it may be a virus or program designed to cause harm to your computer or data.

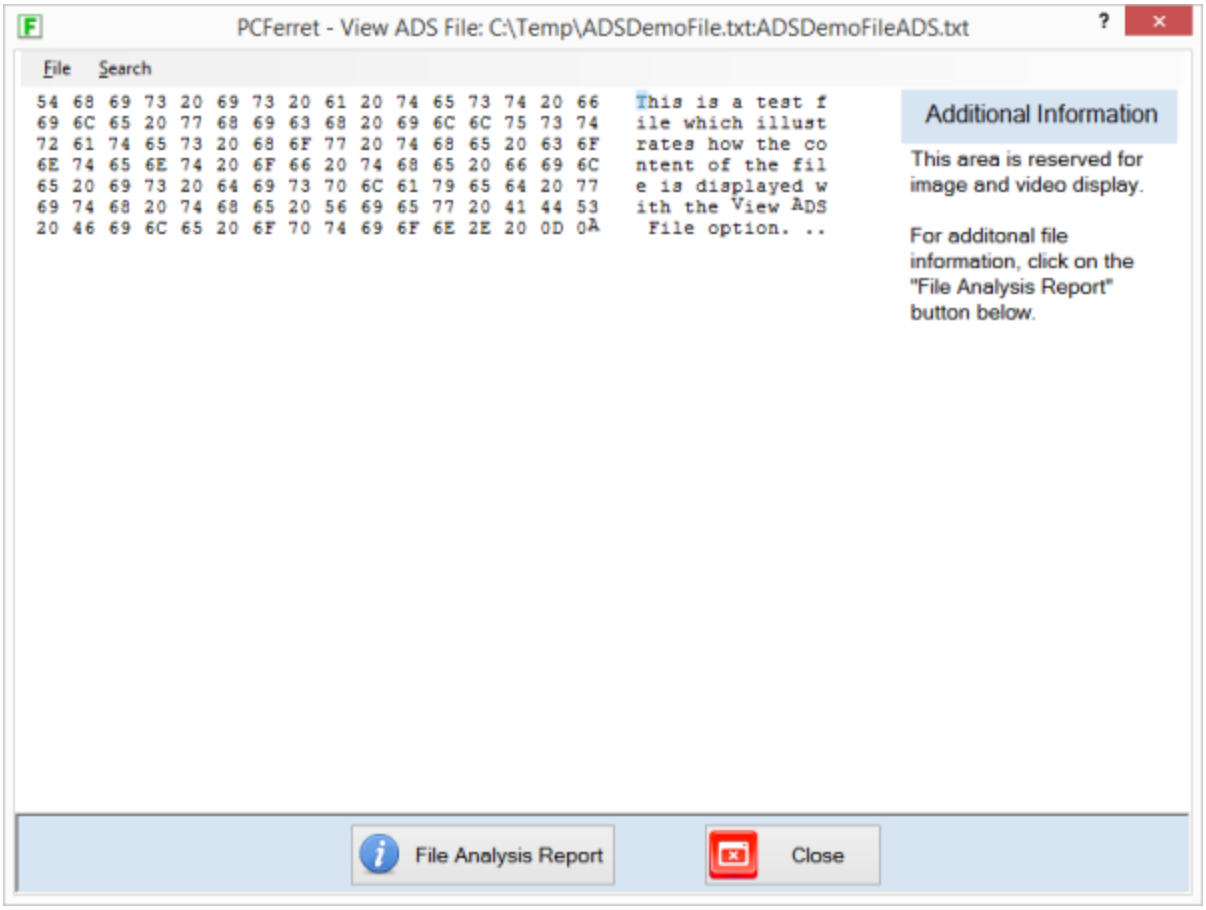


Figure 1. The ViewADS File Window. Image reduced to 75%.

For information relating to the *File Analysis Report* button, click here.

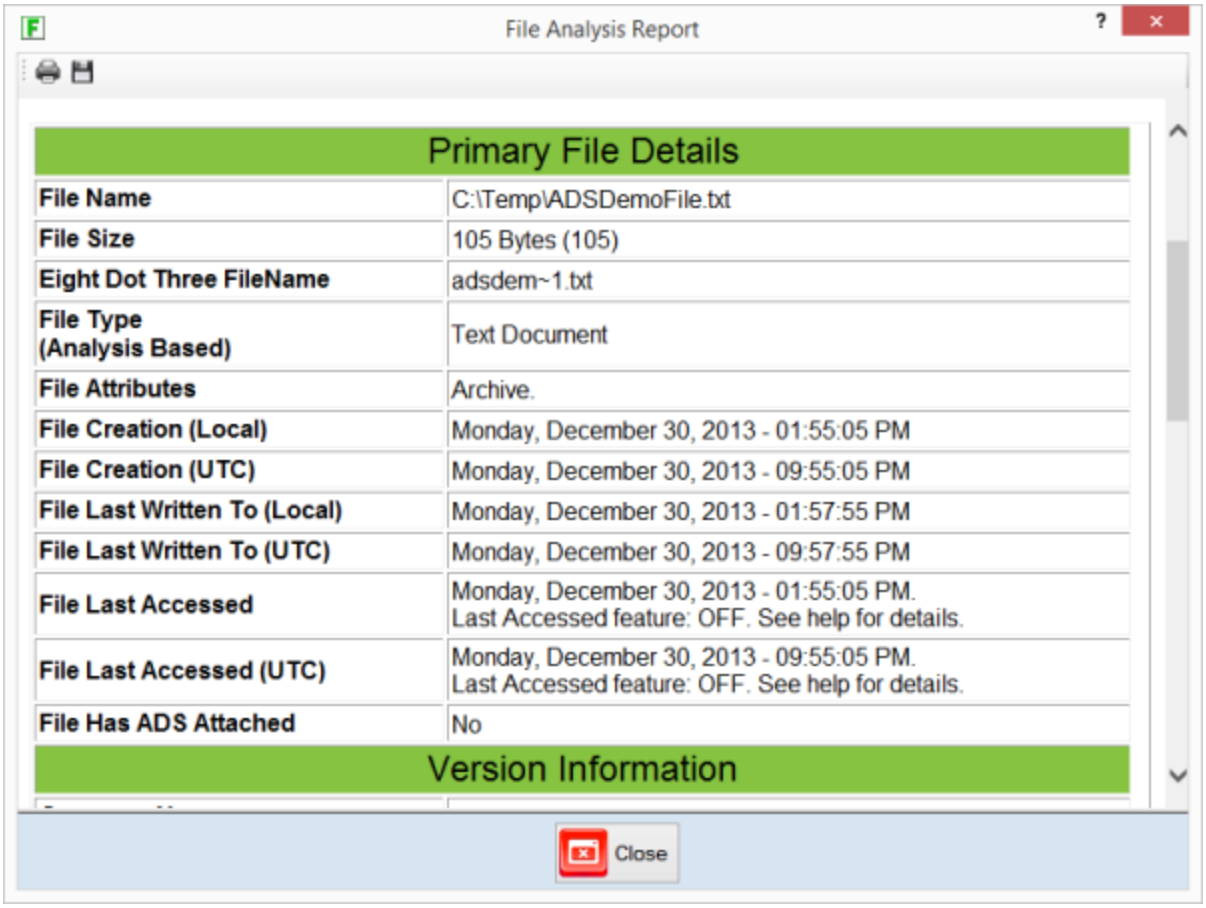
File Analysis Report

This report (see figure 1 below) is available from the ADS Folder and File Selection dialog box, the Tools >> Analyze File menu option and the Find Files By Type results window.

When selected, this report gives an analysis of the selected file including, but not limited to, date and time stamps, attributes and content analysis.

This report can be saved to disk or printed.

The information contained in the report may vary depending on the type of file selected.



Primary File Details	
File Name	C:\Temp\ADSDemoFile.txt
File Size	105 Bytes (105)
Eight Dot Three FileName	adsdem~1.txt
File Type (Analysis Based)	Text Document
File Attributes	Archive.
File Creation (Local)	Monday, December 30, 2013 - 01:55:05 PM
File Creation (UTC)	Monday, December 30, 2013 - 09:55:05 PM
File Last Written To (Local)	Monday, December 30, 2013 - 01:57:55 PM
File Last Written To (UTC)	Monday, December 30, 2013 - 09:57:55 PM
File Last Accessed	Monday, December 30, 2013 - 01:55:05 PM. Last Accessed feature: OFF. See help for details.
File Last Accessed (UTC)	Monday, December 30, 2013 - 09:55:05 PM. Last Accessed feature: OFF. See help for details.
File Has ADS Attached	No
Version Information	

Figure 1. The File Analysis Report. Section of report shown at 75% of its actual size.

Invalid File Name - See Help for further details

When the above message is displayed in red adjacent to the file name in the report, it indicates that the file name contains characters which are not valid in file names. When this occurs, certain Microsoft Windows functions will reject the file name which means that PCFerret will be forced to skip certain details on the report.

Updates

Whenever PCFerret is run, it will check the PCFerret server via your Internet connection (if available) to see if an update is available. You can read more about this in the EULA. This option can be disabled by changing the *Check For Updates On Startup* option on PCFerret's Options screen.

If an update is available, PCFerret will provide you with the details of the update and an option to automatically download and install it.

You can also check for updates by selecting *Help >> Check For Updates*.

Support

PCFerret is now free to download, install and use. Therefore, no technical support is offered nor provided.

What is an Alternate Data Stream (ADS)?

Overview

Alternate Data Streams (ADS) are part of the NTFS file system in Windows operating systems. They are not included in the FAT and FAT32 file systems. ADSs were originally included in NTFS to provide compatibility with the Macintosh File System.

What is an ADS?

Every file has a primary data stream called :$DATA. This stream contains the information we are used to seeing, such as the content of a word processor file or plain text document. The ADS is another data stream (file) which can be attached to the primary data stream (file). It contains information which is not typically accessible to the computer's user and it not visible in programs such as Windows Explorer. The command line command DIR was not able to list ADSs prior to Windows Vista. From Vista onwards, the /r switch can be added to the DIR command (dir /r) in order to list ADSs, albeit in a somewhat crude format.

So what are they used for?

Most frequently, ADSs are used as meta data (data about data) relating to the main file (or stream). For example, a typical ADS would be a Zone.Identifier. This contains information relating to the file's source. "Internet" is a very common example of a source. You will see many examples of these files when you use the ADS tab in PCFerret. It is worth noting at this point that a Zone.Identifier should contain information relating to the primary file's source, but in reality, it could contain anything, including an executable program which has been maliciously placed there. But don't worry, PCFerret can detect this and make you aware of it.

Should I worry if a lot of my files have an ADS associated with them?

No. There are many legitimate reasons for files to have ADSs.

Are ADSs a threat?

They can be. This is why PCFerret scans for them. An ADS can, for example, contain an executable program which can be executed nefariously. With PCFerret, you can view the contents of ADSs and if PCFerret detects anything odd about them, it will inform you. If an ADS contains a video or image, it will play or display it for you if it is a common type, otherwise, PCFerret will warn you of its presence but not display it.

Examples of ADSs

If you wish to experiment with ADSs, here is an example of how to create one.

In order to follow this example, you will need to create a command line prompt. In order to do this, press the **Windows Key** and the letter **R** key simultaneously. This will result in a **Run Dialog** box appearing. In the dialog box, type **cmd** then click or tap on the **OK** button.

The example below uses the prompt **c:\>**, but this may be different on your computer. Regardless of the prompt, the example will work just the same.

Creating an ADS

First, use Notepad to create and save a simple text file called ADSCarrier.txt containing any text you wish. Then, type the following on the command line;

echo This is the content of my newly created ADS file. > ADSCarrier.txt:MyHiddenFile.txt

Next, press **Enter**.

Now you have created an ADS with the file name of MyHiddnFile.txt, containing the text, "This is the content of my newly created ADS file." This ADS is now invisibly attached to the file you created using Notepad called, ADSCarrier.txt. Try experimenting by using other file types to create your ADSs. There are plenty of online tutorials which demonstrate further examples.

Now you can use PCFerret to view the contents of the ADS you just created. Remember, if you need help, press the F1 button within PCFerret.

Can I separate an ADS from the main file?

Yes. PCFerret gives you an option to do this. While on the *ADS Tab* in PCFerret, right click on the file with the ADS you wish to view and select the appropriate option from the resultant menu.

What is a Reboot Operation

Reboot Operations are events relating to folders and files which take place when your PC is rebooted, or switched-off and back on again.

These events fall in to the following categories:

Delete files / folders
Rename files / folders
Move files / folders

These operations are required to take place during the reboot phase as they are locked by a process (program) and the operation cannot be performed during normal PC operation. A typical example of this would be when a new program has been installed or an update to an existing program has been applied. Windows updates sometimes requires that a PC is rebooted after installation, and this one of the reasons why.

PCFerret will list these operations via the **Reboot Operations** tab so that you know what to expect the next time your PC is restarted.

PCFerret enables you to remove any suspect entries from the list of reboot operations (if any) it displays.

PCFerret also enables you to add your own entries. This is particularly useful if you are unable to perform folder or file operations while your PC is fully operational due to the folder(s) or file(s) being locked by a running process.

Index

.

.NET, 4

A

Accounts, 4
ADS, 9, 43, 48
ADS Example, 48
ADS Tab, 9, 32, 48
Alternate Data Stream, 9
An Introduction To PCFerret, 2
Analyze File, 38, 43, 45
Auto Copy, 30

B

bat, 43, 45
Browser, 4, 18
Browser Cache, 18
Browser Media Tab, 18

C

Cache, 18, 27
Cached URLs, 22, 27
Cached URLs Tab, 22
Calculate Hash, 32
Check For Updates, 46
Clean Uninstall, 41
cmd, 43, 45
com, 43, 45
Compression, 13
Computer Manufacturer, 3, 4
Computer Name, 4
Contact, 47
Contact Us, 47
Context Menu, 22
Control Panel, 41
Copy All To Clipboard, 30
Copy File's Path, 22
Copy URL, 22
Copy URL Host, 22
CPU, 4
Create An ADS, 48
Ctrl+F, 22

D

Delete ADS, 9, 48
Delete Alternate Data Stream, 9, 48
Delete Files, 50
Delete Folders, 50
Disk, 4, 13

DOC, 13
DOCX, 13

E

Encryption, 13
Event ID, 35
Event Viewer, 35
EventID.net, 35
exe, 43, 45
Executable, 13
External IP Address, 4

F

FAQ, 47
File, 13, 18, 42, 43, 45
File Analysis, 13, 22, 42, 43, 45
File Analysis Report, 42, 43, 45
File Content, 13, 27, 45
Files, 13, 18, 27, 45
FileSuffix.com, 13
Find, 22, 27
Find File, 13, 27
Find Files By Type, 27
Find Tor, 39
Full System Details Tab, 3, 4

G

Generate A Password, 30
Generate Hash, 32
Generate Hash Value, 32
Generate Password, 30
Green, 22, 27

H

Hard Disk, 4
Hash, 32
HD, 4, 13
Hidden, 13, 18

I

Image, 18
Images, 13, 18
Introduction, 2
IP Address, 3, 4

L

Level 1, 22, 27
Level 2, 22, 27
License, 41
List View, 18
Locked, 50

M

Manufacturer, 3, 4
MD5, 32
Media, 4
Memory, 3, 4
Motherboard, 3, 4
Move Files, 50
Move Folders, 50
msi, 43, 45
msp, 43, 45
mst, 43, 45

N

Network, 4

O

Office, 13
Operating System, 3, 4
Options, 27
Orange, 22, 27

P

Page File, 4
Password, 30
Password Generator, 30
PCFerret Explained, 2
PDF, 13
pif, 43, 45
Pornographic, 18
Pornography, 18
Process, 50
Program File, 13
Public IP Address, 4
Purple, 22, 27

Q

Quick System Details, 3, 4

R

Reboot, 6, 50
Reboot Operations Tab, 6, 50
Red, 22, 27
reg, 43, 45
Remove, 41
remove ADS, 48
Rename Files, 50
Rename Folders, 50
Renamed File, 13
Results, 22

S

Save, 22
Screen Saver, 4
Search, 13

Search For Tor, 39
Serial Number, 4
Service Pack, 3, 4
SHA1, 32
SHA256, 32
SHA384, 32
SHA512, 32
Show Image, 18
Storage, 4
Stream, 9
Support, 2, 47

T

Tech Support, 47
Technical Support, 47
tga, 43
Thumbnail, 18
Thumbnail View, 18
Tip, 35
Tor, 39
Tor Browser, 39
Tor Project, 39

U

uninstall, 41
Update, 46
Updates, 46
URL, 22
USB, 4
User Name, 4
Users, 4

V

vbs, 43, 45
vbscript, 43, 45
Video, 4, 18
Video Card, 4
Videos, 13
View ADS File Option, 43
View File, 22, 42
Visit Host, 22
Visit URL, 22

W

Warning, 27
Warning Levels, 22
Warning Messages, 27
What Is PCFerret, 2
Windows Error and Warning Event Viewer , 35
Windows Events, 35
Windows Media Player, 42, 43
WMP, 42, 43

Workgroup, 4
ws, 43, 45
wsf, 43, 45

Y

Yellow, 22, 27