

Win Forensic Analysis

Directory Analysis

Directory Analysis lists all of the programs within a directory as well as all sub-directories located within it. This also lists such properties such as the full file path, file extensions, whether or not a file is read only, file size, file attributes, time created, last time accessed, last write time (all three given in local, and GMT time formats), and the final field it gives is the MD5 hash of each of the files. This will also list hidden files not normally seen by looking in the directory.

File Hash Analysis

File Hash Analysis takes a single file or takes all of the files in a directory and all sub directories if so chosen, and reads the file(s) in byte by byte. It then generates the MD5, SHA1, and CRC32 hash of each file found. This will also list the full path as well as the modified time, created time, and the size of the file in bytes. This will also list hidden files not normally seen by looking in the directory.

IE Cookie Analysis

IE Cookie Analysis reads the index.dat associated with the cookie files. The information that is read out of the index.dat is the cookie file name, the record type (always URL in the case of cookies), the offset in hex to the location of the record in the index.dat, record size in bytes, number of hits, the site that created the cookie, the modified date and accessed date as embedded in the index.dat, the name of the user that it was found under, and the MD5 of the actual cookie file. The bottom portion of the screen shows the individual cookie contents from the cookie file that is selected at the top portion of the program. This information includes the cookie key, the cookie value, host that created the cookie file, whether or not the cookie came from a secure web site, expire date and modified date as embedded within the cookie. Options specific to this program is the ability to open the creating page in Internet Explorer, the ability to open the cookie file in either Notepad or Wordpad.

IE Favorite Analysis

IE Favorite Analysis goes through the favorites folder of Internet Explorer and parses out the internet shortcut files. The information gathered from these files includes the favorite title, URL, embedded create date and modified date, folder name (if file is located within a sub folder), full path, and icon file if one is associated with the shortcut. This can be useful due to the fact that a shortcut can be named anything and point to something else. This shortens the time needed to look through hundreds of shortcuts.

IE Index.dat Analysis

IE Index.dat Analysis goes through a specified index.dat file and using the hash tables pulls out the records stored there. The records are then parsed into their separate informational portions. These fields include the record URL, record size in bytes, offset to the record location, record date and server

date as embedded in the index.dat, the record type (includes LEAK, URL, REDR), file name (stored in temporary files), the name of the folder stored in, and the HTTP headers. Options specific to this program are the ability to right click on a record and open that particular page in Internet Explorer.

INFO2 Analysis

INFO2 Analysis goes through a selected INFO2 file and pulls out the records of the files currently stored in the recycle bin. The information collected from the INFO2 file includes the original file name, the index (order in which files were deleted), the date and time that the files were deleted, the drive number that the file was deleted from (this corresponds to the drive letter where A = 0, B =1, C=2 and so forth), and the size of the file that was deleted.

Link File Analysis

The Link File Analysis program goes through a selected link file, folder, or folder and subfolders and retrieves the pertinent information located within these files. The information that is gathered from these files includes the file name, GUID, the created date, last access date, last modified date, file size of the file that is at the other end of the shortcut, the state that the window will open in (ShowWnd), any hotkey assigned to the shortcut, the volume type that the linked to file resides on, the volume serial number, the full file path to the file linked to, the MAC address of the drive, and the NetBIOS name of the drive. This is especially useful if the original file is no longer accessible. The link file holds the information even if the original file is no longer accessible or even if the original file has been deleted. The structure of this file is one of the hardest to figure out, but the information located within is invaluable.

Mozilla Cookie Analysis

The Mozilla Cookie Analysis program takes the cookies.txt file and parses it out the records stored there. The information gathered from this file includes domain / host name, whether or not the record came from a domain or a host, path in the site that the cookie came from, whether or not the cookie came from a secure site, the cookies expire date, the cookie name, and the value of the cookie. The original file is a text file, however the expire date is not stored in standard date and time format. This program converts it from number of seconds since Jan 1, 1970 to standard format, and gives a column header to make understanding the fields easier.

Mozilla History Analysis

The Mozilla History Analysis program deciphers the Mozilla history.dat file. This file uses the Mork file structure; this involves using multiple tables and can be quite tricky to assemble into a format that is easily read. There is also not much in the form of documentation on this file structure. The information that is gathered from this file is the URL of the website, the referrer if there is one, the last visit date and first visit date, the visit count, the display name, the host name, if the site is hidden, and if the user typed the address into the URL Bar. Options specific to this program is the ability to right click and open the web site in Internet Explorer.

NK2 Analysis

The NK2 Analysis program goes through the NK2 file that is created by Microsoft Outlook and pulls out relevant information found within the file. This file is created by Outlook and stores the E-Mail addresses that a user has sent e-mail to. The records stored here are long, and the separators are hard to find. This program goes through and pulls out the display name, e-mail address, the auto complete value, the index (order in which the records were found), whether or not the e-mail was sent by SMTP or through an Exchange Server. If the e-mail was sent through an Exchange server this program attempts to retrieve the lingering Exchange information that is stored in the NK2 file. This information can be extremely useful if a user is suspected of e-mailing someone that they claim that they have never contacted before.

Windows Prefetch Analysis

The Windows Prefetch Analysis program can take a single prefetch file or directory full of prefetch files and obtain the pertinent information located within them. Prefetch files are created by Windows with the intention of speeding up the load time of commonly used programs. The information that is obtained from these files is the full file name, the file header (important because it changes from XP to Vista), created date, write date, last accessed date, embedded date, the number of times ran, the file path hash, and the MD5 hash of the file.

Safari Cookie Analysis

The Safari Cookie Analysis program pulls in and parses the cookies.pl file that is created by the Safari web browser. This file is stored using the XML file format. Safari Cookie Analysis uses the tags located in the cookies.pl file to pull out the information stored in the file. Information extracted includes domain information, the created date, the date the cookie expires, the cookie name, the cookie path, and the value stored in the cookie.

Safari History Analysis

The Safari History Analysis program pulls in and parses the history.pl file that is created by the Safari web browser. This file is stored using the XML file format. Safari History Analysis uses the tags located in the history.pl file to pull out the information stored in the file. Information extracted includes the website, the last visit date, the web site title, and the visit count.

Vista Recycle Bin Analysis

The Vista Recycle Bin Analysis program retrieves the information regarding files that have been deleted to the recycle bin in Windows Vista. This differs from the INFO2 in that Vista no longer contains an INFO2 file. Files that are sent to the recycle bin in Windows Vista are renamed using the \$I and \$R file scheme. The \$I is much like the INFO2 that was found in previous versions of Windows. The \$I contains the following information which is extracted by the Vista Recycle Bin Analysis program. The information extracted is the original file name, the deleted time and date of the file, the original file size, and the corresponding file name with the \$R precedent. The files are named \$I with random info following and will have a corresponding \$R file that is the actual file that was deleted.

General Options and Features

These are the general options and features that can be found in all of the above programs.

Reporting

Reporting is available in three formats. The first format is the creation of a CSV file. This format is used due to the ability of being able to open this file type in almost any program or OS. CSV files can easily be imported into databases, read by Excel or any other spreadsheet program, or viewed in something as simple as a text editor.

The second and third types of reports are HTML reports. These are used again because of the portability of HTML files. The difference between the two types of HTML reports is in the formatting. The vertical report creates a separate table for each of the records selected and place them vertically one above the next. The horizontal report creates one table with a single row for each of the exported records.

The reports can be done as all records or just the selected records.

Copy Records

The copy option takes the selected records and places them onto Windows Clipboard. This allows you to take the records and paste them in a readable format into any type of text editor.

Select All / Deselect All

Allows you to either select all current records or deselects all of the current records.

Show Gridlines

This option places gridlines into the display that make telling where the records and the fields separate a lot easier. This can be turned on or off and is turned off by default.

Choose Columns

This option allows you to choose which columns will be visible. By turning off a column it is hidden from view and will not be exported into the report when it is created. Columns can be added and removed at will at any time.

Autosize Columns

This option will auto reset the width of each of the columns to the longest member. This can also be done manually by double clicking the separator between the columns. If this is enabled in the menu, it will remain when clearing and opening new files.

Always On Top

This option will keep the window open over top of all other windows. This option can be enabled or disabled at any time.