NetAnalysis v1.50

Overview

Version 1.50 of NetAnalysis is a significant milestone on the development routemap for NetAnalysis. We have added new features to increase product stability and reliability as well as making significant improvements to increase the usefulness and functionality of the product. All of the extraction and analysis engines have been re-written from scratch to take into account this new research, and as a result, we are now extracting data which no other currently available tools can extract. We have added a whole host of new features to NetAnalysis v1.50 as well improvements to the user interface to make it easier to understand the evidence. Web page rebuilding and cache extraction has been completely re-written in addition to new enhanced forensic auditing.

Browser Support

A considerable amount of time has gone into researching the index data produced by all of the popular Internet browsers. Microsoft Vista has presented a new set of challenges for us all, and this has been echoed with the changes to Internet Explorer. The extraction engines for the existing browsers had to be re-written to take into account the changes delivered with new Operating Systems, but also because of research and development. NetAnalysis v1.50 now supports the following browsers.

> **Warning**
>
> The following table relates to NetAnalysis v1.50. Further support has been added for later releases. To review the current supported browser, please visit: Supported Browsers

Browser / Version	Information	History	Cache	Rebuild
Microsoft Internet Explorer v3	Client UrlCache MMF Ver 3.2	✓	✓	✓
Microsoft Internet Explorer v4	Client UrlCache MMF Ver 4.7	✓	✓	✓
Microsoft Internet Explorer v5 - 8	Client UrlCache MMF Ver 5.2	✓	✓	✓
Mozilla Firefox v1 - 2	Mork DB and Cache Map	✓	✓	✓
Mozilla Firefox v3	SQLite and Cache Map	✓	✓	✓
Flock v2	Mozilla based browser	✓	✓	✓
Orca v1	Orca Browser	✓	✓	✓
Avant v7 - 11	Avant Browser	✓	✓	✓
Netscape Communicator v4.0 - 4.08	Little and Big Endian Versions	✓	✓	✓
Netscape Communicator v4.5 - 4.8	Little and Big Endian Versions	✓	✓	✓
Netscape v6.0 - 6.2.3	Netscape Browser	✓	✓	✓
Netscape v7.0 - 7.2	Netscape Browser	✓	✓	✓
Netscape v8.0 - 8.1.3	Netscape Browser	✓	✓	✓
Netscape v9.0 - 9.0.0.6	Netscape Browser	✓	✓	✓
AOL Browser ARL File	AOL Browser	✓	✓	✓
Opera v9 - 10	Cache support in development	✓	✗	✗
Yahoo! BT Browser	Yahoo British Telecom Browser	✓	✓	✓
Apple Safari Windows v3 - 4	Cache support in development	✓	✗	✗
Apple Safari Mac OSX v1 - 4	Cache support in development	✓	✗	✗
Apple Safari XML PLIST	XML formatted PLIST	✓	N/A	N/A
Apple Safari Binary PLIST	Binary Formatted PLIST	✓	N/A	N/A
Mozilla / Firefox / Netscape Bookmark	XML Bookmark File	✓	N/A	N/A

Cache Extraction and Page Rebuilding

The cache extraction and rebuilding engine has also been re-written from scratch. The engine is now recursive and supports GZIP compressed data. When cached items are extracted or web pages rebuilt, the data is exported to an external export folder. The output paths are relative so the entire folder can be moved to external media and still be viewable. There is also an option to have cached items exported and grouped by extension for easy review.

During the page rebuild process, a new audit log file is created. This page details the content of the page and shows how it was rebuilt. It also contains hyperlinks to all of the page elements. Our HTML/File viewer QDV has also been completely re-written with a new HTML rendering engine and is more stable than before. Support for rebuilding pages and extracting cached items from Firefox v1-3 cache has been added.

Time Zone Support

Historically, one of the biggest confusion for users was time zones and date/time stamps. In this version, date/time stamp analysis has been improved considerably and the secondary date column has been replaced. NetAnalysis now takes DST into account rather than just applying an offset bias. It also allows the user to set the exact time zone the suspect system was set to, thereby accurately recreating the date/times. Figure 1 shows the Time Zone options page.

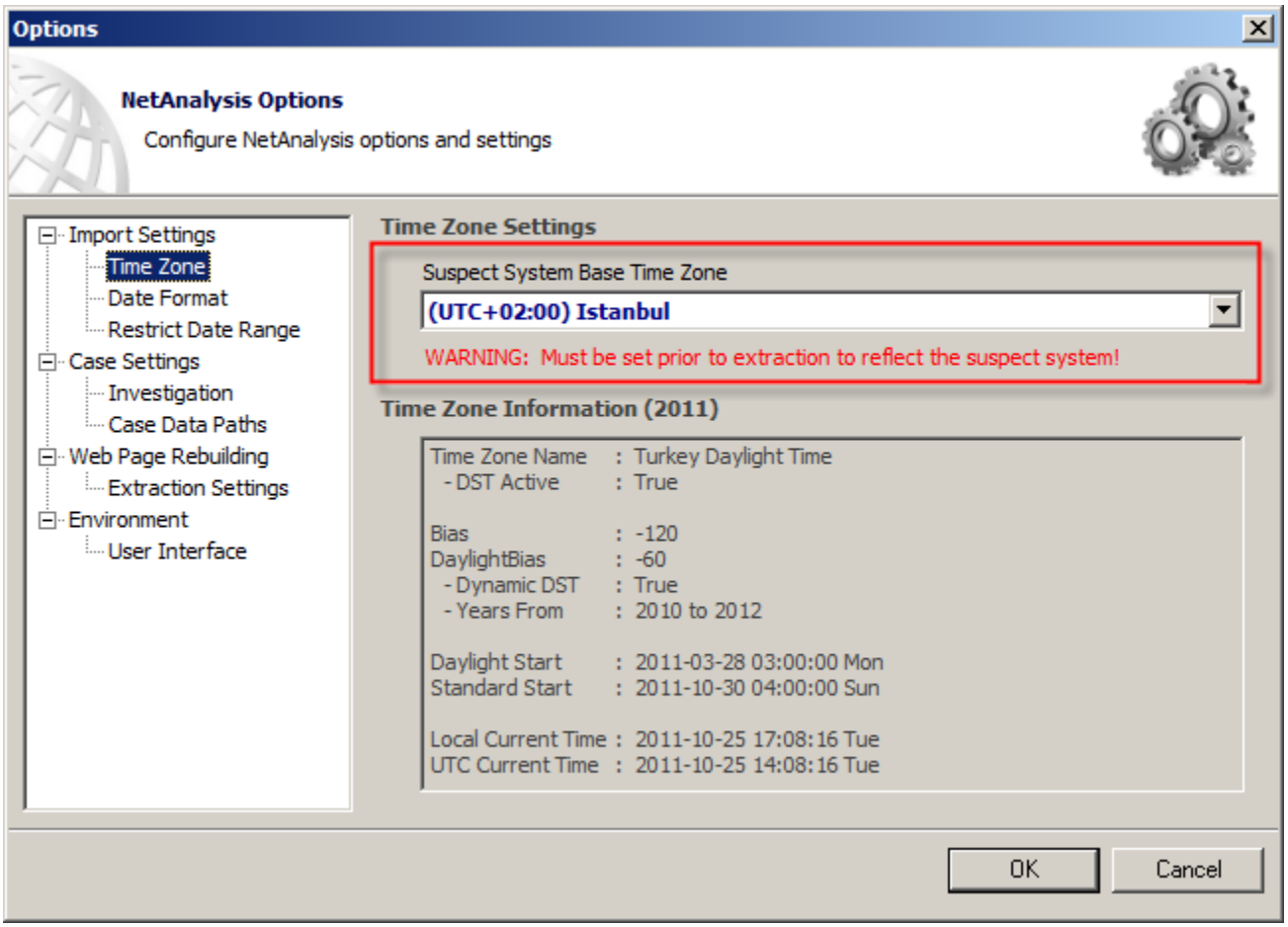

Figure 1

NetAnalysis will also flag and report any issues it identifies with Time Zones after the data has been imported. It will identify if the Time Zone settings are incorrectly set.

New Improved Workspace File

The NetAnalysis workspace database has been updated and improved. It now contains 40 new fields.

Internet Explorer Redirect and LEAK Entries

As a result of research and testing, NetAnalysis now has greater support for Redirect and LEAK entries. NetAnalysis is now able to provide date/times for some redirects as well as showing where the user was redirected to. The new Redirect URL column shows where the user was redirected to. LEAK support has been greatly improved with additional date/time reporting and flagging of partial overwrite status. A LEAK entry occurs when Internet Explorer has attempted to remove a cache or cookie file and was unable to do so at that time. It flags the entry as LEAK so that it can remove the item at a later date.

HstEx v3 Support

NetAnalysis v1.50 now supports HstEx v3 extraction files. HstEx can recover deleted browser data from a forensic image or disk. When Hstex v3 files are loaded into NetAnalysis, a new feature identifies the physical location of the internet history record on the original disk. If you right click on the status bar at this point, the physical sector offset can be copied to the clipboard. This allows the examiner to quickly navigate to that physical location in the forensic tool of choice.

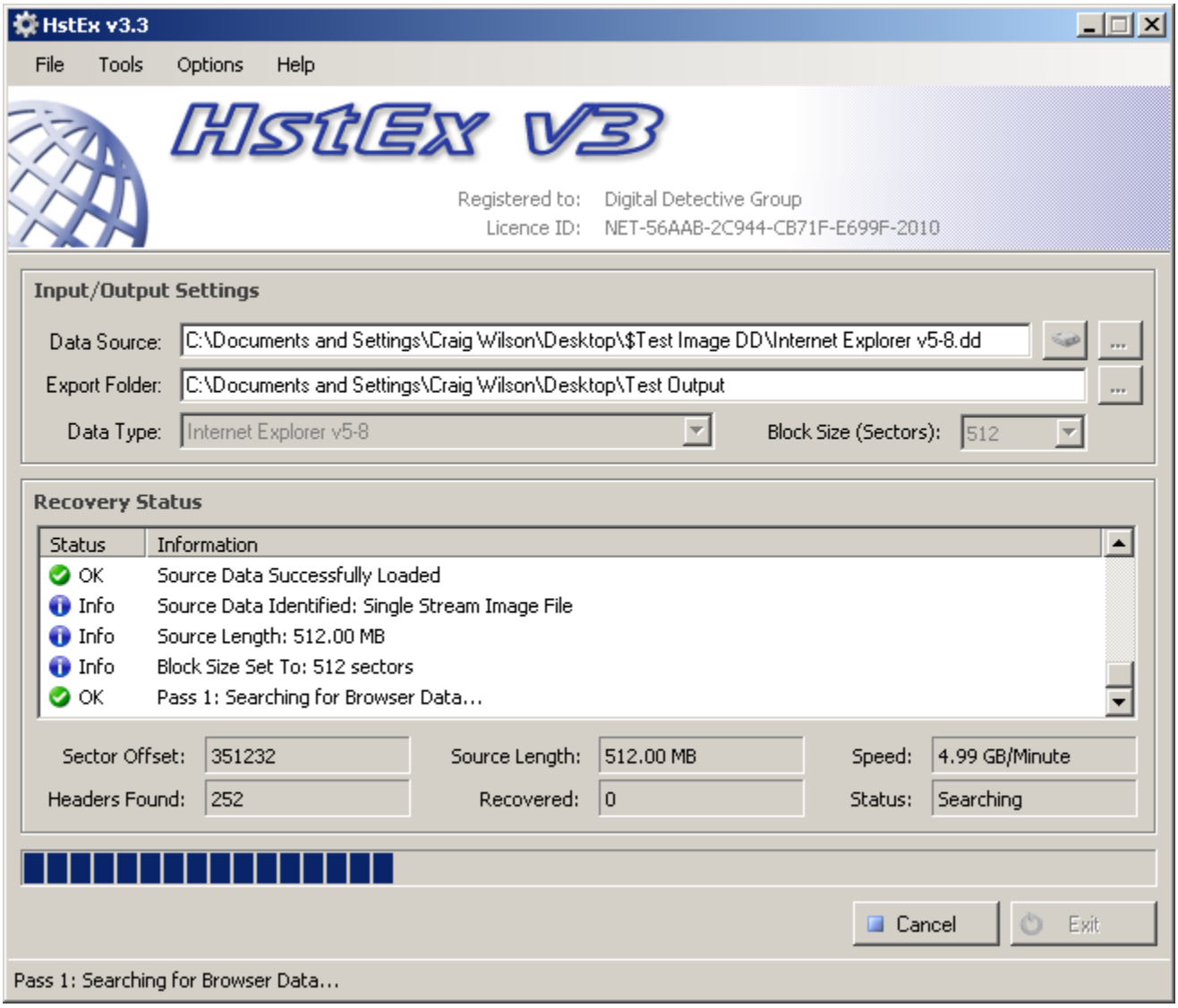

Figure 2

NetAnalysis also logs the metadata from the original EnCase or FTK image.

Improved Audit Logging

In previous versions of NetAnalysis, there was a system log which recorded some limited information. In the new version, this has been replaced by an audit log. The audit log will record far more information than previously to enhance disclosure under the United Kingdom's CPIA (Criminal Procedure and Investigations Act 1996).

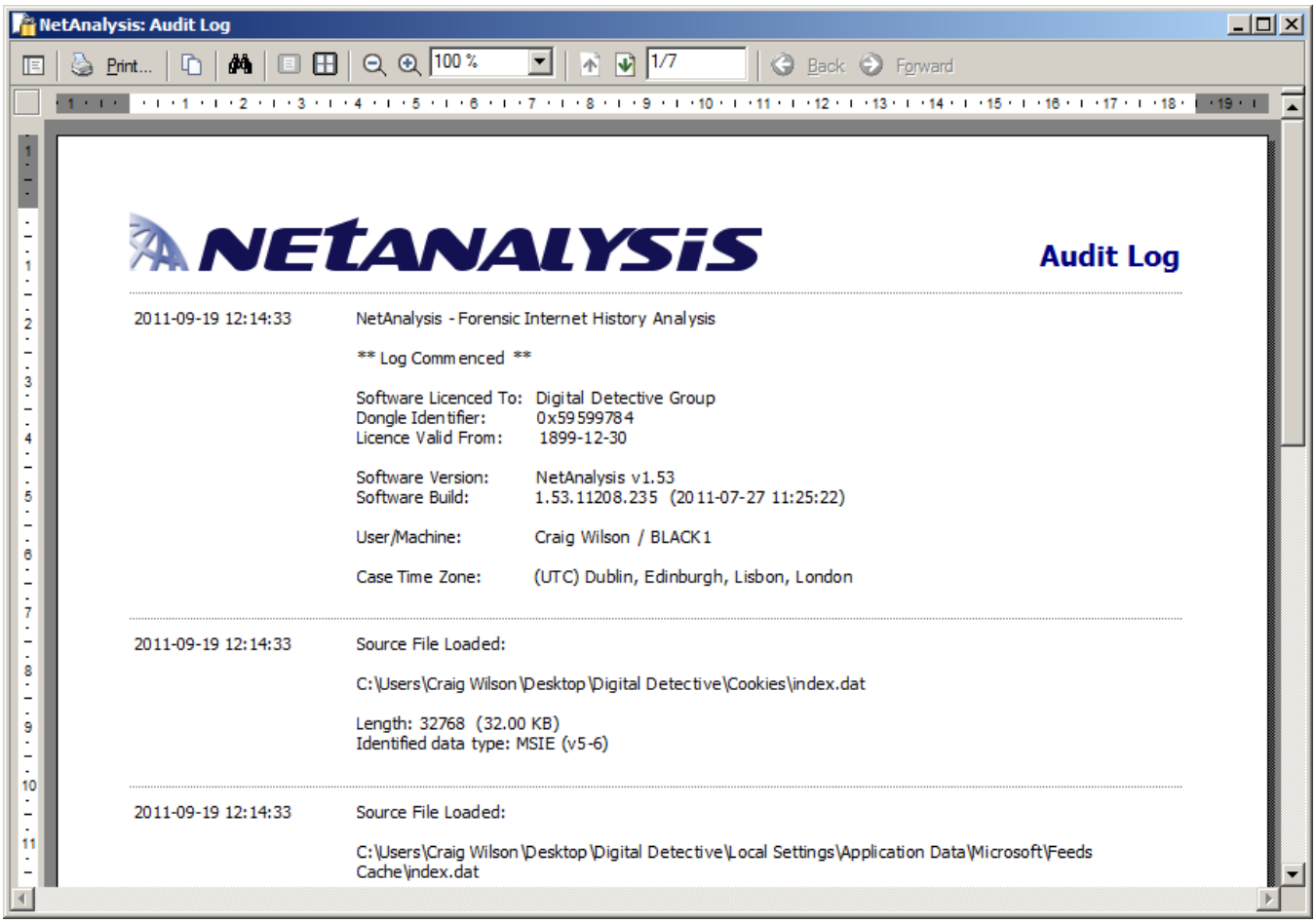

Figure 3

Improved Error Handling

A new and improved error handler has been added to the software. The error reports have comprehensive information regarding each issue which allows the developers to quickly identify the cause of a problem. Each session maintains its own error log. The logs can be sent to support if required. This will assist in making NetAnalysis a more robust product.

Error logging can be accessed from Help » Error Reporting. If numerous errors are reported (such as with very corrupt data), the user can disable error reporting for the rest of that session. NetAnalysis will continue to log the errors to the log file. Figure 4 shows the error reporting window:

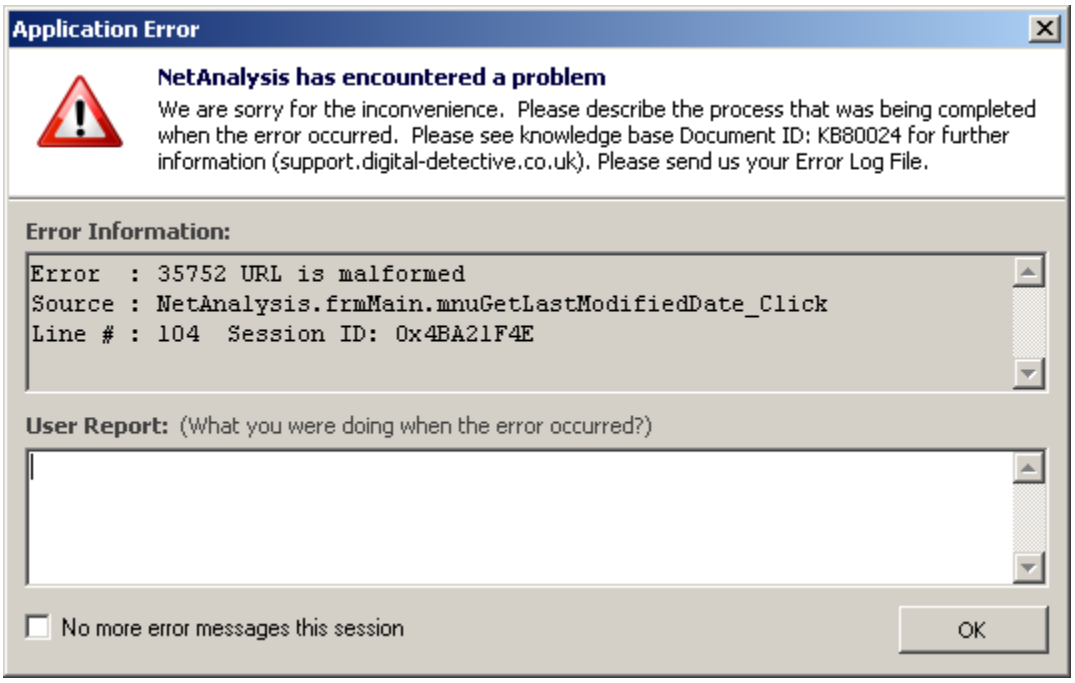

Figure 4

Improved Option Management

NetAnalysis Case and Properties have been merged into one location. All of the software and case properties can be accessed by selecting Tools » Options. NetAnalysis also remembers many of the options you set as you work. For example, the location of source data or export folders are remembered so they are automatically selected when you use the function again.

Improved Filtering, Keyword and SQL Queries

NetAnalysis v1.50 now has some new and improved features for record filtering, keyword management and SQL Query building. All of these functions have been re-written from scratch to improve their usability. The main searching/filtering form (accessed via the F8 function key) has been redesigned. The Filter Text field is now a drop-down field which remembers the last 15 filters that have been set. If you apply a filter and have the URL View window open, your filter keywords will be highlighted for easy review. The column sort order is now retained between searches as well as any date specific filtering.

You can now easily filter a specific field value by right clicking on the column/record and selecting 'Filter Records by Selected Field Data'. If you select a live cache entry, you can also select 'Open Containing Folder'. This will take you to the location of the exported cache item and highlight it in Explorer. SQL Queries can easily be saved and exported so they can be shared between users or archived for later use.

Change Log and Release History

To see the full software release history, see the following Article:

- Change Log v1.50