NetAnalysis v1.54

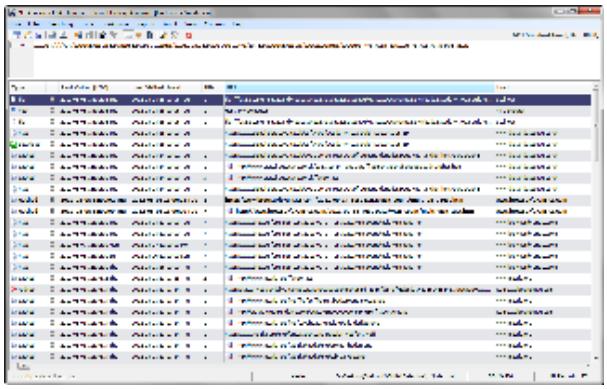
Introduction to NetAnalysis v1.54

Overview

In this release we have added a number of new features and improvements. Please see the Change Log for a full list of changes, which should assist with feature testing and validation. NetAnalysis v1.54 has been tested against all the current release versions of supported browsers. Please see the following list:

- Full Change Log for version 1.54
- List of supported browsers and versions
- Full Change Log for HstEx v3.8
- Release notes for HstEx v3.8

The corresponding version of HstEx for this release of NetAnalysis is HstEx v3.8. HstEx v3.8 uses an updated file format which can only be opened in NetAnalysis v1.54 and above.



Mozilla Firefox

Since the release of NetAnalysis v1.53, we have seen some significant changes in the world of browser forensics. Mozilla has committed to a more aggressive release schedule for the Firefox web browser. There were nearly three years between the launch of Firefox 3 and Firefox 4, however, versions 5 to 12 have been released within a matter of months. This has been a technical challenge from a support point of view as many artefacts have changed during these releases. We are pleased to report that NetAnalysis now supports all versions of Mozilla Firefox from version 1 through to the current release, Firefox version 12.

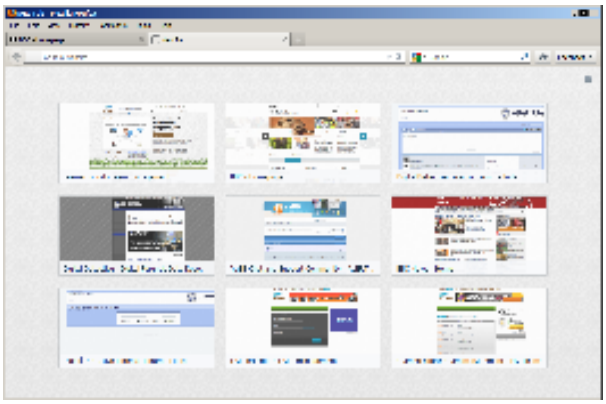
Firefox moz-page-thumbs

Firefox v13 will bring a slightly new look to some parts of the browser. Both the New Tab and the Home Page have been redesigned. The New Tab page now has links to your most recently and frequently visited sites which looks more or less just like Opera's Speed Dial, which Chrome also mimics. Some of this functionality has been added to Firefox v12 in anticipation of the release of Firefox v13. Whilst Firefox v12 does not show the new Speed Dial page when new tab is selected, the page thumbnails are still saved to the cache when a page is visited. The URL portion of the cache entry looks like this:

Firefox moz-page-thumb cache entry
`moz-page-thumb:http://www.browserforensics.com/2011-09-14-Test-Data/visit-count/multi-visit-test.htm`

We have added additional support to HstEx to recover these entries as part of the Firefox cache recovery. NetAnalysis v1.54 also supports these cache entries, with the added bonus of being able to extract the page-thumb file (which is usually stored in PNG format). Read more about Firefox Version 13.

These thumbnails can easily be exported and reviewed by the investigator. Using the new 'Export/Rebuild Current Filtered Cache Items' feature added to NetAnalysis v1.54, the thumbnail entries can be filtered and then the actual PNG thumbnail files can be exported from the cache. To filter the records, search for "moz-page-thumb" across the imported Firefox v12 records and then select Tools » Export/Rebuild Current Filtered Cache Items. The thumbnail files can then be examined from the "Extracted Files/PNG" folder.



Firefox moz_formhistory

We have added support to import data from the 'moz_formhistory' table. This contains artefacts relating to web form completion.

https	☐	2012-02-22 11:03:17 Wed	2012-02-22 15:03:17 Wed	1	https://mail.google.com/mail/?shva=1#drafts
https	☐	2012-02-22 11:03:11 Wed	2012-02-22 15:03:11 Wed	1	https://mail.google.com/mail/?shva=1#drafts/135a55f862d94e65
form-hist	☑	**2012-02-22 11:03:00 Wed**	**2012-02-22 15:03:00 Wed**	**1**	**subject : Some research I've done**
file	☐	2012-02-22 11:02:52 Wed	2012-02-22 15:02:52 Wed	1	file:///C:/Users/Alexei_Axe/Downloads/Research.zip

Figure 1 - Form History Completion (Example 1)

The screen shot in Figure 1 shows an example where the browser user opened a ZIP attachment whilst viewing Google Mail; they then created a draft email using the subject line "Some research I've done".

form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**newaccountcaptcha : chavoiava**
form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**Birthday :** [redacted]
form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**SecondaryEmail :** [redacted]
form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**ownquestion :** [redacted]
form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**LastName :** [redacted]
form-hist	☑	**2012-02-22 08:43:30 Wed**	**2012-02-22 12:43:30 Wed**	**1**	**FirstName :** [redacted]
cached	☐	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	id=4f44a7da&uri=https://accounts.google.com/CreateAccount?service=mail&continue=http%3A%2F%2Fmail.google.com%2Fmail%2Fe-11-...

Figure 2 - Form History Completion (Example 2)

The screen shot in Figure 2 shows the user creating a new Google Mail account. It also takes the user through the question and answer fields which are required to create a new account. Although the details in this image have been redacted, you can see the field names which have been completed as part of the process. These artefacts when viewed in context can provide some very interesting information.

Google Chrome

We have added significant extra functionality for Google Chrome artefacts. Chrome maintains a number of SQLite databases for data storage, and NetAnalysis v1.54 now extracts data from most of the significant databases.

History Index YYYY-MM c2body

We have added support for Google Chrome Page Content (c2body). Chrome's history system keeps a full text index for each page the user visits, making it easy to find pages based on their content, not just title and URL. The user's history is exposed through the History page, accessible via the Tools menu, or by pressing **Ctrl+H**. A user may also directly search their history by typing a search query in the address bar, and selecting the **See all pages in history containing [query]** item that appears if any results match the entered query.

When a user visits a page, the textual contents (those actually shown on screen) are stripped out and stored in the 'History Index YYYY-MM' database files (one file per month). NetAnalysis v1.54 allows the examiner to extract all of this information in one simple operation. The text files generated have been shown to contain potentially important information including Facebook and webmail data.

The text page content can be extracted by selecting Tools » Export Google Chrome c2body.

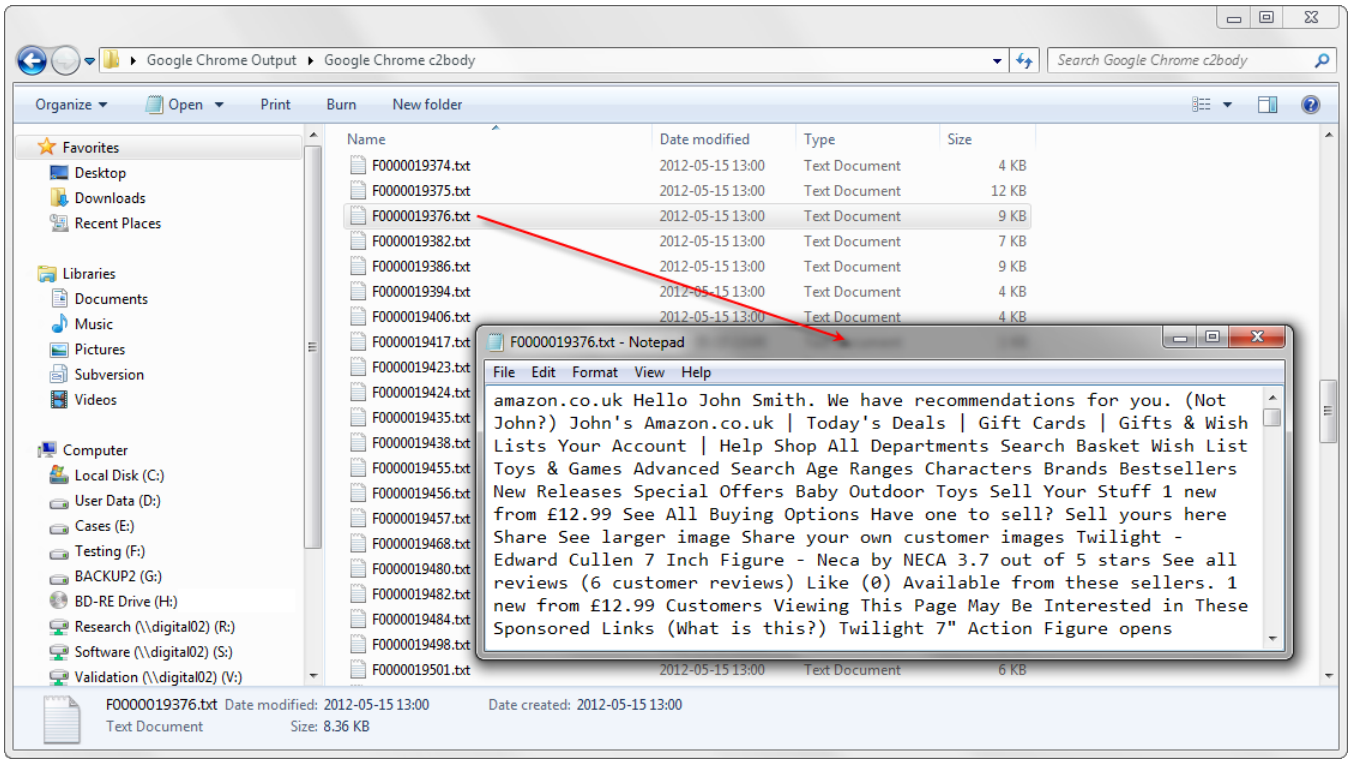


Figure 3 - Google Chrome c2body Extraction

Page Transitions

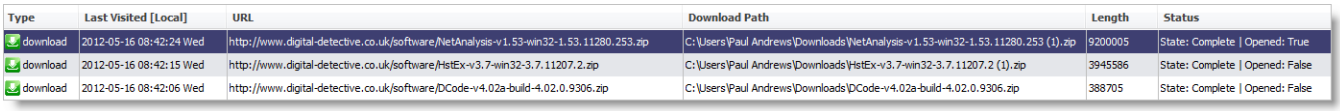
Google Chrome stores a transition value which identifies the type of transition between pages. These are stored in the history database to separate visits, and are reported by the renderer for page navigations. NetAnalysis now extracts and decodes the page transition value and displays the transitions in the 'Status' column. By examining the page transitions, it is possible to see how a user landed on a page. To understand the meaning of each transition, please see Page Transitions.

Source Offset	Index Type	Browser Version	Status
Index: 6246	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_END and SERVER_REDIRECT
Index: 6267	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_END and SERVER_REDIRECT
Index: 4472	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START
Index: 4476	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START
Index: 6396	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START and CHAIN_END
Index: 6398	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START and CHAIN_END
Index: 4470	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and SERVER_REDIRECT
Index: 4500	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_END and SERVER_REDIRECT
Index: 6392	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_END and SERVER_REDIRECT
Index: 4647	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_START and CHAIN_END
Index: 5529	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CLIENT_REDIRECT
Index: 6361	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CLIENT_REDIRECT
Index: 5917	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and FORWARD_BACK and CHAIN_START and CHAIN_END
Index: 74	History	Google Chrome v0-18 (History)	Page transition: LINK and CHAIN_START and CHAIN_END
Index: 5948	History	Google Chrome v0-18 (History)	Page transition: LINK and CLIENT_REDIRECT
Index: 6323	History	Google Chrome v0-18 (History)	Page transition: LINK and SERVER_REDIRECT
Index: 6226	History	Google Chrome v0-18 (History)	Page transition: MANUAL_SUBFRAME and CHAIN_START
Index: 6264	History	Google Chrome v0-18 (History)	Page transition: MANUAL_SUBFRAME and CHAIN_START and CHAIN_END
Index: 6340	History	Google Chrome v0-18 (History)	Page transition: START_PAGE and CHAIN_START

Figure 4 - Google Chrome Page Transitions

Downloads

We have also added support for Google Chrome download history.

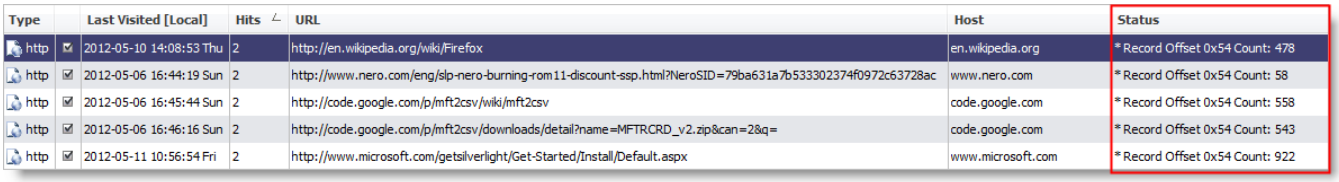


Type	Last Visited [Local]	URL	Download Path	Length	Status
download	2012-05-16 08:42:24 Wed	http://www.digital-detective.co.uk/software/NetAnalysis-v1.53-win32-1.53.11280.253.zip	C:\Users\Paul Andrews\Downloads\NetAnalysis-v1.53-win32-1.53.11280.253 (1).zip	9200005	State: Complete | Opened: True
download	2012-05-16 08:42:15 Wed	http://www.digital-detective.co.uk/software/HstEx-v3.7-win32-3.7.11207.2.zip	C:\Users\Paul Andrews\Downloads\HstEx-v3.7-win32-3.7.11207.2 (1).zip	3945586	State: Complete | Opened: False
download	2012-05-16 08:42:06 Wed	http://www.digital-detective.co.uk/software/DCode-v4.02a-build-4.02.0.9306.zip	C:\Users\Paul Andrews\Downloads\DCode-v4.02a-build-4.02.0.9306.zip	388705	State: Complete | Opened: False

Figure 5 - Downloads

Internet Explorer Visit Count

Recent testing has exposed an issue with the accuracy of Internet Explorer hit count values stored in the Master INDEX.DAT file. Normally, the hit count would be stored as a 32bit integer at record offset 0x54 (decimal 84). In many cases, comparing the record value to the hit count returned by Internet Explorer would show a mismatch. In these cases, Internet Explorer has an additional record object which stores an additional visit count. Testing has shown this additional count object to be accurate and is the value presented by the application. When the additional record object is present, NetAnalysis parses that block and displays that value in the Hits column. The original value stored at offset 0x54 is now displayed in the Status column as can be seen from the figure below.



Type		Last Visited [Local]	Hits	URL	Host	Status
http	☑	2012-05-10 14:08:53 Thu	2	http://en.wikipedia.org/wiki/Firefox	en.wikipedia.org	* Record Offset 0x54 Count: 478
http	☑	2012-05-06 16:44:19 Sun	2	http://www.nero.com/eng/slp-nero-burning-rom11-discount-ssp.html?NeroSID=79ba631a7b533302374f0972c63728ac	www.nero.com	* Record Offset 0x54 Count: 58
http	☑	2012-05-06 16:45:44 Sun	2	http://code.google.com/p/mft2csv/wiki/mft2csv	code.google.com	* Record Offset 0x54 Count: 558
http	☑	2012-05-06 16:46:16 Sun	2	http://code.google.com/p/mft2csv/downloads/detail?name=MFTRCRD_v2.zip&can=2&q=	code.google.com	* Record Offset 0x54 Count: 543
http	☑	2012-05-11 10:56:54 Fri	2	http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx	www.microsoft.com	* Record Offset 0x54 Count: 922

Figure 6 - Status column showing 'Hits count' from Record Offset 0x54

Updated Query Manager

This release has an updated Query Manager with additional features. It is now possible to sort the 'Database Field List' and 'SQL Query Operators' by clicking on the corresponding column header. The 'SQL Query Operators' now have a 'Description' entry which explains the function of the Operator. The Operators have also been re-written to show the full Operator with parameters and wild card characters. This should make it much easier to build and understand your SQL queries. The 'Check SQL Syntax' button has been added as a more convenient way to verify the syntax of a query. For further information, please see SQL Query Operators.

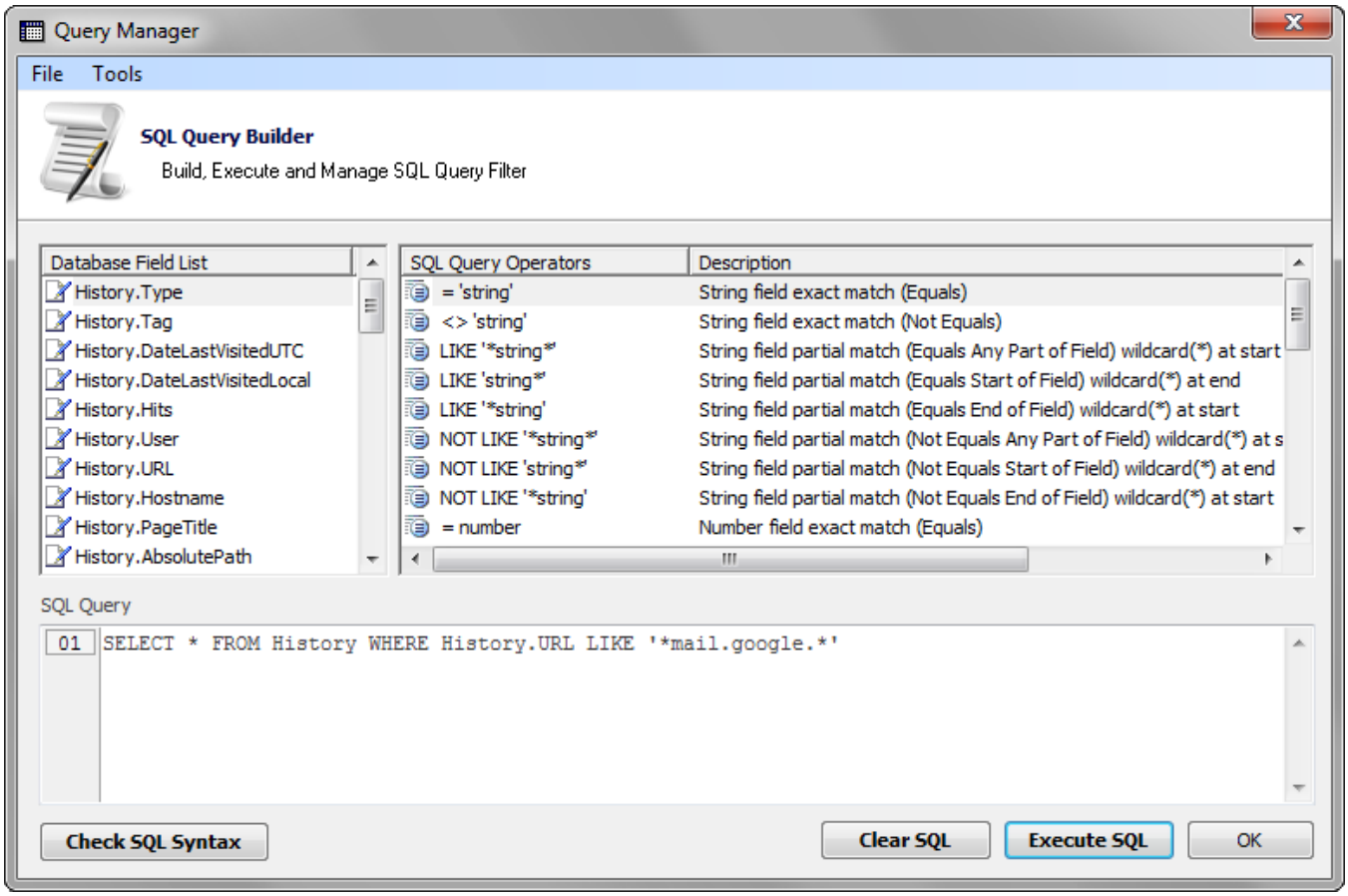


Figure 7 - Updated Query Manager

Rebuilding and Exporting Filtered Cached Pages (and Objects)

NetAnalysis has long had the capability to rebuild either single webpages, or the entire cache in one operation. NetAnalysis v1.54 now allows the forensic examiner to rebuild part of the cache. Using the various filtering techniques available, the forensic examiner can generate a targeted subset of the browser data, and then rebuild only the live webpages (or export cached objects) contained within that subset.

For example, if you wanted to export only the moz-page-thumb files, search for "moz-page-thumb" across the imported Firefox v12 records and then select Tools » Export/Rebuild Current Filtered Cache Items. The thumbnail files can then be examined from the "Extracted Files/PNG" folder.

Add Bookmark to Multiple Records

The bookmarking feature in NetAnalysis v1.54 has been enhanced to allow the forensic examiner to bookmark many records with the same bookmark text. The forensic examiner can create a filtered list of specific records, and then apply the same bookmark text to all of these records in one operation. The bookmark column can also be used for filtering, so this functionality is a powerful addition to the armoury.

Web Page Rebuilding

We have enhanced the web page rebuilding engine to make it more robust and provide better results. We have also released v4 of QDV™, our internal web page viewing software. This new version suppresses script errors in web pages, so the forensic investigator will no longer need to cancel multiple error messages when reviewing some rebuilt web pages.