

New Artefacts in v2.5

Introduction

This release of NetAnalysis® brings support for some new browsers and new artefacts as well as adding support for the modified cache format in Mozilla Firefox. We have also added support for the new versions of the Microsoft Edge download object.

New Browser Support

We have added support for the following browsers:

360 Security Browser

360 Secure/Security Browser (360) is a web browser developed by the Qihu company of Beijing, China. It offers page layout using either the Trident engine, as used in Internet Explorer, or the WebKit engine that was adapted for Google Chrome. It was first released in September 2008.

We have added support for the import of bookmarks which are stored in a format specific to 360 Security Browser. NetAnalysis also now supports history and downloads from the earlier versions (v3-5) as well as all the standard artefacts from v6+. We also support the import of the UnClosed Pages SQLite database which contains information on pages saved by the user when the Browser was shut down.

360 Speed (Extreme) Browser

360 Speed (or 360 Extreme) Browser (360) is another freeware Chromium-based browser by the Qihu 360 Software Company. It offers a cloud synchronisation account and claims protection against phishing.

NetAnalysis now supports the import of all the standard artefacts from 360 Speed Browser including the cross-domain Cookies found in v7.

UC Browser

UC Browser is a mobile browser developed by Chinese mobile Internet company UCWeb. Originally launched in April 2004 as a J2ME-only application, it is available on platforms including Android, iOS, Windows Phone, Symbian, Java ME, and BlackBerry.

With a huge user base in China, India, Indonesia, Pakistan and continued growth in emerging regional markets, UC Browser reached 100 million global users in March 2014. According to StatCounter, UC browser is the second most used smartphone/mobile web browser worldwide, passing Apple Safari in October 2015.

We have added support for the import of all the standard artefacts from UC Browser. NetAnalysis will also import URL shortcuts from the UC Browser Omnibox SQLite database.

Updated Support for New Versions of Existing Browsers

Some of the mainstream browsers have made modifications to their file formats to add new features. NetAnalysis® has been updated to support these new file formats. We have also added support for the following files and databases:

Microsoft Edge v25 - 38 (EdgeHTML v14) Downloads

Microsoft has released new iterations of the download object stored in the iedownload container. We now support these latest versions.

Apple Safari v10

The latest version of Safari updated the Downloads.plist and the History.db database schema. NetAnalysis® v2.5 has been updated to support Apple Safari v10 history and downloads.

Additional Support for Existing Browsers

We have also added support for the following artefacts:

Mozilla Firefox Backup Bookmarks

Mozilla Firefox and many Mozilla Based Browsers backup their bookmark data to JSON format and more recently LZ4 compressed JSON format files. We have added support for the import of these file types into NetAnalysis®.

Opera Session Database

Opera v15-29 stored its tab and session data in a session.db SQLite database. We have now added support to NetAnalysis® for the import of this database.

Mozilla Firefox Cache

In the recent versions of Mozilla Firefox, the cache version 2 format has been updated. We have added support to NetAnalysis® (and HstEx®) for this new structure.

Google Chrome Segment Usage

Google Chrome and many Chromium-based browsers store URL segment and segment usage information in the History SQLite database. The segment usage information contains details on the number of visits per day to a particular segment. A segment is a generic and simplified version of a URL which means similar URLs may be grouped together as a single segment. This usage information allows the browser to calculate the highest ranked segments which can then be used for the most visited view. We have now added support for the import of these tables to NetAnalysis®.

Chromium Form History and Login Data Recovered from HstEx®

We have added a number of new artefacts in HstEx® v4.5. With Chromium-based browsers, you can now recover individual entries from the "logins" table located in the Login Data SQLite database. You can also recover individual entries from the "autofill" table located in the Web Data SQLite database. All of these artefacts can be recovered and loaded into NetAnalysis® for review and analysis.

Torch Browser Accelerated Downloads Recovered from HstEx®

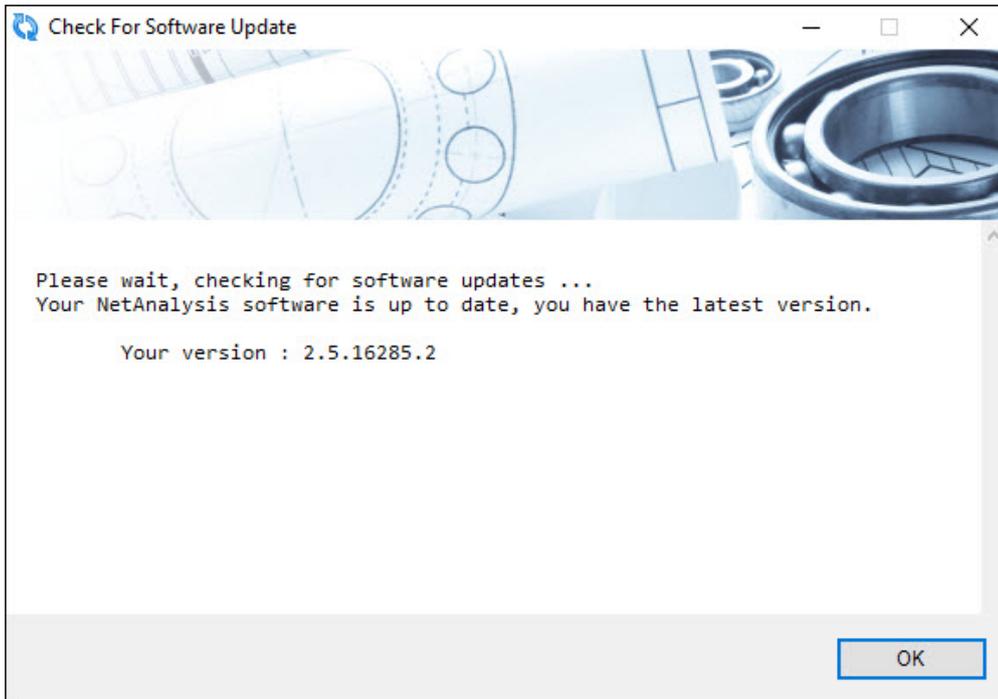
Torch browser stores its downloads in the History SQLite database in a table called "accelerated_downloads". We have added the ability to recover these entries in HstEx® v4.5 and import them into NetAnalysis® for review.

New Features

We have added some new features to NetAnalysis® to make the software easier to use and to assist with productivity. We have also added some new analytical tools which can be used to drill down into the various artefacts of stored URL data and cookie values.

Check for Software Update

In previous versions of NetAnalysis®, we had a feature to allow the user to check whether a new version of the software was available for download. We have had numerous requests to add this feature back, so from this release, you can check for new versions and get direct access to the latest download. This feature can be accessed from the Help menu by selecting Help » Check for software update.



New Decoding/Analysis Options

To enhance the data analysis capabilities built-in to NetAnalysis®, we have added some new timestamp decoding support. In the data examination/analysis window, the user can now select Mac Absolute, HFS+ (Mac OS) and OLE Automation timestamps.