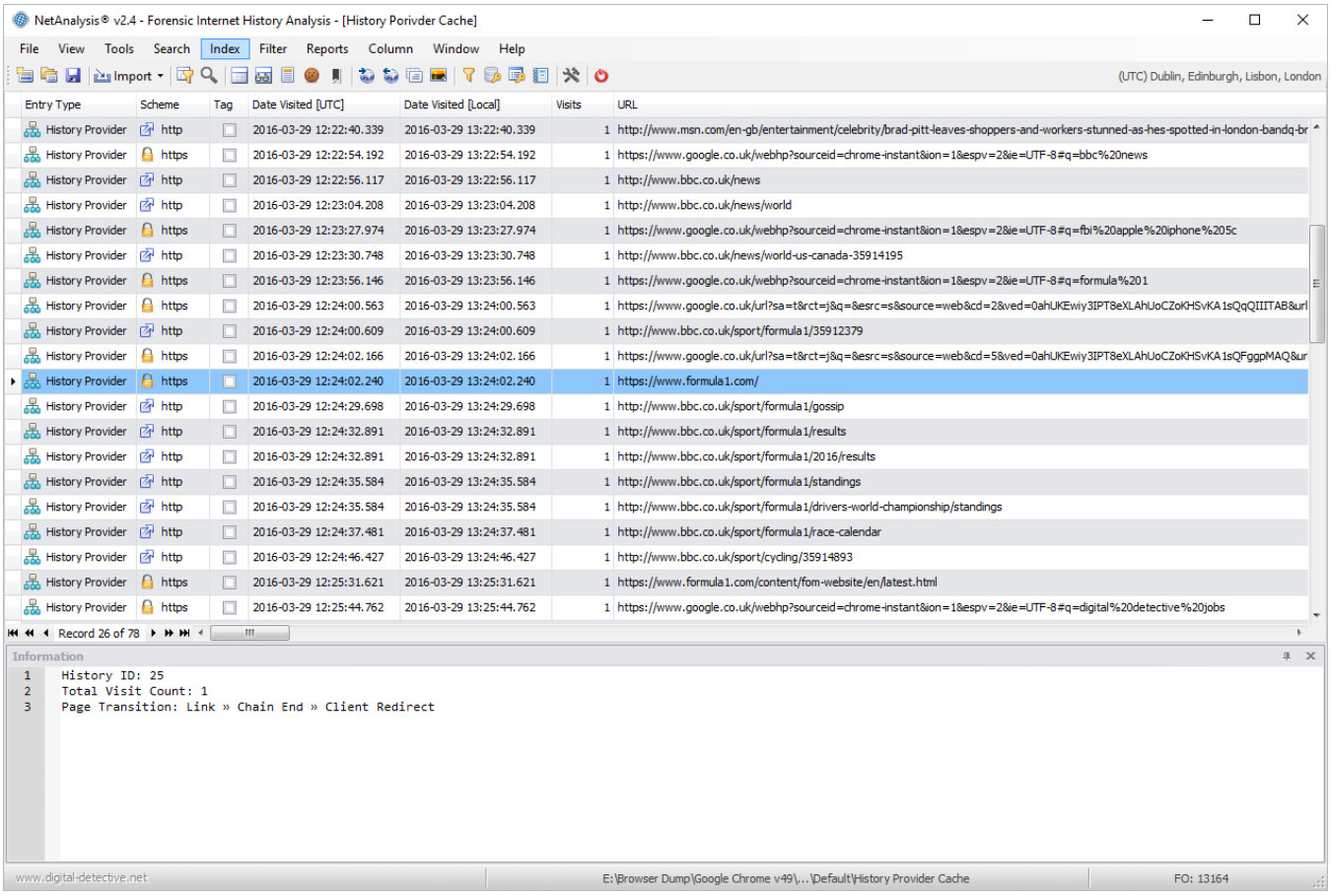
NetAnalysis v2.4

Introduction

This release brings support for Google Chrome's History Provider Cache and Network Action Predictors, Microsoft's Internet Explorer and Edge Typed URLs and Bookmarking across the various supported Browsers.

History Provider Cache

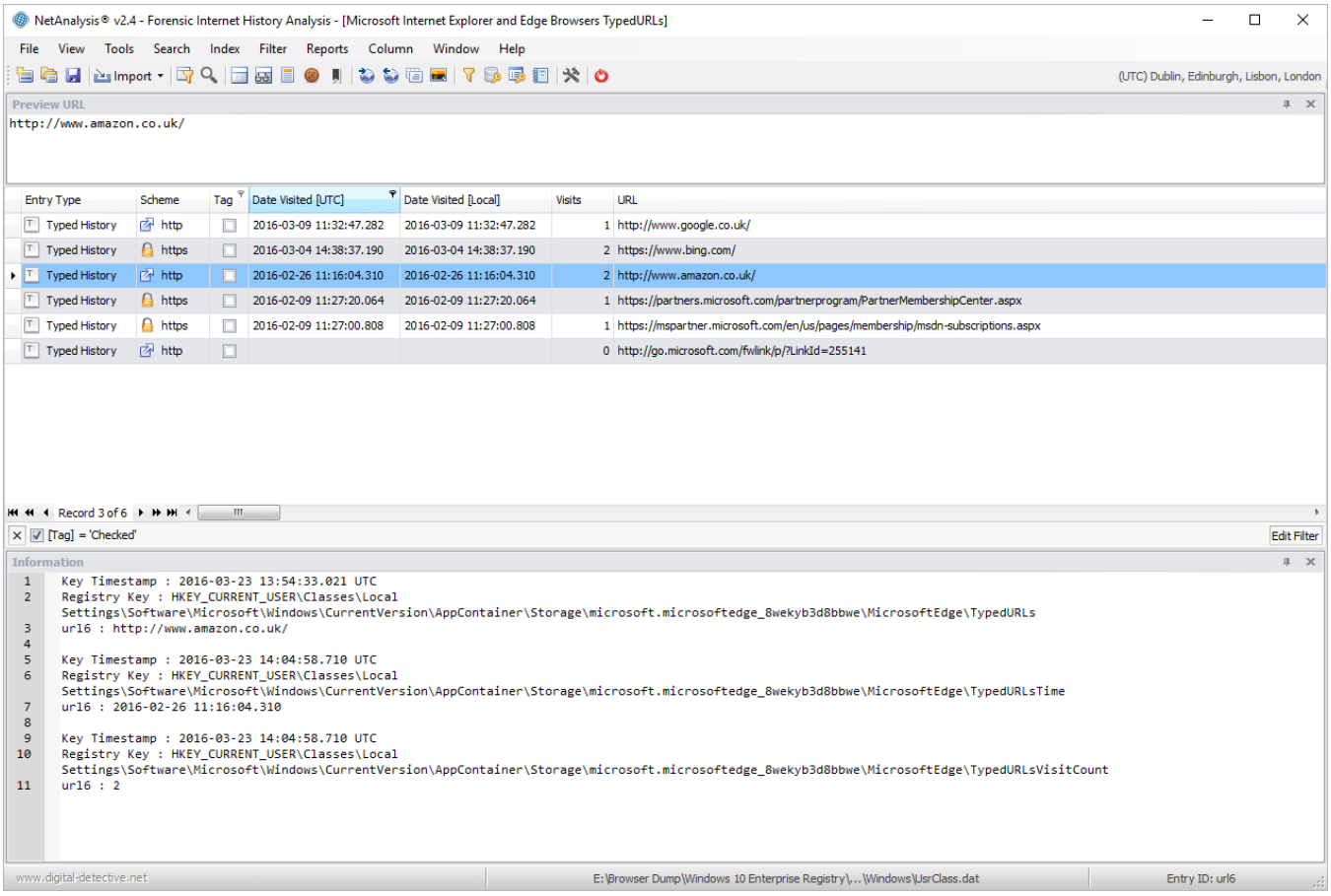
The History Provider Cache is a binary file which contains the data used by Google's HistoryQuickProvider (HQP). The HQP serves up autocomplete candidates from the profile's history database. As the user starts typing into the omnibox, the HQP performs a search in its index of significant historical visits for the term or terms which have been typed. The resulting candidates are scored and a limited number of only the most relevant matching URLs visited are presented to the user.



The image above shows the History Provider entries from a Google Chrome History Provider Cache file loaded into NetAnalysis. The History Provider Cache contains `WordListItem` and `WordMapItem` objects. These objects store the list of words used to search against. When the file is processed, they are written out to an external text file (located in the Export Folder) and are included in the list of files added to the search index.

Microsoft Internet Explorer and Edge Typed URLs

Microsoft Internet Explorer and Edge browsers also have a similar feature to Google Chrome's History Quick Provider. As entries are typed into and/or selected from the Address Bar, the browser saves the entry to a location in the Registry under the sub-key `TypedURLs`. Over different Operating Systems and browsers, the number of entries stored has varied. In later releases, Microsoft has also added corresponding `TypedURLsTime` and `TypedURLsVisitCount` sub-keys. In NetAnalysis v2.4, we have added support for reading registry hive files and can extract the typed URL information. We can also read the corresponding time and visit count information. The information panel in the screen shot below shows the corresponding registry sub-keys for the data.



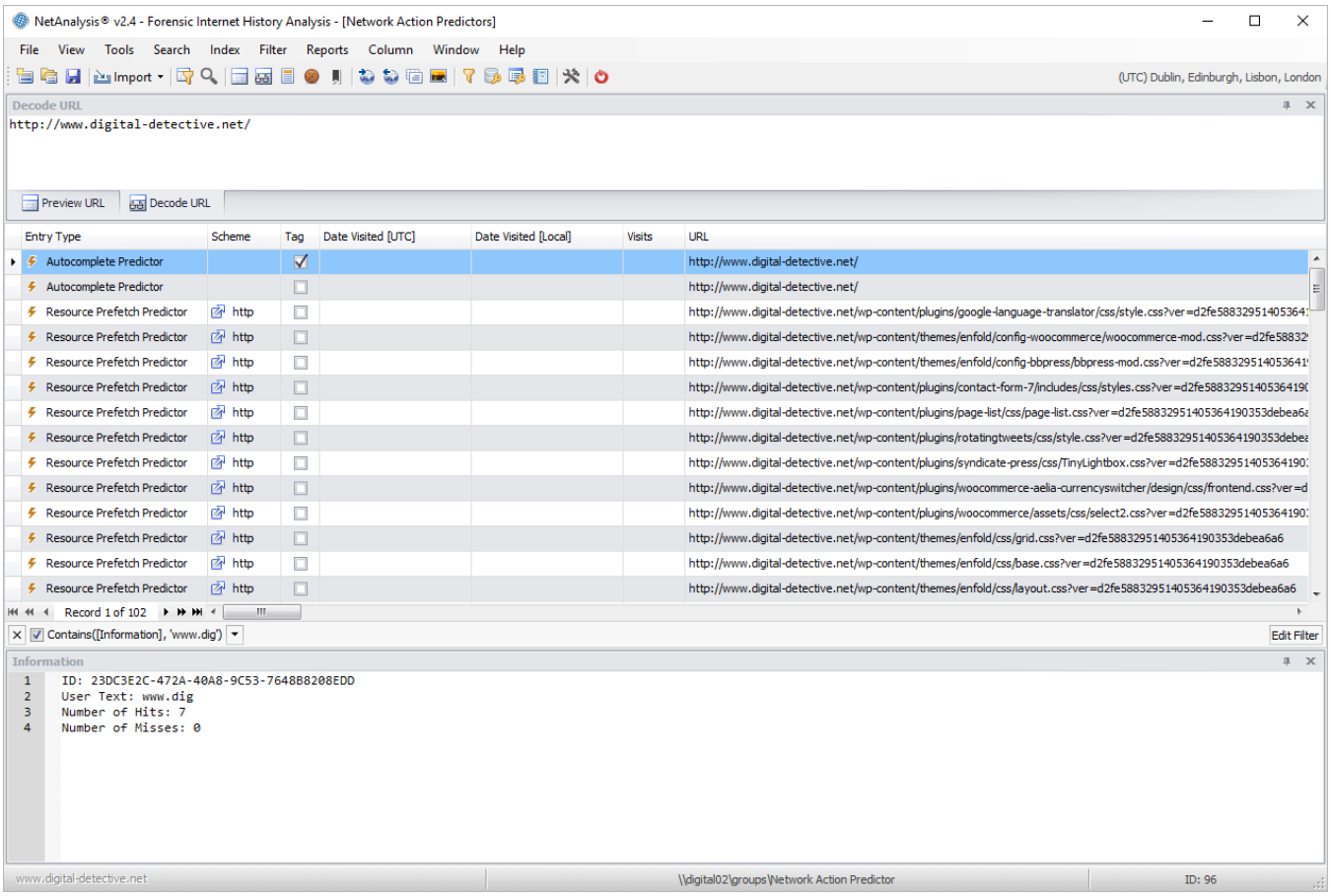
Network Action Predictor

We have added support for the import of Network Action Predictor data for Google Chrome and Chromium Based Browsers. This data can be either autocomplete predictor, resource prefetch predictor or logged in predictor entries.

If the autocomplete prediction feature is enabled, Chrome will use a prediction service to help complete searches and URLs typed into the omnibox. If the Chrome prerendering feature is enabled, the Browser will attempt to speed up navigation for a user by prerendering pages that it predicts the user is likely to navigate to.

The stored prediction data can be viewed live in the Browser by typing: `chrome://predictors` in the Chrome omnibox. Chrome will display tabs for both the Autocomplete Action Predictor and the Resource Prefetch Predictor entries. The Logged In Predictor entries were made obsolete as of Chrome v44.

The Autocomplete Action Predictor entries show a history of the characters the user typed into the omnibox and the URL that was then selected.
The Resource Prefetch Predictor entries list the resources that were predicted to be needed for a given URL. The Browser determines which resources to fetch based on prior browsing history.



In the screen capture above, the user text entered by the user is shown in the information panel against the associated Autocomplete Predictor entry.

Bookmarks

We have added support for the import of bookmark data as well as extraction of associated Bookmark images to the export folder for the following browsers:

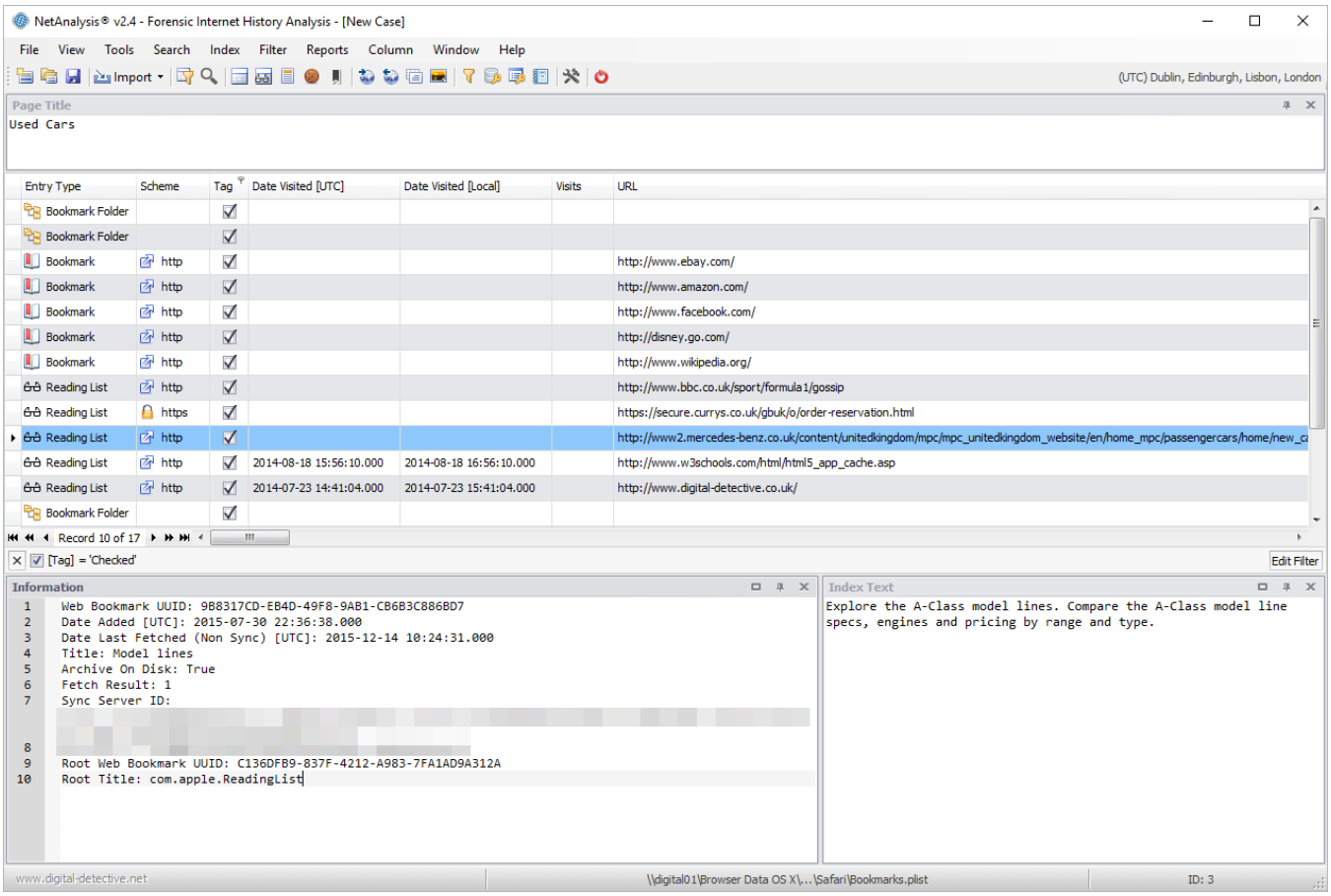
- Mozilla Firefox and Mozilla Based Browsers
- Google Chrome and Chromium Based Browsers
- Apple Safari (including Reading List)
- Opera Presto v3-12
- Opera Presto v7-12 Notes
- Opera v15-16
- Opera v25+
- Netscape HTML Bookmarks

Apple Safari bookmarks are stored in the `Bookmarks.plist` file. On Mac OS X, Safari also stores the user Reading List entries in this file whereas under Windows, these were stored in a separate `ReadingList.plist` file. When Reading List entries are extracted, any preview text is copied to the export folder. We support importing data from both `Bookmarks.plist` and `ReadingList.plist` files.

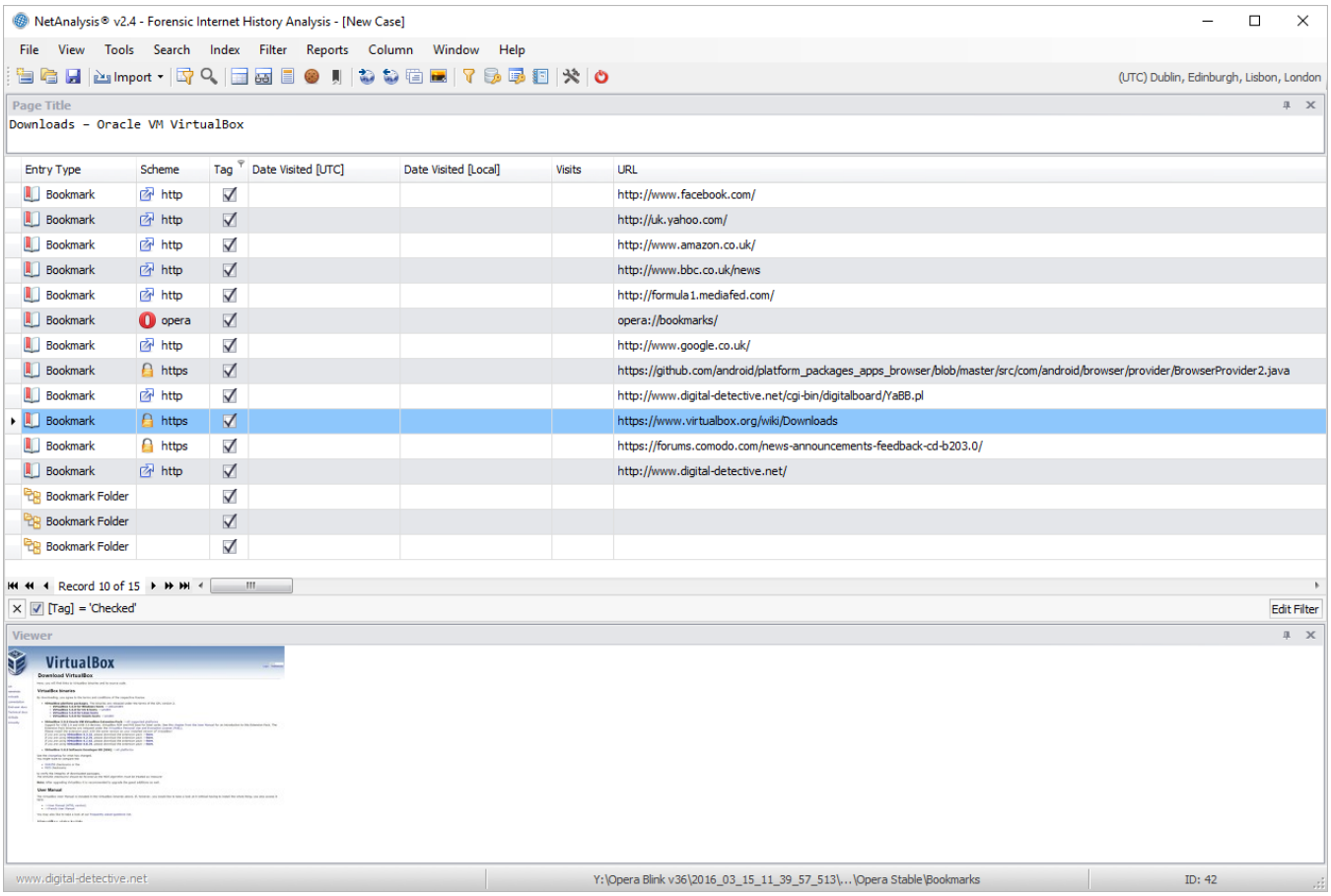
Opera Presto stored its bookmarks in a Hotlist format file. This format was also used to store Opera notes. NetAnalysis can now extract bookmarks for Opera v3-12 and notes for Opera v7-12.

Opera v15-16 stored its bookmarks in a `bookmarks.db` database. Opera v17+ then reverted to using the Chromium based file format. Opera added their own extra structure on top of the Chromium format from Opera v25+. NetAnalysis now supports all of these format variations. Any bookmark web page preview image files are also extracted to the export folder. These previews can be displayed using the Viewer panel.

The Netscape HTML file format is still widely used as a data exchange format by the current Browsers. The latest versions of Chrome, Firefox and Safari allow the user to import and export bookmarks in this format; while Opera allows the user to import Netscape HTML format bookmarks. Any Netscape HTML file format bookmark favicons are therefore copied to the export folder under folder name "Unidentified Browser".



The screen capture above shows bookmark and reading list data from Apple Safari v9. The screen capture below shows bookmark data from Opera v36.



Change Log

To review the full list of changes for this release, please see: Change Log v2.4.