

# NetAnalysis v2.4



- [Introduction](#)
- [History Provider Cache](#)
- [Microsoft Internet Explorer and Edge Typed URLs](#)
- [Network Action Predictor](#)
- [Bookmarks](#)
- [Change Log](#)



## 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.

NetAnalysis® v2.4 - Forensic Internet History Analysis - [History Provider Cache]						
File View Tools Search Index Filter Reports Column Window Help						
(UTC) Dublin, Edinburgh, Lisbon, London						
Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
History Provider	http		2016-03-29 12:22:40.339	2016-03-29 13:22:40.339	1	http://www.msn.com/en-gb/entertainment/celebrity/brad-pitt-leaves-shoppers-and-workers-stunned-as-hes-spotted-in-london-band-q-br
History Provider	https		2016-03-29 12:22:54.192	2016-03-29 13:22:54.192	1	https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&esprv=2&ie=UTF-8#q=bbc%20news
History Provider	http		2016-03-29 12:22:56.117	2016-03-29 13:22:56.117	1	http://www.bbc.co.uk/news
History Provider	http		2016-03-29 12:23:04.208	2016-03-29 13:23:04.208	1	http://www.bbc.co.uk/news/world
History Provider	https		2016-03-29 12:23:27.974	2016-03-29 13:23:27.974	1	https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&esprv=2&ie=UTF-8#q=fbi%20apple%20phone%205c
History Provider	http		2016-03-29 12:23:30.748	2016-03-29 13:23:30.748	1	http://www.bbc.co.uk/news/world-us-canada-35914195
History Provider	https		2016-03-29 12:23:56.146	2016-03-29 13:23:56.146	1	https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&esprv=2&ie=UTF-8#q=formula%201
History Provider	https		2016-03-29 12:24:00.563	2016-03-29 13:24:00.563	1	https://www.google.co.uk/url?sa=t&ct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiy3IPT8eXLAHJocZokHSvKA1sQqQIIITAB&url
History Provider	http		2016-03-29 12:24:00.609	2016-03-29 13:24:00.609	1	http://www.bbc.co.uk/sport/formula1/35912379
History Provider	https		2016-03-29 12:24:02.166	2016-03-29 13:24:02.166	1	https://www.google.co.uk/url?sa=t&ct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwiy3IPT8eXLAHJocZokHSvKA1sQqQIIITAB&url
History Provider	https		2016-03-29 12:24:02.240	2016-03-29 13:24:02.240	1	https://www.formula1.com/
History Provider	http		2016-03-29 12:24:29.698	2016-03-29 13:24:29.698	1	http://www.bbc.co.uk/sport/formula1/gossip
History Provider	http		2016-03-29 12:24:32.891	2016-03-29 13:24:32.891	1	http://www.bbc.co.uk/sport/formula1/results
History Provider	http		2016-03-29 12:24:32.891	2016-03-29 13:24:32.891	1	http://www.bbc.co.uk/sport/formula1/2016/results
History Provider	http		2016-03-29 12:24:35.584	2016-03-29 13:24:35.584	1	http://www.bbc.co.uk/sport/formula1/standings
History Provider	http		2016-03-29 12:24:35.584	2016-03-29 13:24:35.584	1	http://www.bbc.co.uk/sport/formula1/drivers-world-championship/standings
History Provider	http		2016-03-29 12:24:37.481	2016-03-29 13:24:37.481	1	http://www.bbc.co.uk/sport/formula1/race-calendar
History Provider	http		2016-03-29 12:24:46.427	2016-03-29 13:24:46.427	1	http://www.bbc.co.uk/sport/cycling/35914893
History Provider	https		2016-03-29 12:25:31.621	2016-03-29 13:25:31.621	1	https://www.formula1.com/content/fom-website/en/latest.html
History Provider	https		2016-03-29 12:25:44.762	2016-03-29 13:25:44.762	1	https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&esprv=2&ie=UTF-8#q=digital%20detective%20jobs
Record 26 of 78						
Information						
1	History ID: 25					
2	Total Visit Count: 1					
3	Page Transition: Link » Chain End » Client Redirect					
www.digital-detective.net			E:\Browser Dump\Google Chrome v49\...\Default\History Provider Cache			FO: 13164

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.

NetAnalysis® v2.4 - Forensic Internet History Analysis - [Microsoft Internet Explorer and Edge Browsers TypedURLs]

FileViewToolsSearchIndexFilterReportsColumnWindowHelp

(UTC) Dublin, Edinburgh, Lisbon, London

Preview URL

http://www.amazon.co.uk/

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Typed History	http		2016-03-09 11:32:47.282	2016-03-09 11:32:47.282	1	http://www.google.co.uk/
Typed History	https		2016-03-04 14:38:37.190	2016-03-04 14:38:37.190	2	https://www.bing.com/
Typed History	http		2016-02-26 11:16:04.310	2016-02-26 11:16:04.310	2	http://www.amazon.co.uk/
Typed History	https		2016-02-09 11:27:20.064	2016-02-09 11:27:20.064	1	https://partners.microsoft.com/partnerprogram/PartnerMembershipCenter.aspx
Typed History	https		2016-02-09 11:27:00.808	2016-02-09 11:27:00.808	1	https://mspartner.microsoft.com/en/us/pages/membership/msdn-subscriptions.aspx
Typed History	http				0	http://go.microsoft.com/fwlink/p/?LinkId=255141

Record 3 of 6

[X] [Tag] = 'Checked'

Edit Filter

Information

1Key Timestamp : 2016-03-23 13:54:33.021 UTC

2Registry Key : HKEY\_CURRENT\_USER\Classes\Local

3Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge\_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs

4ur16 : http://www.amazon.co.uk/

5Key Timestamp : 2016-03-23 14:04:58.710 UTC

6Registry Key : HKEY\_CURRENT\_USER\Classes\Local

7Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge\_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsTime

8ur16 : 2016-02-26 11:16:04.310

9Key Timestamp : 2016-03-23 14:04:58.710 UTC

10Registry Key : HKEY\_CURRENT\_USER\Classes\Local

11Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge\_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsVisitCount

ur16 : 2

www.digital-detective.net

E:\Browser Dump\Windows 10 Enterprise Registry\...\Windows\UsrClass.dat

Entry ID: ur16

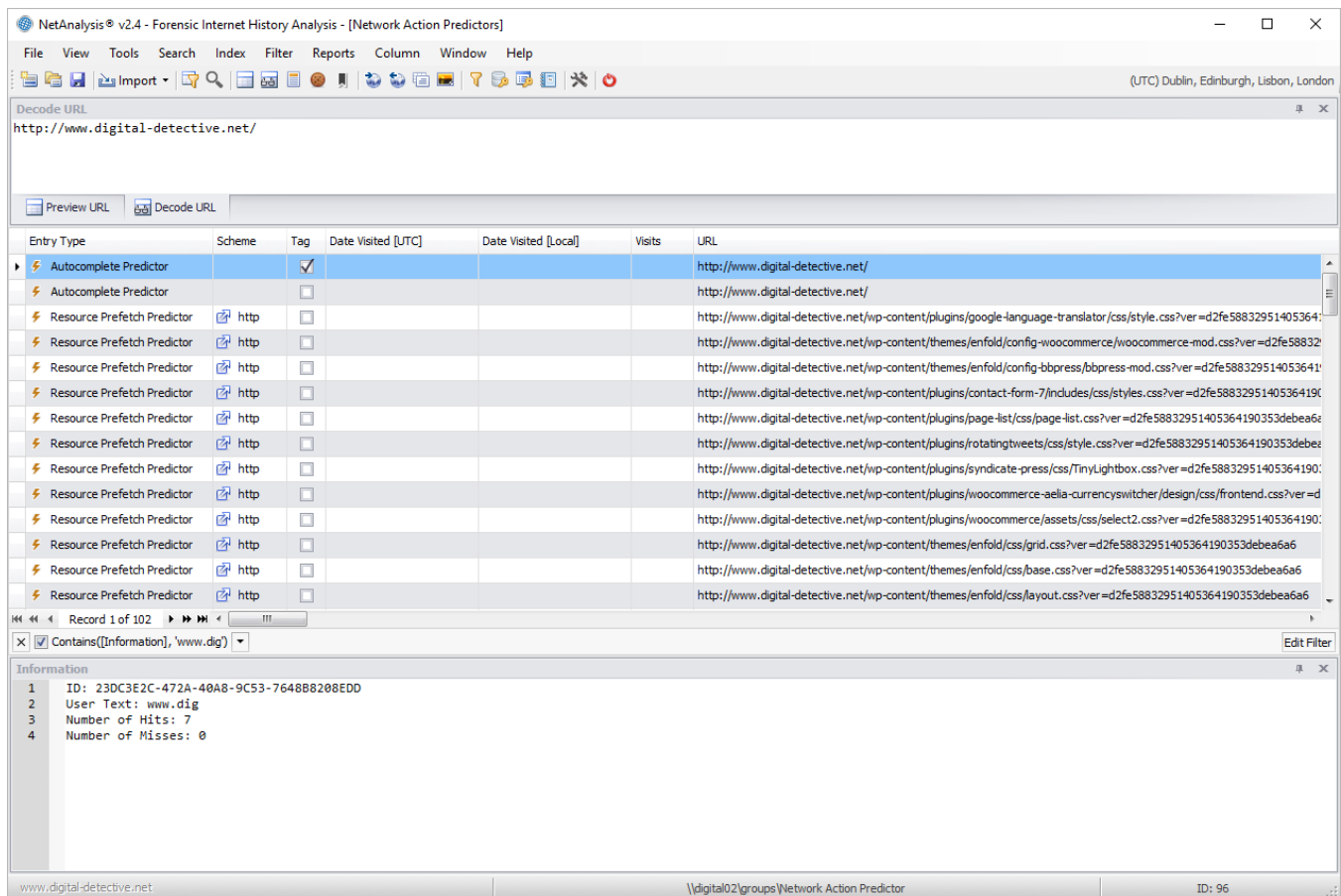
## Network Action Predictor

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".

NetAnalysis® v2.4 - Forensic Internet History Analysis - [New Case]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Page Title  
Used Cars

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Bookmark Folder		<input checked="" type="checkbox"/>				
Bookmark Folder		<input checked="" type="checkbox"/>				
Bookmark	http	<input checked="" type="checkbox"/>				http://www.ebay.com/
Bookmark	http	<input checked="" type="checkbox"/>				http://www.amazon.com/
Bookmark	http	<input checked="" type="checkbox"/>				http://www.facebook.com/
Bookmark	http	<input checked="" type="checkbox"/>				http://disney.go.com/
Bookmark	http	<input checked="" type="checkbox"/>				http://www.wikipedia.org/
Reading List	http	<input checked="" type="checkbox"/>				http://www.bbc.co.uk/sport/formula1/gossip
Reading List	https	<input checked="" type="checkbox"/>				https://secure.currys.co.uk/gbuk/o/order-reservation.html
Reading List	http	<input checked="" type="checkbox"/>				http://www2.mercedes-benz.co.uk/content/unitedkingdom/mpc/mpc_unitedkingdom_website/en/home_mpc/passengercars/home/new_c
Reading List	http	<input checked="" type="checkbox"/>	2014-08-18 15:56:10.000	2014-08-18 16:56:10.000		http://www.w3schools.com/html/html5_app_cache.asp
Reading List	http	<input checked="" type="checkbox"/>	2014-07-23 14:41:04.000	2014-07-23 15:41:04.000		http://www.digital-detective.co.uk/
Bookmark Folder		<input checked="" type="checkbox"/>				

Record 10 of 17

[Tag] = 'Checked'

Information

```

1 Web Bookmark UUID: 9B8317CD-E84D-49F8-9AB1-CB683C8868D7
2 Date Added [UTC]: 2015-07-30 22:36:38.000
3 Date Last Fetched (Non Sync) [UTC]: 2015-12-14 10:24:31.000
4 Title: Model lines
5 Archive On Disk: True
6 Fetch Result: 1
7 Sync Server ID:
8
9 Root Web Bookmark UUID: C136DFB9-837F-4212-A983-7FA1AD9A312A
10 Root Title: com.apple.ReadingList

```

Index Text

Explore the A-Class model lines. Compare the A-Class model line specs, engines and pricing by range and type.

www.digital-detective.net

\\digital01\Browser Data OS X\...\Safari\Bookmarks.plist

ID: 3

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

NetAnalysis® v2.4 - Forensic Internet History Analysis - [New Case]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Page Title  
Downloads - Oracle VM VirtualBox

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Bookmark	http	✓				http://www.facebook.com/
Bookmark	http	✓				http://uk.yahoo.com/
Bookmark	http	✓				http://www.amazon.co.uk/
Bookmark	http	✓				http://www.bbc.co.uk/news
Bookmark	http	✓				http://formula1.mediafed.com/
Bookmark	opera	✓				opera://bookmarks/
Bookmark	http	✓				http://www.google.co.uk/
Bookmark	https	✓				https://github.com/android/platform_packages_apps_browser/blob/master/src/com/android/browser/provider/BrowserProvider2.java
Bookmark	http	✓				http://www.digital-detective.net/cgi-bin/digitalboard/YaBB.pl
Bookmark	https	✓				https://www.virtualbox.org/wiki/Downloads
Bookmark	https	✓				https://forums.comodo.com/news-announcements-feedback-cd-b203.0/
Bookmark	http	✓				http://www.digital-detective.net/
Bookmark Folder		✓				
Bookmark Folder		✓				
Bookmark Folder		✓				

Record 10 of 15

[X] [Tag] = 'Checked' Edit Filter

Viewer

VirtualBox

Download VirtualBox

VirtualBox is a software emulation of a computer system. It allows you to run other operating systems, called guest operating systems, on your host operating system. VirtualBox can run on Windows, Linux, and Solaris. It can also run on Mac OS X, but only on Intel-based Macs. VirtualBox can run on a wide range of hardware, from low-end PCs to high-end servers. It can also run on a wide range of operating systems, from Windows XP to Linux. VirtualBox is a powerful tool for testing and development. It can be used to create virtual machines, which are emulated computers that can run their own operating systems. Virtual machines can be used to test software, develop applications, and run legacy software. VirtualBox is a free and open-source software project. It is developed by Oracle Corporation. VirtualBox is available for download from the Oracle website.

www.digital-detective.net

Y:\Opera Blink v36\2016\_03\_15\_11\_39\_57\_513\...\Opera Stable\bookmarks

ID: 42

## Change Log

To review the full list of changes for this release, please see: [Change Log v2.4](#).