NetAnalysis v2.2

Introduction

This release brings a number of new features and improvements. We have added support for six new browsers as well as making the necessary updates required to support the changes in the mainstream browsers. We have also added support for some new artefacts.

New Browser Support

We have added new support for the following browsers:

Browser		Details
	360 Browser v7	360 Browser is a web browser developed by the Qihoo 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.
	Comodo Chromodo v36 - 43	Comodo Chromodo is a Chromium technology-based browser that offers all of Chrome's features plus a claimed increase in speed, security and privacy.
	Sleipnir (Windows) v3 - 6 Sleipnir (OS X) v3 - 4	Sleipnir is a freeware web browser developed by Fenrir Inc of Osaka, Japan. The browser's main features are customisation and tab functions. The Windows version supports different layout engines. Sleipnir version 5 introduced proprietary text rendering which visually resembles Mac OS text rendering.
	Titan Browser v1 - 33	Titan Browser is a freeware Chromium based web browser and Internet suite developed by Titan Browser Corp. It is a simple browser focused on security and privacy; protecting the user from installing unwanted add-ons, toolbars, or applications. The default search engine uses the Titan search engine to provide secure and anonymous search results powered by search providers such as Bing and Yahoo.
	Vivaldi v1	Vivaldi is a freeware Chromium based web browser developed by Vivaldi Technologies, a company founded by former Opera Software co-founder and CEO Jon Stephenson von Tetzchner. The browser is aimed at power users and previous Opera web browser users disgruntled by Opera's transition from the Presto layout engine to the Blink layout engine, which removed many popular features in the process. Vivaldi aims to revive the old, popular features of Opera 12 and introduce new, more innovative ones.

	Yandex v1 - 15	Yandex Browser is a Chromium based web browser developed by the Russian web search corporation Yandex. The browser checks web page security with the Yandex security system and checks downloaded files with Kaspersky anti-virus. The browser also uses Opera Software's Turbo technology to speed web browsing on slow connections. The browser's SmartBox uses Yandex Search as its default search engine.

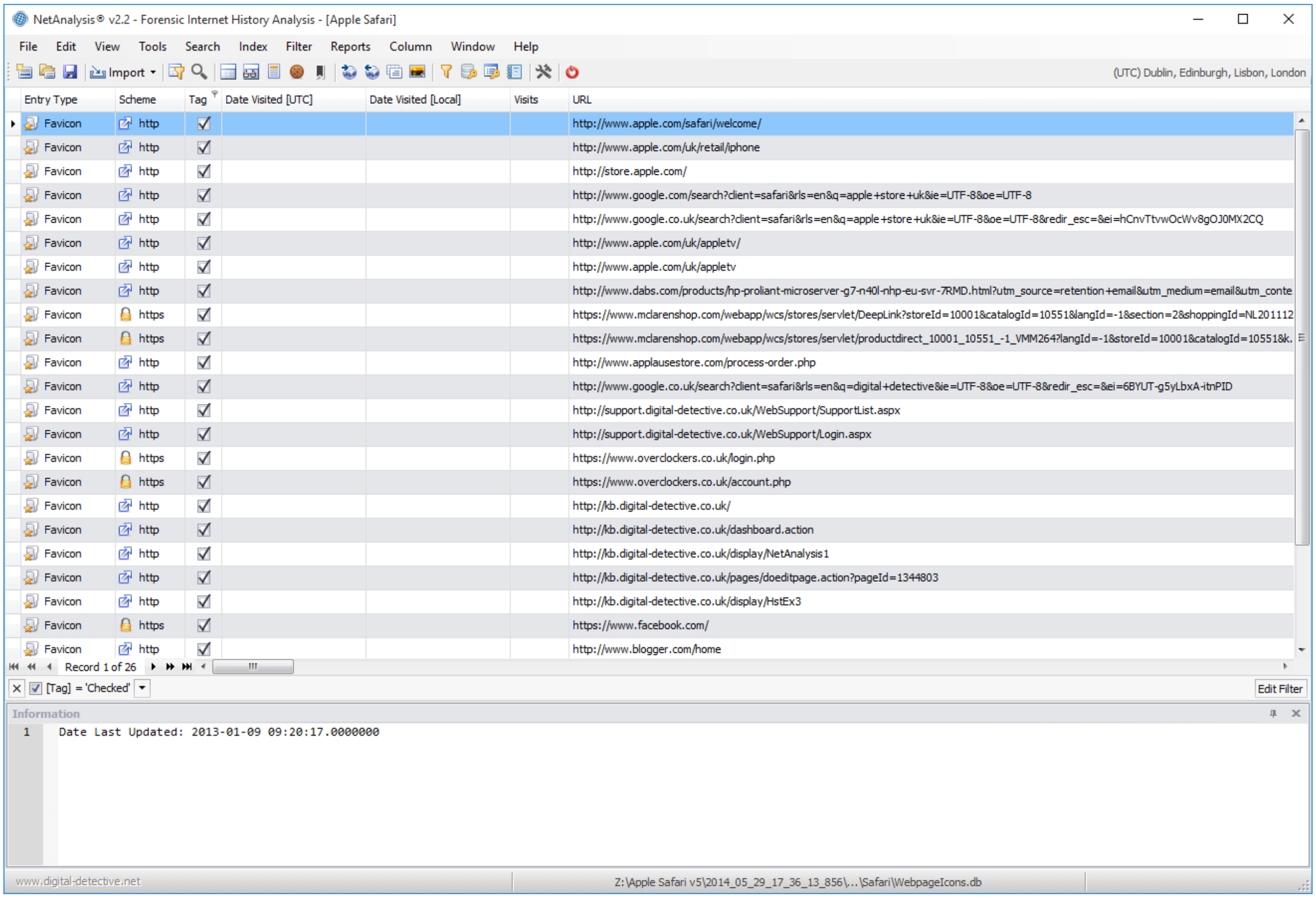
New Artefacts

Favicons

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

- Apple Safari
- Google Chrome and Chromium Based Browsers
- Mozilla Firefox and Mozilla Based Browsers
- Opera (Presto)
- Opera

The following screen shows some filtered Favicon entries from Safari.


NetAnalysis® v2.2 - Forensic Internet History Analysis - [Apple Safari]
File
Edit
View
Tools
Search
Index
Filter
Reports
Column
Window
Help
Import
(UTC) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Favicon	http	✓				http://www.apple.com/safari/welcome/
Favicon	http	✓				http://www.apple.com/uk/retail/iphone
Favicon	http	✓				http://store.apple.com/
Favicon	http	✓				http://www.google.com/search?client=safari&rls=en&q=apple+store+uk&ie=UTF-8&oe=UTF-8
Favicon	http	✓				http://www.google.co.uk/search?client=safari&rls=en&q=apple+store+uk&ie=UTF-8&oe=UTF-8&redir_esc=&ei=hCnvTtvwOcWv8gOJ0MX2CQ
Favicon	http	✓				http://www.apple.com/uk/appletv/
Favicon	http	✓				http://www.apple.com/uk/appletv
Favicon	http	✓				http://www.dabs.com/products/hp-proliant-microserver-g7-n40l-nhp-eu-svr-7RMD.html?utm_source=retention+email&utm_medium=email&utm_conte
Favicon	https	✓				https://www.mclarenshop.com/webapp/wcs/stores/servlet/DeepLink?storeId=10001&catalogId=10551&langId=-1&section=2&shoppingId=NL201112
Favicon	https	✓				https://www.mclarenshop.com/webapp/wcs/stores/servlet/productdirect_10001_10551_-1_VMM264?langId=-1&storeId=10001&catalogId=10551&k.
Favicon	http	✓				http://www.applausestore.com/process-order.php
Favicon	http	✓				http://www.google.co.uk/search?client=safari&rls=en&q=digital+detective&ie=UTF-8&oe=UTF-8&redir_esc=&ei=6BYUT-g5yLbxA-itnPID
Favicon	http	✓				http://support.digital-detective.co.uk/WebSupport/SupportList.aspx
Favicon	http	✓				http://support.digital-detective.co.uk/WebSupport/Login.aspx
Favicon	https	✓				https://www.overclockers.co.uk/login.php
Favicon	https	✓				https://www.overclockers.co.uk/account.php
Favicon	http	✓				http://kb.digital-detective.co.uk/
Favicon	http	✓				http://kb.digital-detective.co.uk/dashboard.action
Favicon	http	✓				http://kb.digital-detective.co.uk/display/NetAnalysis1
Favicon	http	✓				http://kb.digital-detective.co.uk/pages/doeditpage.action?pageId=1344803
Favicon	http	✓				http://kb.digital-detective.co.uk/display/HstEx3
Favicon	https	✓				https://www.facebook.com/
Favicon	http	✓				http://www.blogger.com/home

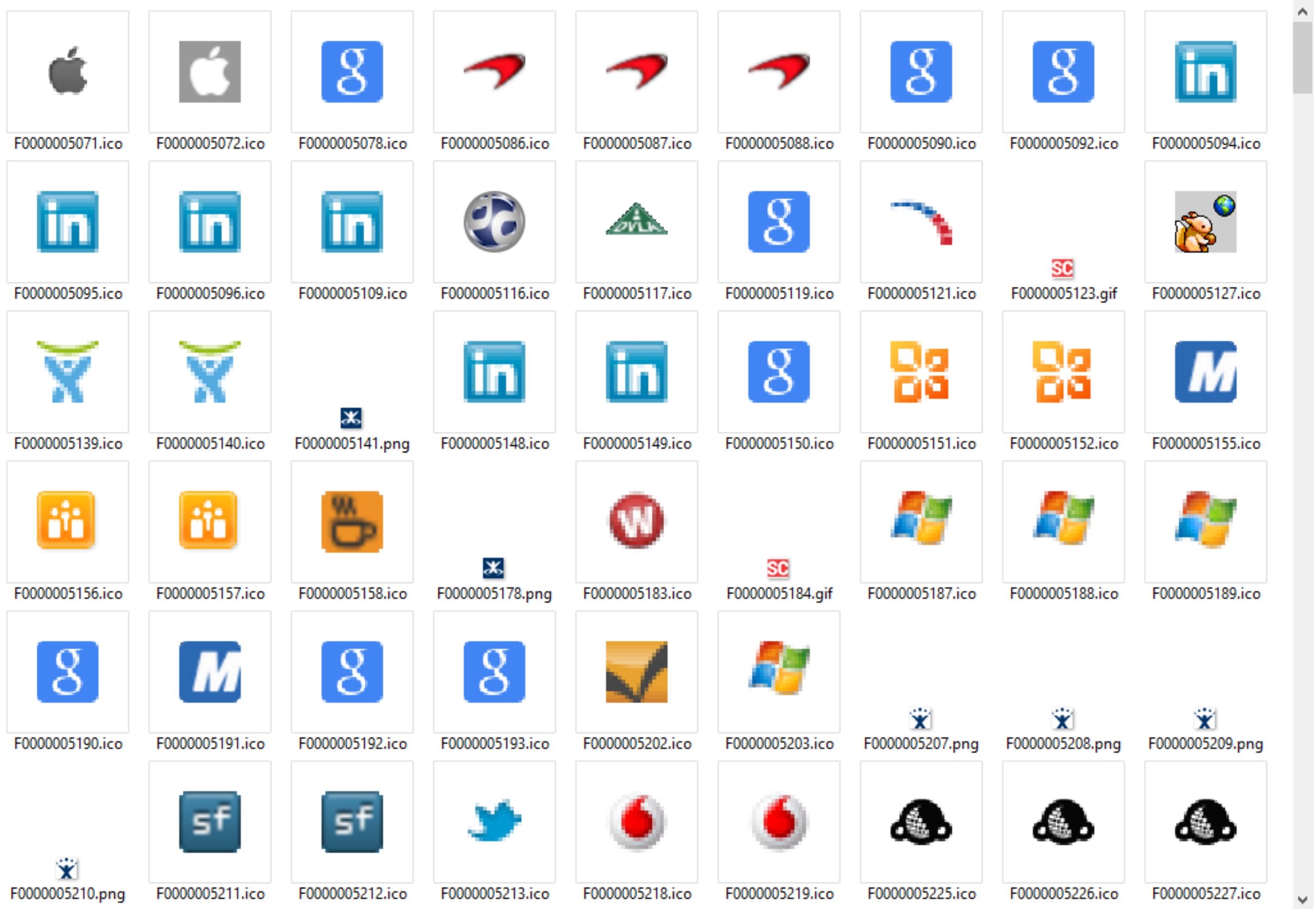
Record 1 of 26

☑ [Tag] = 'Checked'

```
1    Date Last Updated: 2013-01-09 09:20:17.0000000
```

www.digital-detective.net   Z:\Apple Safari v5\2014_05_29_17_36_13_856\...\Safari\WebpageIcons.db

During the import process, the actual icons/image files are extracted to the export folder. Open the export folder by selecting Tools » Open Case Export Folder and select the Favicons folder for the corresponding browser. This will show you all of the extracted images. You can match the unique reference number for the image (URN) to the unique reference number of the record entry. The image below shows a typical Favicons folder.



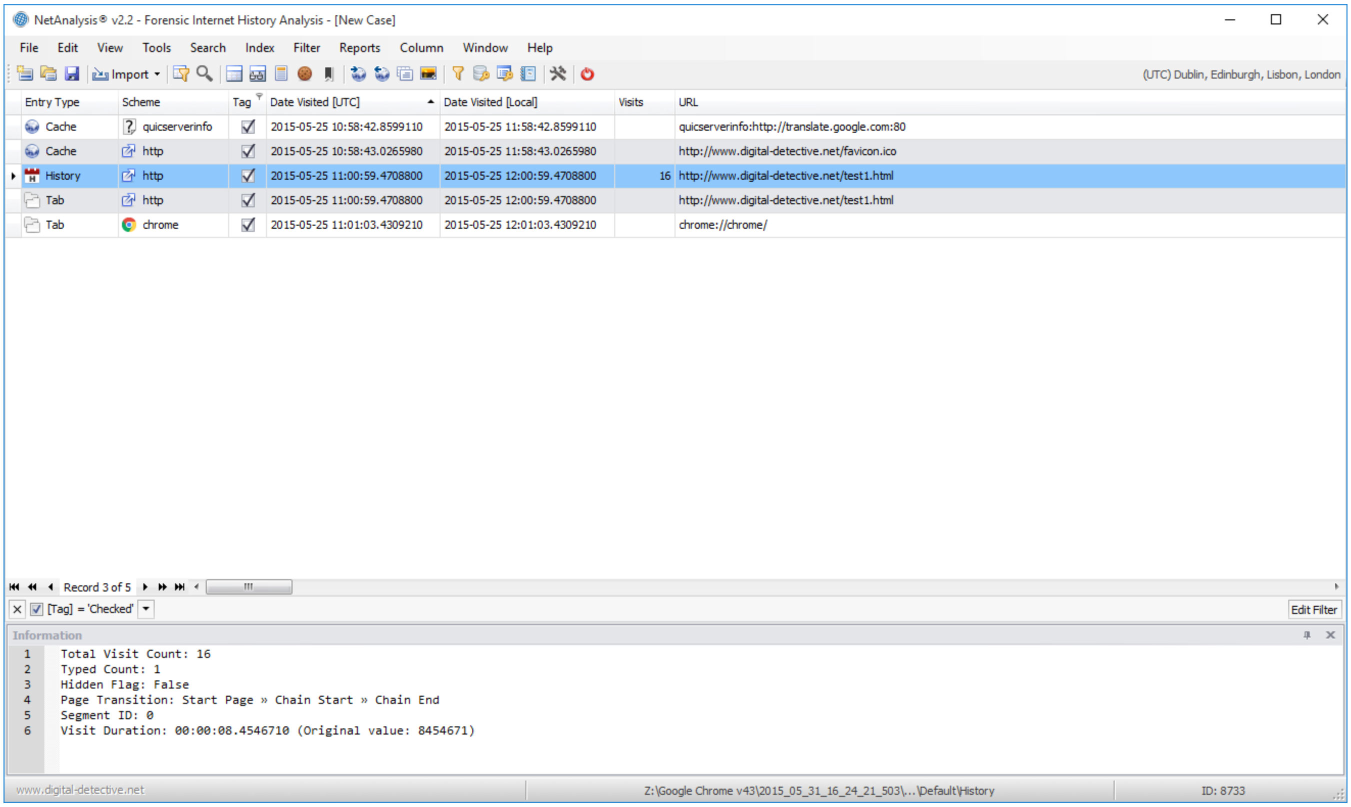
Any History record which has an associated Favicon entry will have the Favicon URL displayed in the Favicon URL column for that entry.

Chromium Session / Tab Restore

Google Chrome and many of the Chromium based browsers store session and tab information in four files:

- Current Session
- Current Tabs
- Last Session
- Last Tabs

These files store information relating to the current and last browsing session and can be very helpful in a forensic investigation. We have now added support to import the tab navigation information. The screen below shows opening a new session with the default new tab selected and then directly navigating to a test page on the Digital Detective web site.


NetAnalysis® v2.2 - Forensic Internet History Analysis - [New Case]
File
Edit
View
Tools
Search
Index
Filter
Reports
Column
Window
Help
Import
(UTC) Dublin, Edinburgh, Lisbon, London
Edit Filter
Information

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	quicserverinfo	☑	2015-05-25 10:58:42.8599110	2015-05-25 11:58:42.8599110		quicserverinfo:http://translate.google.com:80
Cache	http	☑	2015-05-25 10:58:43.0265980	2015-05-25 11:58:43.0265980		http://www.digital-detective.net/favicon.ico
History	http	☑	2015-05-25 11:00:59.4708800	2015-05-25 12:00:59.4708800	16	http://www.digital-detective.net/test1.html
Tab	http	☑	2015-05-25 11:00:59.4708800	2015-05-25 12:00:59.4708800		http://www.digital-detective.net/test1.html
Tab	chrome	☑	2015-05-25 11:01:03.4309210	2015-05-25 12:01:03.4309210		chrome://chrome/

Record 3 of 5

☑ [Tag] = 'Checked'

```
Total Visit Count: 16
Typed Count: 1
Hidden Flag: False
Page Transition: Start Page » Chain Start » Chain End
Segment ID: 0
Visit Duration: 00:00:08.4546710 (Original value: 8454671)
```

www.digital-detective.net | Z:\Google Chrome v43\2015_05_31_16_24_21_503\...\Default\History | ID: 8733

Base58 Decoding

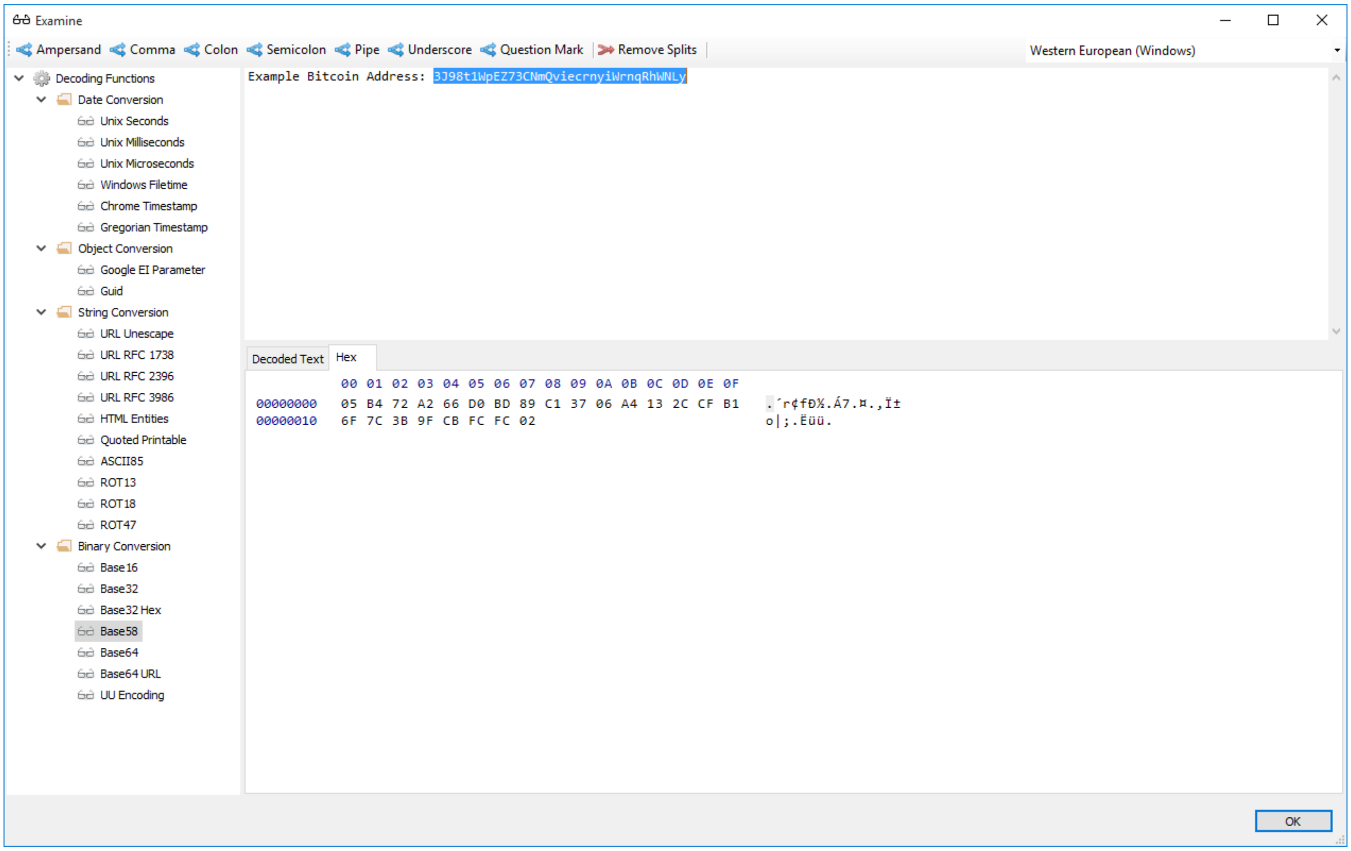
Base58 is a group of binary-to-text encoding schemes used to represent large integers as alphanumeric text. It is similar to Base64 but has been modified to avoid both non-alphanumeric characters and letters which might look ambiguous when printed. It is therefore designed for human users who manually enter the data, copying from some visual source, but also allows easy copy and paste because a double-click will usually select the whole string.

Compared to Base64, the following letters have been omitted from the alphabet: 0 (zero), O (capital o), I (capital i) and l (lower case L) as well as the non-alphanumeric characters + (plus) and / (slash). In contrast to Base64, the digits of the encoding don't line up well with byte boundaries of the original data. For this reason, the method is well-suited to encode large integers, but not designed to encode longer portions of binary data. The actual order of letters in the alphabet depends on the application, which is the reason why the term “Base58” alone is not enough to fully describe the format.

Base58 is used for:

- Bitcoin addresses
- Ripple addresses
- Short URLs for Flickr

We have added Base58 decoding to the decoding/examination window. The following shows an example Bitcoin address being decoded:



```
Example Bitcoin Address: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
```

```
            00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000    05 B4 72 A2 66 D0 BD 89 C1 37 06 A4 13 2C CF B1    .´r¢fÐ½.Á7.¤.,Ï±
00000010    6F 7C 3B 9F CB FC FC 02                            o|;.Ëüü.
```

Change Log

To review the full list of changes for this release, please see: Change Log v2.2.