NetAnalysis v2.1

Introduction

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

Some of the significant features for this release include support for the automatic decryption of usernames and passwords in Mozilla Firefox, Mozilla Firefox on Android, Sea Monkey, Pale Moon, Wyzo, Comodo IceDragon and K-Meleon. We have also added support for the changes made in Apple Safari v8.

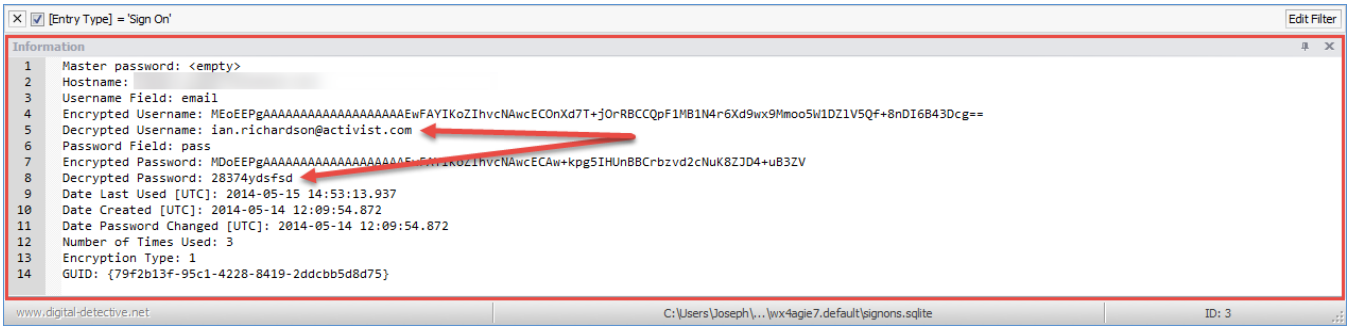
New Features

We have added a whole host of new features to this release. The following represents some of the more important changes.

Username and Password Decryption

Firefox and other Mozilla based browsers include a Password Manager that can save the passwords provided by the user as they log in to websites. The Password Manager securely stores the usernames and passwords used to access websites and then automatically fills them in for the user when they next visit the site. For additional security, the user can also set a Master Password to protect the Password Manager. The user is then prompted to enter the Master Password when the browser needs to access the stored passwords. Usernames and passwords are encrypted and stored within the Mozilla profile.

NetAnalysis® v2.1 is now able to decrypt and display the usernames and passwords stored for each web site. The following image shows the NetAnalysis® Information Panel with some decrypted Username and Password values. Also, the entry on line number 1 shows that the Master Password has not been set in this case.



Read more about Username and Password decryption here: Username and Password Decryption.

New Browser Support

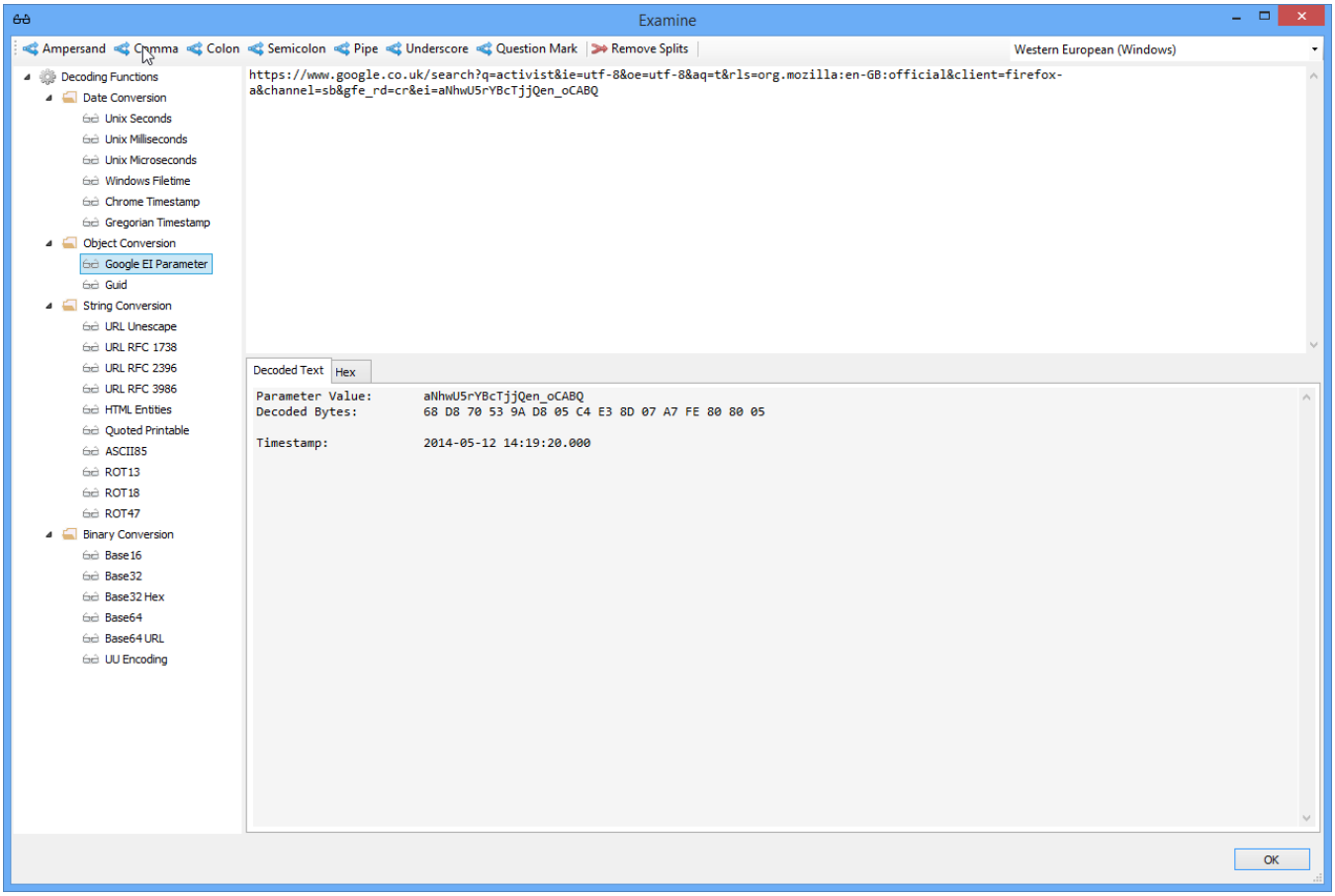
In addition to extending support for the existing browsers and their recent changes, we have now added support for two new browsers:

- SRWare Iron v1 - 38
- K-Meleon v1 - 74

New Artefacts

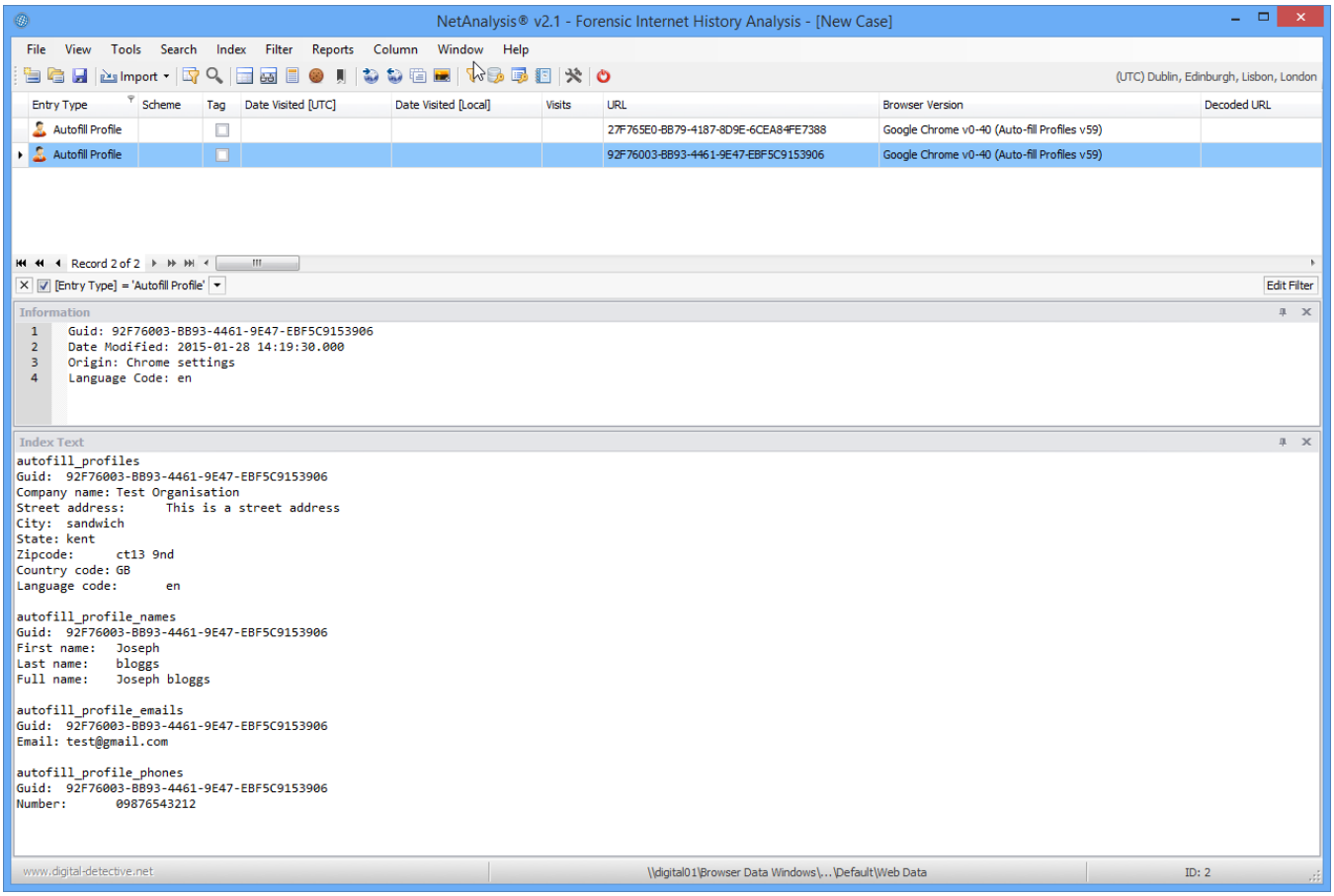
Google Search EI/SEI Parameter Decoding

The Window below shows the automatic decoding of a Google URL which contains an EI parameter. The EI parameter is a Base64 encoded 16 byte value. The first 4 bytes contain a timestamp which can be seen in the example above.



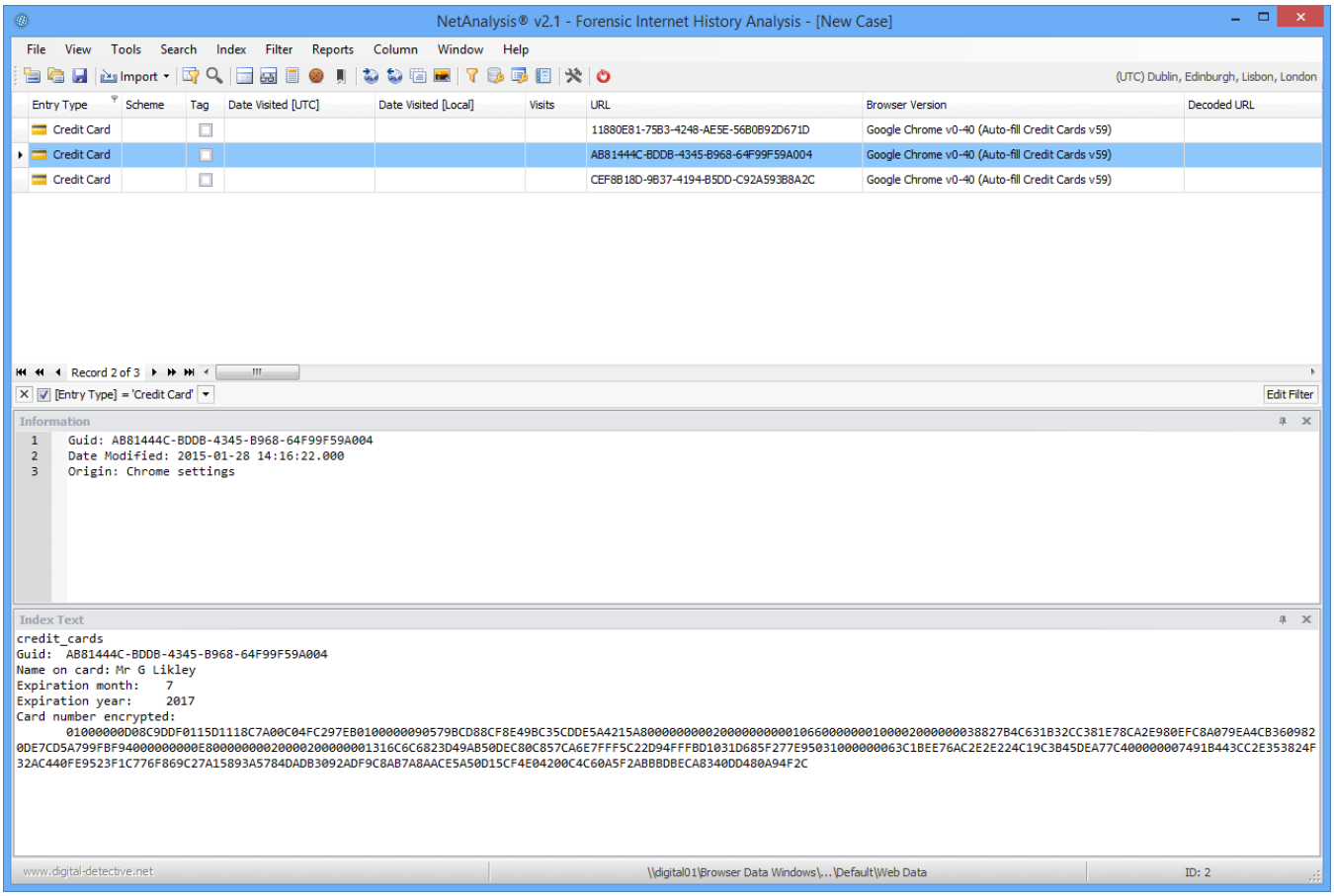
Google Chrome Autofill Profiles

The window below shows the extraction of Google Chrome Autofill Profile data. The text relating to the autofill fields are extracted to the export folder so that the data can be indexed and searched.



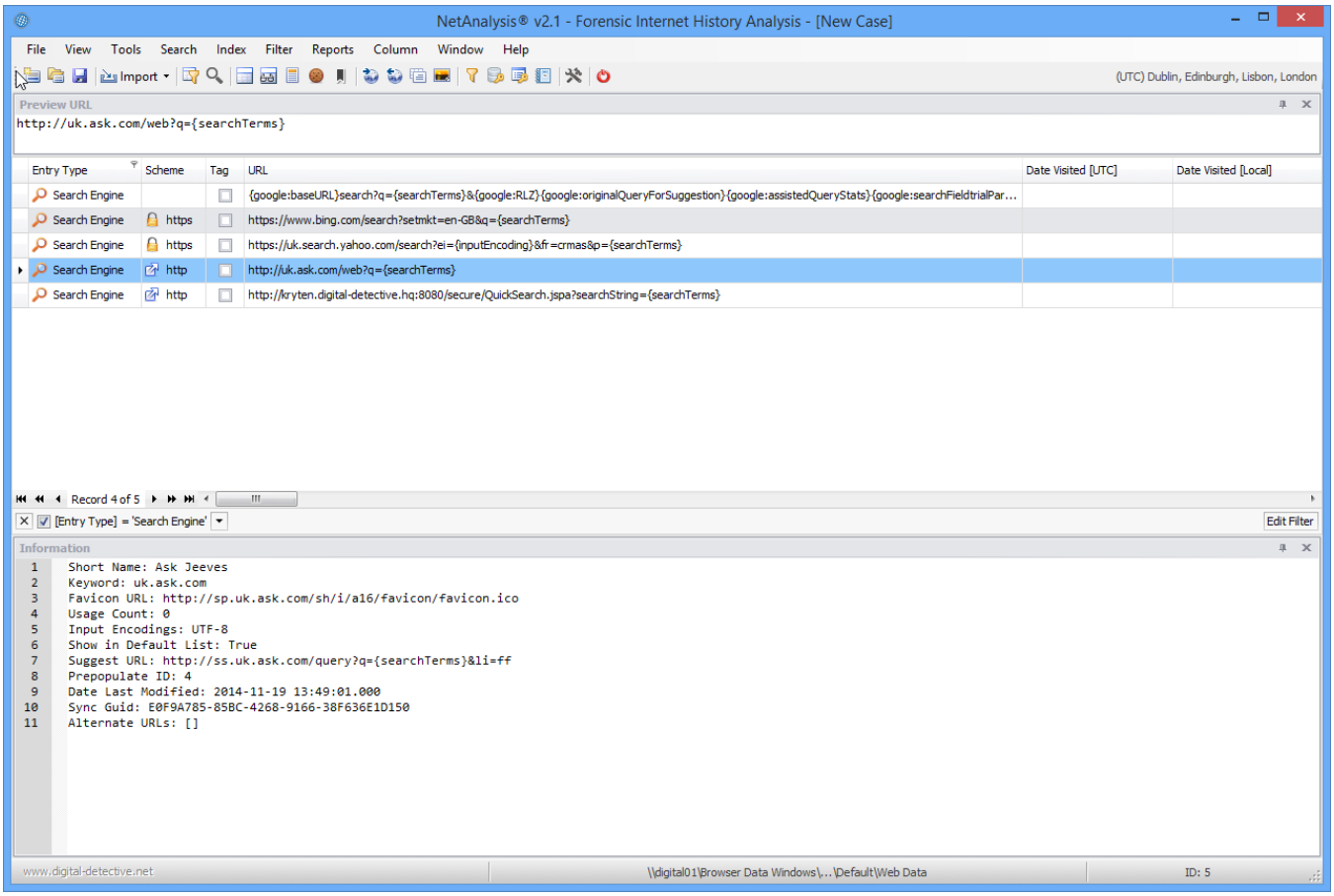
Google Chrome Credit Card Autofill Profiles

The window below shows the extraction of Google Chrome Credit Card Autofill data. The text relating to the autofill fields are extracted to the export folder so that the data can be indexed and searched.



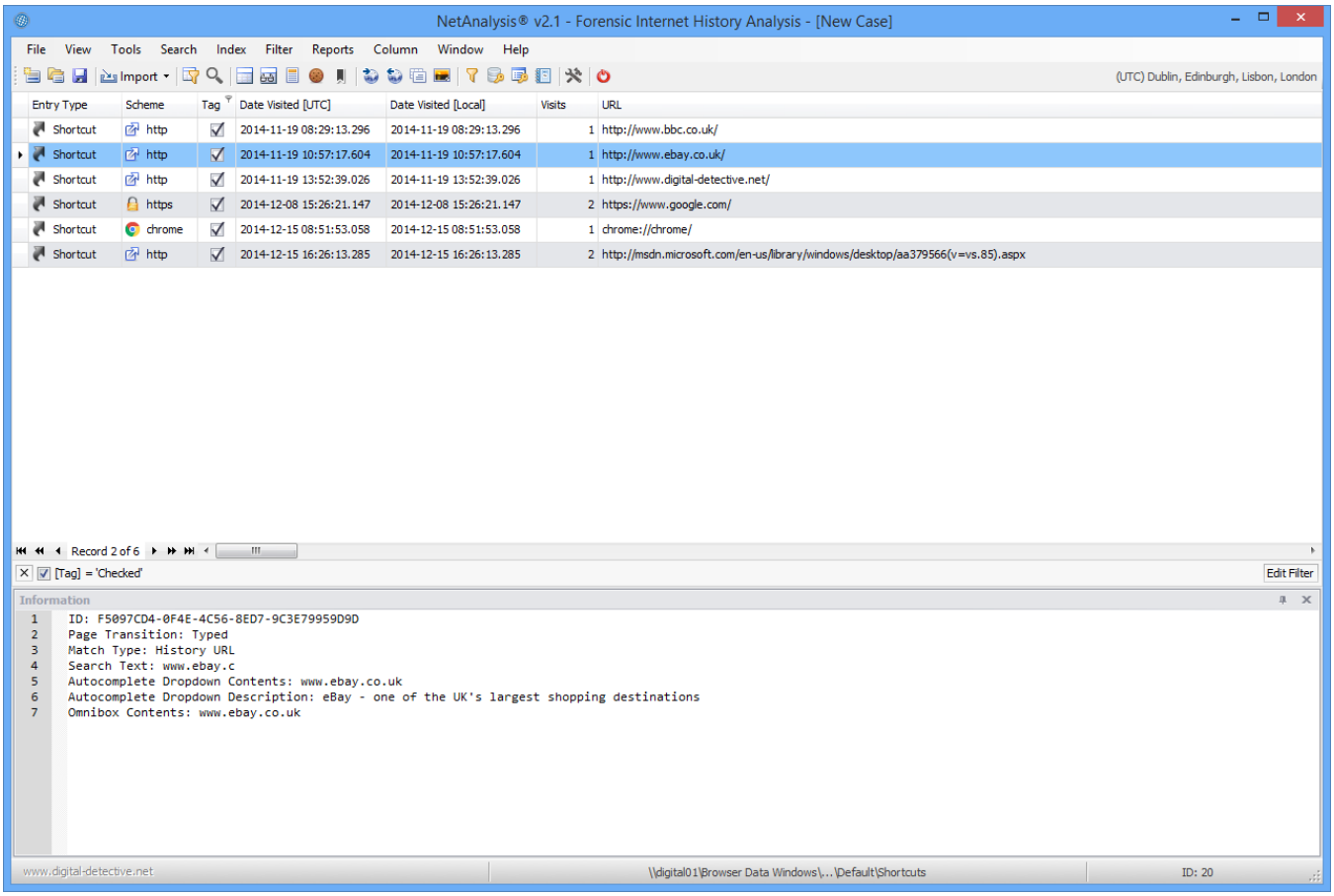
Google Chrome Search Engine Parameters

The window below shows the Search Engine entry type extracted from a Google Chrome keywords table. This information is used to setup standard and bespoke searching for the user when keywords are entered into the omnibox.

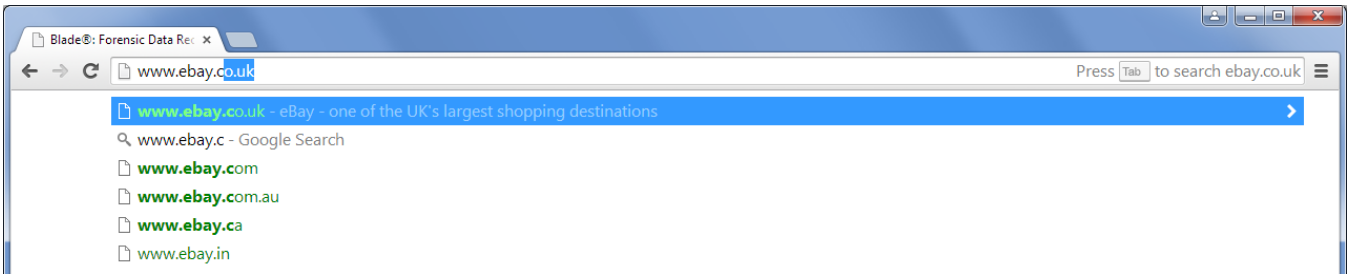


Google Chrome Shortcuts

The window below shows a number of Google Chrome shortcut entries. These entries represent the transition between the text entered by a user into the omnibox and the selected suggestion as presented by Google Chrome. The shortcut entry is created when the user selects a suggested entry from the dropdown list and visits the corresponding page.

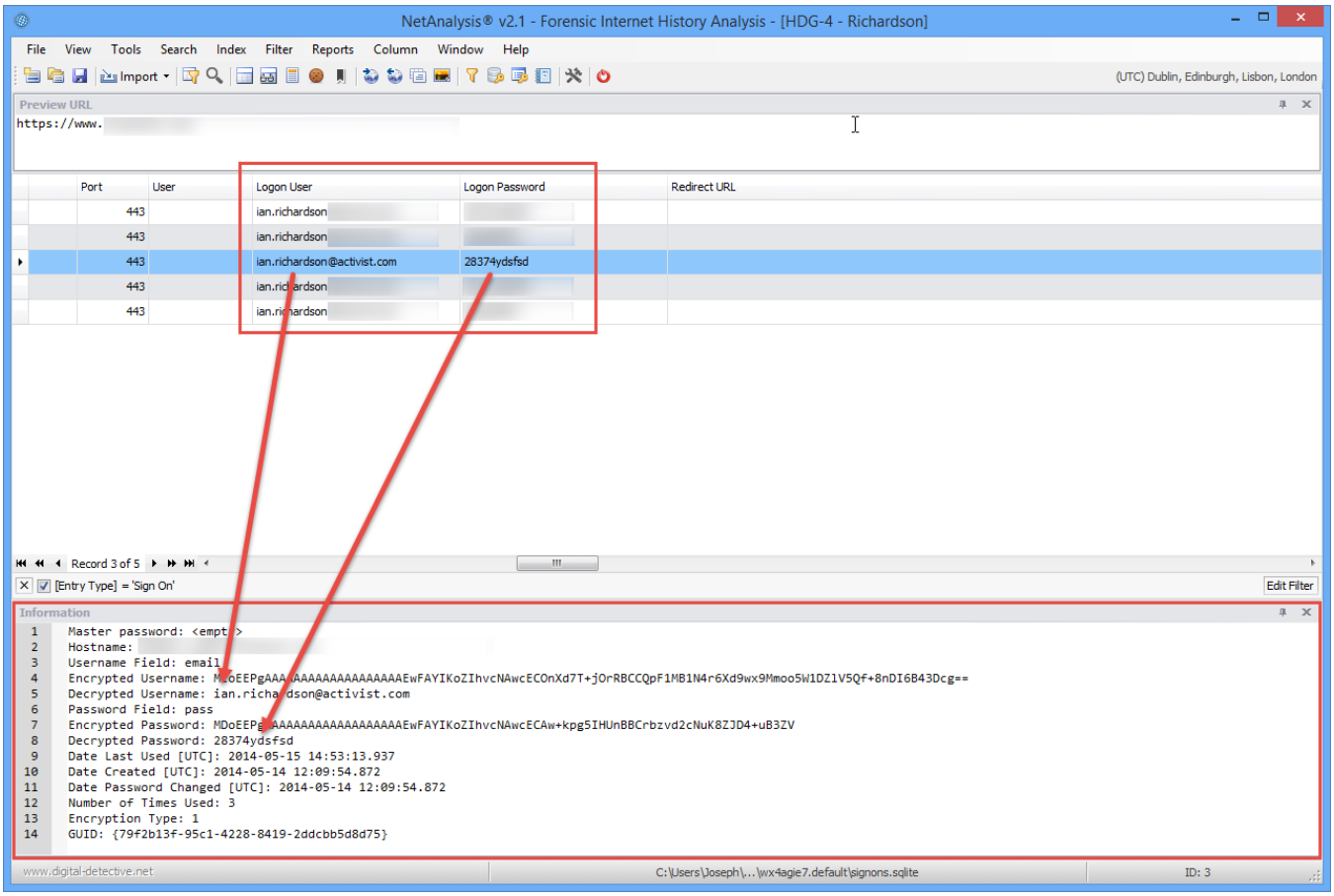


In the example above, the user typed "www.ebay.c" into the omnibox (see the image below) and the browser displayed a number of suggestions in the list below the omnibox. The user then selected the top entry in the suggestion list (or pressed enter) and subsequently visited the ebay site.



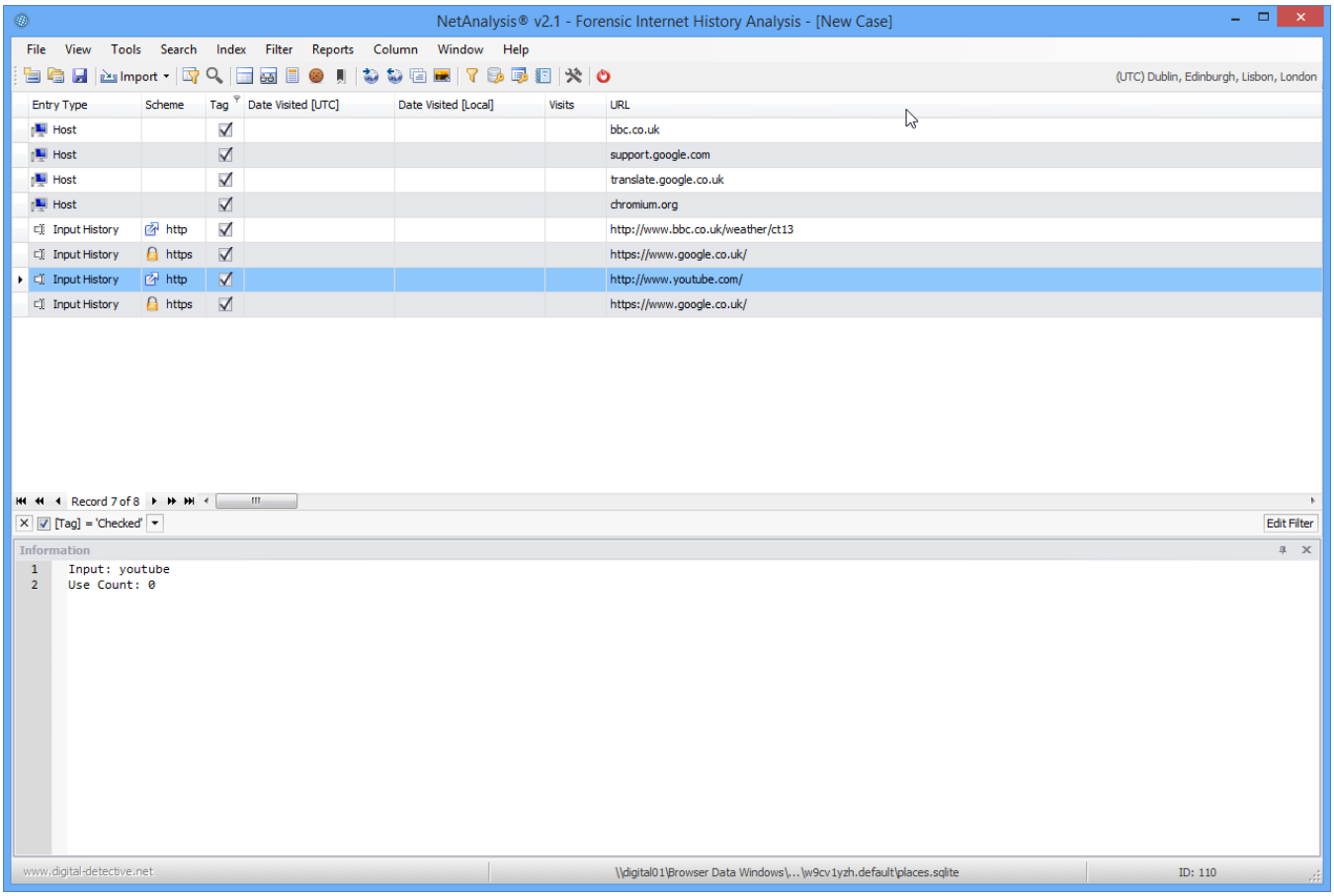
Mozilla Firefox Username and Password Decryption

The window below shows the automatic decryption of usernames and passwords as stored by Mozilla Firefox. NetAnalysis v2 can automatically decrypt these usernames and passwords.



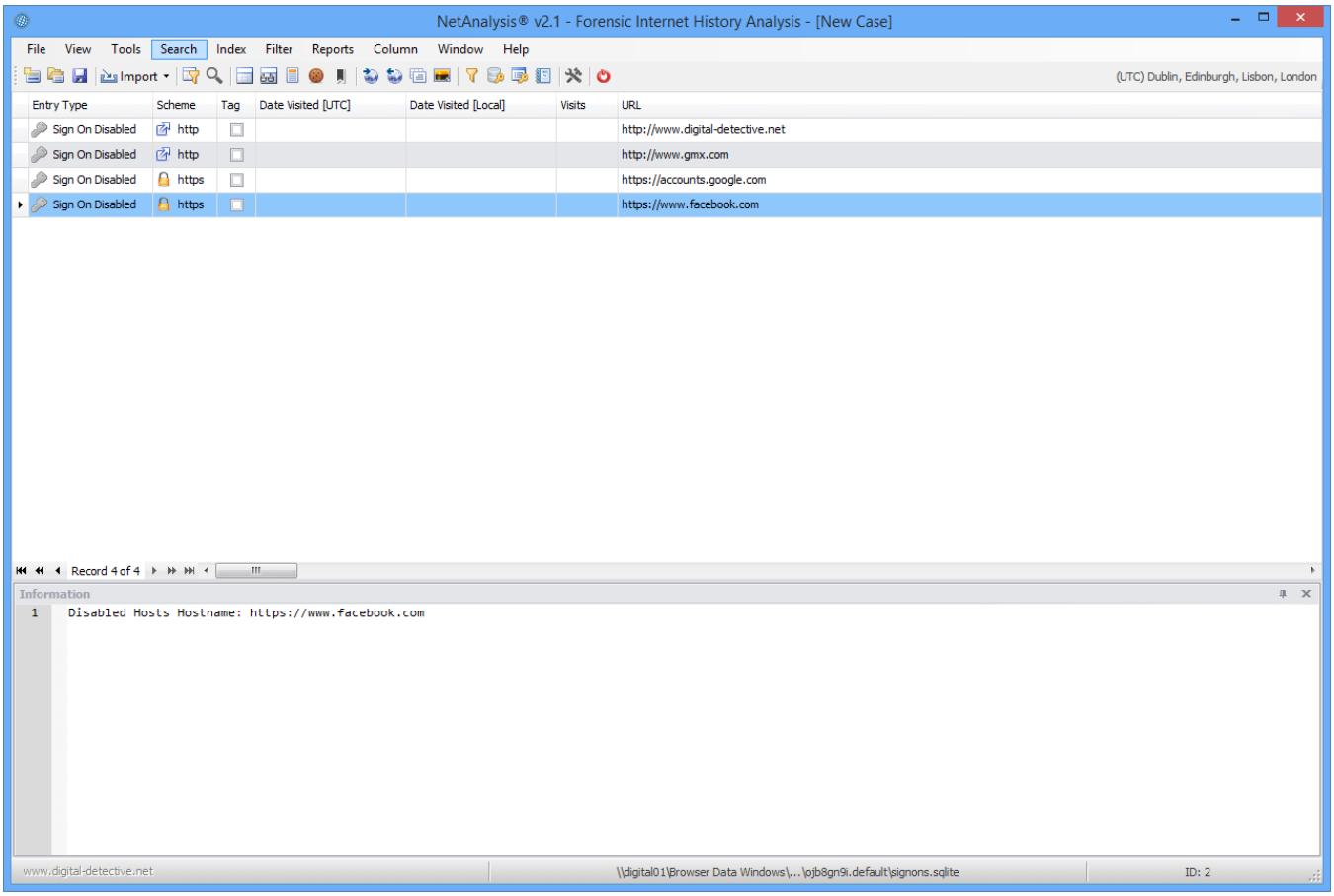
Mozilla Firefox moz_hosts and moz_inputhistory

The window below shows some Host and Input History entry type records. Input History entries show what the user entered into the address bar and the associated URL that was clicked as the result of the suggestion made by Firefox. Host entries are similar to Internet Explorer Host entries and show the hostname relating to a visit to a URL.



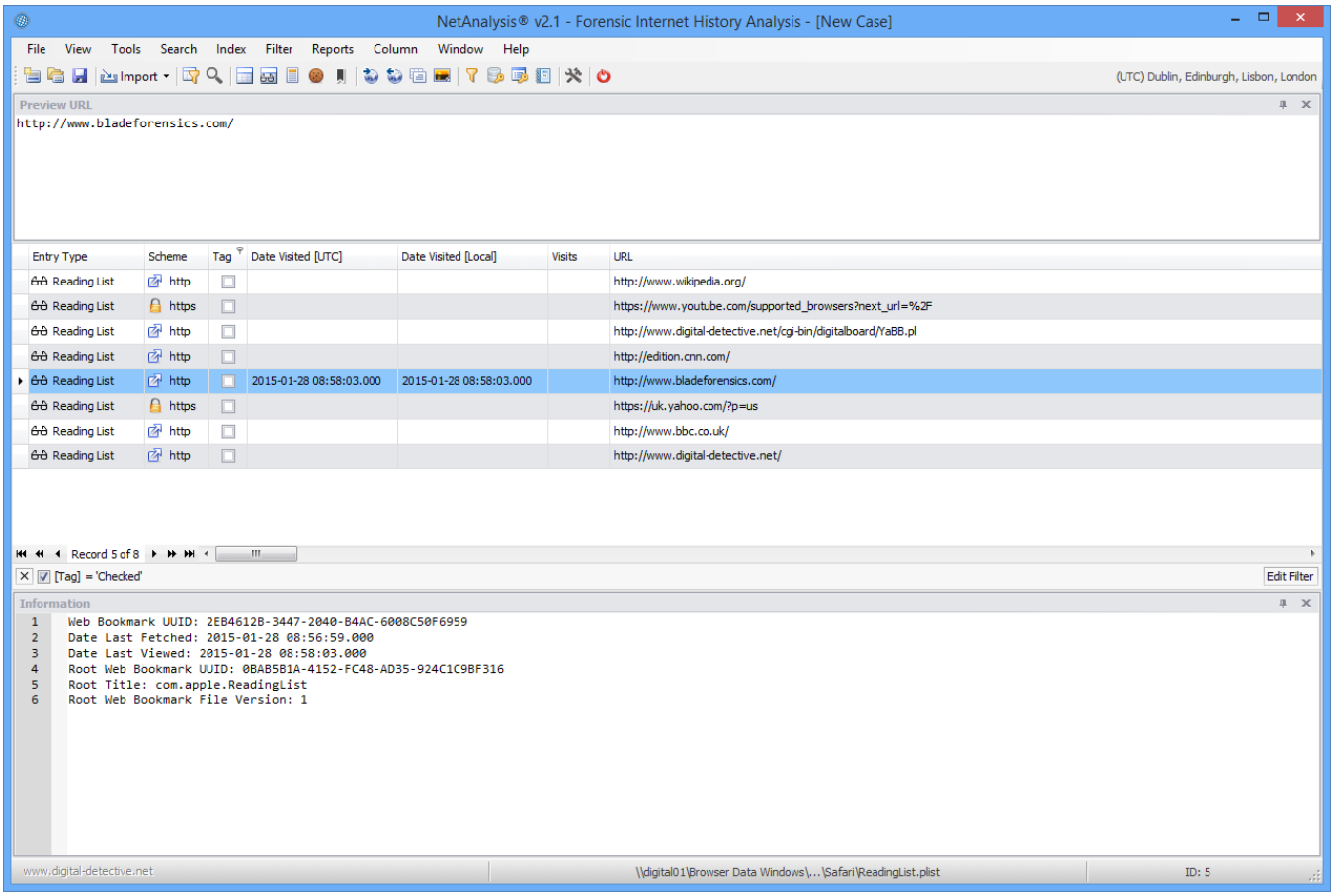
Mozilla Firefox moz_disabledhosts

The window below shows some Firefox moz_disabledhosts entries. These entries show sites where the user has selected NOT to save a username or password.



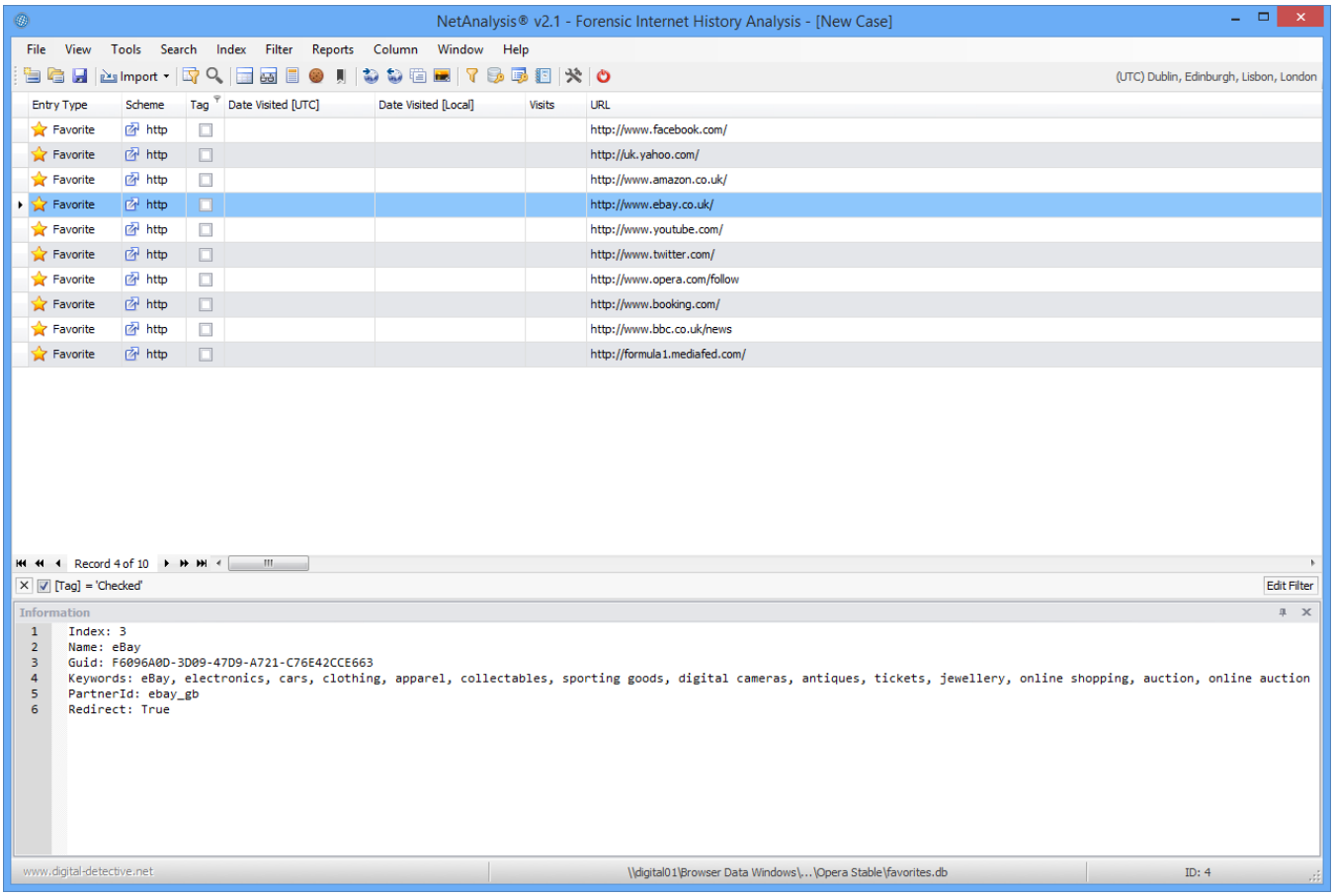
Apple Safari Reading Lists

The window below shows a number of Apple Safari Reading List entries. These represent sites the user has selected to view at a later date. Once the user visits a site from the Reading List, the Date Visited is updated to reflect the date and time of the visit.



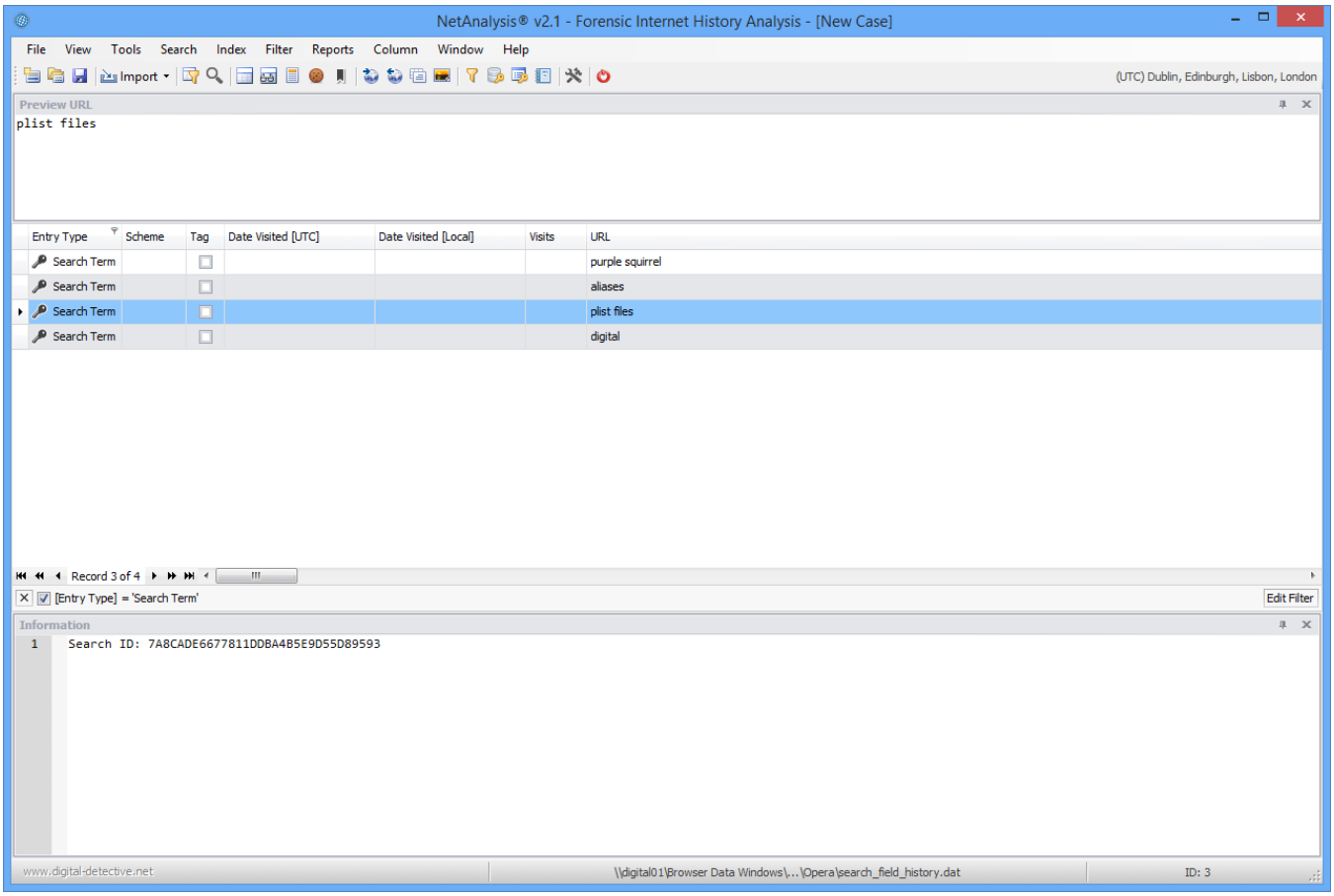
Opera Blink Favorite Entries

The window below shows a number of Opera Favorite entries.



Opera Presto Search Field History

The window below shows a number of entries from the Opera Presto `search_field_history.dat` file. These entries represent the text entered by the user into the search box.



Improvements

We have also made a number of improvements for this release such as improving the way we deal with encoding throughout the case, improving the way we deal with the new Firefox Cache v2 entries (added support for orphaned and doomed entries), adding new filters, report templates, layout files and keyword lists. We have also increased the evaluation period to 21 days.

Change Log

You can find the complete change log for NetAnalysis® v2.1 here:

- NetAnalysis v2.1 Change Log