

# NetAnalysis v2.1



- [Introduction](#)
- [New Features](#)
  - [Username and Password Decryption](#)
- [New Browser Support](#)
- [New Artefacts](#)
  - [Google Search EI/SEI Parameter Decoding](#)
  - [Google Chrome Autofill Profiles](#)
  - [Google Chrome Credit Card Autofill Profiles](#)
  - [Google Chrome Search Engine Parameters](#)
  - [Google Chrome Shortcuts](#)
  - [Mozilla Firefox Username and Password Decryption](#)
  - [Mozilla Firefox moz\\_hosts and moz\\_inpuhistory](#)
  - [Mozilla Firefox moz\\_disabledhosts](#)
  - [Apple Safari Reading Lists](#)
  - [Opera Blink Favorite Entries](#)
  - [Opera Presto Search Field History](#)
- [Improvements](#)
- [Change Log](#)



## 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.

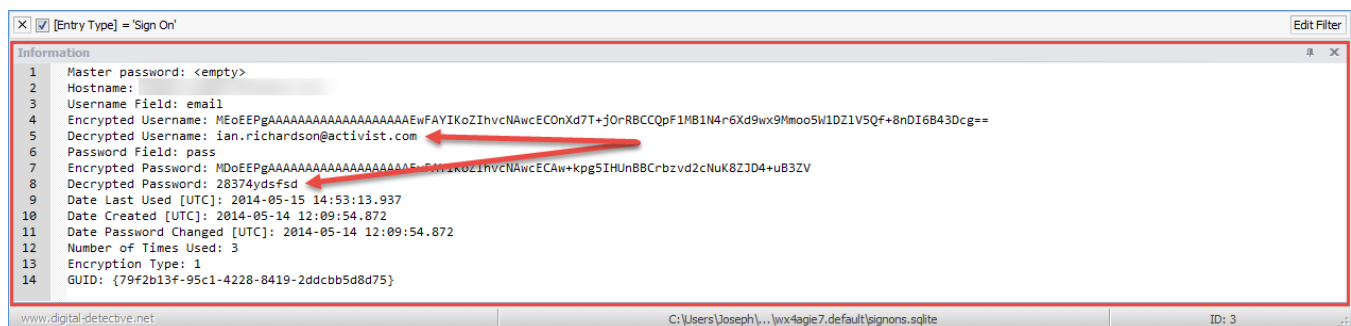
## New Features

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

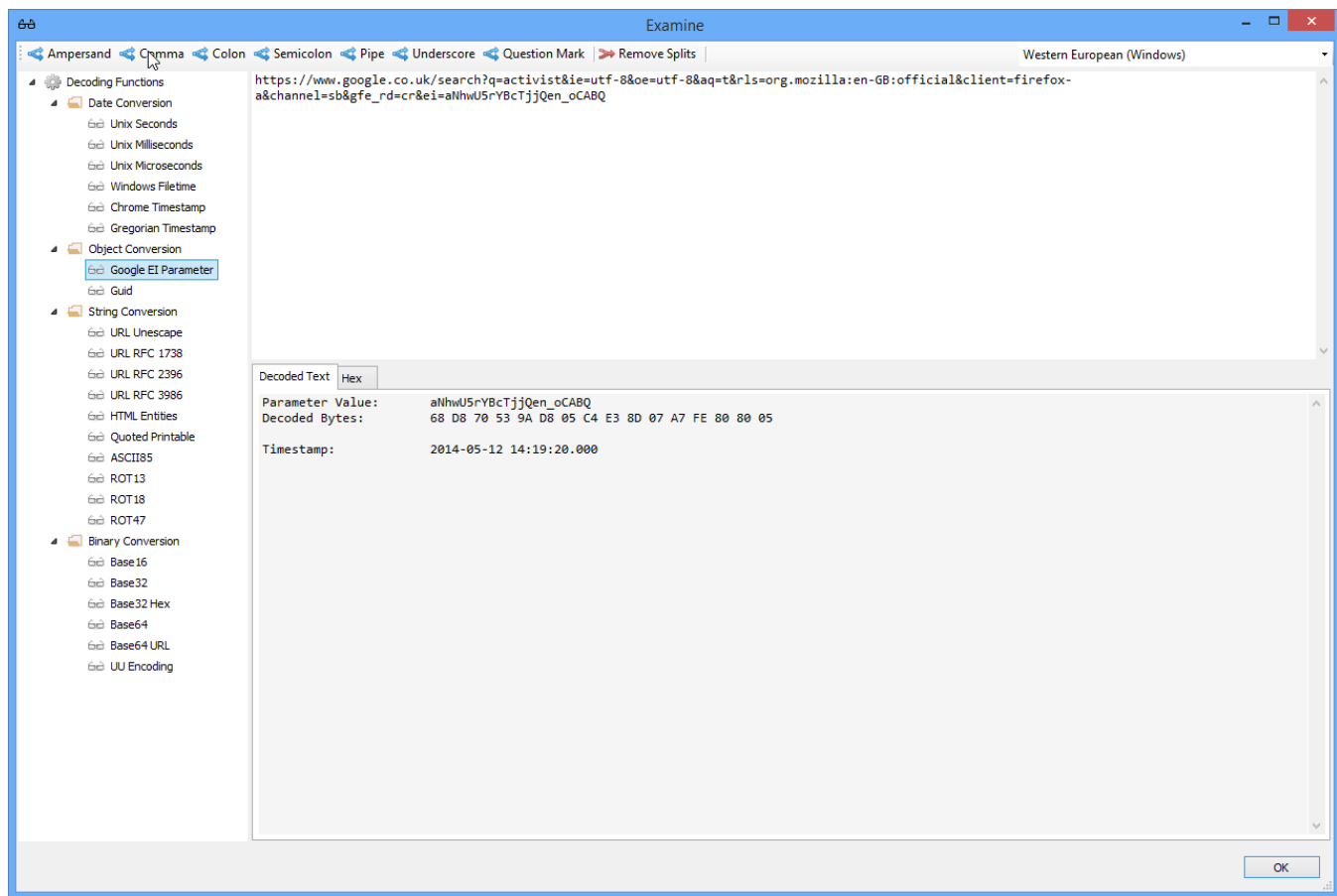
In addition to extending support for the existing browsers and their recent changes, we have now added support for two new browsers:

- [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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [New Case]

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	Browser Version	Decoded URL
Autofill Profile						27F765E0-BB79-4187-8D9E-6CEA84FE7388	Google Chrome v0-40 (Auto-fill Profiles v59)	
Autofill Profile						92F76003-BB93-4461-9E47-EBF5C9153906	Google Chrome v0-40 (Auto-fill Profiles v59)	

Record 2 of 2

[X] [Entry Type] = 'Autofill Profile'

Information

- Guid: 92F76003-BB93-4461-9E47-EBF5C9153906
- Date Modified: 2015-01-28 14:19:30.000
- Origin: Chrome settings
- Language Code: en

Index Text

```
autofill_profiles
Guid: 92F76003-BB93-4461-9E47-EBF5C9153906
Company name: Test Organisation
Street address: This is a street address
City: sandwich
State: kent
Zipcode: ct13 9nd
Country code: GB
Language code: en

autofill_profile_names
Guid: 92F76003-BB93-4461-9E47-EBF5C9153906
First name: Joseph
Last name: bloggs
Full name: Joseph bloggs

autofill_profile_emails
Guid: 92F76003-BB93-4461-9E47-EBF5C9153906
Email: test@gmail.com

autofill_profile_phones
Guid: 92F76003-BB93-4461-9E47-EBF5C9153906
Number: 09876543212
```

www.digitaldetective.net | \\digital01\Browser Data Windows\...\Default\Web Data | ID: 2

## 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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [New Case]

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	Browser Version	Decoded URL
Credit Card						11880E81-75B3-4248-AE5E-5680B92D67ID	Google Chrome v0-40 (Auto-fill Credit Cards v59)	
Credit Card						AB81444C-B0DB-4345-B968-64F99F59A004	Google Chrome v0-40 (Auto-fill Credit Cards v59)	
Credit Card						CEF8B18D-9B37-4194-B5DD-C92A59388A2C	Google Chrome v0-40 (Auto-fill Credit Cards v59)	

Record 2 of 3

[X] [Entry Type] = 'Credit Card' Edit Filter

Information

- Guid: AB81444C-B0DB-4345-B968-64F99F59A004
- Date Modified: 2015-01-28 14:16:22.000
- Origin: Chrome settings

Index Text

credit\_cards  
 Guid: AB81444C-B0DB-4345-B968-64F99F59A004  
 Name on card: Mr G Likley  
 Expiration month: 7  
 Expiration year: 2017  
 Card number encrypted:  
 01000000D08C9DDF0115D1118C7A00C04FC297E80100000090579BCD88CF8E49BC35CDD0E5A4215A8000000002000000000106600000000100002000000038827B4C631B32CC381E78CA2E980EFC8A079EA4C8360982  
 0DE7CD5A799FBF94000000000E80000000020000200000001316C6C6823D49AB50DEC80C857CA6E77FF5C22D94FFFB01031D685F277E950310000000063C18EE76AC2E2E224C19C3B45DEA77C400000007491B443CC2E353824F  
 32AC440FE9523F1C776F869C27A15893A5784DADB3092ADF9C8AB7A8AAACE5A50D15CF4E04200C4C60A5F2AB8BDBE8CA8340DD480A94F2C

www.digital-detective.net | \\digital01\Browser Data Windows\...\Default\Web Data | ID: 2

## 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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [New Case]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Preview URL  
http://uk.ask.com/web?q={searchTerms}

Entry Type	Scheme	Tag	URL	Date Visited [UTC]	Date Visited [Local]
Search Engine		<input type="checkbox"/>	{google:baseURL}search?q={searchTerms}&{google:RLZ}({google:originalQueryForSuggestion})({google:assistedQueryStats})({google:searchFieldtrialPar...		
Search Engine	https	<input type="checkbox"/>	https://www.bing.com/search?setmkt=en-GB&q={searchTerms}		
Search Engine	https	<input type="checkbox"/>	https://uk.search.yahoo.com/search?ei={inputEncoding}&fr=cmas&p={searchTerms}		
Search Engine	http	<input checked="" type="checkbox"/>	http://uk.ask.com/web?q={searchTerms}		
Search Engine	http	<input type="checkbox"/>	http://kryten.digital-detective.hq:8080/secure/QuickSearch.jspa?searchString={searchTerms}		

Record 4 of 5

[X] [Entry Type] = 'Search Engine' Edit Filter

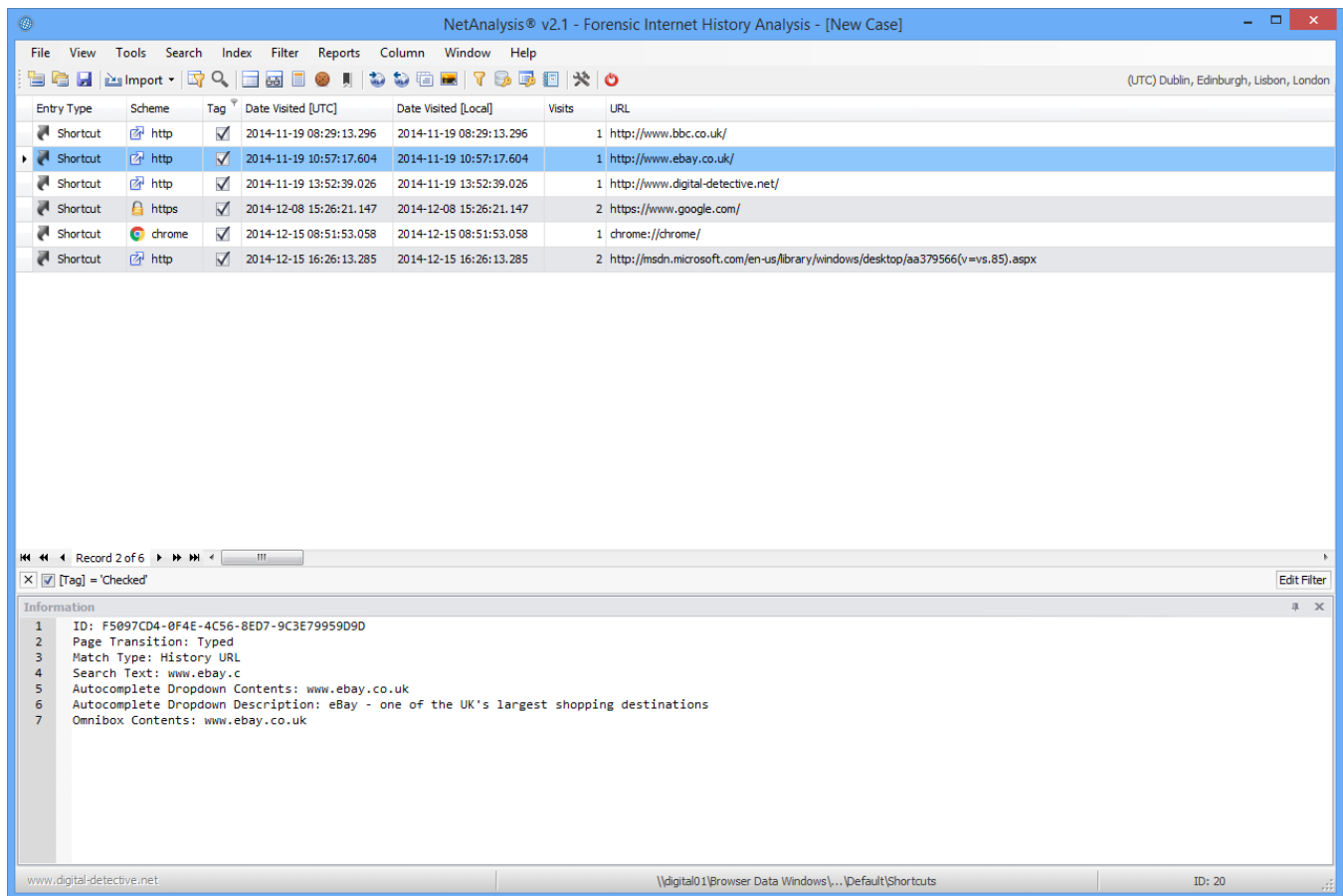
Information

- Short Name: Ask Jeeves
- Keyword: uk.ask.com
- Favicon URL: http://sp.uk.ask.com/sh/i/a16/Favicon/Favicon.ico
- Usage Count: 0
- Input Encodings: UTF-8
- Show in Default List: True
- Suggest URL: http://ss.uk.ask.com/query?q={searchTerms}&li=ff
- Prepopulate ID: 4
- Date Last Modified: 2014-11-19 13:49:01.000
- Sync Guid: E0F9A785-85BC-4268-9166-38F636E1D150
- Alternate URLs: []

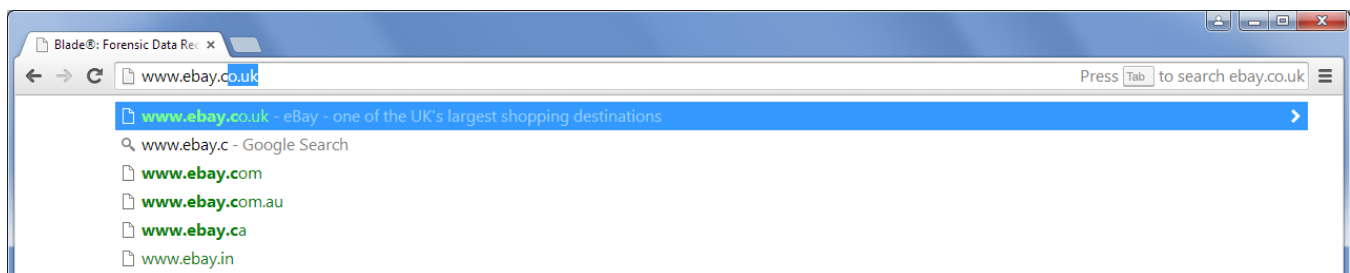
www.digital-detective.net | \\digital01\Browser Data Windows\...\Default\Web Data | ID: 5

## 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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [HDG-4 - Richardson]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Preview URL  
https://www.

Port	User	Logon User	Logon Password	Redirect URL
443		ian.richardson		
443		ian.richardson		
443		ian.richardson@activist.com	28374ydsfsd	
443		ian.richardson		
443		ian.richardson		

Record 3 of 5

[X] [Entry Type] = 'Sign On' Edit Filter

Information

```

1 Master password: <empty>
2 Hostname:
3 Username Field: email
4 Encrypted Username: MD0EEPgAAAAAFAAYIKoZIhvcNAwECOnXd7T+j0rRBCCQpF1MB1N4r6Xd9wx9Mmo5W1DZ1V5Qf+8nDI6B43Dcg==
5 Decrypted Username: ian.richardson@activist.com
6 Password Field: pass
7 Encrypted Password: MD0EEPgAAAAAFAAYIKoZIhvcNAwECaw+kpg5IHUnBBcrbzd2cNuk8ZJD4+uB3ZV
8 Decrypted Password: 28374ydsfsd
9 Date Last Used [UTC]: 2014-05-15 14:53:13.937
10 Date Created [UTC]: 2014-05-14 12:09:54.872
11 Date Password Changed [UTC]: 2014-05-14 12:09:54.872
12 Number of Times Used: 3
13 Encryption Type: 1
14 GUID: {79f2b13f-95c1-4228-8419-2ddcbb5d8d75}

```

www.digital-detective.net C:\Users\Joseph\... \wx4gie7.default\signons.sqlite ID: 3

## 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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [New Case]

(UTC) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Host		<input checked="" type="checkbox"/>				bbc.co.uk
Host		<input checked="" type="checkbox"/>				support.google.com
Host		<input checked="" type="checkbox"/>				translate.google.co.uk
Host		<input checked="" type="checkbox"/>				chromium.org
Input History	http	<input checked="" type="checkbox"/>				http://www.bbc.co.uk/weather/ct13
Input History	https	<input checked="" type="checkbox"/>				https://www.google.co.uk/
Input History	http	<input checked="" type="checkbox"/>				http://www.youtube.com/
Input History	https	<input checked="" type="checkbox"/>				https://www.google.co.uk/

Record 7 of 8

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

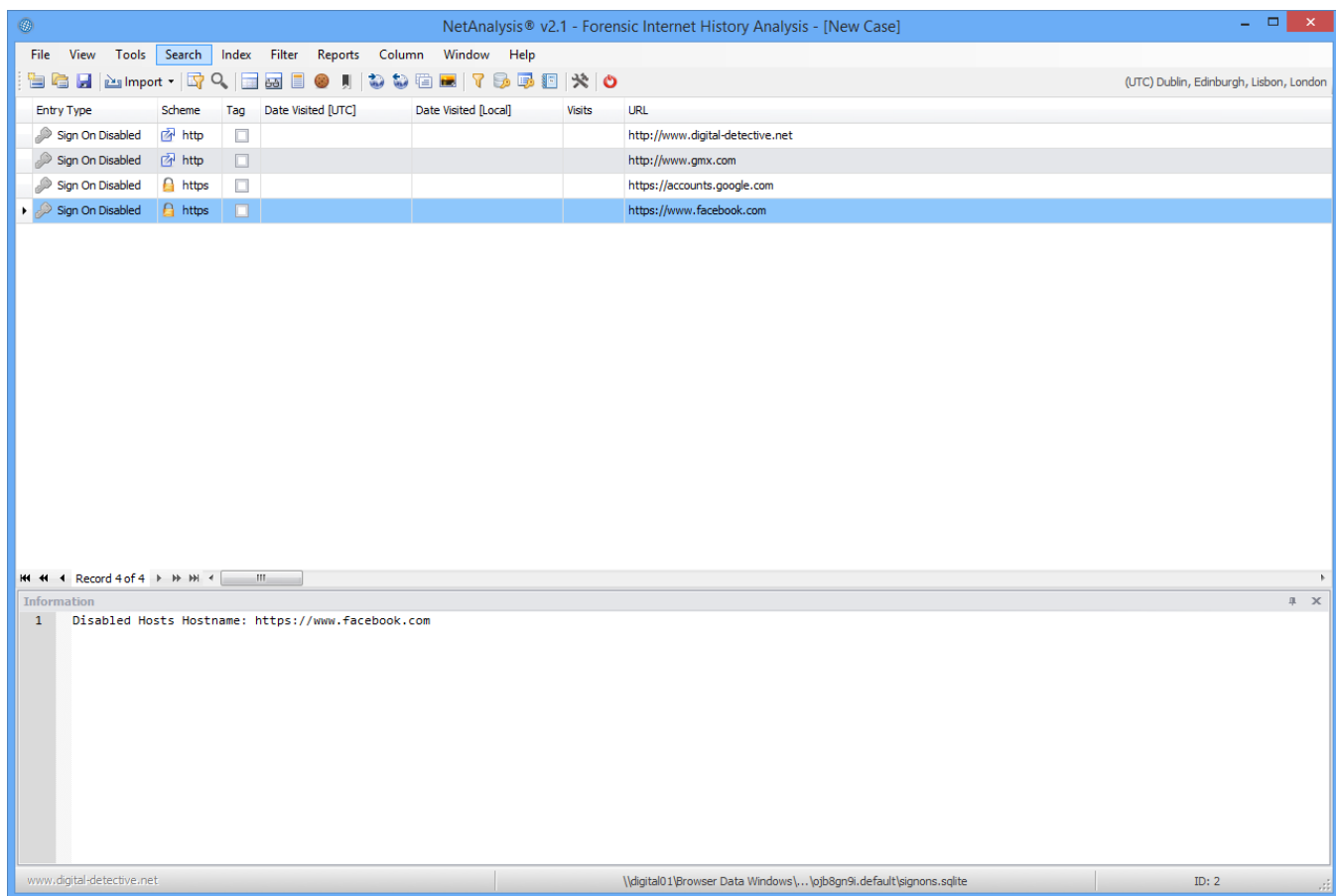
Information

- Input: youtube
- Use Count: 0

www.digital-detective.net | \\digital01\Browser Data Windows\... \w9cv1yzh.default\places.sqlite | ID: 110

## 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.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [New Case]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Preview URL  
http://www.bladeforensics.com/

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Reading List	http	<input type="checkbox"/>				http://www.wikipedia.org/
Reading List	https	<input type="checkbox"/>				https://www.youtube.com/supported_browsers?next_url=%2F
Reading List	http	<input type="checkbox"/>				http://www.digital-detective.net/cgi-bin/digitalboard/YaBB.pl
Reading List	http	<input type="checkbox"/>				http://edition.cnn.com/
Reading List	http	<input checked="" type="checkbox"/>	2015-01-28 08:58:03.000	2015-01-28 08:58:03.000		http://www.bladeforensics.com/
Reading List	https	<input type="checkbox"/>				https://uk.yahoo.com/?p=us
Reading List	http	<input type="checkbox"/>				http://www.bbc.co.uk/
Reading List	http	<input type="checkbox"/>				http://www.digital-detective.net/

Record 5 of 8

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

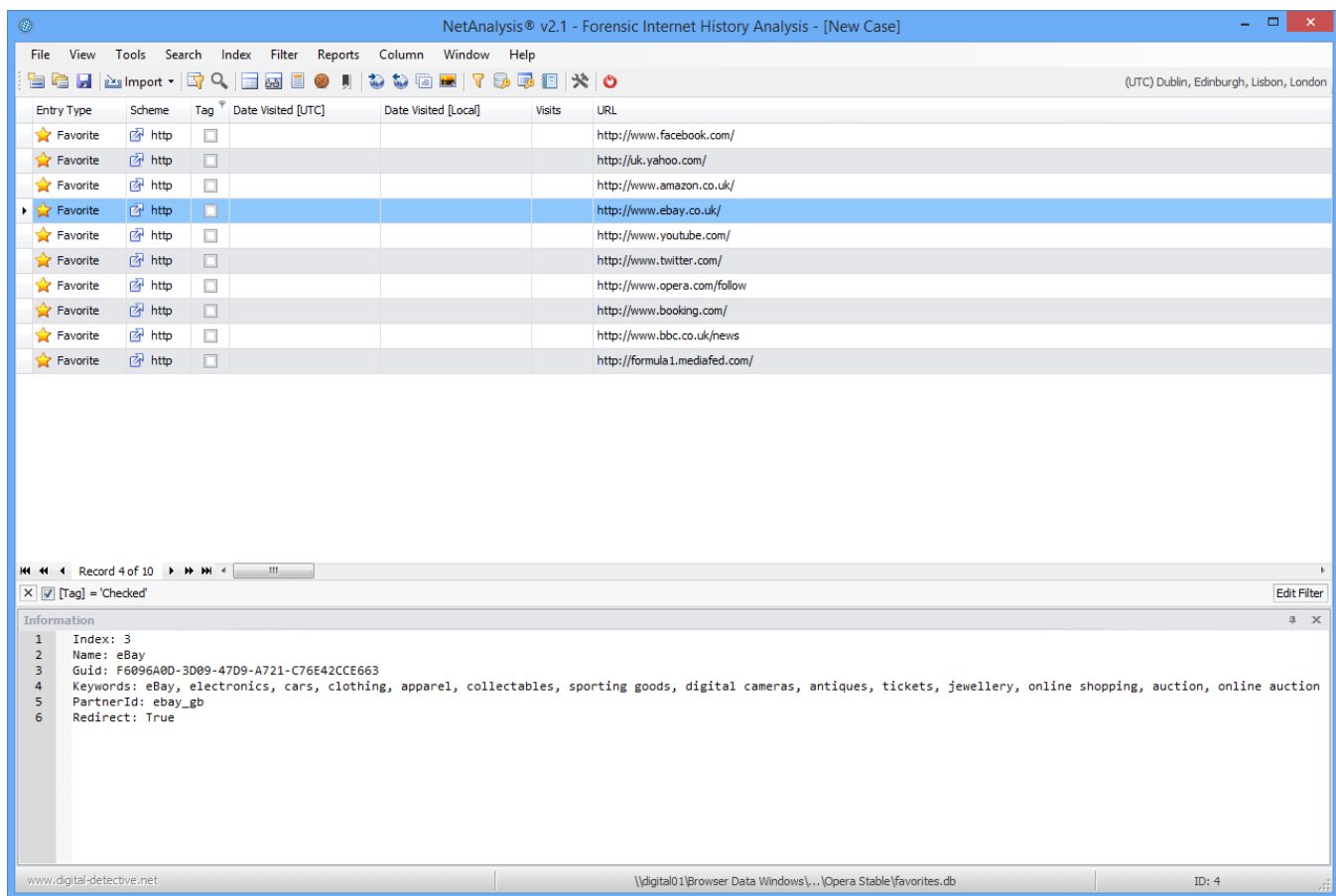
Information

- Web Bookmark UUID: 2EB4612B-3447-2040-B4AC-6008C50F6959
- Date Last Fetched: 2015-01-28 08:56:59.000
- Date Last Viewed: 2015-01-28 08:58:03.000
- Root Web Bookmark UUID: 0B4B5B1A-4152-FC48-AD35-924C1C9BF316
- Root Title: com.apple.ReadingList
- Root Web Bookmark File Version: 1

www.digital-detective.net | \\digital01\Browser Data Windows\...\Safari\ReadingList.plist | ID: 5

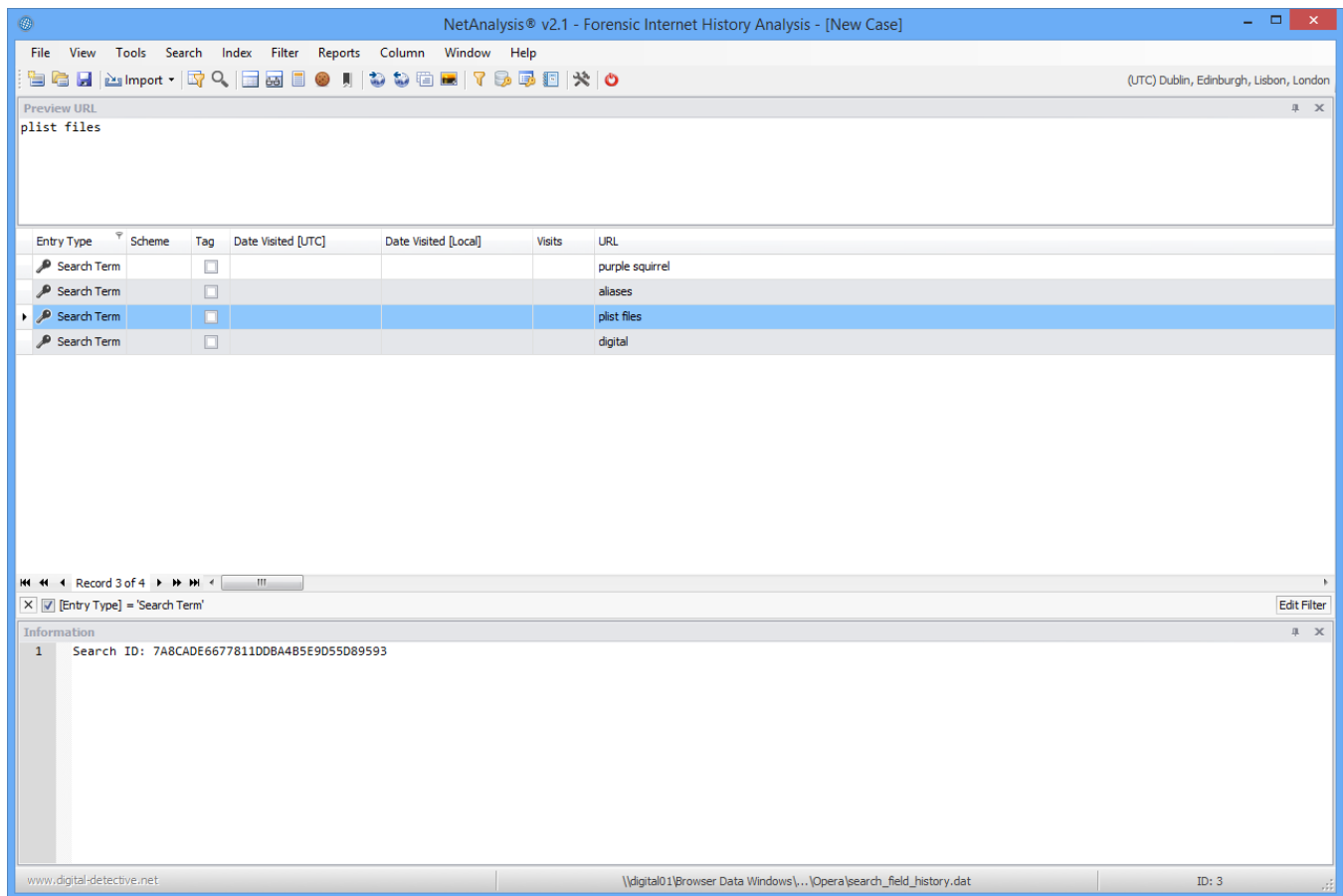
## Opera Blink Favorite Entries

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](#)