

What's New in Version 2



NetAnalysis[®]

Evidence you can trust

What's new in NetAnalysis® v2



Introduction

The primary goal of Digital Detective Group is to develop innovative new technologies that offer significant improvements over existing applications and methodologies. We focus our efforts on areas where science presents new opportunities most likely to lead to significant forensic advances.

We aim to build upon our reputation as a pioneer in the field of digital forensic science and are committed to developing leading products that will advance our mission to make the world a safer place through digital forensic expertise.

Research and development is a key element to developing advanced, cutting-edge technology. Our team works to solve the challenges that exist in the highly dynamic, hi-tech world of digital forensics.

We aim to create new knowledge about scientific and technological topics for the purpose of uncovering and enabling development of valuable new products, processes, and services.

NetAnalysis®

Through a significant investment in research and development, we have authored a completely new groundbreaking product, engineered through innovation and fresh thinking.

NetAnalysis® v2 is a state-of-the-art application for the extraction, analysis and presentation of forensic evidence relating to Internet browser and user activity on computer systems and mobile devices. It is a software product that offers significant improvements over existing applications and methodologies.

We support more web-browser artefacts than any other forensic tool.

Browser Support



We have added support for the latest browsers and currently support:

- 360 Browser v7
- 360 Security Browser v3 - 10
- 360 Speed Browser v4 - 11
- AOL Desktop Browser v9
- Apple Safari v3 - 13
- Avast Secure Browser v64 - 81
- AVG Secure Browser v75 - 81
- Basilisk v2017.11.12 - 2020.05.08
- Blisk v0 - 12
- Brave v0 - 1
- CCleaner Browser v75 - 81
- Chromium v1 - 83
- Cốc Cốc v26 - 86
- Comodo Chromodo v36 - 52
- Comodo Dragon v4 - 80
- Comodo IceDragon v13 - 65
- CoolNovo v1 - 2
- Cyberfox v17 - 52
- Epic Privacy Browser v29 - 80
- Flock v0 - 3
- Google Chrome v0 - 83
- IceCat v1 - 52
- K-Meleon v1 - 76
- Microsoft Edge v20 - 44
- Microsoft Edge (Chromium) v74 - 83
- Microsoft Internet Explorer v3
- Microsoft Internet Explorer v4
- Microsoft Internet Explorer v5 - 9
- Microsoft Internet Explorer v10 - 11
- Microsoft Internet Explorer XBOX
- Min Browser v0 - 1
- Mozilla Firefox v1 - 77
- Netscape v6 - 9
- Opera v15 - 68
- Opera GX v60 - 68
- Opera Neon v1
- Opera (Presto) v3 - 12
- Pale Moon v3 - 28
- QQ Browser (Windows) v9 - 10
- SeaMonkey v1 - 2
- Sleipnir (Windows) v3 - 6
- Sleipnir (OS X) v3 - 4
- SRWare Iron v1 - 81
- Titan Browser v1 - 33
- Torch v1 - 69
- UC Browser v4 - 7
- Vivaldi v1 - 3
- Waterfox v4 - 2020.05
- Wyzo v0 - 3
- Yandex v1 - 20
- Other Chromium Based Browsers
- Other Mozilla Based Browsers

Database

NetAnalysis® utilises a powerful transactional SQL database where imported data is held and analysed. Two different databases are currently supported, SQLite and MySQL.



SQLite is a self-contained, serverless, zero-configuration, transactional SQL database engine. It is extremely powerful and is integrated with NetAnalysis® as our default desktop database. It is very fast and can deal with workspace files containing many millions of records. The data is located in a single self-contained file which can easily be shared with other users.

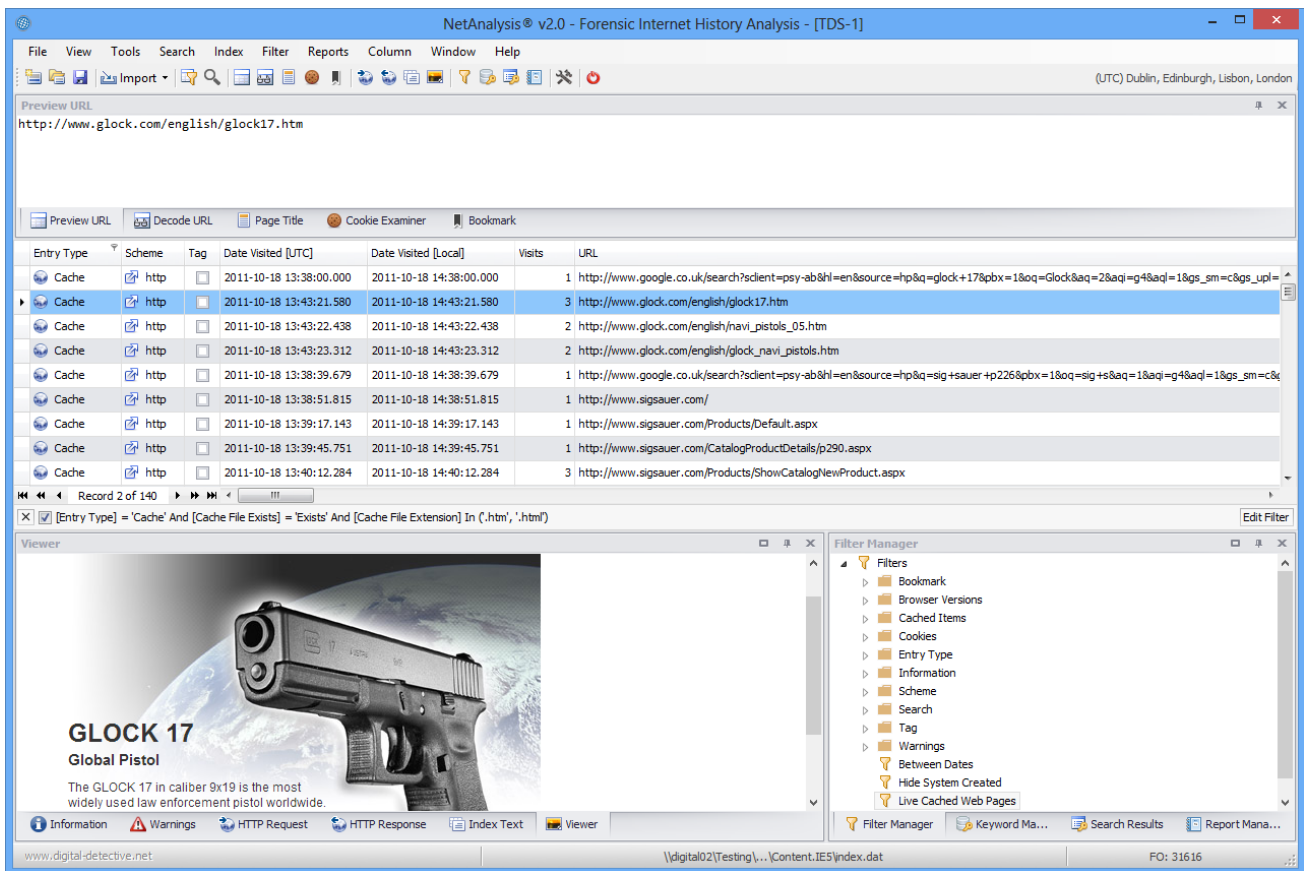


MySQL is the world's most popular, open source, relational database management system. It is developed, distributed, and supported by Oracle Corporation. This high-end solution is easy to use, includes solid data security layers that protects sensitive data as well as being scalable. It can handle almost any amount of data and offers a unique opportunity for collaborative analysis.

User Interface

NetAnalysis® v2 has a completely new user interface that has been designed to make the work of the forensic analyst easier and more productive. It is intuitive, easy to use and will be instantly familiar to previous users of our software.

The main components of the interface are contained within dockable panels which are fully customisable. Layouts can also be saved and reloaded.



The screen above shows NetAnalysis® v2 with some docking panels visible.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	http		2011-10-19 08:43:17.516	2011-10-19 09:43:17.516	1	http://www.filehippo.com/download/file/7c901f85c49c87452fc81477d80a0ae9381ac5fcc64a90109c98583035d5f14b/
Leak			2011-10-19 08:43:18.000	2011-10-19 09:43:18.000	0	*ccsetup311.exe
Cookie			2011-10-19 08:43:39.216	2011-10-19 09:43:39.216	45	Cookies:victor bushell@cnet.com/
Master	http		2011-10-19 08:43:46.376	2011-10-19 09:43:46.376	1	http://www.piriform.com/ccleaner/download
Cache	http		2011-10-19 08:44:06.298	2011-10-19 09:44:06.298	2	http://www.bing.com/imagenevfetcher.aspx?q=http%3a%2f%2fwww.ghacks.net%2fwp-content%2fuploads%2f2011%2f10%2fwpive-2011
Daily	http		2011-10-19 08:44:06.313	2011-10-19 11:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IEBSRC
Master	http		2011-10-19 08:44:06.313	2011-10-19 09:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IEBSRC
Cache	http		2011-10-19 08:44:06.313	2011-10-19 09:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IEBSRC
Cache	http		2011-10-19 08:44:07.370	2011-10-19 09:44:07.370	6	http://www.bing.com/sa/0824002445/answerAll2_c.css
Leak			2011-10-19 08:44:12.000	2011-10-19 09:44:12.000	0	*How%20to%20Use%20CCleaner.pdf
Master	file		2011-10-19 08:44:16.215	2011-10-19 09:44:16.215	1	file:///C:/Users/Victor%20Bushell/Desktop/How%20to%20Use%20CCleaner.pdf
Daily	file		2011-10-19 08:44:16.215	2011-10-19 11:44:16.215	1	file:///C:/Users/Victor%20Bushell/Desktop/How%20to%20Use%20CCleaner.pdf
Daily	host		2011-10-19 08:44:16.215	2011-10-19 11:44:16.215	1	Host: Computer
Cache	http		2011-10-19 08:44:29.054	2011-10-19 09:44:29.054	1	http://www.bing.com/captioniHandler.aspx?IG=36d1545b7d234cc08dbe9ff9b4ef32b48pu=http%3a%2f%2fwww.mangocomp.com%2fAsse
Master	http		2011-10-19 08:44:37.088	2011-10-19 09:44:37.088	1	file:///C:/Users/Victor%20Bushell/Desktop/CCleaner_Disk_File_Cleanup.pdf
Daily	file		2011-10-19 08:44:37.088	2011-10-19 11:44:37.088	1	file:///C:/Users/Victor%20Bushell/Desktop/CCleaner_Disk_File_Cleanup.pdf
Download	http		2011-10-19 08:44:37.837	2011-10-19 09:44:37.837	1	http://www.freewebs.com/reliantpc/Docs/How%20to%20Use%20CCleaner.pdf
Download	http		2011-10-19 08:44:38.024	2011-10-19 09:44:38.024	1	http://mlcug.org/CCleaner_Disk_File_Cleanup.pdf
Master	http		2011-10-19 08:45:02.095	2011-10-19 09:45:02.095	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IEBSRC
Cache	http		2011-10-19 08:45:06.946	2011-10-19 09:45:06.946	1	http://www.bing.com/td/sa/7_09_0_1095051/AutoSug.js
Cache	http		2011-10-19 08:45:08.132	2011-10-19 09:45:08.132	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=d&cp=1&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:08.210	2011-10-19 09:45:08.210	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=d&cp=2&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:08.444	2011-10-19 09:45:08.444	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=4&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:08.537	2011-10-19 09:45:08.537	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=4&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:08.803	2011-10-19 09:45:08.803	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=6&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:08.896	2011-10-19 09:45:08.896	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=7&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:09.021	2011-10-19 09:45:09.021	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=7&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:09.224	2011-10-19 09:45:09.224	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=9&sid=72DB06C79E18429F8C2B666
Cache	http		2011-10-19 08:45:09.317	2011-10-19 09:45:09.317	1	http://db3.api.bing.com/qsonhs.aspx?FORM=ASAPIW&mkt=en-GB&type=cb&cb=sa_inst.apiCB&q=dow&cp=9&sid=72DB06C79E18429F8C2B666

The screen above shows the traditional NetAnalysis® layout.

Preview URL
http://www.youtube.com/watch?v=8Et7gJ6SAaM

Page Title

Index Text
RAVE in swansea 2008 - YouTube

Cookies help us deliver our services. By using our services, you agree to our use of cookies. Learn more Got it

GB

Upload Sign in Search

Preview URL Decode URL Cookie Examiner

Date Visited [UTC]	Date Visited [Local]	Visits
2014-05-15 14:42:47.000	2014-05-15 15:42:47.000	

Using drag-and-drop, the user can dock any panel to any edge of a parent container or to other dock panels, or make any panel float over other controls. Panels can also be extracted and viewed in a second monitor if desired.

NetAnalysis® v2.0 - Forensic Internet History Analysis - [TDS-1]

(UTC) Dublin, Edinburgh, Lisbon, London

Bookmark

Cookie Examiner

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	http		2011-10-19 08:43:17.516	2011-10-19 09:43:17.516	1	http://www.filehippo.com/download/file/7c901f85c49c87452fc81477d80a0ae9381ac5fcc64e90109c98583035d5f14b/
Leak			2011-10-19 08:43:18.000	2011-10-19 09:43:18.000	0	%ccsetup311.exe
Cookie			2011-10-19 08:43:39.216	2011-10-19 09:43:39.216	45	Cookie: victor_bushell@cnet.com/
Master	http		2011-10-19 08:43:46.376	2011-10-19 09:43:46.376	1	http://www.piriform.com/cleaner/download
Cache	http		2011-10-19 08:44:06.298	2011-10-19 09:44:06.298	2	http://www.bing.com/imagewebfetcher.aspx?q=http%3a%2f%2fwww.ghacks.net%2fwp-content%2fuploads%2f2011%2f10%2fwipe-2011
Cache	http		2011-10-19 08:44:06.313	2011-10-19 11:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IE8SRC
Master	http		2011-10-19 08:44:06.313	2011-10-19 09:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IE8SRC
Cache	http		2011-10-19 08:44:06.313	2011-10-19 09:44:06.313	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IE8SRC
Cache	http		2011-10-19 08:44:07.370	2011-10-19 09:44:07.370	6	http://www.100m.com/1824002445/answerAll2_c.css
Leak						Decode URL http://www.glock.com/english/glock17.htm
Master	file					Cleaner.pdf
Daily	file					el/Desktop/How%20to%20Use%20CCleaner.pdf
Daily	host					ushell/Desktop/How%20to%20Use%20CCleaner.pdf
Cache	http					andler.aspx?IG=36d1545b7d23cc08dbe9ff9b4ef32b48pu=http%3A%2F%2Fwww.mangocomp.com%2FAsses
Master	file					el/Desktop/CCleaner_Disk_File_Cleanup.pdf
Daily	file					ushell/Desktop/CCleaner_Disk_File_Cleanup.pdf
Download	http					antpc/Docs/How%20to%20Use%20CCleaner.pdf
Download	http		2011-10-19 08:44:38.024	2011-10-19 09:44:38.024		http://mfcug.org/CCleaner_Disk_File_Cleanup.pdf
Master	http		2011-10-19 08:45:02.095	2011-10-19 09:45:02.095	1	http://www.bing.com/search?q=cleaner+filetype%3Apdf&FORM=IE8SRC
Cache	http		2011-10-19 08:45:06.946	2011-10-19 09:45:06.946	1	http://www.100m.com/1824002445/answerAll2_c.css
Cache	http		2011-10-19 08:45:08.132	2011-10-19 09:45:08.132	1	http://db3.alicdn.com/assonhs.aspx?FORM=ASAPIW&mkt=en-GB&vpe=cb&cb=sa_inst.aotCB8a=d&co=1&sid=72DB06C79E18429F8C2B6B6

www.digital-detective.net

\\digital02[Testing]...Content.IE5\index.dat

FO: 31616

HTTP Response

```

1 HTTP/1.1 200 OK
2 P3P: policyref="http://googleads.g.doubleclick.net/pagead/gcn_p3p.xml", CP="CURa ADMa DEVa TAIo PSAo PSDO
  OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
3 Content-Type: image/gif
4 X-Content-Type-Options: nosniff
5 Content-Length: 38789
6 X-XSS-Protection: 1; mode=block

```

Information Warnings HTTP Request HTTP Response Index Text Viewer

When panels are docked together, they are available through tabs. All panels can be closed and opened as required.

The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main window shows a table of cache files with the following columns: Cache Folder, Cache File, Cache File Extension, Cache File Length, Cache File Exists, Date HTTP Response [UTC], Date HTTP Last Modified [UTC], and HTTP Request. The selected row is for a file named '_CACHE_001_.json' with a length of 648 bytes, last modified on 2014-05-15 at 11:21:53.000 UTC, and a GET request with Accept-Encoding: gzip, deflate.

Cache Folder	Cache File	Cache File Extension	Cache File Length	Cache File Exists	Date HTTP Response [UTC]	Date HTTP Last Modified [UTC]	HTTP Request
	_CACHE_001_	.jpg	313	✓	2014-05-15 11:21:38.000	2010-05-28 14:03:31.000	GET Accept-Encoding: gzip, deflate
5 7B	13E21d01	.js	4074	✓	2014-05-15 11:21:44.000	2014-05-13 23:30:26.000	GET Accept-Encoding: gzip, deflate
5 94	735E1d01	.js	64327	✓	2014-05-15 11:21:44.000	2014-05-13 23:30:24.000	GET Accept-Encoding: gzip, deflate
	_CACHE_001_	.json	648	✓	2014-05-15 11:21:53.000		GET Accept-Encoding: gzip, deflate
	_CACHE_002_	.json	2038	✓	2014-05-15 11:21:53.000		GET Accept-Encoding: gzip, deflate
2 C4	B8621d01	.js	5944	✓	2014-05-15 11:21:55.000		GET
	_CACHE_002_	.jpg	1469	✓	2014-05-15 11:22:32.000	2014-05-10 17:48:52.000	GET
	_CACHE_003_	.htm	3094	✓	2014-05-15 11:22:37.000		GET Accept-Encoding: gzip, deflate
	_CACHE_002_	.htm	1358	✓	2014-05-15 11:22:37.000	2013-08-13 08:30:33.000	GET
	_CACHE_001_	.gif	298	✓	2014-05-15 11:31:07.000	2012-12-10 17:38:52.000	GET
	_CACHE_003_	.jpg	11488	✓	2014-05-15 11:22:42.000	2012-10-11 08:00:09.000	GET
	_CACHE_003_	.png	9818	✓	2014-05-15 11:22:43.000		GET
	_CACHE_002_	.ico	1150	✓	2014-05-15 11:22:44.000	2013-06-29 23:16:44.000	GET
	_CACHE_002_	.png	944	✓	2014-05-15 11:22:51.000	2013-06-29 23:16:57.000	GET

The docked panels show the following details for the selected record:

HTTP Response:

```

1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Content-Encoding: gzip
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/8.0
6 X-BM-TraceID: 017baa25bf57414cb7cb0ddda62e2843
7 X-VE-TFE: DB30031008
8 X-BM-Srv: DB30031008
9 X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11 Content-Length: 648
12 Cache-Control: public, max-age=31434676
13 Expires: Thu, 14 May 2015 07:13:09 GMT
14 Date: Thu, 15 May 2014 11:21:53 GMT

```

HTTP Request:

```

1 GET
2 Accept-Encoding: gzip, deflate

```

NetAnalysis® v2 showing cache information and HTTP request and response data in the docking panels.

The screenshot displays the NetAnalysis v2.1 interface with a 'Time Zone Information' dialog box open. The dialog box shows the following parameters for the time zone (UTC) Dublin, Edinburgh, Lisbon, London:

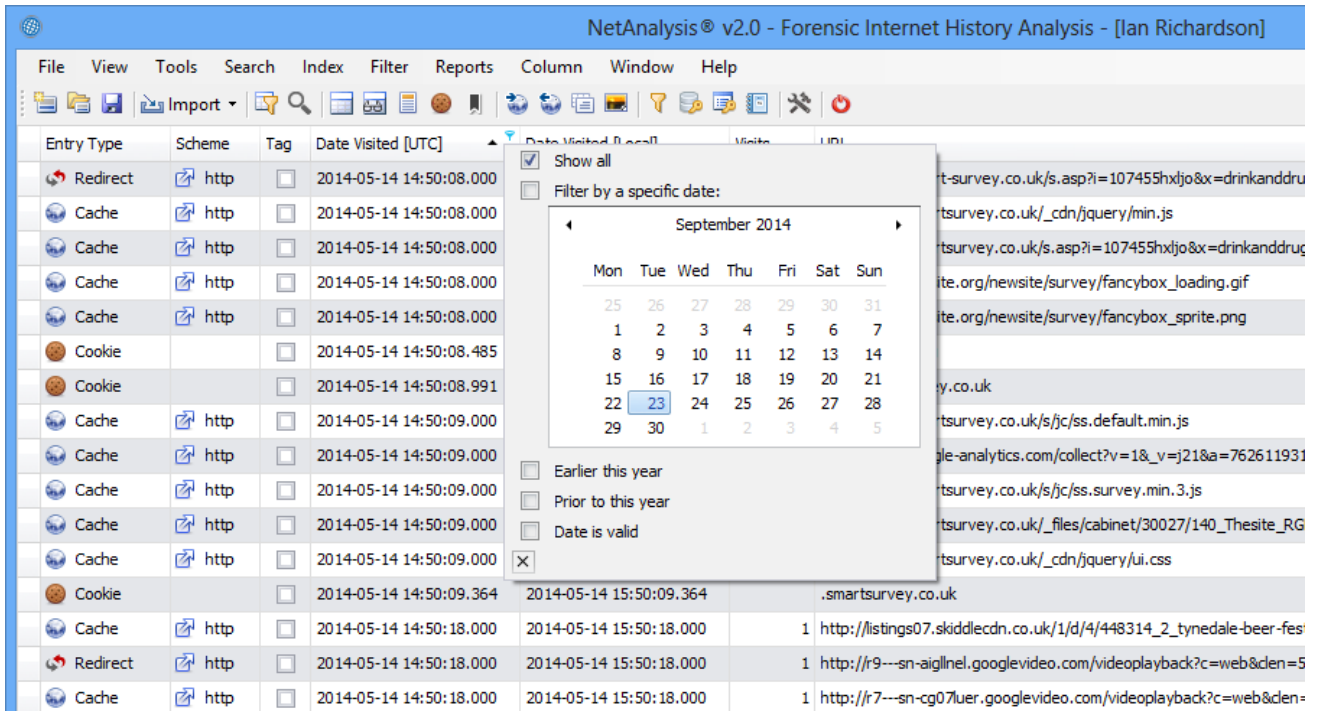
Name	Value
Base UTC Offset	00:00:00
Display Name	(UTC) Dublin, Edinburgh, Lisbon, London
Standard Name	GMT Standard Time
Daylight Name	GMT Summer Time
Has Daylight Saving	True
0001 to 9999	
Daylight Bias	01:00:00
Start	01:00 on Sunday of week 5 in March
End	02:00 on Sunday of week 5 in October

The background interface shows a list of cache entries with columns for Entry Type, Scheme, Tag, and Date Visited. The selected entry is a cache record for an HTTP request to a Microsoft Maps API endpoint. Below the list, the HTTP response details are visible, including status (200 OK), content type (application/json), and various headers like Server, X-TraceID, and X-VE-TFE.

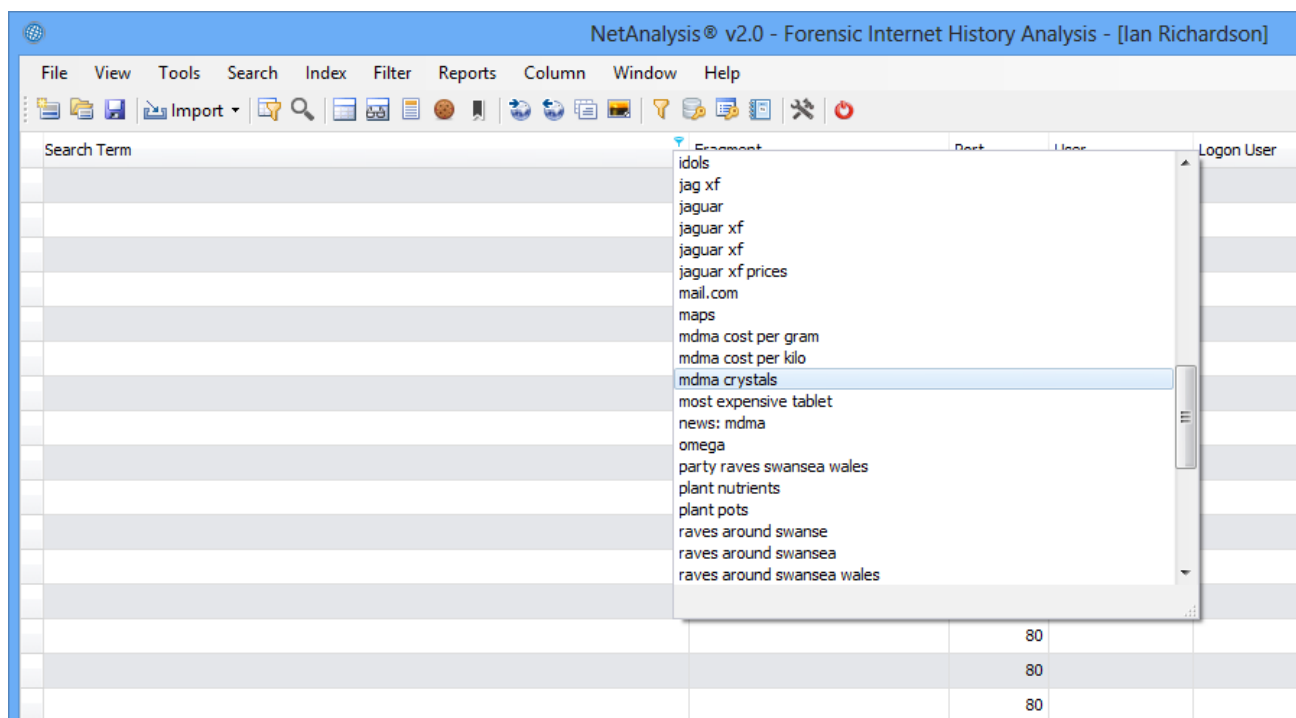
The above screen shows the Time Zone information window with a breakdown of Time Zone Parameters and Dynamic DST Information.

Filtering and Searching

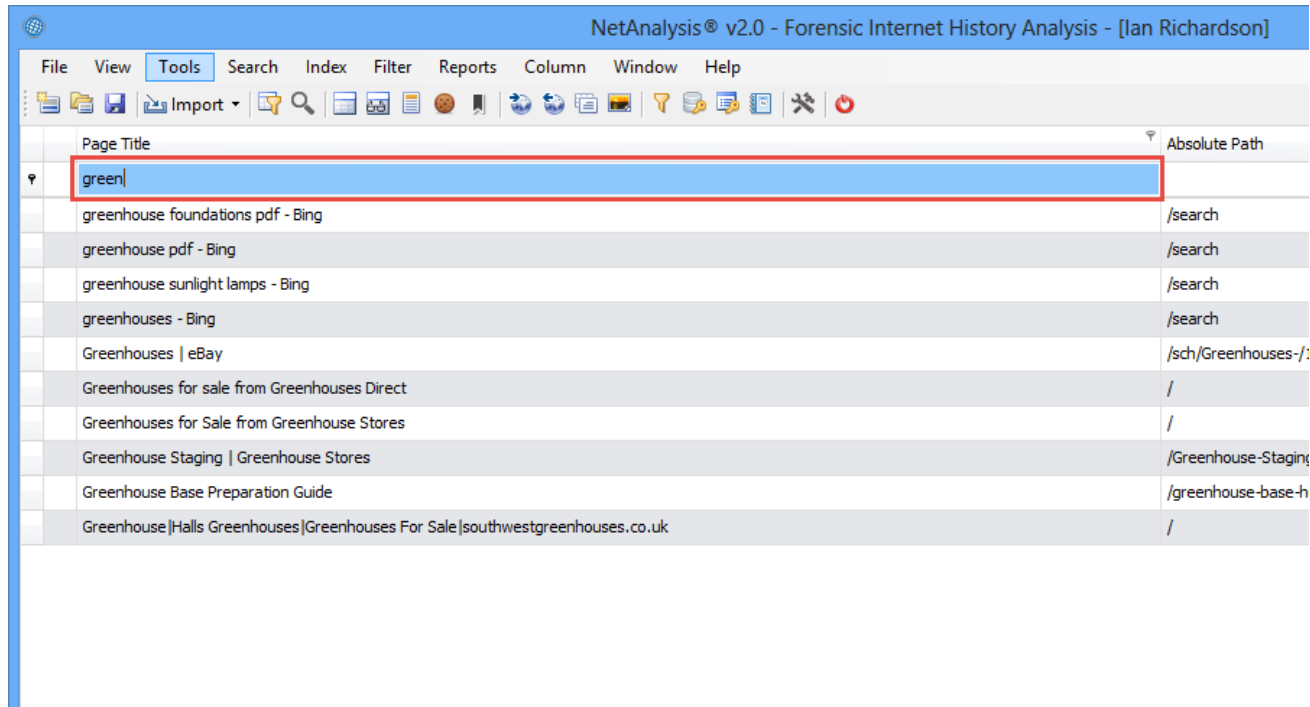
The filtering and searching capabilities have been considerably enhanced. The user can filter records via column filters, the auto-filter row, filter editor, filter manager and quick search panel. The filter manager allows the user to store, order and configure any number of filters.



Each column header has a small filter icon; clicking on this icon allows the user to select filter criteria for that column. In the case above, the user has selected a date filter.



In the screen above, the user has selected a column filter for the Search Term column, if a specific term is selected, all the records which contained that search term will be filtered.



The auto-filter row, when activated, appears under the column header. This allows the user to filter rows based on the search string. In the example above, the user is searching for Page Titles which start with the text "green".

NetAnalysis® v2.0 - Forensic Internet History Analysis - [Ian Richardson]

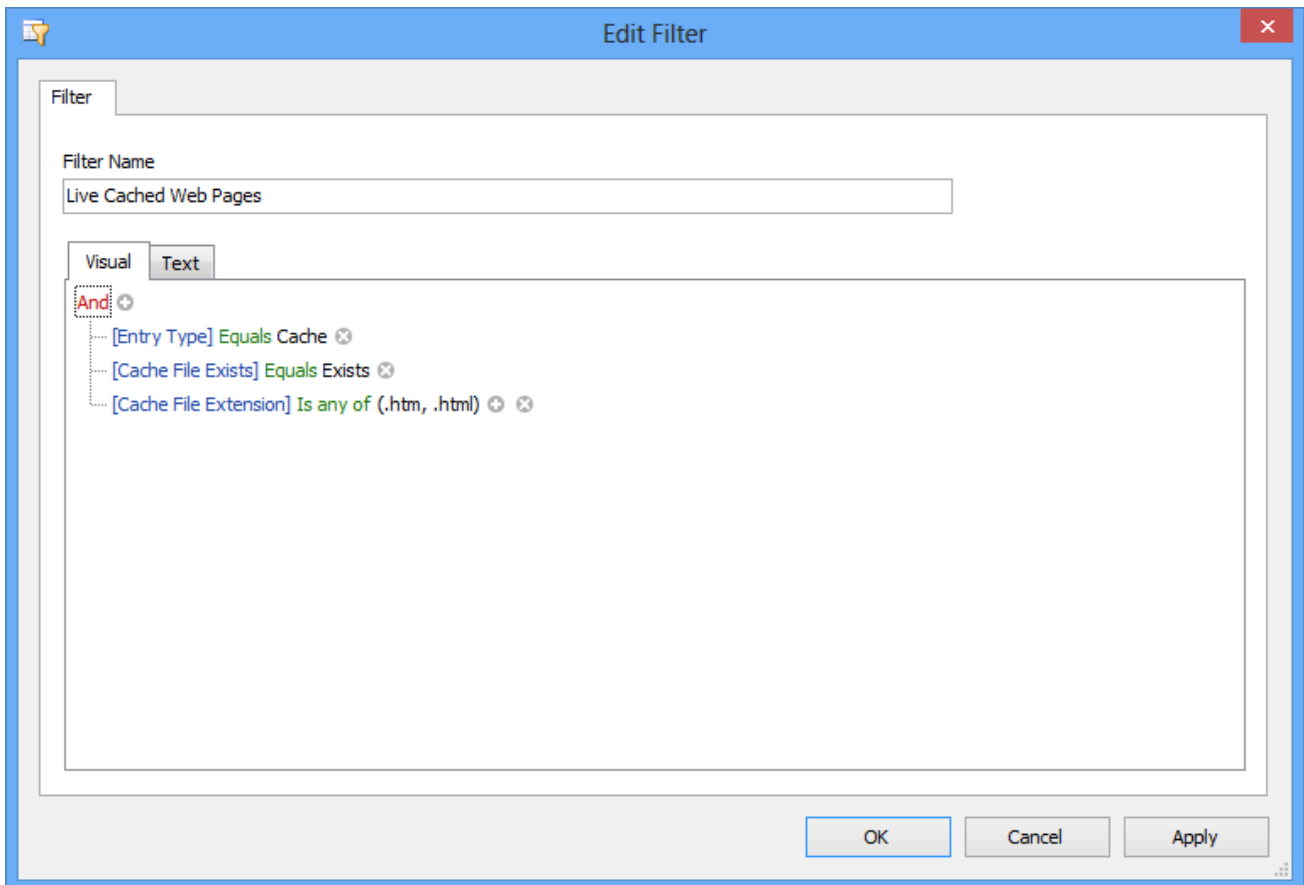
File View Tools Search Index Filter Reports Column Window Help

Import Find Clear

X google

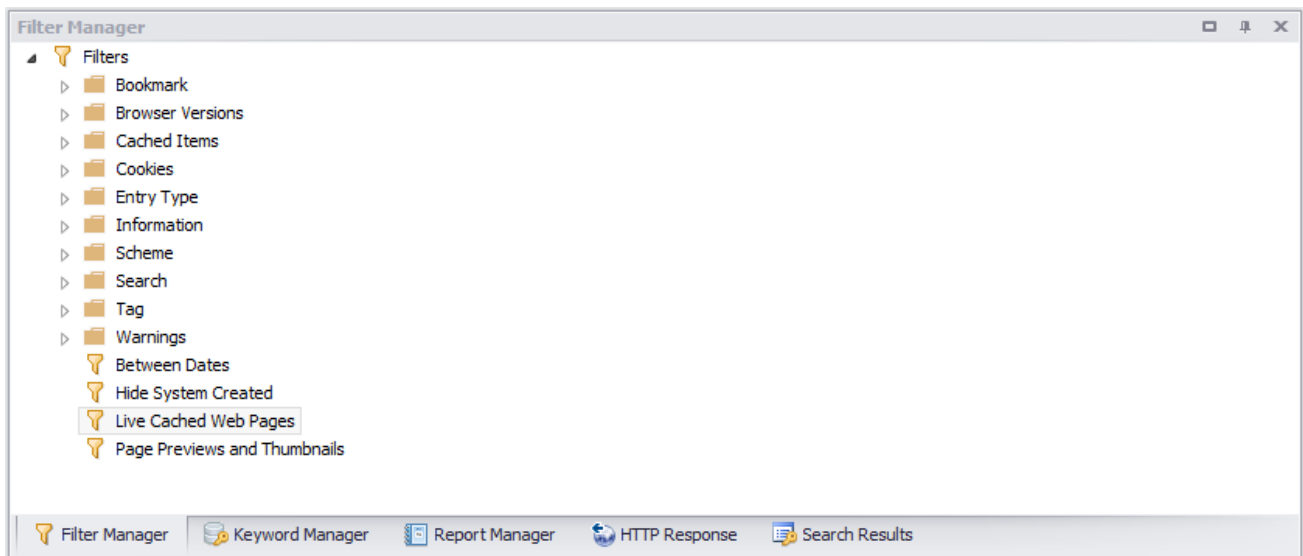
Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cookie		<input type="checkbox"/>	2014-05-21 11:17:32.282	2014-05-21 12:17:32.282		.google.com
Cache	https	<input type="checkbox"/>	2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	58	https://apis.google.com/js/plusone.js
Cache	https	<input type="checkbox"/>	2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	17	https://apis.google.com/js/api.js
Cache	http	<input type="checkbox"/>	2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	38	http://www.google-analytics.com/analytics.js
Cache	http	<input type="checkbox"/>	2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	1	http://www.google-analytics.com/collect?v=1&_v=j21&a=933818&t=
Cache	https	<input type="checkbox"/>	2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	28	https://oauth.googleusercontent.com/gadgets/js/core:rpc:shindig.rar
Cache	http	<input type="checkbox"/>	2014-05-21 11:15:03.000	2014-05-21 12:15:03.000	1	http://www.google-analytics.com/_utm.gif?utmwv=5.5.1&utms=1&
Cache	http	<input type="checkbox"/>	2014-05-21 11:15:02.000	2014-05-21 12:15:02.000	142	http://www.google-analytics.com/ga.js
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:59.000	2014-05-21 12:14:59.000	1	http://ajax.googleapis.com/ajax/libs/jquery/1.2.6/jquery.min.js
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:56.000	2014-05-21 12:14:56.000	1	http://ad.uk.doubleclick.net/N4215/adj/amzn.uk.sr.aps;sz=160x600;
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:56.000	2014-05-21 12:14:56.000	1	http://www.google-analytics.com/_utm.gif?utmwv=1.4&utm=1382
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	10	http://www.google-analytics.com/urchin.js
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	1	http://pubads.g.doubleclick.net/activity;dc_u=/7369/nreaudience;df
Cache	http	<input type="checkbox"/>	2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	1	http://ad.doubleclick.net/activity;src=3401595;dcnet=7194;boom=6

In the example above, the user has searched for the text “google” across all rows and columns. NetAnalysis® automatically filters and highlights the hits so the user can easily review the matches.

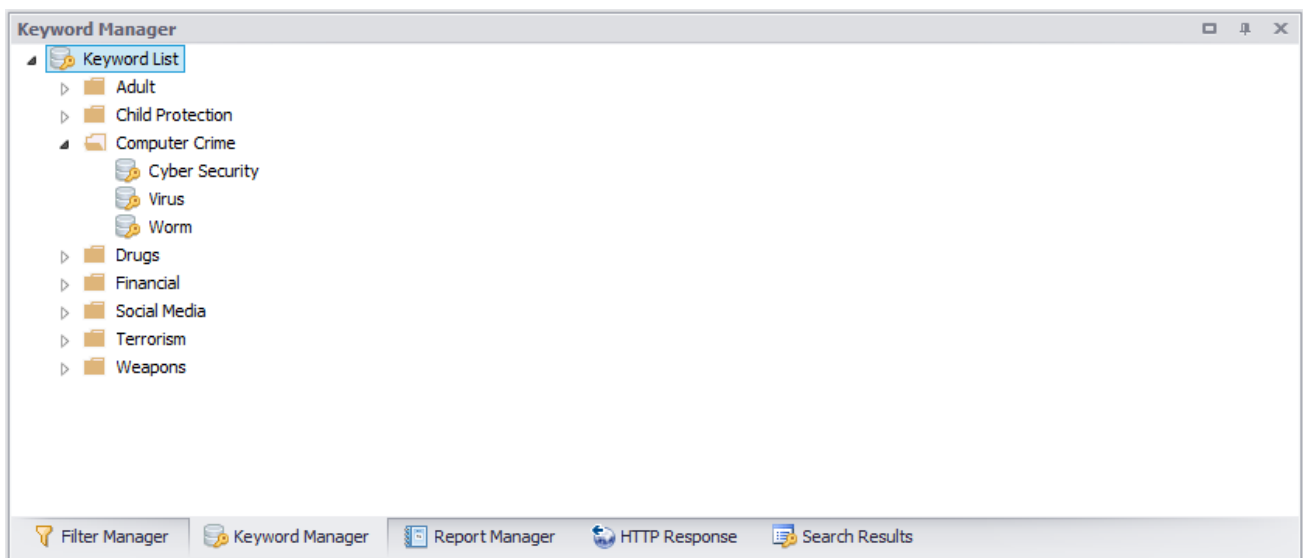


The visual filter editor is extremely powerful and makes it a simple task for the user to build complex queries

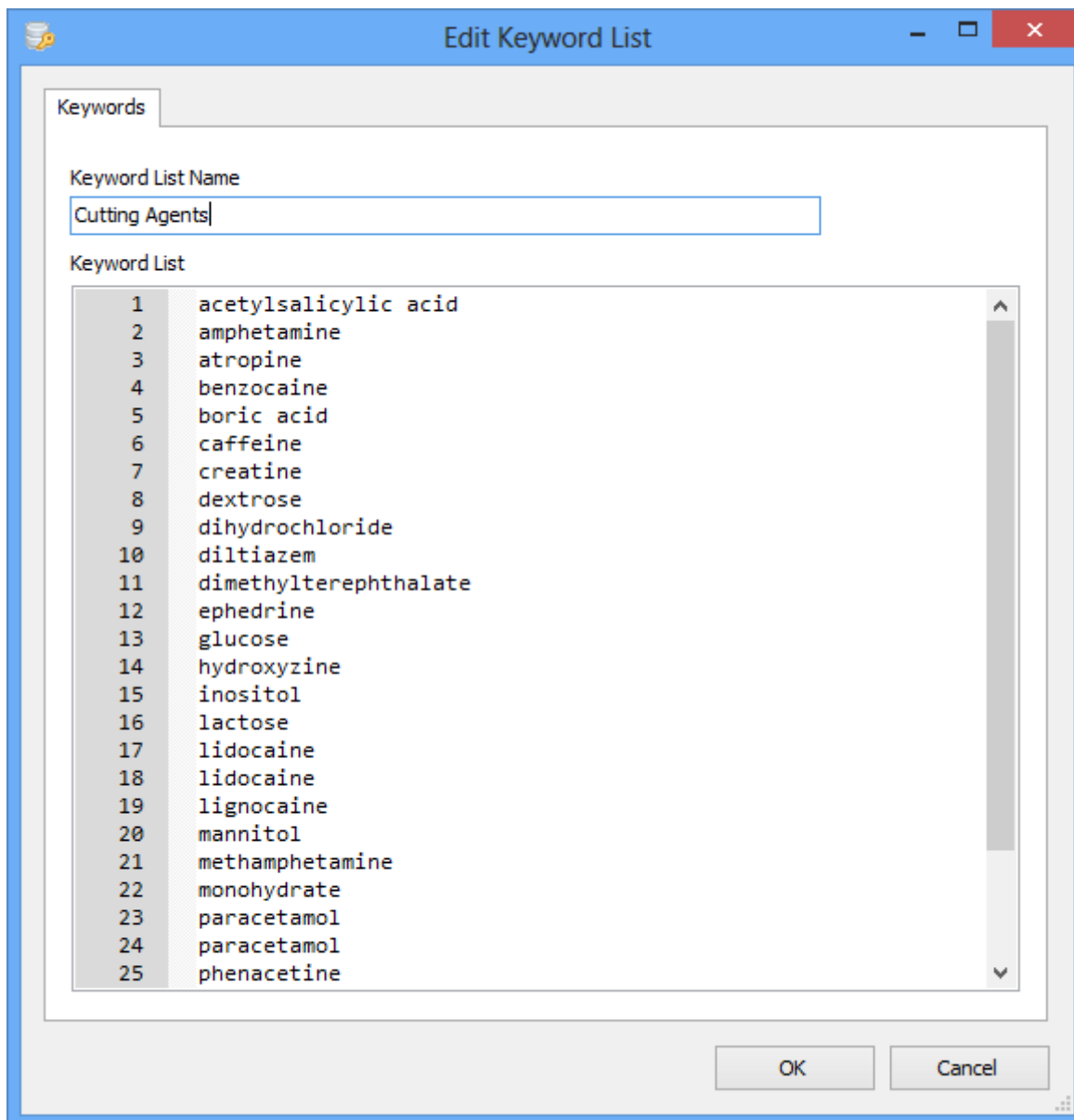
which can be saved for later re-use. The user no longer has to have an understanding of SQL to create powerful queries.



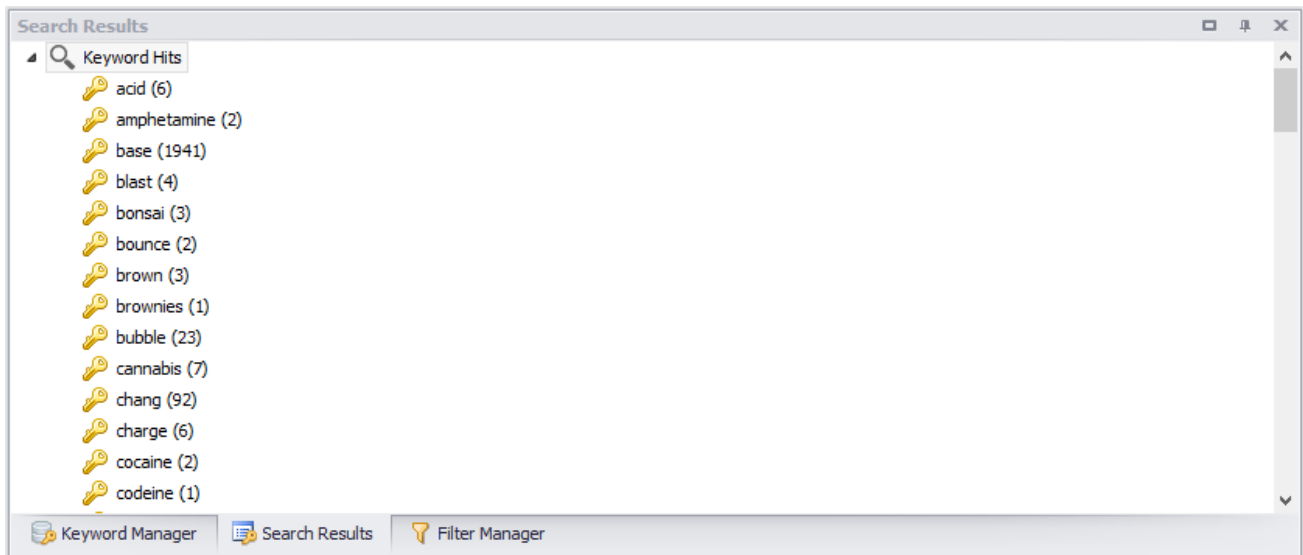
The filter manager is located in a docking panel and allows the user to easily create, edit, save and categorise all the filters they would need during a forensic investigation.



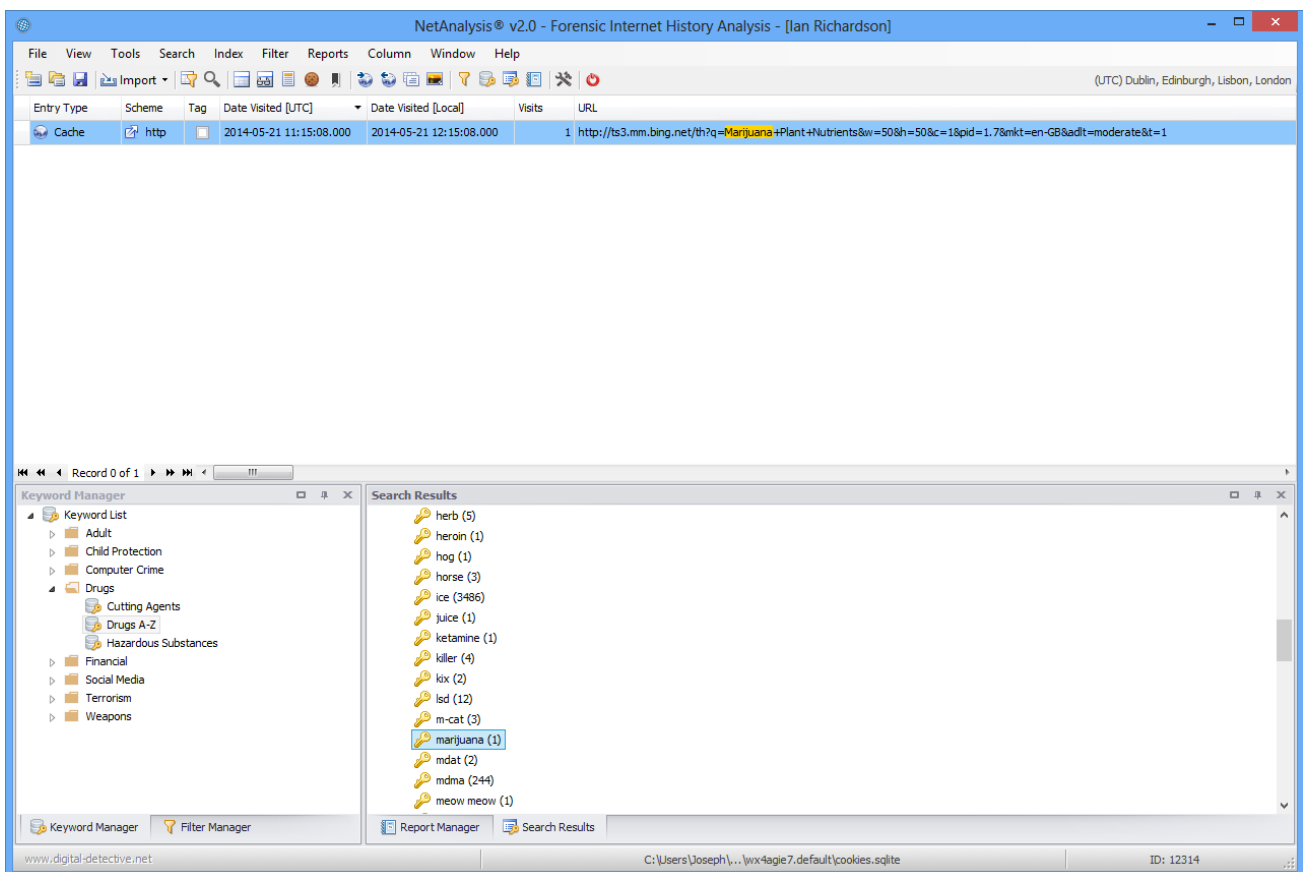
The keyword manager is also located in a docking panel and allows the user to create, edit, save and categorise lists of keywords that can be searched against imported data. Keywords can be easily shared between users.



Keyword lists can be easily maintained via the keyword manager. The above example shows a list of keywords relating to drugs.



When a keyword list is searched, any hits are added to the search results panel for review.



To review the search results, the user double clicks on a keyword from the list and the corresponding hits are automatically filtered and highlighted in the grid.

Indexing and Searching

To assist with rapid evidence identification, we have added a high-performance, full-featured text search engine to NetAnalysis® v2. The following data types are added to the search index:

- **Indexed Text:** Many web browsers maintain their own index to assist with searching. NetAnalysis® can extract the original data from these search databases. This data is then written out for indexing and searching.
- **Text Extracted from Web Pages:** During cache extraction and web page rebuilding, NetAnalysis® extracts the text from web pages by stripping HTML code, CSS and script, leaving behind the content of the page. This data is then written out for indexing and searching.
- **HTTP Entity Body:** Some browsers store HTTP entity body information. This data can contain a wide variety of valuable information which may be of interest in an investigation. This data is written out for indexing and searching.
- **Reading List Preview Text:** Some web browsers have Reading List entries that represent sites the user has selected to view at a later date. As part of the reading list, the browser stores a text preview of the start of the page, or a description. This data is written out for indexing and searching.
- **Bookmark Descriptions:** All browsers have the ability to bookmark web pages; however, some browsers also store a text description as part of the bookmark. This data is written out for indexing and searching.
- **Chromium Autofill, AutofillProfile and CreditCard Autofill Information:** Autofill forms is a feature of Google Chrome and other Chromium based browsers. It allows for the user to store information such as name, address, phone number and email address as an Autofill entry so that forms can be automatically populated. Another feature of the AutofillProfiles is the storage of credit card information. In NetAnalysis® v2, we extract this data and display it in the main grid and text display window. We also extract the corresponding user data and save it to the export folder for indexing and searching.
- **Login Credentials:** Any web site login information which is available in plain-text is written out for indexing and searching.
- **Collections and Notes:** Microsoft Edge (Chromium based) has a feature called Collections where the user can keep track of ideas on the web such as collecting notes for research or lesson plans, whilst grouping that information with web site links. Opera and Vivaldi have a similar feature called Notes which allows the user to take notes, add a description and take screen shots whilst surfing the web. The text from both of these features are extracted and saved to the export folder for indexing and searching.

Once the user has created an index, it can be easily searched as can be seen in the window below.

The screenshot shows the NetAnalysis® Search Index interface. The search term is 'mdma'. The results table lists 30 records, with the first record (URN 16722) highlighted in blue. The table columns are URN, File Path, Search Hit Count, and Document Score.

URN	File Path	Search Hit Count	Document Score
16722	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000016722.txt	30	1.033785
16715	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000016715.txt	37	0.9567292
8288	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000008288.txt	24	0.9246451
20564	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000020564.txt	56	0.7062093
19899	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000019899.txt	7	0.6658205
19358	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000019358.txt	11	0.6259876
19360	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000019360.txt	20	0.5627211
495	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000000495.txt	512	0.5338441
2448	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000002448.txt	15	0.4873307
12882	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000012882.txt	6	0.3852688
18752	C:\Cases\Export\CASE-20140923\ID-121055\Mozilla Firefox\HTML to Text\F0000018752.txt	4	0.3774847

Below the table, the viewer shows the content of the selected record (URN 16722), which is a Bing search result for 'mdma cost per kilo'. The viewer includes navigation tabs for Web, Images, Videos, Maps, News, and More. The search results show 13,000,000 results and several links related to MDMA prices and costs.

The search viewer highlights the corresponding hits allowing the user to easily navigate through the list.

The screenshot shows the NetAnalysis® v2.0 - Forensic Internet History Analysis interface. The search term is 'mdma cost per kilo'. The results table shows one record (URN 16722) with a search hit count of 1. The viewer shows the content of the selected record, which is a Bing search result for 'mdma cost per kilo'. The viewer includes navigation tabs for WEB, IMAGES, VIDEOS, MAPS, NEWS, and MORE. The search results show 13,000,000 results and several links related to MDMA prices and costs.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	http		2014-05-14 14:48:31.000	2014-05-14 15:48:31.000	1	http://www.bing.com/search?q=mdma+cost+per+kilo&qs=n&form=QBRE&pq=mdma+cost+per+kilo&sc=0-18&sp=-1&sk=&cid=e135f5e57e104

The viewer shows the content of the selected record, which is a Bing search result for 'mdma cost per kilo'. The search results show 13,000,000 results and several links related to MDMA prices and costs.

Double clicking the search index entry will filter the original record entry which corresponds to the search hit. In this case, we have identified a hit in the original text for a web page. NetAnalysis® is showing the rebuilt web page in the internal viewer.

URL Analysis

We have added new powerful tools to NetAnalysis® for the analysis and breakdown of URLs and Cookie Name/Value information. Source input includes the URL examination and analysis window, the Cookie Examination windows, Decoded URL column and any other URL column.

Decoded URL Column

Query	Search Term
?q=%E6%BC%A2%E8%AA%9E&oq=%E6%BC%A2%E8%AA%9E&espv=2&es_sm=9...	漢語
?q=%E6%BC%A2%E8%AA%9E&oq=%E6%BC%A2%E8%AA%9E&espv=2&es_sm=9...	漢語

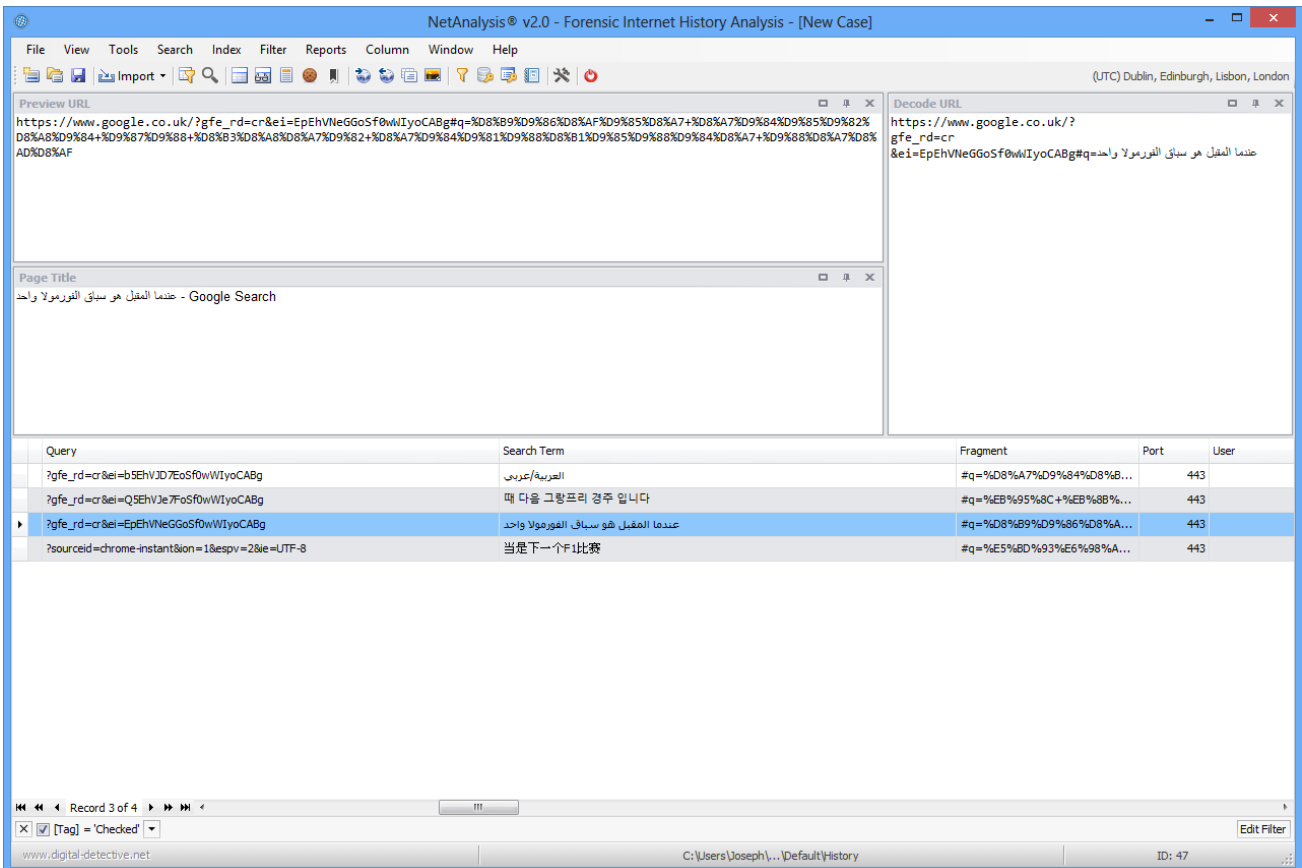
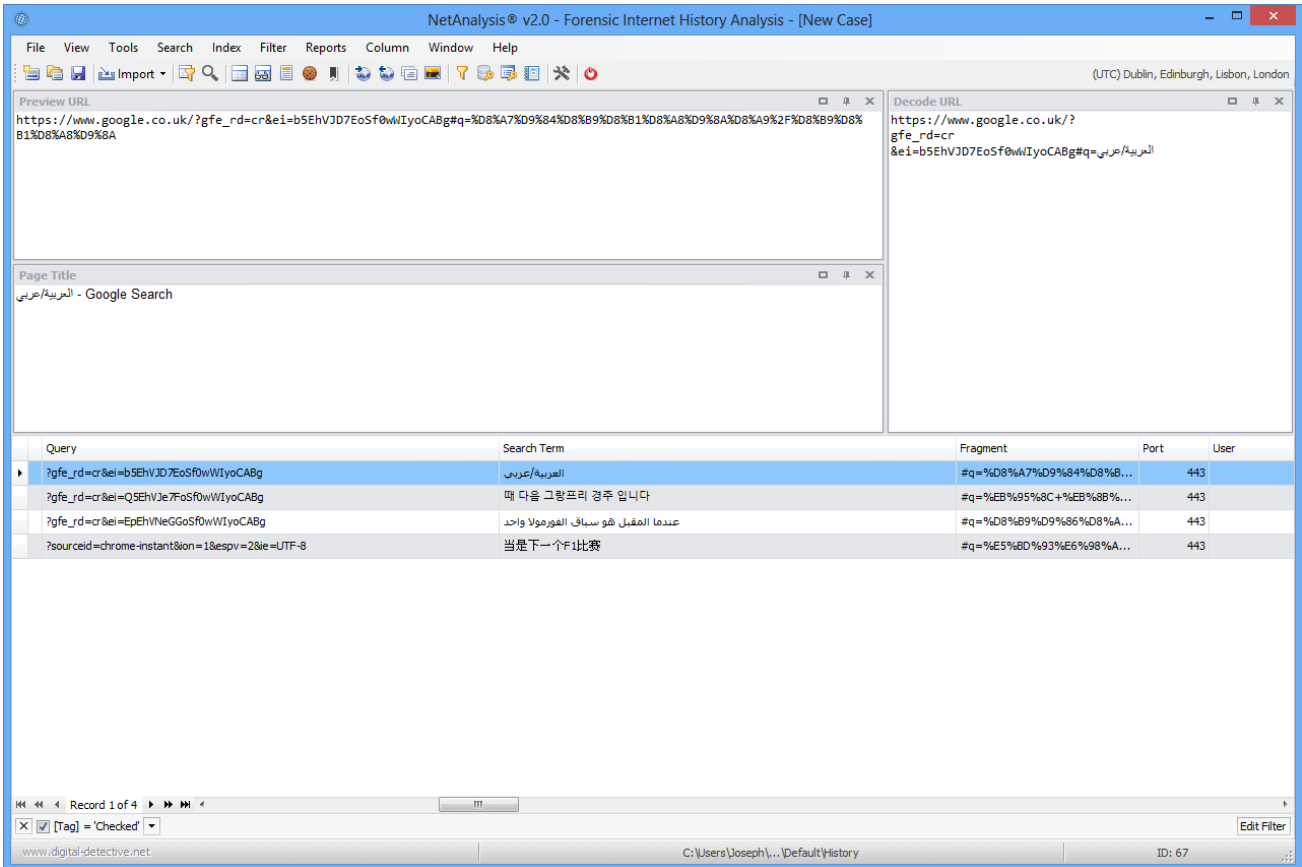
The above panels and grid show the automatic decoding of encoded Chinese characters as well as the extraction of the search terms.

Foreign Language Encoding Support including Unicode/UTF-8

Query	Search Term	Fragment
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&oq=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&espv=2&es_sm=90&ie=UTF-8	العربية/عربي	
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&oq=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&espv=2&es_sm=90&ie=UTF-8	العربية/عربي	
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&oq=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A&espv=2&es_sm=90&ie=UTF-8	العربية/عربي	

The above panels and grid show the automatic decoding of encoded Arabic characters, as well as the extraction of the search terms.

NetAnalysis® v2 fully supports Unicode/UTF-8 encoding as well as user selected code pages.



Search Term Extraction

Query	Search Term
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9...	العربية/عربي
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9...	العربية/عربي
?q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9...	العربية/عربي

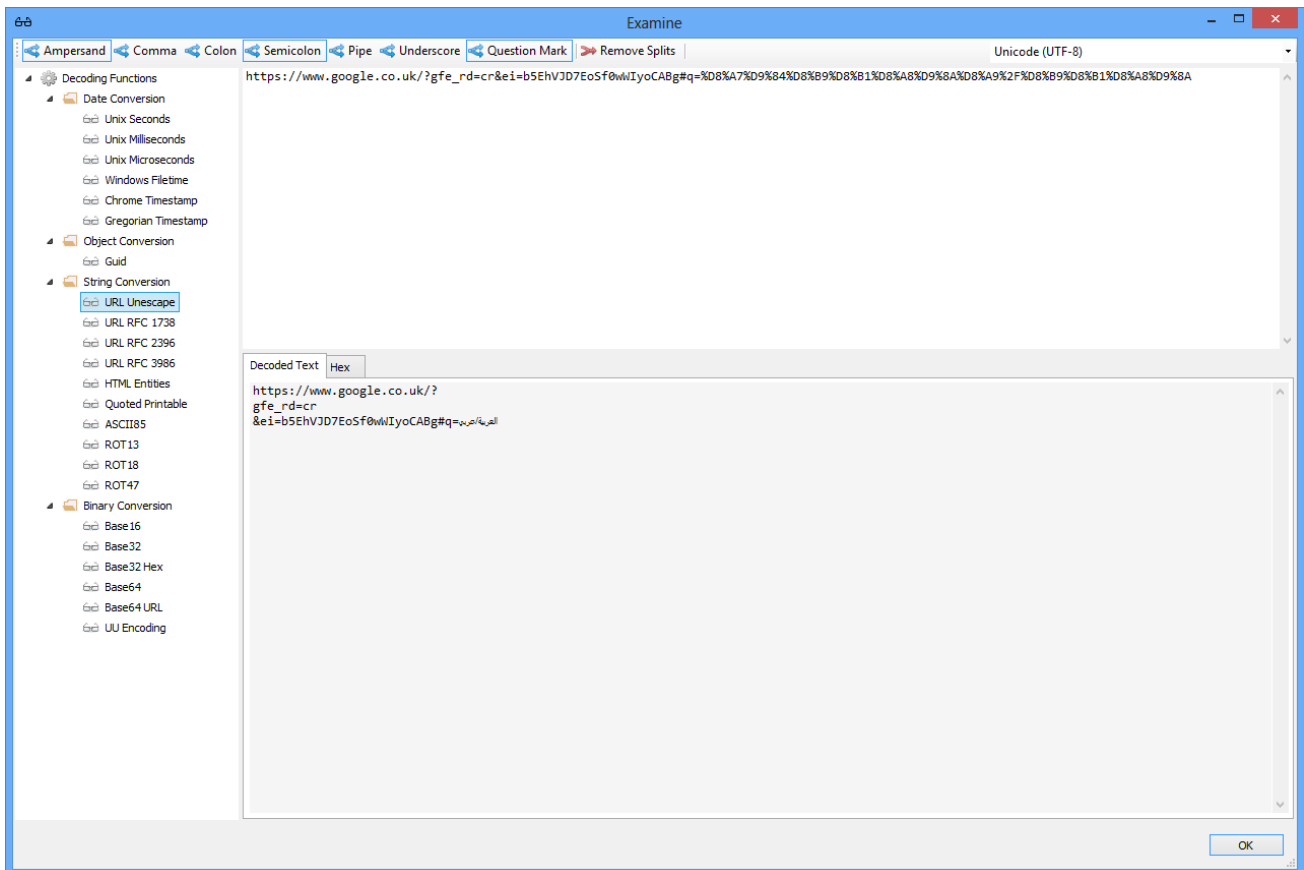
NetAnalysis® also extracts search keywords and phrases and displays them in the Search Term column. The above screen shows an Arabic search term highlighted using the Quick Search feature.

The screenshot displays the NetAnalysis v2.0 interface. At the top, the title bar reads "NetAnalysis® v2.0 - Forensic Internet History Analysis - [New Case]". The menu bar includes File, View, Tools, Search, Index, Filter, Reports, Column, Window, and Help. Below the menu bar is a toolbar with various icons. A "Preview URL" field shows a long URL with a search query parameter: `https://www.google.co.uk/?gfe_rd=cr&ei=b5EHVJD7EoSf0wWIyoCABg#q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9...`. Below the URL field is a search input field containing "العربية/عربي" and "Find" and "Clear" buttons. The main area is a table with the following columns: Query, Search Term, Fragment, Port, and User. The first row is highlighted and contains: Query: `?gfe_rd=cr&ei=b5EHVJD7EoSf0wWIyoCABg`, Search Term: العربية/عربي, Fragment: `#q=%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%2F%D8%B9...`, Port: 443, and User: (empty). At the bottom, there is a status bar showing "Record 1 of 1", a filter dropdown set to "[Tag] = 'Checked'", and the file path "C:\Users\Joseph\...\Default\History" with ID: 67.

The above screen shows an Arabic search term highlighted using the Quick Search feature.

URL Examination and Analysis Window

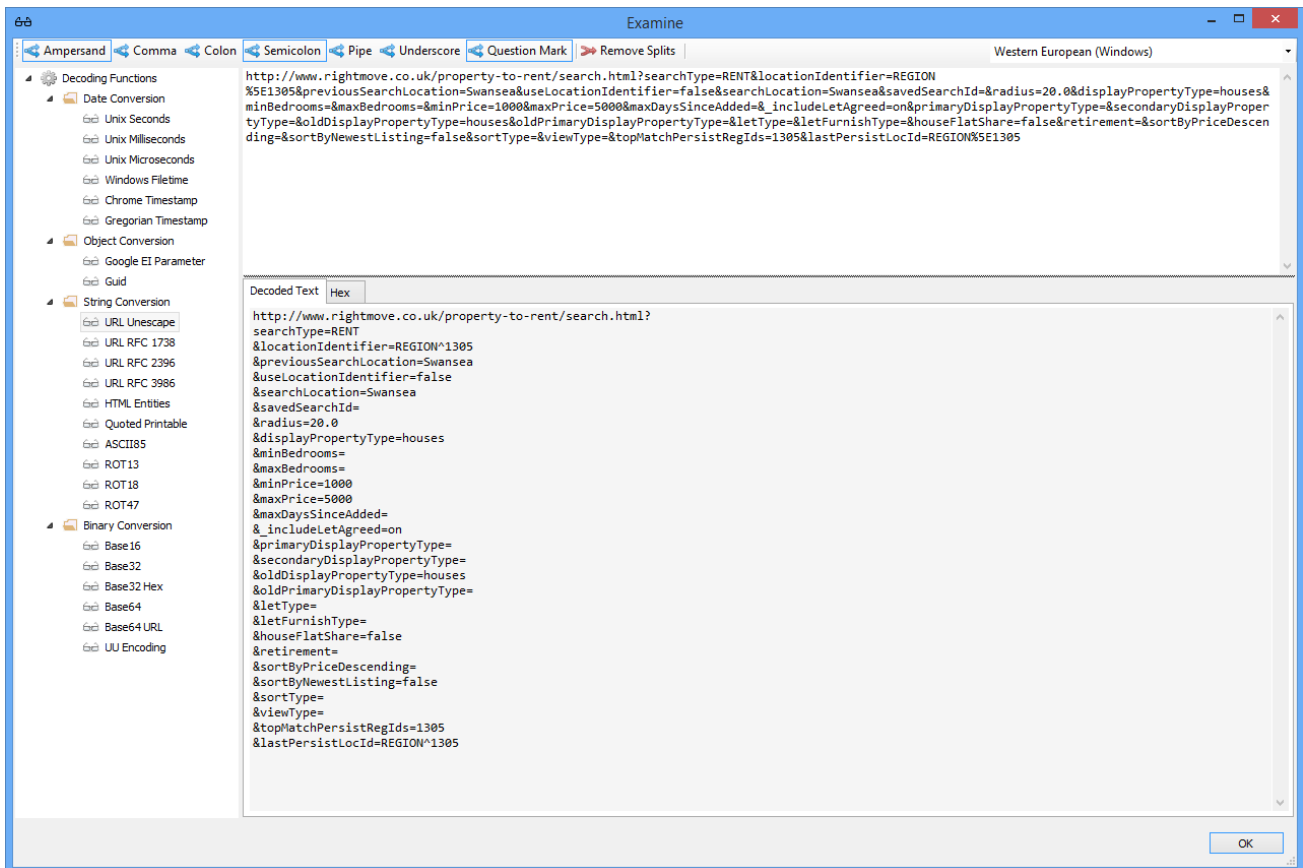
The examination window offers the user a number of options for splitting, decoding and analysing URL records and cookie values.



From the window above, we can see there are a number of conversion options for decoding selected text such as ROT13, Base64, ASCII85 and HTML Entities.

There are also a number of date/time conversion functions and a Guid converter.

URL Parameter Analysis



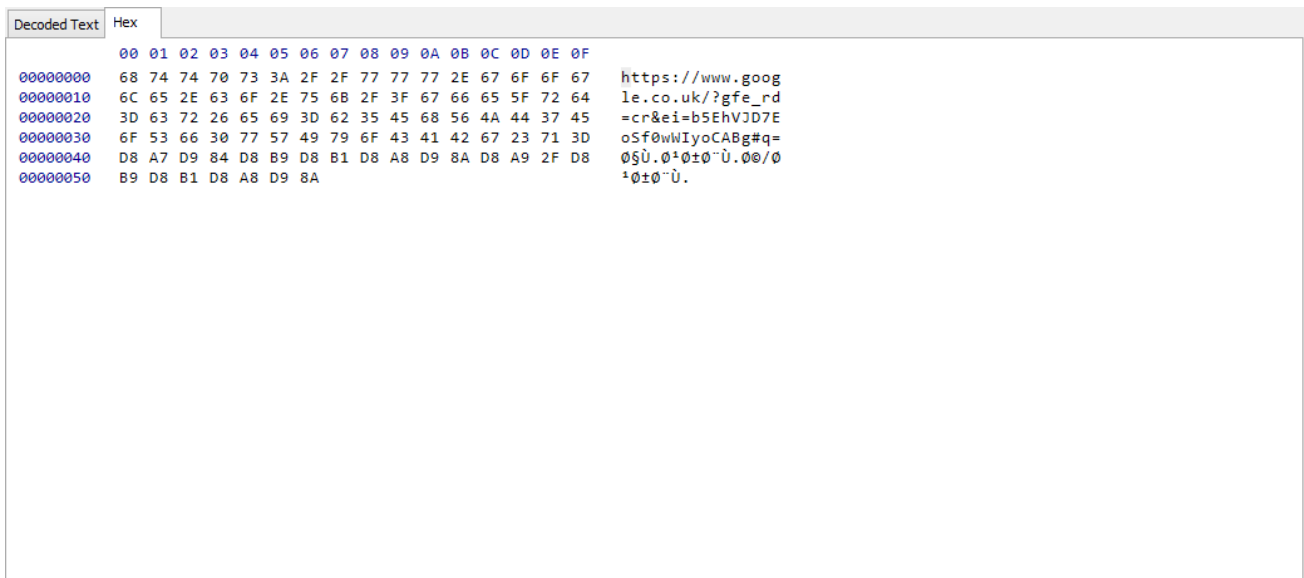
The above screen shows a URL which has been decoded and split into its component parameters.

Guid Decoding



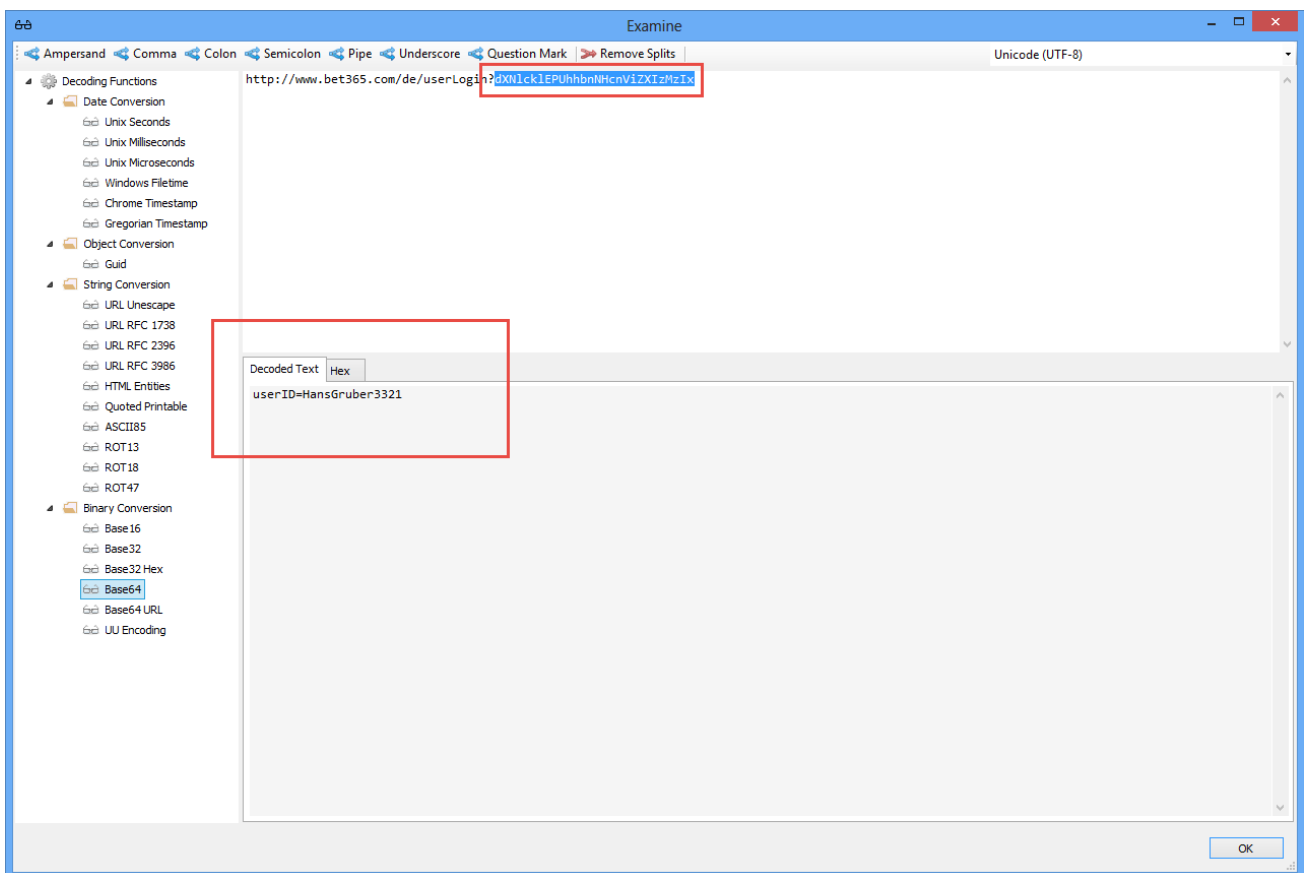
The screen above shows the breakdown of a version 1 Guid.

Hex/Text Examination



The above Conversion window shows the raw data from a decoded URL as displayed in the Hex view tab.

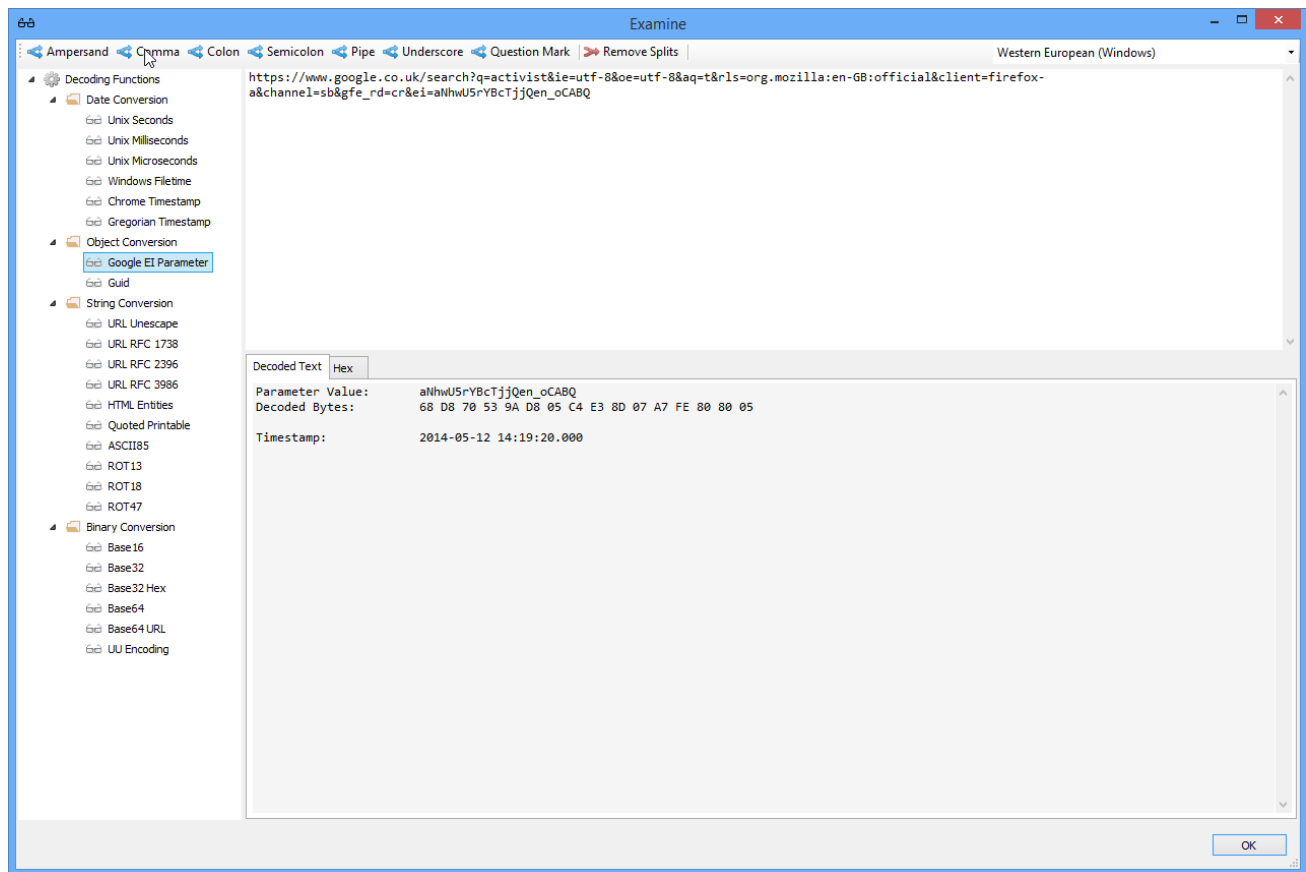
Base64 Decoding



The window above shows part of a URL being decoded from Base64; the Decoded Text window shows the

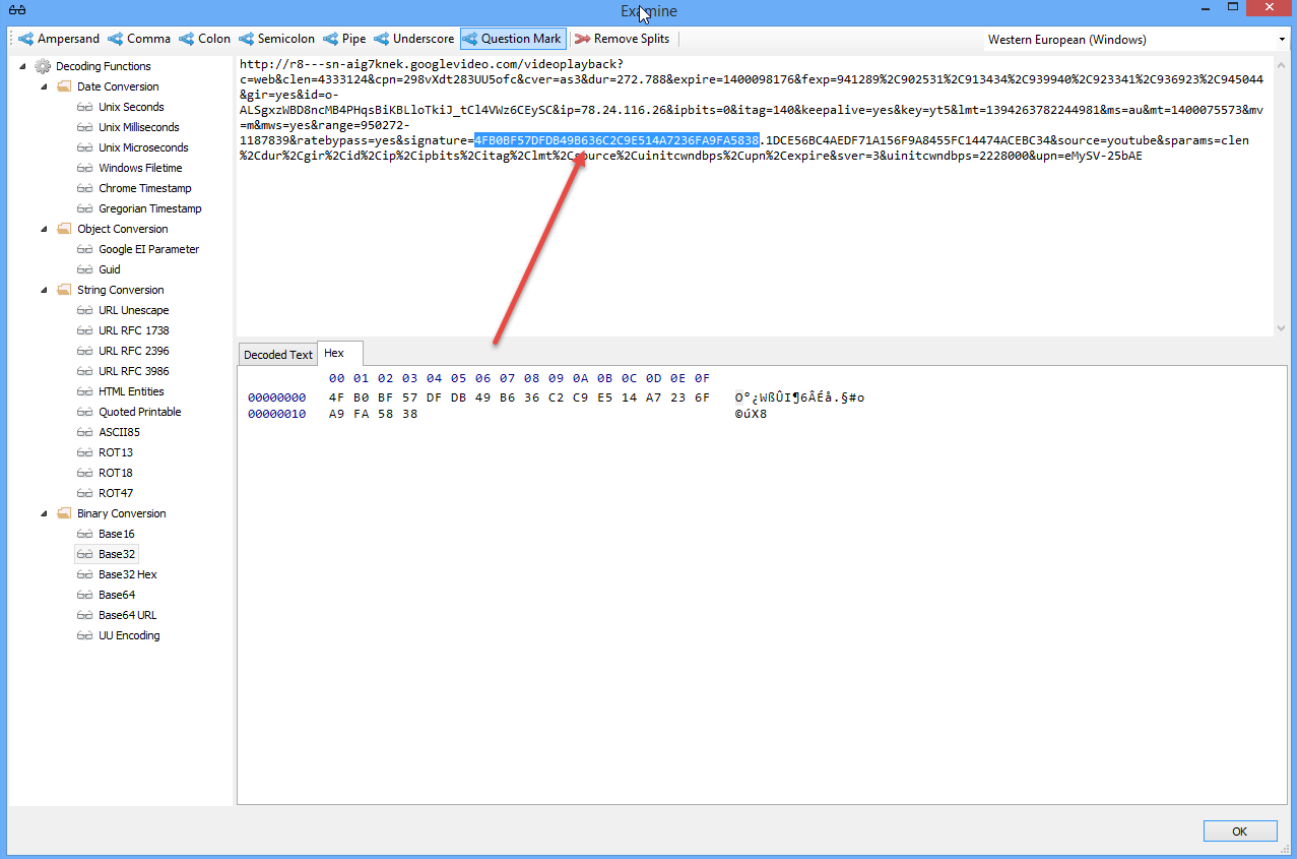
encoded portion of the URL contained a User ID.

Google EI/SEI Parameter Decoding



The Window above 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.

Base32 Decoding



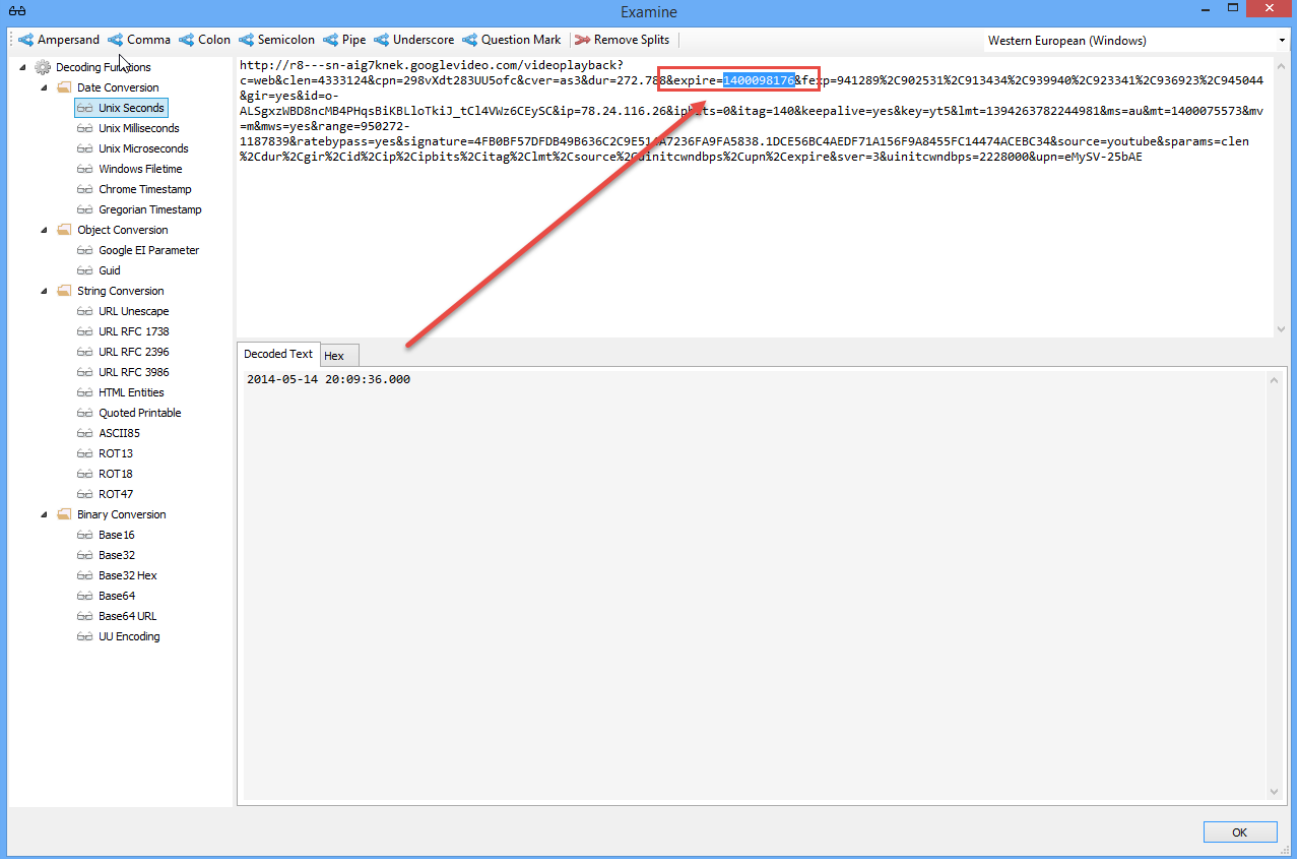
The screenshot shows the 'Examine' tool interface. The main text area contains a URL with a Base32 encoded parameter: `http://r8--sn-aig7knek.googlevideo.com/videoplayback?c=web&cLen=4333124&cpn=298vXdt283UU5ofc&cver=as3&dur=272.788&expire=1400098176&exp=941289%2C90251%2C913434%2C939940%2C923341%2C936923%2C945044&gir=yes&id=o-ALSgxzw8D8ncNB4PHqs8iKBLloTkiJ_tCl4Vwz6CEySC&ip=78.24.116.26&ipbits=0&itag=140&keepalive=yes&key=yt5&limit=1394263782244981&ms=au&mt=1400075573&mv=#&mwms=yes&range=950272-1187839&ratebypass=yes&signature=4F808F57DFD849B636C2C9E514A7236FA9FA5030.10CE56BC4AEDF71A156F9A8455FC14474ACEBC34&source=youtube&sparams=cLen%2Cdur%2Cgir%2Cid%2Cip%2Cipbits%2Citag%2Clmt%2Csource%2Cuinitcwndbps%2Cupn%2Cexpire&sver=3&uinitcwndbps=2228000&upn=efySV-25bAE`. A red arrow points from the Base32 parameter to the 'Hex' tab in the decoding results.

The 'Decoded Text' tab shows the decoded URL. The 'Hex' tab shows the following hex values:

Decoded Text	Hex
00000000	4F B0 BF 57 DF DB 49 B6 36 C2 C9 E5 14 A7 23 6F
00000010	A9 FA 58 38

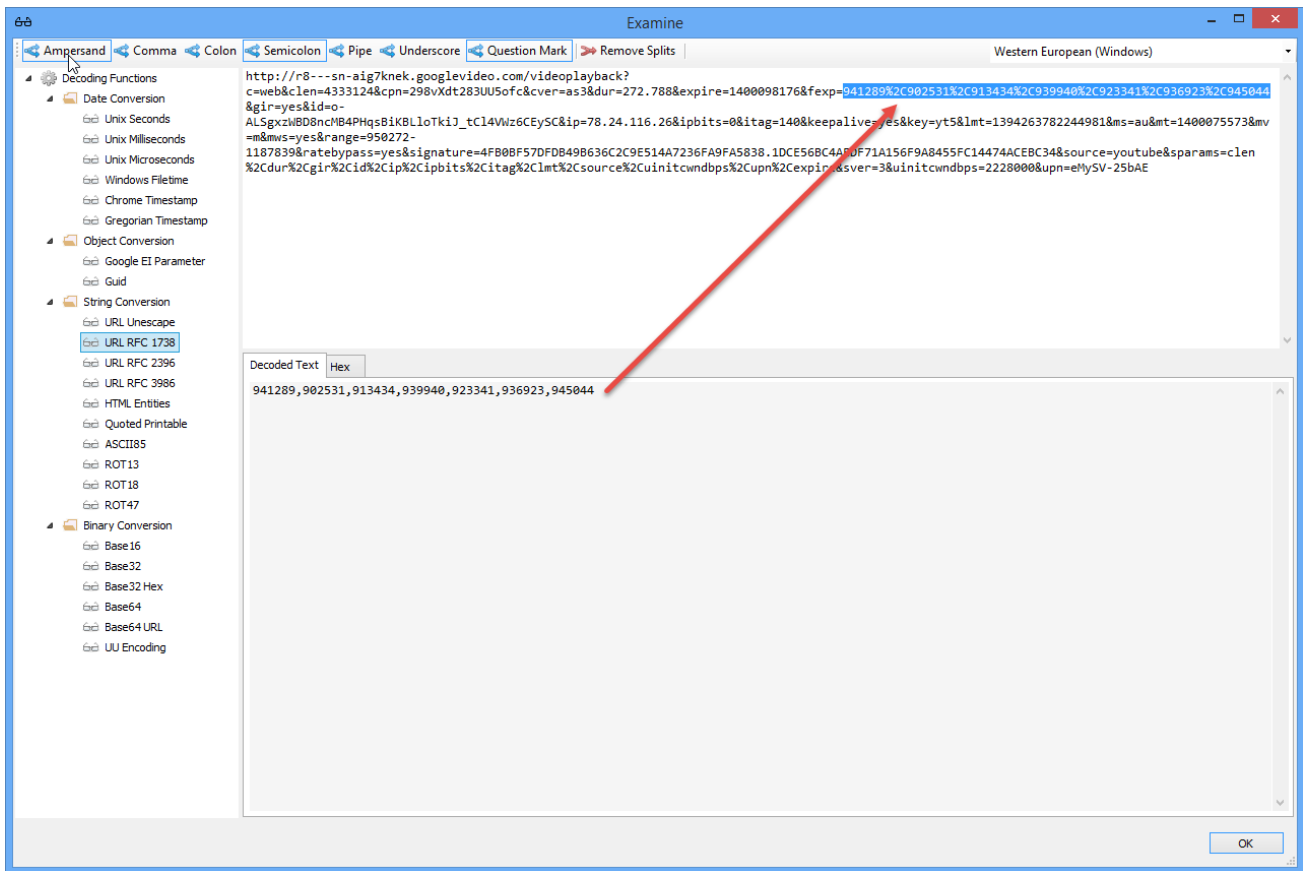
The hex values correspond to the Base32 encoded string '0°zWB0UI76ÅÊ\$.#o@úx8'.

Date Decoding



The screenshot displays the 'Examine' tool interface. The top menu bar includes options like Ampersand, Comma, Colon, Semicolon, Pipe, Underscore, Question Mark, and Remove Splits. The main window is titled 'Western European (Windows)'. On the left, a tree view shows 'Decoding Functions' with sub-categories: Date Conversion (Unix Seconds, Unix Milliseconds, Unix Microseconds, Windows Filetime, Chrome Timestamp, Gregorian Timestamp), Object Conversion (Google EI Parameter, GUID), String Conversion (URL Unescape, URL RFC 1738, URL RFC 2396, URL RFC 3986, HTML Entities, Quoted Printable, ASCII85, ROT13, ROT18, ROT47), and Binary Conversion (Base 16, Base 32, Base 32 Hex, Base 64, Base 64 URL, UU Encoding). The main text area shows a URL with a red box highlighting the parameter `&expire=1400098176&fe`. Below the text area, the 'Decoded Text' tab is active, showing the decoded value: `2014-05-14 20:09:36.000`. An 'OK' button is located at the bottom right.

Selective Decoding



Information and Warnings

The information and warning panels hold additional information relating to a single record. The information panel may show further data from a browser record where there is no corresponding column in the grid.

Further information may include data such as record transition information, or name/value pairs from form history etc.

```

Information
1 Download Start [UTC]: 2014-05-14 10:09:51.606
2 Download Total Length: 123368360 bytes
3 Download Received Length: 8376028 bytes
4 Download State: Cancelled
5 Download Danger Type: The content of this download may be malicious but SafeBrowsing has not finished checking the content
6 Download Interrupt Reason: The user cancelled the download
7 Download Opened: False
8 ETag: "c6c53f8a68d0c71:0"
9 Last Modified Date [UTC]: 2007-07-27 16:09:41.000
10 Url Download Chain Index 0:
    http://download.microsoft.com/download/7/7/8/778493c2-ace3-44c5-8bc3-d102da80e0f6/Office2003SP3-KB923618-FullFile-ENU.exe
  
```

The above window shows information from a Google Chrome Download entry.

```

Information
1 Username Element: email
2 Username Value: geoff.likely@gmail.com
3 Password Element: pass
4 Password Value:
01-00-00-00-D0-8C-9D-DF-01-15-D1-11-8C-7A-00-C0-4F-C2-97-EB-01-00-00-00-DC-8D-8A-C2-D3-52-22-45-98-22-C5-16-1B-BF-AF-0C-00-00-00-00-
02-00-00-00-00-10-66-00-00-01-00-00-20-00-00-00-31-E0-77-56-95-BD-9E-30-C7-44-79-0C-7B-A1-36-31-72-F9-37-15-49-7A-6C-62-B1-C1-
DD-02-CC-01-12-1F-00-00-00-00-0E-80-00-00-00-02-00-00-20-00-00-00-CA-01-34-21-11-5B-0F-E0-2F-CE-49-AB-AE-86-53-52-22-06-DB-77-48-1F-
43-81-E4-69-F5-39-E4-8A-8C-F2-10-00-00-00-CB-30-FC-C4-5C-B4-31-C9-D7-91-93-8E-F0-1A-5B-D3-40-00-00-00-87-7C-46-BF-57-7C-D8-B6-47-FD-
27-46-03-60-39-D7-3B-A3-15-6C-0E-34-F4-62-26-ED-A8-E3-4C-B2-24-90-40-C5-54-6E-D3-8C-F0-5A-3D-07-50-23-DA-26-7C-CE-76-0C-2A-6B-36-D7-
0D-1D-75-DA-E3-2F-E8-C7-EF-9B
5 Signon Realm: https://www.facebook.com/
6 SSLValid: True
7 Preferred: True
8 Blacklisted by User: False
9 Times Used: 6
10 Use Additional Authentication: False
11 Date Created: 2014-05-12 16:08:00.000
  
```

The above window shows information from a Google Chrome Login Data entry.

```

Information
1 Total Visit Count: 1
2 Typed Count: 0
3 Hidden Flag: False
4 FavIconId: 0
5 Page Transition: Link » Chain Start » Chain End
6 Segment ID: 0
7 Visit Duration: 00:04:26.5913910 (Original value: 266591391)
  
```

The above window shows information from a Google Chrome History entry.

The warnings panel shows any warning that the user should be aware of regarding a specific record. If a record contains a warning, a warning icon will be placed before the URL in the grid.

The screenshot shows the NetAnalysis v2.0 interface. The main table displays history entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. A warning icon (a triangle with an exclamation mark) is visible next to the URL of the first entry. Below the table, a warnings panel is open, displaying the following message:

```

Warnings
1 Orphaned 'moz_places' entry with no corresponding 'moz_historyvisits' entry
  
```

The status bar at the bottom indicates the file path: C:\Users\Joseph\... \wx4agle7.default\places.sqlite and ID: 2.

The above window shows a warning relating to a Mozilla Firefox history record. In this case, NetAnalysis® is showing that there is no corresponding visit entry for this record which is located in the "moz_places" table.

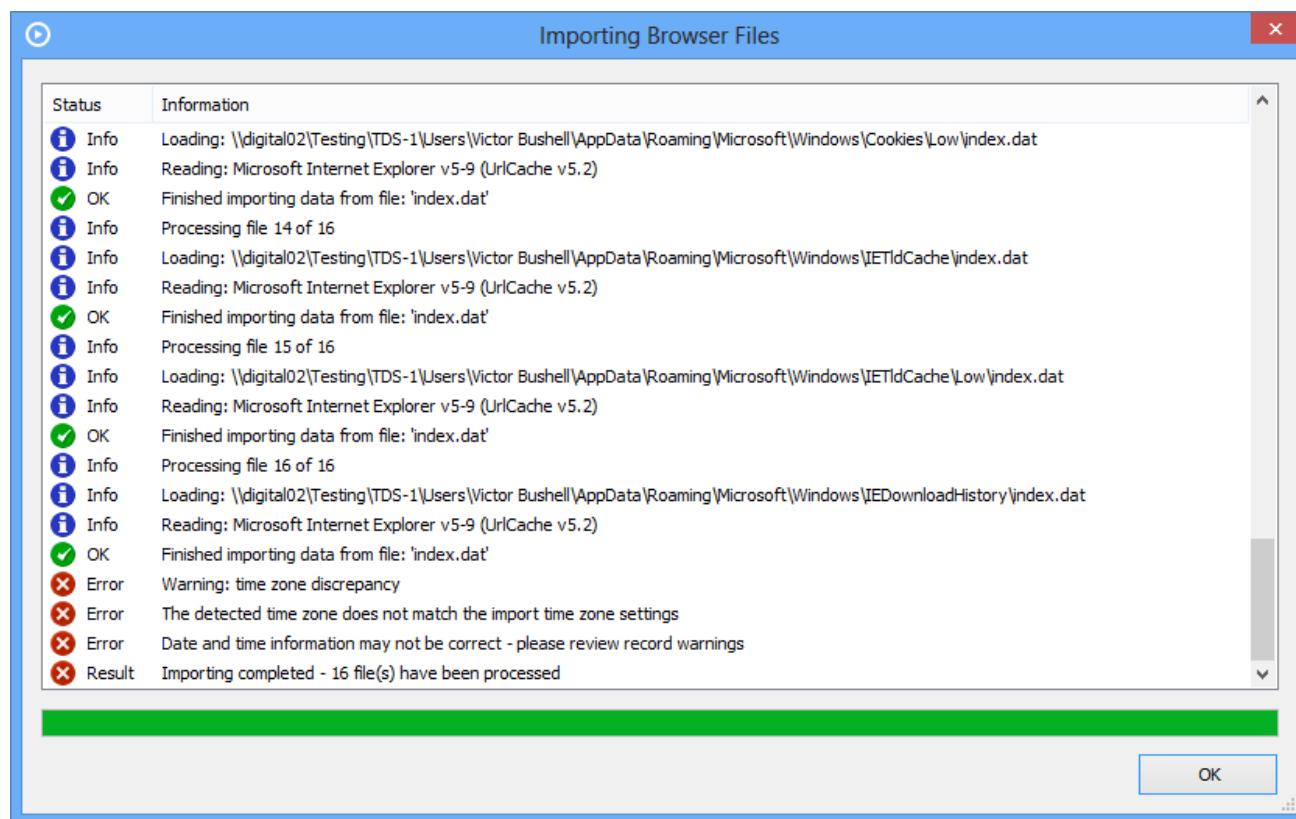
The screenshot shows a warnings panel with the following entries:

```

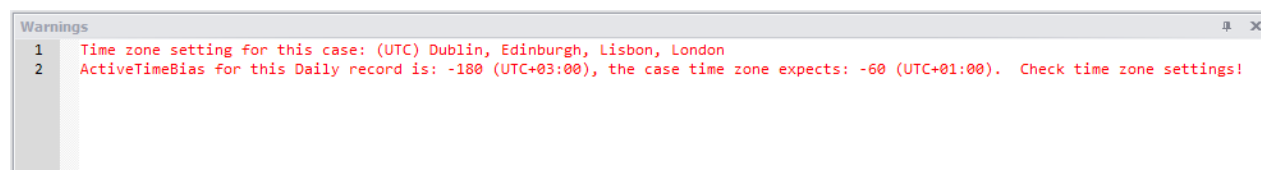
Warnings
1 Record partially overwritten, expected length: 512 bytes, actual length: 256 bytes
2 Title object partially overwritten, object position: 168, expected length: 264 bytes, actual length: 88 bytes
  
```

The window above shows a Microsoft Internet Explorer record which has been partially overwritten. This warning is particularly relevant when establishing the integrity of a record that may have evidential value.

If there are any issues encountered during data import, NetAnalysis® will flag this to the user in the progress window.



In the window above, NetAnalysis® is warning that an issue with the initial time zone settings has been identified.



The above window shows the corresponding time zone warning for a specific record which identifies the actual problem.

Cookie Examiner

The cookie examiner displays information relating to cookie entries and has been considerably enhanced. We also now have support for Google Analytics cookies where the component parts are extracted and displayed.

The screenshot shows the NetAnalysis v2.0 interface with the Cookie Examiner window open. The window displays details for a cookie from sigsauer.com. The 'Original Value' field is expanded to show Google Analytics data.

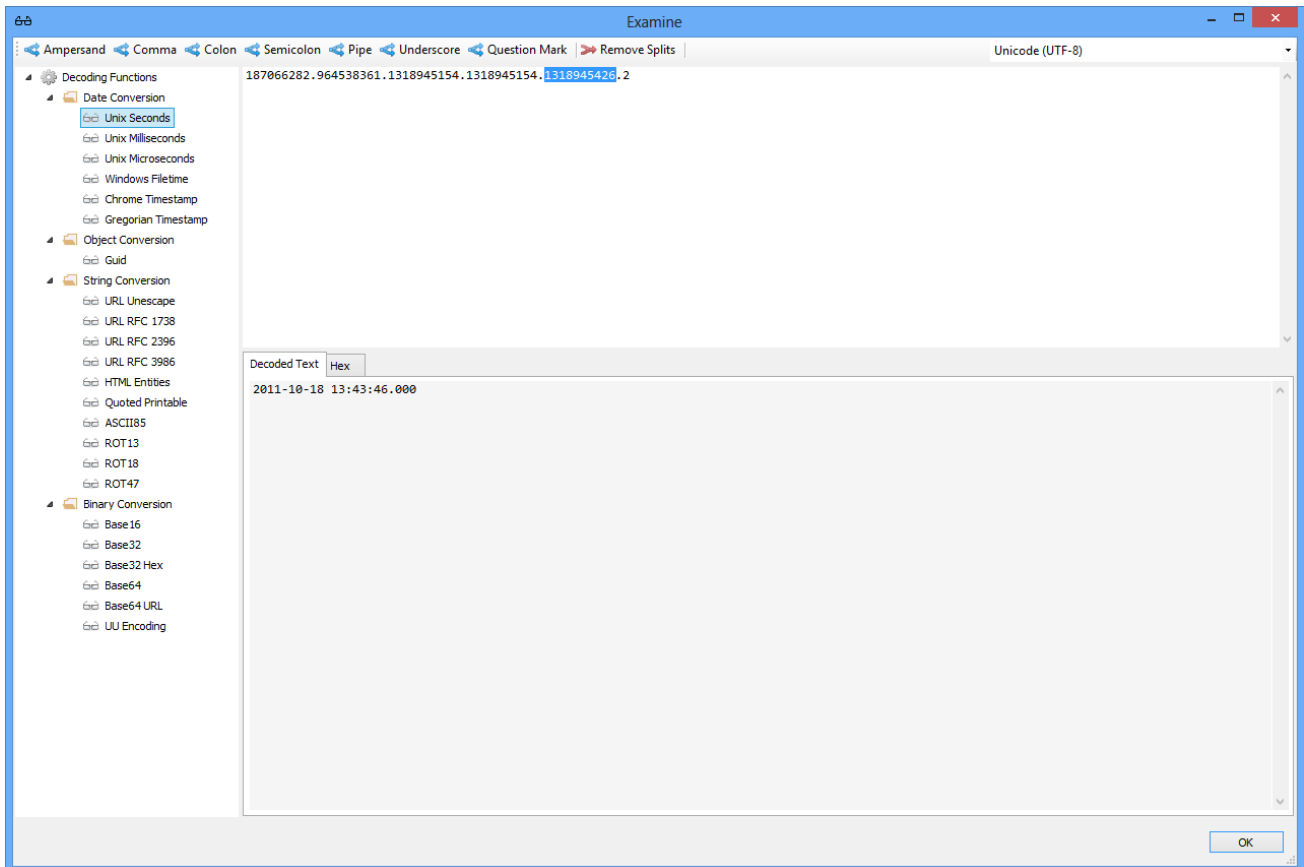
Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cookie		<input type="checkbox"/>	2011-10-18 13:43:45.771	2011-10-18 14:43:45.771	36	Cookie:victor bushell@sigsauer.com/
Cookie		<input type="checkbox"/>	2011-10-18 13:42:09.757	2011-10-18 14:42:09.757	19	Cookie:victor bushell@bladeops.com/
Cookie		<input type="checkbox"/>	2011-10-18 13:42:29.104	2011-10-18 14:42:29.104	16	Cookie:victor bushell@themicrotechstore.com/
Cookie		<input type="checkbox"/>	2011-10-18 15:00:57.008	2011-10-18 16:00:57.008	6	Cookie:victor bushell@guard-dog-security.com/
Cookie		<input type="checkbox"/>	2011-10-18 15:03:56.060	2011-10-18 16:03:56.060	5	Cookie:victor bushell@forum.pafoa.org/
Cookie		<input type="checkbox"/>	2011-10-18 15:03:54.279	2011-10-18 16:03:54.279	3	Cookie:victor bushell@pafoa.org/

The 'Original Value' field for the selected cookie is expanded to show the following information:

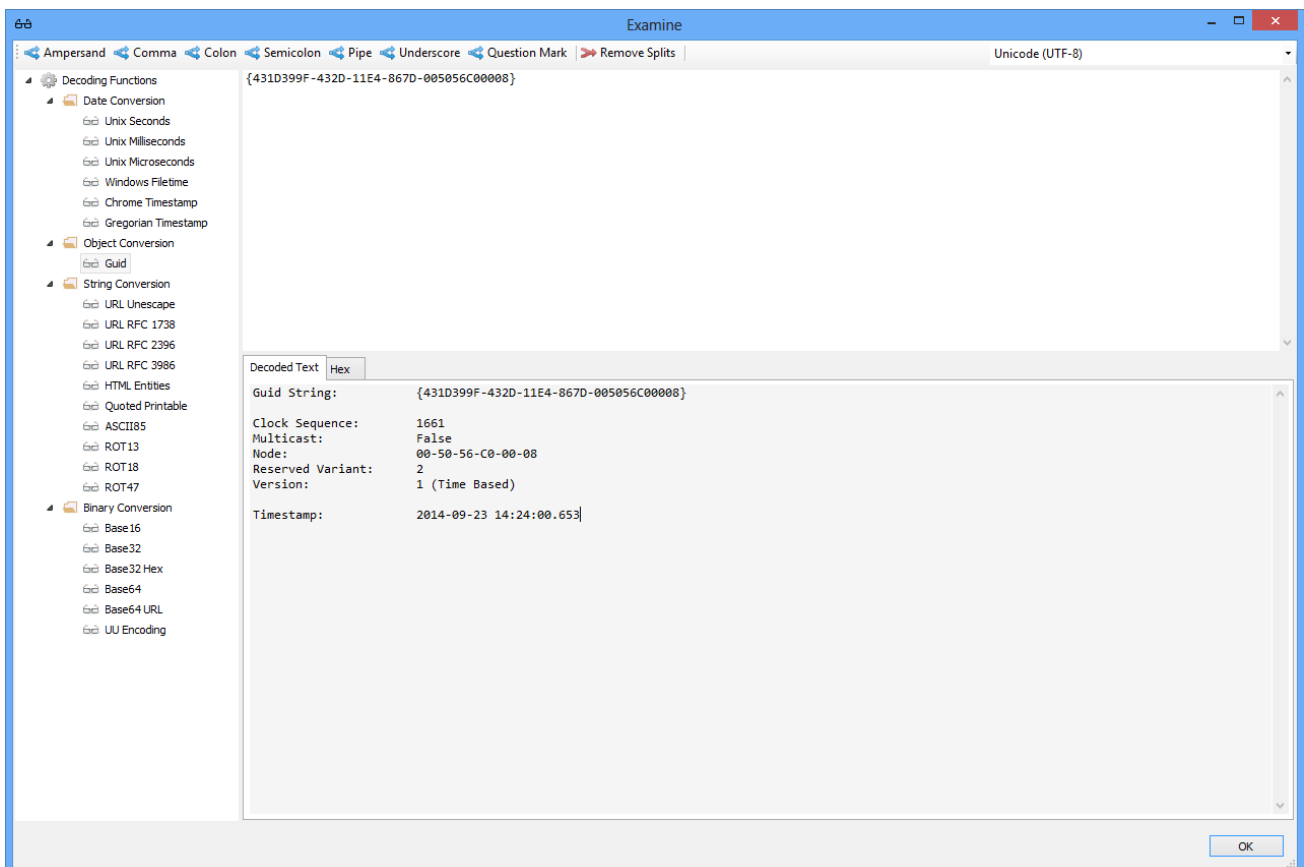
- Domain: sigsauer.com
- Path: /
- Date Last Modified [UTC]: 2011-10-18 13:43:45.771
- Date Expiration [UTC]: 2013-10-17 13:43:45.000
- HTTP Only: False
- Secure: False
- Information: Client-Side (Persistent)
- Original Value: 187066282.964538361.1318945154.1318945154.1318945426.2
- Domain Hash: 187066282
- Unique ID: 964538361
- Date First Visited [UTC]: 2011-10-18 13:39:14.000
- Date Previous Visit [UTC]: 2011-10-18 13:39:14.000
- Date Current Visit [UTC]: 2011-10-18 13:43:46.000
- Visit Count: 2

The window above shows a Google Analytics cookie for the sigsauer.com domain. The fields under the "Original Value" show the various Google Analytic name/value pairs.

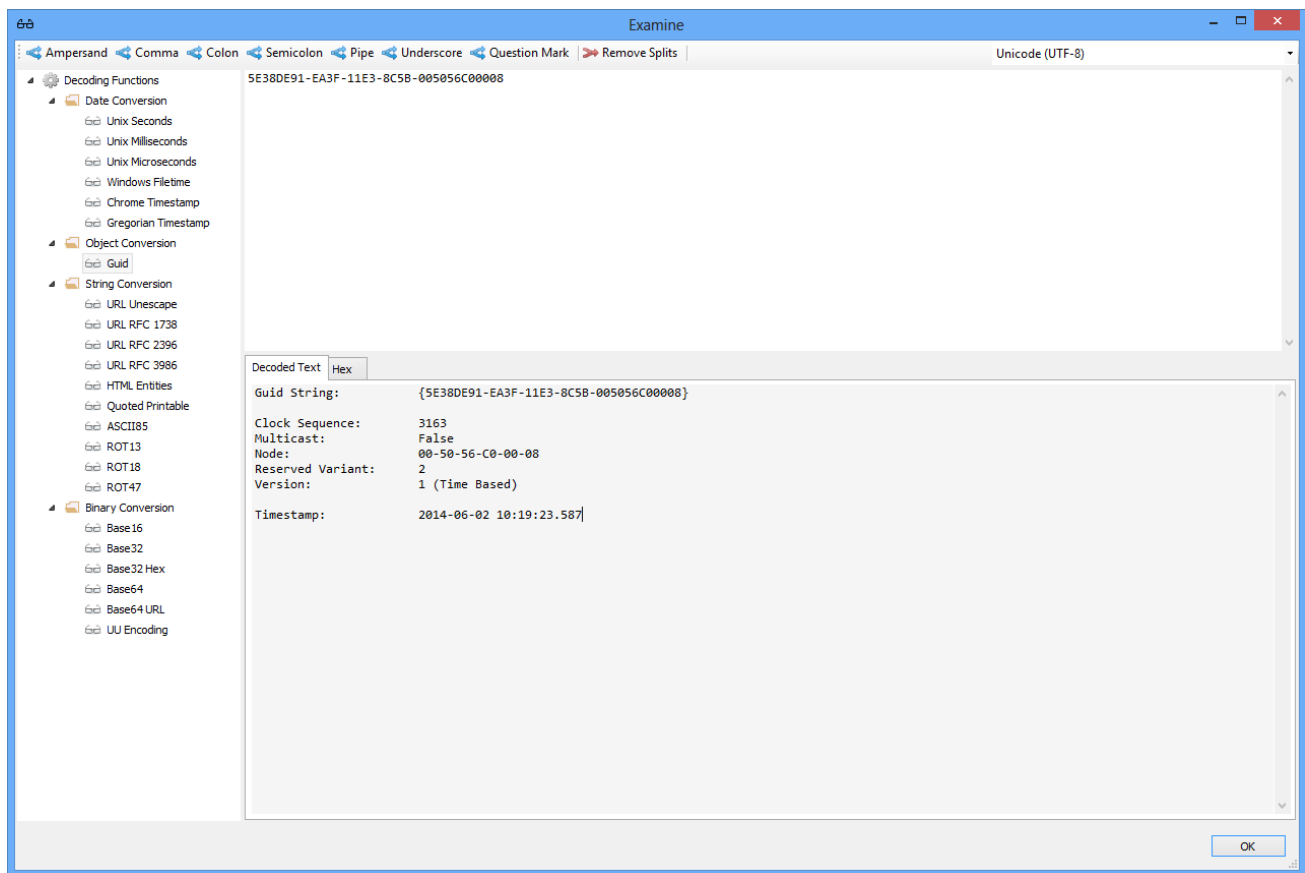
Google Analytics cookies can contain a wealth of information which may be relevant to a forensic investigation.



Cookie values can also be examined and decoded. In the case above, the user has selected some data from the top pane (which represents the original cookie value) and has selected to decode the value as a Unix timestamp.



In the window above and below, the cookie value contains a version 1 Guid. This object has been broken down into its component parts by selecting the Guid type from the Decoding Functions tree.



The above window shows another example of a version 1 Guid.

Name	Value
▲ __utma	
Domain	sigsauer.com
Path	/
Date Last Modified [UTC]	2011-10-18 13:43:45.771
Date Expiration [UTC]	2013-10-17 13:43:45.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
▲ Original Value	187066282.964538361.1318945154.1318945154.1318945426.2
Domain Hash	187066282
Unique ID	964538361
Date First Visited [UTC]	2011-10-18 13:39:14.000
Date Previous Visit [UTC]	2011-10-18 13:39:14.000
Date Current Visit [UTC]	2011-10-18 13:43:46.000
Visit Count	2
▲ __utmb	
Domain	sigsauer.com
Path	/
Date Last Modified [UTC]	2011-10-18 13:43:45.771
Date Expiration [UTC]	2011-10-18 14:13:45.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
▶ Original Value	187066282.1.10.1318945426
▲ __utmz	
Domain	sigsauer.com
Path	/
Date Last Modified [UTC]	2011-10-18 13:43:45.740
Date Expiration [UTC]	2012-04-18 01:43:45.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
▲ Original Value	187066282.1318945426.2.2.utmcsr=bing utmccn=(organic) utmcmd=organic utmctr=sig%20sauer
Domain Hash	187066282
Date First Visited [UTC]	2011-10-18 13:43:46.000
Session Number	2
Campaign Number	2
Campaign Source	bing
Campaign Name	(organic)
Campaign Medium	organic
Campaign Term	sig sauer

The window above shows three Google Analytic cookie records from a Microsoft Internet Explorer cookie file. In this case, the three cookies are __utma, __utmb and __utmz.

Web Page Rebuilding

The web page rebuilding engine for NetAnalysis® v2 has been completely re-engineered. It is now considerably faster and more capable than its predecessor.

We have added an offline HTML5-compliant viewer which is capable of displaying cached web pages, video, images and other content; it can also play audio files.

Rebuilding Web Pages

The following screens show some examples of rebuilt web pages being displayed in our offline viewer.

The screenshot displays the NetAnalysis v2.0 interface. The top window shows a list of web history records with columns for Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected record is:

Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
http		2011-10-18 13:38:39.679	2011-10-18 14:38:39.679	1	http://www.google.co.uk/search?scient=psy-ab&hl=en&source=hp&q=sig+sauer+p226&pbx=1&sq=sig+s&aq=1&aq=g4&aq=1&gs_sm=c&gs_upl...
http		2011-10-18 13:38:51.815	2011-10-18 14:38:51.815	1	http://www.sigsauer.com/
http		2011-10-18 13:39:17.143	2011-10-18 14:39:17.143	1	http://www.sigsauer.com/Products/Default.aspx
http		2011-10-18 13:39:45.751	2011-10-18 14:39:45.751	1	http://www.sigsauer.com/CatalogProductDetails/p290.aspx
http		2011-10-18 13:40:12.284	2011-10-18 14:40:12.284	3	http://www.sigsauer.com/Products/ShowCatalogNewProduct.aspx

The bottom window shows a preview of the SIG SAUER website. The page features a navigation menu on the left with options like HOME, PRODUCTS, CUSTOM SHOP, CUSTOMER SERVICE, SIG STORE, SIG SAUER ACADEMY, LE/MILITARY, INTERNATIONAL, DEALERS, TEAM SIG, and PRODUCT ALERTS. The main content area displays a large image of a SIG SAUER P290 handgun, with a smaller image below it and the text "P290".

As the cache is processed and all available web pages are rebuilt (allowing them to be safely viewed offline), NetAnalysis® will extract all cached items and categorise them based on their file type. This allows the forensic investigator to quickly review all cached items (such as images, video, documents, etc.) for evidential value.

Page Rebuild Audit Log

As each page is rebuilt, NetAnalysis® builds a log showing the original URL and corresponding extracted, cached item. It also identifies where each cached item was extracted from and provides a hyperlink to the file.

Source Information

Reference	CASE-20140923 / ID-112446
Page URL	http://www.db.com/unitedkingdom/
Source Path	\\digital02\Testing\TDS-1\Users\Victor Bushell\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\PGQ57MZE\unitedkingdom[1].htm
Output File	F0000003593.htm
Rebuild Date	2014-09-23 11:36:27.329

Rebuild Log

URL	Exists	Cache File	Output File
http://www.db.com/unitedkingdom/data/js/new_en.js	✓	new_en[1].js	F0000003601.js
http://www.db.com/unitedkingdom/img/db_UnitedKingdom.gif	✓	db_UnitedKingdom[1].gif	F0000003595.gif
http://www.db.com/unitedkingdom/img/ondak_2011_static_en.jpg	✓	ondak_2011_static_en[1].jpg	F0000003616.jpg
http://www.db.com/unitedkingdom/img/tran_px[1].gif	✓	tran_px[1].gif	F0000003594.gif
http://www.db.com/unitedkingdom/img/Deutsche_Bank_-_The_BrandSpace.gif	✓	Deutsche_Bank_-_The_BrandSpace[1].gif	F0000003597.gif
http://www.db.com/unitedkingdom/img/ArtMag_67_en.jpg	✓	ArtMag_67_en[1].jpg	F0000003600.jpg
http://www.db.com/unitedkingdom/img/db_map_button_uk.gif	✓	db_map_button_uk[1].gif	F0000003598.gif
http://www.db.com/unitedkingdom/data/js/webtrekk.js	✓	webtrekk[1].js	F0000003606.js
http://tp-cs.db.com/868192610003433/wt.pl?p=203,unitedkingdom/index.html	✗		
http://www.db.com/unitedkingdom/img/favicon.ico	✗		
http://www.db.com/unitedkingdom/img/background_verlauf.gif	✓	background_verlauf[1].gif	F0000003603.gif
http://www.db.com/unitedkingdom/img/footer_apollo.gif	✓	footer_apollo[1].gif	F0000003615.gif

NetAnalysis® also supports the automatic decompression of cached data which has been compressed by Gzip or deflate.

The screenshot displays the NetAnalysis v2.0 interface. The top window shows a table of web history records with columns for Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected record is:

Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
http		2011-10-18 15:12:37.968	2011-10-18 16:12:37.968	1	http://www.ehow.com/services/views/modules/shared/tombstone/corporate/5/1220/3385/
http		2011-10-18 15:12:38.240	2011-10-18 16:12:38.240	1	http://fr.nexac.com/e/getdata.xg?dt=br&pkkey=kdi33k3nbxia&u=http%3A%2F%2Fpix04.revsci.net%2FD08734%2Fa1%2F0%2F3%2F0.js%3FD%3...
http		2011-10-18 15:12:39.949	2011-10-18 16:12:39.949	1	http://www.facebook.com/extern/login_status.php?api_key=63203377906&app_id=63203377906&channel_url=http%3A%2F%2Fstatic.ak.fbcdn.n...
http		2011-10-19 08:27:50.260	2011-10-19 09:27:50.260	1	http://www.db.com/unitedkingdom/
http		2011-10-19 08:28:17.306	2011-10-19 09:28:17.306	1	http://www.google.co.uk/search?scient=psy-ab&hl=en&source=hp&q=deutsche+bank+money+transfer+online&pbx=1&oq=deutsche+bank+mone...

The viewer window shows a rebuilt web page for Deutsche Bank United Kingdom. The page features a navigation menu with links for Home, Company, Products and Services, Press, Social Responsibility, and Careers. The main content area includes a large image of Roman Ondák, a young man with short brown hair, and a headline that reads "Roman Ondák Artist of the Year 2012" with the tagline "Passion to Perform". A "more" button is visible next to the headline. The footer contains a date "October 13, 2011" and a news snippet: "Deutsche Bank selects Roman Ondák as 'Artist of the Year 2012'". There are also links for "Private Clients and Asset Management", "Corporate and Investment Banking", and "Locations in the UK".

As web pages are extracted, NetAnalysis® converts any page content from HTML to plain text for subsequent indexing and viewing.

The above page shows an example of a rebuilt web page, the next screen shows the extracted text from the page.

The screenshot displays the NetAnalysis v2.0 interface for forensic internet history analysis. The main window shows a table of records with columns for Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected record is for the URL <http://www.db.com/unitedkingdom/>, visited on 2011-10-19 09:27:50.260.

Below the table, the 'Index Text' window shows the extracted content of the web page. The text includes navigation links, company information, and news headlines.

```

Deutsche Bank - Home

Jump to meta navigation
Jump to main navigation
Jump to breadcrumb navigation
Jump to content
Jump to secondary navigation
Jump to footer navigation
Deutsche Bank Group
Contact
Sitemap

Deutsche Bank Search Search Query
Home
Company
  Headlines
  Awards
  History
  Deutsche Bank global
Products and Services
  Global Markets
  Global Banking
  Asset Management
  Private Wealth Management
  DNS
Press
Social Responsibility
  About Corporate Citizenship UK
  Sustainability
  Education
  Social Investments
  Art & Music
  Employee Engagement
Careers
October 13, 2011
Deutsche Bank selects Roman Ondák as "Artist of the Year 2012"
October 12, 2011
Frieze Art Fair 2011 opens its doors tomorrow
September 30, 2011
Deutsche Insurance wins Reactions' "Best Asset Manager" award for fourth straight year

more headlines
Index Text Viewer
www.digital-detective.net \\digital02\Testing\...\Content.IE5\index.dat FO: 1597056

```

The window above shows the text of a web page which has been extracted during the cache exporting process. This text can be indexed and searched with our text indexing engine.

Examples of Rebuilt Web Pages

The following screens show a sample of rebuilt web pages.

The screenshot displays the NetAnalysis v2.0 interface. The top window shows a list of web entries with columns for Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected entry is:

Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
http		2011-10-18 13:41:51.075	2011-10-18 14:41:51.075	1	http://www.bladeops.com/Microtech-Halo-Knives-s/130.htm
http		2011-10-18 13:42:11.458	2011-10-18 14:42:11.458	1	http://www.themicrotechstore.com/Microtech_Halo_V_s/22.htm
http		2011-10-18 13:42:15.634	2011-10-18 14:42:15.634	1	http://www.facebook.com/extern/login_status.php?api_key=your%20app%20id&app_id=your%20app%20id&channel_uri=http%3A%2F%2Fstatic...
http		2011-10-18 13:42:28.420	2011-10-18 14:42:28.420	1	http://www.themicrotechstore.com/Microtech_HALO_V_151_1_SE_Black_Plain_p/151-1.htm
http		2011-10-19 08:45:17.044	2011-10-19 09:45:17.044	5	http://s7.addthis.com/static/r07/sh63.html

The selected entry is viewed in the 'Viewer' window, showing a rebuilt page for 'The Microtech Store'. The page features a navigation bar with links for Home, About Us, View Cart, My Account/Order Status, and Help. The main content area displays the product 'Microtech HALO V 151-1 SE Black Plain' with a price of \$550.00, a quantity selector, and an 'Add to cart' button. The page also includes a search bar, a mailing list sign-up form, and a 'CERTIFIED Volusion SSL SECURE SITE' badge. The footer shows the website URL 'www.digital-detective.net' and the file path '\\digital02\Testing\...\Content.IES\index.dat'.

NetAnalysis® v2.0 - Forensic Internet History Analysis - [TDS-1]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
http		2011-10-18 13:42:15.634	2011-10-18 14:42:15.634	1	http://www.facebook.com/extern/login_status.php?api_key=your%20app%20id&app_id=your%20app%20id&channel_url=http%3A%2F%2Fstatic...
http		2011-10-18 13:42:28.420	2011-10-18 14:42:28.420	1	http://www.themicrotechstore.com/Microtech_HALO_V_151_1_SE_Black_Plain_p/151-1.htm
http		2011-10-19 08:45:17.044	2011-10-19 09:45:17.044	5	http://s7.addthis.com/static/07/sh63.html
http		2011-10-18 13:42:30.695	2011-10-18 14:42:30.695	1	http://www.facebook.com/extern/login_status.php?api_key=your%20app%20id&app_id=your%20app%20id&channel_url=http%3A%2F%2Fstatic...
http		2011-10-18 13:43:33.254	2011-10-18 14:43:33.254	1	http://www.bing.com/search?q=sig+sauer&FORM=IEBSRC

Record 18 of 140

[Entry Type] = 'Cache' And [Cache File Exists] = 'Exists' And [Cache File Extension] In ('.htm', '.html')

Viewer

Web Images Videos Shopping News Maps More | MSN Hotmail Sign in United Kingdom Preferences

bing

sig sauer

Web Images News More

RELATED SEARCHES

- Glock
- Sig Sauer Pistols
- Sig Sauer Mosquito
- Sig Sauer P226
- Sig Sauer P239
- Sig Sauer Arms
- Sig Sauer GSR
- Sig Sauer USA

SEARCH HISTORY

Search more to see your history

See all

Clear all · Turn off

NARROW BY REGION

Only from United Kingdom

NARROW BY DATE

All results

Past 24 hours

Past week

Past month

ALL RESULTS 1-10 of 10,400,000 results · [Advanced](#)

SIG SAUER

Features weapons made by this firm, B. Rizzini, and Hammerli. Also provides information about the academy and a dealer locator.

sigsauer.com

- Products & Services
- Dealer Locator
- Sig Store
- About
- Customer Service
- Contact
- Team Sig
- Warranty Information

Show more results from sigsauer.com

SIG SAUER - Wikipedia, the free encyclopedia

SIG Sauer GmbH is the German representative of Switzerland-based manufacturing firm Swiss Arms AG, which was spun off from Schweizerische Industrie Gesellschaft (SIG) in 2000.

en.wikipedia.org/wiki/SIG_Sauer


SIG SAUER

Khaki Washed Twill...

sigsauer.com/Default.aspx

Images of sig sauer

Discover images of sig sauer with Bing Image Search



See also: Sig Sauer P226, Sig Sauer P229, Sig Sauer Mosquito, Sig Sauer 556

News: [sig sauer](#)

www.digital-detective.net | \\digital02\Testing\...\Content.IE5\index.dat | FO: 233728

NetAnalysis® v2.0 - Forensic Internet History Analysis - [TDS-1]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
http		2011-10-18 15:11:54.699	2011-10-18 16:11:54.699	1	http://www.facebook.com/extern/login_status.php?api_key=172525162793917&app_id=172525162793917&channel_url=http%3A%2F%2Fstatic.a...
http		2011-10-19 08:45:16.896	2011-10-19 09:45:16.896	8	http://platform.twitter.com/widgets/hub.html
http		2011-10-18 15:12:20.950	2011-10-18 16:12:20.950	1	http://www.bing.com/search?q=wipe+computer&FORM=IE8SRC
http		2011-10-18 15:12:31.281	2011-10-18 16:12:31.281	1	http://www.bing.com/captionHandler.aspx?IG=f398202b4e2e4b19a84269c4e323cb538pu=http%3A%2F%2Fwww.ehow.com%2Fhow_4451527_co...
http		2011-10-18 15:12:32.888	2011-10-18 16:12:32.888	1	http://www.ehow.com/how_4451527_completely-wipe-computer-clean.html

Record 60 of 140

[Entry Type] = 'Cache' And [Cache File Exists] = 'Exists' And [Cache File Extension] In ('.htm', '.html')

Viewer

eHow
Discover the expert in you.

Google™ Custom Search

food home style money family health Shift more

This Season [Halloween](#) | [Tailgating](#)

Home » Computers » Use & Customize Your Computer » Clean a Computer for Free » How to Completely Wipe a Computer Clean

How to Completely Wipe a Computer Clean

Related Searches:

Computers tirelessly perform complicated tasks to alleviate some of the time-consuming burdens of their human owners. Over time, these machines' calculating speeds are reduced to a snail's pace as they become plagued with anything from viruses to malware programs. Computer users from as spam pop-up browser windows unexpectedly appear or, even worse, the blue screen of death emerges. Completely wiping the junk applications from the machines clears up the issues, guaranteeing their owners smooth-sailing when navigating around the desktop. All it takes is patience and a little technical knowledge.

Instructions Difficulty: Moderately Challenging

Related Ads

Related Articles & Videos

[How to Wipe a Hard Drive Clean With Freeware](#)

www.digital-detective.net | \\digital02\Testing\...Content\IES\index.dat | FO: 1525760

Built-In Viewer

In addition to displaying rebuilt web pages, the built-in viewer can also display web page previews and thumbnails which are stored by the various browsers:

- Apple Safari Top Sites web page previews
- Apple Safari History web page previews
- Google Chrome and Chromium based Top Sites web page previews
- Google Chrome and Chromium based History web page previews
- Mozilla Firefox and Mozilla based History web page previews
- Opera Blink Stash web page previews
- Opera Blink Thumbnails
- Opera Presto Thumbnails

Web Page previews

The screenshot displays the NetAnalysis v2.0 interface for forensic internet history analysis. The main window shows a list of history entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected entry is a history record for 'http://www.moneysupermarket.com/loans/'. Below the list, the 'Viewer' pane displays a preview of the Money Super Market website. The website features a navigation menu with categories like HOME, MONEY, INSURANCE, TRAVEL, ENERGY, MOBILE PHONES, SHOPPING, BROADBAND, VOUCHERS, and NEWS & COMMUNITY. A prominent banner advertises a 'Home Bill Checker' that could save up to £500* by comparing Home Insurance, Energy, and Broadband costs. A sidebar lists various services and their savings: Car Insurance (£220), Home Insurance (£70), Credit Cards (£250), Energy (£174), Loans (£99), Savings (£300), Holidays (£250), and Travel Insurance (£53). A 'Cookie Use' notification is visible in the bottom right corner of the preview.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
History	http		2014-05-15 15:07:42.000	2014-05-15 16:07:42.000	1	http://www.moneysupermarket.com/loans/
History	http		2014-05-15 15:07:09.500	2014-05-15 16:07:09.500	1	http://www.moneysupermarket.com/
History	http		2014-05-15 14:52:16.600	2014-05-15 15:52:16.600	1	http://search.yahoo.com/search?ei=utf-8&fr=aaplw&p=ketamine+capsules+street+price
History	http		2014-05-15 14:50:52.500	2014-05-15 15:50:52.500	1	http://www.apple.com/quicktime/download/thankyou/index.html

The screenshot displays the NetAnalysis v2.0 interface for forensic internet history analysis. The main window shows a table of top sites with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The first entry is a Top Site with scheme http, URL http://www.takeaway.com/order-pizza-newcastle. Below the table is a filter bar showing the current filter is '[Entry Type] = Top Site'. The main content area is a preview of the 'takeaway.com' website, featuring the logo, navigation links like 'Order takeaway food', 'Customer service', and 'Login', and a large orange banner with the text 'Order pizza'. The banner includes a location selection form with the postcode 'NE3 1UB' and a 'Search' button, along with a Facebook 'Like' button and a pizza image. The bottom status bar shows the file path '\\digital01\Scenario Data Sets\...\Safari\TopSites.plist' and ID: 1.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Top Site	http					http://www.takeaway.com/order-pizza-newcastle
Top Site	http					http://en.wikipedia.org/wiki/Ketamine
Top Site	http					http://www.liverpoolcho.co.uk/news/liverpool-news/hooked-now-mersey-drug-dealers-6735907
Top Site	https					https://www.facebook.com/melissa.black.54922169

The above window shows an Apple Safari Top Sites web page preview.

NetAnalysis® v2.0 - 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
Stash	http		2014-05-13 15:10:33.965	2014-05-13 16:10:33.965		http://www.eztestkits.com/en/drug-purity-and-cutting-agents/
Stash	http		2014-05-14 09:48:55.927	2014-05-14 10:48:55.927		http://www.pof.com/lastonlinemycity.aspx?SID=wuyckuota1eu0suhb0v0l2&guid=82114605&page=42&count=700
Stash	http		2014-05-14 10:16:35.351	2014-05-14 11:16:35.351		http://purebulk.com/creatine-monohydrate-powder.html#.U3NBWdwaUk
Stash	http		2014-05-14 10:16:44.442	2014-05-14 11:16:44.442		http://www.alibaba.com/showroom/white-creatine-powder.html

Record 14 of 14

[Entry Type] = 'Stash'

Viewer

Join Free | Sign In Buy | Sell | Community | My Alibaba | Messages | Help

Alibaba.com Global trade starts here.™

Products white creatine powder Search or Post Buying Request

Advanced Search

Region of Suppliers

- East Asia (2137)
- South Asia (1)
- North America (12)
- Europe (3)

Country of Suppliers

- China (Mainland) (2137)
- United States (12)
- Australia (1)
- Germany (1)
- Austria (2)
- India (1)

Categories

- Health & Medical
- Sports Supplements (149)
- Vitamins, Amino Acids and Coenzymes (537)
- Providing Energy (65)
- Immune & Anti-Fatigue (50)
- Disinfectant and Preservatives (14)

Showroom > Health & Medical > Health Care Products > Health Care Supplement > Sports Supplements > white cre

2,143 Product(s) from 107 Supplier(s) + Manufacturers


Related Searches: [whey protein powder](#), [creatine monohydrate](#), [goat milk powder](#), [whey protein powder](#) | More...

Products Suppliers

Sort by: Gold Supplier Onsite Check Assessed Supplier ESCROW e-Credit Line

Minimum Order: Online white creatine powder in City View as:

Customer who searched white creatine powder also searched: [diamond detector](#), [led ring light](#), [tuning light](#), | More...

 **Creatine Monohydrate White powder** ★ Favorites + Compare

US \$3.5-3.8 / Kilogram (FOB Price)

25 Kilograms (Min. Order)


20 Metric Ton/Metric Tons per Month (Supply Ability)


Tags: Creatine Monohydrate White

Shanghai Fine Chemicals Co., Ltd. China (Mainland) | [Contact Details](#)

[Contact Supplier](#) [Leave Messages](#)

Premium Related Products

 sodium alginate, potassium alginate.

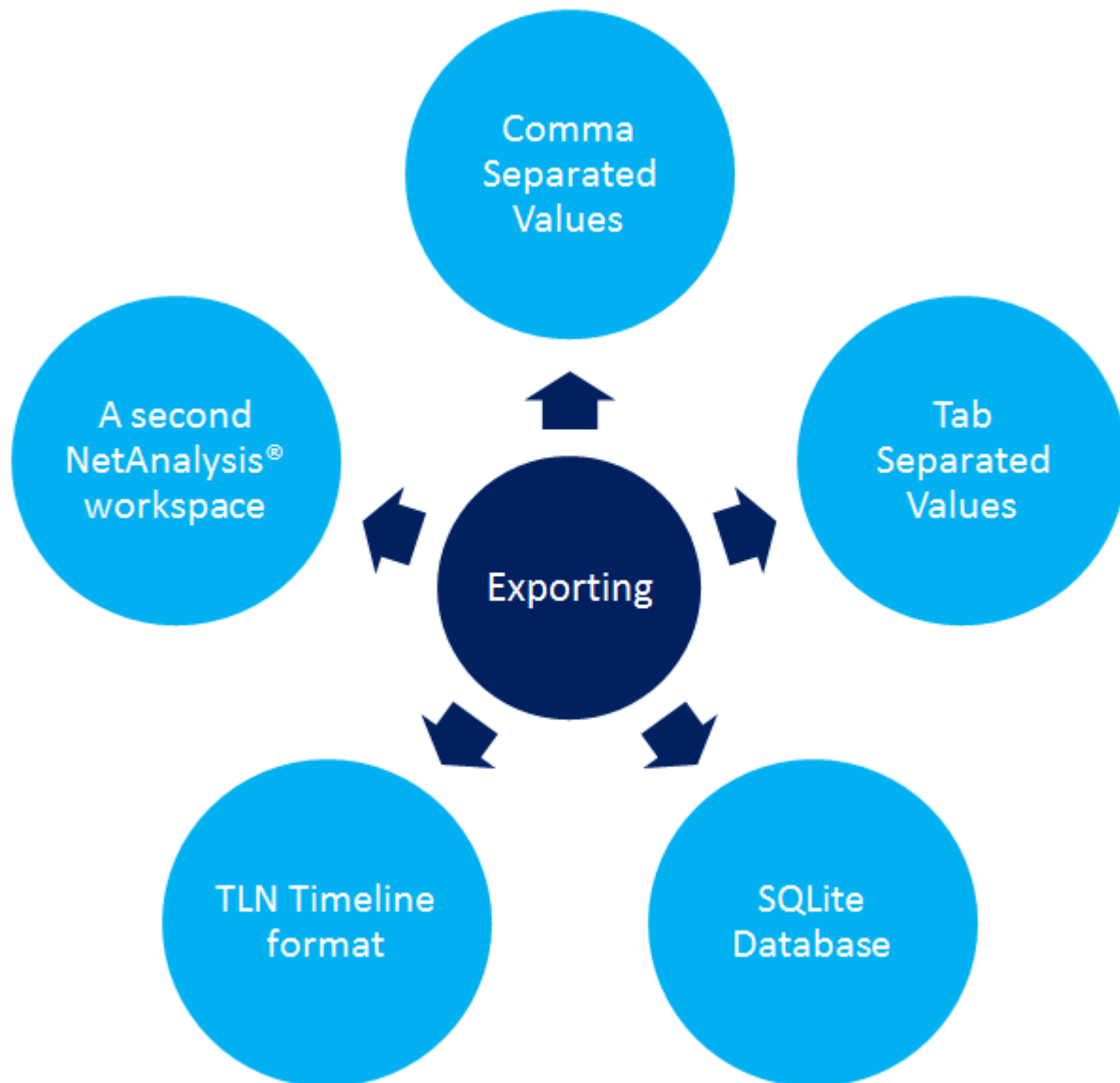
 Peanut Powder

www.digital-detective.net | \\digital01\Scenario Data Sets\... \Opera Stable\stash.db | ID: 15

The above window shows an Opera Blink Stash web page preview.

Exporting

We have added a number of different options for exporting data (either all records or a selected subset) from the NetAnalysis® workspace. We now support exporting to:



We have also added support for extracting a subset of records to a new NetAnalysis® workspace. This allows the user to remove any non-relevant data, system created data, or items which may be of legal privilege.

Reporting

The NetAnalysis® v2 reporting suite offers reporting, data analysis and visualisation. It also provides all the tools necessary, in the end-user report designer, to create virtually any report type, be it hierarchical master-detail reports, record and multi-column reports or interactive drill-down and drill-through reports.

The report manager provides the capability to save a report template to file and then re-use it as and when required.

NetAnalysis® Detailed Report Preview

File View Background

100%

NetAnalysis®

Case Reference CASE-20140923 - ID-183252
Prepared by Robert Bruce - Digital Detective

Printed 2014-09-23 18:41:17.172
Workspace 603bef5012e92

Damien Smithers Facebook registration

Scheme	https	Browser Version	Opera v15-24 (Stash v4)	Record URN	2999
Entry Type	Stash	Time Zone	GMT Standard Time	Source Offset	ID: 1
Date Visited [Local]	2014-05-12 17:11:17.550				
Date Visited [UTC]	2014-05-12 16:11:17.550				
Source File	\\digital01\Scenario Data Sets\Damien Smithers\Damien Smithers - Session 5\Roaming\Opera Software\Opera Stable\stash.db				
Visits					
Page Title	Facebook				
URL	https://www.facebook.com/register/confirm.php?ce=damiensmithers%40techie.com				
Search Term					

Scheme	http	Browser Version	Opera v15-24 (History v28)	Record URN	31
Entry Type	History	Time Zone	GMT Standard Time	Source Offset	ID: 18
Date Visited [Local]	2014-05-12 17:11:17.986				
Date Visited [UTC]	2014-05-12 16:11:17.986				
Source File	\\digital01\Scenario Data Sets\Damien Smithers\Damien Smithers - Session 5\Roaming\Opera Software\Opera Stable\History				
Visits	1				
Page Title					
URL	http://service.mail.com/mcstarter/mail.html?sid=20796913904567219JPTX3-mbQcIL3sI_v1ahZbMO2UNbLUh:11&partnerdata=partneranonymous#				
Search Term					

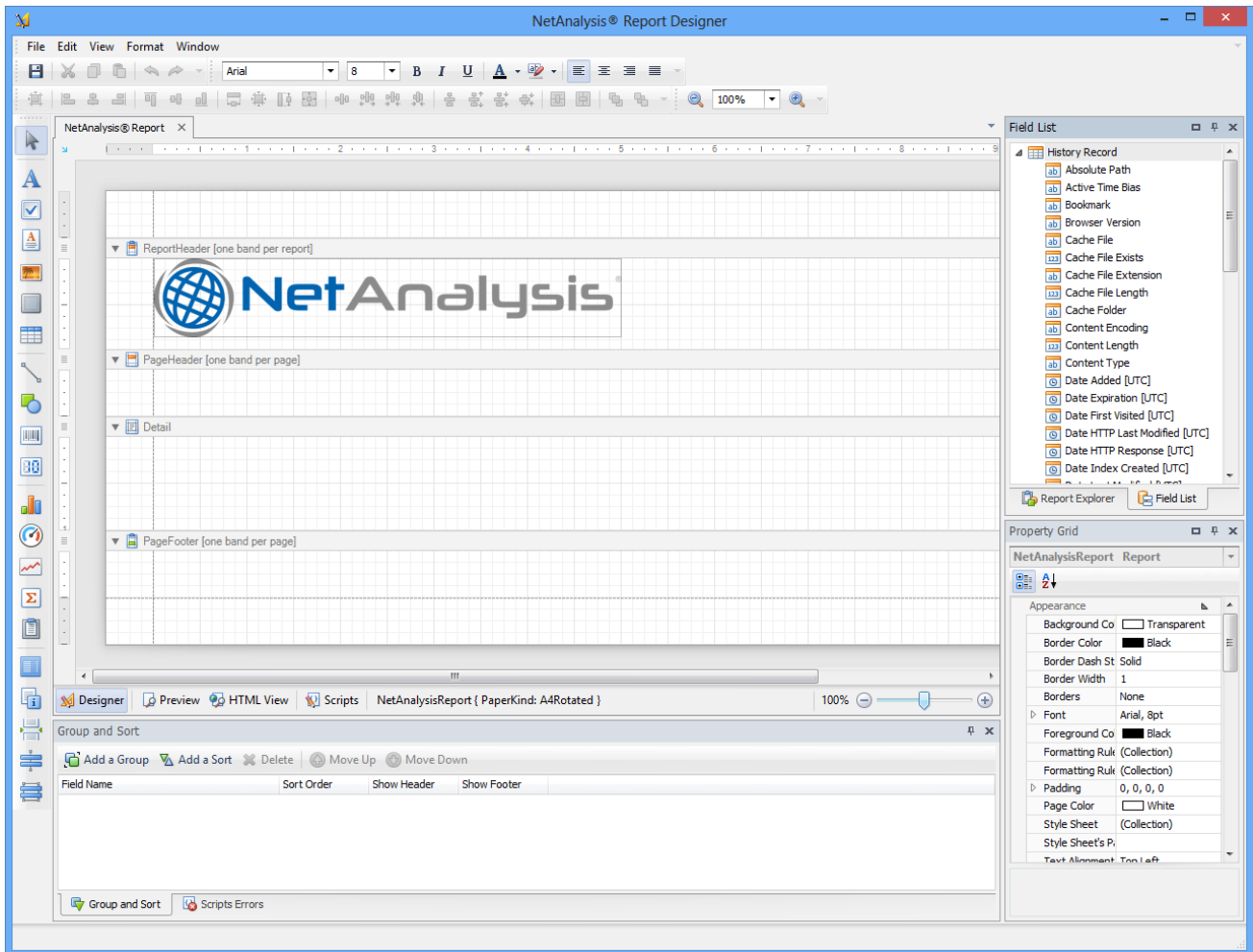
NetAnalysis v2.0
Licensed to Digital Detective

1/2

Page 1 of 2

100%

The above window shows the Detailed Report preview.



The Report Designer provides the user with the capability to create new reports from scratch and fully customise them. Reports can be previewed, printed and exported in a variety of formats.

The screenshot displays the NetAnalysis Report Designer application. The main workspace shows a report template with the following sections:

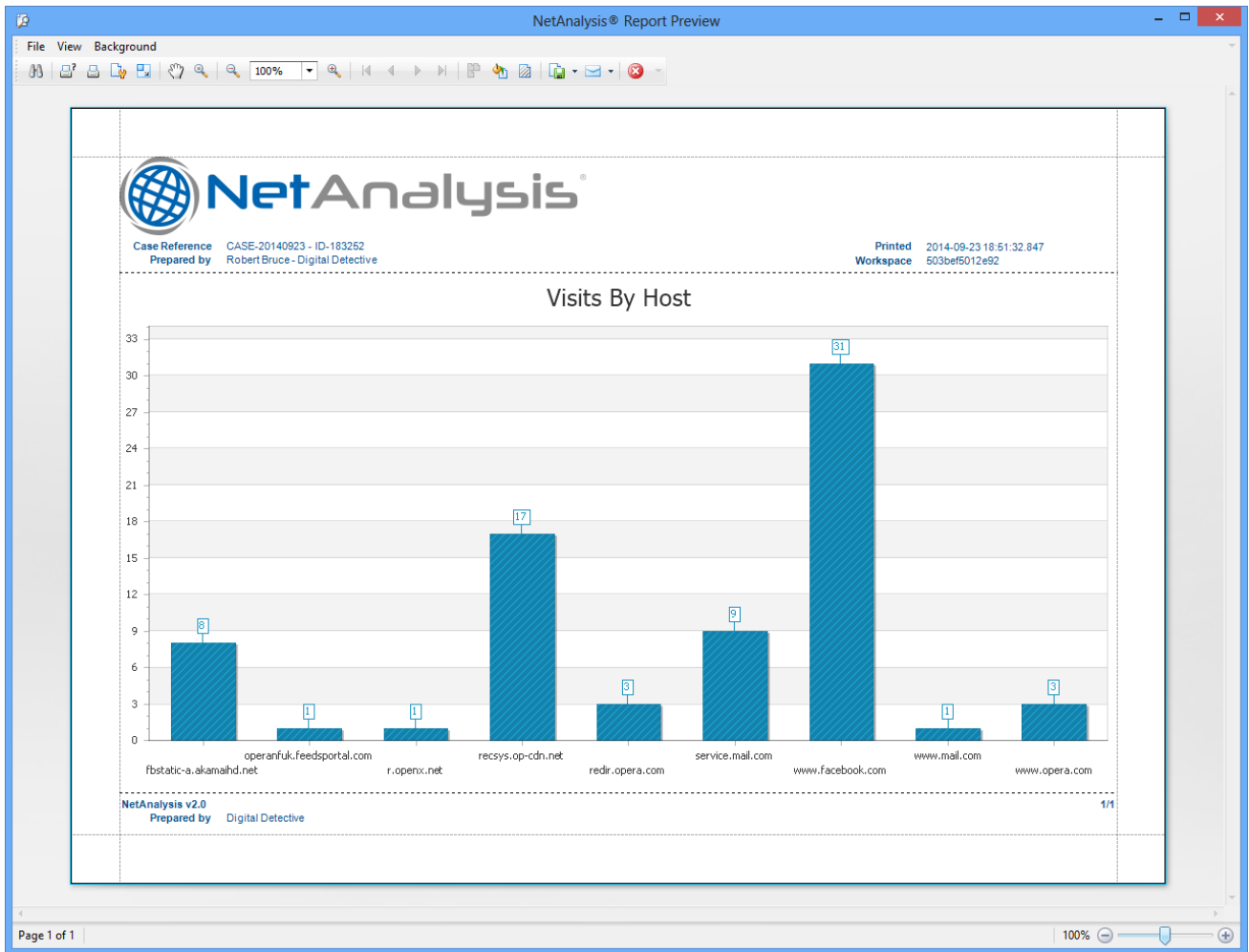
- ReportHeader** (one band per report): Contains the NetAnalysis logo.
- PageHeader** (one band per page): Includes fields for Case Reference, Prepared by, Printed, and Workspace.
- Detail**: A table with the following fields:

Field	Value
[Bookmark]	
Scheme	[Scheme]
Entry Type	[Entry Type]
Date Visited [Local]	[Date Visited [Local]]
Date Visited [UTC]	[Date Visited [UTC]]
Source File	[Source File]
Visits	[Visits]
Page Title	[Page Title]
URL	[URL]
Search Term	[Search Term]
Browser Version	[Browser Version]
Time Zone	[Parameters.TimeZone]
Record U	
Source Of	
- PageFooter** (one band per page): Includes fields for SoftwareVersion and Licensed to.

On the right side, the **Field List** panel shows a list of available fields, including History Record, Absolute Path, Active Time Bias, Bookmark, Browser Version, Cache File, Cache File Exists, Cache File Extension, Cache File Length, Cache Folder, Content Encoding, Content Length, Content Type, Date Added [UTC], Date Expiration [UTC], Date First Visited [UTC], Date HTTP Last Modified [UTC], Date HTTP Response [UTC], and Date Index Created [UTC].

The **Property Grid** panel shows the appearance settings for the report, including Background Color (Transparent), Border Color (Black), Border Dash Style (Solid), Border Width (1), Borders (None), Font (Arial, 8.25pt), Foreground Color (Black), and Text Alignment (Top Left).

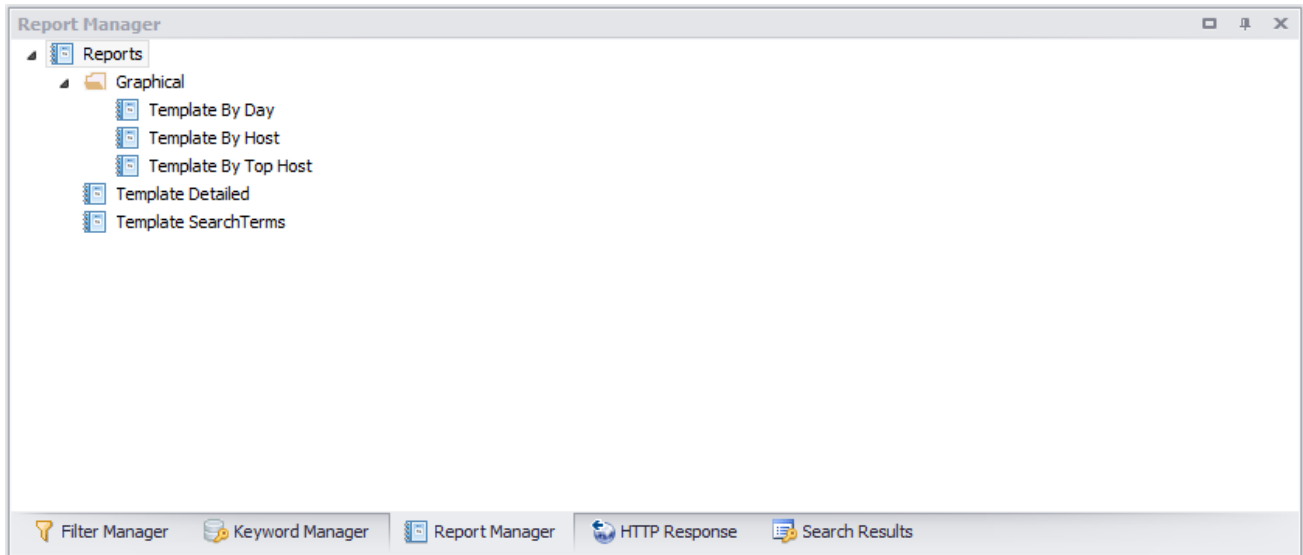
At the bottom, the **Group and Sort** panel provides options to Add a Group, Add a Sort, Delete, Move Up, and Move Down. It also includes a table for defining field names, sort orders, and whether to show headers or footers.



The above report shows a chart which breakdowns the visit by host for a specific day.

Report Manager

The Report Manager allows the user to categorise and store report templates. Report templates can be reused at any time.



The above window shows the report manager displaying a number of report templates.



Case Reference CASE-20140923 - ID-183252
 Prepared by Robert Bruce - Digital Detective

Printed 2014-09-23 18:47:01.010
 Workspace 503bef5012e92

Damien Smithers Facebook registration

Scheme	https	Browser Version	Opera v15-24 (Stash v4)	Record URN	2999
Entry Type	Stash	Time Zone	GMT Standard Time	Source Offset	ID: 1
Date Visited [Local]	2014-05-12 17:11:17.550				
Date Visited [UTC]	2014-05-12 16:11:17.550				
Source File	\digital01\Scenario Data Sets\Damien Smithers\Damien Smithers - Session 5\Roaming\Opera Software\Opera Stable\stash.db				
Visits					
Page Title	Facebook				
URL	https://www.facebook.com/register/confirm.php?ce=damiensmithers%40techie.com				
Search Term					

Scheme	http	Browser Version	Opera v15-24 (History v28)	Record URN	31
Entry Type	History	Time Zone	GMT Standard Time	Source Offset	ID: 18
Date Visited [Local]	2014-05-12 17:11:17.986				
Date Visited [UTC]	2014-05-12 16:11:17.986				
Source File	\digital01\Scenario Data Sets\Damien Smithers\Damien Smithers - Session 5\Roaming\Opera Software\Opera Stable\History				
Visits	1				
Page Title					
URL	http://service.mail.com/mcstarter/mail.html?sid=20796913904:587219JPTx3-mbQcIL3sl_v1ahZbMO2UNbLUh:11&partnerdata=partner.anonymous#				
Search Term					

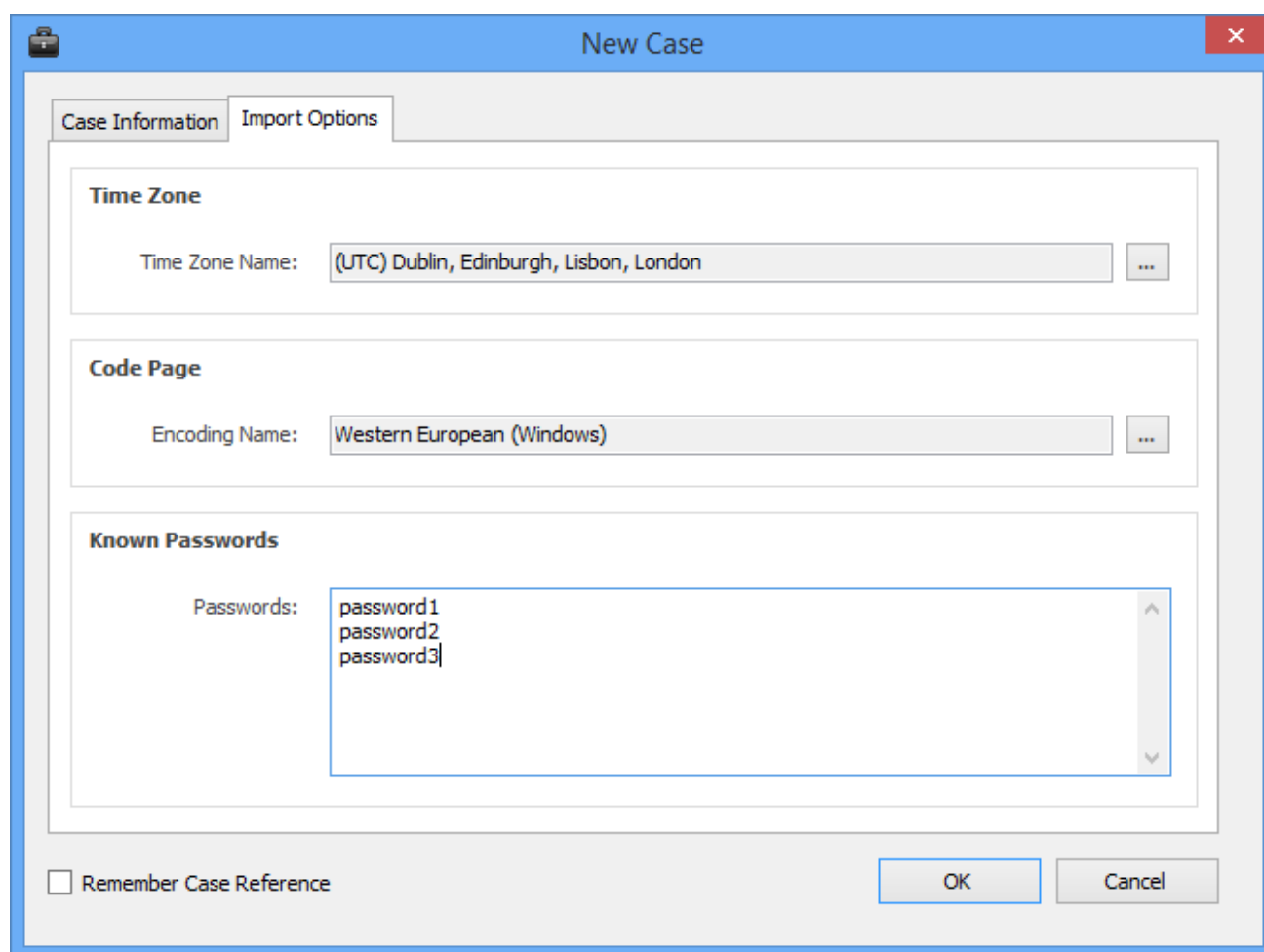
Reports can be saved in a number of formats such as PDF, MHT, RTF, XLS, XLSX, CSV, Text and Images. The above example shows a report in PDF format.

Username and Password Decryption

Most web browsers include a Password Manager so that the usernames and passwords required to log in to websites can be securely stored. These usernames and passwords are often encrypted and stored in a file in the user profile. 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.

Firefox and Mozilla Based Browsers

With NetAnalysis® v2.1, we have added the ability to decrypt and display any stored usernames and passwords for Mozilla Firefox and any browsers based on Mozilla. If a Master Password is known to the forensic examiner, he/she can enter this information when starting a new case.



The screenshot shows the 'New Case' dialog box with the following details:

- Case Information** tab selected.
- Time Zone**: Time Zone Name: (UTC) Dublin, Edinburgh, Lisbon, London
- Code Page**: Encoding Name: Western European (Windows)
- Known Passwords**: Passwords: password1, password2, password3
- Remember Case Reference
- Buttons: OK, Cancel

The screen above shows a number of known Master passwords added to the list so NetAnalysis® can check each one for validity. If the Master password is correct, the stored usernames and passwords will be displayed

in the grid and the information field for the appropriate records.

The screenshot shows the NetAnalysis v2.1 interface. At the top, there is a menu bar (File, View, Tools, Search, Index, Filter, Reports, Column, Window, Help) and a toolbar. Below the toolbar is a 'Preview URL' field containing 'https://www.'. A table displays logon records with columns for Port, User, Logon User, Logon Password, and Redirect URL. A red box highlights a record with Port 443, User 'ian.richardson', Logon User 'ian.richardson@activist.com', and Logon Password '28374ydsfsd'. Below the table is an 'Information' panel for the selected record, containing fields 1 through 14. Red arrows point from numbered boxes (1-5) to specific fields in the information panel: 1 points to 'Master password: <empty>', 2 points to 'Username Field: email', 3 points to 'Decrypted Username: ian.richardson@activist.com', 4 points to 'Decrypted Password: 28374ydsfsd', and 5 points to 'Date Last Used [UTC]: 2014-05-15 14:53:13.997'.

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		

```

1 Master password: <empty>
2 Hostname:
3 Username Field: email
4 Encrypted Username: MDoEEPgAAAAAAAAAAAAAAAAAAEWfYIKoZIHvcNAwcEConXd7T+jOrRBCCQpF1MB1N4r6Xd9wx9Mmoo5WIDZ1V5Qf+8nDI6B43Dcg==
5 Decrypted Username: ian.richardson@activist.com
6 Password Field: pass
7 Encrypted Password: MDoEEPgAAAAAAAAAAAAAAAAAAEWfYIKoZIHvcNAwcEConXd7T+jOrRBCCQpF1MB1N4r6Xd9wx9Mmoo5WIDZ1V5Qf+8nDI6B43Dcg==
8 Decrypted Password: 28374ydsfsd
9 Date Last Used [UTC]: 2014-05-15 14:53:13.997
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}
  
```

In the example above, the various fields identified by the numbers above are explained in the table below. Any decrypted usernames and passwords are also displayed in the Logon User and Logon Password columns.

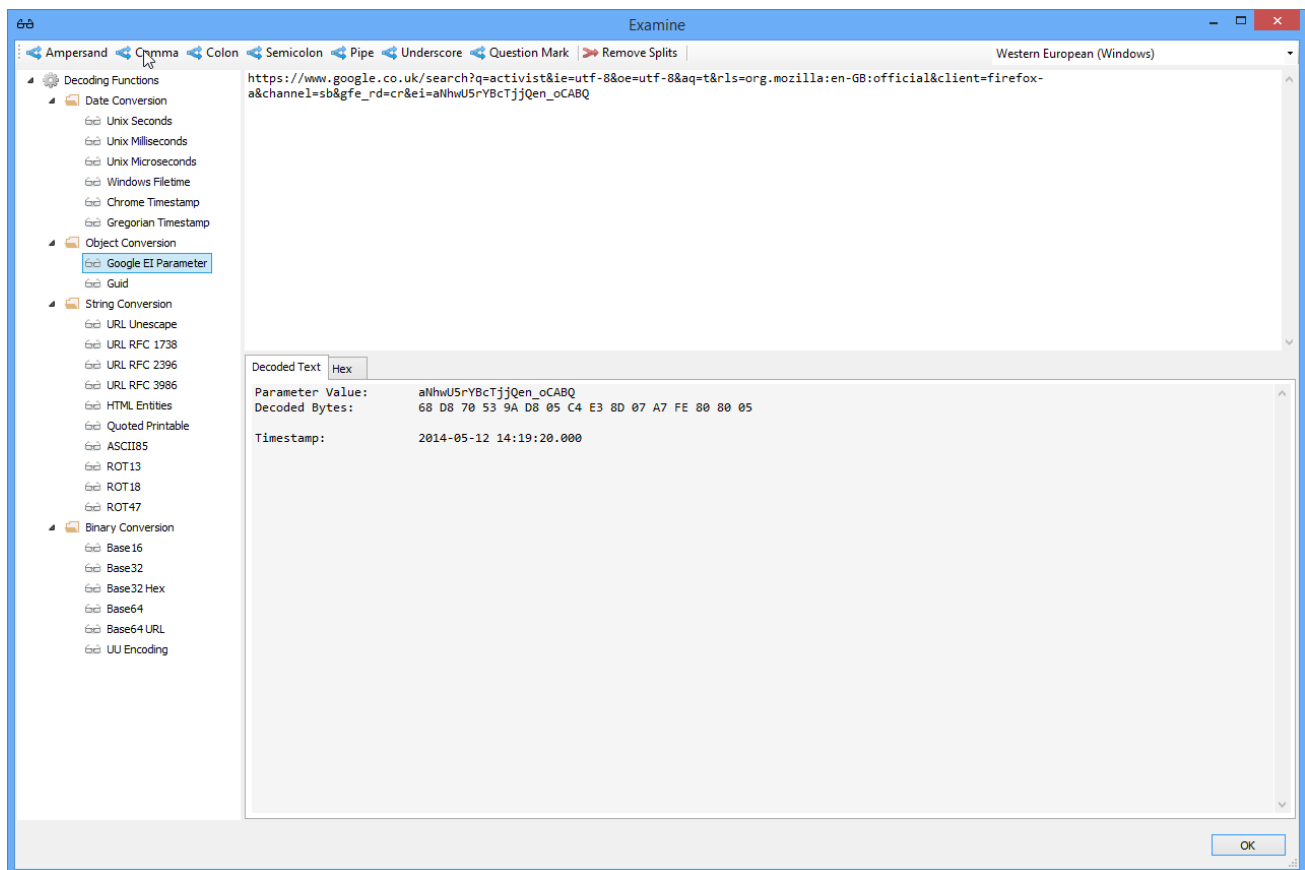
Number	Information
1	Master Password: This value is shown as empty which indicates no master password has been set. If the correct master password was provided, then it would be displayed here.
2	Username Field: This value shows the field name used to identify the username value. In this case, it is 'email'
3	Decrypted Username: This value shows the decrypted string for the username field.
4	Password Field: This value shows the field name used to identify the password value. In this case, it is 'pass'.
5	Decrypted Password: This value shows the decrypted string for the password field.

New Artefacts in v2.1

The following shows some of the new artefacts that have been added to NetAnalysis® v2.1.

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 below.



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.

The screenshot displays the NetAnalysis v2.1 interface for a 'New Case'. The main data table is as follows:

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL	Browser Version	Decoded URL
Autofill Profile						2F765E0-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)	

The selected profile's details are shown in the 'Information' pane:

```

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

The 'Index Text' pane shows the extracted data for the selected profile:

```

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
  
```

The status bar at the bottom shows the source path: \\digital01\Browser Data Windows\...\Default\Web Data and the 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.

The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main table shows three entries of type 'Credit Card'.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL	Browser Version	Decoded URL
Credit Card						11880E81-7583-4248-AE5E-5680B92D671D	Google Chrome v0-40 (Auto-fill Credit Cards v59)	
Credit Card						ABB1444C-BDD8-4345-B968-64F99F59A004	Google Chrome v0-40 (Auto-fill Credit Cards v59)	
Credit Card						CEF8818D-9B37-4194-B5DD-C92A593B8A2C	Google Chrome v0-40 (Auto-fill Credit Cards v59)	

The selected entry (GUID: ABB1444C-BDD8-4345-B968-64F99F59A004) is expanded to show the following details:

Information

- 1 Guid: ABB1444C-BDD8-4345-B968-64F99F59A004
- 2 Date Modified: 2015-01-28 14:16:22.000
- 3 Origin: Chrome settings

Index Text

```
credit_cards
Guid: ABB1444C-BDD8-4345-B968-64F99F59A004
Name on card: Mr G Likley
Expiration month: 7
Expiration year: 2017
Card number encrypted:
01000000008C90DF0115D1118C7A00C04FC297EB010000090579BCD88CF8E49BC35CDE5A4215A800000000200000000010660000000100002000000038827B4C631B32CC381E78CA2E980EFC8A079EA4CB360982
0DE7CD5A799FBF9400000000E8000000002000020000001316C6C6823D49AB50DEC00C857CA6E7FF5C22D94FFFD1031D685F277E95031000000063C1BEE76AC2E2E224C19C3B45DEA77C400000007491B443CC2E353824F
32AC440FE9523F1C776F869C27A15893A5784DADB3092ADF9C8AB7A8AAACE5A50D15CF4E04200C4C60A5F2AB8BDBEAC8340D480A94F2C
```

The status bar at the bottom shows the file path: \\digital01\Browser Data Windows\...\Default\Web Data and 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.

The screenshot displays the NetAnalysis v2.1 interface for a 'New Case'. The main window shows a table of search engine entries. The selected entry is for 'Ask Jeeves' with the URL `http://uk.ask.com/web?q={searchTerms}`. Below the table, the 'Information' panel provides details for this entry.

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

Record 4 of 5

[Entry Type] = 'Search Engine'

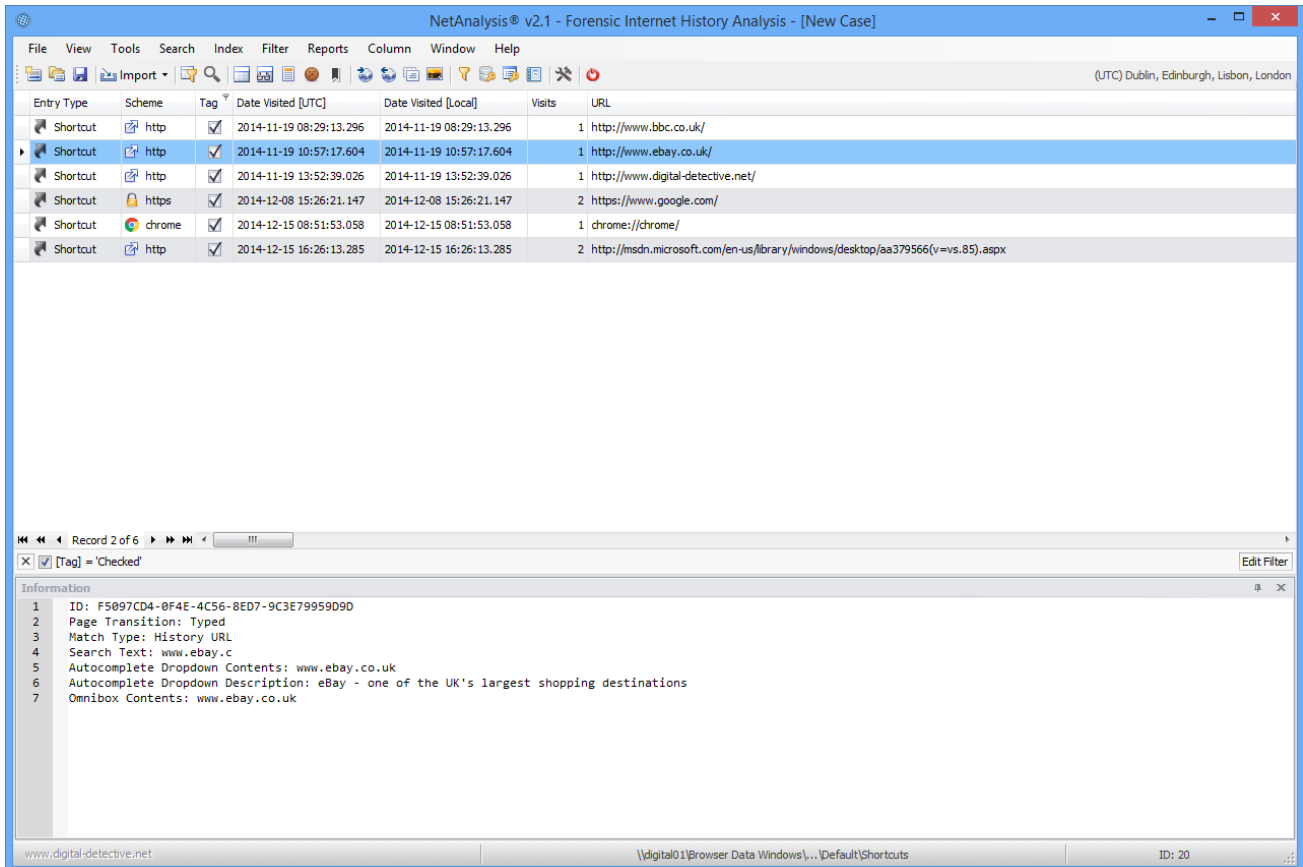
Information

- Short Name: Ask Jeeves
- Keyword: uk.ask.com
- Favicon URL: http://sp.uk.ask.com/sh/1/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}&l1=ff
- Prepopulate ID: 4
- Date Last Modified: 2014-11-19 13:49:01.000
- Sync Guid: E0F9A785-85BC-4268-9166-38F636E1D150
- Alternate URLs: []

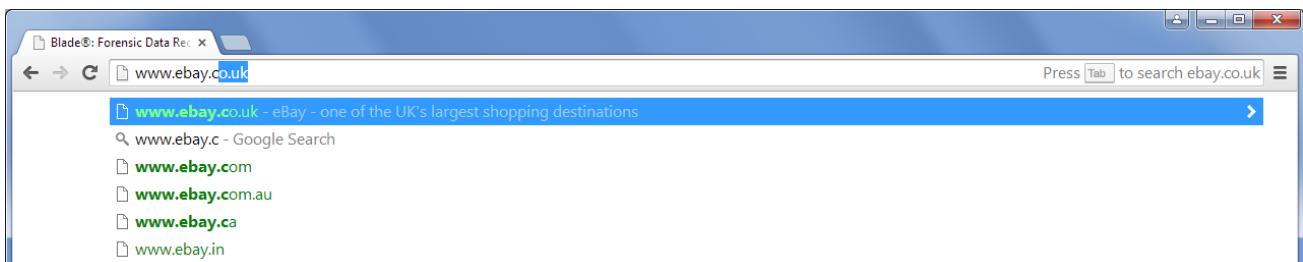
www.digital-detective.net | \\digital01\Browser Data Windows\... \Default\Web Data | ID: 5

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.

The screenshot displays the NetAnalysis v2.1 interface. At the top, the title bar reads "NetAnalysis® v2.1 - Forensic Internet History Analysis - [HDG-4 - Richardson]". The menu bar includes File, View, Tools, Search, Index, Filter, Reports, Column, Window, and Help. The main window shows a "Preview URL" field with "https://www..." and a table of logon data.

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		

Below the table, the "Information" pane for the selected entry (Record 3 of 5) is shown:

```

1 Master password: <empt>
2 Hostname:
3 Username Field: email
4 Encrypted Username: MDoEEPgAAA_AAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwECOnXd7T+jOrRBCCQpF1MB1M4r6Xd9wx9Mmoo5W1DZ1V5QF+8nDI6B43Dcg==
5 Decrypted Username: ian.richardson@activist.com
6 Password Field: pass
7 Encrypted Password: MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwECaw+kpg5IHUnBbCrbzd2cNuK8ZJ04+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}
  
```

Red arrows in the image point from the "Logon User" and "Logon Password" columns of the table to the corresponding fields in the "Information" pane, illustrating the decryption process.

Mozilla Firefox moz_hosts and moz_inphistory

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.

The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main window shows a table with the following data:

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/

Below the table, the interface shows navigation controls for 'Record 7 of 8' and a filter set to '[Tag] = 'Checked''. An 'Information' pane at the bottom left displays the following details for the selected record:

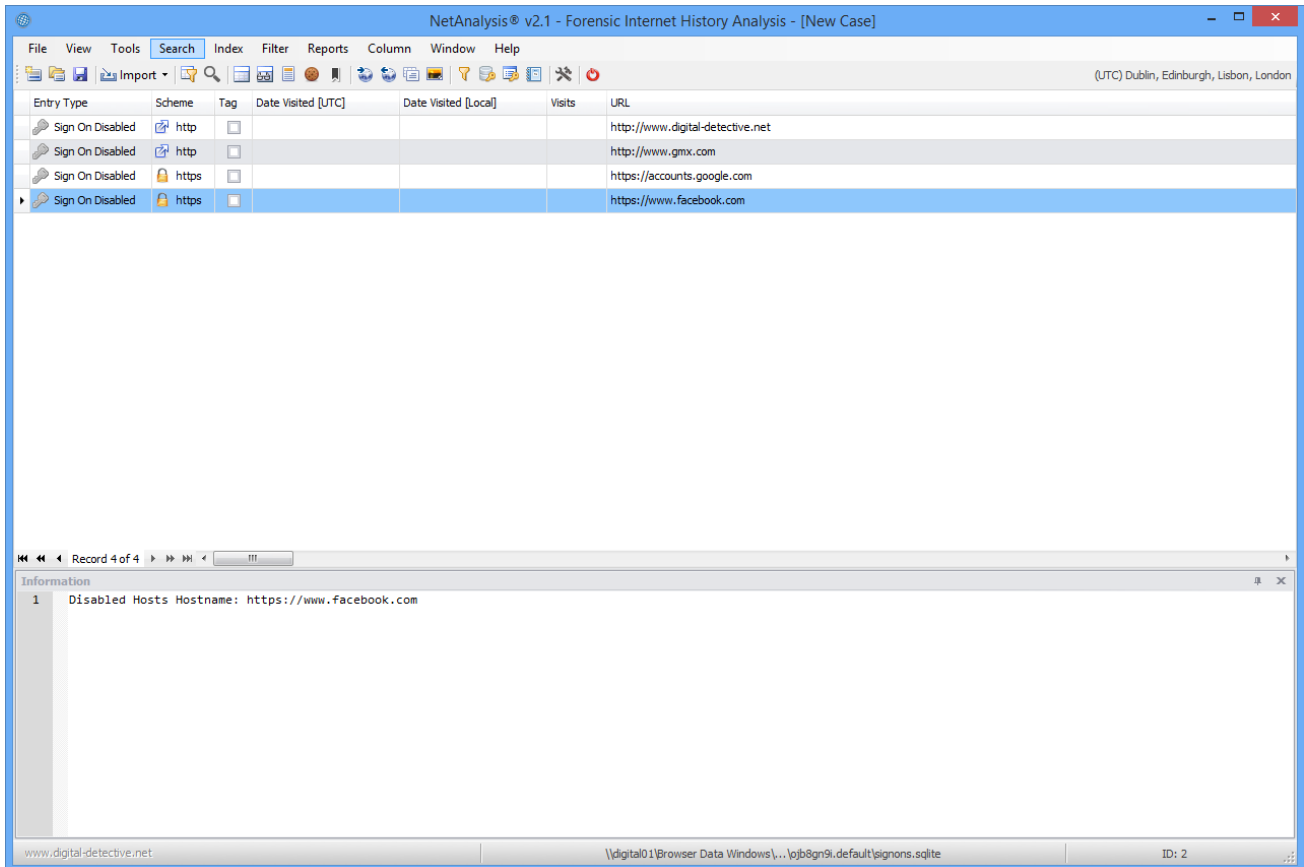
```

1 Input: youtube
2 Use Count: 0
  
```

The status bar at the bottom of the window shows the website 'www.digital-detective.net', the file path '\\digital01\Browser Data Windows\... \w9cv1yzh.default\places.sqlite', and the 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.



The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main window shows a table of disabled hosts entries. The table has columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The entries are as follows:

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Sign On Disabled	http					http://www.digital-detective.net
Sign On Disabled	http					http://www.gmx.com
Sign On Disabled	https					https://accounts.google.com
Sign On Disabled	https					https://www.facebook.com

Below the table, the 'Information' pane shows details for the selected entry (Record 4 of 4):

```
1 Disabled Hosts Hostname: https://www.facebook.com
```

The status bar at the bottom indicates the current URL is `www.digital-detective.net`, the file path is `\\digital01\Browser Data Windows\...lojb8gn9i.default\signons.sqlite`, and the ID is 2.

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

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

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

Record 5 of 8

[Tag] = 'Checked'

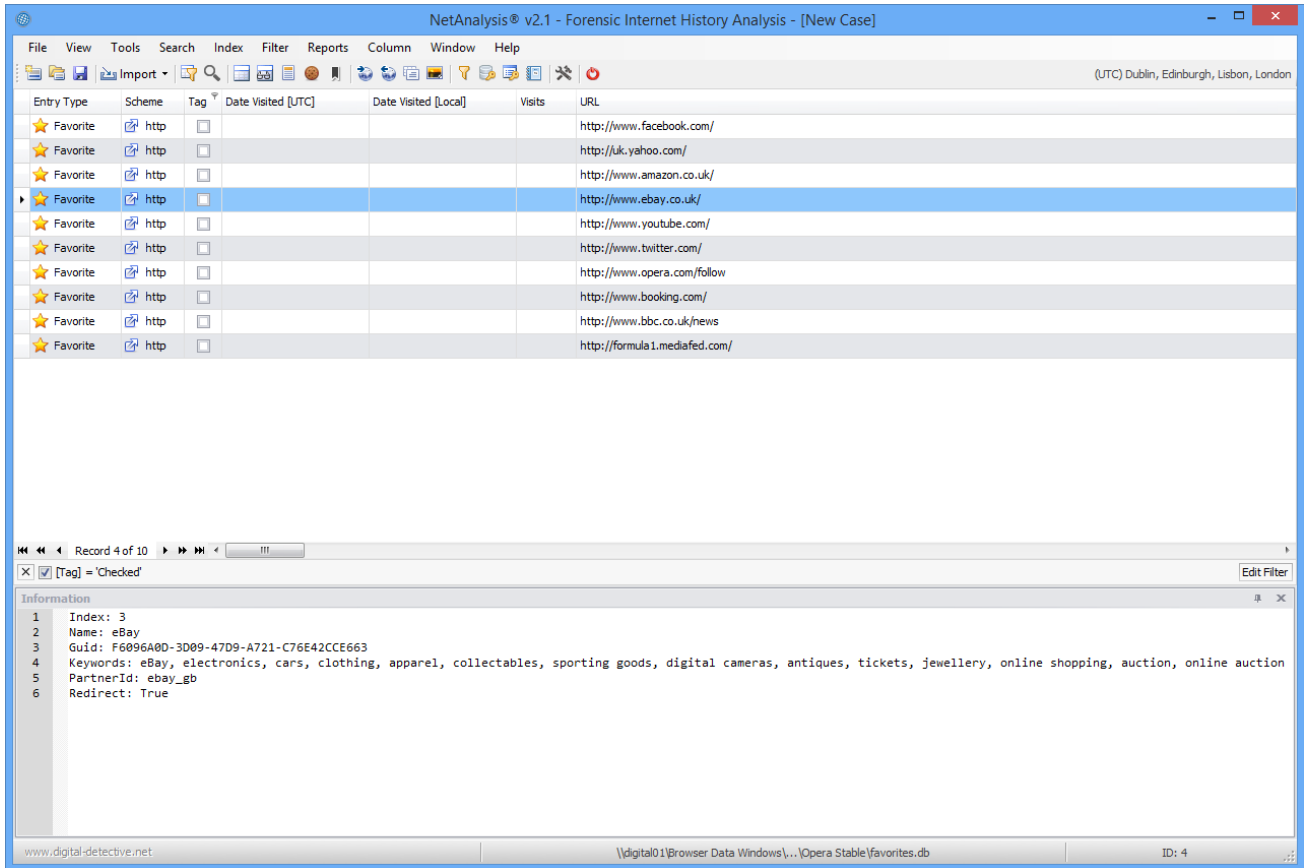
Information

- 1 Web Bookmark UUID: 2EB4612B-3447-2040-B4AC-6008C50F6959
- 2 Date Last Fetched: 2015-01-28 08:56:59.000
- 3 Date Last Viewed: 2015-01-28 08:58:03.000
- 4 Root Web Bookmark UUID: 0B485B1A-4152-FC48-A035-924C1C9BF316
- 5 Root Title: com.apple.ReadingList
- 6 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.



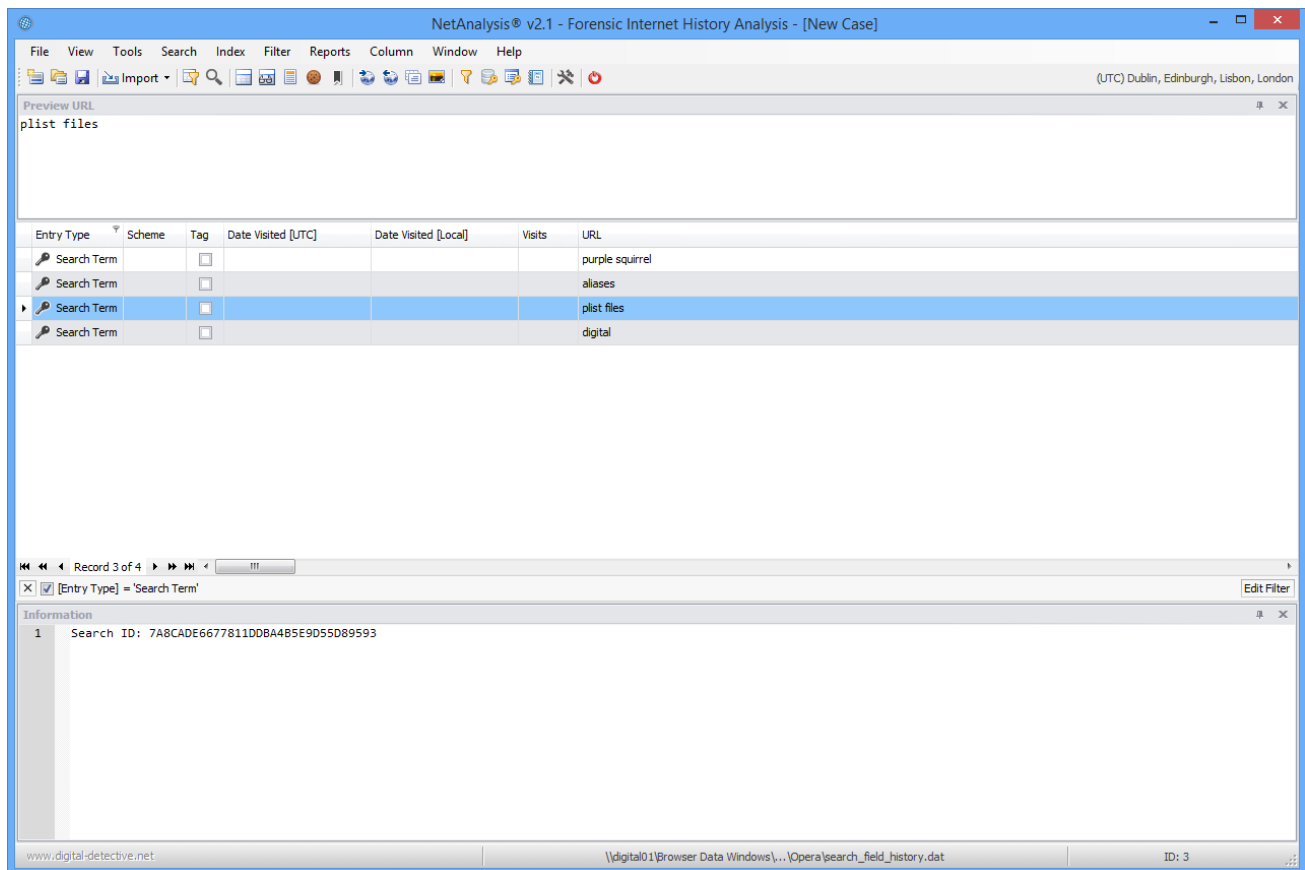
The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main window shows a table of favorite entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The fourth entry, for the URL <http://www.ebay.co.uk/>, is selected and highlighted in blue. Below the table, a filter is applied: [Tag] = 'Checked'. The information panel for the selected entry shows the following details:

Index	Value
1	Index: 3
2	Name: eBay
3	Guid: F6096A00-3D09-47D9-A721-C76E42CCE663
4	Keywords: eBay, electronics, cars, clothing, apparel, collectables, sporting goods, digital cameras, antiques, tickets, jewellery, online shopping, auction, online auction
5	PartnerId: ebay_gb
6	Redirect: True

The status bar at the bottom indicates the file path: \\digital01\Browser Data Windows\...\Opera Stable\favorites.db and the record ID: 4.

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.



The screenshot displays the NetAnalysis v2.1 interface for forensic internet history analysis. The main window shows a table of search entries. The 'Preview URL' field contains 'plist files'. The table below lists search terms and their corresponding URLs.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Search Term		<input type="checkbox"/>				purple squirrel
Search Term		<input type="checkbox"/>				aliases
Search Term		<input type="checkbox"/>				plist files
Search Term		<input type="checkbox"/>				digital

Navigation controls at the bottom indicate 'Record 3 of 4' and a filter for '[Entry Type] = Search Term'. An information panel shows the search ID: 7A8CADE6677811D0BA485E9D55089593.

www.digital-detective.net | \\digital01\Browser Data Windows\...\Opera\search_field_history.dat | ID: 3

New Artefacts in v2.2

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.2.

New Browser Support

We have added support for the following browsers:

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.

Tina 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 the extraction of icons and associated Favicon images to the export folder for the following browsers:

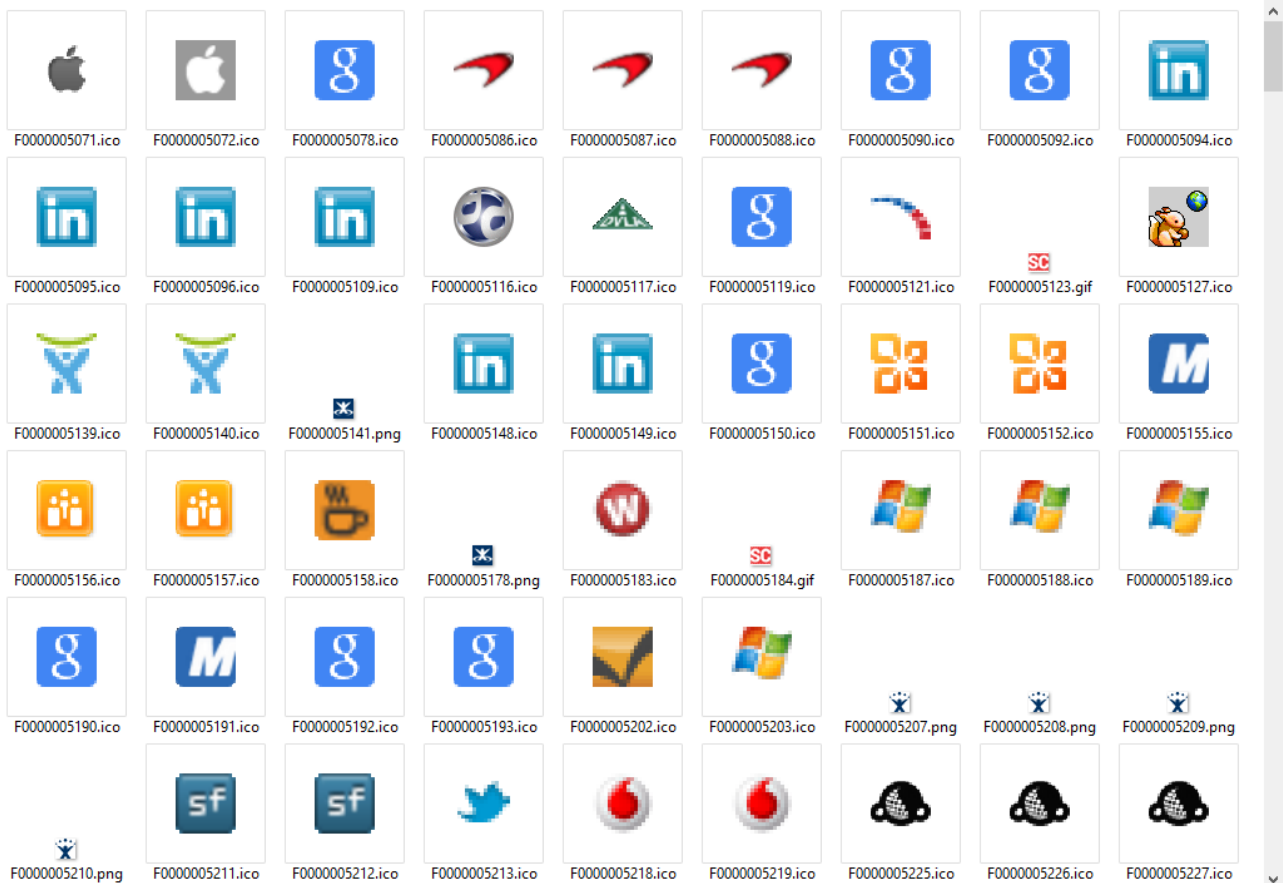
- Apple Safari
- Google Chrome and Chromium Based Browsers
- Mozilla Firefox and Mozilla Based Browsers
- Opera (Presto)
- Opera

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							
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=	
Favicon	http	✓				http://www.google.co.uk/search?client=safari&rls=en&q	
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-3	
Favicon	https	✓				https://www.mdarens.com/webapp/wcs/stores/servi	
Favicon	https	✓				https://www.mdarens.com/webapp/wcs/stores/servi	
Favicon	http	✓				http://www.applausestore.com/process-order.php	
Favicon	http	✓				http://www.google.co.uk/search?client=safari&rls=en&q	
Favicon	http	✓				http://support.digital-detective.co.uk/WebSupport/Supp	
Favicon	http	✓				http://support.digital-detective.co.uk/WebSupport/Login	

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.

The screenshot displays the NetAnalysis v2.2 interface for forensic internet history analysis. The main window shows a table of entries with the following data:

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

The selected record (History) is expanded to show the following information:

```

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

```

The interface also shows a navigation bar with "Record 3 of 5" and a filter dropdown set to "[Tag] = 'Checked'". The status bar at the bottom indicates the current URL is "www.digital-detective.net" and the file path is "Z:\Google Chrome v43\2015_05_31_16_24_21_503\...\Default\History".

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), l (capital i) and I (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:

The screenshot shows the 'Examine' window with a list of decoding functions on the left and a decoding result on the right. The 'Base58' function is selected under 'Binary Conversion'.

Example Bitcoin Address: `3J98t1WpEZ73CNmQviecnyyiWnqRhwNLY`

Decoded Text	Hex
	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
00000010	6F 7C 3B 9F CB FC FC 02

Decoded Text: `r4f0%.Á7.¤.,İ±
o|;.Ëüü.`

New Artefacts in v2.3

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.3.

Introduction

This release brings official support for installing on Microsoft Windows 10. We have also added support for Microsoft's new minimalist web browser Edge.

There are some improvements with this release, such as improved logging when dealing with ESE/SQLite databases, as well as improved time zone error reporting. There have been some improvements to the progress log window where the user can now select and copy multiple log entries. There is also an option to save the entire log to a text file.




Microsoft Edge Browser

Microsoft Edge (formerly Project Spartan) is the name of Microsoft's next-generation web browser built into Windows 10. The browser, both in name and its core rendering engine, are set to replace the ageing Internet Explorer, although parts of IE11 remains for legacy websites.

The data storage for Microsoft Edge, in many ways, is similar to Internet Explorer; however, there are some database structure changes as well as data location changes. Edge also introduces a new way of storing download information; we have updated NetAnalysis® to identify and interpret this new structure.

NetAnalysis® v2.3 supports Microsoft Edge, as well as introducing support for the new Reading List feature.

Reading List and Reading View

The Reading List is a feature in Microsoft Edge where the user can save articles to read later. In addition, it features a Reading View that strips out adverts and page clutter, making it much easier to read articles on different platforms. It also has an option for capturing a web page and making annotations directly to the page. To change between the standard website view mode and the Reading View mode, the user clicks the  button

to the right of the Web address.

The screenshot shows a web browser window displaying the BBC Sport website. The address bar shows bbc.co.uk/sport/0/formula1/34513738. The page features a yellow header with 'SPORT FORMULA 1' and navigation links for Home, Football, Formula 1, Cricket, Rugby U, Rugby L, Tennis, Golf, and Athletics. Below the header is a navigation bar with links for Results, Standings, Race Calendar, Gossip, Teams, and Drivers. The main content area displays a large image of two men in Red Bull racing suits, with the headline 'Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey'. The article is dated 13 October 2015 and has 2.6K shares. A 'READING LIST' sidebar on the right contains several related articles, including one about Porsche Great Britain.

BBC Sign in News Sport Weather iPlayer TV Radio

SPORT FORMULA 1

Home Football Formula 1 Cricket Rugby U Rugby L Tennis Golf Athletics

Results Standings Race Calendar Gossip Teams Drivers

Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey

13 October 2015
Last updated at 10:50
2.6K
Share

Red Bull could quit Formula 1 because rival manufacturers are too fearful of supplying them with engines, according to their chief technical officer.

READING LIST

Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey
bbc.co.uk

Last week

Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey
bbc.co.uk

'Rivals' fear may mean Red Bull exit'
bbc.co.uk

Digital Detective | NetAnalysis® v2.2 and HstEx® v4.2 Released
digital-detective.net

Porsche Great Britain - Dr. Ing. h.c. F.

The screenshot shows the article content from the BBC Sport website. The address bar shows bbc.co.uk/sport/0/formula1/34513738. The main content area displays a large image of two men in Red Bull racing suits, with the headline 'Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey'. The article is dated 13 October 2015 and has 2.6K shares. A 'READING LIST' sidebar on the right contains several related articles, including one about Porsche Great Britain.

Red Bull: Rivals' 'fear' may mean F1 exit – Adrian Newey

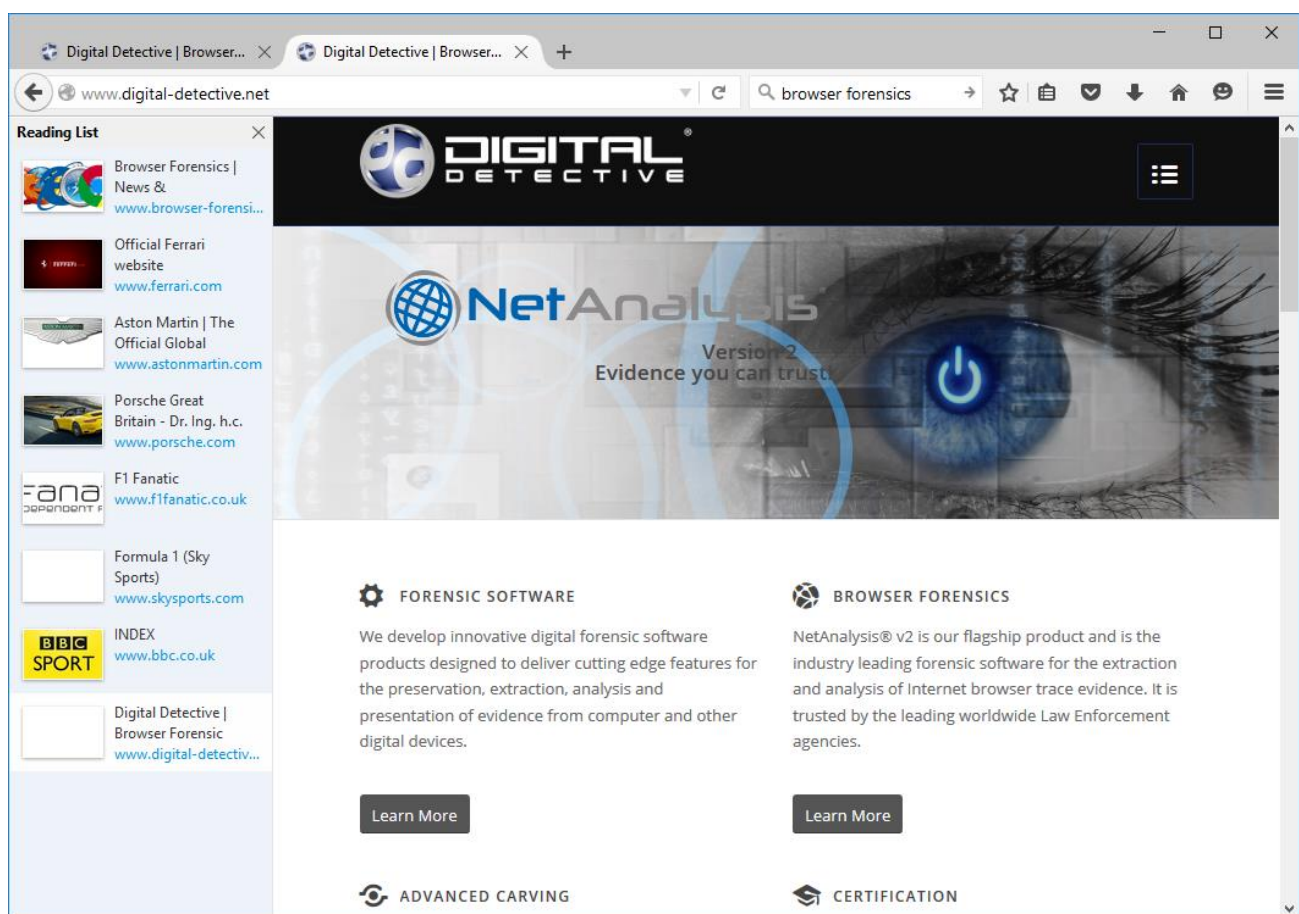
Red Bull could quit Formula 1 because rival manufacturers are too fearful of supplying them with engines, according to their chief technical officer.

BBC Sport | 13 October 2015

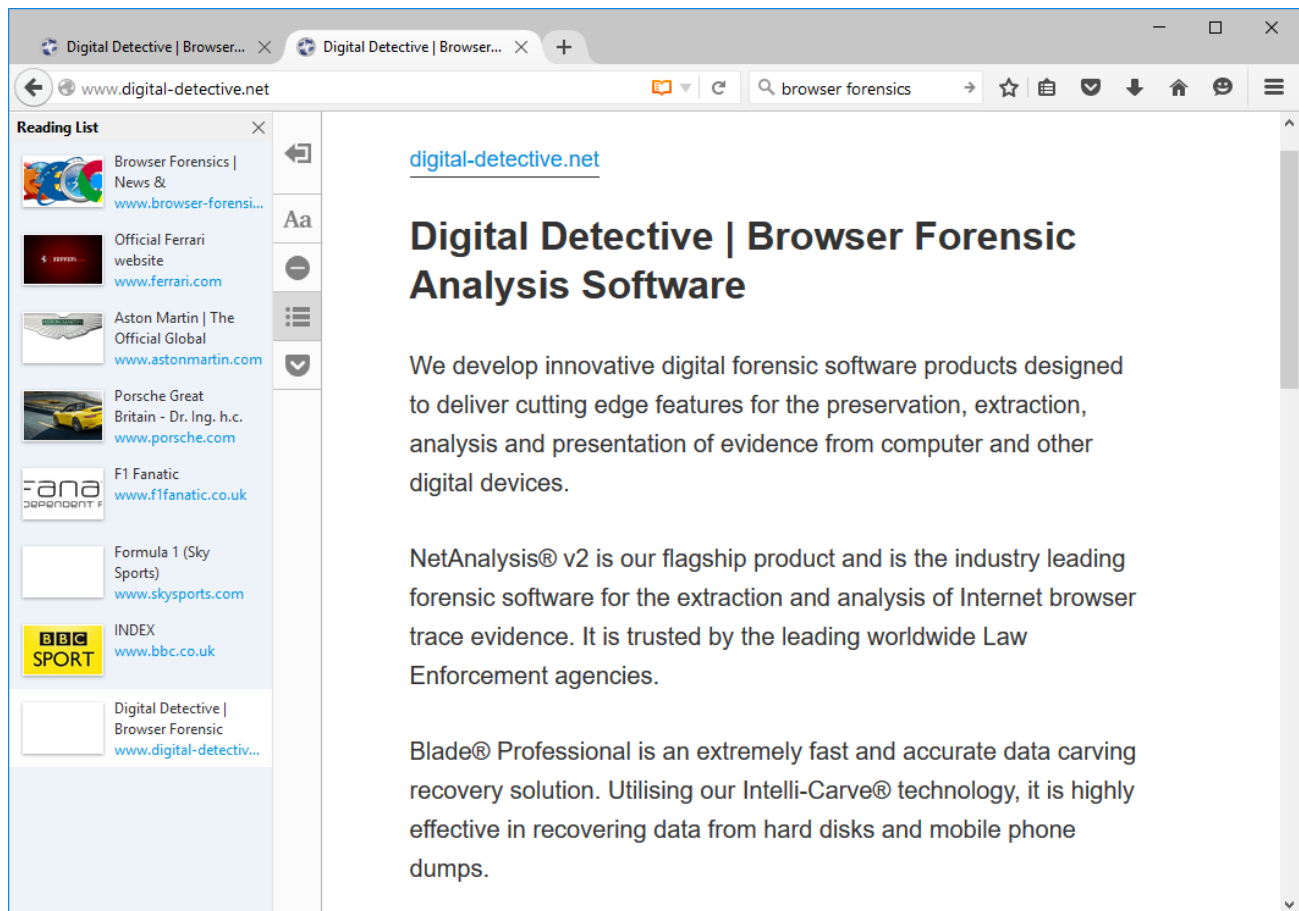
NetAnalysis® v2.3 can rebuild pages that have been stored in Reading View mode and display them in the internal viewer.

Mozilla Firefox Reading List

Mozilla Firefox has also introduced a Reading List feature in Firefox version 38.0 beta. This allows users to save links to web pages to be able to read them later.



The browser also has a Reading View mode.



NetAnalysis® v2.3 supports Mozilla Firefox Reading Lists.

Favicon Display

A favicon (short for favourite icon), also known as a shortcut icon, Web site icon, tab icon or bookmark icon, is a file containing one or more small icons, associated with a particular website or web page. NetAnalysis® v2.3 now supports the extraction (and viewing) of SVG favicons in addition to the standard format icons. We have also added the ability to view these individual image files through our internal viewer.

New Artefacts in v2.4

The following pages outline some of the new artefacts that have been added to 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.

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-bandq-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&espv=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&espv=2&ie=UTF-8#q=fbi%20apple%20iphone%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&espv=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&rc=1&u=https://www.bbc.co.uk/news/world-us-canada-35914195&usq=QIIITAB&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&rc=1&u=https://www.bbc.co.uk/sport/formula1/35912379&usq=QIIITAB&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&espv=2&ie=UTF-8#q=digital%20detective%20jobs

Record 26 of 78

Information

- History ID: 25
- Total Visit Count: 1
- 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.

The screenshot displays the NetAnalysis v2.4 interface for forensic internet history analysis. The main window shows a table of Typed URLs with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected entry is a typed history entry for 'http://www.amazon.co.uk/' with 2 visits, recorded on 2016-02-26 at 11:16:04.310 UTC.

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

The information panel below the table provides detailed registry data for the selected entry:

```

1 Key Timestamp : 2016-03-23 13:54:33.021 UTC
2 Registry Key : HKEY_CURRENT_USER\Classes\Local
  Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
3 ur16 : http://www.amazon.co.uk/
4
5 Key Timestamp : 2016-03-23 14:04:58.710 UTC
6 Registry Key : HKEY_CURRENT_USER\Classes\Local
  Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsTime
7 ur16 : 2016-02-26 11:16:04.310
8
9 Key Timestamp : 2016-03-23 14:04:58.710 UTC
10 Registry Key : HKEY_CURRENT_USER\Classes\Local
  Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsVisitCount
11 ur16 : 2
  
```

The status bar at the bottom indicates the entry ID is 'ur16' and the registry path is 'E:\Browser Dump\Windows 10 Enterprise Registry\...\Windows\UsrClass.dat'.

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.

The screenshot displays the NetAnalysis v2.4 interface for forensic internet history analysis. The main window shows a list of Network Action Predictors for the URL `http://www.digital-detective.net/`. The table below summarizes the data shown in the interface.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Autocomplete Predictor		<input checked="" type="checkbox"/>				<code>http://www.digital-detective.net/</code>
Autocomplete Predictor		<input type="checkbox"/>				<code>http://www.digital-detective.net/</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/google-language-translator/css/style.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/themes/enfold/config-woocommerce/woocommerce-mod.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/themes/enfold/config-bbpress/bbpress-mod.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/page-list/css/page-list.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/rotatingtweets/css/style.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/syndicate-press/css/TinyLightbox.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/woocommerce-aella-currencyswitcher/design/css/frontend.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/plugins/woocommerce/assets/css/select2.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/themes/enfold/css/grid.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/themes/enfold/css/base.css?ver=d2fe58832951405364190353debea6a6</code>
Resource Prefetch Predictor	http	<input type="checkbox"/>				<code>http://www.digital-detective.net/wp-content/themes/enfold/css/layout.css?ver=d2fe58832951405364190353debea6a6</code>

The interface also includes a search filter at the bottom: `Contains([Information], 'www.dig')`. The information panel shows the following details for the selected entry:

```

1 ID: 23DC3E2C-472A-40A8-9C53-7648B8208E0D
2 User Text: www.dig
3 Number of Hits: 7
4 Number of Misses: 0
  
```

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]

Page Title: Used Cars

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Bookmark Folder		✓				
Bookmark Folder		✓				
Bookmark	http	✓				http://www.ebay.com/
Bookmark	http	✓				http://www.amazon.com/
Bookmark	http	✓				http://www.facebook.com/
Bookmark	http	✓				http://disney.go.com/
Bookmark	http	✓				http://www.wikipedia.org/
Reading List	http	✓				http://www.bbc.co.uk/sport/formula1/gossip
Reading List	https	✓				https://secure.currys.co.uk/gbuk/0/order-reservation.html
Reading List	http	✓				http://www2.mercedes-benz.co.uk/content/unitedkingdom/mpc/mpc_unitedkingdom_website/en/home_mpc/passengercars/home_new_c
Reading List	http	✓	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	✓	2014-07-23 14:41:04.000	2014-07-23 15:41:04.000		http://www.digital-detective.co.uk/
Bookmark Folder		✓				

Record 10 of 17

[Tag] = 'Checked'

Information

- Web Bookmark UUID: 9B8317CD-E84D-49F8-9A81-C86B3C886BD7
- Date Added [UTC]: 2015-07-30 22:36:38.000
- Date Last Fetched (Non Sync) [UTC]: 2015-12-14 10:24:31.000
- Title: Model lines
- Archive On Disk: True
- Fetch Result: 1
- Sync Server ID:

Index Text

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

Root Web Bookmark UUID: C136DFB9-837F-4212-A983-7FA1AD9A312A
Root Title: com.apple.ReadingList

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]

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

[Tag] = 'Checked'

Viewer

VirtualBox

Download VirtualBox

www.digital-detective.net | Y:\Opera Blink v36\2016_03_15_11_39_57_513\...\Opera Stable\Bookmarks | ID: 42

New Artefacts in v2.5

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.5.

Introduction

This release of NetAnalysis® brings support for some new browsers and new artefacts as well as adding support for the modified cache format in Mozilla Firefox. We have also added support for the new versions of the Microsoft Edge download object.

New Browser Support

We have added support for the following browsers:

360 Security Browser



360 Secure/Security Browser (360安全浏览器) is a web browser developed by the Qihu 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. It was first released in September 2008.

We have added support for the import of bookmarks which are stored in a format specific to 360 Security Browser. NetAnalysis® also now supports history and downloads from the earlier versions (v3-5) as well as all the standard artefacts from v6+. We also support the import of the UnClosed Pages SQLite database which contains information on pages saved by the user when the Browser was shut down.

360 Speed (Extreme) Browser



360 Speed (or 360 Extreme Explorer) Browser (360极速浏览器) is another freeware Chromium-based browser by the Qihu 360 Software Company. It offers a cloud synchronisation account and claims protection against phishing.

NetAnalysis® now supports the import of all the standard artefacts from 360 Speed Browser including the cross-domain Cookies found in v7.

UC Browser



UC Browser is a mobile browser developed by Chinese mobile Internet company UCWeb. Originally launched in April 2004 as a J2ME-only application, it is available on platforms including Android, iOS, Windows Phone, Symbian, Java ME, and BlackBerry.

With a huge user base in China, India, Indonesia, Pakistan and continued growth in emerging regional markets, UC Browser reached 100 million global users in March 2014. According to StatCounter, UC browser is the second most used smartphone/mobile web browser worldwide, passing Apple Safari in October 2015.

We have added support for the import of all the standard artefacts from UC Browser. NetAnalysis® will also import URL shortcuts from the UC Browser Omnibox SQLite database.

Updated Support for New Versions of Existing Browsers

Some of the mainstream browsers have made modifications to their file formats to add new features. NetAnalysis® has been updated to support these new file formats. We have also added support for the following files and databases:

Microsoft Edge v25 - 38 (EdgeHTML v14) Downloads

Microsoft has released new iterations of the download object stored in the iedownload container. We now support these latest versions.

Apple Safari v10

The latest version of Safari updated the Downloads.plist and the History.db database schema. NetAnalysis® v2.5 has been updated to support Apple Safari v10 history and downloads.

Additional Support for Existing Browsers

We have also added support for the following artefacts:

Mozilla Firefox Backup Bookmarks

Mozilla Firefox and many Mozilla Based Browsers backup their bookmark data to JSON format and more recently LZ4 compressed JSON format files. We have added support for the import of these file types into NetAnalysis®.

Opera Session Database

Opera v15-29 stored its tab and session data in a session.db SQLite database. We have now added support to NetAnalysis® for the import of this database.

Mozilla Firefox Cache

In the recent versions of Mozilla Firefox, the cache version 2 format has been updated. We have added support to NetAnalysis® (and HstEx®) for this new structure.

Google Chrome Segment Usage

Google Chrome and many Chromium-based browsers store URL segment and segment usage information in the History SQLite database. The segment usage information contains details on the number of visits per day to a particular segment. A segment is a generic and simplified version of a URL which means similar URLs may be grouped together as a single segment. This usage information allows the browser to calculate the highest ranked segments which can then be used for the most visited view. We have now added support for the import of these tables to NetAnalysis®.

Support for HstEx® Recovered Chromium Form History and Login Data

We have added a number of new artefacts in HstEx® v4.5. With Chromium-based browsers, you can now recover individual entries from the "logins" table located in the Login Data SQLite database. You can also recover individual entries from the "autofill" table located in the Web Data SQLite database. All of these artefacts can be recovered and loaded into NetAnalysis® for review and analysis.

Support for HstEx® Recovered Torch Browser Accelerated Downloads

Torch browser stores its downloads in the History SQLite database in a table called "accelerated_downloads". We have added the ability to recover these entries in HstEx® v4.5 and import them into NetAnalysis® for review.

New Features

We have added some new features to NetAnalysis® to make the software easier to use and to assist with productivity. We have also added some new analytical tools which can be used to drill down into the various artefacts of stored URL data and cookie values.

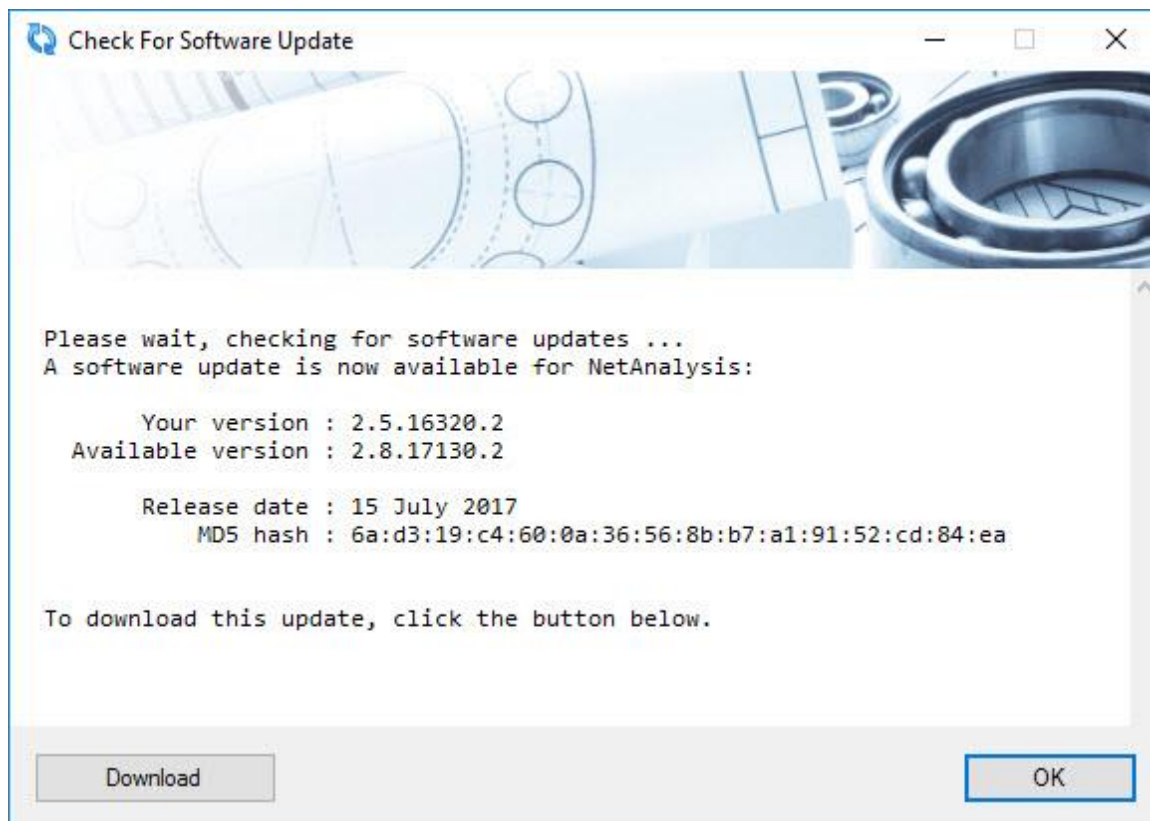
New Decoding/Analysis Options

To enhance the data analysis capabilities built-in to NetAnalysis®, we have added some new timestamp decoding support. In the data examination/analysis window, the user can now select:

- Mac Absolute,
- HFS+ (Mac OS), and
- OLE Automation timestamps.

Check for Software Update

In previous versions of NetAnalysis®, we had a feature to allow the user to check whether a new version of the software was available for download. We have had numerous requests to add this feature back, so from this release, you can check for new versions and get direct access to the latest download. This feature can be accessed from the Help menu by selecting Help » Check for software update.



New Artefacts in v2.6

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.6.

Introduction

This version of NetAnalysis® introduces support for a number of new browsers as well as adding support for Chromium Simple Cache format used by a number of the mobile browsers. We have also added support for Microsoft Internet Explorer and Edge Recovery Store, Tab Session, Travel Log, Roaming Tab Sessions and the detection of InPrivate browsing.

New Browser Support

We have added support for the following browsers:

Opera Neon



Opera Neon is a new concept browser: "a vision of what browsers could become". It was first released in January 2017 and is available for Mac and Windows. The browser is Chromium based but with some additional unique features. Opera Neon gives the user new ways to interact with web content, including the ability to drag, push and pop the tab icons.

NetAnalysis® will recover the standard Chromium based artefacts as well as the top sites, tab page icons and the gallery snapshots. The tab page icons and the gallery snapshots are written to the case export folder and loaded into the Viewer window.

Brave



Brave is another new, open-source, multi-platform web browser developed by Brave Software; it is based on the Chromium web browser and its Blink engine. It claims to block website trackers and remove intrusive Internet advertisements. The browser also claims to improve online privacy by sharing less data with advertising customers.

NetAnalysis® will recover the standard Chromium based artefacts.

Updated Support for New Versions of Existing Browsers

All of the mainstream browsers have updated their file formats and added new features. In addition to adding

new browser support, we have enhanced the support provided for existing browsers:

Google Chrome/Chromium Based Simple Cache for HTTP

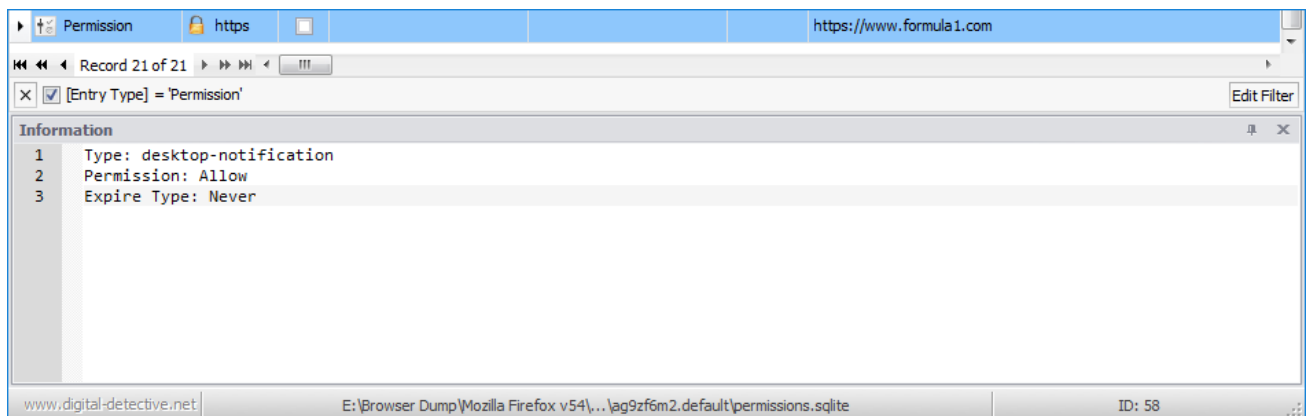
This disk cache is used by default in Google Chrome on Mac OS X, Linux and Android mobile devices. It can also be enabled on Chrome and most Chromium based browsers running on Windows desktop. It was initially designed as a simple cache back-end to deal with the IO bottlenecks which impaired mobile browsing performance on some platforms.

NetAnalysis® supports processing Google Chrome and Chromium based Simple disk cache and well as exporting and rebuilding web pages.

Firefox and Mozilla based permissions.sqlite

This database holds preferences about which sites are allowed or prohibited to set cookies, to display images, to open pop up windows and to initiate extensions installation.

NetAnalysis® can read this information and display the permission settings in the Information panel.



Vivaldi Notes

Vivaldi browser allows the user to save notes while they browse. A note can be linked to a specific web page and the user can attach full page or selected area screenshots as well as files from their computer.

NetAnalysis® now recovers Vivaldi Notes. The note content is written to the case export folder and indexed. Any attachments are written to the case export folder.

Mozilla Firefox v2 Cache

The Disk Cache format v2 for Mozilla Firefox has evolved and changed. NetAnalysis® supports all versions of this disk cache format and allows cache objects to be exported as well as rebuilding web pages.

Microsoft Recovery Store, Tab Sessions, Roaming Tab Sessions and Travel Logs

Microsoft Internet Explorer and Edge browsers keep track of browsing history in two main ways; History and Travel Log. The active tab's list of back/forward navigations is called the Travel Log. Within Internet Explorer, you can see this list with a click-and-hold on the back or forward arrow. This data can also be used for recovering sessions in the event of the browser crashing, or by starting a new session with tabs from the last session when set as an option by the user. The browsers store this data in recovery store and tab session files.

NetAnalysis® v2.7 - Forensic Internet History Analysis - [Edge v38 Recovery Store]

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Recovery Store	https		2017-05-11 08:38:56.292	2017-05-11 09:38:56.292		RecoveryStore.{45543F42-3625-11E7-9C01-00268331AE30}
Tab	https		2017-05-11 13:01:50.616	2017-05-11 14:01:50.616		https://www.msn.com/spartan/http?locale=en-US&market=GB&enableregulatorypsm=0
Travel Log	https					https://www.msn.com/spartan/http?locale=en-US&market=GB&enableregulatorypsm=0

Record 1 of 3

Contains[Information], f40cd465-3649-11e7-9c01-00268331ae30

Information

1 Recovery Store ID: 45543F42-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:38:56.292]

2 Created [UTC]: 2017-05-11 08:38:56.292

3 Modified [UTC]: 2017-05-11 13:21:06.808

4

5 Tab Sessions: (Count = 21)

6 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: 95b56f0f-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:41:11.147]

7 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: 2b1aeb4a-3633-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 10:18:25.250]

8 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: ca199fb3-3635-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 10:37:10.993]

9 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: ab4da32d-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:41:47.377]

10 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: d651f043-3633-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 10:23:12.501]

11 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: fe783d4f5-3649-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:01:49.628]

12 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: 190502de-364a-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:02:33.332]

13 Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA== ID: 3f60d267-364a-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:03:37.687]

14 Stream Name: ClosedTabList ID: 45543f44-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:38:56.292]

15 Stream Name: ClosedTabList ID: 8d2efa18-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:40:56.844]

16 Stream Name: ClosedTabList ID: a2d48181-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:41:33.161]

17 Stream Name: ClosedTabList ID: e52759e2-362f-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 09:54:59.401]

18 Stream Name: ClosedTabList ID: 8a049b3b-363d-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 11:32:39.455]

19 Stream Name: ClosedTabList ID: 864ede80-3625-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 08:40:45.309]

20 Stream Name: ClosedTabList ID: 09d0e20f-3645-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 12:26:20.341]

21 Stream Name: ClosedTabList ID: 17797d45-3645-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 12:26:43.257]

22 Stream Name: ClosedTabList ID: 938928b1-363d-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 11:32:55.423]

23 Stream Name: ClosedTabList ID: bc51d12c-3646-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 12:38:29.317]

24 Stream Name: ClosedTabList ID: f40cd465-3649-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:01:31.308]

25 Stream Name: ClosedTabList ID: 190502dd-364a-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:02:33.332]

26 Stream Name: O_TSDI1N1Uk25xGcAQAmgzGuMA== ID: d54d890d-3649-11e7-9c01-00268331ae30 [Date [UTC]: 2017-05-11 13:00:39.723]

27

28 Properties

29 Operating System: 10.0 [Microsoft Windows 10]

30 Locale ID: 2057 [en-GB English (United Kingdom)]

31 Version: 14

www.digital-detective.net |vel Logs\Microsoft Edge v38 (14393) TravelLog\...Active\RecoveryStore.{45543F42-3625-11E7-9C01-00268331AE30} FO: 512

Detection of InPrivate Browsing



If a user activates InPrivate browsing, the browser continues to write Travel Log data to the Recovery Store and Tab Session files. At the end of the InPrivate session, the browser deletes these files. NetAnalysis® has the ability to genuinely identify InPrivate browsing sessions and will flag them by placing an icon at the start of the URL (as shown below).

HstEx® also has the ability to recover deleted InPrivate Recovery Store and Tab Session files. Some forensic tools claim to recover InPrivate browsing, but in fact are only searching for URLs in the Travel Log stream and have no idea whether they relate to InPrivate browsing or not.

The screenshot displays the NetAnalysis v2.7 interface for forensic internet history analysis. At the top, a table lists records with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected record is a 'Tab' entry with the URL 'http://www.pcworld.com/article/152966/private_browsing.html'.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Recovery Store			2017-06-16 12:29:22.503	2017-06-16 13:29:22.503		RecoveryStore-{6D43A1F7-528F-11E7-9C48-000A3A840851}
Tab	http		2017-06-16 12:33:20.690	2017-06-16 13:33:20.690		http://www.pcworld.com/article/152966/private_browsing.html
Travel Log	http					http://www.pcworld.com/article/152966/private_browsing.html

Below the table, a 'Viewer' pane shows a preview of the webpage 'How Private—or Secure—is So-Called Private Browsing?' from PCWorld. An 'Information' pane on the right displays details for the selected record, including Tab Session ID, Session State, Stream Name, CLSID, and Folder ID.

Improved Reporting

Reporting has been completely overhauled to allow reports to be generated on records filtered with a Find Panel active search as well as an active filter. Previously, reports could be generated on all rows in the grid or on the rows visible when a filter is active.

There are some additional report templates. A template based on the original NetAnalysis® v1 "Print - Current to PDF" report has been added named "Simple History". There is a new template based on the original v1 "Group By Host" named "History By Host" and a new template based on the original v1 "Group by Index Type" named "History By EntryType".

Improved Cache Exporting and Page Rebuilding

The cache exporting engine has been revisited and considerably improved. We have increased processing speed, as well as enhancing the capability of the process. The following bullet points highlight some of the enhancements we have made.

- Cache extraction and page rebuilding has been improved to speed up processing and is able to handle much larger volumes of cached page data.
- Improved content detection.

- Added support for Brotli decompression.
- Google Chrome / Chromium Based cache v2 Sparse data entries are now extracted and used in cache export and page rebuilding. Chrome uses this method to store large cache data in its disk cache. Internally the cache stores the data as sparse chunks among a set of child cache entries that are linked together from a main parent entry.
- Processing "srcset" attribute has been added.
- Processing "data-thumb" attribute has been added.
- Processing "data-src" attribute has been added.
- Added support for Chrome Dictionary files during export.

Improved Exporting

Exporting functionality has been improved to include records filtered with a Find Panel active search as well as an active filter. Previously, the exported rows would be dependent upon the active filter or all rows in the grid would be included.

User Interface Improvements

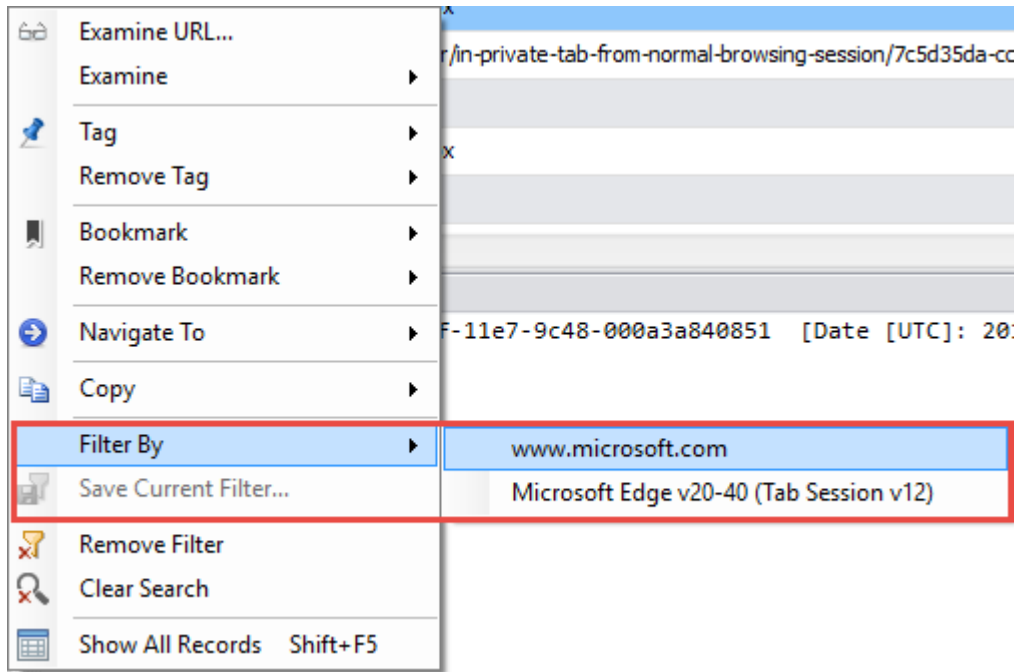
We have made some changes to the user interface to enhance usability:

Save and Load Column Layout

It is now possible to save and reuse grid column layouts. We have provided a number of sample layouts to demonstrate the feature. This is particularly useful if you like to arrange the columns in a certain order, or if you like to remove some of the columns altogether. To save a column layout, select Column » Save Column Layout. To load a column layout, select Column » Load Column Layout. There is also an option to save data grouping if you select save with Data Settings when saving the layout.

Right Click Grid Filter By

We have added two new dynamic filters which can be accessed by right clicking a target record. By selecting Filter By, a sub-menu will appear showing the Host Name and Browser Version strings for this record. Clicking either entry will result in a filter being applied relating to the clicked item.



Clear All Active Filters and Searches

Following user feedback, we have added a simple, one-click, option to remove all active filters and searches thereby restoring the full record count to the grid. This can be activated by selecting Tools » Show All Records (Shift + F5) or Right Click » Show All Records.

New Artefacts in v2.7

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.7.

Introduction

This version of NetAnalysis® introduces support for a number of new browsers as well as adding support for the latest release versions of existing browsers which are already supported. The major features for this version includes support for the changes to the latest Mozilla Firefox cache and favicons as well as adding support for processing Mozilla based cache with a missing index file. We have also considerably enhanced our support for Sleipnir.

New Browser Support

We have added support for the following browsers:

Cyberfox



Cyberfox is a Mozilla based browser designed by 8pecxstudios™. They claim they take over where Mozilla left off by working to make a fast, stable and reliable 64bit web browser that is accessible to all. It is available for Windows in two processor-specific builds, one optimized for Intel based CPU's, and one optimized for AMD based CPU's. It is also available in x86 versions. Cyberfox is also available for 64bit Linux.

Cyberfox ships with many customizable options allowing the user to personalize their web browsing experience. It has advertising features and components removed that collect information. It also has the ability to turn off the automatic loading of images on the web.

IceCat



GNU IceCat, formerly known as GNU IceWeasel, is a free web browser distributed by the GNU Project. It is based on the Mozilla platform and is available for installation of GNU/Linux, Windows, macOS and Android.

IceCat includes additional security features such as the option to block third party zero-length image files resulting in third party cookies, also known as web bugs. The software also provides warnings for URL redirection and has functionality to set a different user agent string for different domains.

Waterfox



Waterfox is an open-source web browser based on Mozilla which is available for 64bit Windows, macOS and Linux systems. It has been designed to take advantage of 64bit system architecture and claims to provide speed improvements over Firefox.

Updated Support for New Versions of Existing Browsers

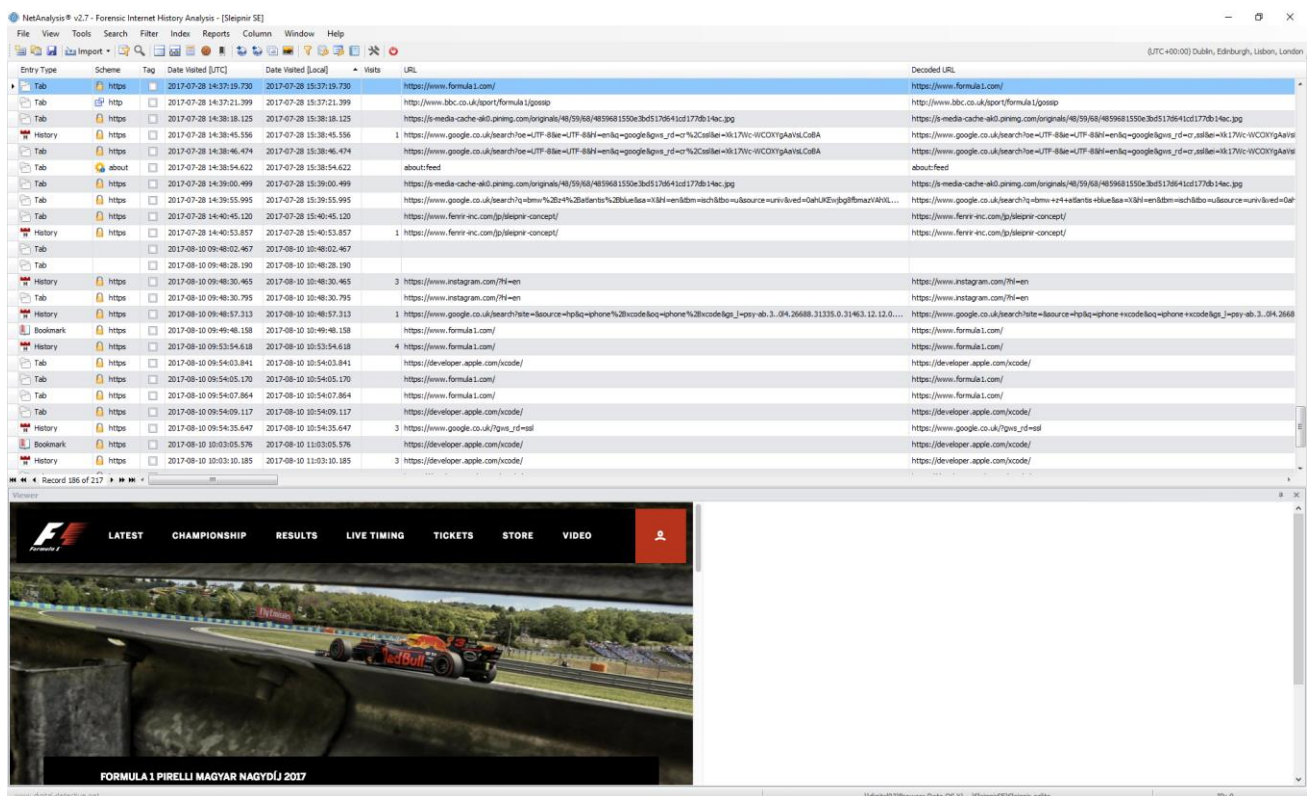
All of the mainstream browsers have updated their file formats and added new features. In addition to adding new browser support, we have enhanced the support provided for existing browsers:

Mozilla Firefox Cache v2 Missing Index

In the situation where the Index file is not present in the Mozilla cache v2 folder, we have added support for NetAnalysis® v2.7 to process these orphaned entries.

Sleipnir SE

We have considerably enhanced our support for Sleipnir. With added support for the Sleipnir.sqlite database, NetAnalysis® v2.7 now extracts History, Downloads, Bookmarks, Tab Groups, Tab Information and Tab History. We also extract Favicons, History Thumbnails and Tab Previews. The screen below shows a Tab entry with the Preview image displayed.



New Artefacts in v2.8

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.8.

Introduction

This version of NetAnalysis® introduces support for two new browsers as well as adding support for the latest release versions of existing browsers which are already supported.

Some notable new features include support for decrypting the logins and passwords from the latest Mozilla based browsers as well as processing Mozilla session and search engine files. We have also added support for Microsoft Edge backups and Apple Safari recently closed tabs, last session files, user notification permissions and search descriptions.

Some improvements to the software include DirectX hardware acceleration support for the data grid which increases performance. We have also added the ability to save data stored in encoded data URLs.

New Browser Support

We have added support for the following browsers:

AOL Desktop Browser v9



AOL Desktop was an Internet suite produced by AOL which contained an integrated web browser. Prior to version 9.8, the browser was based on the Trident layout engine as used by Internet Explorer. From v9.8 onward, Trident was replaced with CEF (Chromium Embedded Framework) to provide users with a more modern browsing experience. Despite AOL Desktop being discontinued in 2018, it is still encountered during investigations.

Blisk Browser v0 - 8



Blisk is a Chromium based web browser which has been designed to be used by web developers. It provides an array of tools for web development and testing across a number of different devices. It contains a pre-installed set of emulation tools for testing phones, tablets, laptop and desktop devices. This makes it a simple task for web developers to test how their code renders across multiple devices, browsers and screen resolutions.

Updated Support for Existing Supported Browsers

NetAnalysis® currently supports a wide variety of desktop and mobile browsers. There have been a number of changes to the currently supported browsers. Here are some of these changes:

Login and Password Decryption

A recent change to the encryption/decryption methodology for Firefox Desktop browsers resulted in the process requiring access to a new file called key4.db; using this file matches the behaviour of some mobile versions of the browser. NetAnalysis® supports the decryption of login information and passwords using both key store files.

New Support for Existing Browsers

To enhance our support for existing web browsers, we have added the following:

Mozilla Session Stores

Mozilla Firefox and many of the Mozilla based browsers store session information relating to the state of a user's browsing session so that the windows and tabs that were open when the browser was last closed, terminated unexpectedly or a software update applied can be restored.

There are usually multiple versions of a user's session store file located in the user profile folder with backup copies saved to the sessionstore-backups folder. Session store files have different file names depending on how the browser uses them during the session restore process:

- sessionstore,
- recovery,
- previous,
- upgrade.

As well as information on the currently open windows and tabs, a session store file also stores information on recently closed windows and tabs and cookies relating to the saved session. In the more recent versions of Firefox these session store files are now saved in a compressed format.

NetAnalysis® now recovers all versions of Mozilla based session store files.

The screenshot displays the NetAnalysis v2.8 interface with a table of browser history entries. The table has columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The entries include sessions, tabs, and tab history records for various websites like Facebook, BBC, Amazon, and Mozilla.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Session			2018-04-09 08:46:05.056	2018-04-09 09:46:05.056		SessionStore (sessionstore)
Tab	https		2018-04-09 08:44:10.948	2018-04-09 09:44:10.948		https://www.facebook.com/
Tab History	about					about:home
Tab History	https					https://www.facebook.com/
Tab	http		2018-04-09 08:46:04.990	2018-04-09 09:46:04.990		http://www.bbc.co.uk/sport/formula1
Tab History	about					about:newtab
Tab History	https					https://www.bbc.co.uk/
Tab History	http					http://www.bbc.co.uk/sport
Tab History	http					http://www.bbc.co.uk/sport/formula1
Tab	https		2018-04-09 08:46:02.796	2018-04-09 09:46:02.796		https://www.amazon.co.uk/Dark-Matter-Mind-Blowing-Twisted-Thriller/dp/144729758X/ref=pd_bxgy_14_img_3?encoding=UTF8&psc=1
Tab History	about					about:newtab
Tab History	https					https://www.amazon.co.uk/
Tab History	https					https://www.amazon.co.uk/gp/product/0099560437/ref=s9u_r1_gw_l4/260-4964358-6941626?e=UTF8&fpl=fresh&pd_rd_i=009956043
Tab History	https					https://www.amazon.co.uk/Dark-Matter-Mind-Blowing-Twisted-Thriller/dp/144729758X/ref=pd_bxgy_14_img_3?encoding=UTF8&psc=1
Tab	http		2018-04-09 08:46:02.158	2018-04-09 09:46:02.158		http://www.bbc.co.uk/sport/formula1/43693167
Tab History	http					http://www.bbc.co.uk/sport/formula1/43693167
Tab	http		2018-04-09 08:45:57.836	2018-04-09 09:45:57.836		http://www.bbc.co.uk/sport/formula1
Tab History	http					http://www.bbc.co.uk/sport/formula1/43693181
Tab History	http					http://www.bbc.co.uk/sport/formula1
Tab	http		2018-04-09 08:45:43.214	2018-04-09 09:45:43.214		http://www.bbc.co.uk/sport/formula1/43693302
Tab History	http					http://www.bbc.co.uk/sport/formula1/43693302
Session			2018-04-09 08:44:04.674	2018-04-09 09:44:04.674		SessionStore Backup (previous)
Tab	https		2018-04-09 08:44:04.612	2018-04-09 09:44:04.612		https://www.mozilla.org/en-US/privacy/firefox/
Tab History	https					https://www.mozilla.org/en-US/privacy/firefox/
Tab	https		2018-04-09 08:44:03.108	2018-04-09 09:44:03.108		https://www.mozilla.org/en-GB/firefox/59.0.2/firstrun/
Tab History	https					https://www.mozilla.org/en-GB/firefox/59.0.2/firstrun/
Tab History	https					https://www.mozilla.org/en-GB/firefox/59.0.2/firstrun/
Session			2018-04-09 08:47:17.838	2018-04-09 09:47:17.838		SessionStore (sessionstore)

Mozilla Search Engine Data

Mozilla Firefox and many of the Mozilla based browsers store their search engine data in a JSON format search file. This includes the default search engines that come preinstalled with the browser and user installed search engines and search engine add-ons. The user can then choose to search with one of these alternative search engines rather than the default. In the most recent versions of Firefox the search engine file is now saved in a compressed format.

We have added support for the import of all versions of this file to NetAnalysis®.

Microsoft Edge Backups

Microsoft Edge recently added a feature to create an automatic backup of the user's 'favourite' entries using the Netscape bookmark file format. NetAnalysis® can identify and import these files.

Apple Safari Search Descriptions

Quick Website Search was a feature added to Safari v8. If a website includes an OpenSearch description document, the site can be identified by the browser as having searchable content. The first time a user visits such a website, Safari will add it to the Manage Websites panel of Safari's Search Preferences. The user can then access content from this website directly from Safari's Smart Search field thus bypassing their normal search engine. Safari stores this Quick Website Search information in a SearchDescriptions.plist file.

NetAnalysis® now recovers Safari Quick Website Search information.

Apple Safari User Notification Permissions

Safari allows the user to manage website push notifications. The list of websites that have asked for permission to display alerts can be viewed in Safari's Notifications Preferences. Each website has an option to allow or deny the push notifications.

NetAnalysis® now recovers this information and details the notification permission setting to the Information panel.

Apple Safari Last Session

All versions of Safari v3+ on both Mac OS X and Windows contain a LastSession.plist file which records the current state of the browser. Safari can use this file to reopen all the windows and tabs which were open the last time the browser closed or terminated unexpectedly. The Safari menu item Reopen All Windows from Last Session allows the user to do this manually.

Apple Safari Recently Closed Tabs

Apple Safari v10+ keeps track of recently closed tabs in a RecentlyClosedTabs.plist file. This allows the user to reopen closed tabs using the Recently Closed Safari menu item.

We have added support for the import of Last Session and Recently Closed Tabs into NetAnalysis®.

New Features

We have added some new features to NetAnalysis®:

Saving Data from Encoded Data URLs

Data URLs are prefixed with the data: scheme and allow content creators to embed small files inline in documents. They are composed of four parts: a prefix (data:), a MIME type indicating the type of data stored, an optional base64 token if the data is non-text, and the data itself:

```
data: [<mediatype>] [;base64], <data>
```

Right clicking on the data URL allows the user to select **Save Data from URL**, this will show a Save File window prompting the user to select a location and file name. The decoding engine will automatically identify the correct file extension based on the source data.

The screenshot displays the NetAnalysis v2.8 interface. At the top, there's a menu bar with options like File, View, Tools, Search, Filter, Index, Reports, Column, Window, and Help. Below the menu is a toolbar with various icons. The main area shows a 'Preview URL' section with a long, complex URL. Below this is a table with columns: Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], and URL. The table contains several entries, with the last one selected. A context menu is open over the selected entry, showing options such as 'Examine URL...', 'Examine', 'Save Data from URL...', 'Tag', 'Remove Tag', 'Bookmark', 'Remove Bookmark', 'Navigate To', 'Copy', 'Filter By', 'Save Current Filter...', 'Remove Filter', 'Clear Search', and 'Show All Records'. The status bar at the bottom shows 'Record 4 of 4', 'Scheme = 'data'', and 'Window: 2 Closed Tab: 1 ID: 38'.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	URL
Tab	data		2018-04-09 08:26:17.620	2018-04-09 09:26:17.620	data:image/png;base64,iVBORw0KGgoAAAANSUgAABicAAQAQAIAAAAm50vZAAgAEIEQVR4n0y9V5AKSxrf+XOPiFRVWVp0tZbT06P17GzPKmCW2...
Tab History	data		2018-04-09 08:26:17.620	2018-04-09 09:26:17.620	data:image/png;base64,iVBORw0KGgoAAAANSUgAABicAAQAQAIAAAAm50vZAAgAEIEQVR4n0y9V5AKSxrf+XOPiFRVWVp0tZbT06P17GzPKmCW2...
Tab	data		2018-04-09 08:26:17.620	2018-04-09 09:26:17.620	data:image/png;base64,iVBORw0KGgoAAAANSUgAABicAAQAQAIAAAAm50vZAAgAEIEQVR4n0y9V5AKSxrf+XOPiFRVWVp0tZbT06P17GzPKmCW2...
Tab History	data		2018-04-09 08:26:17.620	2018-04-09 09:26:17.620	data:image/png;base64,iVBORw0KGgoAAAANSUgAABicAAQAQAIAAAAm50vZAAgAEIEQVR4n0y9V5AKSxrf+XOPiFRVWVp0tZbT06P17GzPKmCW2...

DirectX Hardware Acceleration Support

In this release of NetAnalysis®, we have added support for DirectX hardware acceleration. This allows us to employ the client machine's video card (integrated or dedicated) to render the data grid. DirectX acceleration provides us with an incredible speed boost. If the source system is unable to provide the resources for DirectX painting, the application will revert to GDI+ rendering.

New Artefacts in v2.9

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.9.

Introduction

This release of NetAnalysis® adds support for Basilisk Browser, Epic Privacy Browser, Cốc Cốc Browser and QQ Browser. We have also improved support for many of the existing browsers.

Some notable new features include the update of our internal HTML Viewer, as well as adding some valuable new functionality to aid with evidence processing and productivity.

New Browser Support

We have added support for the following browsers:

Basilisk



Basilisk is a free and Open Source XUL-based web browser, featuring the well-known Firefox-style interface and operation, created by the developers of the Pale Moon browser. It is based on the Goanna layout and rendering engine (a fork of Gecko) and builds on the Unified XUL Platform (UXP), which in turn is a fork of the Mozilla code base.

The developers describe Basilisk as "development software" and states "it should be considered more or less beta at all times; it may have some bugs and is provided as-is, with potential defects". It was initially released in November 2017 for Microsoft Windows and Linux.

Epic Privacy Browser



Epic Privacy Browser was released on August 29, 2013 and is developed by Hidden Reflex using the Chromium source code, developed for the security conscious. Epic Privacy Browser is (by default) always in "private browsing mode", taking a proactive approach to ensuring that session data (such as cookies, history, and cache etc.) are removed upon exit. The browser also removes Google tracking and blocks other organisations from tracking users.

Cốc Cốc Browser



Cốc Cốc browser is a web browser primarily focused on the Vietnamese market. It is available for Windows and macOS operating systems and supports both the English and Vietnamese languages. It is developed by Vietnamese company Cốc Cốc and based on the Chromium open source code. Cốc Cốc is the second most popular browser in Vietnam, with a market share of 16.89%, according to data from StatCounter.

QQ Browser



QQ Browser (QQ浏览器) is a Chromium-based web browser for Android, Windows, macOS, and iOS platforms. It is developed by Chinese Internet giant Tencent. The application offers a number of features such as tabbed windows and integration with chat platforms. QQ browser version 9.0 was the first released version which used the Chromium source code (Chromium v43). Prior to this QQ Browser was based on the Trident engine.

New Support for Existing Browsers

Microsoft Edge Swept Tabs

Microsoft has added a feature to its Edge browser to make it easy to sweep aside all the tabs the user has open into a collection that can be restored at any time. We have now added support to NetAnalysis® for viewing these Swept Tab entries (see below).

The screenshot shows the NetAnalysis v2.9 interface. The main window displays a table of Swept Tab entries. The table has columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. Below the table, there is a navigation bar showing 'Record 1 of 6' and a filter dropdown set to '[Tag] = 'Checked''. An 'Information' panel is open at the bottom, displaying details for the selected record.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Swept Tab	https	✓	2019-01-17 11:19:51.124	2019-01-17 11:19:51.124		https://www.msn.com/en-gb/news/world/japan-robot-hotel-fires-most-of-its-annoying-robotic-staff/ar-BB51k4F
Swept Tab	https	✓	2019-01-17 11:19:51.124	2019-01-17 11:19:51.124		https://www.msn.com/en-gb/news/uknews/paul-massey-and-john-kinsella-murders-hitman-mark-fell...
Swept Tab	https	✓	2018-08-06 12:15:11.142	2018-08-06 13:15:11.142		https://www.bbc.co.uk/sport/formula1
Swept Tab	https	✓	2018-08-06 12:15:11.142	2018-08-06 13:15:11.142		https://www.bbc.co.uk/sport/formula1/45053384
Swept Tab	https	✓	2018-08-06 12:13:18.064	2018-08-06 13:13:18.064		https://www.msn.com/en-gb/cars/enthusiasts/meeting-the-man-who-owns-24-aston-martins/ar-BBL...
Swept Tab	https	✓	2018-08-06 12:08:50.978	2018-08-06 13:08:50.978		https://www.msn.com/en-gb/news/uknews/hunt-for-reckless-driver-who-drove-at-cyclist/ar-BBLxLLz...

Information

- 1 Recovery GUID (Tab Session ID): e2b4b27e-c92e-4d09-83db-cc76d189eff5
- 2 Date Swept [UTC]: 2019-01-17 11:19:51.124
- 3 Sweep Group ID: e8bd1011-b40a-41c2-9b10-7c2ff74c5526
- 4 Order Number: 2

The Recovery GUID shown above is a unique identifier which relates to Recovery Store entries (Tab Session ID). In the screen capture below, you can see we have created a filter looking for records that contain the Swept Tab Recovery GUID in the Information field. This filter returns three records which can be seen below.

NetAnalysis® v2.9 - Forensic Internet History Analysis - [New Case]

File View Tools Search Filter Index Reports Column Window Help

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Preview URL
<https://www.msn.com/en-gb/news/world/japan-robot-hotel-fires-most-of-its-annoying-robotic-staff/ar-BBS1k4F>

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Swept Tab	https	<input checked="" type="checkbox"/>	2019-01-17 11:19:51.124	2019-01-17 11:19:51.124		https://www.msn.com/en-gb/news/world/japan-robot-hotel-fires-most-of-its-annoying-robotic-staff/
Tab	https	<input type="checkbox"/>	2019-01-17 11:19:21.484	2019-01-17 11:19:21.484		https://www.msn.com/en-gb/news/world/japan-robot-hotel-fires-most-of-its-annoying-robotic-staff/
Travel Log	https	<input type="checkbox"/>				https://www.msn.com/en-gb/news/world/japan-robot-hotel-fires-most-of-its-annoying-robotic-staff/

Record 2 of 3

Contains([Information], 'e2b4b27e-c92e-4d09-83db-cc76d189eff5')

Information

```

1 Tab Session ID: e2b4b27e-c92e-4d09-83db-cc76d189eff5
2 Session State: Orphaned
3 Modified [UTC]: 2019-01-17 11:19:52.126
4
5 Parent Name: <none>
6
7 Travel Logs: (Count = 1)
8 Stream Name: TL0
9
10 Travel Log: 0 (Last Displayed: 0)
11
12 Properties
13 Operating System: 10.0 [Microsoft Windows 10]
14 Locale ID: 2057 [en-GB English (United Kingdom)]
15 Tab Icon Exists: True

```

www.digital-detective.net | E:\Browser Dump\Microsoft Edge v42 (17134)\...\Active\{E2B4B27E-C92E-4D09-83DB-CC76D189EFF5}.dat | FO: 512

Microsoft Edge Downloads

Another area we have improved, in this release, is the processing of the download information object for Microsoft browsers. We have greatly improved the processing of corrupt and partially recovered data through HstEx® and added support for all known versions of the download object (including those versions released in beta and pre-release products).

We have also reformatted the output displayed in the Information panel, to make it clearer and easier to understand (see the screen capture below for an example).

The screenshot shows the NetAnalysis v2.9 interface. The main window displays a table with one entry: a download of a Microsoft Edge update. The entry is highlighted in blue. Below the table, the 'Information' panel is expanded, showing detailed download properties, digital signature information, and container details.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Download	https	✓	2018-11-02 17:25:51.302	2018-11-02 17:25:51.302		https://download.microsoft.com/download/9/3/F/93FCF1E7-E6A4-478B-96E7-D4B285925B00/vc_redist.x64.exe

Information

```

1 Download Properties
2 Download ID: iedownload:{3D1E6411-DEC4-11E8-B30C-FCAA14290F80}
3 Browser Session Started [UTC]: 2018-11-02 17:22:43.574
4 Download Started [UTC]: 2018-11-02 17:25:05.515
5 Download Completed [UTC]: 2018-11-02 17:25:51.302
6 Received Length: 584776 (571.07 KB)
7 Total Length: 14572000 (13.90 MB)
8 Cached Path: C:\Users\Craig Wilson\AppData\Local\Microsoft\Windows\INetCache\Low\IE\33JNY8LB\vc_redist.x64[1].exe
9 Download Path: D:\Downloads\vc_redist.x64 (1).exe
10 IP Address: 84.53.169.106
11 SHA256: 5EEA714E1F22F1875C1C87B1738B0C0B1F02AEC5ECB95F0F0B1C5171C6CD93A3
12
13 Digital Signature
14 Issuer: US, Washington, Redmond, Microsoft Corporation, Microsoft Code Signing PCA
15 Subject: US, Washington, Redmond, Microsoft Corporation, MOPR, Microsoft Corporation
16 Signed By: Microsoft Corporation
17 Hash Algorithm: SHA1
18
19 Containers
20 Name: iedownload
21 PartitionId: M
22 Directory: C:\Users\Craig Wilson\AppData\Local\Microsoft\Windows\IEDownloadHistory\
23 Flags: 64
24 Limit: 1024
25 LastAccessTime: 2018-11-12 08:08:00.214
26
27 Containers_45
28 EntryId: 1
29 UrlHash: 7267118684066474843 (0x64D9FDF08862EB5B)
30 Type: 9
31 Flags: 4
32 AccessCount: 4
33 SyncTime: 2018-11-02 17:25:51.302
34 AccessedTime: 2018-11-02 17:25:51.302

```

www.digital-detective.net | E:\Browser Dump\Microsoft Edge v42 (17134)\...\WebCache\WebCacheV01.dat | ID: 1 Container: 45

Microsoft Edge Typed URLs

Microsoft Edge v42 changed the location of Typed URLs from the Registry to a table within the spartan.edb database. We have added support for importing Typed URL data from the new location.

Microsoft Edge Cookies

With the release of Microsoft Edge v40, the structure of the table relating to cookie entries completely changed. The older table structure contained information pointing to an externally stored cookie file which was located in the file system. The new cookie table structure brought the actual cookie information into the database table,

negating the need to save this information to an external file.

We have added support for importing Cookie data from the new location.

Microsoft Edge HSTS Entries

We have added support for the import of data from the HstsEntry tables. This data relates to HTTP Strict Transport Security (HSTS) and is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure HTTPS connections, and never via the insecure HTTP protocol.

Netscape HTML Bookmark File Description

We have added some additional functionality to our processing of Netscape HTML Bookmark files. If you are unfamiliar with this file type, it is a common format, shared by many browsers, for the import/export of bookmarks and "favorite" entries.

In addition to extracting image and favicon files (which will be displayed in the Viewer panel), we extract the description portion of the entry so it can be added to the search index. The actual text data can be viewed from the Index panel (as shown below), and can be searched via our Search Index feature.

The screenshot displays the NetAnalysis v2.9 interface. The main window shows a list of bookmark entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected entry is a bookmark for <https://theintercept.com/2014/02/24/jtrig-manipulation/>.

The Index Text panel shows the extracted description for the selected bookmark:

```
One of the many pressing stories that remains to be told from the Snowden archive is how western intelligence agencies are attempting to manipulate and control online discourse with extreme tactics of deception and reputation-destruction.
```

A search window titled "NetAnalysis® Search Index" is overlaid, showing a search for "Snowden". The search results table is as follows:

URN	File Path	Search Hit Count	Document Score
36	D:\Documents\CASE-20190117\ID-135236\Unidentified Browser\Bookmark Description\F0000000036.txt	1	1.113387

The search window also displays the extracted text for the hit, with "Snowden" highlighted in red. The status bar at the bottom right of the search window indicates "Document Search Hit: 1 of 1".

New Features

Internal HTML Viewer

We have updated our internal viewer so that it supports the latest HTML standards and world wide web technology. We have also added some additional functionality which is accessible from the right-click context menu. The new items are as follows:

- **Save as PDF** - You can now save a rebuilt webpage (or other supported type) to a PDF file.
- **Open Containing Folder** - This will open an Explorer window and will highlight the source file for the content being displayed in the viewer.
- **Open with External Viewer** - This will send the content being displayed in the viewer to the default viewer for your system. For example, if the content relates to a video file, it will send the source to your default video player.
- **Zoom** - The zoom options allow the user to zoom in, out, or reset the zoom level to the content displayed in the viewer.

New Artefacts in v2.10

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.10.

Introduction

This release of NetAnalysis® adds support for the new Microsoft Edge (Chromium) browser, which has been released in Dev and Canary builds; we have also added support for the new Opera GX gaming browser as well as adding support for fifty-eight new versions of other browsers.

New Browser Support

We have added support for the following browsers:

Microsoft Edge (Chromium)



In December 2018, Microsoft announced their intention to adopt the Chromium open source project in the development of their Microsoft Edge browser. As of July 2019, they have released Developer and Canary editions. Microsoft Edge is currently available for Windows 7, 8, 8.1 and 10 as well as supporting macOS.

Opera GX



Opera GX is a special version of the Opera browser built specifically to complement gaming. The web browser includes unique features to help the user get the most out of both gaming and browsing. It is a desktop web browser for Windows PCs.

New Features

Login Stats Entries

We have added support for the recovery of Login Data stats entries for Chromium based browsers. This table records the number of times a user has logged into a password protected domain and dismissed the save password dialogue (for a maximum of three times). Once three instances have been recorded, the browser will no longer offer to save the username/password for the domain.

The screenshot displays the NetAnalysis v2.10 interface. The main window title is "NetAnalysis® v2.10 - Forensic Internet History Analysis - [Login Data Stats]". The menu bar includes File, View, Tools, Search, Filter, Index, Reports, Column, Window, and Help. The toolbar contains various icons for file operations and search. The main area shows a table with the following data:

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Login Stats	https		2019-07-01 08:43:59.980	2019-07-01 09:43:59.980	1	https://account.bbc.com/
Login Stats	https		2019-07-15 11:51:08.223	2019-07-15 12:51:08.223	1	https://www.nectar.com/

Below the table, there is a navigation bar showing "Record 1 of 2". An "Information" panel is open at the bottom, displaying the following details for the selected entry:

- 1 Origin Domain: https://account.bbc.com/
- 2 Username Value: vladimir.petrovich154@gmail.com
- 3 Dismissal Count: 1
- 4 Date Updated [UTC]: 2019-07-01 08:43:59.980

The status bar at the bottom shows the website "www.digital-detective.net", the file path "E:\Browser Dump\Microsoft Edge (Canary) v77...\Default\Login Data", and the ID "ID: 1".

Examine Selected Text

This new feature allows you to select text from the Information panel and send it to the Examination Window for analysis and/or decoding. Simply open the Information panel, select the text you wish to examine, right click and select Examine Selected.

NetAnalysis® v2.10 - Forensic Internet History Analysis - [New Case]

File View Tools Search Filter Index Reports Column Window Help

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Redirect	https		2019-07-15 11:51:31.232	2019-07-15 12:51:31.232		https://sync.crowdctrl.net/map/c=12451/tp=NWIQ?https://beacon.krxd.net/usermatch.gif?part
Redirect	https		2019-07-11 15:31:31.754	2019-07-11 16:31:31.754		https://pixel.advertising.com/lups/55859/sync?uid=7985b0af-df1d-496e-be19-8c58cd400256&c
Redirect	https		2019-07-15 10:10:31.835	2019-07-15 11:10:31.835		https://match.deepintent.com/usersync/122
Redirect	https		2019-07-15 11:58:18.295	2019-07-15 12:58:18.295		https://ad.doubleclick.net/ddm/activity/src=9480726?type=invmedia;cat=ina_u000;dc_lat=dc_j
Redirect	http		2019-07-12 10:22:55.171	2019-07-12 11:22:55.171		http://police.net-positive.org/
Redirect	https		2019-07-15 11:51:33.137	2019-07-15 12:51:33.137		https://ads.yahoo.com/pixel?id=2551957&t=2&piggyback=https%3A%2F%2Fads.yahoo.com%2Fcms%2Fv1%3Fesig%3D1~17e68b1b86afcfd8436104fe567484ccc2161b0f%26nwid%3D10000602235%26sigv%3D1
Redirect	https		2019-07-15 11:57:00.995	2019-07-15 12:57:00.995		https://ad.doubleclick.net/ddm/activity/src=9480726?type=invmedia;cat=ina_u000;dc_lat=dc_j

Record 6 of 467

[Entry Type] = 'Redirect'

Information

```

1 Cache Key:
2 https://ads.yahoo.com/pixel?id=2551957&t=2&piggyback=https%3A%2F%2Fads.yahoo.com%2Fcms%2Fv1%3Fesig%3D1~17e68b1b86afcfd8436104fe567484ccc2161b0f%26nwid%3D10000602235%26sigv%3D1
3 Date Created [UTC]: 2019-07-01 08:49:32.593
4 Date Last Used [UTC]: 2019-07-15 11:51:33.137
5 Date Last Modified [UTC]: 2019-07-15 11:51:33.137
6 Date Validated (Request Time): 2019-07-15 11:51:33.115
7 Date Validated (Response Time): 2019-07-15 11:51:33.137
8 Source IP: 217.12.15.83 Port: 80
9 Protocol: http/1.1
10 Connection Info: http/1.1
11 Date Cache Created [UTC]: 2019-07-01 08:49:32.593
    
```

www.digital-detective.net | E:\Browser Dump\Microsoft Edge (Canary) v77\...\Cache\index | FO: 6256

Examine

Amperсанд Comma Colon Semicolon Pipe Underscore Question Mark Remove Splits Unicode (UTF-8)

Decoding Functions

- Date Conversion
 - Mac Absolute
 - HFS+ (Mac OS)
 - Unix Minutes
 - Unix Seconds
 - Unix Milliseconds
 - Unix Microseconds
 - Windows Filetime
 - Chrome Timestamp
 - Gregorian Timestamp
 - OLE Automation Date
- Object Conversion
 - Google EI Parameter
 - Guid
- String Conversion
 - URL Unescape
 - URL RFC 1738
 - URL RFC 2396
 - URL RFC 3986
 - HTML Entities
 - Quoted Printable
 - ASCII85
 - ROT13
 - ROT18
 - ROT47
- Binary Conversion
 - Base16
 - Base32
 - Base32 Hex
 - Base58

```

https://ads.yahoo.com/pixel?id=2551957&t=2&piggyback=https%3A%2F%2Fads.yahoo.com%2Fcms%2Fv1%3Fesig%3D1~17e68b1b86afcfd8436104fe567484ccc2161b0f%26nwid%3D10000602235%26sigv%3D1
    
```

Decoded Text Hex

```

https://ads.yahoo.com/pixel?
id=2551957
&t=2
&piggyback=https://ads.yahoo.com/cms/v1?
esig=1~17e68b1b86afcfd8436104fe567484ccc2161b0f
&nwid=10000602235
&sigv=1
    
```

OK

New Report Template

We have added a new report template titled "Template with Decoded URL". This can be accessed by opening the **Report Manager** from the **View** menu, or typing **CTRL + Shift + R**. This template demonstrates how to take the Decoded URL data and display it in the split format as displayed in the Decoded URL panel. This is achieved by taking the data from the Decoded URL column, and processing it through a **SplitDecodedUri()** function. The script for the report can be seen by clicking on the **Scripts** tab in the **Report Designer**. The script is shown in the image below.

```
13
14 private string SplitDecodedUri(string uriToSplit)
15 {
16     if (string.IsNullOrEmpty(uriToSplit))
17         return (string.Empty);
18
19     uriToSplit = uriToSplit.Replace("?", "?" + Environment.NewLine);
20     uriToSplit = uriToSplit.Replace("%", Environment.NewLine + "%");
21     uriToSplit = uriToSplit.Replace(";", Environment.NewLine + ";");
22
23     return uriToSplit;
24 }
25
26
27 private void ReportDetailedTemplate_DataSourceRowChanged(object sender, DevExpress.XtraReports.UI.DataSourceRowEventArgs e) {
28
29     // Send the decoded URL value through the splitting routine
30     LabelDecodedUrl.Text = SplitDecodedUri((System.String)GetCurrentColumnValue("DecodedURL"));
31
32 }
```

Cache Prefix Handling

The URI key for an entry stored in the cache is normally the URI of the resource (for example ***https://www.digital-detective.net/favicon.ico***).

A cache key may also contain one or more prefix values. These prefixes can be an internal scheme used by the browser when retrieving entries from the cache (Firefox) or indicate a sparse entry where the browser is able to store only parts of a resource (Chrome). The prefixes may contain attribute values used to map the cache entry to a partitioned area of the cache storage (Firefox) or to indicate protocol information stored in the cache (Chrome).

The image below shows a cache entry with prefix as displayed in NetAnalysis® v2.9.

The screenshot shows the NetAnalysis v2.9 interface. The main table displays cache entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The second entry is highlighted in blue and has its URL field containing a prefix: `1564477979288937/https://www.redhat.com/en/search/node`. Below the table, the Information panel shows details for the selected entry:

Field	Value
1 Date Created [UTC]	2019-07-30 09:13:51.196
2 Date Last Used [UTC]	2019-07-30 12:55:15.249
3 Date Last Modified [UTC]	2019-07-30 12:55:15.249
4 Date Cache Created [UTC]	2019-06-19 11:11:00.722

Browsers have now started to include cache key prefixes that indicate cross-origin resource cache entries. The cache keys for these entries actually contain two or more URIs so that the top-level origin can be stored along with the resource URI. This can make cache handling problematic.

As a result of these changes, we have had to revisit the way NetAnalysis® handles cache entries containing prefixes. From NetAnalysis® v2.10, if a cache entry has a prefix, we will remove this data when handling URLs. This allows for easier URL handling and processing. To retain the original value, we will show this in the Information panel. With the exception of Chrome v2 sparse entries, the prefix will be retained to aid with sparse entry identification.

The image below shows a cache entry with prefix as displayed in NetAnalysis® v2.10. The prefix has been removed and the Information Panel shows the original cache key. The sparse entry prefix "Range_" can be seen in the other entries below.

NetAnalysis® v2.10 - Forensic Internet History Analysis - [New Prefix Handling]

File View Tools Search Filter Index Reports Column Window Help

Preview URL
https://www.redhat.com/en/search/node

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	https	✓	2019-07-26 15:15:36.037	2019-07-26 16:15:36.037		Range_https://learn2.open.ac.uk/pluginfile.php/2656045/mod_oucontent/oucontent/987609/a6fd5
Cache	https	✓	2019-07-30 12:55:15.249	2019-07-30 13:55:15.249		https://www.redhat.com/en/search/node
Cache	https	✓	2019-07-30 12:55:15.234	2019-07-30 13:55:15.234		https://www.facebook.com/tr/
Cache	https	✓	2019-07-26 15:15:36.039	2019-07-26 16:15:36.039		Range_https://learn2.open.ac.uk/pluginfile.php/2656045/mod_oucontent/oucontent/987609/a6fd5
Cache	https	✓	2019-07-26 16:23:31.526	2019-07-26 17:23:31.526		https://learn2.open.ac.uk/pluginfile.php/2656045/mod_oucontent/oucontent/987609/a6fd59f4/ecb
Cache	https	✓	2019-07-30 15:17:50.829	2019-07-30 16:17:50.829		https://veh-detax.service.gov.uk/
Cache	https	✓	2019-07-26 15:15:34.531	2019-07-26 16:15:34.531		Range_https://learn2.open.ac.uk/pluginfile.php/2656045/mod_oucontent/oucontent/987609/a6fd5

Record 2 of 7

[Tag] = 'Checked'

Information

- Cache Key: 1564477979288937/https://www.redhat.com/en/search/node
- Date Created [UTC]: 2019-07-30 03:13:31.190
- Date Last Used [UTC]: 2019-07-30 12:55:15.249
- Date Last Modified [UTC]: 2019-07-30 12:55:15.249
- Date Cache Created [UTC]: 2019-06-19 11:11:00.722

www.digital-detective.net | \\digital03\Browser Data Windows\... \Cache\index | FO: 138816

Firefox Pinned Tabs

Firefox recently added a new feature for pinning the tabs of frequently used web site for easy access. The pinned tabs are small and cannot be closed accidentally, they also open automatically when the browser is restarted. The user can easily pin a tab by right clicking on any tab and selecting Pin Tab from the menu (see the image below for Firefox pinned tabs, shown to the top left of this browser).

Digital Detective Forensic Forum - | X | Pinned Tabs - keep favorite we... X | +

https://www.formula1.com

FIA | F1® F2® F3® | F1® TV STORE TICKETS HOSPITALITY EXPERIENCES | SIGN IN SUBSCRIBE

Latest Video Races Standings Drivers Teams Gaming Live Timing

02 - 04 August

HUNGARY 2019 >

GRAND PRIX WEEKEND

01 DAYS 21 HRS 46 MINS

To identify a pinned tab, open the sessionstore file in NetAnalysis® and review the Information window as shown below.

Chromium Login Data Name/Value Pairs

We have enhanced the handling of Chromium based login data in NetAnalysis® v2.10. The name/value pairs are now extracted and displayed in the Index Text window. The data is also written to the export folder so that the information can be indexed by our search engine. In the example below, our user has logged in to the web site of a local pizza company so that some tasty food can be ordered (and delivered). The Index Text window in this case shows the user's name, contact number and delivery address. The Information window shows other information relevant to this transaction.

The screenshot shows the NetAnalysis v2.10 interface with the following components:

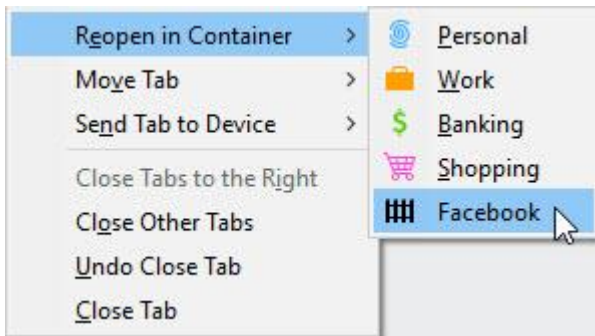
- Preview URL:** `https://www.papajohns.co.uk/stores/folkestone/checkout.aspx`
- Table:**

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Login Data	https	✓	2018-10-08 11:17:46.189	2018-10-08 12:17:46.189		<code>https://www.papajohns.co.uk/stores/folkestone/checkout.aspx</code>
- Information Window:**
 - 1 Origin URL: `https://www.papajohns.co.uk/stores/folkestone/checkout.aspx`
 - 2 Action URL: `https://www.papajohns.co.uk/stores/folkestone/checkout.aspx`
 - 3 Username Element: `ctl00$cphBody$txtGuestEmail`
 - 4 Username Value: `juleswinfield1637@hotmail.com`
 - 5 Password Element: `ctl00$cphBody$txtPassword`
 - 6 Password Value: [Redacted]
 - 7 Signon Realm: `https://www.papajohns.co.uk/`
 - 8 Preferred: True
 - 9 Blacklisted by User: False
 - 10 Times Used: 0
 - 11 Date Created [UTC]: 2018-10-08 11:17:46.189
 - 12 Skip Zero Click: True
 - 13 Generation Upload Status: No Signal Sent
- Index Text Window:**
 - `ctl00$cphBody$txtGuestContactNumber` 07825137211
 - `ctl00$cphBody$txtGuestPostcode` CT99 4DD
 - `ctl00$cphBody$txtGuestStreet` Pulp Fiction Street
 - `ctl00$cphBody$txtGuestTown` Sandford
 - `ctl00$cphBody$txtGuestFirstName` Jules
 - `ctl00$cphBody$txtGuestSurname` Winfield
 - `ctl00$cphBody$txtGuestHouse` 137a

Mozilla Firefox Containers

The Firefox Multi-Account Containers extension lets the user create a separate box for each of their online lives; which means they don't have to open a different browser to separate work and home browsing. The extension separates website storage into tab-specific Containers. Cookies downloaded by one Container are not available to other Containers, so the user can log into the same site with different accounts and online trackers can't easily connect the browsing. Custom labels and colour-coded tabs help keep the different activities or personas separate.

Existing tabs can be re-opened in a specific container by selecting from a right-click menu (see below).



NetAnalysis® 2.10 now supports the import of data from Firefox Multi-Account Containers. The image below shows a container entry, and the Information window shows the corresponding unique user context ID. This value identifies the Container. In this case, we are looking at the Facebook container. This ID can then be used to identify other entries and activity related to that container.

The screenshot shows the NetAnalysis v2.10 interface with a search for 'userContextId=6'. The search results table is as follows:

Entry Type	Scheme	Tag	URL	Information
Cache	https		https://scontent-lht6-1.xx.fbcdn.net/v/t1...	Cache Key: O^userContextId=6,;https://scontent-lht6-1.xx.fbcdn.net/v/t1.0-1/p32x32/36176788_19883081345130...
Cache	https		https://external-lht6-1.xx.fbcdn.net/safe...	Cache Key: O^userContextId=6,;https://external-lht6-1.xx.fbcdn.net/safe_image.php?d=AQCWVr61S2UyLcLoS&w=...
Cache	https		https://static.xx.fbcdn.net/rsrc.php/v3/yv...	Cache Key: O^userContextId=6,a,;https://static.xx.fbcdn.net/rsrc.php/v3/yv/r/nM4v-4osyIT.js?_nc_x=9bBrSuYMla5...
Cache	https		https://scontent-lht6-1.xx.fbcdn.net/v/t45...	Cache Key: O^userContextId=6,;https://scontent-lht6-1.xx.fbcdn.net/v/t45.1600-4/cp0/q90/spS444/p160x160/655...
Cache	https		https://scontent-lht6-1.xx.fbcdn.net/v/t1...	Cache Key: O^userContextId=6,;https://scontent-lht6-1.xx.fbcdn.net/v/t1.0-0/p526x296/67527362_22509105552...
Cache	https		https://video-lht6-1.xx.fbcdn.net/v/t42.17...	Cache Key: O^userContextId=6,a,;https://video-lht6-1.xx.fbcdn.net/v/t42.1790-2/65174354_746578235744973_8...
Cache	https		https://video-lht6-1.xx.fbcdn.net/v/t42.17...	Cache Key: O^userContextId=6,a,;https://video-lht6-1.xx.fbcdn.net/v/t42.1790-2/24144863_512605352450805_6...
Cache	https		https://static.xx.fbcdn.net/rsrc.php/v3/iy...	Cache Key: O^userContextId=6,a,;https://static.xx.fbcdn.net/rsrc.php/v3/iy/ll/en_GB/9PjBRDo9Caf.js?_nc_x=...
Cache	https		https://static.xx.fbcdn.net/rsrc.php/v3/yC...	Cache Key: O^userContextId=6,a,;https://static.xx.fbcdn.net/rsrc.php/v3/yC/0,cross/VY9sX7bdZJS.css?_nc_x=9b...
Container		<input checked="" type="checkbox"/>		User Context ID: 6 Public: True Icon: fence Color: toolbar Name: Facebook
Cookie		<input type="checkbox"/>	.facebook.com	Base Domain: facebook.com Origin Attributes: ^userContextId=6 Same-site: Unset
Cookie		<input type="checkbox"/>	.facebook.com	Base Domain: facebook.com Origin Attributes: ^userContextId=6 Same-site: Unset
Cookie		<input type="checkbox"/>	.instagram.com	Base Domain: instagram.com Origin Attributes: ^userContextId=6 Same-site: Unset
Cookie		<input type="checkbox"/>	www.instagram.com	Base Domain: instagram.com Origin Attributes: ^userContextId=6 Same-site: Unset
Cookie		<input type="checkbox"/>	.doubleclick.net	Base Domain: doubleclick.net Origin Attributes: ^userContextId=6 Same-site: Unset
Cookie		<input type="checkbox"/>	.instagram.com	Base Domain: instagram.com Origin Attributes: ^userContextId=6 Same-site: Unset

The 'Container' entry is expanded to show the following information:

```

1 User Context ID: 6
2 Public: True
3 Icon: fence
4 Color: toolbar
5 Name: Facebook
  
```

The status bar at the bottom shows: www.digital-detective.net | E:\Browser Dump\Mozilla Firefox v68\...\8ro655j.default\containers.json | ID: 6

New Artefacts in v2.11

The following pages outline some of the new artefacts that have been added to NetAnalysis® v2.11.

Introduction

This release of NetAnalysis® adds support for two browsers which have been designed for the security/privacy market, Avast Secure Browser and CCleaner Browser. We have also added support for seventy-four new versions of other browsers.

New Browser Support

We have added support for the following browsers:

Avast Secure Browser



Avast Secure Browser (previously Avast Safe-Zone) is a Chromium based web browser developed by Avast. Initially, the browser was available alongside Avast's paid versions of their Avast Antivirus software. However, as of March 2016, the company included the web browser as part of its free antivirus software.

CCleaner Browser



CCleaner Browser is a Chromium based web browser developed by Piriform, the same company responsible for the data erasing, security software, CCleaner. The company describes the software as *"a web browser with built-in security and privacy features to keep you safe online. It comes packed with all the tools you need to manage your online privacy, identity, and personal data."*

New Features

Apple Safari

We have added support for auto-fill corrections, touch icon cache settings, per-site preferences and favicons.

Improvements

Property Set Information

Microsoft Internet Explorer and Edge (non-Chromium) browsers maintain files for recovering sessions and tracking browser navigation between tabs. NetAnalysis® shows this data when viewing Recovery Store, Tab Session, Roaming Tab Session and Travel Log entries. Some of the data for these types is stored in a data structure called a Property Set. This is simply a collection of properties, along with a FMTID (Format Identifier) to identify the property set format.

In previous version of NetAnalysis®, we only displayed a summary of the known properties in the Information panel. This has now been updated so we show all property IDs along with the raw values, as well as the CLSID for the Format Identifier. Some examples are shown below.

The following images show the Information panels from Recovery Store entries. The raw Property Set values are below the FMTID.

```

Information
1 Recovery Store ID: b15f4845-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
2 Created [UTC]: 2017-04-27 08:51:24.265
3 Modified [UTC]: 2017-04-27 08:54:30.008
4
5 Tab Sessions: (Count = 8)
6 Stream Name: O_TSRkhfsSYr5xG#jwAwG0hXiw== ID: b15f4847-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
7 Stream Name: O_TSRkhfsSYr5xG#jwAwG0hXiw== ID: df96d884-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:52:41.804]
8 Stream Name: O_TSRkhfsSYr5xG#jwAwG0hXiw== ID: f0616cee-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:09.975]
9 Stream Name: O_TSRkhfsSYr5xG#jwAwG0hXiw== ID: fd5fbf27-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:31.775]
10 Stream Name: ClosedTabList ID: b15f4849-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
11 Stream Name: ClosedTabList ID: b15f4848-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
12 Stream Name: ClosedTabList ID: c06400ba-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:49.462]
13 Stream Name: ClosedTabList ID: f0616cef-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:09.975]
14
15 Properties
16 Operating System: 10.0 [Microsoft Windows 10]
17 Locale ID: 2057 [en-GB English (United Kingdom)]
18 Version: 9
19
20 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
21 ID: 2 [0x02] VT_UI4 Value: 9
22 ID: 3 [0x03] VT_CLSID Value: b15f4845-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
23 ID: 7 [0x07] VT_CLSID Value: b15f4844-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]

```

```

Information
1 Recovery Store ID : 21e7dddc-33b4-4f97-98ba-c98d3dfc1064
2 Created [UTC]: 2020-01-16 08:09:57.148
3 Modified [UTC]: 2020-01-16 08:12:06.516
4
5 Tab Sessions: (Count = 1)
6 Stream Name: O_TSegGnGtLL1UiXD0ezfitFyg== ID: 0eabebad-a354-447b-a0c9-f531d9bbfc3c
7
8 Properties
9 Operating System: 10.0 [Microsoft Windows 10]
10 Locale ID: 2057 [en-GB English (United Kingdom)]
11 Version: 19
12
13 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
14 ID: 2 [0x02] VT_UI4 Value: 19
15 ID: 3 [0x03] VT_CLSID Value: 21e7dddc-33b4-4f97-98ba-c98d3dfc1064
16 ID: 7 [0x07] VT_CLSID Value: 958ae36b-3837-11ea-b397-fcaa14290f80 [Date [UTC]: 2020-01-16 08:09:57.148]
17 ID: 11 [0x0B] VT_BOOL Value: True
18 ID: 12 [0x0C] VT_BOOL Value: True

```

```

Information
1 Recovery Store ID: 16cf0cbe-98d9-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:43:06.266]
2 Created [UTC]: 2015-12-02 09:39:02.172
3 Modified [UTC]: 2015-12-04 17:31:27.787
4
5 Tab Sessions: (Count = 28)
6 Stream Name: O_TSIktrRhdIY5RGCD#yqFAY+cw== ID: 81498986-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
7 Stream Name: O_TSIktrRhdIY5RGCD#yqFAY+cw== ID: 81498987-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
8 Stream Name: O_TSIktrRhdIY5RGCD#yqFAY+cw== ID: 81498988-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
9 Stream Name: O_TSIktrRhdIY5RGCD#yqFAY+cw== ID: 81498989-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
10 Stream Name: O_TSIktrRhdIY5RGCD#yqFAY+cw== ID: 8149898a-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
11 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad11c-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
12 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad11d-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
13 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad11e-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
14 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad11f-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
15 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad120-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
16 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad121-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
17 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad122-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
18 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad123-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
19 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad124-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
20 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad125-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
21 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad126-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
22 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad127-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
23 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad128-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
24 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad129-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
25 Stream Name: O_TStdUsr9uY5RGCD#yqFAY+cw== ID: d0aad12a-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
26 Stream Name: O_TSU3+k+t2Y5RGCD#yqFAY+cw== ID: 8149c81-98de-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:21:52.392]
27 Stream Name: O_TSVUp2k96Y5RGCD#yqFAY+cw== ID: 4e7a9bcd-98e0-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:34:46.142]
28 Stream Name: O_TSVUp2k96Y5RGCD#yqFAY+cw== ID: 4e7a9bce-98e0-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:34:46.142]
29 Stream Name: O_TSNej2Vma6SRGCD#yqFAY+cw== ID: 78d1fa96-9a6e-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 10:04:56.877]
30 Stream Name: O_TSVHzByqKa5RGCD#yqFAY+cw== ID: 577538eb-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
31 Stream Name: O_TSVHzByqKa5RGCD#yqFAY+cw== ID: 577538ec-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
32 Stream Name: O_TSVHzByqKa5RGCD#yqFAY+cw== ID: 577538ed-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
33 Stream Name: O_TStqQE2aqa5RGCD#yqFAY+cw== ID: ea44a478-9aaa-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 17:17:37.015]
34
35 Properties
36 Operating System: 6.3 [Microsoft Windows 8.1]
37 Locale ID: 2057 [en-GB English (United Kingdom)]
38 Version: 9
39
40 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
41 ID: 2 [0x02] VT_UI4 Value: 9
42 ID: 3 [0x03] VT_CLSID Value: 16cf0cbe-98d9-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:43:06.266]
43 ID: 7 [0x07] VT_UI4 Value: 85514b88-98d8-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:39:02.172]

```

The following images show the Information panels from Tab Session entries. The raw Property Set values are below the FMTID.

```

Information
1 Tab Session ID: b15f4847-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
2 Session State: Ordered
3 Modified [UTC]: 2017-04-27 08:53:44.751
4
5 Parent Name: RecoveryStore.{B15F4845-2B26-11E7-BF8F-00301B48578B}
6 Stream Name: O_TSRkhfsYr5Xg#jAwG0hXiw==
7
8 Travel Logs: (Count = 6)
9 Stream Name: TL1
10 Stream Name: TL2
11 Stream Name: TL3
12 Stream Name: TL4
13 Stream Name: TL5
14 Stream Name: TL6
15
16 Travel Log: 0, 1, 2, 3, 4, 5, 6 (Last Displayed: 6)
17
18 Properties
19 Operating System: 10.0 [Microsoft Windows 10]
20 Locale ID: 2057 [en-GB English (United Kingdom)]
21 Version: 9
22
23 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
24 ID: 2 [0x02] VT_UI4 Value: 9
25 ID: 4 [0x04] VT_UI4 Value: 6
26 ID: 6 [0x06] VT_FILETIME Value: 2017-04-27 08:52:47.833 [UTC]
27 ID: 7 [0x07] VT_I4 Value: 0
28 ID: 9 [0x09] VT_UI4 Value: 1
29 ID: 10 [0x0A] VT_FILETIME Value: 2017-04-27 08:53:11.955 [UTC]
30 ID: 13 [0x0D] VT_UI4 Value: 1
31 ID: 14 [0x0E] VT_UI4 Value: 0
32 ID: 17 [0x11] VT_UI4 Value: 0

```

```

Information
1 Tab Session ID: 22a7ff1d-cc86-11e2-bee6-00301b46bd20 [Date [UTC]: 2013-06-03 19:45:25.365]
2 Session State: Ordered
3 Modified [UTC]: 2013-06-03 19:45:26.381
4
5 Parent Name: RecoveryStore.{22A7FF1D-CC86-11E2-BEE6-00301B46BD20}
6 Stream Name: ORDERED_TS0
7
8 Travel Logs: (Count = 1)
9 Stream Name: TL2
10
11 Travel Log: 0, 1, 2 (Last Displayed: 2)
12
13 Properties
14 Operating System: 6.2 [Microsoft Windows 8]
15 Locale ID: 2057 [en-GB English (United Kingdom)]
16 Version: 6
17
18 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
19 ID: 2 [0x02] VT_UI4 Value: 6
20 ID: 4 [0x04] VT_UI4 Value: 2
21 ID: 6 [0x06] VT_FILETIME Value: 2013-06-03 18:44:54.749 [UTC]
22 ID: 7 [0x07] VT_I4 Value: 0
23 ID: 9 [0x09] VT_UI4 Value: 4
24 ID: 10 [0x0A] VT_FILETIME Value: 2013-06-03 18:44:57.452 [UTC]
25 ID: 13 [0x0D] VT_UI4 Value: 1

```

The following images show the Information panels from Tab Roaming entries. The raw Property Set values are below the FMTID.

```

Information
1 Tab Session ID: 666504d7-9aab-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 17:21:05.264]
2 Session State: Roaming
3 Modified [UTC]: 2015-12-04 17:21:58.210
4
5 Parent Name: <none>
6
7 Travel Logs: (Count = 5)
8 Stream Name: TL0
9 Stream Name: TL1
10 Stream Name: TL2
11 Stream Name: TL3
12 Stream Name: TL4
13
14 Travel Log: 0, 1, 2, 3, 4 (Last Displayed: 4)
15
16 Properties
17 Operating System: 6.3 [Microsoft Windows 8.1]
18 Locale ID: 2057 [en-GB English (United Kingdom)]
19 Version: 9
20
21 Tab Roaming Machine Information v2
22 Source: \\digital02\IE TravelLog\Travel Logs\Internet Explorer v11 (9600) TravelLog\2016_01_08_15_03_32_272\Local\Microsoft\Internet
Explorer\TabRoaming\{D8501CB7-A63B-43FC-83B4-869E5E2CD0A8}\MachineInfo.dat
23 Machine Name: RECOVERY1
24 Operating System: 6.3 [Microsoft Windows 8.1]
25 Locale ID: 2057 [en-GB English (United Kingdom)]
26
27 Modified [UTC]: 2015-12-04 17:21:58.210
28 Timestamp [UTC]: 2015-12-04 10:04:00.965
29
30 FMTID: 8d06be37-1a1a-4762-9d01-33fd4881f84
31 ID: 2 [0x02] VT_UI4 Value: 9
32 ID: 4 [0x04] VT_UI4 Value: 4
33 ID: 9 [0x09] VT_UI4 Value: 0
34 ID: 10 [0x0A] VT_FILETIME Value: 2015-12-04 17:21:13.456 [UTC]
35 ID: 14 [0x0E] VT_UI4 Value: 0
36 ID: 1000 [0x3E8] VT_UI4 Value: 2
37 ID: 1001 [0x3E9] VT_LPWSTR Value: {666504d7-9AAB-11E5-8277-FCAA14063E73}
38 ID: 1002 [0x3EA] VT_LPWSTR Value: http://static-news-neu.s-msn.com/sc/d7/97297b.ico

```

```

Information
1 Tab Session ID: 79a678b2-98dc-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:07:20.584]
2 Session State: Roaming
3 Modified [UTC]: 2015-12-04 17:21:17.348
4
5 Parent Name: <none>
6
7 Travel Logs: (Count = 1)
8 Stream Name: TL3
9
10 Travel Log: 3 (Last Displayed: 3)
11
12 Properties
13 Operating System: 6.3 [Microsoft Windows 8.1]
14 Locale ID: 2057 [en-GB English (United Kingdom)]
15 Version: 9
16
17 Tab Roaming Machine Information v2
18 Source: \\digital02\IE TravelLog\Travel Logs\Internet Explorer v11 (9600) TravelLog\2016_01_08_15_03_32_272\Local\Microsoft\Internet
Explorer\TabRoaming\{D8501CB7-A63B-43FC-83B4-869E5E2CD0A8}\MachineInfo.dat
19 Machine Name: RECOVERY1
20 Operating System: 6.3 [Microsoft Windows 8.1]
21 Locale ID: 2057 [en-GB English (United Kingdom)]
22
23 Modified [UTC]: 2015-12-04 17:21:17.348
24 Timestamp [UTC]: 2015-12-04 10:04:00.965
25
26 FMTID: 8d06be37-1a1a-4762-9d01-33fd4881f84
27 ID: 2 [0x02] VT_UI4 Value: 9
28 ID: 4 [0x04] VT_UI4 Value: 3
29 ID: 9 [0x09] VT_UI4 Value: 0
30 ID: 10 [0x0A] VT_FILETIME Value: 2015-12-04 17:20:57.785 [UTC]
31 ID: 14 [0x0E] VT_UI4 Value: 0
32 ID: 1000 [0x3E8] VT_UI4 Value: 2
33 ID: 1001 [0x3E9] VT_LPWSTR Value: {79A678B2-98DC-11E5-8277-FCAA14063E73}
34 ID: 1002 [0x3EA] VT_LPWSTR Value: http://www.neowin.net/images/orion/icons/favicon-196x196.png

```

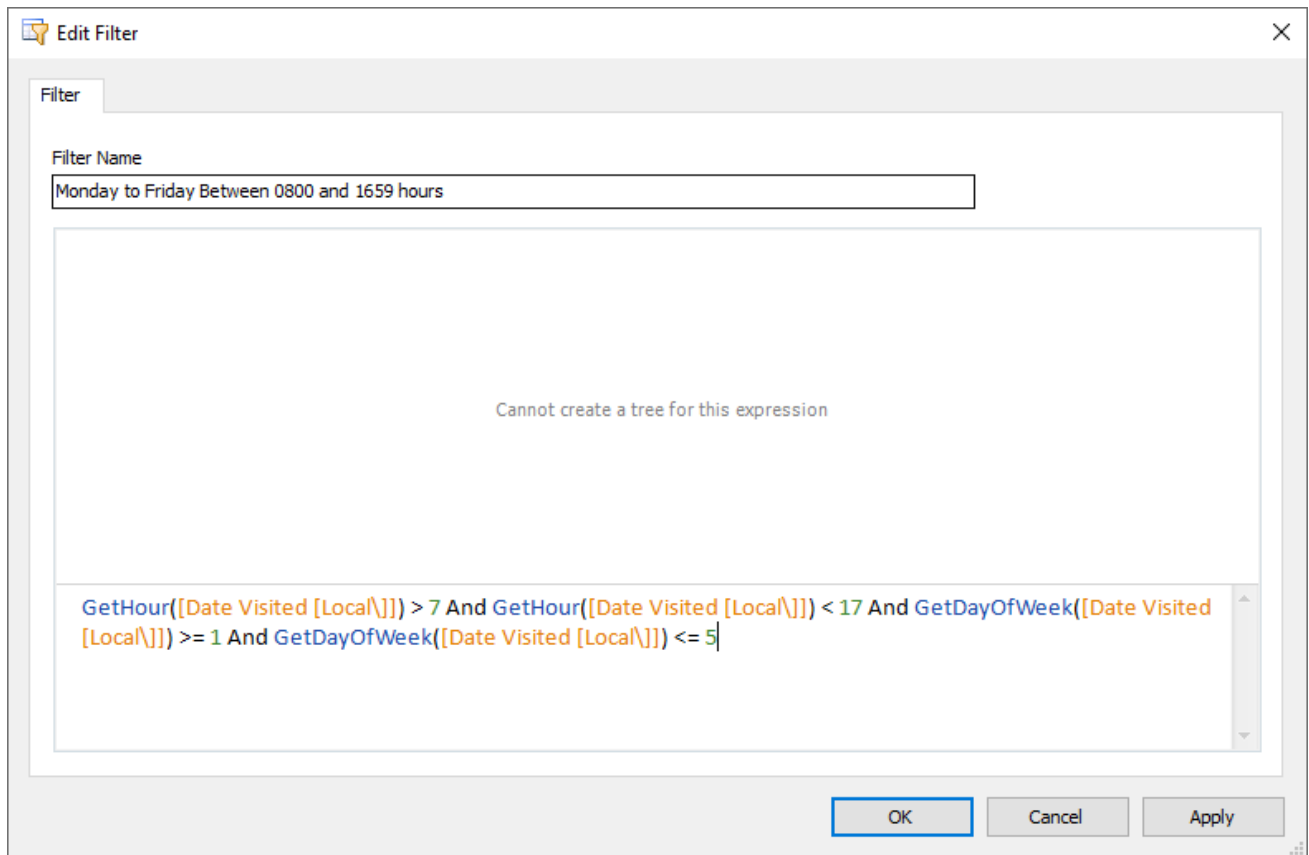
Filter Functions

A common scenario is to examine the records between specific days of the week and between specific times. In NetAnalysis® v2.11 we have added some new Filter files which demonstrates this.

The first example is a filter which will only show entries where the Date Visited falls between Monday and Friday, and the local time is between 08:00 and 16:59 hours. As this filter uses the Function facility, it will not be able to

display the results in the expression tree.

This Filter uses the `GetHour()` and `GetDayOfWeek()` functions. The `GetDayOfWeek()` function returns an integer which corresponds to the day of the week. Monday = 1, Tuesday = 2 and so on. The `GetHour()` function also returns an integer which represents the hour in the 24-hour clock.



New Artefacts in v2.12

The following pages outline some of the new artefacts and features that have been added to NetAnalysis® v2.12.

Introduction

This release of NetAnalysis® adds support for another two browsers, namely AVG Secure Browser and Min Browser. We have also added support for thirty-eight new versions of other browsers.

New Browser Support

We have added support for the following browsers:

AVG Secure Browser



AVG Secure Browser is a web browser with built-in security and privacy features designed by AVG Technologies, a subsidiary of Avast. It claims to be a fast, secure browser with built-in adblock, anti-phishing, safer online banking, password manager and a host of other security focused features.

Min Browser



Min Browser is an open-source web browser which has been designed with a minimalist outlook. The tabs in Min take up less space as they are combined with the search bar into one row. Another interesting feature is the ability to organise tabs into Tasks, this is similar to the Tab Groups feature in Firefox. It also has a Focus Mode which hides the other tabs with an aim to prevent distractions.

New Features

Apple Safari

We have added support for remote user notification permissions and enhanced the support for recently closed tabs.

Microsoft Edge Collections

We have added support for the new Microsoft Edge Collections feature.

Collections offers a way to save and group information found on the Internet. Microsoft suggests that Edge users may use Collections to "collect and compare" shopping items, to gather holiday ideas and plan trips, or to group selected sites by theme, for example, news sites.

Yandex Login Data

Yandex browser has recently changed the way it stores a user's login credentials. NetAnalysis® now has support to import and interpret data from this new file.

Chromium Based Quota Manager

There are a number of web technologies that store data of one kind or another on the client-side (i.e., on the local disk). The process by which the browser works out how much space to allocate to web data storage and what to delete when that limit is reached is not simple, and differs between browsers. In Chromium-based browsers, this is achieved by the Quota Management API which controls storage limits and the eviction of client-side web data.

NetAnalysis® now has support for importing data from the Quota Manager.

Improvements

We have made the following improvements in this release of NetAnalysis®:

Internal Viewer

Our internal viewer has been updated to deal with the latest in browser technology. In addition, we have added support for data URLs, so they may be displayed in the viewer; depending on the format of the data, you can right-click on the page and save the data in its native format.

We have also added support for viewing MHTML documents (MIME HTML Web Archive Format).

The image below shows a Data URL being displayed in the Internal Viewer.

The screenshot displays the NetAnalysis v2.12 interface. The top menu includes File, View, Tools, Search, Filter, Index, Reports, Column, Window, and Help. The main area shows a list of bookmarks with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected bookmark is a Data URL pointing to a GLENMORANGIE website. Below the list, the 'Viewer' pane shows a preview of the website's homepage, which features the GLENMORANGIE logo and a large image of whisky glasses with the text 'DISCOVER THE UNSEEN'.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Bookmark	data					data:image/png;base64,iVBORw0KGgoAAAANSUHEugAABicAAAQ5CAIAAAAm50vZAAAgAE1EQVR4n0y9V5AkSXr-f+XOPiFRVWp0tZbT06P176zPKmCW2CXEEqAdcEbY8Qy90/DEw5nd3QPvXvF4D/cCwx3BH/C08EhCkAryCV2sTuzmJ2ZnR3dPT0zrXVdVdemqVBHu9xARmZGZEZGRoQ1aMv/m3tuoqDw9X4eHx+d8/1e7+FuHQEem7B9Fwr/B/SbkxonQWAW0vRjtye3tKakh/wLkPznj8I4gvpP88kkGeQUEhLLAi3u5YiNBsMfckEKDRVXVQGGQ6aA5JetiS1sps9FXRFkk0PVbhoLZxthB6bPmDggaBLCLzLa3shKg8HdMfgLOC2kAYyCmMcXBwVnHwQGJMY4y
Bookmark	data					data:image/jpeg;base64,iVBORw0KGgoAAAANSUHEugAAA0IAAAK8CAIAAAE61khoaAAAAAXNSR0IArs4c6QAAAAARnQU1BAACxgww8YQUA
Bookmark	data					data:text/html,<script>alert('hi');</script>
Bookmark	data					data:text/html,<a%20href='www.digital-detective.net'>Visit%20DD
Bookmark	data					data:text/html,<img%20src='data:image/png;base64,iVBORw0KGgoAAAANSUHEugAAAAIAAAAFCAyAAACNbybIAAAAHIEEQVQ1I2P4/f

Reporting

All our report templates have been updated for improved performance in relation to speed and memory usage.

In addition, we have added support for caching reports to disk as they are rendered, which allows for very large numbers of report pages to be created without running into memory issues.

The screenshot shows the 'NetAnalysis® Detailed Report Preview' window. The interface includes a menu (File, View, Background) and a toolbar with various icons. The main content area displays the NetAnalysis logo, which consists of a globe icon and the text 'NetAnalysis®'. Below the logo, the following information is shown:

- Case Reference: CASE-20200527 - ID-090432
- Prepared by: Craig Wilson - Digital Detective
- Printed Workspace: 2020-06-11 14:52:11.537+01:00
- TestLarge Workspace

The following screen shows an example of a generated report containing 297,452 pages:

The screenshot displays the NetAnalysis® Detailed Report Preview window. The window title is "NetAnalysis® Detailed Report Preview". The menu bar includes "File", "View", and "Background". The toolbar shows various icons for file operations and navigation, with a zoom level of 100%. The main content area is divided into sections by dashed lines. The top section features the NetAnalysis logo and metadata: "Case Reference CASE-20200527 - ID-090432", "Prepared by Craig Wilson - Digital Detective", "Printed 2020-06-11 14:52:11.537 +01:00", and "Workspace TestLargeWorkspace". Below this, two record entries are shown. Each entry includes fields for Scheme (https), Entry Type (Cache), Date Visited [Local] and [UTC], Source File, Visits (1), Browser Version (Mozilla Firefox v32-76 (Cache v2.3.9)), Time Zone (GMT Standard Time), Record URN (1 and 2), and Source Offset (FO: 12 and FO: 53). The Page Title and URL fields contain detailed information, including a Google syndication URL and a Google Maps URL. The bottom of the window shows "Page 1 of 297452" and a zoom level of 100%.

User Interface Enhancements

When the grid contains many rows of data, it is sometimes difficult to know which row is focused or which rows are selected. To help locate these rows quickly, we have added scrollbar annotations. These are coloured marks on the vertical scrollbar which reflect the location of corresponding rows in the grid.

We have also added support for hot-track (mouse hover) row highlighting; this allows the user to visually see the mouse cursor's hover position within the grid.

Improved Support for Processing Mounted File Systems



We have reviewed a number of different file mounting applications to see if we can improve the way we handle read-only file systems. This has resulted in a number of improvements. We have enhanced our support for files

and folders containing reparse points as well as improving the way we deal with file system artefacts which require elevated permissions.

Additional Content Available for Search Indexing

During import, cache exporting and page rebuilding, we identify relevant content for adding to our search index. In this release, we have added:

- Chromium-based autofill name and value fields.
- Plain-text login credentials from Mozilla-based and Chromium-based browsers.
- Text content from Microsoft Edge (Chromium-based) Collections

This text information, is written out to the export folder, where it is included in the Search Index when it is created by the user. The following image shows the index being searched. Create and search the Indexed data by accessing the Index menu in NetAnalysis®.

The screenshot displays the NetAnalysis Search Index window. The search term 'Identity Card' is entered in the search bar. The results table shows the following data:

URN	File Path	Search Hit Count	Document Score
17830	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000017830.txt	577	1.088646
16250	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000016250.txt	3	0.1213707
16613	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000016613.txt	1	0.07007339
10299	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000010299.txt	2	0.04414405
10988	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000010988.txt	3	0.0364112
17574	D:\Desktop\Output\CASE-20200612\ID-124958\Microsoft Edge\HTML to Text\F0000017574.txt	2	0.01981975

Below the table, the selected document (URN 17830) is displayed. The content is a Wikipedia article titled 'Identity document - Wikipedia'. The article text is as follows:

Identity document - Wikipedia

Identity document

From Wikipedia, the free encyclopedia
 Jump to navigation Jump to search
 Several terms redirect here. For a list of national **identity cards**, see List of national **identity card** policies by country . For other uses of "**Identity Card**" see **Identity Card** (disambiguation) . For other uses of "ID", see ID (disambiguation) .
 Any document that may be used to identify a person
 This article may be too long to read and navigate comfortably. The readable prose size is 96 kilobytes. Please consider splitting content into sub-articles, condensing it, or adding subheadings . (March 2015)

An **identity document** (also called a piece of identification or ID, or colloquially as papers) is any document that may be used to prove a person's **identity**. If issued in a small, standard credit card size form, it is usually called an **identity card** (IC, ID card, citizen card), [a] or passport card. [b] Some countries issue formal **identity documents**, as national identification **cards** which may be compulsory or non-compulsory , while others may require **identity verification** using regional identification or informal documents. When the **identity document** incorporates a person's photograph, it may be called photo ID . [1]

In the absence of a formal **identity document**, a driver's license may be accepted in many countries for **identity verification**. Some countries do not accept driver's licenses for identification, often because in those countries they do not expire as documents and can be old or easily forged. Most countries accept passports as a form of identification. Some countries require all people to have an **identity document** available at any time. Many countries require all foreigners to have a passport or occasionally a national **identity card** from their home country available at any time if they do not have a residence permit in the country.

The **identity document** is used to connect a person to information about the person, often in a database . The photo and the possession of it is used to connect the person with the document. The connection between the **identity document** and information database is based on personal information present on the document.

Document Search Hit: 7 of 577



Introduction

HstEx® v4 is an advanced, Windows-based, multi-threaded, forensic data recovery solution which has been designed to recover deleted browser history and cache data from a variety of source forensic evidence files as well as physical and logical devices.

Specifically designed to work in conjunction with NetAnalysis® (and is provided as part of the suite), this powerful software can recover deleted data from a variety of Internet browsers, whether they have been installed on Windows, Linux or Apple Mac systems.

HstEx® supports a number of different source evidence types such as EnCase® e01 (Expert Witness) image files, EnCase® 7 ex01 files, AccessData® FTK™ image files or traditional monolithic and segmented dd image files. It also supports direct sector access to physical and logical devices such as hard disks. HstEx® natively supports these sources for direct access and does not rely upon third party mounting software.

HstEx® is able to extract browser history and cache records directly from source forensic files enabling the recovery of evidence, not only from unallocated clusters, but also from cluster slack, memory dumps, paging files and system restore points amongst others. It is an extremely powerful tool in your forensic tool-box.

HstEx® v4

The latest version of HstEx® is a completely new product which has been engineered from scratch. Utilising powerful parallel processing and Intelli-Carve® technology, HstEx® offers a considerable speed increase over our previous version, allowing the user to select multiple recovery types in a single session.

Another important new feature for HstEx® v4 is the ability to create and queue recovery jobs for later processing.

Supported Browsers



We have added support for the latest browsers. We currently support:

Apple Safari v3 - 13

- History Entries (XML Plist)
- History Files (Binary Plist)
- History Item Entries (v8+)
- History Visit Entries (v8+)
- Download Entries (XML Plist)
- Download Files (Binary Plist)
- Cookie Entries (XML Plist)
- Cache Entries
- TopSite Files (Binary Plist)
- Recently Closed Tab Files (Binary Plist)
- Last Session Files (Binary Plist)
- Bookmarks Files (Binary Plist)
- Reading List Files (Binary Plist)
- Search Descriptions Files (Binary Plist)
- User Notification Permissions Files (Binary Plist) v8+
- Remote Notifications Permissions Files (Binary Plist)

Google Chrome v1 - 83

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v48+)
- Shortcut Entries

Microsoft Internet Explorer v5 - 9

- All History, Cache and Cookie Entries
- Travel Log Entries (v8+)
- Recovery Store, Tab Session (v8+)

Microsoft Internet Explorer v10 - 11

- All History, Cache and Cookie Entries
- Travel Log Entries
- Recovery Store, Tab Session, Roaming Tab Session

Microsoft Internet Explorer XBOX

- All History, Cache and Cookie Entries

Microsoft Edge v20 - 44

- All History, Cache and Cookie Entries
- Reading List Entries
- Travel Log Entries (v20 - 38)
- Recovery Store, Tab Session
- Top Site Entries (v25+)
- Favorite Entries (v25+)
- Cookie Entries (v40+)

Microsoft Edge (Chromium) v74 – 83

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Mozilla Firefox v1 - 77

- History Entries (v3+)
- Cookie Entries (v3+)
- Cache v1 Entries (v1 - 31)
- Cache v2 Entries (v32+)

- Form History Entries (v4+)
- Bookmark Entries (v4+)
- SignOns Entries (v4+)
- Permission Entries (v42+)

Opera Presto v4 - 12

- Typed History Entries
- Search Field History Entries

Opera v15 - 68

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v22+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v35+)
- Shortcut Entries

360 Browser v7

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries

360 Security Browser v6 - 10

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v7+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Shortcut Entries

360 Speed Browser v4 - 11

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v7+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Shortcut Entries

AOL Desktop Browser v9

- Cookie Entries
- Cache Entries

Avast Secure Browser v64 - 81

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

AVG Secure Browser v75 - 81

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Basilisk v2017.11.12 - 2020.05.20

- History Entries
- Cookie Entries
- Cache v2 Entries
- Form History Entries
- Bookmark Entries
- Permission Entries

Blisk v0 - 12

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Brave v0 - 1

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

CCleaner v75 - 81

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Chromium v1 - 83

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v48+)
- Shortcut Entries

Cốc Cốc v26 - 86

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v54+)
- Shortcut Entries

Comodo Chromodo v36 - 52

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v48+)
- Shortcut Entries

Comodo Dragon v4 - 80

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries

- Login Data Entries
- Login Stats Entries (v48+)
- Shortcut Entries

Comodo Ice Dragon v13 - 65

- History Entries
- Cookie Entries
- Cache v1 Entries (v13 - 26)
- Cache v2 Entries (v38+)
- Form History Entries (v26+)
- Bookmark Entries (v26+)
- Permission Entries (v42+)

CoolNovo v1 - 2

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Shortcut Entries

Cyberfox v17 - 52

- History Entries
- Cookie Entries
- Cache v1 Entries (v17 - 31)
- Cache v2 Entries (v32+)
- Form History Entries
- Bookmark Entries
- Permission Entries (v42+)

Epic Privacy Browser v29 - 80

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v48+)

- Shortcut Entries

Flock v2

- Cache Entries

Flock v3

- History Entries
- Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries

IceCat v1 - 52

- History Entries (v3+)
- Cookie Entries (v3+)
- Cache v1 Entries (v1 - 31)
- Cache v2 Entries (v32+)
- Form History Entries (v4+)
- Bookmark Entries (v4+)
- Permissions Entries (v42+)

K-Meleon v1 - 76

- History Entries
- Cookie Entries
- Cache v1 Entries (v1 - 75)
- Cache v2 Entries (v76+)
- Form History Entries (v74+)

Min Browser v0 - 1

- Cookie Entries
- Cache Entries
- Simple Cache Entries

Netscape v6 - 9

- Cache Entries

Opera GX v60 - 68

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Opera Neon v1

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Pale Moon v3 - 28

- History Entries
- Cookie Entries
- Cache v1 Entries (v3 - 26)
- Cache v2 Entries (v27+)
- Form History Entries (v24+)
- Bookmark Entries (v24+)

QQ Browser (Windows) v9 - 10

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Shortcut Entries

SeaMonkey v1 - 2

- History Entries (v2+)
- Cookie Entries (v2+)
- Cache v1 Entries (v1 - 2)
- Cache v2 Entries (v2+)
- Form History Entries (v2+)
- Bookmark Entries (v2+)
- Permission Entries (v2+)

Sleipnir (Windows) v3 - 6

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v4+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v6+)
- Shortcut Entries
- Internet Explorer v5 - 9 Mode Data
- Internet Explorer v10 - 11 Mode Data

Sleipnir (OS X) v3 - 4

- History Files (Binary Plist)
- Cache Entries

SRWare Iron v1 - 81

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v48+)
- Shortcut Entries

Titan Browser v1 - 33

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Shortcut Entries

Torch v1 - 69

- History Entries
- Accelerated Download Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v29+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v51+)
- Shortcut Entries

UC Browser v4 - 7

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v5+)
- Shortcut Entries

Vivaldi v1 - 3

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries

- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Waterfox v4 - 2020.05

- History Entries
- Cookie Entries
- Cache v1 Entries (v4 - 31)
- Cache v2 Entries (v32+)
- Form History Entries
- Bookmark Entries
- Permission Entries (v42+)

Wyzo v3

- History Entries
- Cookie Entries
- Cache Entries

Yandex v1 - 20

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v2+)
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries (v16+)
- Shortcut Entries
- Autofill Data Entries (v19+)
- Credit Card Entries (v19+)

Other Chromium Based Browsers

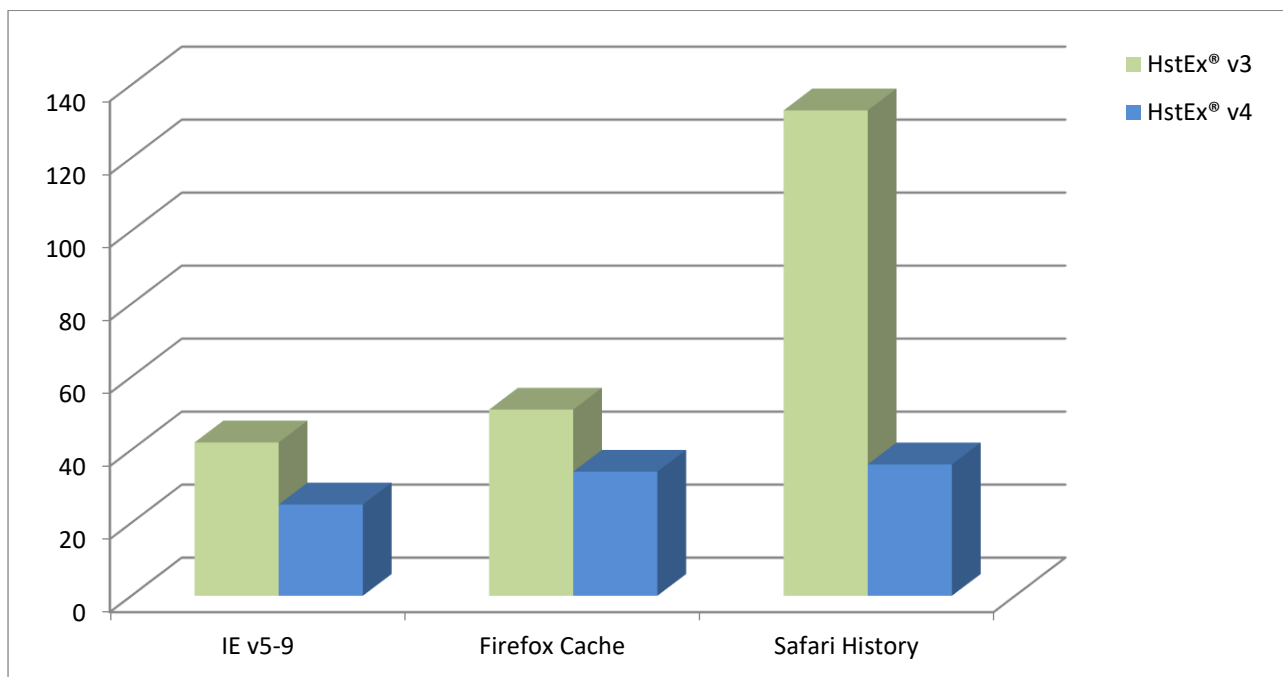
- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries
- Keyword Search Term Entries
- Autofill Entries
- Login Data Entries
- Login Stats Entries
- Shortcut Entries

Other Mozilla Based Browsers

- History Entries
- Cookie Entries
- Cache v1 Entries
- Cache v2 Entries
- Form History Entries
- Bookmark Entries
- Permission Entries

Speed Comparison

Many personal computers and workstations have two or four cores that enable multiple threads to be executed simultaneously. Computers in the near future are expected to have significantly more cores. To take advantage of the hardware of today and tomorrow, we have utilised the power of parallel processing to distribute work across multiple processors. As a result, HstEx® v4 has a considerable speed advantage over other tools which utilise only serial processing.



The above chart shows the total time (in seconds) to search and recover from a 5 GiB image.

Recovery Type	Microsoft Internet Explorer	Mozilla Firefox Cache	Apple Safari History
Recovered	1,947	68,171	29,395
HstEx® v4 Speed	13.26 GB/Min	13.77 GB/Min	12.21 GB/Min

Session File

HstEx® v4 allows the user to create a session and then add multiple recovery jobs as required. Each recovery job has a single data source and allows the user to select as many recovery types as required.

Each job can then be prioritised by moving them up or down the queue. The job at the top of the queue is processed first.

Job ID	Exhibit	Case	Notes	Status
1	CRP-3	HQ-008232-15	Write blocked Seagate ST9750420AS, SN: 5XS57TQQ	Running
2	ID-180036	DD14137	Image of Seagate ST9750420AS Seagate, SN: SDS11TKL	Queued
3	JJB-12	HQ-008232-15	Image of Western Digital	Queued

Status

Information

- Info Physical device Drive Number: 0
- Info Physical device Win32 Name: \\.\PHYSICALDRIVE0
- Info Physical device Total Size: 64,424,509,440
- Info Physical device Drive Type: Fixed
- Info Physical device Interface Type: SCSI
- Info Physical device PNP Device ID: SCSI\Disk&Ven_VMware_8Prod_VMware_Virtual_S\5&1982005&0&000000
- Info Physical device Vendor: VMware
- Info Physical device Product: VMware Virtual S
- Info Physical device is Virtual: True
- Info Selected for processing: Internet Explorer v5 - 9 History • Cache • Cookie Entries
- Info Recovery block size set to: 512 sectors
- Info Data source selected: \\.\PHYSICALDRIVE0
- Info Export Session Folder: C:\Cases\PHYSICALDRIVE0\2014_09_24_18_06_15_992
- Info Available free space on export drive: 43.69 GB
- Info Pass 1: Searching for data...

Summary Information

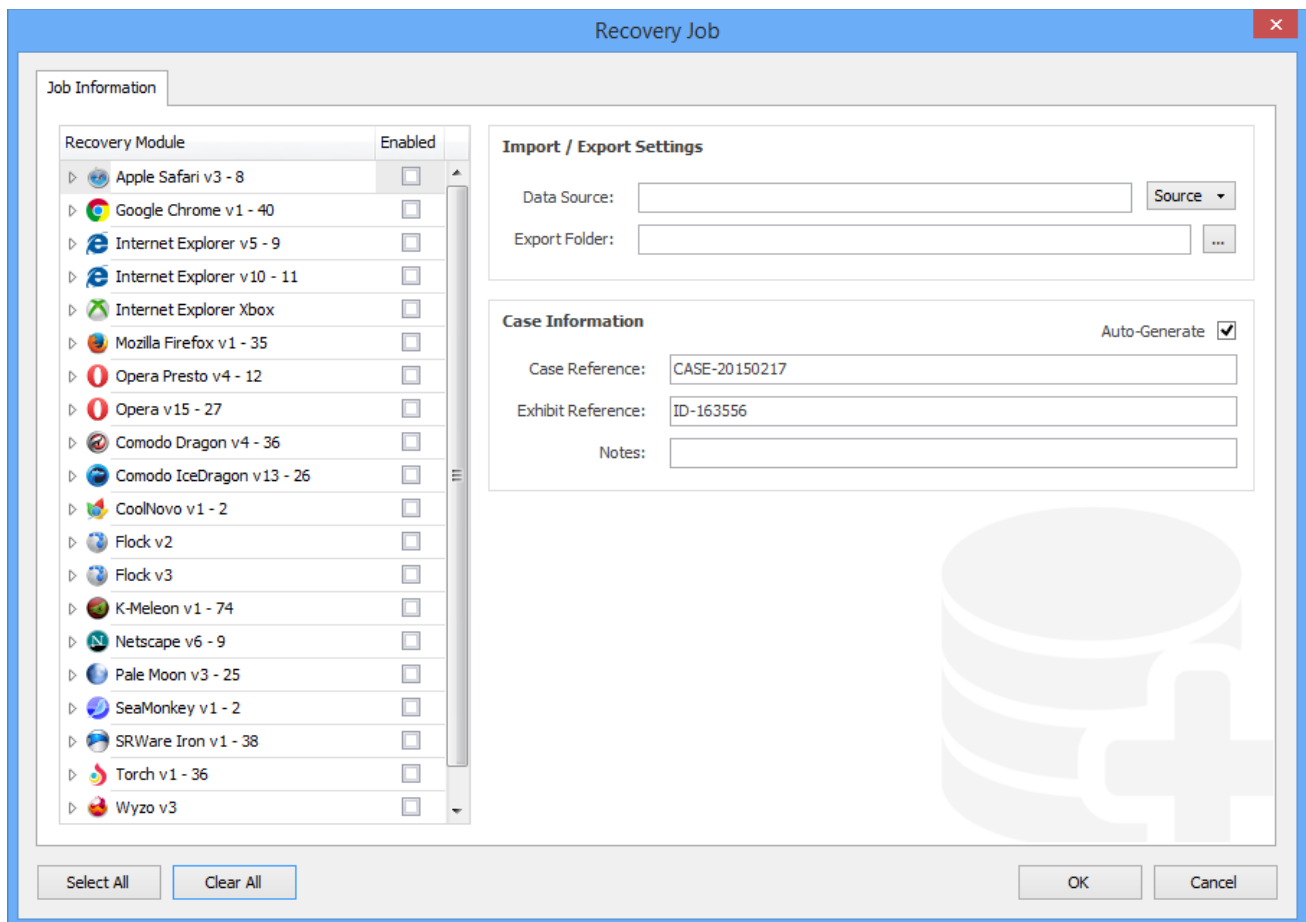
Source: \\.\PHYSICALDRIVE0	Length: 60.00 GB
Export: C:\Cases	Time Left: 3 Minutes, 17 Seconds
Offset: 29,710,352,384	Possible: 10,329
Recovered: 0	Speed: 10.44 GB/Minute

www.digital-detective.net Running

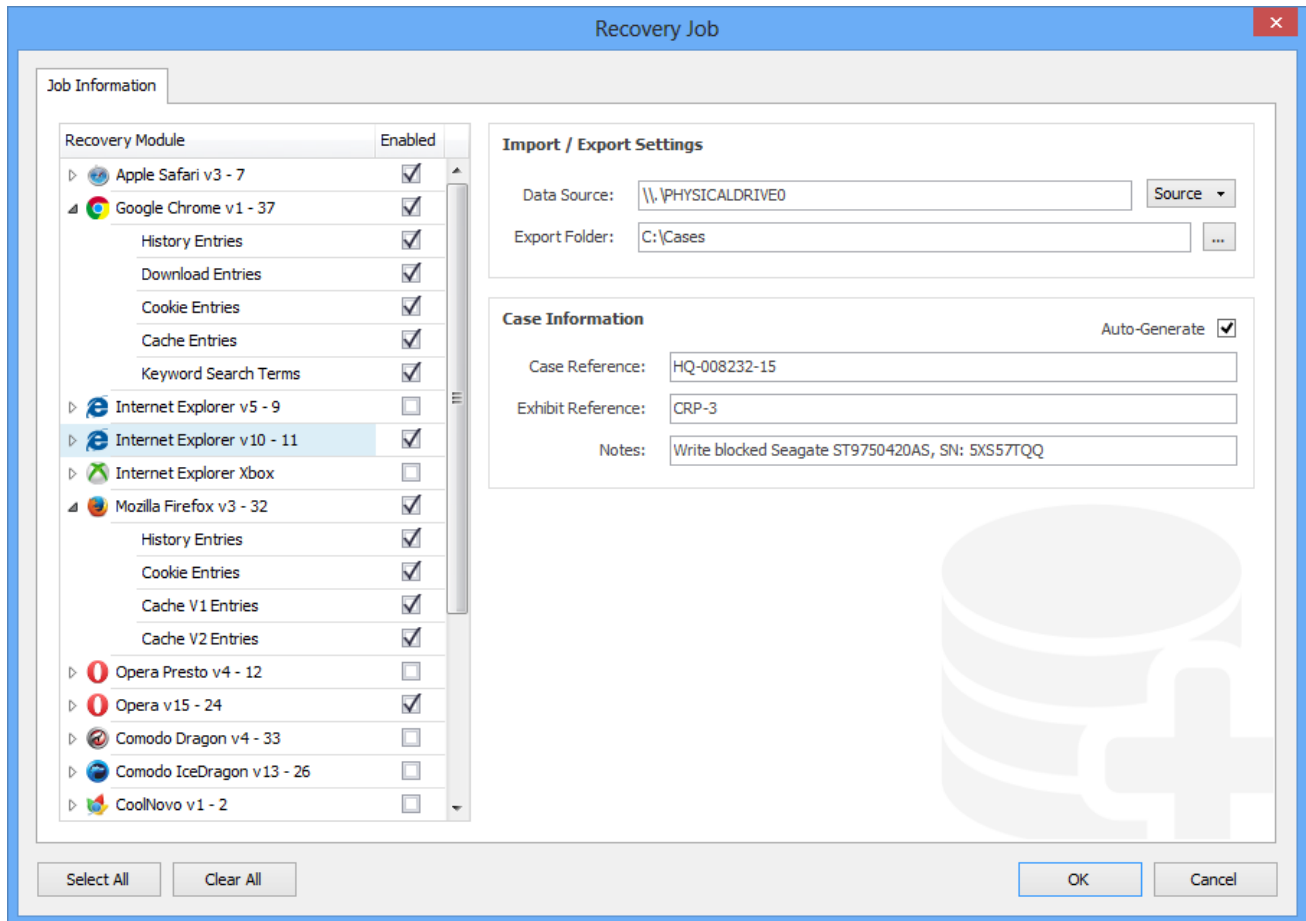
The session in the window above shows three active jobs, with job number one running. The user interface has been enhanced to show the estimated time to completion for the current processing job.

Recovery Job

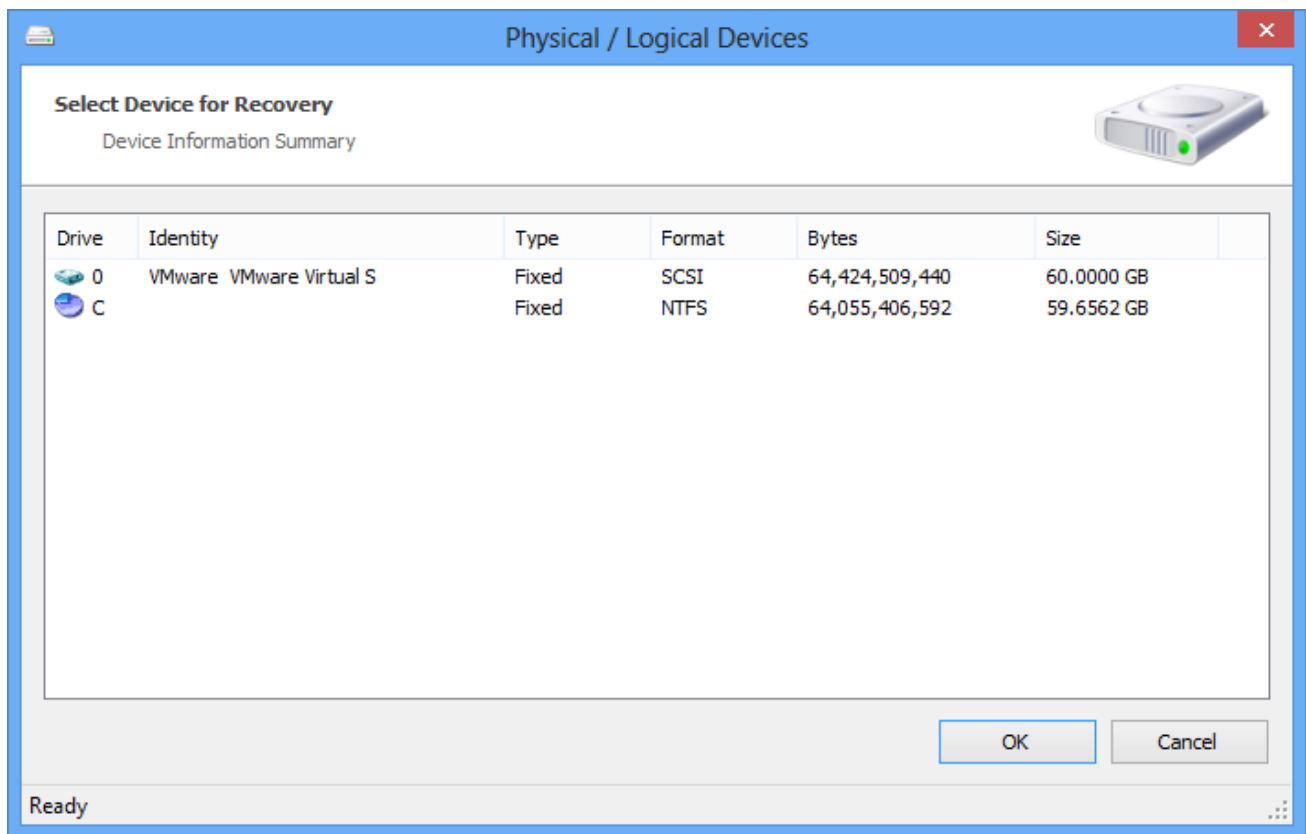
A recovery job contains all the parameters for recovering data against a single source. A powerful new feature for HstEx® v4 is the ability to select multiple recovery modules to run against a source.



The window above shows a recovery job. The user can click to enable recovery of data for a specific browser, or select the individual data types if required. Case information can also be saved for each recovery job.



The window above shows a configured recovery job. In this case, the user has selected to recover data from physical drive 0. When the user selects a physical/logical attached device, the following window is shown.



The window above shows a list of any logical/physical devices attached to the system, along with corresponding technical information relating to that device.

Intelli-Carve®



HstEx® v4 now contains our Intelli-Carve® technology. Intelli-Carve® is an intelligent data recovery and validation engine which can verify data structures during the recovery process.

This powerful technology allows for more accurate recovery of data from unstructured data sources; it also has the capability of detecting errors and corruption.

The window below shows a selected record containing data which Intelli-Carve® has detected as being truncated/corrupt.

NetAnalysis® v2.1 - Forensic Internet History Analysis - [Warning Test]

File View Tools Search Index Filter Reports Column Window Help

Preview URL
 http://lapo.it/asn1js/#
 30821E5206092A864886F70D010702A0821E4330821E3F0201013108300906052B0E03021A05003068060A2B06010401823702010F3025030100A020A21E801C003C003C003C004F00620073006F006C006500740065003E003E003E3021300906052B0E03021A0500041481518A3C25F42888E8F5437FB30E471FE189D04DA0821942308203EE30820357A00302010202107E93EBFB7CC64E59EA489A77D406FC3B300D06092A864886F70D0101050030818B31083009060355040613025A41311530130603550408130C5765737465726E2043617065311430120603550407130B44757262616E76696C6C65310F300D060355040A130654686177465311D301B060355040813145468617746520436572746966696361746966F6E311F301D06035504031316546861774652054696D657374616D70696E667204341301E170D3132313232313030303030305A170D3230313233303233353935395A305E31083009060355040613025553311D301B060355040A131453796D616E74656320436F72706F7261746966F6E3130302E0603550403132753796D616E7465632054696D65205374616D70696E667205365727669636573204341202D20473230820122300D06092A864886F70D010105000382010F003082010A028201010081ACB349544B971C120AD825799122572A6FDCB826C4437368C2BF2E505A FB14C2768E43012543B4A1E245F4E8B77BC374CC22D784940002F74DED8FB487442468CD5F453BD144CE43127317828B69842BCB991EAC721B264D711FB131DDFB51610253A6AAF5492C057845A52F89CEE79E7FE8CE257

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
History	http				0	http://lapo.it/asn1js/#30821E5206092A864886F70D010702A0821E4330821E3F0201013108300906052B0E03021A05003068060A2B06010401823702010F3025030100A020A21E801C003C003C003C004F00620073006F006C006500740065003E003E003E3021300906052B0E03021A0500041481518A3C25F42888E8F5437FB30E471FE189D04DA0821942308203EE30820357A00302010202107E93EBFB7CC64E59EA489A77D406FC3B300D06092A864886F70D0101050030818B31083009060355040613025A41311530130603550408130C5765737465726E2043617065311430120603550407130B44757262616E76696C6C65310F300D060355040A130654686177465311D301B060355040813145468617746520436572746966696361746966F6E311F301D06035504031316546861774652054696D657374616D70696E667204341301E170D3132313232313030303030305A170D3230313233303233353935395A305E31083009060355040613025553311D301B060355040A131453796D616E74656320436F72706F7261746966F6E3130302E0603550403132753796D616E7465632054696D65205374616D70696E667205365727669636573204341202D20473230820122300D06092A864886F70D010105000382010F003082010A028201010081ACB349544B971C120AD825799122572A6FDCB826C4437368C2BF2E505A FB14C2768E43012543B4A1E245F4E8B77BC374CC22D784940002F74DED8FB487442468CD5F453BD144CE43127317828B69842BCB991EAC721B264D711FB131DDFB51610253A6AAF5492C057845A52F89CEE79E7FE8CE257
History	http				0	http://lapo.it/asn1js/#30821E5206092A864886F70D010702A0821E4330821E3F0201013108300906052B0E03021A05003068060A2B06010401823702010F3025030100A020A21E801C003C003C003C004F00620073006F006C006500740065003E003E003E3021300906052B0E03021A0500041481518A3C25F42888E8F5437FB30E471FE189D04DA0821942308203EE30820357A00302010202107E93EBFB7CC64E59EA489A77D406FC3B300D06092A864886F70D0101050030818B31083009060355040613025A41311530130603550408130C5765737465726E2043617065311430120603550407130B44757262616E76696C6C65310F300D060355040A130654686177465311D301B060355040813145468617746520436572746966696361746966F6E311F301D06035504031316546861774652054696D657374616D70696E667204341301E170D3132313232313030303030305A170D3230313233303233353935395A305E31083009060355040613025553311D301B060355040A131453796D616E74656320436F72706F7261746966F6E3130302E0603550403132753796D616E7465632054696D65205374616D70696E667205365727669636573204341202D20473230820122300D06092A864886F70D010105000382010F003082010A028201010081ACB349544B971C120AD825799122572A6FDCB826C4437368C2BF2E505A FB14C2768E43012543B4A1E245F4E8B77BC374CC22D784940002F74DED8FB487442468CD5F453BD144CE43127317828B69842BCB991EAC721B264D711FB131DDFB51610253A6AAF5492C057845A52F89CEE79E7FE8CE257
History	data				0	data:image/jpeg;base64,iVBORwOKGgoAAAANSURUlgAAAOIAAAK8CAIAAAE6IKhoAAAAAXNSR0IArs4cQAARnQUlBAACxjiwv8YQUAA
History	http				0	http://lapo.it/asn1js/#30821E5206092A864886F70D010702A0821E4330821E3F0201013108300906052B0E03021A05003068060A2B06010401823702010F3025030100A020A21E801C003C003C003C004F00620073006F006C006500740065003E003E003E3021300906052B0E03021A0500041481518A3C25F42888E8F5437FB30E471FE189D04DA0821942308203EE30820357A00302010202107E93EBFB7CC64E59EA489A77D406FC3B300D06092A864886F70D0101050030818B31083009060355040613025A41311530130603550408130C5765737465726E2043617065311430120603550407130B44757262616E76696C6C65310F300D060355040A130654686177465311D301B060355040813145468617746520436572746966696361746966F6E311F301D06035504031316546861774652054696D657374616D70696E667204341301E170D3132313232313030303030305A170D3230313233303233353935395A305E31083009060355040613025553311D301B060355040A131453796D616E74656320436F72706F7261746966F6E3130302E0603550403132753796D616E7465632054696D65205374616D70696E667205365727669636573204341202D20473230820122300D06092A864886F70D010105000382010F003082010A028201010081ACB349544B971C120AD825799122572A6FDCB826C4437368C2BF2E505A FB14C2768E43012543B4A1E245F4E8B77BC374CC22D784940002F74DED8FB487442468CD5F453BD144CE43127317828B69842BCB991EAC721B264D711FB131DDFB51610253A6AAF5492C057845A52F89CEE79E7FE8CE257
History	data				0	data:image/jpeg;base64,iVBORwOKGgoAAAANSURUlgAAAOIAAAK8CAIAAAE6IKhoAAAAAXNSR0IArs4cQAARnQUlBAACxjiwv8YQUAA
History	http				0	http://lapo.it/asn1js/#30821E5206092A864886F70D010702A0821E4330821E3F0201013108300906052B0E03021A05003068060A2B06010401823702010F3025030100A020A21E801C003C003C003C004F00620073006F006C006500740065003E003E003E3021300906052B0E03021A0500041481518A3C25F42888E8F5437FB30E471FE189D04DA0821942308203EE30820357A00302010202107E93EBFB7CC64E59EA489A77D406FC3B300D06092A864886F70D0101050030818B31083009060355040613025A41311530130603550408130C5765737465726E2043617065311430120603550407130B44757262616E76696C6C65310F300D060355040A130654686177465311D301B060355040813145468617746520436572746966696361746966F6E311F301D06035504031316546861774652054696D657374616D70696E667204341301E170D3132313232313030303030305A170D3230313233303233353935395A305E31083009060355040613025553311D301B060355040A131453796D616E74656320436F72706F7261746966F6E3130302E0603550403132753796D616E7465632054696D65205374616D70696E667205365727669636573204341202D20473230820122300D06092A864886F70D010105000382010F003082010A028201010081ACB349544B971C120AD825799122572A6FDCB826C4437368C2BF2E505A FB14C2768E43012543B4A1E245F4E8B77BC374CC22D784940002F74DED8FB487442468CD5F453BD144CE43127317828B69842BCB991EAC721B264D711FB131DDFB51610253A6AAF5492C057845A52F89CEE79E7FE8CE257

Record 6 of 57

Contains([Warning], 'truncated')

Warnings

1 Truncated field: 'url1' - expected length: 15555, actual length: 3315

www.digital-detective.net C:\Users\Craig Wilson\Desktop\Browser Test 2.Ex01 PS: 8018593 SO: 250

Supported Source Data Formats

HstEx® v4 natively supports a number of different image and output file formats. The following table represents a summary of the supported file types.

File Format	File Extensions
EnCase® v1-7 Image File (EVF / Expert Witness Format)	*.e01
EnCase® v7 Evidence File Format v2	*.ex01
EnCase® v5 - 8 Logical Evidence File Format v1	*.L01
EnCase® v7 - 8 Logical Evidence File Format v2	*.Lx01
SMART/Expert Witness Image File	*.s01
X-Ways Forensics Image File	*.e01
VMWare Virtual Disk File	*.vmdk
Virtual Hard Disk	*.vhd
Segmented Image Unix / Linux DD / Raw Image Files	*.000, *.0000, *.00000, *.001, *.0001, *.00001
Single Image Unix / Linux DD / Raw / Monolithic Image Files	*.dd; *.img; *.ima; *.raw
Memory Dumps	*.dmp; *.dump; *.crash; *.mem; *.vmem; *.mdmp
Binary Dumps	*.bin; *.dat; *.unallocated; *.rec; *.data; *.binary
Mobile Phone Raw Binary Memory Dumps	*.bin

Digital Detective Group

Motis Business Centre
Cheriton High Street
Folkestone
Kent, CT19 4QJ
United Kingdom



DIGITAL®
DETECTIVE

©2020 Digital Detective Group. All rights reserved.

Digital Detective, the Digital Detective logo, and the NetAnalysis, HstEx product and service names mentioned herein are registered trademarks or trademarks of Digital Detective Group, or its affiliated entities.

All other trademarks are the property of their respective owners.