New Artefacts in 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.

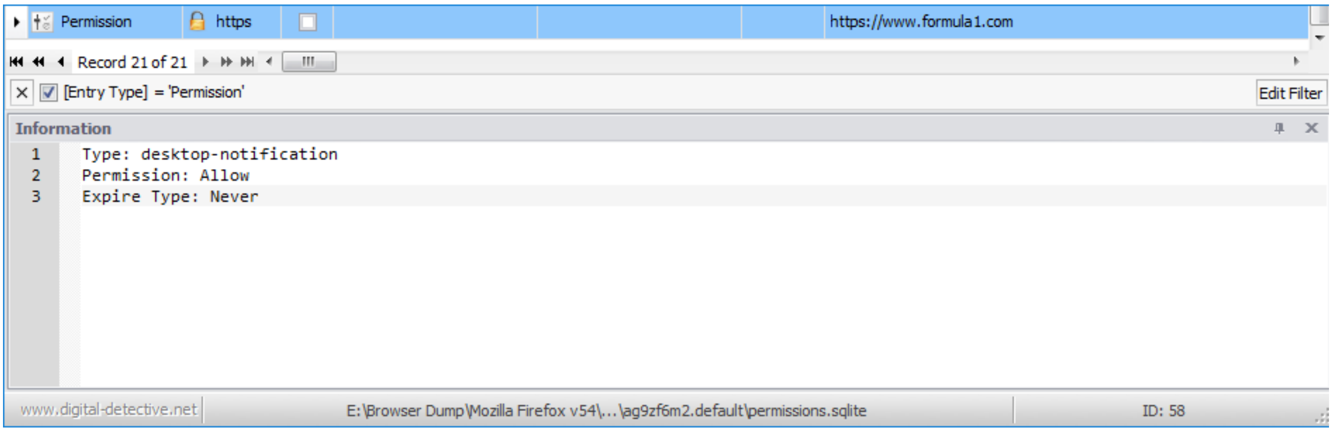
NetAnalysis® supports processing Google Chrome and Chromium based Simple disk cache and well as exporting and rebuilding web pages.

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 popup windows and to initiate extensions installation.

- http://kb.mozillazine.org/Cookies

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



Permission https https://www.formula1.com

Record 21 of 21

☑ [Entry Type] = 'Permission'

```
Type: desktop-notification
Permission: Allow
Expire Type: Never
```

www.digital-detective.net E:\Browser Dump\Mozilla Firefox v54\...\ag9zf6m2.default\permissions.sqlite ID: 58

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.

- https://help.vivaldi.com/article/notes/

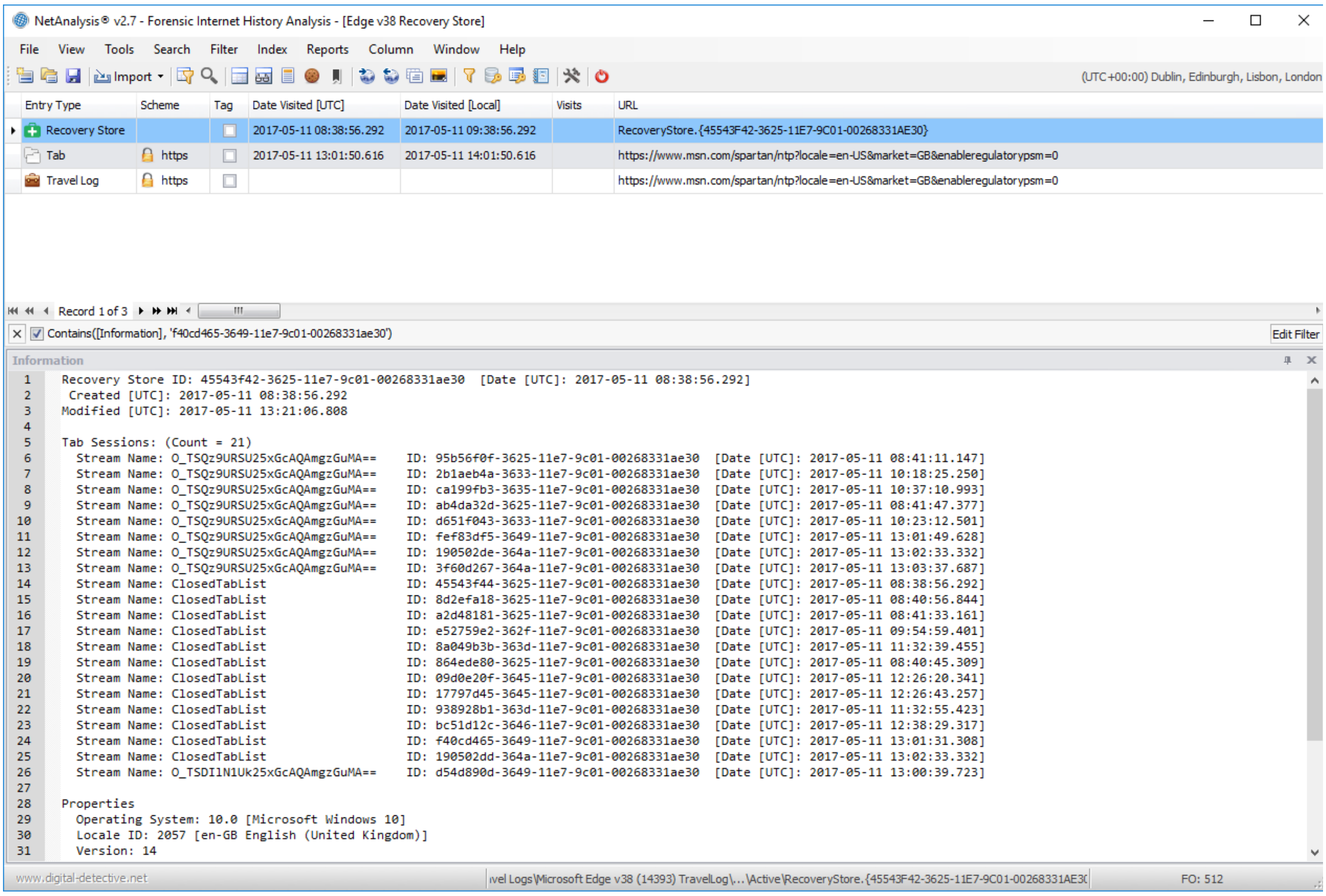
NetAnalysis® now recovers Vivaldi Notes. The note content is written to the case export folder and indexed. Any attachments are written to the case export folder.

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]
File View Tools Search Filter Index Reports Column Window Help
Import
(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Recovery Store		□	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/ntp?locale=en-US&market=GB&enableregulatorypsm=0
Travel Log	https	□				https://www.msn.com/spartan/ntp?locale=en-US&market=GB&enableregulatorypsm=0

☑ Contains([Information], 'f40cd465-3649-11e7-9c01-00268331ae30')

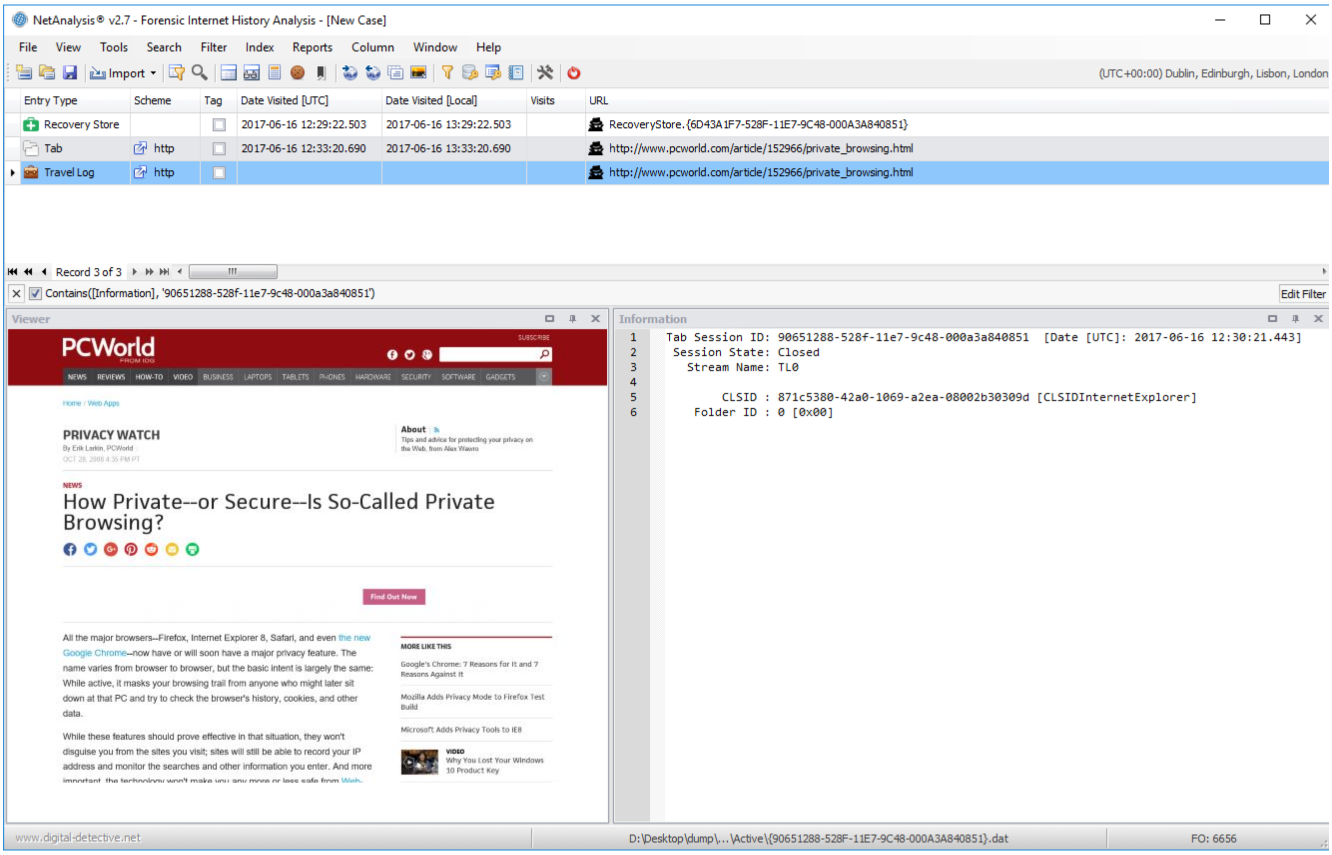
```
Recovery Store ID: 45543f42-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:38:56.292]
 Created [UTC]: 2017-05-11 08:38:56.292
Modified [UTC]: 2017-05-11 13:21:06.808

Tab Sessions: (Count = 21)
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: 95b56f0f-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:41:11.147]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: 2b1aeb4a-3633-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 10:18:25.250]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: ca199fb3-3635-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 10:37:10.993]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: ab4da32d-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:41:47.377]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: d651f043-3633-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 10:23:12.501]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: fef83df5-3649-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:01:49.628]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: 190502de-364a-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:02:33.332]
  Stream Name: O_TSQz9URSU25xGcAQAmgzGuMA==    ID: 3f60d267-364a-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:03:37.687]
  Stream Name: ClosedTabList                   ID: 45543f44-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:38:56.292]
  Stream Name: ClosedTabList                   ID: 8d2efa18-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:40:56.844]
  Stream Name: ClosedTabList                   ID: a2d48181-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:41:33.161]
  Stream Name: ClosedTabList                   ID: e52759e2-362f-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 09:54:59.401]
  Stream Name: ClosedTabList                   ID: 8a049b3b-363d-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 11:32:39.455]
  Stream Name: ClosedTabList                   ID: 864ede80-3625-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 08:40:45.309]
  Stream Name: ClosedTabList                   ID: 09d0e20f-3645-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 12:26:20.341]
  Stream Name: ClosedTabList                   ID: 17797d45-3645-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 12:26:43.257]
  Stream Name: ClosedTabList                   ID: 938928b1-363d-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 11:32:55.423]
  Stream Name: ClosedTabList                   ID: bc51d12c-3646-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 12:38:29.317]
  Stream Name: ClosedTabList                   ID: f40cd465-3649-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:01:31.308]
  Stream Name: ClosedTabList                   ID: 190502dd-364a-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:02:33.332]
  Stream Name: O_TSDI1N1Uk25xGcAQAmgzGuMA==    ID: d54d890d-3649-11e7-9c01-00268331ae30  [Date [UTC]: 2017-05-11 13:00:39.723]

Properties
  Operating System: 10.0 [Microsoft Windows 10]
  Locale ID: 2057 [en-GB English (United Kingdom)]
  Version: 14
```

www.digital-detective.net
ıvel Logs\Microsoft Edge v38 (14393) TravelLog\...\Active\RecoveryStore.{45543F42-3625-11E7-9C01-00268331AE3(
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.


NetAnalysis® v2.7 - Forensic Internet History Analysis - [New Case]
File
View
Tools
Search
Filter
Index
Reports
Column
Window
Help
Import
(UTC+00:00) Dublin, Edinburgh, Lisbon, London
Record 3 of 3
Edit Filter
Viewer
Information
www.digital-detective.net
FO: 6656

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

☑ Contains([Information], '90651288-528f-11e7-9c48-000a3a840851')

```
Tab Session ID: 90651288-528f-11e7-9c48-000a3a840851  [Date [UTC]: 2017-06-16 12:30:21.443]
 Session State: Closed
   Stream Name: TL0

        CLSID : 871c5380-42a0-1069-a2ea-08002b30309d [CLSIDInternetExplorer]
     Folder ID : 0 [0x00]
```

D:\Desktop\dump\...\Active\{90651288-528F-11E7-9C48-000A3A840851}.dat

PCWorld FROM IDG

SUBSCRIBE

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Home / Web Apps

PRIVACY WATCH
By Erik Larkin, PCWorld
OCT 28, 2008 4:35 PM PT

About
Tips and advice for protecting your privacy on the Web, from Alex Wawro

NEWS

How Private--or Secure--Is So-Called Private Browsing?

Find Out Now

All the major browsers--Firefox, Internet Explorer 8, Safari, and even the new Google Chrome--now have or will soon have a major privacy feature. The name varies from browser to browser, but the basic intent is largely the same: While active, it masks your browsing trail from anyone who might later sit down at that PC and try to check the browser's history, cookies, and other data.

While these features should prove effective in that situation, they won't disguise you from the sites you visit; sites will still be able to record your IP address and monitor the searches and other information you enter. And more important, the technology won't make you any more or less safe from Web-

MORE LIKE THIS

Google's Chrome: 7 Reasons for It and 7 Reasons Against It

Mozilla Adds Privacy Mode to Firefox Test Build

Microsoft Adds Privacy Tools to IE8

VIDEO
Why You Lost Your Windows 10 Product Key

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

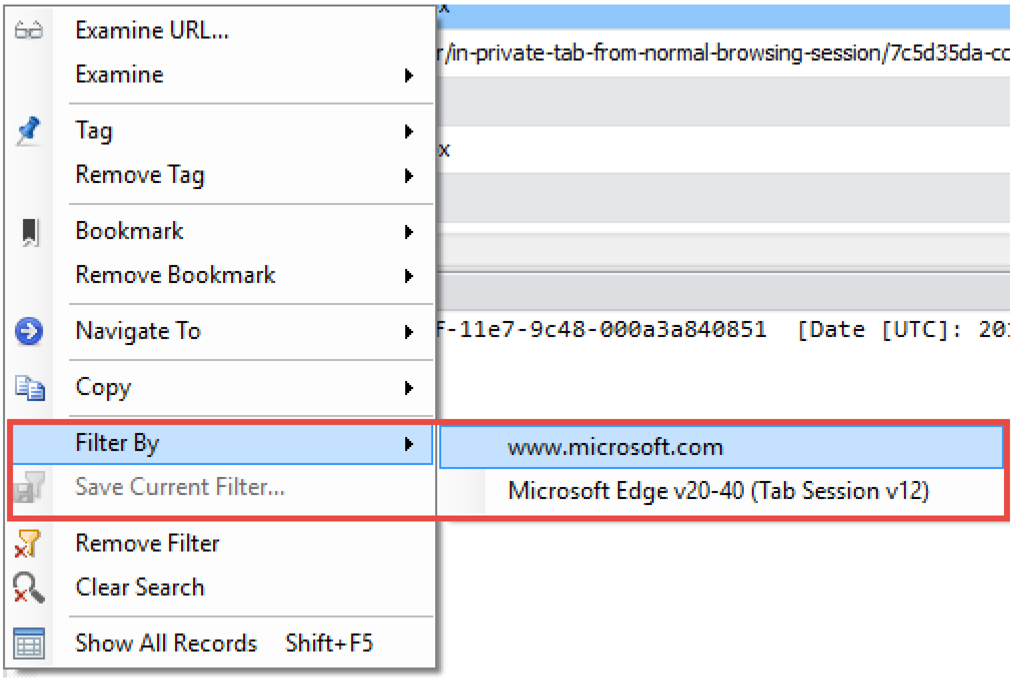
We have made some changes to the user interface to enhance usability:

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.



Examine URL...
Examine
Tag
Remove Tag
Bookmark
Remove Bookmark
Navigate To
Copy
Filter By
Save Current Filter...
Remove Filter
Clear Search
Show All Records Shift+F5
www.microsoft.com
Microsoft Edge v20-40 (Tab Session v12)
r/in-private-tab-from-normal-browsing-session/7c5d35da-cc
x
F-11e7-9c48-000a3a840851 [Date [UTC]: 20

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.