

NetAnalysis v2.12



- Introduction
- New Features
 - AVG Secure Browser
 - Min Browser
 - Apple Safari
 - Microsoft Edge Collections
 - Yandex Login Data
 - Chromium Based Quota Manager
- Improvements
 - Internal Viewer
 - Reporting
 - User Interface Enhancements
 - Improved Support for Processing Mounted File Systems
 - Additional Content Available for Search Indexing
- Change Log

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.

The screenshot displays the NetAnalysis v2.12 interface. The main window shows a list of cache entries with columns for Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, and URL. The selected entry is a cache entry for the URL <https://apis.google.com/js/googleapis.proxy.js?onload=startup>. Below the list, the 'Information' pane shows details for the selected entry, including the Cache Key, Date Created, Date Last Used, Date Last Modified, Date Validated (Request Time), Date Validated (Response Time), Source IP, Protocol, Connection Info, and Date Cache Created. The 'HTTP Response' pane shows the response details, including the status (200), content type (application/javascript), and various headers.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	https		2017-09-15 14:23:05.396	2017-09-15 15:23:05.396		https://apis.google.com/_js/abc-static/_js/k=gapi.gapi.en.ZPSwvoEq44A.O/m=rpc,shindig_random/rt=js/v=1/d=1/ed=1/am=AAg/rs=...
Cache	https		2017-09-15 14:23:05.414	2017-09-15 15:23:05.414		https://apis.google.com/js/googleapis.proxy.js?onload=startup
Cache	https		2017-09-15 14:23:05.749	2017-09-15 15:23:05.749		https://apis.google.com/_js/abc-static/_js/k=gapi.gapi.en.ZPSwvoEq44A.O/m=googleapis_proxy/rt=js/v=1/d=1/ed=1/am=AAg/rs=...
Cache	https		2017-09-15 14:23:05.877	2017-09-15 15:23:05.877		https://mail.google.com/_js/cs/mail-static/_js/k=gmail.main.en.ujO6RgBCjN0.O/m=sy45,syl7,syl6,e/am=ccE8JN8PAQ4zYnzSDMLS__zloV...
Cache	https		2017-09-15 14:23:07.729	2017-09-15 15:23:07.729		https://mail.google.com/mail/u/0/images/cleardot.gif?zx=ugufil9ojph
Cache	https		2017-09-15 14:23:10.149	2017-09-15 15:23:10.149		https://www.google.co.uk/search?q=chic%40broxbear.co.uk&rlz=1C1GIWA_engB600GB6008oq=chic%40broxbear.co.uk&qs=chrom...
Cache	https		2017-09-15 14:23:11.012	2017-09-15 15:23:11.012		https://www.google.co.uk/_js/cs/_js/k=xjs.s.en.QPabDn8ZQkA.O/m=aa,abd,aspn,asyn,dlv,foot,fpe,ipv6,ju,m,mppck,sf,spch,tl,vs,d3,tn...
Cache	https		2017-09-15 14:23:11.102	2017-09-15 15:23:11.102		https://www.google.co.uk/images/iphd/px.gif
Cache	https		2017-09-15 14:23:11.105	2017-09-15 15:23:11.105		https://www.google.co.uk/gen_204?etyp=&ct=phandle&cad=0,deb:0&ei=TeK7WduVGOCgAbr-YroAw&zx=1505485391025
Cache	https		2017-09-15 14:23:18.380	2017-09-15 15:23:18.380		https://notifications.google.com/_js/cs/social-static/_js/k=boq.NotificationsOgbUi.en.Q_dDoszwr0.O/ck=boq.NotificationsOgbUi.1cyl4f...
Cache	https		2017-09-15 14:23:18.404	2017-09-15 15:23:18.404		https://notifications.google.com/_js/cs/social-static/_js/k=boq.NotificationsOgbUi.en.Q_dDoszwr0.O/ck=boq.NotificationsOgbUi.1cyl4f...
Cache	https		2017-09-15 14:23:28.154	2017-09-15 15:23:28.154		https://www.google.co.uk/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=&ig=ibroxbear.co.uk&it=3&cp=15&pgd...
Cache	https		2017-09-15 14:24:05.260	2017-09-15 15:24:05.260		https://www.google.co.uk/complete/search?client=psy-ab&hl=en-GB&gs_ri=64&gs_rm=64&gs_rj=report-ab&tok=rJGINfXVKOHL1gyQ6ejjw&cp=0&g...
Cache	https		2017-09-15 14:24:05.284	2017-09-15 15:24:05.284		https://www.google.co.uk/?gfe_rd=cr&cdr=0&ei=g-K7WaOLEPh38AfxkLIACA

Record 2853 of 6823

Information

```
1 Cache Key: https://apis.google.com/js/googleapis.proxy.js?onload=startup
2 Date Created [UTC]: 2017-09-15 14:23:05.229
3 Date Last Used [UTC]: 2017-09-15 14:23:05.414
4 Date Last Modified [UTC]: 2017-09-15 14:23:05.414
5 Date Validated (Request Time) [UTC]: 2017-09-15 14:23:05.229
6 Date Validated (Response Time) [UTC]: 2017-09-15 14:23:05.379
7 Source IP: 2a00:1450:4009:80c::200e Port: 443
8 Protocol: http/2+quic/37
9 Connection Info: http/2+quic/37
10 Date Cache Created [UTC]: 2014-08-08 16:36:22.443
```

HTTP Response

```
1 HTTP/1.1 200
2 status:200
3 content-type:application/javascript; charset=utf-8
4 content-security-policy:script-src 'unsafe-inline' 'unsafe-eval' 'self'
  https://*.gstatic.com https://www.google-analytics.com
  https://pagead2.googleservices.com https://pagead2.googlesyndication.com
  https://tpc.googlesyndication.com https://s.yimg.com
  https://www.youtube.com/report-uri/_/_/cspreport/es_oz_20170913.14_p0
5 x-ua-compatible:IE=edge, chrome=1
6 timing-Allow-Origin:*
7 etag:"07c1ba480e588816aedbfe6a5e904376"
8 expires:Fri, 15 Sep 2017 14:23:05 GMT
9 Date: Fri, 15 Sep 2017 14:23:05 GMT
```

New Features

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.

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

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.

NetAnalysis® v2.12 - Forensic Internet History Analysis - [Vivaldi Test Data]

File View Tools Search Filter Index Reports Column Window Help

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

Preview URL
 data:image/png;base64,iVBORw0KGgoAAAANSU...
 data:image/jpeg;base64,iVBORw0KGgoAAAANSU...
 data:text/html,<script>alert('hi');</script>
 data:text/html,<a%20href='www.digital-detective.net'>Visit%20DD
 data:text/html,<img%20src='data:image/png;base64,iVBORw0KGgoAAAANSU...>

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Bookmark	data					data:image/png;base64,iVBORw0KGgoAAAANSU...
Bookmark	data					data:image/jpeg;base64,iVBORw0KGgoAAAANSU...
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,iVBORw0KGgoAAAANSU...

Record 1 of 109

[Scheme] = 'data' Edit Filter

Viewer

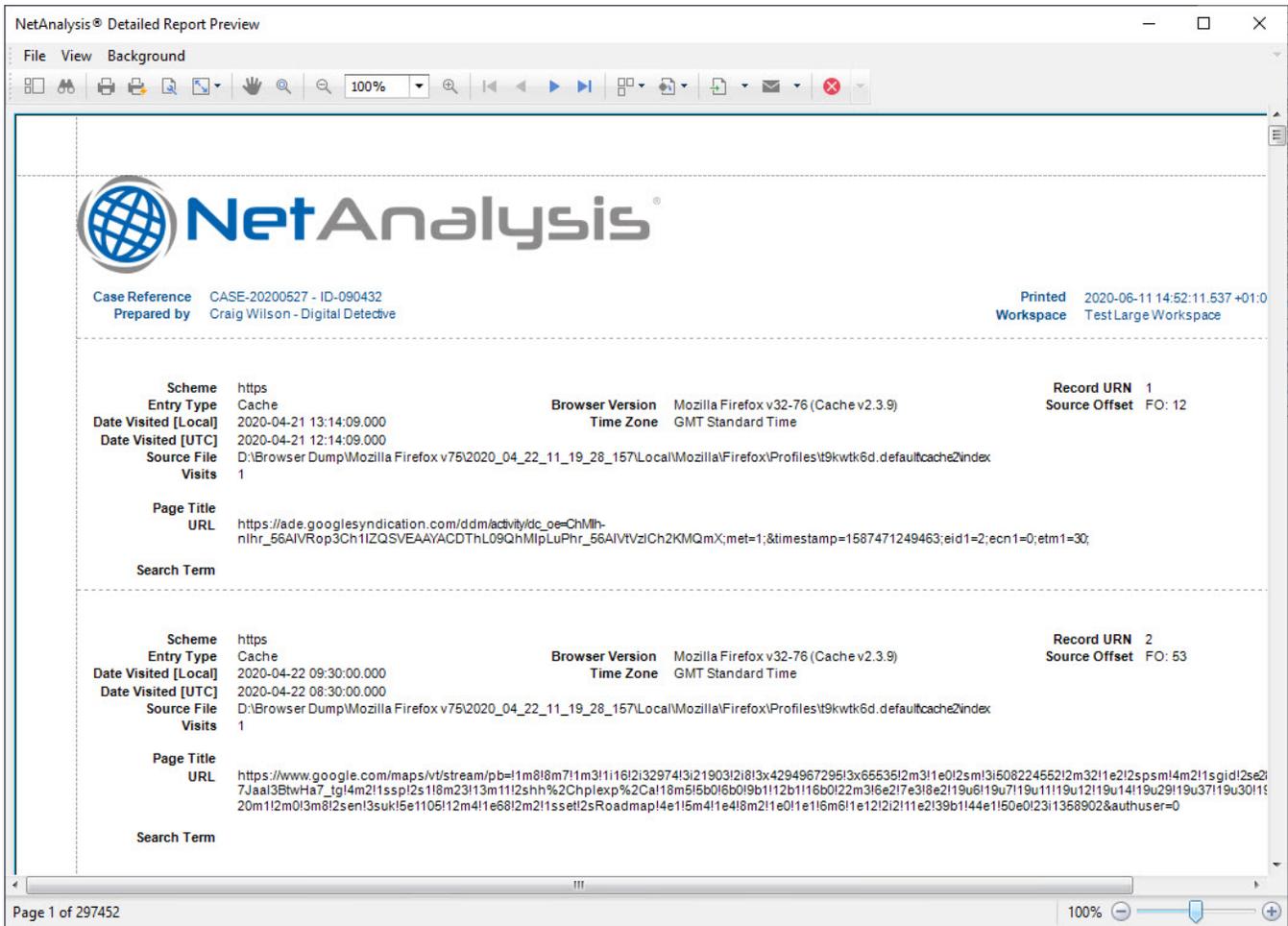
www.digital-detective.net \\digital03\Browser Data Windows\... Default\Bookmarks ID: 127

We have also added support for viewing MHTML documents.

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 following screen shows a generated report containing 297,452 pages:



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.

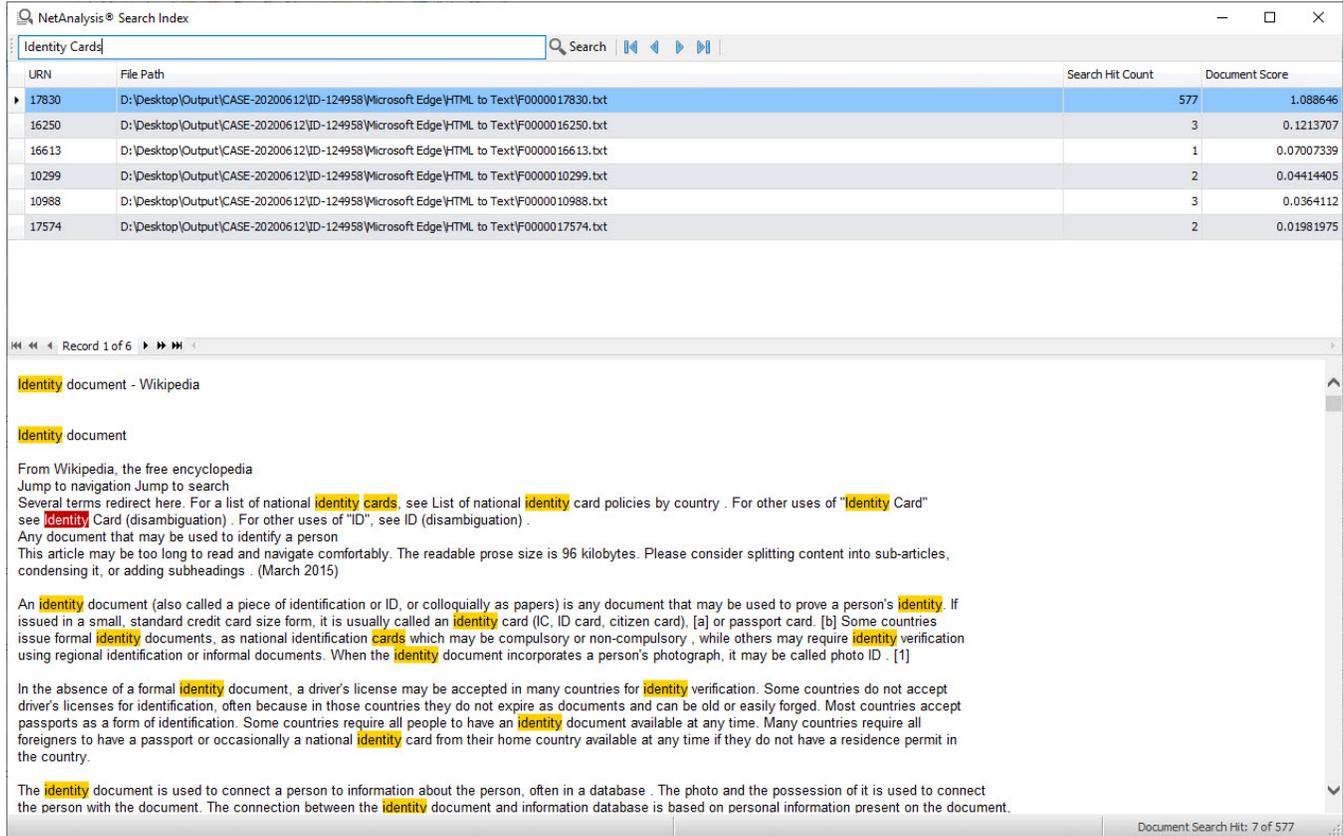
Additional Content Available for Search Indexing

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®.



Change Log

To review the full list of changes for this release, please see: [Change Log v2.12](#).