

NetAnalysis v3.0



- Release Notes for NetAnalysis® Version 3.0
- Enhanced Filtering
 - New Filter Editor
- Progress Filtering
- New Properties Examiner
- Improved Search Index
- Zone Identifier ADS
- Change Log
- Release Notes for HstEx® Version 5.0

Release Notes for NetAnalysis® Version 3.0

Version 3 is a major release of NetAnalysis® and adds over **200 new artefacts** as well as new support for **mobile** and **portable** browsers. The user interface has been completely re-written and adds major improvements and new features in a number of key areas. We have improved the layout of the user interface, with the goal of improving productivity, and added support for light and dark themes. Our grids now boast powerful Excel-style column filtering with easy access string, number and date filtering. Another key feature is the built-in **Properties Examiner** with powerful examination, analysis and reporting of browser preferences.

In combination with **HstEx® v5**, NetAnalysis® is the most powerful, comprehensive, browser forensic analysis suite available. However, don't just take our word for it, **take it for a spin** and see the powerful features in action.

The screenshot displays the NetAnalysis v3.0 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 is divided into several sections:

- Preview URL:** Shows the current URL being analyzed: `https://m.media-amazon.com/images/S/sash/E6vgqilrVgGb3f.png`.
- Table:** A table with columns: Entry Type, Scheme, Tag, Date Visited [UTC], Date Visited [Local], Visits, URL, and Decoded URL. It lists various cache entries and history items.
- Properties Examiner:** A section on the right that provides detailed information about the selected entry, including 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.
- Filter Manager:** A section on the right that allows users to manage filters. It shows a list of filters with columns for Name, Date Modified, and Size.

The bottom of the interface includes a status bar with information like 'Record 8386 of 12655', 'www.digital-detective.net', and 'K:\Test Data Sets\CDS\Google Chrome\v90\2021_05_20_11_12_21_458\Local\Google\Chrome\User Data\Default\Cache\index'.

Enhanced Filtering

Our grids now support enhanced Excel-style column filters. The menus contain two tabs: Values and Filters. The Values tab allows the user to select specific values or value ranges. The Filter tab allows the user to create custom filters using comparison operators that match the data type. The video below shows the Filter for a Date column in action.

NetAnalysis® v3.1 - Forensic Internet History Analysis - [UC Browser on Android]

FileViewToolsSearchFilterIndexReportsColumnWindowHelp

ImportFilterSearchCalendarIndexReportsColumnWindowHelp

| | Entry Type | Scheme | Tag | Date Visited [UTC] | Date Visited [Local] | URL |
|--|-------------|--------|-----|-------------------------|-------------------------|---|
| | Login Data | https | | 2021-09-13 13:09:19.309 | 2021-09-13 14:09:19.309 | https://m.facebook.com/login/device-based/regular/login/ |
| | Login Data | https | | 2021-09-13 13:10:03.213 | 2021-09-13 14:10:03.213 | https://m.facebook.com/login/device-based/regular/login/ |
| | Login Data | https | | 2021-09-13 13:12:45.704 | 2021-09-13 14:12:45.704 | https://mega.nz/login |
| | Login Data | https | | 2021-09-14 10:24:56.872 | 2021-09-14 11:24:56.872 | https://mega.nz/login |
| | Login Data | https | | 2021-09-14 10:26:05.741 | 2021-09-14 11:26:05.741 | https://www.pcloud.com/eu |
| | Login Data | https | | 2021-09-14 10:26:53.951 | 2021-09-14 11:26:53.951 | https://www.myheritage.com/ |
| | Login Data | https | | 2021-09-14 10:31:47.695 | 2021-09-14 11:31:47.695 | https://m.facebook.com/login/device-based/regular/login/ |
| | Login Data | https | | 2021-09-14 10:33:56.721 | 2021-09-14 11:33:56.721 | https://accounts.google.com/signin/v2/challenge/password/e |
| | Login Data | https | | 2021-09-14 10:35:13.913 | 2021-09-14 11:35:13.913 | https://accounts.google.com/signin/v2/challenge/password/e |
| | Login Data | https | | 2021-09-14 11:21:26.803 | 2021-09-14 12:21:26.803 | https://www.digital-detective.net/cgi-bin/digitalboard/YaBB.p |
| | Quota Usage | https | | 2021-09-13 13:20:05.091 | 2021-09-13 14:20:05.091 | https://www.digital-detective.net/ |
| | Quota Usage | https | | 2021-09-14 11:22:12.636 | 2021-09-14 12:22:12.636 | https://mega.nz/ |

New Filter Editor

The Filter Editor allows the user to build complex filters with an unlimited number of filter conditions combined by logical operators. The visual styling of the Filter Editor has been improved to make it much easier to view, edit and build powerful data filters.

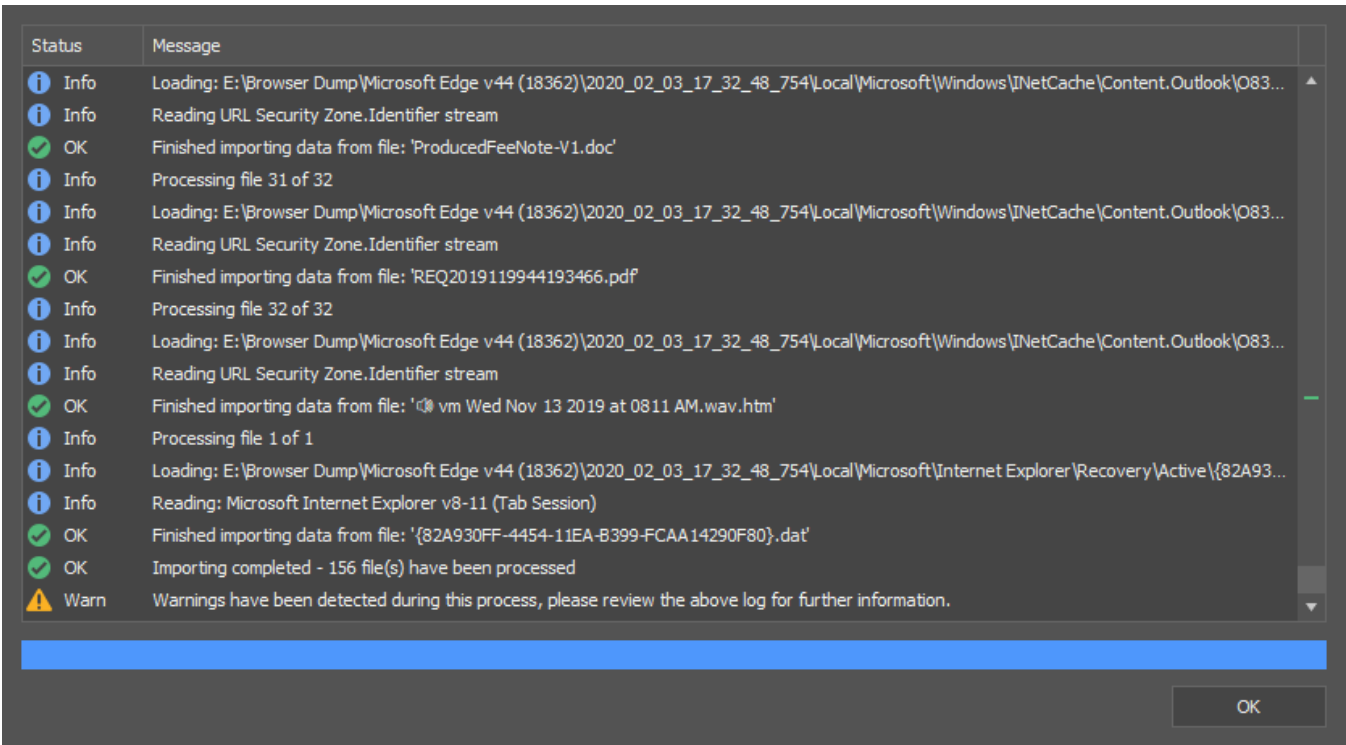
Filter Editor

And

OKCancelApply

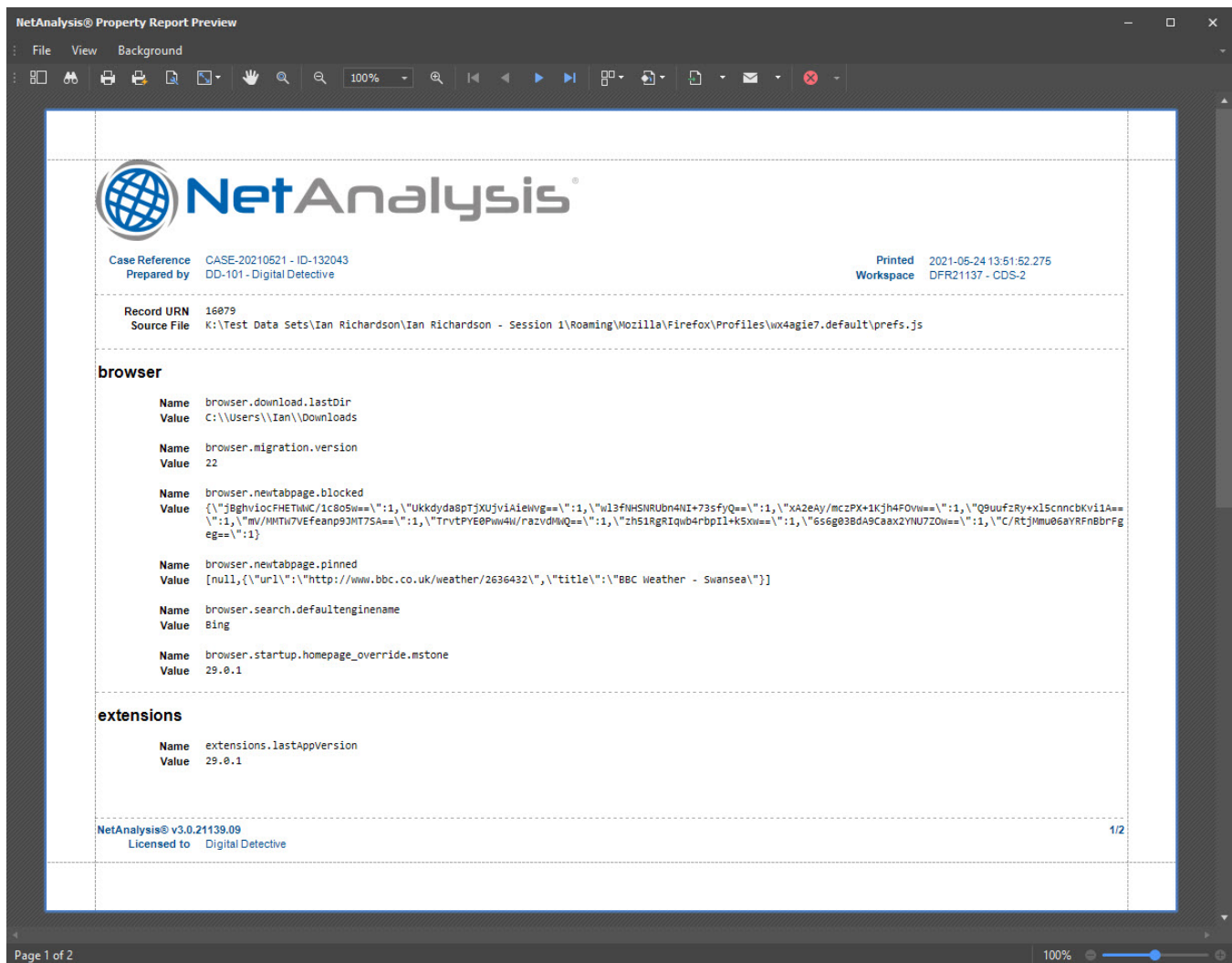
Progress Filtering

We have also enhanced the Progress Window with the same column filters. When processing data, it is now easy to filter rows containing a specific status. This makes it a simple process to review the log for warnings and other status values of interest.



New Properties Examiner

The **Properties Examiner** allows the user to view and perform detailed analysis on the various Preference values set by Mozilla and Chromium-based browsers. You can search, filter, group, sort and even print reports on the extensive property sets available. We have added support for saving and loading Property Filters to make it easier to identify items of interest. Various timestamp property values are automatically converted to Date/Time values and displayed in their own column. Property types are identified by a small icon before the Property Name.



Improved Search Index

The Search Index database is a powerful feature of NetAnalysis@ and has been enhanced in this release. It allows the user to rapidly search across the text extracted from the input data and identify key items of interest. We have updated the search syntax to include wild-card characters. The image below shows how to use a wild-card search to identify all email addresses in the search index:

Search Index

@**

Search

Clos

| URN | File Path | Hits | Score |
|-------|---|------|-------|
| 239 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000000239.txt | 1 | 1 |
| 241 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000000241.txt | 1 | 1 |
| 1463 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000001463.txt | 1 | 1 |
| 1483 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000001483.txt | 1 | 1 |
| 3317 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000003317.txt | 1 | 1 |
| 3413 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000003413.txt | 1 | 1 |
| 4630 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000004630.txt | 1 | 1 |
| 8467 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000008467.txt | 2 | 1 |
| 11111 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000011111.txt | 1 | 1 |
| 12208 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000012208.txt | 2 | 1 |
| 14224 | J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000014224.txt | 13 | 1 |

Record 2 of 121

Yeah man, what do you need?

Add me on Facebook - Ian Richardson

----- Original Message -----

From: Victor Bushell

Sent: 05/13/14 09:25 AM

To: ian.richardson@activist.com

Subject: Cardiff

Can you do some work for me in Cardiff. We met a week back & you were interested.

Let me know

J:\CASE-20210521\ID-132043\Mozilla Firefox\HTML to Text\F0000000241.txt

Document Search Hit: 1 of 1

Zone Identifier ADS

NetAnalysis® v3 now checks for Zone.Identifier Alternate Data Streams when processing files. When a file is downloaded, a Zone.Identifier ADS is created and can contain the source URL of the download. The Information panel will show the various metadata properties for the download.

NetAnalysis® v3.1 - Forensic Internet History Analysis - [Zone.Identifier]

FileViewToolsSearchFilterIndexReportsColumnWindowHelp

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

Decoded URL

https://github-releases.githubusercontent.com/46080325/222bab80-a5d0-11eb-9527-491a5b97e8e4?
X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A/20210524/us-east-1/s3/aws4_request
&X-Amz-Date=20210524T073326Z
&X-Amz-Expires=300
&X-Amz-Signature=7907877c6b99d425b21d1024d95e6d1787d2bfa169e996f4fe26fbf6142c2470
&X-Amz-SignedHeaders=host
&actor_id=0
&key_id=0
&repo_id=46080325

| Entry Type | Scheme | Date Visited [UTC] | Date Visited [Local] | Visits | URL |
|-----------------|--------|-------------------------|-------------------------|--------|--|
| Zone Identifier | https | 2021-05-25 10:56:29.761 | 2021-05-25 10:56:29.761 | | https://fra-zip-04.easynews.com/5d729f02xfjm9VnHlW_m2xD4b5JhuTDhc-8JoiqKL3Lu9cO76VE2FmvVPusIhhsdkvg0VqUJvIXVVVhWxgrVWBQ |
| Zone Identifier | https | 2021-05-25 10:56:34.312 | 2021-05-25 10:56:34.312 | | https://fra-zip-04.easynews.com/8fae4f71kMY7XfEtp6TEt2z7V3atl.ergy3p5_h8wcGsOYJ72L1z0fw9TTZJF3glIGtygrDE0P38hXkr_y3Iyv0eoNBv |
| Zone Identifier | https | 2021-05-25 10:56:38.881 | 2021-05-25 10:56:38.881 | | https://fra-zip-03.easynews.com/bc3e2c3ewBUuAizPyKw31bdu6UM-qqvqOQtdR0rvf8YQa-SNC0eAJCxx5w64j9uMcg56AkUYGD943Fbr69m8 |
| Zone Identifier | https | 2021-05-25 10:56:07.569 | 2021-05-25 10:56:07.569 | | https://fra-zip-03.easynews.com/8b084ef83WDTY4IGgYVJODMXiaJf2gvawz7xnthX6jab0XeGIGg50oQSQxchDA2SEhwYudRb7gIBfZr7mIzoUkE1 |
| Zone Identifier | https | 2021-05-25 10:56:13.145 | 2021-05-25 10:56:13.145 | | https://fra-zip-05.easynews.com/74067143bsaoTsClQ3gBHKRVE3NDIR-Zpet5YXAyXoHX1QtgjCAFS6_XUCfv0RF4q4wmEDWOAGF7Dl6FkpWjgp |
| Zone Identifier | https | 2021-05-24 09:53:41.851 | 2021-05-24 09:53:41.851 | | https://storage.googleapis.com/support-kms-prod/Y2dvjj4vUhx0iLqzWmhjplW3b38alWuW8L |
| Zone Identifier | https | 2021-05-24 08:33:53.065 | 2021-05-24 08:33:53.065 | | https://github-releases.githubusercontent.com/46080325/222bab80-a5d0-11eb-9527-491a5b97e8e4?X-Amz-Algorithm=AWS4-HMAC-SHA256 |
| Zone Identifier | https | 2021-05-24 08:33:27.845 | 2021-05-24 08:33:27.845 | | https://github-releases.githubusercontent.com/46080325/222bab80-a5d0-11eb-9527-491a5b97e8e4?X-Amz-Algorithm=AWS4-HMAC-SHA256 |
| Zone Identifier | https | 2021-02-12 09:13:33.538 | 2021-02-12 09:13:33.538 | | https://downloads.pwnedpasswords.com/passwords/pwned-passwords-sha1-ordered-by-hash-v7.7z |

Record 7 of 9

Tag = Checked

Edit Filter

Information

1File Information

2Name: win-acme.v2.1.17.1065.x64.pluggable(1).zip

3Location: D:\Downloads

4Date Created [UTC]: 2021-05-24 07:33:53.065

5Date Modified [UTC]: 2021-05-24 07:34:07.137

6Length: 31868672 (30.39 MB)

7

8Zone Transfer

9Zone ID: 3 (Internet)

10Length: 614 (0.60 KB)

www.digital-detective.net

D:\Downloads\win-acme.v2.1.17.1065.x64.pluggable(1).zip:Zone.Identifier:\$DATA

FO: 0

9

Change Log

To review the full list of changes for this release, please see: [Change Log v3.0](#).

Release Notes for HstEx® Version 5.0

Don't forget to review the release notes for HstEx® which can be found here: [HstEx v5.0 Release Notes](#).