

User Guide Version 2



NetAnalysis®

An evolution in browser forensic analysis

NetAnalysis® v2 User Guide



Copyright © 2001 - 2018 Digital Detective Group Ltd. All rights reserved worldwide.

Copyright, Legal Notice and Disclaimer

This publication is protected under the UK Copyright, Designs and Patents Act of 1988 and all other applicable international, federal, state and local laws, and all rights are reserved, including resale rights: you are not allowed to give or sell this manual to anyone else. The copyright, patents, trademarks and all other intellectual property rights in the software and related documentation are owned by and remain the property of Digital Detective Group or its suppliers and are protected by national laws and international treaty provisions.

Limit of Liability and Disclaimer of Warranty

The publisher has used its best efforts in preparing this manual and the information provided herein is provided as is. Digital Detective Group makes no representation or warranties with respect to the accuracy or completeness of the contents of this manual and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential, or other damages.

Trademarks

This manual identifies product names and services known to be trademarks, registered trademarks, or service marks of their respective holders. They are used throughout this document in an editorial fashion only. In addition, terms suspected of being trademarks, registered trademarks, or service marks have been appropriately capitalised, although Digital Detective Group cannot attest to the accuracy of this information. Use of a term in this manual should not be regarded as affecting the validity of any trademark, registered trademark or service mark. Digital Detective Group is not associated with any product or vendor mentioned in this manual. NetAnalysis®, HstEx® and Digital Detective® are registered trademarks belonging to the Digital Detective Group.

Sharing this Document

No part of this document or the related files may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without the prior written permission of the publisher.

Digital Detective Group Limited

Discovery Park • Innovation House • Innovation Way • Sandwich • Kent • CT13 9FF • United Kingdom

Web: <http://www.digital-detective.net>

Phone: +44 (0) 20 3384 3587

Table of Contents

Document Revision Information	10
Version History.....	10
Getting Help	11
Knowledge Base	11
Support Portal.....	11
Software Release Notes	11
Introduction.....	12
Overview	12
Our Focus.....	12
Introduction to NetAnalysis®	13
NetAnalysis® Supported Browsers.....	14
Supported Browser by Version.....	14
Installing NetAnalysis®	21
Introduction	21
Operating System Requirements.....	21
Operating System	21
Additional Requirements.....	21
Latest Release.....	22
Verification of Digital Signature	22
Running Setup	22
End User Licence Agreement	24
USB Hardware Dongles.....	29
Introduction	29
Installation and Use.....	29
Troubleshooting.....	30
Updating your USB Dongle	31
Download the Licence Manager	32
Performing a Dongle Update.....	32
Practice Files	34
Sample Data.....	34
NetAnalysis® - A Guided Tour	35

Introduction	35
Tab Groups.....	36
Split Windows	36
Arranging and Docking Windows.....	37
Closing and Auto-Hiding Windows	37
Specifying a Monitor.....	37
Reset, Name and Switch Between Window Layouts.....	38
Create and Save Custom Layouts	38
Main Toolbar	38
Status Bar.....	41
Main Menu.....	42
Columns	47
Entry Type.....	55
Docking Panels	61
Navigating Through Rows and Cells.....	71
Resizing Columns.....	71
Selecting Rows.....	72
Expanding and Collapsing Group Rows in Grid Views.....	73
Sorting	74
Grouping.....	75
Ungroup Data.....	76
Change Grouping Order	77
Time Zone Configuration	78
Introduction	78
Date/Time Values.....	78
Universal Coordinated Time	78
Daylight Saving and Standard Time.....	79
How NetAnalysis® Deals with Time Zones.....	79
New Case Import Options.....	79
Identification of Source Time Zone.....	82
Control Sets.....	82
Time Zone Information Sub-Key.....	84
Dynamic DST	88
SYSTEMTIME Structure.....	89
Calculating Signed Integer Bias Values.....	90
Two's Complement.....	90
ActiveTimeBias.....	92
Bias Calculations.....	93
Returning Daylight and Standard Name Values.....	94
NetAnalysis® Active Time Bias Column.....	95
Time Zone Warnings.....	96
Dealing with Data from Mixed Time Zones.....	99

Encoding Configuration	100
Introduction	100
ASCII	100
Extended ASCII.....	101
Unicode.....	101
Codepoint.....	102
UTF-8, UTF-16 and UTF-32	103
Browser Data	103
NetAnalysis® Quick Start	104
Introduction	104
Creating a New Case.....	104
Import Options	105
Time Zone.....	106
Code Page	106
Importing Data.....	107
Reviewing the Imported Data	109
Docking Panel Layout.....	109
Quick Search.....	110
URL Examination and Analysis.....	111
Cookie Examination and Analysis	111
Saving Your Workspace	114
Filtering and Searching	115
Introduction	115
Filtering	115
Create a Simple Filter Condition	115
Create Complex Filter Criteria	116
Clearing a Filter.....	117
Disable/Enable a Filter.....	117
Invoke the Filter Dropdown List	118
Filter Editor.....	118
Add Conditions.....	120
Delete Conditions	120
Change a Column in a Filter Condition.....	121
Change an Operator in a Filter Condition.....	121
Edit a Condition's Value.....	121
Navigation	121
Launching the Filter Editor.....	122
Filter Editor - Building Filter Criteria	123
Constructing Simple Filter Conditions.....	123
Constructing Complex Filters with Logical Operators.....	130
Constructing Filters with Multiple Logical Operators.....	134

Locating Rows Using Search (Find) Panel	140
Open the Find Panel.....	140
Closing the Find Panel.....	141
Auto Filter Row	141
Opening the Auto Filter Row.....	142
Closing the Auto Filter Row	142
Showing All Records	142
Web Page Rebuilding	143
Introduction	143
Exporting the Cache.....	143
Page Rebuild Audit Log	146
Web Page Text Content.....	148
Export Folder.....	148
Built-In Viewer.....	150
Indexing and Searching	152
Introduction	152
Data Types Added to the Search Index	152
Creating a Search Index.....	153
How to Search.....	155
Search Index Columns.....	157
Identifying the Original Source.....	158
Viewing the Indexed Document.....	159
Saving the Indexed Document.....	159
Adding a Bookmark to the Original Source	160
Query Parser Syntax.....	160
Wildcard Searches.....	161
Fuzzy Searches.....	161
Proximity Searches.....	162
Boosting a Term	162
Boolean Operators.....	163
AND.....	163
+	164
NOT	164
-	164
Grouping.....	164
Escaping Special Characters	165
Reporting.....	166
Introduction	166
Preview Detailed Report	166
Report Preview Window	167

Working with a Report Preview Selection.....	169
Report Designer.....	171
Creating a New User Defined Report	171
Report Designer Window Layout.....	172
Designing a Report.....	174
Data Grouping and Sorting	182
Preview, Printing and Exporting	183
Exporting.....	184
Introduction	184
Setting Visible Columns.....	185
Filtering Records.....	186
Exporting to CSV (Comma Separated Values)	186
Exporting to TSV (Tab Separated Values)	186
Exporting to SQLite Database	186
Exporting to TLN Timeline Format	186
Exporting to a NetAnalysis® Workspace.....	187
Database	188
Introduction	188
Creating a New Server Based Case.....	189
Opening a Server Based Case	191
HstEx®	194
Introduction	194
HstEx® v4.....	195
Deleted Data Recovery.....	196
Introduction	196
Data Carving	196
Supported Source Data Formats.....	198
Understanding Data Recovery	199
Intelli-Carve®	199
Recommended Methodology.....	200
HstEx® Supported Browsers	201
Apple Safari v3 - 11	201
Google Chrome v1 - 65.....	201
Microsoft Internet Explorer v5 - 9.....	202
Microsoft Internet Explorer v10 - 11.....	202
Microsoft Internet Explorer XBOX.....	202
Microsoft Edge v20 - 41.....	202
Mozilla Firefox v1 - 59	202

Opera v4 - 12.....	203
Opera v15 - 51.....	203
360 Browser v7.....	203
360 Security Browser v6 - 9.....	204
360 Speed Browser v4 - 9.....	204
AOL Desktop Browser v9.....	204
Blisk v0 - 8.....	205
Brave v0 - 1.....	205
Comodo Chromodo v36 - 52.....	205
Comodo Dragon v4 - 60.....	206
Comodo Ice Dragon v13 - 57.....	206
CoolNovo v1 - 2.....	206
Cyberfox v17 - 52.....	207
Flock v2.....	207
Flock v3.....	207
IceCat v1 - 52.....	207
K-Meleon v1 - 76.....	208
Netscape v6 - 9.....	208
Opera Neon v1.....	208
Pale Moon v3 - 27.....	208
SeaMonkey v1 - 2.....	209
Sleipnir (Windows) v3 - 6.....	209
Sleipnir (OS X) v3 - 4.....	210
SRWare Iron v1 - 64.....	210
Titan Browser v1 - 33.....	210
Torch v1 - 55.....	211
UC Browser v4 - 7.....	211
Vivaldi v1.....	211
Waterfox v4 - 56.....	212
Wyzo v3.....	212
Yandex v1 - 18.....	212
Other Chromium Based Browsers.....	213
Other Mozilla Based Browsers.....	213
Installing HstEx®	214
Introduction.....	214
Operating System Requirements.....	214
Operating System.....	214
Additional Requirements.....	214
Latest Release.....	215
Verification of Digital Signature.....	215
Running Setup.....	215
End User Licence Agreement.....	217

HstEx® - A Guided Tour.....	222
Introduction	222
Main Toolbar	223
Recovery Job Window	225
Recovery Job Main Toolbar	227
Physical/Logical Devices Window.....	228
Options Window	228
File Extensions.....	230
HstEx® Recovery File (*.hstx).....	230
 HstEx® Quick Start.....	 232
Introduction	232
Recovery Sessions.....	232
Creating a New Session	232
Adding a Recovery Job.....	233
Opening an Existing Session	236
Running the Recovery	237
Importing HstEx® Recovery Files into NetAnalysis®	239
 Technical Support.....	 240
Introduction	240
Identifying Software Version	240
Submitting an Issue Report	241
Background Information.....	242
Change Log and Version History	242
Audit and Error Logs	243
Submitting a Request	243
 List of References	 244
Reference Index.....	244
 Appendix A	 245
NetAnalysis® Keyboard Shortcuts.....	245
 Appendix B.....	 247
HstEx® Keyboard Shortcuts.....	247
 Appendix C.....	 248
Extended ASCII Table.....	248

Document Revision Information

Version History

The release history for this document is shown in Table 1 below. For ease of comparison, the NetAnalysis® and HstEx® major version numbers are also shown.

NetAnalysis®	HstEx®	Date	Comments
2.5	4.5	2016-11-16	First release as single PDF document
2.6	4.6	2017-06-13	Changes relating to this software release
2.7	4.7	2018-02-06	Changes relating to this software release
2.8	4.8	2018-04-19	Changes relating to this software release

Table 1

Getting Help

Knowledge Base

The Digital Detective Knowledge Base should be the first port of call for up to date information in relation to our software:

<http://kb.digital-detective.net>

Support Portal

If you cannot find the answer to your question within the pages of this document or our knowledge base, or if you need assistance in using our software, please feel free to open a support ticket at our support portal (please see the chapter on obtaining Technical Support on Page 240):

<http://support.digital-detective.net>

Software Release Notes

The software version history and release notes can be found in our knowledge base at the following location:

NetAnalysis® Documentation

<http://kb.digital-detective.net/x/VoCI>

HstEx® Documentation

<http://kb.digital-detective.net/x/AgCQ>

Introduction

Overview

The forensic examination of digital devices in support of law enforcement and civil investigations is a critical part of the evidence collection process. Almost every crime investigated by law enforcement has an electronic evidence aspect. Over the last two decades, the Internet has consolidated itself as a powerful platform that has changed the way we do business, and the way we communicate.

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease and range with which transactions can be conducted, whilst also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography and paedophile rings, but also drug trafficking and criminal organisations that are more intent upon exploitation than the disruption that is the focus of the hacking community.

Our Focus

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.

Introduction to NetAnalysis®

Through a significant investment in research and development, we have authored a completely new ground-breaking 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 browsing and user activity on computer systems and mobile devices. It is a software product that offers significant improvements over existing applications and methodologies.

To see a full breakdown of the new features, please see the following knowledge base page:

[*http://kb.digital-detective.net/x/QAC*](http://kb.digital-detective.net/x/QAC)

NetAnalysis® Supported Browsers



Supported Browser by Version

The following table lists the currently supported browsers. Whilst newer browsers may work, this is the current list of browsers which have been tested against.

NetAnalysis® Supported Web 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. It was first released in September 2008. 360 Browser is based on the Chromium source code.



360 Secure/Security Browser v3 - 9

360 Secure/Security Browser (360安全浏览器) 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. It was first released in September 2008.



360 Speed (Extreme) Browser v4 - 9

This is another browser by the Qihoo 360 Software Company. 360 Speed (or Extreme Explorer) Browser is a fast, secure, seamless dual-core web browser. Claiming to be the world's first seamless Chrome and Internet Explorer browser, with an innovative UI design, HTML5 and CSS3 support standardisation.



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).



Apple Safari v3 - 11

Safari is a web browser developed by Apple and is included with the Mac OS X and iOS operating systems. It is based on the WebKit engine and was first released in 2003 with Mac OS X Panther.



Blisk 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.



Brave v0 - 1

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.



Comodo Chromodo v36 - 52

Comodo Chromodo is a Chromium technology-based browser that offers all of Chrome's features plus a claimed increase in speed, security and privacy.



Comodo Dragon v4 - 60

Comodo Dragon is a freeware web browser produced by Comodo Group. Sporting a similar interface to Google Chrome, Dragon does not implement Chrome's user tracking and some other potentially privacy-compromising features, and provides additional security measures, such as indicating the authenticity and relative strength of a website's SSL certificate.



Comodo IceDragon v13 - 57

Comodo IceDragon is an open source web browser from the Comodo Group. It is intended to be faster and more secure than Firefox.



CoolNovo v1 - 2

CoolNovo was a freeware Chromium based web browser developed by Maple Studio based in China. The browser was originally called ChromePlus. It offers page layout using either the Trident engine, as used in Internet Explorer, or the WebKit engine that was adapted for Google Chrome.



Cyberfox v17 - 52

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 optimised for Intel based CPUs, and one optimised for AMD based CPUs. It is also available in x86 versions. Cyberfox is also available for 64bit Linux.



Flock v0 - 3

Flock was a web browser that specialised in providing social networking and Web 2.0 facilities built into its user interface. Earlier versions of Flock used the Gecko HTML rendering engine by Mozilla. Version 2.6.2, released on 27th January, 2011, was the last version based on Mozilla Firefox. Starting with version 3, Flock used the WebKit rendering engine.



Google Chrome v0 - 65

Google Chrome is a freeware web browser developed by Google. It used the WebKit layout engine until version 27 and, with the exception of its iOS releases; from version 28 and beyond uses the WebKit fork Blink.



IceCat v1 - 52

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 on GNU/Linux, Windows, macOS and Android.



K-Meleon v1 - 76

K-Meleon is an open-source web browser for the Microsoft Windows platform. Based on the same Gecko layout engine as Mozilla Firefox and SeaMonkey, K-Meleon's design goal is to provide a fast and reliable web browser while providing a highly customisable interface and using system resources efficiently.



Microsoft Internet Explorer v3 - 11

Internet Explorer (formerly Microsoft Internet Explorer and Windows Internet Explorer, commonly abbreviated IE or MSIE) is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems. It was first released in 1995.



Microsoft Edge v20 - 41

Microsoft Edge (previously codenamed Project Spartan) is the new minimalistic browser specifically designed for Windows 10, Windows 10 mobile and Xbox One. It replaces Internet Explorer as the default web browser on all device classes. Edge Apps have also been released for iOS and Android devices.



Microsoft Internet Explorer Xbox

Microsoft Internet Explorer is available as an app for the Xbox. It was released in October 2012.



Mozilla Firefox v1 - 59

Mozilla Firefox is a free and open-source web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation. Firefox is available for Windows, macOS and Linux operating systems, with its Firefox for Android available for Android (formerly Firefox for mobile, it also ran on the discontinued Firefox OS); where all of these versions use the Gecko layout engine to render web pages, which implements current and anticipated web standards.



Netscape v6 - 9

Netscape Browser is the name of a proprietary Windows web browser published by AOL but developed by Mercurial Communications.



Opera (Presto) v3 - 12

Opera was a web browser developed by Opera Software. Presto was the layout engine of the Opera web browser for a decade. It was released on 28th January 2003 in Opera 7 for Windows; Opera continued to use Presto until version 15, at which point the browser was rewritten containing the Blink layout engine.



Opera v15 - 51

Opera is a web browser developed by Opera Software. The latest version is available for Microsoft Windows, OS X, and Linux operating systems, and uses the Blink layout engine. According to Opera Software, the browser had more than 350 million users worldwide in the fourth quarter of 2014. Total Opera mobile users reached 291 million in June 2015.



Opera Neon v1

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.



Pale Moon v3 - 27

Pale Moon is a free and open-source web browser available for Microsoft Windows, Linux and Android, focusing on efficiency and ease of use. It is developed and distributed by Dutch developer M.C. Straver.



SeaMonkey v1 - 2

SeaMonkey is a free and open-source Internet suite. It is the continuation of the former Mozilla Application Suite, based on the same source code.



Sleipnir (Windows) v3 - 6

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 a proprietary text rendering visually resembling Mac OS text rendering.



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 Mac version uses the WebKit layout engine.



SRWare Iron v1 - 64

SRWare Iron is a freeware web browser by SRWare of Germany. It primarily aims to eliminate usage tracking and other privacy-compromising functionality that the Google Chrome browser includes. While Iron does not provide extra privacy compared to Chromium after proper settings are altered in the latter, it does implement some additional features that distinguish it from Google Chrome, such as built-in ad blocking.



Torch v1 - 55

Torch is a free ad-supported, Chromium-based web browser and Internet suite developed by Torch Media. The browser handles common Internet-related tasks such as displaying websites, sharing websites via social networks, downloading torrents, accelerating downloads and grabbing online media, all directly from the browser. Torch Browser is commercial freeware.



Titan 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. Titan Browser is commercial freeware and is based on the Chromium source code.



UC Browser v4 - 7

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.



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.



Waterfox v4 - 56

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.



Wyzo v0 - 3

Wyzo is a web browser based on Mozilla Firefox by Radical Software Ltd. It has built-in BitTorrent capabilities and download acceleration.



Yandex v1 - 18

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.



Chromium Based Browsers

Chromium Based Browsers are based on the Chromium source code. Google Chrome is based on the open-source Chromium browser project. Anyone can take Chromium's source code and modify it to build their own browser. These browsers all build on the core browser and offer unique twists on Chrome.

Each alternative browser has its own focus, whether it is security, social networking, privacy, additional features, or portability.



Mozilla Based Browsers

Mozilla Based Browsers are based on the Mozilla Firefox source code. Mozilla Firefox is an open-source web browser, so anyone can take the source code and modify it. Various projects have taken Firefox and released their own versions, either to optimise it, add new features, or align it with their own philosophy.

Table 2

Installing NetAnalysis®

Introduction

The following procedure will guide you through installing NetAnalysis® for the first time. Please ensure that you close all other applications before starting.

Operating System Requirements

Our software has been designed to run on a Microsoft® Windows® x86/x64 platform. Please note, the following list represents the platforms which have been tested. The software may run on other platforms not listed below.

Operating System

The following Operating System versions are supported:

- Windows 10
- Windows 8
- Windows 7
- Windows Vista SP1 or later
- Windows Server 2008 (Server Core not supported)
- Windows Server 2008 R2 (Server Core not supported)

Additional Requirements

The Operating System must have the following .NET framework runtime installed:

- Microsoft .NET Framework v4

Latest Release

Prior to installing NetAnalysis®, please ensure you have obtained the latest release. There is on-going product research and development which provides new features, important updates and bug fixes. Please check the change log for details of those changes.

The release history and change log can be found here:

[*http://kb.digital-detective.net/x/VoCI*](http://kb.digital-detective.net/x/VoCI)

Verification of Digital Signature

Software vendors can digitally sign and timestamp the software they distribute. The code signing process ensures the end user knows the digitally signed software is legitimate, comes from a known software vendor and the code has not been tampered with since being published. If the Authenticode Digital Signature is not valid, or the MD5 hash provided at the point of download does not match, please do not install the software.

All the software products published by Digital Detective have been digitally signed. This ensures that when you use our software, you can verify that it has not been tampered with and is a product developed and released by Digital Detective Group. The following knowledge base article explains this further and shows you how to verify the integrity of forensic grade software:

[*http://kb.digital-detective.net/x/u4EU*](http://kb.digital-detective.net/x/u4EU)

Running Setup

Now that you have verified the integrity of the setup file (all the individual executables have also been digitally signed) you can install the software. You will note that each release has been named using the version/build information (see Figure 1).



Name	Date modified	Type	Size
 HstEx-x86-EN-4.5.16321.4.exe	2016-11-16 17:01	Application	14,407 KB
 NetAnalysis-x86-EN-2.5.16321.10.exe	2016-11-16 16:56	Application	48,416 KB

Figure 1

Good forensic practice dictates that you archive each release of a software application that you use on a forensic case. This ensures that at any time in the future, you can install a specific version and replicate your results.

When you run the application setup, Windows should prompt you for permission to install the software (see Figure 2).

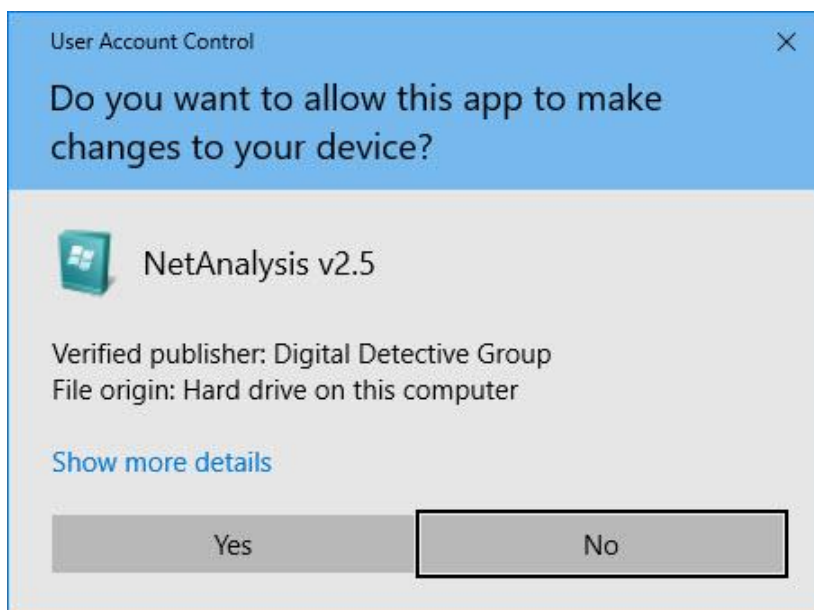


Figure 2

At this point, please ensure the prompt indicates that the publisher is Digital Detective Group and that it is verified.

Click **Yes** and move onto the next stage.

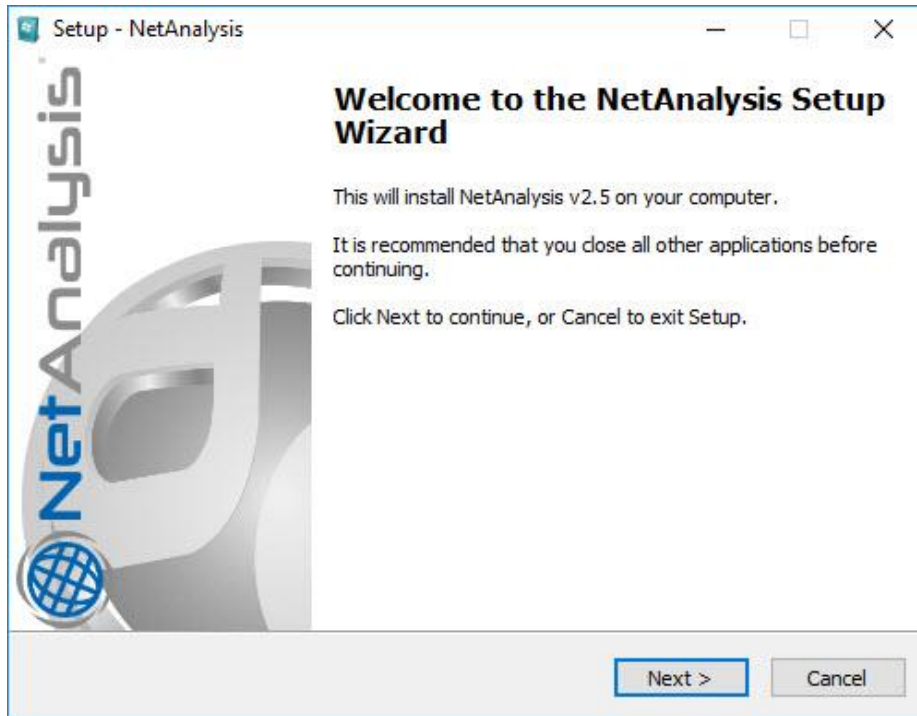


Figure 3

Please ensure that you close any other applications you may have running to prevent them interfering with the setup process.

End User Licence Agreement

The next screen (Figure 4) displays the End User Licence Agreement. Please read this carefully. If you wish to review or print a copy of this agreement, it can be found in our knowledge base at the following link:

<http://kb.digital-detective.net/x/fIUU>

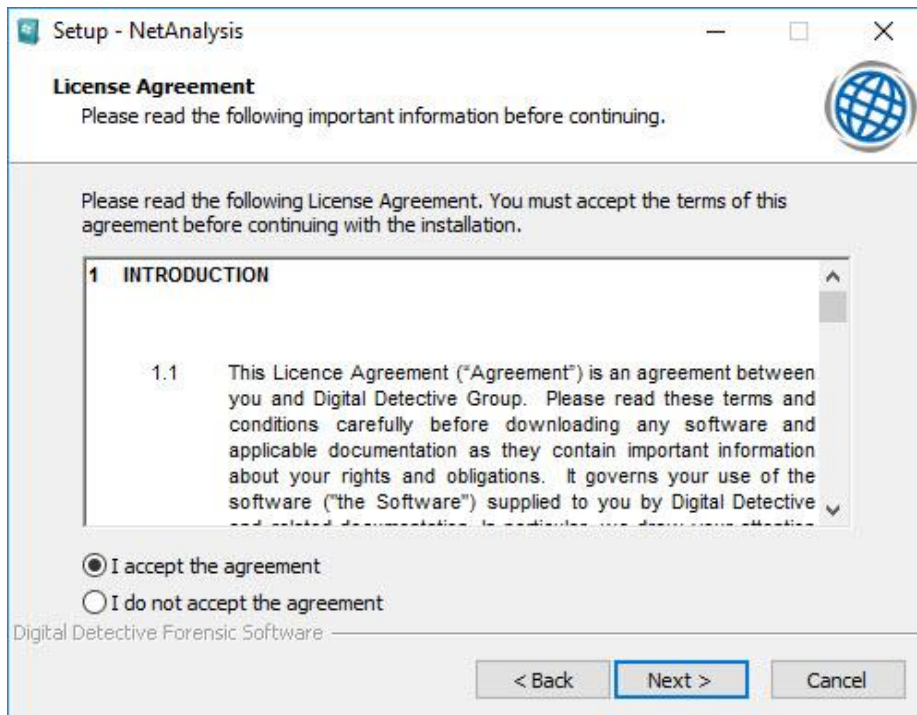


Figure 4

Click the option to accept the licence agreement and then click **Next** to move onto the next stage.

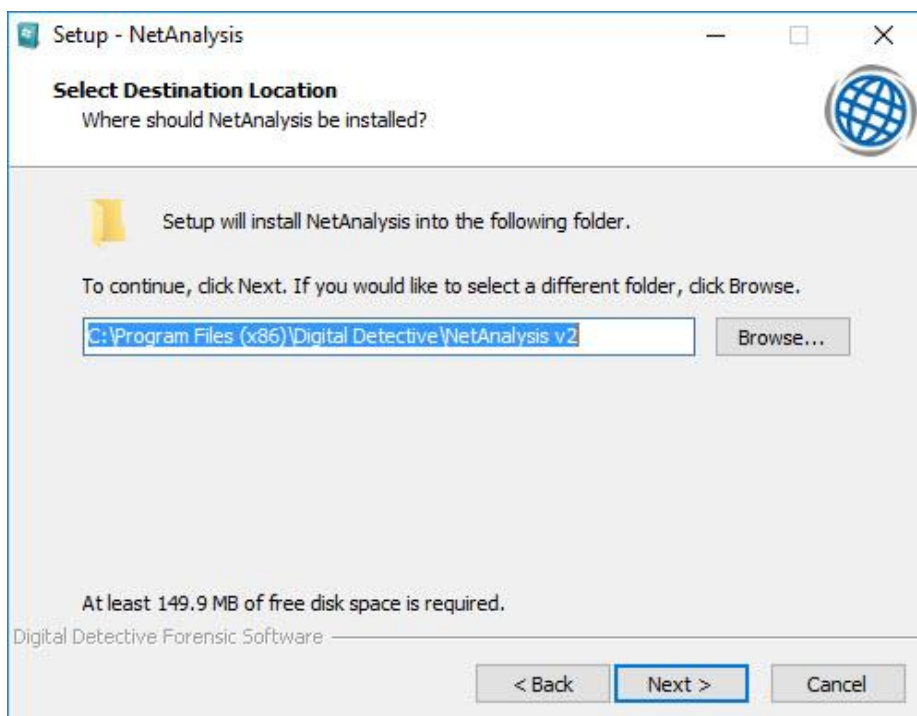


Figure 5

This window (Figure 5) allows you to configure the destination folder where the software will be installed. If this window does not appear, it means the software is already installed. In this case, the setup will use the previously selected values. Click **Next** to continue.

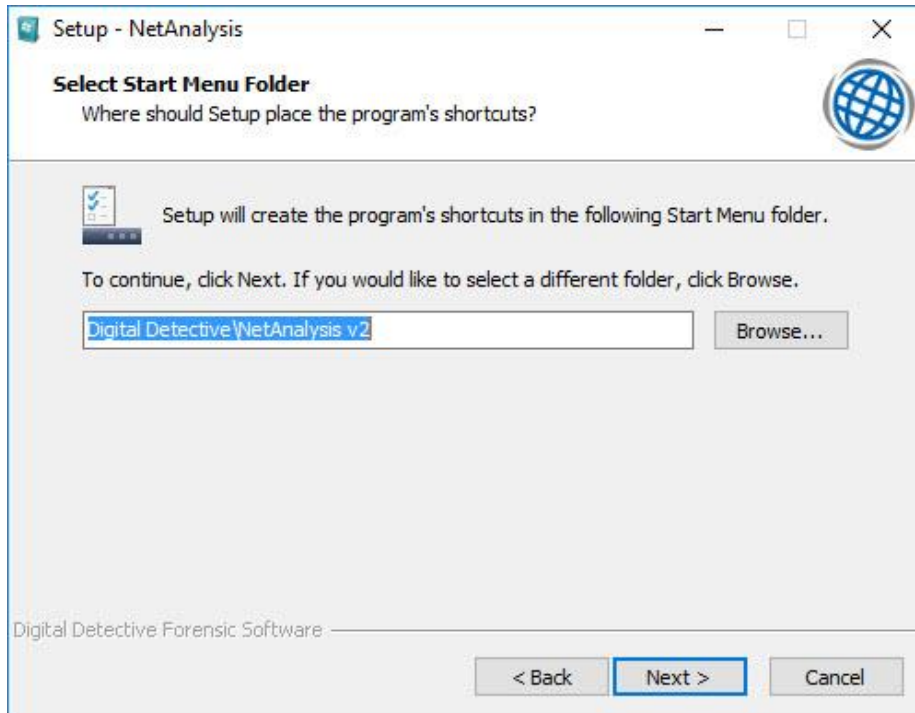


Figure 6

This window (Figure 6) allows you to configure the Start Menu folder. As with the previous window, if this option does not appear, it is because the software is already installed.

Click **Next** to continue.

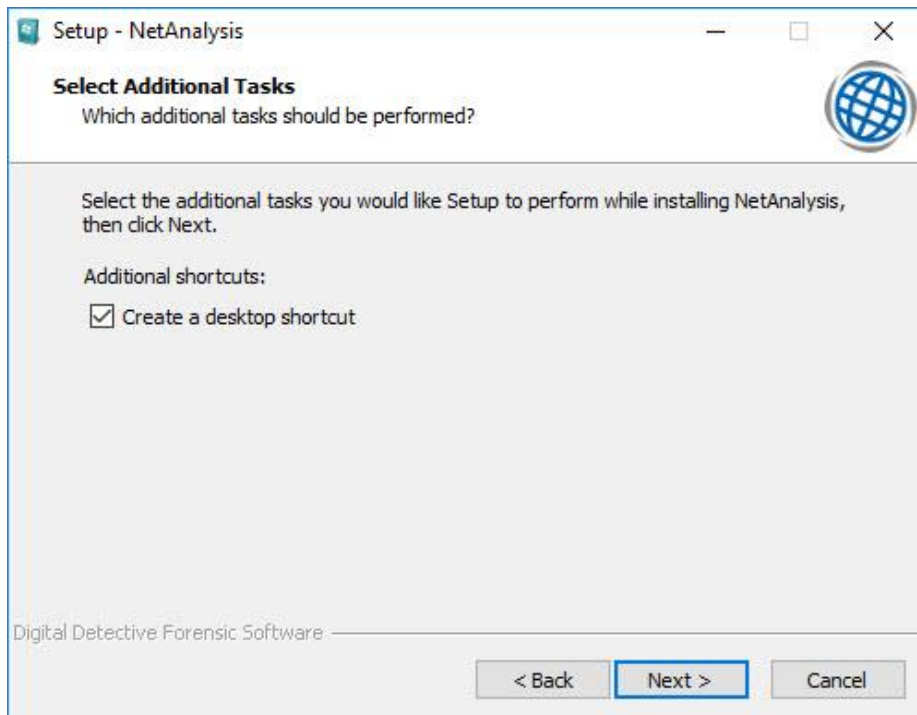


Figure 7

If you want the setup to create a desktop icon for you, select the option as shown in Figure 7. Click **Next** to continue.

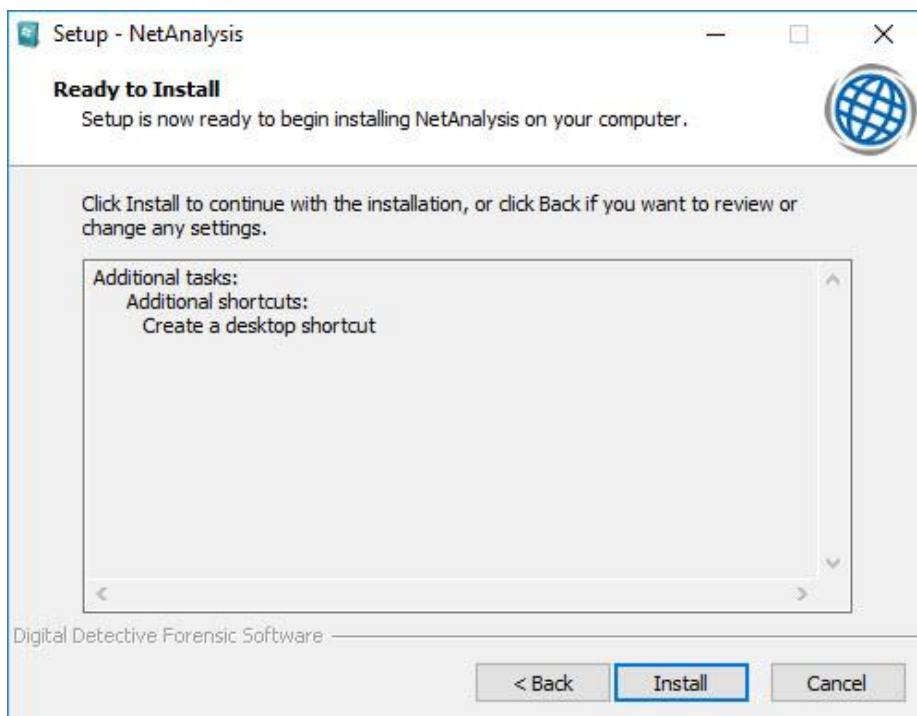


Figure 8

The next window (Figure 8) shows a summary of the installation tasks prior to launching the final installation process. If you are ready to continue, click the **Install** button.

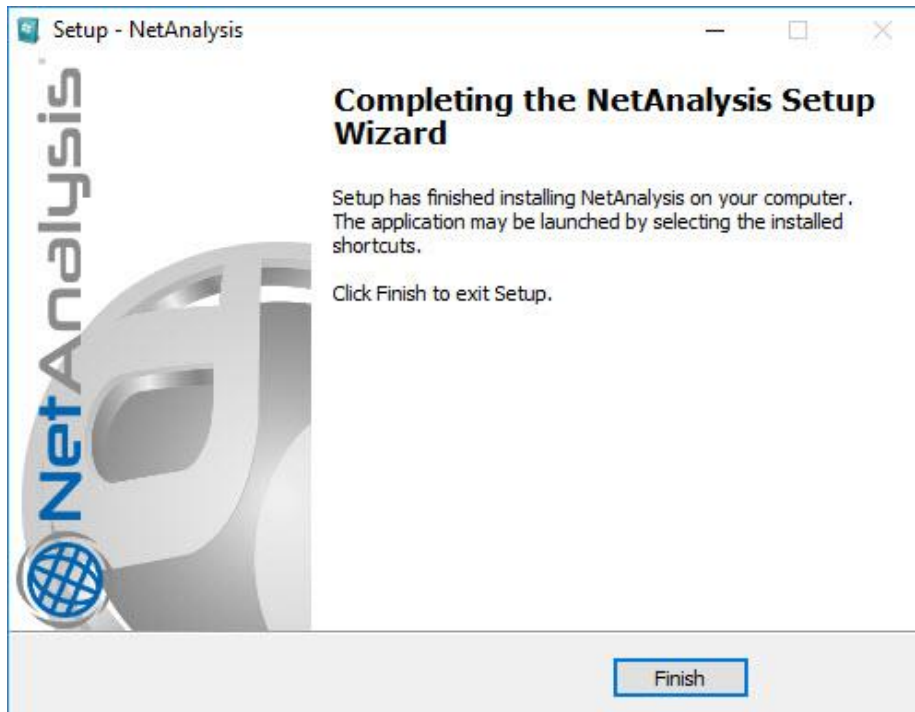


Figure 9

The final window (Figure 9) shows that the setup wizard has completed. Click **Finish** to close the Setup Wizard.

USB Hardware Dongles

Introduction

The USB hardware licence dongle (as shown in Figure 10) is a small hardware device that plugs into a USB port on a host computer to provide licence information to our software.



Figure 10

Our dongles are based on an advanced microprocessor smart chip which has been certified by EAL4+ and ITSEC.

Installation and Use

The dongle registers with the operating system as an HID (Human Interface Device). The generic HID drivers will be installed when the dongle is first inserted. As they require no external device driver during installation, this minimises the common technical issues which surround the use of hardware licences.

Once the HID device driver has been registered, simply inserting the USB dongle into a spare USB port prior to launching the application will allow the software to launch in a registered state.

Troubleshooting

If the software is unable to detect that a valid USB licence dongle is inserted, please check the following:

1. Make sure your USB dongle is inserted directly into a USB slot connected to the main system motherboard. Do not plug the dongle into a USB hub or a USB extension cable. Sometimes if the voltage is low, the USB device may not work correctly.
2. Test the USB dongle on another system to ensure the issue is not computer related.
3. Run the Digital Detective Licence Manager and check if the device is visible in the **Installed Licences** column.
4. When the USB dongle is inserted, does the on-board LED light continuously? If it does not light at all there may be a problem with the device. If it flashes, please try inserting the device into another USB slot.
5. In Windows 7, open **Devices and Printers** and verify that the USB dongle is visible as an HID Dongle as shown in Figure 11.



Figure 11

6. In Windows 10, open **Bluetooth & Other Devices** and look for an HID Dongle as shown in Figure 12.

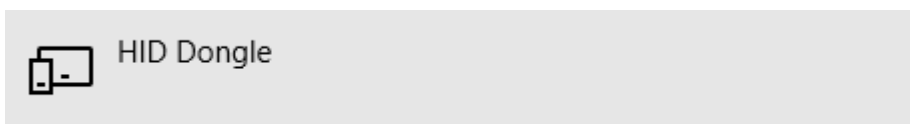


Figure 12

If the device is still not working, please contact support for further advice. You will need to provide the Dongle ID and Serial Number.

Updating your USB Dongle

The Licence Manager application has been designed to help you review and manage the software licence subscriptions held on Digital Detective licence dongles. It also allows us to remotely update your licence subscriptions so you can work with the latest versions of our software.

To update a USB licence dongle, all you will need is a computer running Microsoft Windows XP or later, the Licence Manager software and an Internet connection.

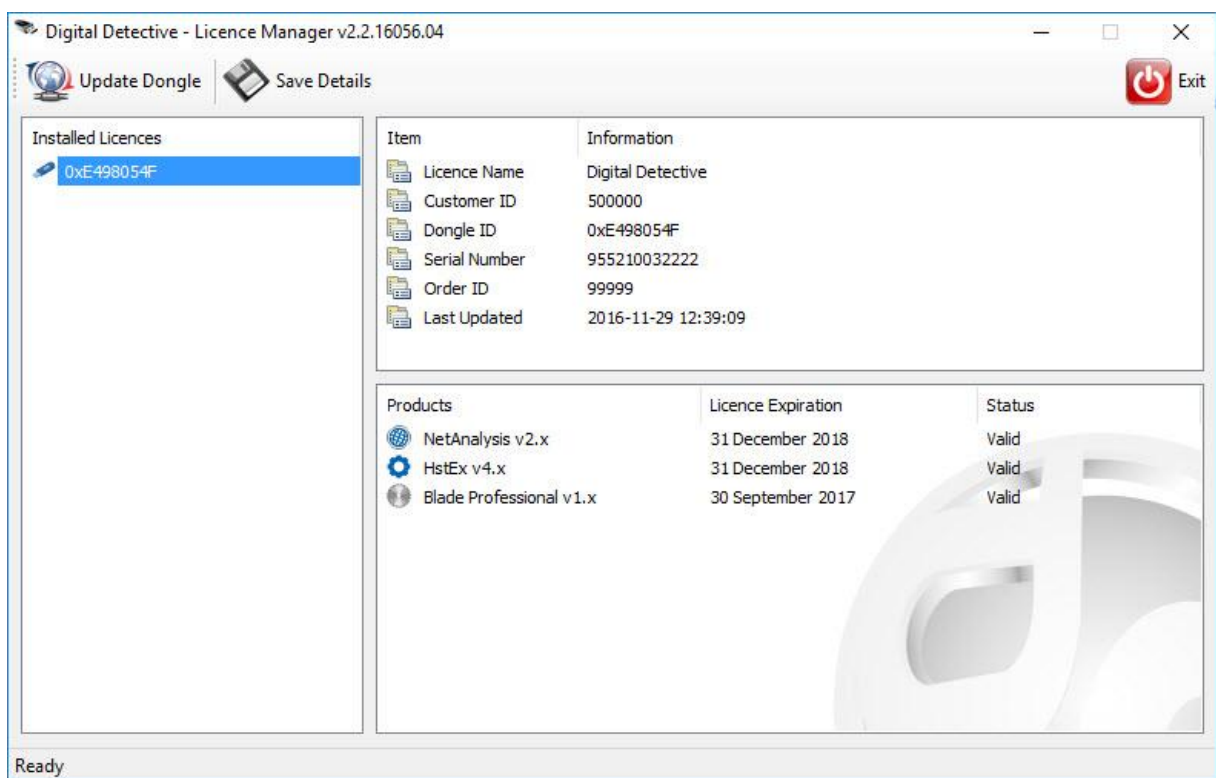


Figure 13

Each dongle is uniquely identified by an electronic ID number (Dongle ID) which is hard coded into the device, and a serial number which is etched on to the outside of the device (or displayed on a barcoded label). The Licence Manager can be used to review the licence information stored on the dongle and will also allow you to copy this information to the clipboard if required. You can also save the details for any inserted dongle(s) to a text file.

The Dongle ID can be seen highlighted in the **Installed Licences** column in Figure 13 above.

Download the Licence Manager

Please visit the following link to obtain the latest version of the Licence Manager software:

<http://kb.digital-detective.net/x/DYU9>

Performing a Dongle Update

The process of updating a USB licence dongle is relatively quick and easy. The Licence Manager software can securely connect to our Remote Licence Server and obtain the information it needs to update your dongle with the latest licence information.



Note: The Licence Manager requires an Internet connection to communicate to our Remote Licence Server. The update only takes a few seconds.



WARNING: It is extremely important that during the update process the dongle is not removed and that the system power remains on. If these instructions are not adhered to, there is a likelihood that the device will be permanently damaged!

The process is as follows:

1. Install and run the Licence Manager software;
2. Insert the USB licence dongle you wish to update;
3. When the dongle appears in the list, click and select the dongle you wish to update;
4. Click the **Update Dongle** button.

Only one USB dongle can be updated at a time. If you have multiple dongles inserted, you will need to carry out the above process for each dongle you wish to update.

When the **Update Dongle** button is pressed, the Licence Manager will contact the Licence Server as shown in Figure 14.

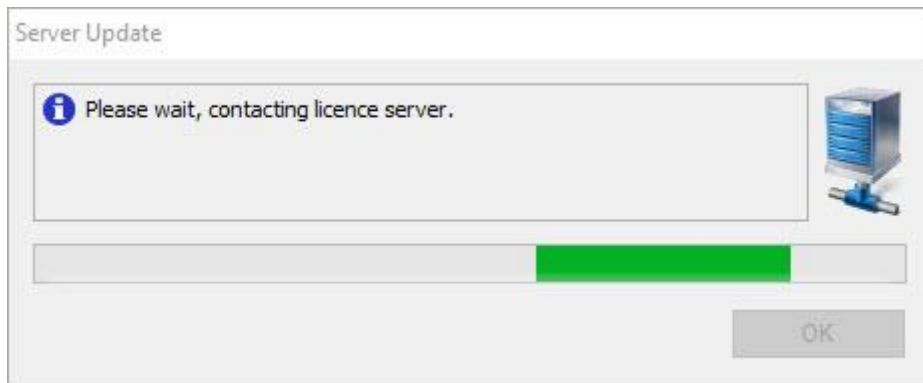


Figure 14

Once the dongle has been successfully updated, you will see a message displayed as show in Figure 15.

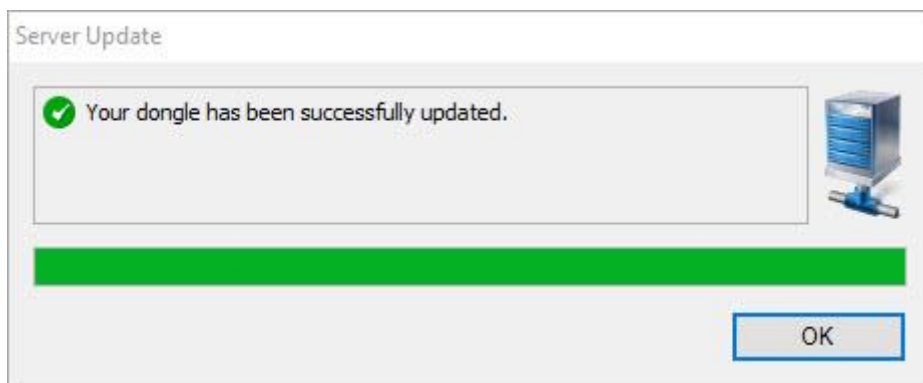


Figure 15

If you receive an error message stating your dongle cannot be found in the system and you were expecting a licence update, please contact support.

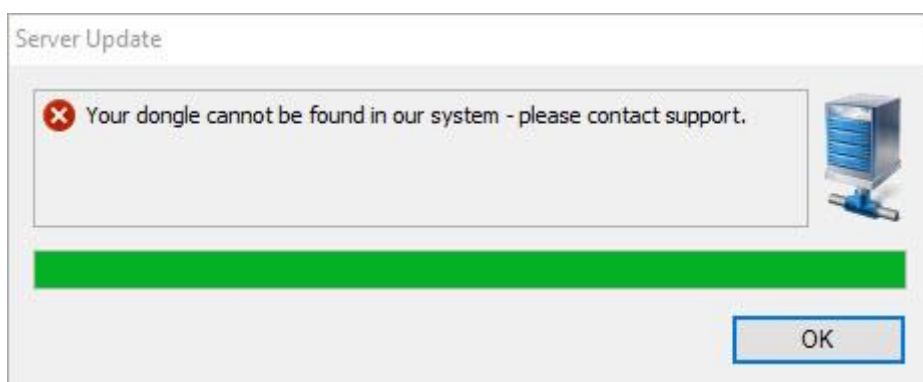


Figure 16

Practice Files

Sample Data

To assist you in getting to know the NetAnalysis® user interface, and to practise using the software in a safe learning environment, we have provided some sample data. Working through the examples will help you become familiar with using our software effectively within a forensic environment.

To access and download the sample data, please visit:

<http://kb.digital-detective.net/x/LQCX>

NetAnalysis® - A Guided Tour

Introduction

To get the most from the software it is important to understand the user interface and know what each feature does. In this chapter, we will take a brief look at the main components of the user interface and describe how they work.

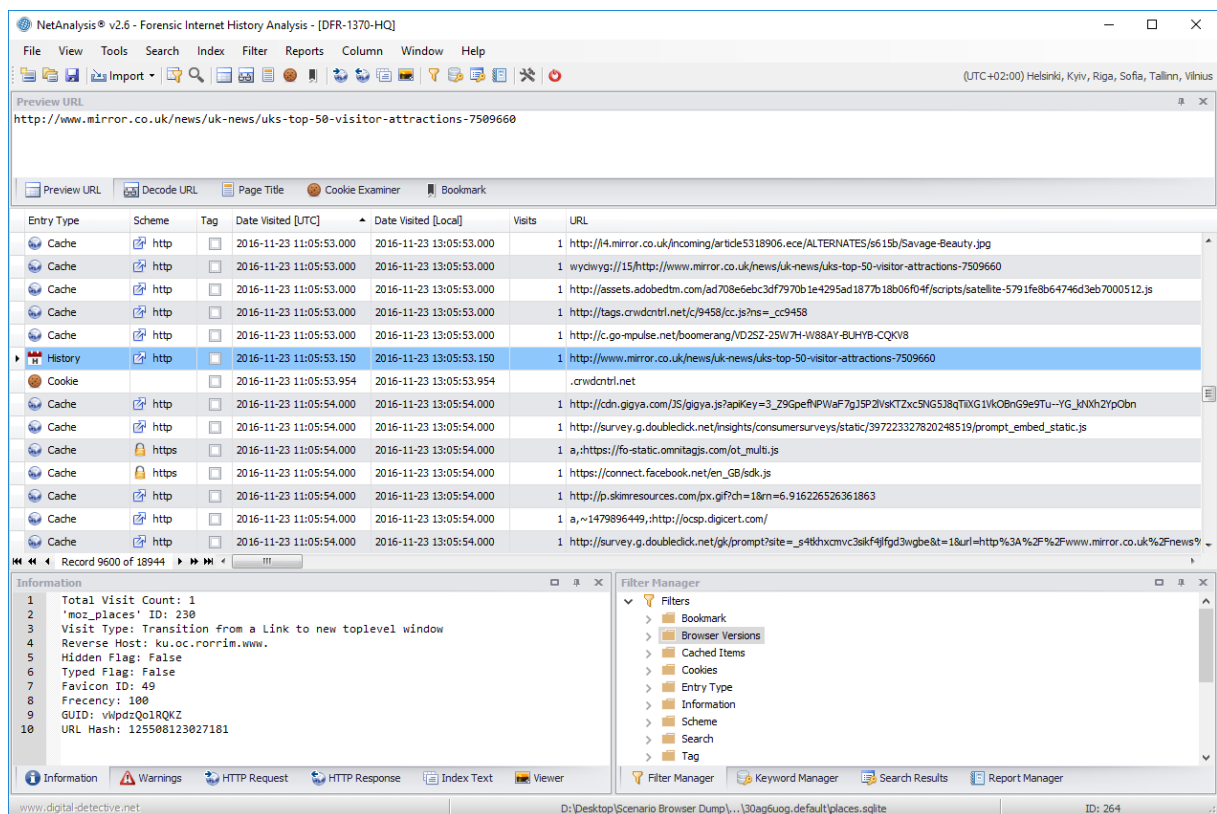


Figure 17

In NetAnalysis® you can customise the position, size and behaviour of windows to create window layouts that work best for the various analysis workflows.

You can also give a custom layout a name and save it, and then switch between layouts by selecting a different layout file. For example, you could create a layout for reviewing rebuilt HTML web pages, and another for reviewing cookie data.

The **Window** menu shows options for loading and saving layouts as well as closing and hiding windows. Right click on a window tab or title bar to see additional options for that specific window.

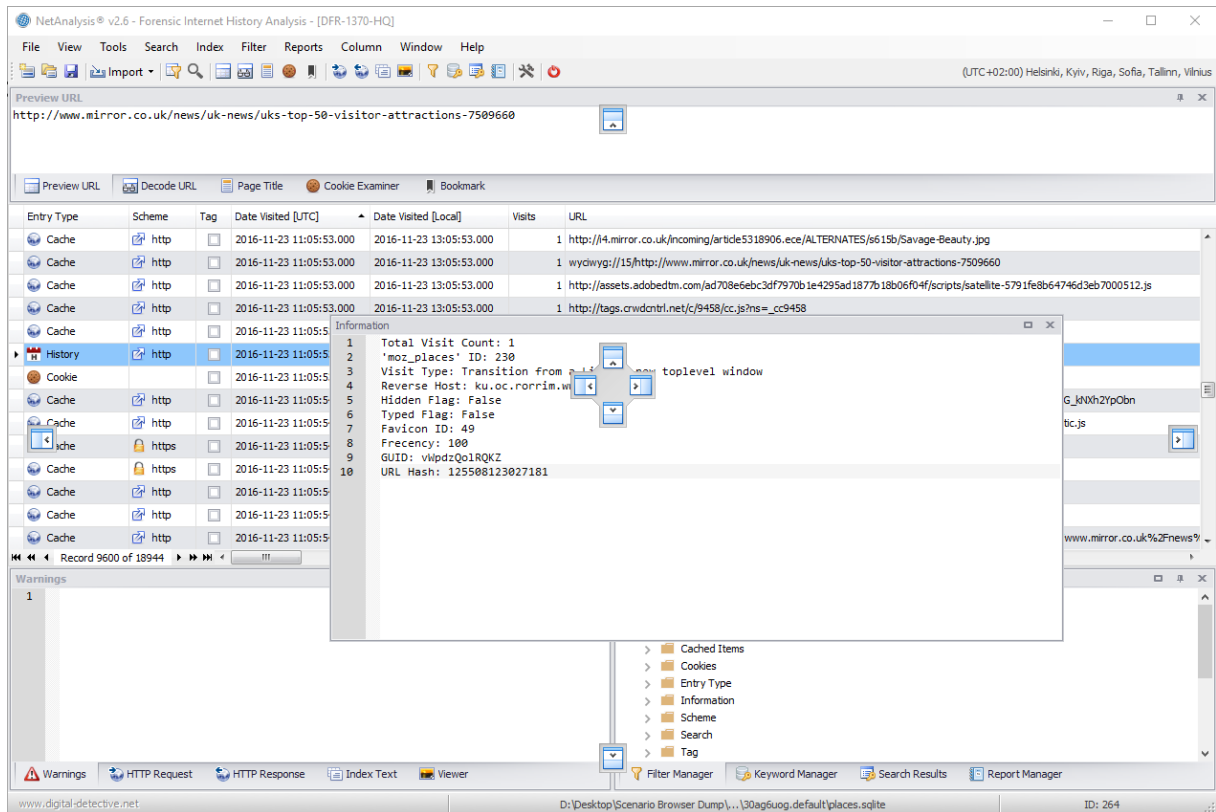


Figure 18

Tab Groups

Tab Groups extend your ability to manage limited screen space while you are working with two or more open windows in the Analysis Environment. You can organise multiple windows into either vertical or horizontal Tab Groups and shuffle windows from one Tab Group to another.

Split Windows

When you have to view two tabbed windows at the same time, you can split the windows. To divide your panels into two independently scrolling sections, click and drag one of the tabs so that the docking guide appears (as can be seen in Figure 18). During the drag operation, when the mouse cursor is over

one of the arrows in the docking guide, a blue shaded area will appear that shows you where the window will be docked if you release the mouse button at that point.

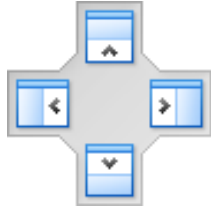


Figure 19

Arranging and Docking Windows

Many of the windows in NetAnalysis® can be docked, so that it has a position and size within the main window frame, or floating as a separate window independent of the main window; also, some windows can be docked within a group of tabs. You can dock multiple windows to float together in a floating Tabbed Group over or outside the main window.

Closing and Auto-Hiding Windows

You can close a window by clicking the X in the upper right of the title bar; to reopen the window, use its keyboard shortcut or menu command. Window panels support a feature named Auto Hide, which causes a window to slide out of the way when you use a different window. When a window is auto-hidden, its name appears on a tab at the edge of the main window.

Specifying a Monitor

If you have a second monitor and your operating system supports it, you can choose which monitor displays a window. You can even group multiple windows together in Tab Groups on other monitors.

Reset, Name and Switch Between Window Layouts

You can return the main Analysis Environment window to the original state by closing all of the open windows. This can be done by selecting **Close All** from the Window menu.

To reset all windows to their default location, select **Reset Window Layout** from the Window menu.

Create and Save Custom Layouts

NetAnalysis® allows you to save custom window layouts and quickly switch between them. The following steps show how to create, save, invoke and manage custom layouts and take advantage of multiple monitors with both docked and floating windows.

First, create a new case and select **Show All Windows** from the Window menu.

1. Close any windows you do not want to use in your layout.
2. Customise the location and size of your windows.
3. Once the window positions and layout are as you want, from the main menu select **Window » Save Window Layout**.
4. Enter a name for this layout and click the Save button.

To load a layout, select **Window » Load Window Layout** or press **CTRL + L**.

Main Toolbar

The toolbar (Figure 20) contains a number of buttons for the more common functions. On the right-hand side of the toolbar (Figure 21), the time zone Indicator shows the currently selected time zone for this investigation (for further information about time zone settings, please see Time Zone Configuration on Page 78).










Figure 20

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

Figure 21

Table 3 holds a detailed explanation about the function of each toolbar button.

NetAnalysis® Main Toolbar	
	<p>New Case</p> <p>This allows you to create a New Case using a portable workspace option. It allows you also to set the critical options prior to importing any data. If you wish to create a MySQL Server case, please see Creating a New Server Based Case on Page 189.</p>
	<p>Open Workspace</p> <p>This allows you to open a previously saved NetAnalysis® portable workspace database. If you wish to open a MySQL Server case, please see Opening a Server Based Case on Page 191.</p>
	<p>Save Workspace</p> <p>This allows you to save the currently loaded data into a portable NetAnalysis® Workspace file. You only have to press this once to save the workspace. Subsequent changes such as record book-marking or comments are automatically saved to the workspace. Workspace files contain a database which can be shared with other NetAnalysis® users.</p>
	<p>Import</p> <p>This activates a drop-down menu with two import options as shown below.</p>
	<p>Import » Data from File(s)</p> <p>This opens a file selection window which allows the user to select which file(s) to import.</p>
	<p>Import » Data from Folder</p> <p>This opens a folder selection window which allows the user to select the root folder to search and import from. Whichever folder is selected, NetAnalysis® will recursively search through all folders and sub-folders looking for supported file types.</p>
	<p>Filter Editor</p> <p>This displays the Filter Editor window. The Filter Editor allows the user to build complex filter criteria with an unlimited number of filter conditions, combined by logical operators. You can enable a tree-like or text-based filter editing style or use both styles.</p>



Quick Search

This displays the built-in Quick Search or Find Panel. Quick Search provides an easy way of searching visible columns.



Preview URL

This opens the Preview URL window which allows this data to be easily examined.



Decode URL

This opens the Decode URL window where the URL is shown with any encoded characters replaced with their unencoded value.



Page Title

This opens the Page Title window which allows for easier examination of records containing Page Titles.



Cookie Examiner

This opens the Cookie Examiner window. When a cookie record is selected, the corresponding cookie information is loaded and displayed in the Cookie Examiner.



Bookmark

This opens the Bookmark window which will show the bookmark text relating to the selected record.



HTTP Request

This opens the HTTP Request window which relates to the currently selected record.



HTTP Response

This opens the HTTP Response window which relates to the currently selected record.



Index Text

This opens the panel which contains text content relating to the currently selected record.



Viewer

This opens the panel containing the offline HTML5-compliant viewer which is capable of displaying cached web pages, video, images and other content; it can also play audio files.



Filter Manager

This opens a panel containing the Filter Manager. The Filter Manager allows the user to store, order and configure any number of filters which are stored in a file/folder structure.



Keyword Manager

This opens a panel containing the Keyword Manager. The keyword manager 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.



Search Results

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



Report Manager

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



Options

This opens the Options window allowing the user to review/change the application options and settings.



Exit

This button will exit the software. NetAnalysis® will prompt the user if the workspace has not been saved.

Table 3

Status Bar

The status bar contains some useful information in relation to the selected record. For example, the icon shown in Figure 22 indicates the selected record contains a bookmark.



Figure 22

Figure 23 shows a panel containing the source file for the selected record. If the user right clicks the mouse cursor over this text, the full path can be copied to the clipboard.

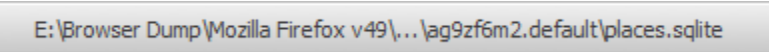


Figure 23

Figure 24 shows a panel containing the location of the data for the currently selected record. In this case, it shows the corresponding row ID for a record in a places.sqlite database.

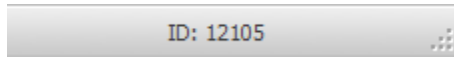


Figure 24

Main Menu

Table 4 highlights the various options available from the main menu.

Menu	Option	Description
File	New Case	Starts a new case.
	New Server Case	Starts a new server-based database case.
	Open Workspace	Opens a saved case.
	Open Server Workspace	Open a saved server-based database case.
	Close Workspace	Closes the current workspace.
	Import » Data from File(s)	Opens a File Import window allowing you to import file(s) for analysis.
	Import » Data from Folder	Opens a Folder Selection window allowing you to import files from a selected folder. The folders are processed recursively.
	Save Workspace	Saves a workspace to file.
	Save Workspace As	Saves a workspace to a new location.
	Export As » Comma Separated Values	Exports the currently filtered records to CSV.
	Export As » Tab Separated Values	Exports the currently filtered records to TSV.
	Export As » SQLite Database	Exports the currently filtered records to SQLite.
	Export As » TLN Timeline	Exports the currently filtered records to TLN.

Menu	Option	Description
	Export As » NetAnalysis® Workspace	Exports the currently filtered records to a new workspace.
	Recent Workspaces	Shows a list of recently accessed workspaces.
	Exit	Exits and closes the application.
View	Preview URL	Opens a window showing a preview of the URL.
	Decode URL	Opens a window showing a decoded version of the URL.
	Page Title	Opens a window showing the Page Title.
	Cookie Examiner	Opens a window containing the Cookie Examiner.
	Bookmark	Opens a window showing the Bookmark.
	HTTP Request	Opens a window showing the HTTP Request data.
	HTTP Response	Opens a window showing the HTTP Response data.
	Index Text	Opens a window showing extracted Index data or text data.
	Viewer	Opens a window containing the offline file/web page Viewer.
	Information	Opens a window showing the Information data.
	Warnings	Opens a window showing the Warning data.
	Filter Manager	Opens a window showing saved Filters in an Explorer style tree.
	Keyword Manager	Opens a window showing saved Keyword files in an Explorer style tree.
	Search Results	Opens a window showing the results of the last Keyword search.
	Report Manager	Opens a window showing saved Report Template files in an Explorer style tree.
Tools	Open Case Export Folder	Opens the Case Export Folder.

Menu	Option	Description
	Export and Rebuild Cache	Executes the task to export all live cached items and to rebuild all available web pages.
	Examine URL	Opens the Examination and Analysis window and loads the URL for analysis.
	Examine » Favicon URL	Opens the Examination and Analysis window and loads the Favicon URL for analysis.
	Examine » Feed URL	Opens the Examination and Analysis window and loads the Feed URL for analysis.
	Examine » Redirect URL	Opens the Examination and Analysis window and loads the Redirect URL for analysis.
	Examine » Referral URL	Opens the Examination and Analysis window and loads the Referral URL for analysis.
	Tag » Selected Records	Tags all selected records.
	Tag » All Visible Records	Tags all visible records
	Remove Tag » Selected Records	Removes tag from all selected records.
	Remove Tag » All Visible Records	Removes tag from all visible records.
	Bookmark » Selected Records	Opens the Bookmark window allowing the same bookmark to be set for all selected records.
	Bookmark » All Visible Records	Opens the Bookmark window allowing the same bookmark to be set for all visible records.
	Remove Bookmark » Selected Records	Removes the bookmark from all selected records.
	Remove Bookmark » All Visible Records	Removes the bookmark from all visible records.
	Navigate To » Record URN	Filters and navigates to a specific record URN.
	Navigate To » Tagged Record » First	Navigates to the first tagged record.
	Navigate To » Tagged Record » Next	Navigates to the next tagged record.
	Navigate To » Tagged Record » Previous	Navigates to the previous tagged record.
	Navigate To » Bookmarked Record » First	Navigates to the first bookmarked record.
	Navigate To » Bookmarked Record » Next	Navigates to the next bookmarked record.

Menu	Option	Description
	Navigate To » Bookmarked Record » Previous	Navigates to the previous bookmarked record.
	Navigate To » Web Site	Opens the default browser and navigates to the URL of the currently selected record.
	Open Source in Hex Viewer	Opens a window containing a hex viewer allowing the user to review the original source data.
	Time Zone Information	Opens a window containing information about the Time Zone settings for the case.
	Show All Records	Removes the active filter and clears the active search.
	Options	Opens the Options window.
Search	Quick Search	Opens the Quick Search panel.
	Clear Search	Clears the active search.
Index	Create Index	Executes the case Indexing engine so that all exported text can be indexed for searching. This will open a progress window showing the indexing progress.
	Search Index	Opens the Search Index window allowing the user to search across the extracted data.
Filter	Filter Editor	Shows the Filter Editor window.
	Save Filter	Allows the user to save the current, active filter to file.
	Open Filter	Opens a File Open window allowing a filter to be opened which had been previously saved to file.
	Auto Filter Row » Show	Opens the Auto Filter panel.
	Auto Filter Row » Hide	Closes the Auto Filter panel.
	Tagged Records	Executes a filter to show all tagged records.
	Bookmarked Records	Executes a filter to show all bookmarked records.
	Information	Executes a filter to show all records containing information.

Menu	Option	Description
	Warnings	Executes a filter to show all records containing warnings.
	Remove Filter	Removes the active filter.
Reports	Preview Detailed Report	Opens a Preview window containing the Detailed Report of the current filtered records.
	User Defined Reports » New Report	Opens the Report Designer with a blank report.
	User Defined Reports » Open Report	Opens a File Open window allowing the user to select and edit a report template.
	User Defined Reports » Preview Report	Opens a File Open window allowing the user to select and run a report template.
Column	Group By Box » Show	Shows the Group By panel.
	Group By Box » Hide	Hides the Group By panel.
	Column Chooser	Opens a window showing the currently hidden columns.
	Best Fit	Resizes all columns so that they are set to the best width.
	Clear Sorting	Clears any active sort.
	Clear Grouping	Clears any active grouping.
	Reset Column Layout	Resets the column layout back to the default setting.
	Save Column Layout	Opens a File Save window allowing the user to save the current column layout with, or without, data filter/grouping settings.
	Load Column Layout	Opens a File Open window allowing the user to select a file containing a previously saved column layout.
Window	Show All Windows	Shows all of the available panel windows.
	Auto Hide All	Sets all of the visible window panels to auto-hide.
	Close All	Closes all of the visible panel windows.
	Reset Window Layout	Resets the panel window layout to default.

Menu	Option	Description
	Save Window Layout	Opens a File Save window allowing the user to save the current panel window layout.
	Load Window Layout	Opens a File Open window allowing the user to select a file containing a previously saved panel window layout.
Help	Knowledge Base	Opens a web browser with a link to the knowledge base.
	Support	Opens a web browser with a link to the support portal.
	Check for Software update	Checks if there is an updated version of the software available, if so, the download link is provided.
	About NetAnalysis®	Shows the About window.

Table 4

Columns

To fully understand the extracted data as presented by NetAnalysis®, it is important to understand the type of data held in each column (or field). In this section, we will examine each column header and identify what type of data is stored in that field.

Entry Type

The Entry Type value is generated by NetAnalysis® and identifies the type of entry the record relates to. For a full breakdown of each value, see Table 5 on Page 55.

Scheme

Each URI begins with a scheme name that refers to a specification for assigning identifiers within that scheme. Scheme names consist of a sequence of characters beginning with a letter and followed by any combination of letters, digits, plus "+", period ".", or hyphen "-". Although schemes are case-insensitive, the canonical form is lowercase.

Tag

This column exists to assist with the examination and analysis of the data loaded into NetAnalysis®. Tags can be set by the user and used for many purposes; for example, they can be used to quickly filter records of interest in the grid.

Date Visited [UTC]

This date and time is stored as a UTC value and represents a visit; it is sourced from a number of different timestamps depending upon the subject data.

Date Visited [Local]

This date and time is usually (although not always) calculated as a local time value from the Date Visited [UTC] value above.

Visits

An integer value which represents the recorded visit count. This is a value read directly from a source record (as stored by the original source browser) and is **not** a calculated value.

URL

URL is an acronym for Uniform Resource Locator and is a reference (an address) to a resource on a network, typically the Internet. A URL is a type of URI (Uniform Resource Identifier) which uses a string of letters, digits and symbols to identify a resource. In addition to identifying a resource, a URL contains the information about how to fetch the resource from its location.

Decoded URL

A URI consists of a restricted set of characters. The restricted set of characters consists of digits, letters, and a few graphic symbols chosen from those common to most of the character encodings and input facilities available to Internet users. They are made up of the "unreserved" and "reserved" character sets as defined in RFC 3986. In addition, any byte (octet) can be represented in a URI by an escape sequence: a triplet consisting of the character "%" followed by two hexadecimal digits. A byte can also be represented directly by a character, using the US-ASCII character for that octet.

Some of the characters are reserved for use as delimiters or as part of certain URI components. These must be escaped if they are to be treated as ordinary data. Read RFC 3986 for further details.

The Decoded URL column displays a string with each %XX sequence replaced with the unencoded value.

Host Name

The Host Name is a string which is usually the DNS host name or IP address of the server.

Page Title

This column displays any associated Page Title. For bookmark folder entries, this column holds the name of the folder.

Absolute Path

The Absolute Path contains the path information that the server uses to resolve requests for information. Typically, this is the path to the desired information on the server's file system, although it also can indicate the application or script the server must run to provide the information.

The path information does not include the scheme, host name, or query portion of the URI.

Query

This column contains any query information included in the URI. Query information is separated from the path information by a question mark "?" and continues to the end of the URI. The query information returned includes the leading question mark.

The query information is escaped according to RFC 2396 by default. If International Resource Identifiers (IRIs) or Internationalized Domain Name (IDN) parsing is enabled, the query information is escaped according to RFC 3986 and RFC 3987.

Search Term

This column contains the search term extracted from the query information in the URI. This field contains data extracted from information contained within the Query field.

Fragment

This column contains any URI fragment information. The Fragment property gets any text following a fragment marker "#" in the URI, including the fragment marker itself.

Port

The port number defines the protocol port used for contacting the server referenced in the URI. A scheme may define a default port. For example, the "http" scheme defines a default port of "80", corresponding to its reserved TCP port number. The type of port designated by the port number (e.g., TCP, UDP, SCTP) is defined by the URI scheme.

User

This value represents the active user account name in Microsoft Windows when the record type relates to Microsoft Internet Explorer or Microsoft Edge browsers. There will be no values in this column for non-Microsoft browsers. Microsoft browsers store the user account name as part of the structure of some records (cache entries).



Note: Sometimes the letter case of the username differs from the actual user account name. NetAnalysis® displays the text using the same case as is stored in the original file.

Logon User / Logon Password

These two columns contain user and password information. The username and password values are either website login or sign-on entries or are extracted from the "userinfo" subcomponent of the authority component of the URI if present. The password values will be decrypted where possible.

Redirect URL

Redirection is the process of forwarding one URL to a different URL. There are three main kinds of redirects: 301, 302, and meta refresh. This column relates to server-side redirects where the HTTP status code is in the 300 range.

Referral URL

The referrer or referring page is the URL of the previous web page from which a link to the current page was followed.

Feed URL

This URL relates to an RSS feed.

Favicon URL

This URL relates to the location of an associated favicon.

Local Path

This column relates to a local path and contains the local operating system representation of a file name. For example, a download record would hold the location where the downloaded file had been saved.

Cache Folder

This column contains folder path information relating to the cached file for this entry.

Cache File

This column contains the file name relating to the cached file for this entry.

Cache File Extension

This column contains the file name extension relating to the cached file for this entry.

Cache File Length

This column contains the data length in bytes relating to the cached file for this entry.

Cache File Exists

This column indicates whether or not the cached file data actually exists and can be viewed. Cached files can be displayed in the Viewer Panel: **View » Viewer** (although Cache entries will need to be exported first).

Date HTTP Response [UTC]

The HTTP response header field Date information can be found in this column. This field contains the date and time at which the response message was originated.

Date HTTP Last Modified [UTC]

The HTTP response header field Last-Modified information can be found in this column. This field contains the date and time at which the server believes the resource was last modified.

HTTP Request

This column contains text relating to the request message made by a browser to the web-server as part of the request/response process using the Hypertext Transfer Protocol (HTTP). This may include the request method and request header fields. When viewed in the grid, the individual elements are separated by a vertical bar character "|". The contents of this column can also be displayed in the HTTP Request Panel: **View » HTTP Request**.

HTTP Response

This column contains text relating to the response message made by a web-server as a result of receiving a request using the Hypertext Transfer Protocol (HTTP). This may include the response status information and response header fields. When viewed in the grid, the individual elements are separated by a vertical bar character "|". The contents of this column can also be displayed in the HTTP Response Panel: **View » HTTP Response**.

Content Type

The HTTP response header field Content-Type information can be found in this column. This field is used to indicate the media type (or MIME type) of the resource. Its purpose is to describe the data contained in the HTTP response body fully enough that the receiving user agent can pick an appropriate agent or mechanism to present the data to the user, or otherwise deal with the data in an appropriate manner.

Content Length

The HTTP response header field Content-Length information can be found in this column. This field holds the length of the HTTP response body in octets (8-bit bytes).

Content Encoding

The HTTP response header field Content-Encoding information can be found in this column. This field is used to indicate any additional content encoding applied to the data contained in the HTTP response body. Its purpose is to let the client know how to decode the data in order to obtain the media type referenced by the Content-Type header field.

Active Time Bias

This column is derived from information stored in daily Microsoft Internet Explorer/Edge records and represents the time zone active bias. The active bias represents the number of minutes to be added to

a local time to convert it back to Coordinated Universal Time. We can use this information to establish if the time zone translation settings are correct. If the record does not relate to a daily history entry belonging to a Microsoft based browser, it will be empty.

Date First Visited [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Created, Added or First Visited. In the case of download entries, this relates to the Start Time.

Date Last Visited [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Last Visited or Last Accessed.

Date Expiration [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Expiration.

Date Last Modified [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Last Modified.

Date Index Created [UTC]

This column is derived from information stored in weekly Microsoft Internet Explorer/Edge records and relates to the date and time at which the daily entries were updated to weekly entries.

If the record does not relate to a weekly history entry belonging to a Microsoft based browser, it will be empty.



Note: For Microsoft based browsers, the source of the timestamp data can be examined by reviewing the Information panel. Select **View » Information**.

Date Added [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Added or Created.

Date Last Synch [UTC]

This date and time value is stored as UTC and is sourced from timestamps described as Synced. In the case of download entries, this relates to the End Time.

Source File

This column shows the file path of the resource containing the information from which the record is extracted.

Source Offset

This column shows a value which points to where the original data containing the information for this record is extracted. This may be a Row Identifier (Row ID), Entry Identifier (Entry ID), File Offset (FO) or Physical Sector and Sector Offset (PS, SO).

Browser Version

This column represents the browser and version information relating to the identified artefact. If it is not possible to identify a specific browser, then NetAnalysis® will identify the family of browsers the data relates to; for example, Chromium Based. This column will also identify the type of data this record relates to; for example, History or Cache.

Warning

If any issues are encountered during the import process, or if any data requires further analysis to establish evidential integrity, a warning flag is set in the URL column and information relating to the warning can be found in the Warning column. One example of this is partially overwritten records recovered by HstEx®. Warnings can be read in the grid (with multiple items separated by a vertical bar character "|"), or displayed in the Warning Panel: **View » Warnings**.

Information

This column is used to display Information relating to the record which does not necessarily have a corresponding column in the grid. The Information panel may also contain further useful information about an entry. Information can be read from the grid (where each item is separated by a vertical bar character "|"), or displayed in the Information Panel: **View » Information**.

Bookmark







This column exists to assist with the examination and analysis of the data loaded into NetAnalysis®. Bookmarks can be set by the user to annotate entries.














URN













Unique Reference Number (URN). NetAnalysis® generates a unique reference number for every entry added to the grid in a workspace. URNs allow the user to quickly access a specific record by selecting: **Tools » Navigate To » Record URN**. URN values are also used internally for identifying specific records in the workspace.















Entry Type
















The Entry Type value is generated by NetAnalysis® and identifies the type of entry the record relates to. Table 5 briefly outlines each type.

















Entry Type	Information
 AppCache	These entries relate to application cache. HTML5 introduces application cache, which means that a web application is cached, and accessible without an internet connection. Application cache gives an application three advantages: <ol style="list-style-type: none"> 1. Offline browsing - users can use the application when they are offline 2. Speed - cached resources load faster 3. Reduced server load - the browser will only download updated/changed resources from the server
 AppCacheEntry	
 Archived	This is a Chromium based browser artefact which relates to archived history entries stored in the Archived History database (Chrome v1 - 36).
 Autocomplete Predictor	This is a Chromium based browser artefact which relates to autocomplete network action predictor entries stored in the Network Action Predictor database.
 Autofill Profile	Chromium based browsers allow autofill profiles to be saved so that forms can be quickly completed from a drop-down list of saved profiles.
 BackgroundTransferApi	This is a Microsoft Internet Explorer/Edge browser artefact. The Background Transfer API enables advanced download and upload transfer capabilities within an app

Entry Type	Information
 Bookmark	This entry relates to a bookmarked web page or website.
 Bookmark Folder	This entry relates to a folder for storing bookmarks. Most browsers allow the user to store their bookmarked pages in a folder hierarchy.
 Bookmark Label	This is a Sleipnir on Mac OS X browser artefact. The entry relates to a user defined bookmark label.
 Bookmark Label Group	This is a Sleipnir on Mac OS X browser artefact. The entry relates to a user defined bookmark label group.
 Bookmark Separator	This entry relates to a bookmark separator item. Some browsers allow the user to manage bookmarks by adding separators to help distinguish different bookmark categories from each other.
 Bookmark Tag	Many Mozilla based browsers allows the user to categorize their bookmarks by adding tags to help identify them.
 Cache	This entry relates to an item which has been cached. A cache is a repository for storing data that is used to expedite the process of retrieving that data. Caches are used to speed up the browsing process so that data does not have to be fetched from its original location every time a page or cached object is requested.
 Cookie	This entry relates to a cookie. A cookie is the term given to describe a type of message that is sent from a website to a browser when browsing a web page. If the server requests that the message persists, it is stored by the browser. When the user re-visits the page, the browser sends the message back to the web server to indicate a previous visit.
 Credit Card	Chromium based browsers allow autofill credit card information to be saved so that forms can be quickly completed from a drop-down list of saved credit cards.
 Cross-Domain	This is a 360 Browser cross-domain cookie artefact.
 Daily	This is a Microsoft Internet Explorer/Edge browser artefact relating to a daily visit entry.
 Dependency Entry	These entries relate to pre-resolve and pre-connect data in Microsoft Edge and Internet Explorer. As the browser processes the HTML of a top-level page, it must perform a number of operations to be able to download the additional resources (dependencies) required to display the page.
 DOM Store	Web storage and DOM storage (Document Object Model storage) are web application software methods and protocols used for storing data in a web browser. Web storage supports persistent data storage, similar to cookies but with a greatly enhanced capacity and no information stored in the HTTP request header.

Entry Type	Information
 Download	<p>This entry relates to artefacts which have been downloaded via the web browser.</p>
 Favicon	<p>A favicon, also known as a shortcut icon, website icon, tab icon or bookmark icon, is a file containing one or more small icons associated with a particular website or web page.</p>
 Favorite	<p>A "favorite" entry is an artefact from the Microsoft Internet Explorer/Edge browser which allows the user to save bookmarks to favourite web pages for later retrieval.</p> <p>It can also be an Opera browser artefact relating to a "favorite" entry stored in the favorites.db database (Opera v15 - 32).</p>
 Favorite Folder	<p>A "favorite" folder entry for the Microsoft Edge browser relates to a folder for storing bookmarks. The user can organise their favourite entries into folders.</p>
 Feedplat	<p>This is a Microsoft Internet Explorer/Edge browser artefact relating to RSS feeds.</p>
 Form History	<p>Most browsers can save information every time the user completes a form so that the next time they access a form, they will see a drop-down list of options to choose from.</p>
 Gallery	<p>This is an Opera Neon browser artefact. The entry relates to the screenshots and web page shortcuts saved by the user into the web browser's gallery.</p>
 History	<p>This entry relates to a standard history visit.</p>
 History Provider	<p>This is a Chromium based browser artefact which relates to autocomplete candidates which have been sourced from the user's history stored in their History Provider Cache.</p>
 Host	<p>This is a Mozilla based browser artefact which relates to host entries taken from either the user's history or bookmarks.</p> <p>This is not related to the Host scheme found in Microsoft Internet Explorer/Edge daily history entries.</p>
 IECompatCache	<p>This is a Microsoft Internet Explorer/Edge browser artefact which relates to the browser Compatibility View list. This is a list of sites that will be displayed in Compatibility View. Sites which appear in the Compatibility View list are sites for which other users have clicked the Compatibility View button. This list is updated automatically by Microsoft and is not necessarily related to any visits made by the user.</p>
 IECompatUA	
 IEFlipahead	<p>This is a Microsoft Internet Explorer/Edge browser artefact. Flip ahead allows the user to explore favourite websites like they would a magazine. By implementing flip ahead, the web developer enables their users to flip through a news article or an online catalogue, regardless of their actual location on the page. Visitors no longer need to click a Next button to go to the next page.</p>

Entry Type	Information
 IETIdCache	This is a Microsoft Internet Explorer/Edge browser artefact. This data is not related to user activity and is generated by Microsoft.
 Index	<p>This is a Chromium based browser artefact which relates to entries containing text-based content from web pages stored in the History Index database (Chrome v1 - 29).</p> <p>It can also be a Safari browser artefact containing text-based content from web pages that the browser uses for indexing and searching.</p>
 Input History	This is a Mozilla based browser artefact which relates to URLs typed by the user.
 Leak	This is a Microsoft Internet Explorer/Edge browser artefact. Leak entries relate to cache or cookie entries that have been scheduled for deletion and have not yet been removed by the cache scavenger.
 Logged In Predictor	This is a Chromium based browser artefact which relates to logged in predictor entries stored in the Network Action Predictor database.
 Login Data	This is a Chromium based browser artefact which relates to website login username and password entries.
 Logins	This is a Mozilla based browser artefact which relates to website login username and password entries stored in the logins.json file (Firefox v32.0+).
 Logins Disabled	This is a Mozilla based browser artefact which relates to host entries stored in the logins.json file for which the user has declined to store login information (Firefox v32.0+).
 Master	This is a Microsoft Internet Explorer/Edge browser artefact. Master entries relate to master history entries.
 Note	This is an artefact which relates to user created notes.
 Note Folder	This is an artefact which relates to a folder for storing notes. This allow the user to store their notes in a folder hierarchy.
 Note Separator	This is an Opera browser artefact which relates to a note separator item. This allows the user to manage notes by adding separators to help distinguish different categories of notes from each other (Opera v7 - 12).
 Page Icon	This is an Opera Neon browser artefact. The entry relates to the icons associated with a particular website or web page.
 Permission	Mozilla based browsers allow the user to adjust the default permissions for a website to be overridden. This entry relates to the user adjusted permission settings.

Entry Type	Information
 PrivacIE	This is a Microsoft Internet Explorer/Edge browser artefact and relates to InPrivate Filtering. InPrivate Filtering helps prevent the websites a user visits from automatically sending details about the visit to other content providers.
 Reading List	This relates to a Reading List entry. During a browsing session, if the user identifies a page to be viewed at a later date, they can add it to a Reading List.
 Reading List (View)	This entry relates to web pages which has been added to the Reading List whilst in Reading View mode. Reading View mode allows the user to view a page in a clutter-free, reader-friendly view.
 Recovery Store	This entry relates to Microsoft Internet Explorer and Edge. The Recovery Store file contains information relating to browsing sessions. It was designed to allow the browser to recover from a crash and then re-open tabs. Each Recovery Store file contains information relating to various tab sessions. The tab session files contain information relating to the various tabs that have been visited along with their order. See the Tab entry type.
 Redirect	This entry relates to server-side redirects.
 Registry	This entry relates to browser artefacts read from the Windows Registry.
 Resource Prefetch Predictor	This is a Chromium based browser artefact which relates to resource prefetch predictor entries stored in the Network Action Predictor database.
 Saved Page	When closing the application, some browsers prompt the user and ask if they wish to save the open page(s) (such as 360 Security browser). This entry relates to pages that have been saved by the user so that they can be visited at a later date.
 Search Engine	This is a Chromium based browser artefact which relates to search engine keyword entries stored in the Web Data database.
 Search Term	This entry relates to a search term history entry.
 Segment Usage	This is a Chromium based browser artefact. It stores URL segment information which is used for the most visited page view in the web browser.
 Server Address	This is a Chromium based browser artefact which relates to Google Wallet autofill address entries stored in the Web Data database.
 Server Credit Card	This is a Chromium based browser artefact which relates to Google Wallet autofill credit card entries stored in the Web Data database.
 Session	This is a Mozilla based browser artefact and relates to a user's browsing session. A session can have windows, tabs and cookies which will be recorded as separate Window, Tab, Tab History and Cookie entries.
 Shortcut	This is a Chromium based browser artefact which relates to Omnibox shortcut entries.

Entry Type	Information
 Sign On	This is a Mozilla based browser artefact which relates to website login username and password entries stored in the signons.sqlite database (Firefox v3 - 31).
 Sign On Disabled	This is a Mozilla based browser artefact which relates to host entries stored in the signons.sqlite database for which the user has declined to store login information (Firefox v3 - 31).
 Stash	This relates to an Opera browser artefact which allows the user to store web pages to be viewed at a later date (Opera v15 - 26).
 Tab	This entry type is used by a number of different browsers and relates to an individual tab. For most browsers, each tab will have a history of visits which will be recorded as Tab History entries; in Microsoft Internet Explorer and Edge the visit history is recorded as Travel Log entries.
 Tab Group	This is a Sleipnir on Mac OS X browser artefact. The entry relates to a user defined tab group.
 Tab History	This entry type is used by a number of different browsers and relates to the visit history of a tab.
 Tab Roaming	This is a Microsoft Internet Explorer and Edge artefact. It relates to Roaming Tabs and is similar to the Tab entry type. There will be a number of Travel Log entries relating to the history of this Roaming Tab.
 Thumbnail	This is an artefact which relates to the thumbnail image used in Speed Dial or Top Sites entries.
 Top Site	This is a browser artefact which relates to the top most visited website entries.
 Top Site Removed	This is a Safari browser artefact which relates to website entries that the user has chosen to remove from their top most visited websites.
 Touch Icon	This is similar to a favicon and is a file containing a small icon associated with a particular website or web page. It is usually used on mobile devices.
 Travel Log	This is a Microsoft Internet Explorer and Edge browser artefact. A Travel Log entry relates to a visit for a specific Tab. The Information panel/column will provide further information about the Tab this Travel Log entry relates to.
 Typed History	This entry relates to a typed history entry.
 User Data	This is a Microsoft Internet Explorer/Edge browser artefact.
 View Source	This is a Microsoft Internet Explorer/Edge browser artefact generated when a user views the source of a web page (normally by right clicking on the page and selecting view source).
 VLink	This is an Opera browser artefact and represents a visited link (Opera v4 - 12).




Entry Type	Information
 Weekly	This is a Microsoft Internet Explorer/Edge browser artefact. These entries relate to weekly history visits.
 Window	This is a Safari and Mozilla based browser artefact and relates to an individual window. Each window will have tabs which will be recorded as Tab entries.
 Wpnidm	This is a Windows 8/Windows 10 artefact which relates to push notifications for tiles.

Table 5

Docking Panels

The main components of the interface are contained within dockable panels which are fully customisable. In the following section, we explain the purpose of each panel.

All of the docking panels can be accessed from the **View** menu. The docking panel layout can be saved to file so that you can quickly switch between custom layouts. To see how this is achieved, review the section titled Reset, Name and Switch Between Window Layouts on Page 38.

Preview URL

The Preview URL panel displays the data from the URL column of the currently selected record. This allows the user to more easily review the whole URL. Figure 25 shows an example URL in the Preview URL panel.

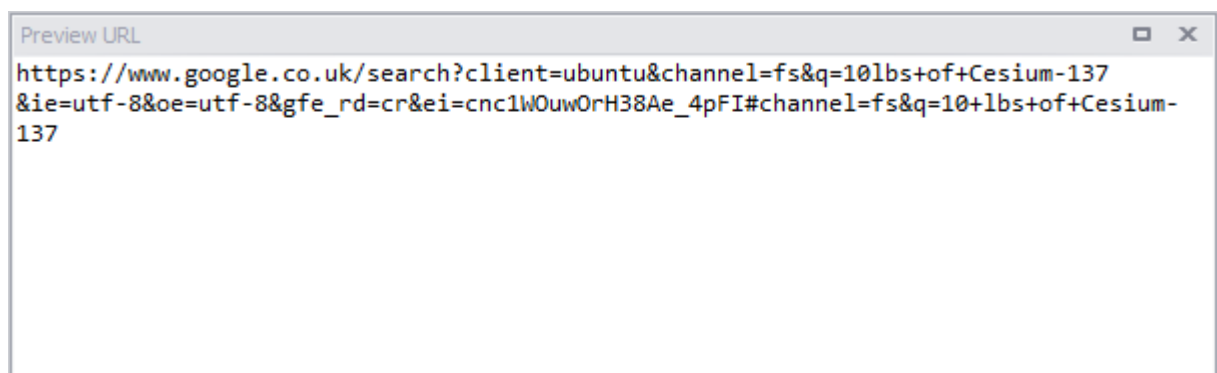


Figure 25

The Preview URL (and Decode URL) panel allows the user to select part of a URL (or the whole URL) and perform analysis on the selected text. This is achieved by right clicking on the selected panel. A context menu is then displayed (as shown in Figure 26). Clicking on **Examine Selected** will display the Examine window.

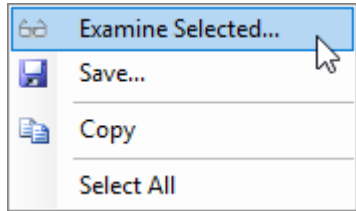


Figure 26

Decode URL

The Decode URL panel displays the data from the Decoded URL column. The panel displays a decoded version of the URL and splits the text at certain characters to make the name/value pairs easier to read and understand (see Figure 27 below which shows a decoded version of the URL from Figure 25).

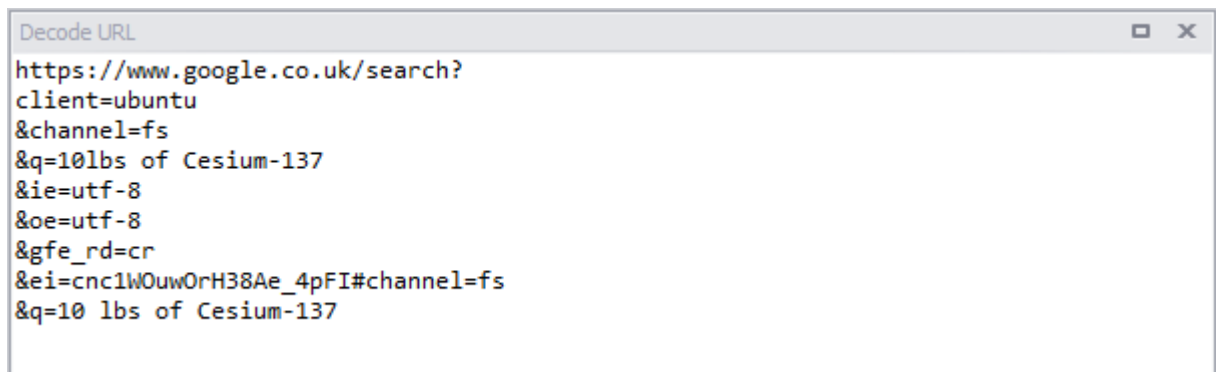


Figure 27

Page Title

The Page Title panel displays the data from the Page Title column.

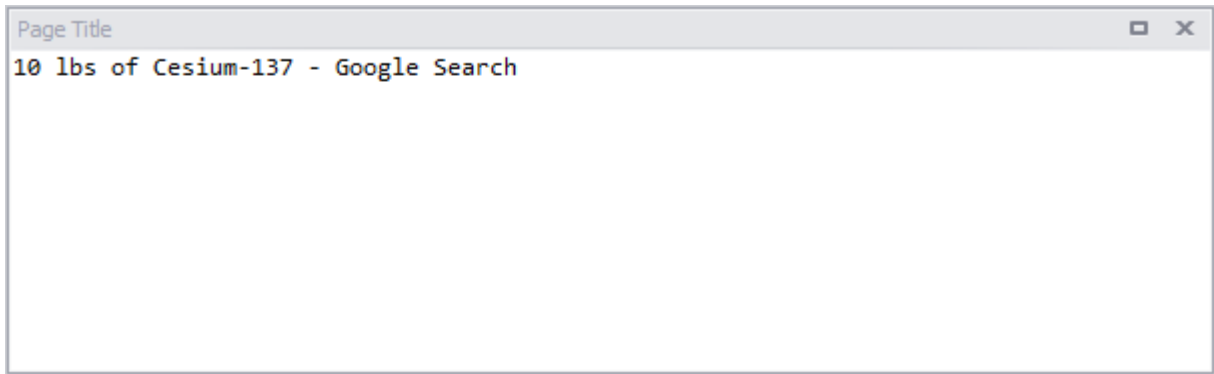


Figure 28

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.

Name	Value
NID	
Domain	.google.com
Path	/
Date Last Accessed [UTC]	2016-11-24 09:55:31.111
Date Created [UTC]	2016-11-23 16:36:38.739
Date Expiration [UTC]	2017-05-25 16:36:38.739
HTTP Only	True
Secure	False
Information	Has Expiration, Persistent, Medium Priority
Original Value	91=C5t0us-Q97-ZfNSy9induIVMYi8VXYh3EoRuzBJP5y7oSwUJVDEst...

Figure 29

For more information on Cookie Examination and Analysis see Page 111.

Bookmark

As you review and analyse the data, you may identify records which are of evidential value or relevant to the particular investigation. The Bookmark panel displays the text which has been set for a specific

record. Right clicking on the panel shows a context menu which allows the user to add or edit the bookmark. The bookmark field can be displayed when producing reports.

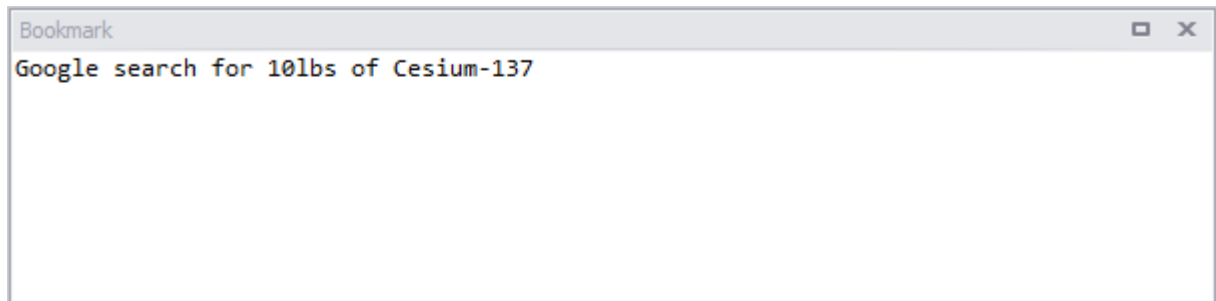


Figure 30

HTTP Request

The Hypertext Transfer Protocol is a stateless, application-layer protocol for communications between distributed systems such as web browsers and web servers. The communication between the host and the client is made via a request/response pair. Many web browsers store one or both of the request/response messages as part of the caching process. The HTTP Request panel shows the text from any saved request message.

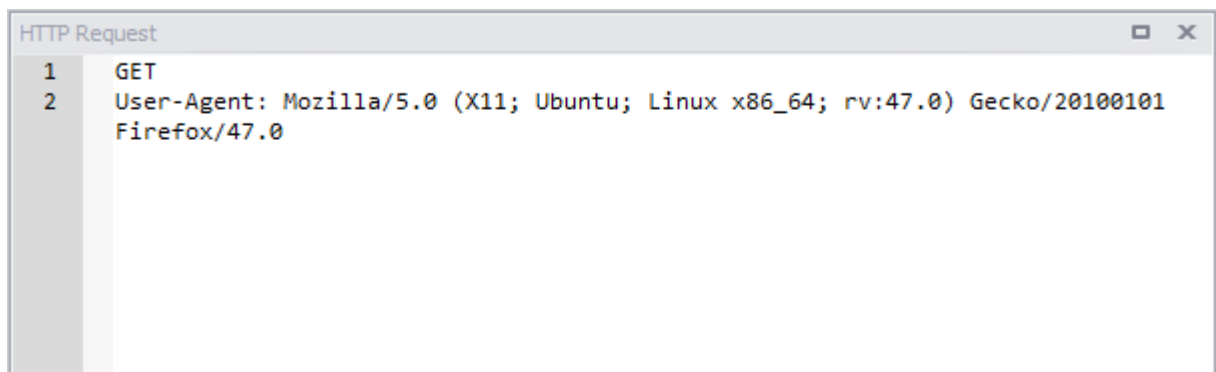


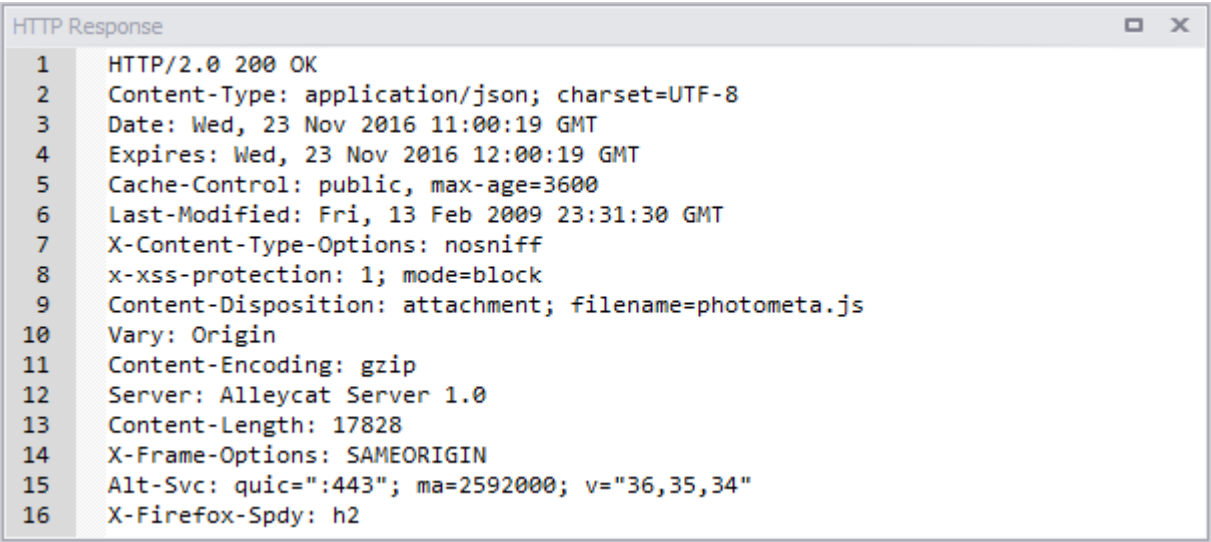
Figure 31

At the heart of web communications is the request message, which is sent via a Uniform Resource Locator (URL). The URL reveals the identity of the particular host with which the browser is communicating. The action that should be performed on the host is specified via an HTTP verb. The most popular verbs are as follows:

- **GET:** Fetch an existing resource. The URL contains all the necessary information the server needs to locate and return the resource;
- **POST:** Create a new resource. POST requests usually carry a payload that specify the data for the new resource;
- **PUT:** Update an existing resource. The payload may contain the updated data for the resource;
- **DELETE:** Delete an existing resource.

HTTP Response

The HTTP Response information relates to the response part of the Hypertext Transfer Protocol request/response messages. Most browsers store a full or partial response message as part of the caching process (see Figure 32).



```
1 HTTP/2.0 200 OK
2 Content-Type: application/json; charset=UTF-8
3 Date: Wed, 23 Nov 2016 11:00:19 GMT
4 Expires: Wed, 23 Nov 2016 12:00:19 GMT
5 Cache-Control: public, max-age=3600
6 Last-Modified: Fri, 13 Feb 2009 23:31:30 GMT
7 X-Content-Type-Options: nosniff
8 x-xss-protection: 1; mode=block
9 Content-Disposition: attachment; filename=photometa.js
10 Vary: Origin
11 Content-Encoding: gzip
12 Server: Alleycat Server 1.0
13 Content-Length: 17828
14 X-Frame-Options: SAMEORIGIN
15 Alt-Svc: quic=":443"; ma=2592000; v="36,35,34"
16 X-Firefox-Spdy: h2
```

Figure 32

Index 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. For further information on indexing within NetAnalysis®, see Indexing and Searching on Page 152.

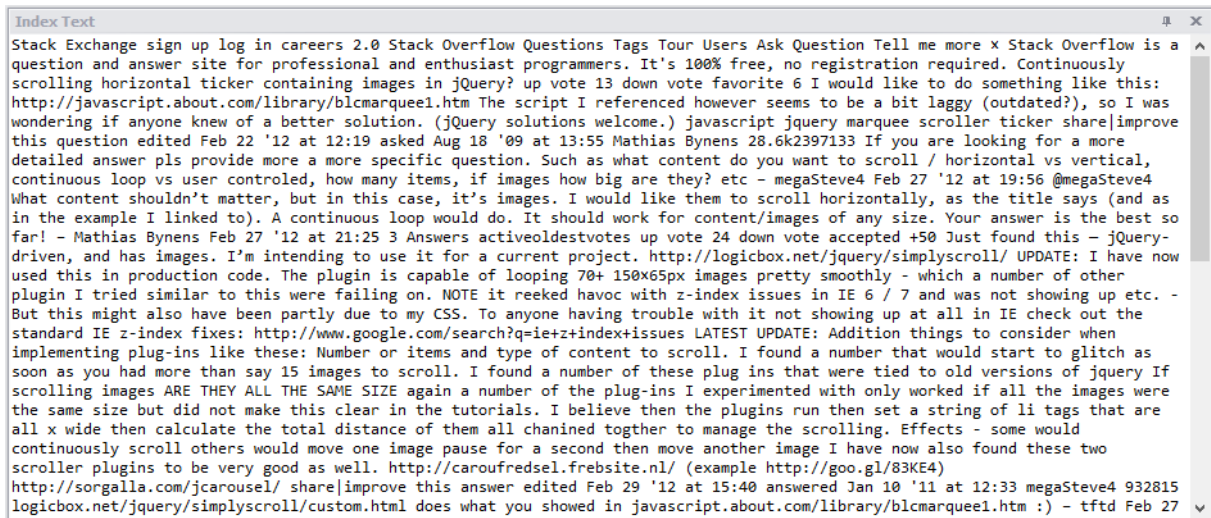


Figure 33

Viewer

The Viewer panel contains an offline, HTML5-compliant viewer which is capable of displaying cached web pages, video, images and other content; it can also play audio files. After the cache has been exported and all available web pages rebuilt, the viewer will display a whole host of visual content.

For further information see Web Page Rebuilding on Page 143.

For further information regarding the type of content displayed in the viewer, see the section Built-In Viewer on Page 150.

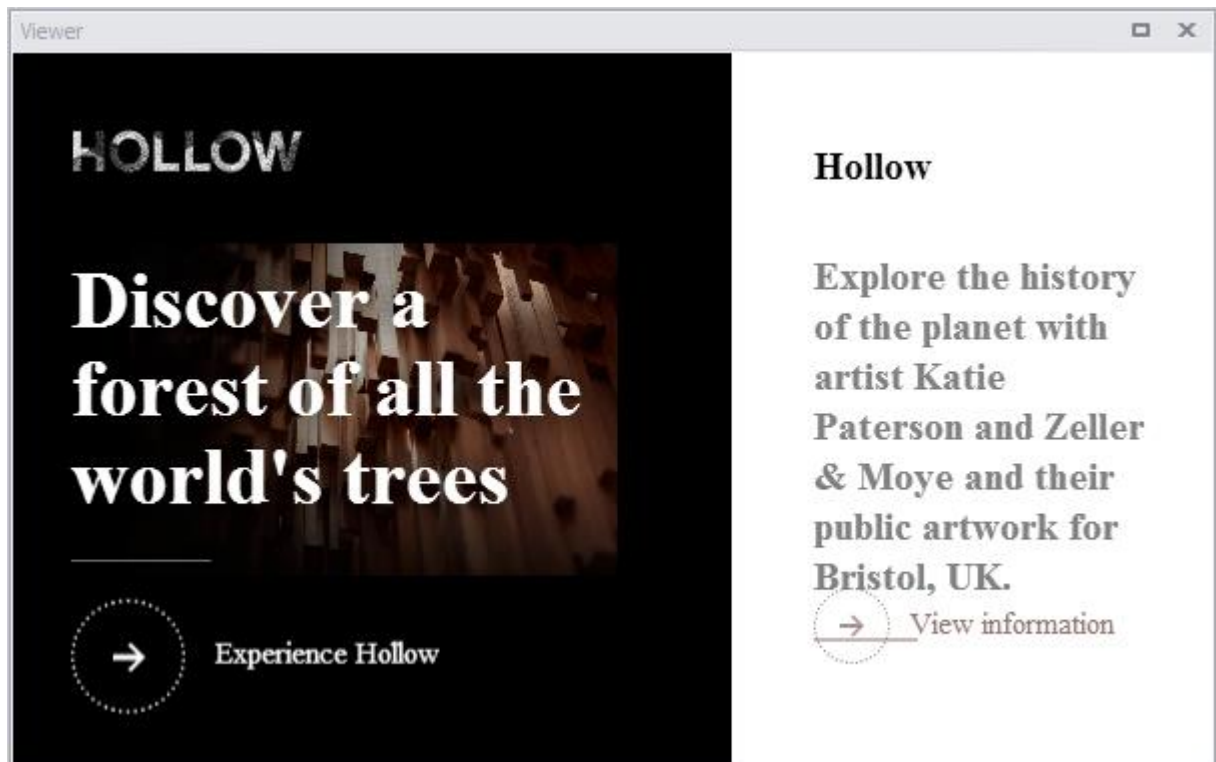


Figure 34

Information

The Information Panel holds additional information relating to the selected record. Further information may include data where there is no corresponding column in the grid, or data such as record transition information. The panel may also include information explaining the meaning of certain data. To show the Information Panel, select **View » Information** or **CTRL + Shift + I**.

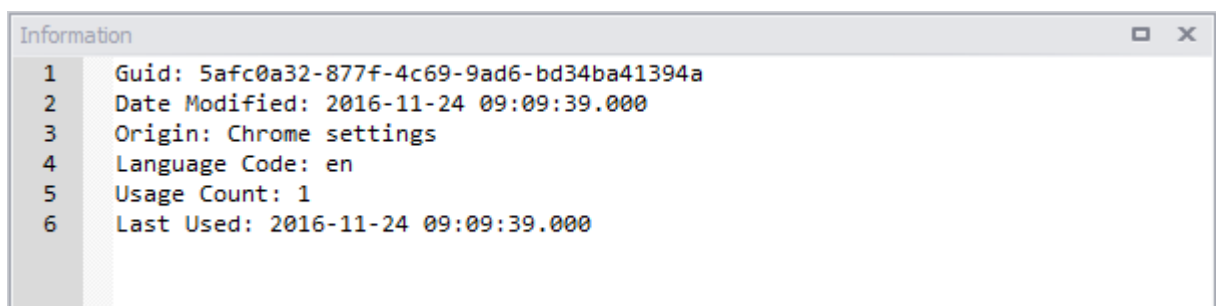


Figure 35

Warnings

The Warnings Panel holds additional warning information relating to the selected record. This warning information allows the analyst to evaluate the forensic value of the displayed data. For example, with HstEx® recovered data, the warning information may indicate where records have been truncated, or partially overwritten. In some circumstances, NetAnalysis® can detect invalid data and will flag this with a warning. To show the Warnings Panel, select **View » Warnings** or **CTRL + Shift + W**.

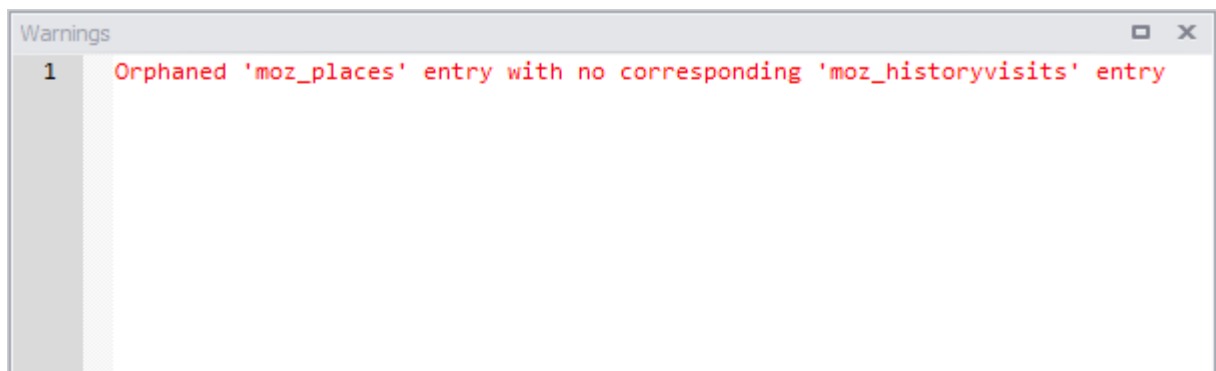


Figure 36

Filter Manager

The Filter Manager Panel shows an Explorer type window containing saved filter files and folders. From here, the user can create, edit, store and run previously saved filters. To show the Filter Manager Panel, select **View » Filter Manager** or **CTRL + Shift + F**.



Figure 37

Keyword Manager

The Keyword Manager Panel shows an Explorer type window containing saved keyword list files and folders. From here, the user can create, edit, store and run previously saved keyword list files. To show the Keyword Manager Panel, select **View » Keyword Manager** or **CTRL + Shift + K**.



Figure 38

Search Results

The Search Results Panel contains the results after a Keyword List has been executed. Each entry shows a keyword and the number of hits found for that keyword. To review the results for a specific keyword either double click that entry, or right click and select Search. The keyword will then be highlighted in the grid. To show the Search Results Panel, select **View » Search Results**.

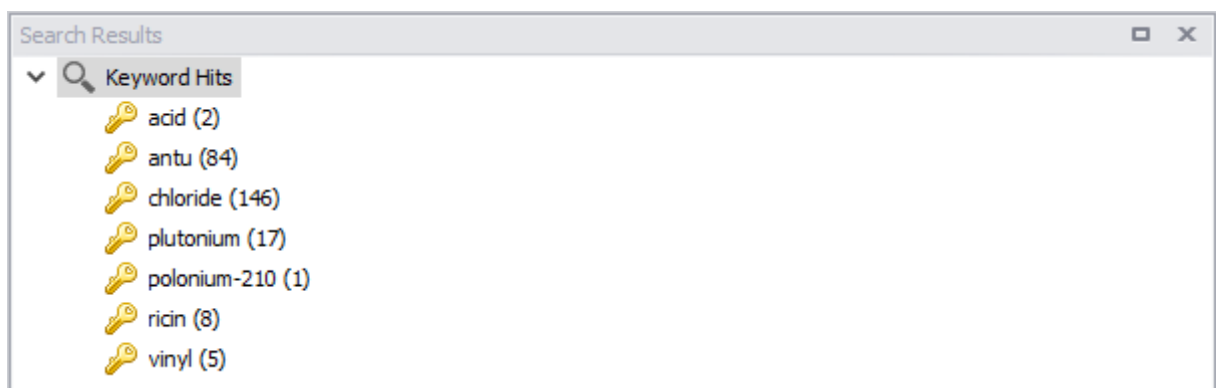


Figure 39

Report Manager

The Report Manager Panel shows an Explorer type window containing saved report template files. From here, the user can create, edit, store and run previously saved report template files. To show the Report Manager Panel, select **View » Keyword Manager** or **CTRL + Shift + R**.

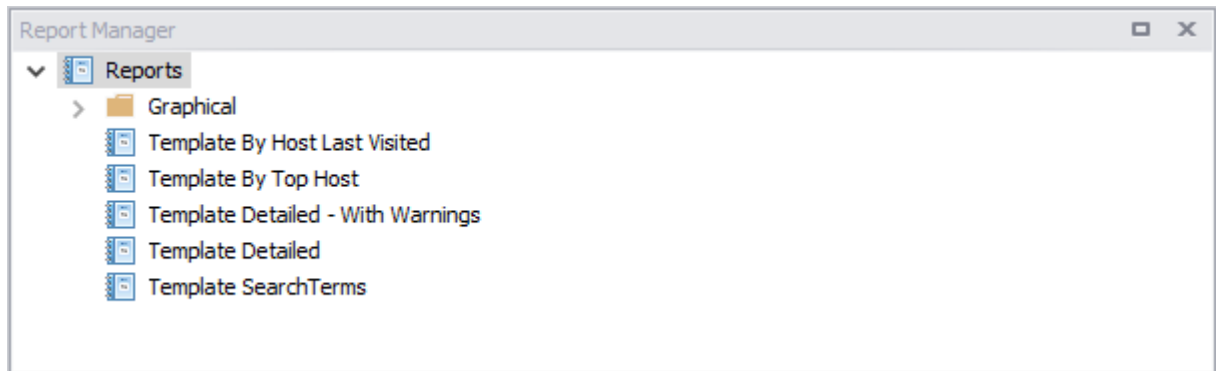


Figure 40

Navigating Through Rows and Cells

To move the focus between cells and rows use the **Arrow**, **Tab**, **Home**, **End**, **Page Up** and **Page Down** keys.

To move the focus to the next cell:

- Press **Tab**, or;
- Press the **Right Arrow**.

To move the focus to the previous cell:

- Press **Shift + Tab**, or;
- Press the **Left Arrow**.

To focus the first cell within the current row, press **Home**. To focus the last cell within the current row, press **End**. To focus the first row, press **CTRL + Home**. To focus the last row, press **CTRL + End**.

Resizing Columns

To resize columns, drag the right edge of the target column header.

















	Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]
▶	 History	 https	<input type="checkbox"/>	2016-11-22 16:07:07.000	2016-11-22 18:07:07.000
	 History Provider	 https	<input type="checkbox"/>	2016-11-22 16:07:07.000	2016-11-22 18:07:07.000
	 History	 https	<input type="checkbox"/>	2016-11-23 08:45:22.000	2016-11-23 10:45:22.000
	 History	 https	<input type="checkbox"/>	2016-11-23 08:45:22.000	2016-11-23 10:45:22.000
	 History Provider	 https	<input type="checkbox"/>	2016-11-23 08:45:22.000	2016-11-23 10:45:22.000
	 History	 https	<input type="checkbox"/>	2016-11-22 16:12:55.000	2016-11-22 18:12:55.000
	 History	 https	<input type="checkbox"/>	2016-11-22 16:12:55.000	2016-11-22 18:12:55.000
	 History Provider	 https	<input type="checkbox"/>	2016-11-22 16:12:55.000	2016-11-22 18:12:55.000

Figure 41

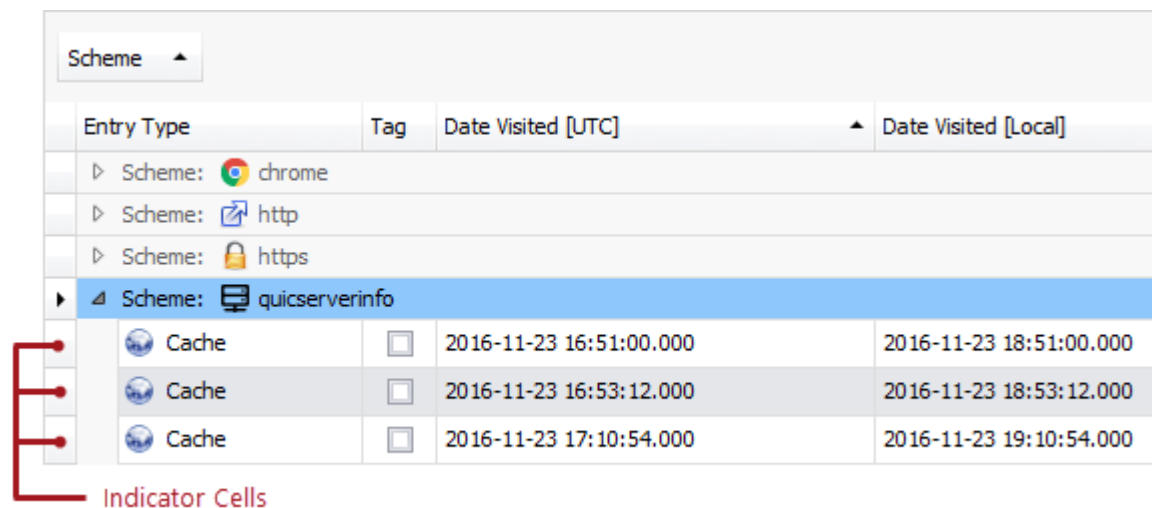
To change a column's width so that it displays the contents in its entirety, do one of the following:

- Double click the right edge of the column header.
- Right click the column's header and select **Best Fit**.

To change the widths of all columns so that they display their contents in the best possible way, right click the header of any column and select **Best Fit (all columns)**.

Selecting Rows

Multiple rows can be selected simultaneously. To select a row and clear an existing selection, click the row's indicator cell or any of its data cells (see Figure 42).



Entry Type	Tag	Date Visited [UTC]	Date Visited [Local]
Scheme: chrome			
Scheme: http			
Scheme: https			
Scheme: quicserverinfo			
Cache	<input type="checkbox"/>	2016-11-23 16:51:00.000	2016-11-23 18:51:00.000
Cache	<input type="checkbox"/>	2016-11-23 16:53:12.000	2016-11-23 18:53:12.000
Cache	<input type="checkbox"/>	2016-11-23 17:10:54.000	2016-11-23 19:10:54.000

Indicator Cells

Figure 42

To select a row and preserve the current selection, click on the row's indicator cell or any of its data cells while holding down the **CTRL** key.

To select all rows, press **CTRL + A**. To select a continuous range of rows, do the following:

- Use the **Arrow**, **Page Up**, **Page Down** keys while holding the **Shift** key down.
- To select all rows between the currently focused row and another one, click the target row while holding the **Shift** key down.

Expanding and Collapsing Group Rows in Grid Views

Do one of the following to expand/collapse a group row:

- Click the rows expand button (see Figure 43).
- Double click the group row.
- Double click the indicator cell corresponding to the group row (see Figure 42).
- Select the group row so that it has focus and press the **Plus** key (to expand the row) or **Minus** key (to collapse the row).
- Select the group row so that it has the focus and press the **Right arrow** (to expand the row) or **Left arrow** (to collapse the row).

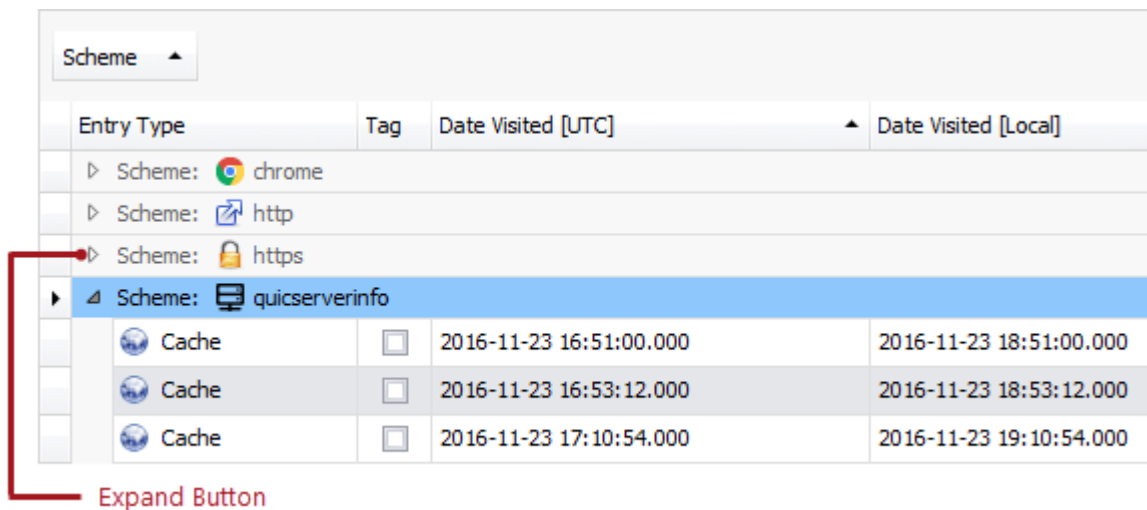


Figure 43

To expand or collapse all group rows, right click the group panel at the top of the control. This opens the group panel context menu; then select **Full Expand** or **Full Collapse** respectively.

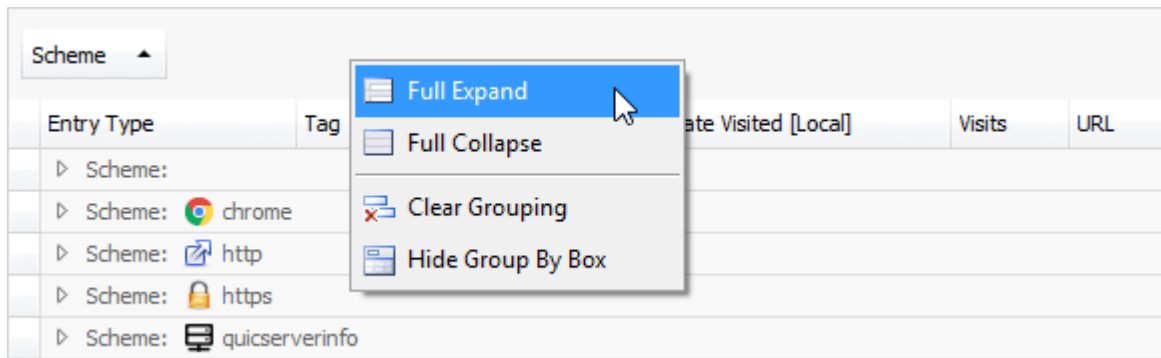


Figure 44

Sorting

To sort records by column values and replace existing sort conditions that are applied to the current or other columns, click the target column's header until an Up or Down Arrow icon is displayed within the header.

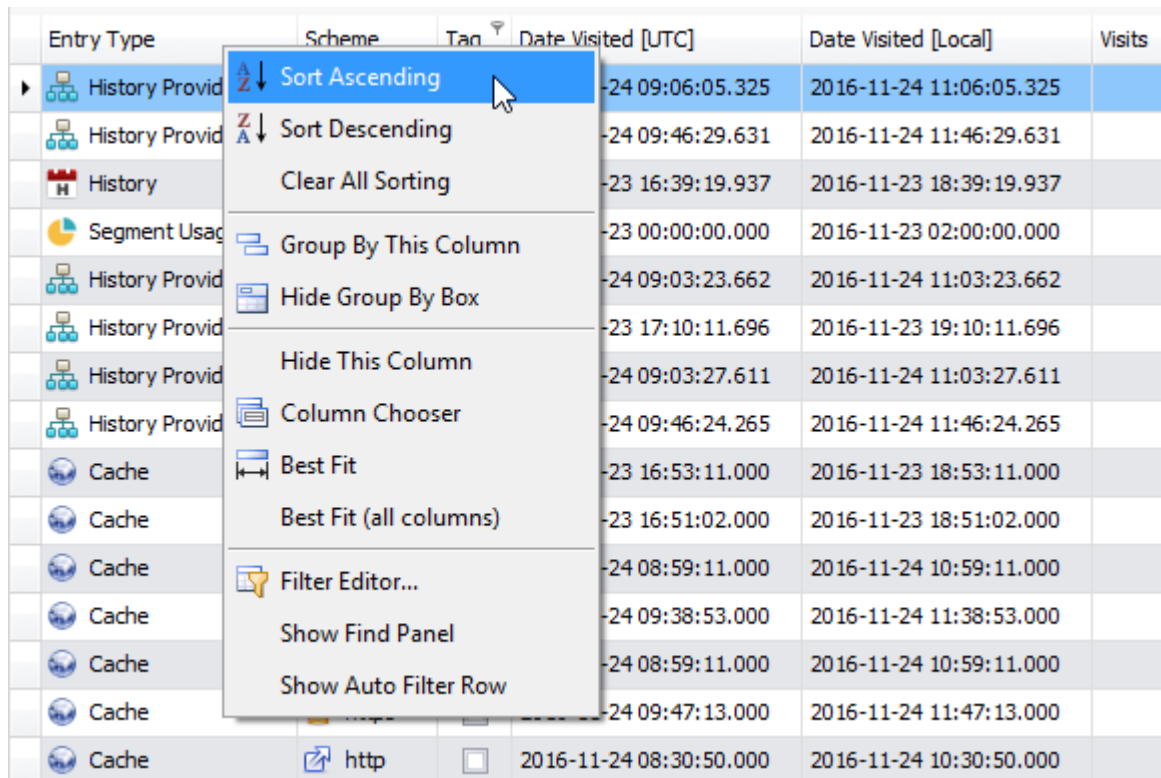
The Up and Down Arrows indicate ascending and descending sort orders respectively.

Visits
33
22
18
18
5
4

Figure 45

To sort records by column values while preserving existing sort conditions, do one of the following:

- Click a column header while holding the **Shift** key down, until an Up or Down Arrow icon is displayed within the header.
- Right click a column header and select **Sort Ascending** or **Sort Descending** from the context menu that will appear.



Entry Type	Scheme	Tan	Date Visited [UTC]	Date Visited [Local]	Visits
History Provid			-24 09:06:05.325	2016-11-24 11:06:05.325	
History Provid			-24 09:46:29.631	2016-11-24 11:46:29.631	
History			-23 16:39:19.937	2016-11-23 18:39:19.937	
Segment Usag			-23 00:00:00.000	2016-11-23 02:00:00.000	
History Provid			-24 09:03:23.662	2016-11-24 11:03:23.662	
History Provid			-23 17:10:11.696	2016-11-23 19:10:11.696	
History Provid			-24 09:03:27.611	2016-11-24 11:03:27.611	
History Provid			-24 09:46:24.265	2016-11-24 11:46:24.265	
Cache			-23 16:53:11.000	2016-11-23 18:53:11.000	
Cache			-23 16:51:02.000	2016-11-23 18:51:02.000	
Cache			-24 08:59:11.000	2016-11-24 10:59:11.000	
Cache			-24 09:38:53.000	2016-11-24 11:38:53.000	
Cache			-24 08:59:11.000	2016-11-24 10:59:11.000	
Cache			-24 09:47:13.000	2016-11-24 11:47:13.000	
Cache	http		2016-11-24 08:30:50.000	2016-11-24 10:30:50.000	

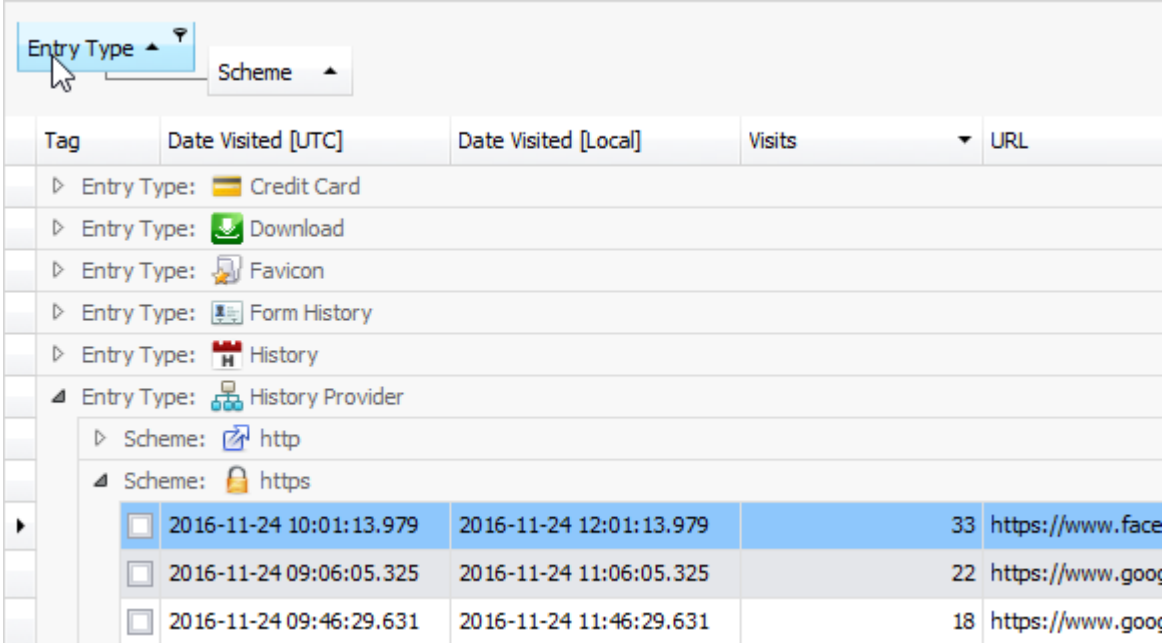
Figure 46

To remove sorting by a column, click a column header while holding down the **CTRL** key.

Grouping

Do one of the following to group by a specific column:

- Activate the Group by box by right clicking on a column header and selecting **Show Group By Box**.
- Drag a column header from the column header panel to the group panel.



Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
▷ Entry Type: Credit Card				
▷ Entry Type: Download				
▷ Entry Type: Favicon				
▷ Entry Type: Form History				
▷ Entry Type: History				
▲ Entry Type: History Provider				
▷ Scheme: http				
▲ Scheme: https				
<input type="checkbox"/> 2016-11-24 10:01:13.979	2016-11-24 10:01:13.979	2016-11-24 12:01:13.979	33	https://www.face
<input type="checkbox"/> 2016-11-24 09:06:05.325	2016-11-24 09:06:05.325	2016-11-24 11:06:05.325	22	https://www.goo
<input type="checkbox"/> 2016-11-24 09:46:29.631	2016-11-24 09:46:29.631	2016-11-24 11:46:29.631	18	https://www.goo

Figure 47

Alternatively, right click on a column header and select **Group By This Column** from the context menu.

Ungroup Data

To ungroup data by a grouping column, do one of the following:

- Drag a column header from the group panel to the column header panel.
- Right click a grouping column's header and select **UnGroup** from the context menu.

To remove grouping by all columns, right click the group panel and select **Clear Grouping** from the context menu.

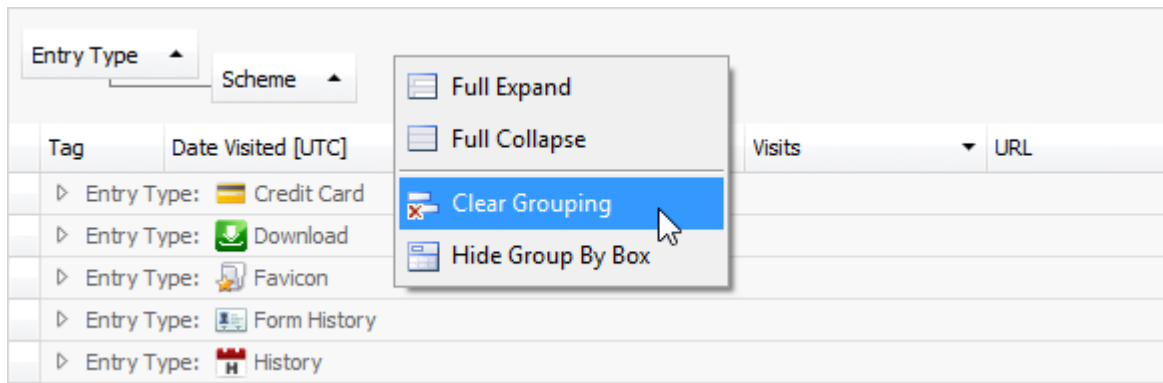


Figure 48

Change Grouping Order

To change group order, move a grouping column header to another position within the group panel.

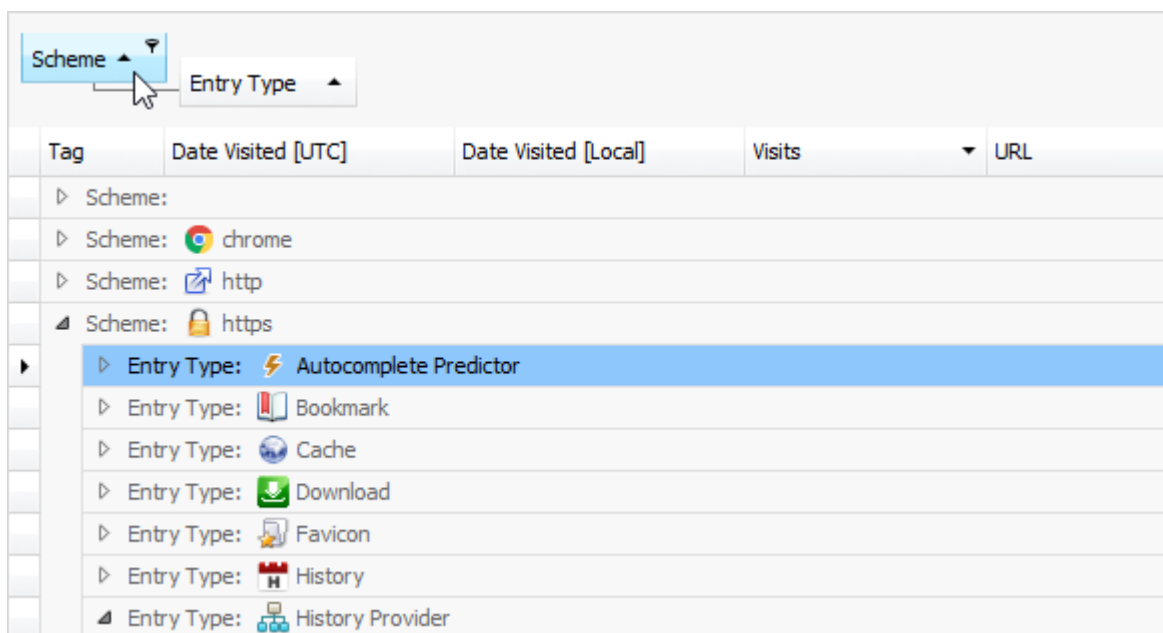


Figure 49

Time Zone Configuration

Introduction

In a forensic examination, establishing the time zone from the suspect system is one of the first tasks for a forensic examiner. If this information is not established at an early stage and taken into account, then the validity of all date/time values may be brought into question due to the way operating systems and browser applications store date/time information.

Date/Time Values

Operating systems and browser applications store date/time information in different ways using a variety of timestamp formats. Many timestamps are stored in UTC, and then converted to local time when presented to the user, and some are stored in local time. It is therefore vital to establish the correct time zone setting for the system to correctly convert these timestamps.

Universal Coordinated Time

Coordinated Universal Time (UTC) is the international standard upon which civil time is based and by which the world regulates time.

UTC is based upon UT1, which is the time determined by the rotation of the Earth. In accordance with international agreement, UTC and UT1 are not permitted to differ by more than 0.9 of a second. When it appears that the difference is approaching this limit, a one second change is introduced to bring the two back into alignment. On average, this occurs once every 12 - 18 months. Since the 1st January 1972, there have been 27 positive leap-second adjustments. The last leap second was inserted on 31st December 2016 at 23:59:60 UTC.

UTC is the time standard used for many Internet and World Wide Web protocols. The Network Time Protocol (NTP) is designed to synchronise clocks and computers over the Internet and encodes time using the UTC system. It is widely used as it avoids confusion with time zones and daylight saving changes.

Each local time is represented as an offset from UTC, with some zones making adjustments during the year for daylight saving.

Greenwich Mean Time is a widely used historical term, however, due to ambiguity, its use is no longer recommended in technical contexts.

Daylight Saving and Standard Time

UTC does not change with a change of seasons; however, local time or civil time may change if a time zone jurisdiction observes Daylight Saving Time or summer time. For example, UTC is 5 hours ahead of local time on the east coast of the United States during the winter but 4 hours ahead during the summer. Not every time zone observes daylight saving.

To deal with the numerous time zone changes throughout the world, Microsoft periodically release a time zone update^[1] to accommodate Daylight Saving Time (DST) changes in several countries.

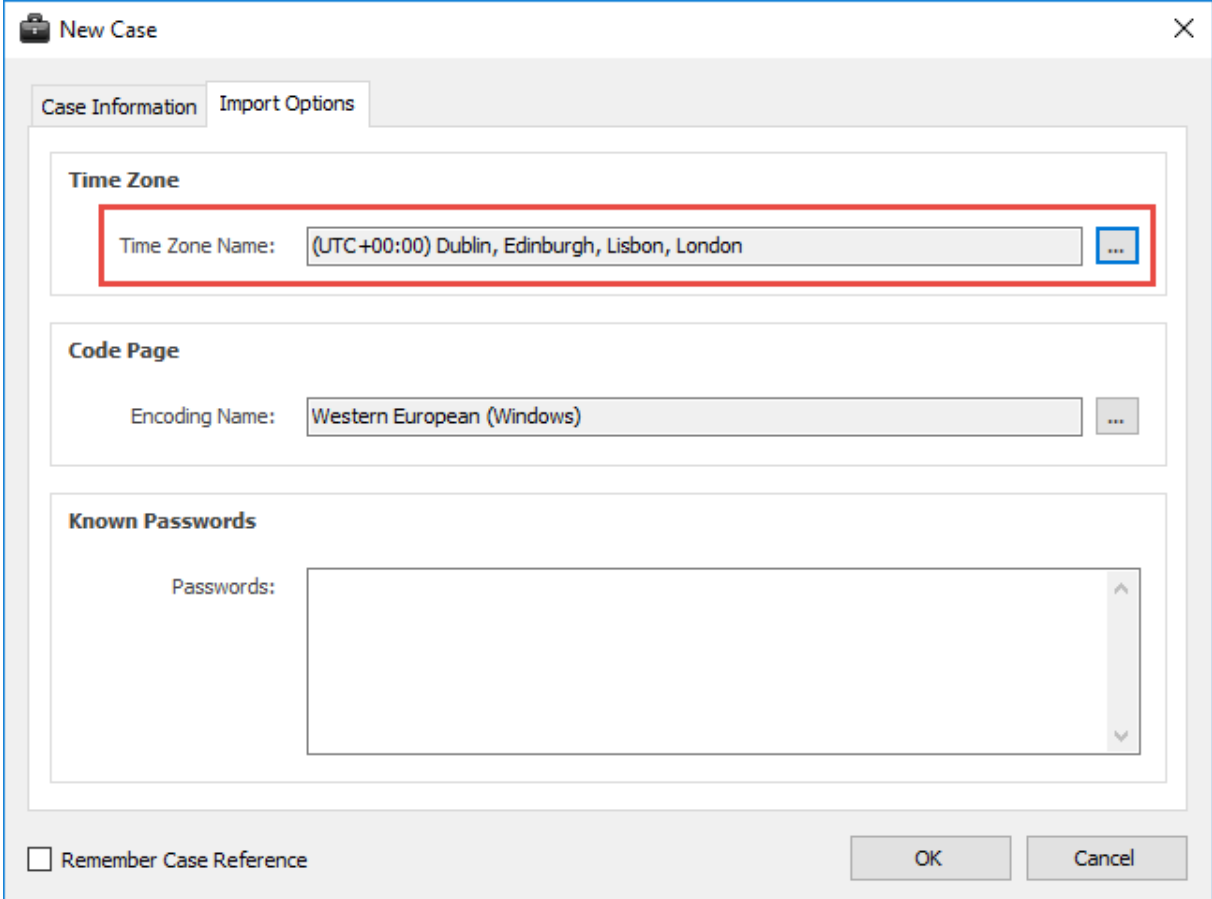
How NetAnalysis® Deals with Time Zones

NetAnalysis® provides the forensic examiner with the necessary tools to automatically convert UTC timestamps to local time (and vice versa) during import. It is important that NetAnalysis® is set to the time zone of the suspect system and not that of the forensic examiner's workstation.

In some situations, you may discover browser records from multiple time zones. In this situation, it is difficult to accurately convert between UTC and local time. NetAnalysis® has built-in functionality to easily deal with this scenario (see Dealing with Data from Mixed Time Zones on Page 99).

New Case Import Options

Once the time zone settings for the source system have been established, they can be used to set the time zone from the **Import Options** tab when creating a new case (see Figure 50).



The screenshot shows the 'New Case' dialog box with the 'Import Options' tab selected. The 'Time Zone' section is highlighted with a red rectangle. It contains a text box with the value '(UTC+00:00) Dublin, Edinburgh, Lisbon, London' and a small blue button with three dots to its right. Below this, the 'Code Page' section shows a text box with 'Western European (Windows)' and a similar button. The 'Known Passwords' section has a text area labeled 'Passwords:'. At the bottom, there is a checkbox labeled 'Remember Case Reference' and 'OK' and 'Cancel' buttons.

Figure 50



WARNING: If the time zone of the source computer is not identified prior to importing data into NetAnalysis® the timestamps may not be accurately represented. It is very important that the time zone is set correctly in the Import Options shown in Figure 50.

Clicking on the button to the right of the **Time Zone Name** text box will bring up the list of available time zones.

Each entry can be expanded to review the settings for that time zone. In the example in Figure 51, we can see that the **Base UTC Offset** for the time zone entry relating to Dublin, Edinburgh, Lisbon and London is 00:00:00.

This entry also has a flag to indicate that there are further adjustments to be made to take Daylight Saving into account.

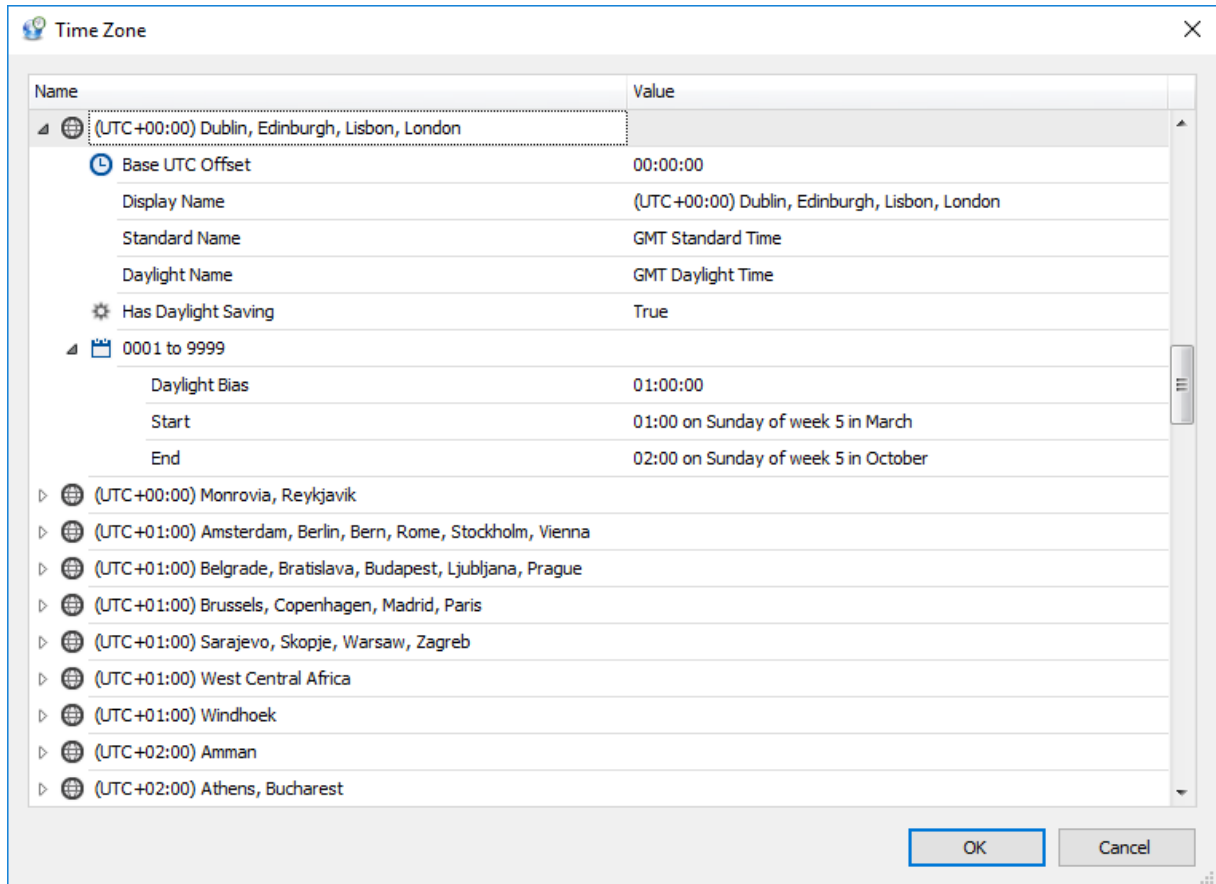


Figure 51

The Daylight Saving information for this time zone is highlighted in Figure 52.

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

Figure 52

This shows that for all years from 1 through to 9999, there will be a 1 hour Daylight Bias applied; this starts at 01:00 hours on the last Sunday in March and ends at 02:00 hours on the last Sunday in October. This entry has only one entry for daylight saving.

▲	🌐 (UTC-05:00) Eastern Time (US & Canada)	
⌚	Base UTC Offset	-05:00:00
	Display Name	(UTC-05:00) Eastern Time (US & Canada)
	Standard Name	Eastern Standard Time
	Daylight Name	Eastern Daylight Time
⚙️	Has Daylight Saving	True
▲	📅 0001 to 2006	
	Daylight Bias	01:00:00
	Start	02:00 on Sunday of week 1 in April
	End	02:00 on Sunday of week 5 in October
▲	📅 2007 to 9999	
	Daylight Bias	01:00:00
	Start	02:00 on Sunday of week 2 in March
	End	02:00 on Sunday of week 1 in November

Figure 53

Other time zones have multiple entries. Figure 53 shows the time zone entry for Eastern Time (US & Canada). This time zone has two daylight saving entries for year 1 through to 2006 and 2007 through to 9999.

Identification of Source Time Zone

When examining the Microsoft Windows NT family of systems, the time zone information can be established by reviewing the SYSTEM registry hive. To enable us to identify the correct Time Zone Information sub-key, we need to establish which Control Set was active when the computer was seized.

Control Sets

A control set contains system configuration information such as device drivers and services^[2]. You may notice several instances of control sets when viewing the registry. Some are duplicates or mirror images of others and some are unique.

Control sets are stored in the HKEY_LOCAL_MACHINE sub tree, under the System key. There may be several control sets depending on how often the user changed their system. A typical installation of Windows NT will contain three:

Windows NT Control Sets
HKEY_LOCAL_MACHINE\System\ControlSet001
HKEY_LOCAL_MACHINE\System\ControlSet002
HKEY_LOCAL_MACHINE\System\CurrentControlSet

Table 6

ControlSet001 may be the last control set the system booted with, while ControlSet002 could be what is known as the last known good control set, or the control set that last successfully booted Windows NT.

The CurrentControlSet sub-key is a pointer to one of the ControlSetXXX keys and will only be visible when viewing a live registry. During a post-mortem examination, this key will not exist. In order to better understand how these control sets are used, you need to be aware of another sub-key, 'Select'.

Windows NT Select Sub-Key
HKEY_LOCAL_MACHINE\System\Select

Table 7

The Select sub-key contains the values (as can be seen in Figure 54) Current, Default, Failed and LastKnownGood.

Each of these values contains a REG_DWORD data type and refers to a specific control set. For example, if the Current value is set to 0x01, then CurrentControlSet would be pointing to ControlSet001. Similarly, if LastKnownGood was set to 0x02, then the last known good control set would be ControlSet002. The

Default value usually agrees with Current, and Failed refers to a control set that was unable to boot Windows NT successfully.

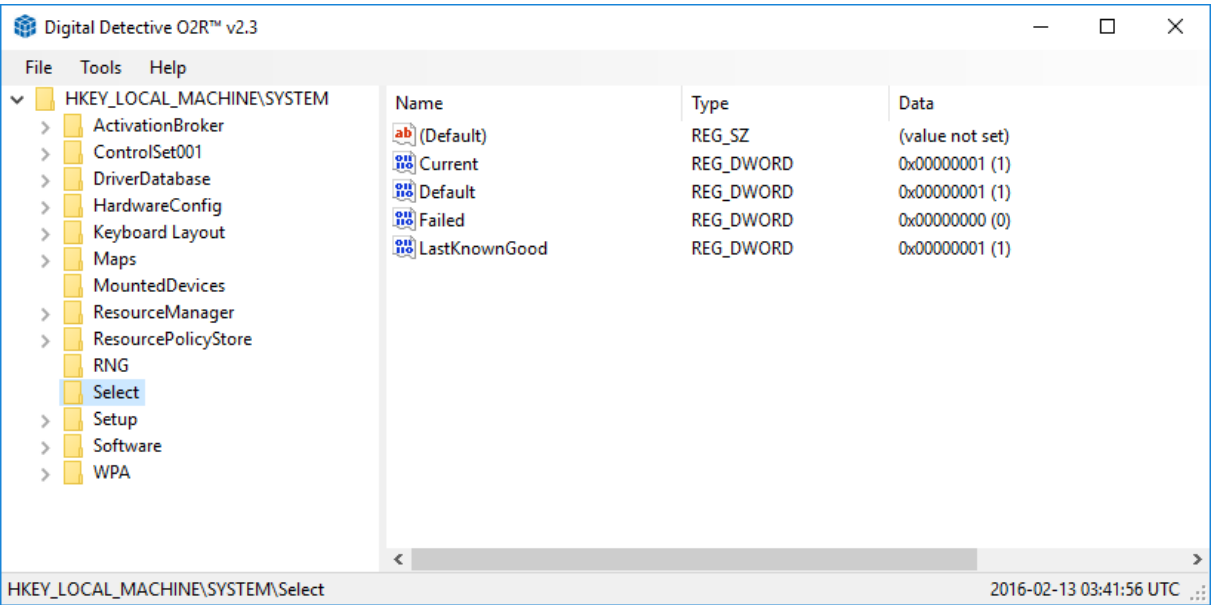


Figure 54

The most valuable set is CurrentControlSet as that reflects the active control set at the time the system was last active. If we examine the SYSTEM hive from our source, we can see that the 'Current' value is 0x01 which reflects ControlSet001 (see Figure 54).

Time Zone Information Sub-Key

Now that the CurrentControlSet has been identified, we can navigate to the sub-key containing the time zone information (see Table 8).

Windows NT TimeZoneInformation Sub-Key
HKEY_LOCAL_MACHINE\ControlSet001\Control\TimeZoneInformation

Table 8

Figure 55 show the various values stored under this sub-key.












Name	Type	Data
 (Default)	REG_SZ	(value not set)
 ActiveTimeBias	REG_DWORD	0xFFFFFFFF4C (4294967116)
 Bias	REG_DWORD	0xFFFFFFFF4C (4294967116)
 DaylightBias	REG_DWORD	0x0000003C (60)
 DaylightName	REG_SZ	@tzres.dll,-1501
 DaylightStart	REG_BINARY	00 00 01 00 01 00 00 00 00 00 00 00 00 00 05 00
 DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
 StandardBias	REG_DWORD	0x00000000 (0)
 StandardName	REG_SZ	@tzres.dll,-1502
 StandardStart	REG_BINARY	00 00 03 00 05 00 03 00 00 00 00 00 00 00 00 00
 TimeZoneKeyName	REG_SZ	Turkey Standard Time

Figure 55

ActiveTimeBias

This value is the current time difference from UTC in minutes, regardless of whether daylight saving is in effect or not. It is this value that helps establish the current time zone settings.

Bias

This value is the normal time difference from UTC in minutes. This value is the number of minutes that would need to be added to local time to return a UTC value.

StandardBias

This value is added to the value of the Bias member to form the bias used during standard time. In most time zones the value of this member is zero.

DaylightBias

This value specifies a bias value to be used during local time translations that occur during daylight time. This value is added to the value of the Bias member to form the bias used during daylight time. In most time zones, the value of this member is -60.

The ActiveTimeBias determines the offset of local time from UTC and is a dynamic value. It is calculated based on the values of the Bias, StandardBias and DaylightBias dependent upon whether Standard Time is in operation or not.

ActiveTimeBias Calculations for DST and Standard Time	
Daylight Saving	$\text{ActiveTimeBias} = \text{Bias} + \text{DaylightBias}$
Standard Time	$\text{ActiveTimeBias} = \text{Bias} + \text{StandardBias}$

Table 9

Table 9 shows the calculations for establishing the ActiveTimeBias during Daylight Saving and Standard Time.

Table 10 shows the calculations for converting between UTC and local time using the ActiveTimeBias. It is also possible to calculate the ActiveTimeBias when a UTC and local time are known.

UTC / Local Time Calculations with ActiveTimeBias
$\text{UTC} = \text{LocalTime} + \text{ActiveTimeBias}$
$\text{LocalTime} = \text{UTC} - \text{ActiveTimeBias}$
$\text{ActiveTimeBias} = \text{UTC} - \text{LocalTime}$

Table 10

DaylightName

The operating system uses this name during daylight saving months to display the current time zone setting (see Returning Daylight and Standard Name Values on Page 94).

DaylightStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that daylight saving will commence for this time zone.

StandardName

The operating system uses this name during non daylight saving months to display the current time zone setting (see Returning Daylight and Standard Name Values on Page 94).

StandardStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that standard time will commence for this time zone.

DynamicDaylightTimeDisabled

This is a Boolean value which indicates whether a DST adjustment is to be applied.

TimeZoneKeyName

This string relates to the sub-key in the SYSTEM hive where all of the available time zones are stored on a Windows NT system (see Table 11).

Windows NT Time Zones

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\{TimeZoneKeyName}

Table 11

Figure 56 shows the time zone registry sub-key for Turkey Standard Time.









Name	Type	Data
 (Default)	REG_SZ	(value not set)
 Display	REG_SZ	(UTC+03:00) Istanbul
 Dlt	REG_SZ	Turkey Daylight Time
 MUI_Display	REG_SZ	@tzres.dll,-2810
 MUI_Dlt	REG_SZ	@tzres.dll,-1501
 MUI_Std	REG_SZ	@tzres.dll,-1502
 Std	REG_SZ	Turkey Standard Time
 TZI	REG_BINARY	4C FF FF FF 00 00 00 3C 00 00 00 00 03 00 00 00 05 00 03 00 00 00 00 ...

Figure 56

Directly below the Turkey Standard Time sub-key, there is a Dynamic DST sub-key. This holds information and structures relating to the dynamic DST settings (See Figure 57).

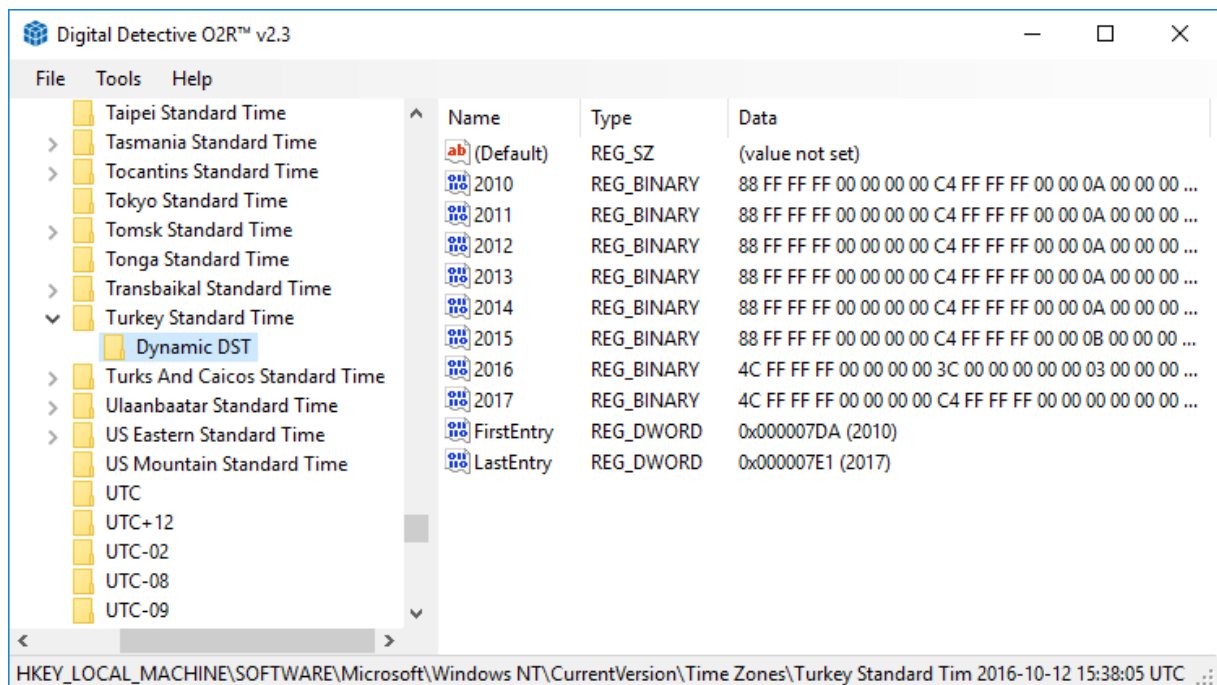


Figure 57

Dynamic DST

The implementation of Daylight Saving Time varies from country to country. Some countries may not observe Daylight Saving Time, whereas other countries may change the start dates and end dates for Daylight Saving Time every year.

Dynamic Daylight Saving Time provides support for time zones whose boundaries for Daylight Saving Time change from year to year. This feature enables easier updating of systems, especially for locales where the yearly DST boundaries are known in advance.

After the time zone has been updated, the current time zone setting is applied to all time operations, even when the time in question occurred before the time zone changed.

SYSTEMTIME Structure

The value containing the start date/time for DaylightStart or StandardStart is stored in a common structure called SYSTEMTIME^[3]. This structure specifies a date and time, using individual members for the month, day, year, weekday, hour, minute, second, and millisecond. Figure 58 shows the structure.

```
1 typedef struct _SYSTEMTIME {
2     WORD wYear;
3     WORD wMonth;
4     WORD wDayOfWeek;
5     WORD wDay;
6     WORD wHour;
7     WORD wMinute;
8     WORD wSecond;
9     WORD wMilliseconds;
10 } SYSTEMTIME, *PSYSTEMTIME
```

Figure 58

In the following example (see Figure 59), the DaylightStart value is a REG_BINARY value containing a number of bytes. These bytes represent the various elements of the SYSTEMTIME structure. The WORD values are stored in Little Endian format.



Figure 59

Figure 59 shows the binary value for DaylightStart. Each WORD from the SYSTEMTIME structure is broken down in Table 12.

Bytes	Value	Information
Bytes 0 - 1	0x0000	Represents the year from a 1900 time base. This is only required if the change is year specific and will normally be zero.
Bytes 2 - 3	0x0003	Represents the month; in this case the third month is March.

Bytes	Value	Information
Bytes 4 - 5	0x0005	Represents the week (starts at 1 and 5 means last); in this case the last week.
Bytes 6 - 7	0x0001	Represents the hour; in this case 0100 hours.
Bytes 8 - 9	0x0000	Represents the minute value; in this case zero.
Bytes 10 - 11	0x0000	Represents the second value; in this case zero.
Bytes 12 - 13	0x0000	Represents the millisecond value; in this case zero.
Bytes 14 - 15	0x0000	Represents the day of the week (Sunday = 0); in this case Sunday.

Table 12

In our example, Daylight Saving Time (DST) will start on Sunday of the last week in March at 0100 hours.

Calculating Signed Integer Bias Values

Within digital systems, all data, whether they are numbers or characters are represented by binary digits. A problem arises when you want to store negative numbers.

Over the years, hardware designers have developed three different schemes for representing negative numbers: sign and magnitude, one's complement, and two's complement. The most common method for storing negative numbers is two's complement.

Two's Complement

With this method, the Most Significant Bit (MSB) is used to store the sign. If the MSB is set, then this represents a negative number. This method affords natural arithmetic operations with no special rules. To represent a negative number in two's complement notation the process is simple:

- Find the binary representation of the positive (+ve) value in n-bits
- Flip all the bits (change 1 to 0 and vice versa)
- Add 1

Figure 60 below shows the binary representation of the positive number 5.

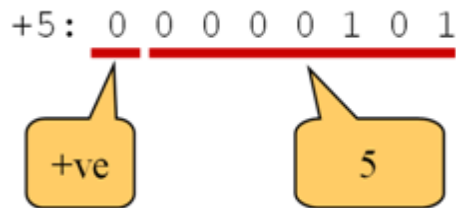


Figure 60

To represent this as a negative number (using 8 bits) then the procedure above is followed. Flip the bits and add one, as shown in Figure 61.

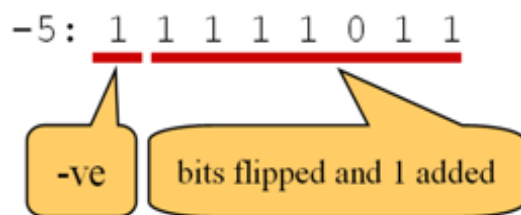


Figure 61

This method makes it simple to add positive and negative numbers together; for example:

$$\begin{array}{r}
 -5: \quad 11111011 \\
 +5: \quad +00000101 \\
 \hline
 \quad 00000000
 \end{array}$$

Figure 62

It also makes it very easy to convert between positive and negative numbers:

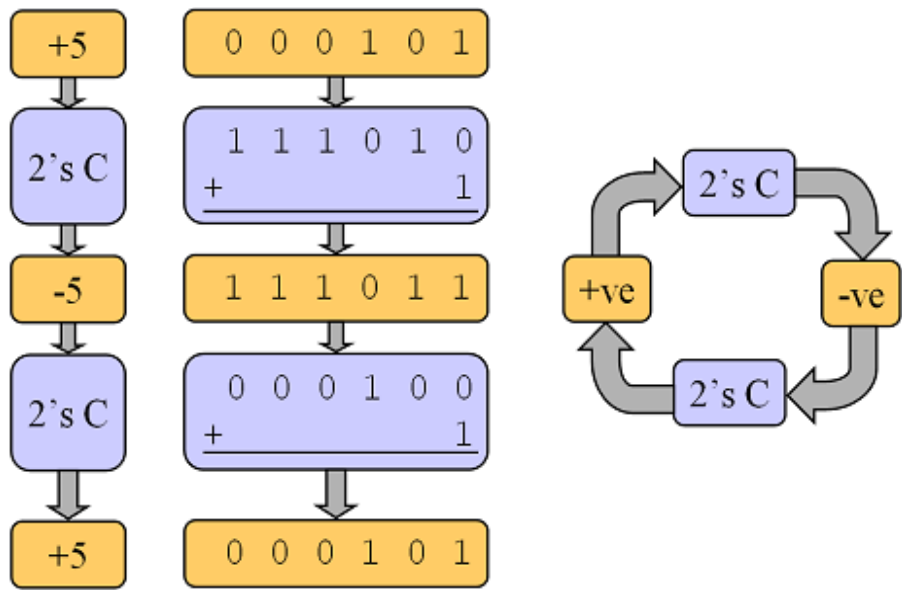


Figure 63

ActiveTimeBias

The ActiveTimeBias information is stored in the Time Zone Information sub-key as a REG_DWORD signed integer value. This value may be positive or negative. To establish the true value of the key, we must examine the information stored (see Figure 64).

 ActiveTimeBias	REG_DWORD	0xFFFFFC4 (4294967236)
--	-----------	------------------------

Figure 64

As the REG_DWORD value can store both signed and unsigned values, with no way to differentiate between each type, it is displayed in the registry viewer as an unsigned value. To establish the two's complement value, we must carry out the following calculation:

0xFFFFF4C (Signed Integer Value)

Figure 65

Convert this value to binary:

```
11111111 11111111 11111111 01001100
```

Figure 66

The MSB is set so we know that the above value will be negative. The next stage is to flip all the bits. This involves changing 1 to 0 and vice versa. This can be achieved quickly using the logical NOT function on a scientific calculator. You must ensure that it is set to deal with the correct number of bits.

```
00000000 00000000 00000000 10110011
```

Figure 67

Add 1 bit to the value above (dropping the leading zeros which are no longer required):

```
10110100
```

Figure 68

And then convert that value back to decimal, remembering that we are dealing with a negative number:

```
-180 (Minus 180)
```

Figure 69



Tip: If the MSB had been zero, then the value would have been positive. With a positive value, just convert it directly to decimal. If using a scientific calculator and using the logical NOT operator, ensure you are dealing with DWORD (32 bits).

Bias Calculations

Examination of the Bias values in our example indicates that DST is active and the local time for that zone is 3 hours ahead of UTC (see Table 13).

Bias	HEX Value	DEC Value	Information
ActiveTimeBias	0xFFFFFFFF4C	-180	Local time is 3 hours ahead of UTC
Bias	0xFFFFFFFF88	-120	2 hours ahead of UTC during Standard Time
DaylightBias	0xFFFFFFFFC4	-60	1 hour ahead of Standard Time when DST active
StandardBias	0x00000000	0	No change for Standard Time

Table 13

Returning Daylight and Standard Name Values

In earlier versions of Windows NT, both DaylightName and StandardName values contain the actual strings relating to those items. In later versions, these values were changed to reference a string of text stored within a string table embedded within a DLL (see Figure 70).

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xFFFFFFFF4C (4294967116)
Bias	REG_DWORD	0xFFFFFFFF4C (4294967116)
DaylightBias	REG_DWORD	0x0000003C (60)
DaylightName	REG_SZ	@tzres.dll,-1501
DaylightStart	REG_BINARY	00 00 01 00 01 00 00 00 00 00 00 00 00 00 05 00
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-1502
StandardStart	REG_BINARY	00 00 03 00 05 00 03 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Turkey Standard Time

Figure 70

For Windows 7, the string table is contained within a dynamic link library called 'tzres.dll'. If this file is opened in a resource viewer, we can examine the string table values. Figure 71 shows a small part of the string table when viewed from Microsoft Visual Studio. In Figure 70, DaylightName is stored as string 1501, with StandardName stored as string 1502. The corresponding values in the string table show 'Turkey Daylight Time' and 'Turkey Standard Time' (see Figure 56 on Page 87 for further references to this string table).

tzres.dll	Block ID	String ID	String
"MUI"	94	1490	(UTC+02:00) Athens, Bucharest
String Table	94	1500	(UTC+02:00) Istanbul
1	94	1501	Turkey Daylight Time
2	94	1502	Turkey Standard Time
3			
4			
5			

Figure 71

NetAnalysis® Active Time Bias Column

Another method for verifying the time zone settings is to examine the data from Microsoft Internet Explorer/Edge browser Daily entries. With these records, two of the stored dates relate to local time and UTC (see Figure 72). NetAnalysis® does not apply any time zone change to this entry type as it already contains a UTC and local time value.

NetAnalysis® v2.6 - Forensic Internet History Analysis - [New Case]						
File View Tools Search Index Filter Reports Column Window Help						
(UTC-07:00) Mountain Time (US Canada)						
Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Active Time Bias	URL
Daily	file		2007-07-12 23:14:17	2007-07-12 17:14:17	360 (UTC-06:00)	file:///E:/Business%20Ideas/untitled.bmp
Daily	host		2007-07-12 23:14:17	2007-07-12 17:14:17	360 (UTC-06:00)	Host: Computer
Daily	file		2007-07-12 23:14:53	2007-07-12 17:14:53	360 (UTC-06:00)	file:///E:/Business%20Ideas/Guts.bmp
Daily	file		2007-07-12 23:15:11	2007-07-12 17:15:11	360 (UTC-06:00)	file:///E:/Business%20Ideas/Camera.bmp
Daily	file		2007-07-12 23:29:42	2007-07-12 17:29:42	360 (UTC-06:00)	file:///E:/Business%20Ideas/ATM_THEFTS1.ppt
Daily	file		2007-07-12 23:28:14	2007-07-12 17:28:14	360 (UTC-06:00)	file:///C:/Users/Wes%20Mantooth/Desktop/ATM_THEFTS1.ppt
Daily	file		2007-07-12 23:48:55	2007-07-12 17:48:55	360 (UTC-06:00)	file:///C:/Users/Wes%20Mantooth/Documents/Dear%20Sweetie.doc
Daily	file		2007-07-12 23:31:25	2007-07-12 17:31:25	360 (UTC-06:00)	file:///C:/Users/Wes%20Mantooth/Desktop/Ape_20shoot.gif
Daily	http		2007-07-12 23:12:16	2007-07-12 17:12:16	360 (UTC-06:00)	http://www.google.com
Daily	host		2007-07-12 23:12:16	2007-07-12 17:12:16	360 (UTC-06:00)	Host: www.google.com
Daily	http		2007-07-12 23:15:24	2007-07-12 17:15:24	360 (UTC-06:00)	http://images.google.com/images?um=1&tab=wi&hl=en&q=z
Daily	http		2007-07-12 23:13:16	2007-07-12 17:13:16	360 (UTC-06:00)	http://www.snopes.com/crime/warnings/atmcamera.asp

Record 1 of 35

[X] [Entry Type] = 'Daily'

Information

1 Daily entry, date range: 2007-07-12 to 2007-07-13

www.digital-detective.net J:\[root]\Users\...\MSHist012007071220070713\index.dat FO: 20480

Figure 72

Table 14 shows the **Date Visited [UTC]** and **Date Visited [Local]** timestamps from the highlighted record in Figure 72.

UTC	Local	Local Time Difference	ActiveTimeBias
23:14:53 Hours	17:14:53 Hours	6 Hours (360 minutes) behind UTC	360

Table 14

The difference between UTC and local time is 360 minutes. As the local time is 360 minutes behind UTC, the ActiveTimeBias should be 360.

Examination of the registry for the source system shows that the time zone was set to Mountain Time and that daylight saving was active (see Figure 73).

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0x00000168 (360)
Bias	REG_DWORD	0x000001A4 (420)
DaylightBias	REG_DWORD	0xFFFFF4C4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-191
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 0...
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-192
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 ...
TimeZoneKeyName	REG_SZ	Mountain Standard Time

Figure 73

Time Zone Warnings

As NetAnalysis® imports data from Microsoft Internet Explorer and Edge Daily records, it checks the bias difference between the **Date Visited [UTC]** and **Date Visited [Local]** timestamps and calculates the value for the **Active Time Bias** column. This information is checked for validity against the time zone information which was set when the case was created. If the time zone has not been set correctly, or there are multiple time zone bias values encountered, NetAnalysis® will flag this potential issue and display a warning message when it completes importing.

Figure 74 shows the Importing Browser Files progress window. The warning messages can be seen at the end of the screen log.

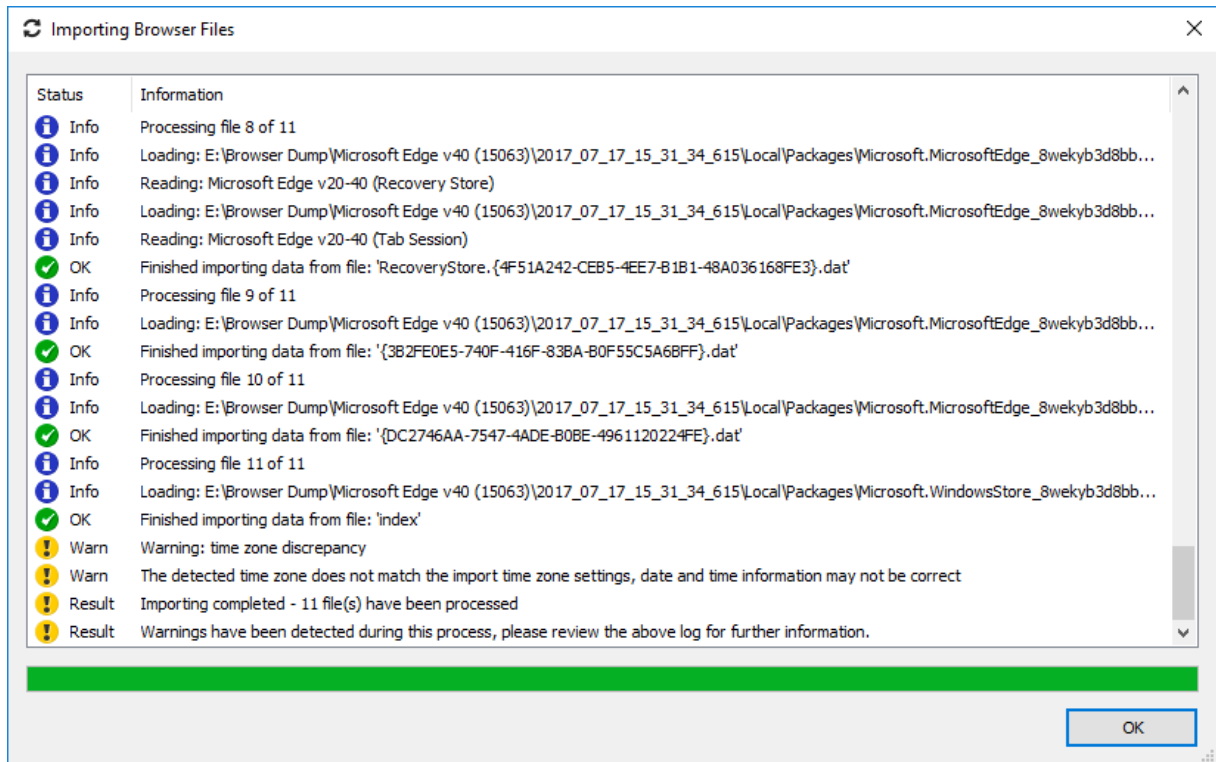


Figure 74



Note: Please verify the system time zone setting and the setting used when the case was created. Also, review the Active Time Bias column and associated warning field. This warning is displayed when a time zone setting is incorrectly applied.

To review only the records containing a time zone warning, create the following filter:

1. Open the Filter Editor by clicking **Filter » Filter Editor**.
2. Click the **+** button next to **And**.
3. Change the fields to show: **[Active Time Bias] Contains ***
4. Click the Apply button.

Your filter should look exactly like Figure 75.

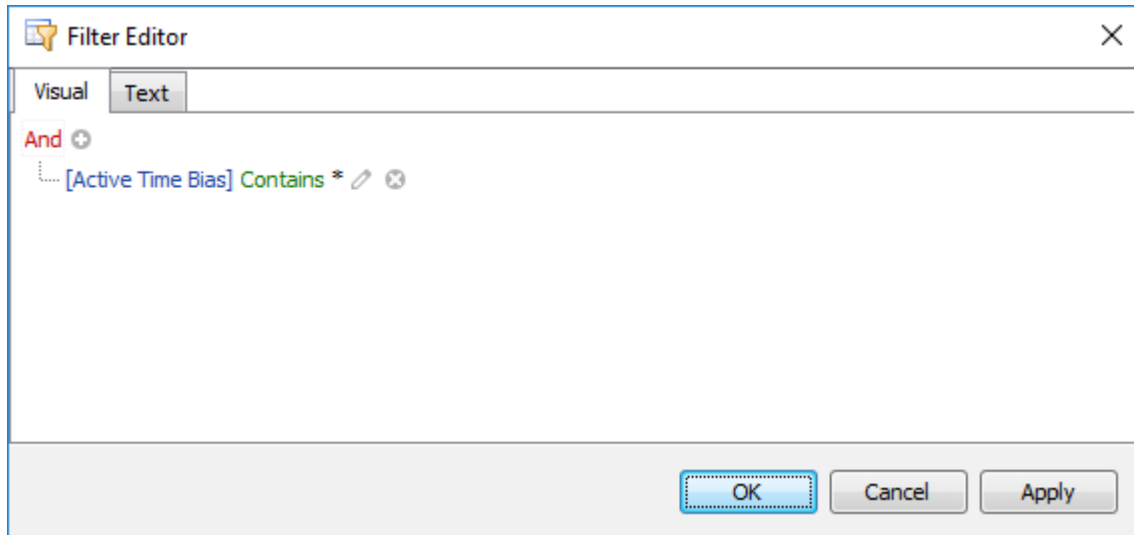


Figure 75

Open the Warnings panel by selecting **View » Warnings**. Navigate to the **Active Time Bias** column, as shown in Figure 76.

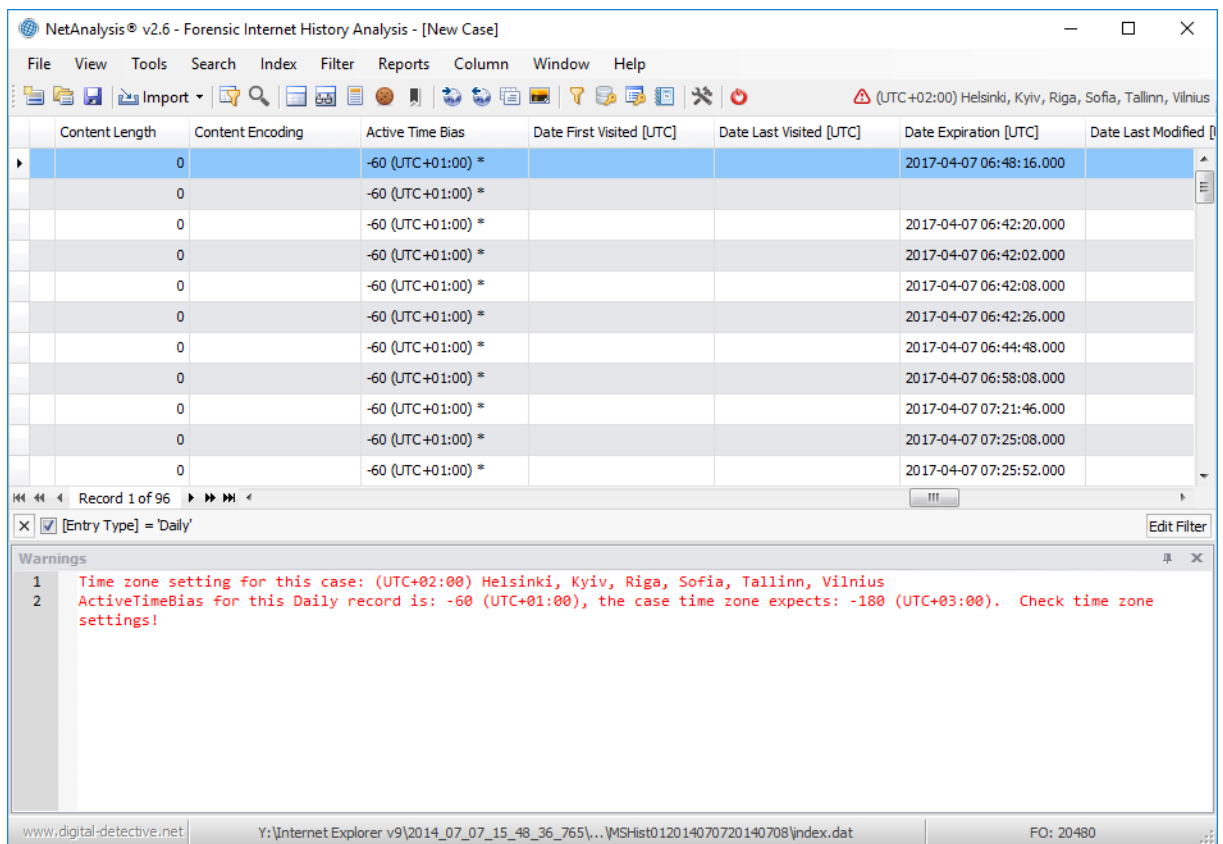


Figure 76

Dealing with Data from Mixed Time Zones

If you have evidence of multiple time zones being used, you may end up with miscalculated timestamps if you select any of the standard time zone settings.

The recommended course of action in this case is to set the NetAnalysis® time zone option to **No Time Zone Adjustment**. With this setting, the imported data will be shown exactly as it was stored in the original source.

To set the No Time Zone Adjustment setting, create a new case as follows:

1. Select **File » New Case**.
2. Click on the **Import Options** tab.
3. Click on the '...' button next to the Time Zone Name.
4. Scroll to the end of the list and select **No Time Zone Adjustment**.
5. Click **OK**.

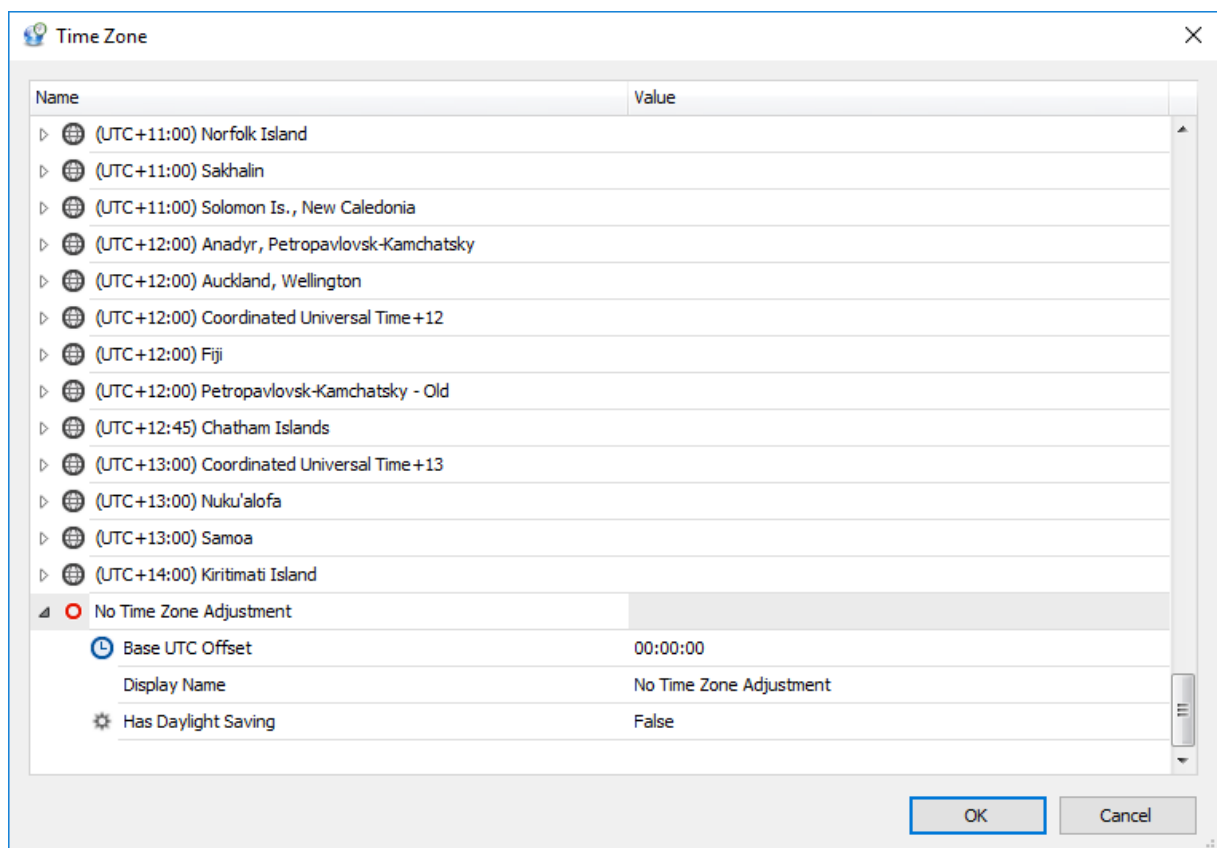


Figure 77

Encoding Configuration

Introduction

Understanding how Character Encoding works is an essential part of understanding digital evidence. It is part of the common core of skills and knowledge.

A character set is a collection of letters and symbols used in a writing system. For example, the ASCII character set covers letters and symbols for English text, ISO-8859-6 covers letters and symbols needed for many languages based on the Arabic script, and the Unicode character set contains characters for most of the living languages and scripts in the world.

Characters in a character set are stored as one or more bytes. Each byte or sequence of bytes represents a given character. A character encoding is the key that maps a particular byte or sequence of bytes to particular characters that the font renders as text.

There are many different character encodings. If the wrong encoding is applied to a sequence of bytes, the result will be unintelligible text.

ASCII

The American Standard Code for Information Interchange, or ASCII code, was created in 1963 by the American Standards Association Committee. This code was developed from the reorder and expansion of a set of symbols and characters already used in telegraphy at that time by the Bell Company.

At first, it only included capital letters and numbers, however, in 1967 lowercase letters and some control characters were added forming what is known as US-ASCII. This encoding used the characters 0 through to 127.

7-bit ASCII is sufficient for encoding characters, number and punctuation used in English, but is insufficient for other languages.

Extended ASCII

Extended ASCII uses the full 8-bit character encoding and adds a further 128 characters for non-English characters and symbols.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000016	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	
00000032	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	!"#\$%&'()*+,-./
00000048	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	0123456789:;<=>?
00000064	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	@ABCDEFGHIJKLMNO
00000080	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	PQRSTUVWXYZ[\]^_
00000096	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	`abcdefghijklmnopqrstuvwxyz
00000112	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F	pqrstuvwxyz{ }~
00000128	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F	¡ ¢ £ ¤ ¥ ¦ § ¨
00000144	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F	               
00000160	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	AF	               
00000176	B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	BA	BB	BC	BD	BE	BF	               
00000192	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF	               
00000208	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	DE	DF	               
00000224	E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	EE	EF	               
00000240	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF	               

Figure 78

Unicode

Fundamentally, computers just deal with numbers. They store letters and other characters by assigning a number for each one. Before Unicode was invented, there were hundreds of different encoding systems for assigning these numbers. No single encoding could contain enough characters: for example, Europe alone requires several different encodings to cover all its languages. Even for a single language like English no single encoding was adequate for all the letters, punctuation, and technical symbols in common use.

These encoding systems also conflict with one another. That is, two encodings can use the same number for two different characters, or use different numbers for the same character. Any given computer (especially servers) needs to support many different encodings; yet whenever data is passed between different encodings or platforms, that data always runs the risk of corruption. Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language.

The Unicode Standard is a character coding system designed to support the worldwide interchange, processing, and display of the written texts of the diverse languages and technical disciplines of the modern world. In addition, it supports classical and historical texts of many written languages^[4]. Unicode 10.0 adds 8,518 characters, for a total of 136,690 characters.

Unicode can be implemented by different character encodings; the Unicode standard defines UTF-8, UTF-16, and UTF-32 (Unicode Transformation Format).

Codepoint

The number assigned to a character is called a codepoint. An encoding defines how many codepoints there are, and which abstract letters they represent e.g. "Latin Capital Letter A". Furthermore, an encoding defines how the codepoint can be represented as one or more bytes.

Figure 79 shows the encoding of an uppercase letter **A** using standard ASCII.

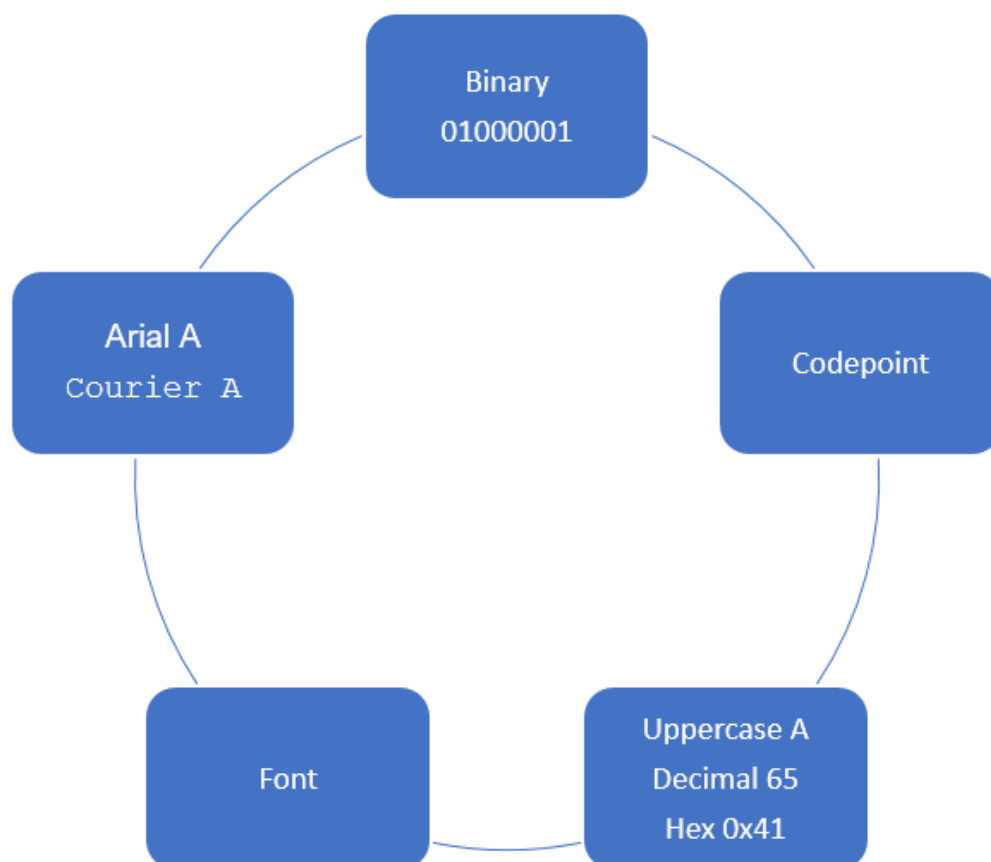


Figure 79

UTF-8, UTF-16 and UTF-32

UTF-8 is the most widely used encoding and is variable in length. It is capable of encoding all valid Unicode code points and can use between 1 and 4 bytes for each code point. The first 128 code points require 1 byte and match ASCII.

UTF-16 is also a variable-length and is capable of encoding all valid Unicode code points. Characters are encoded with one or two 16-bit code units. UTF-16 was developed from an earlier fixed-width 16-bit encoding known as UCS-2 (for 2-byte Universal Character Set).

UTF-32 is a fixed length encoding that requires 4 bytes for every Unicode code point.

Browser Data

It is important to understand character encoding when examining Internet and browser data. Browser applications use a variety of different encoding methods for storing data. For example, some browsers use UTF-16 for storing page titles and the default Windows encoding for storing URL data (e.g. Windows 1252). Windows 1252 is a 1-byte character encoding of the Latin alphabet, used by default in the legacy components of Microsoft Windows in English and some other Western languages.

To set the encoding value for NetAnalysis®, see the Code Page setting on Page 106 when creating a New Case.

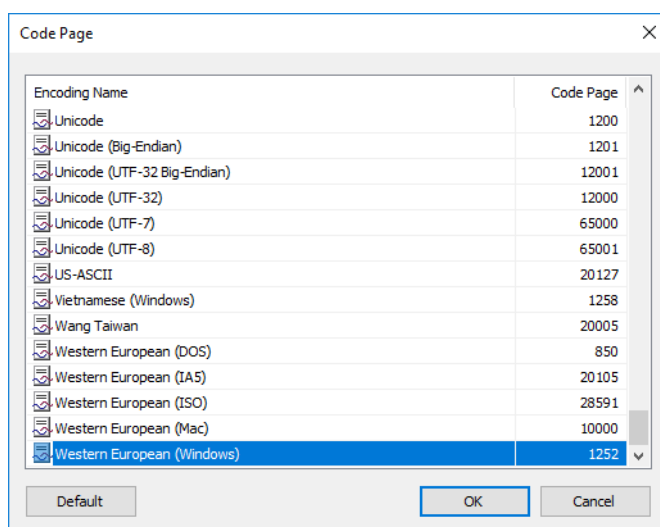


Figure 80

NetAnalysis® Quick Start

Introduction

This chapter provides a brief introduction to working with NetAnalysis® and explains the minimum steps required to import data.

Creating a New Case

Prior to importing any data, you need to create a new case; this can be done by selecting **New Case** from the **File** menu.

New Case

Case Information | Import Options

Case Reference

Auto-Generate ☒

Case Reference: CASE-20161205

Evidence Reference: ID-091950

Agency Information

Examiner Name: Craig Wilson

Agency Name: Digital Detective

Case Folders

Export Folder: D:\Export ...

Temporary Folder: D:\Temp ...

☐ Remember Case Reference

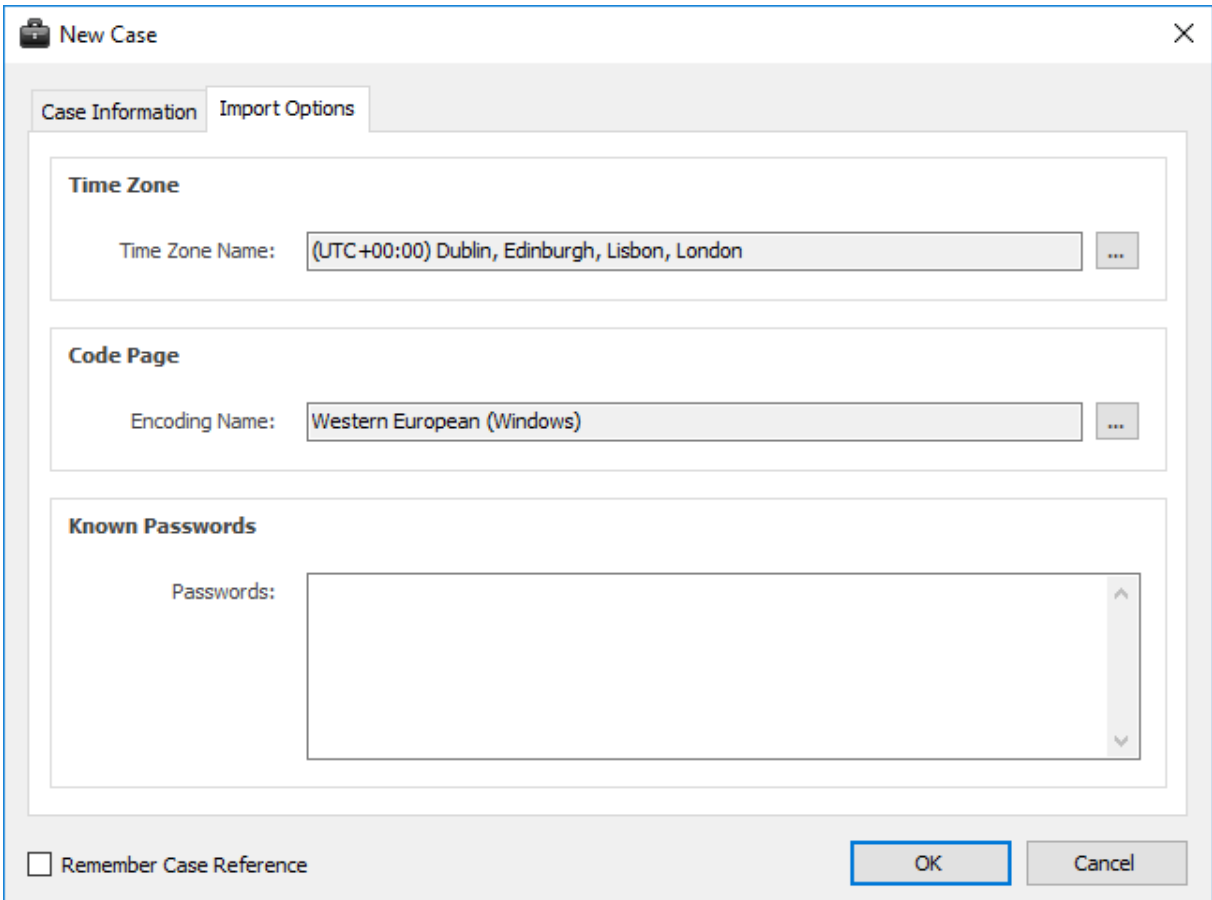
OK Cancel

Figure 81

This allows you to set the case reference and agency/company information. You can also set the location for the export folder and temporary folders. During import, NetAnalysis® will export a number of artefacts such as web page previews, thumbnails and extracted text from search indices. The Auto-Generate option allows NetAnalysis® to create case and evidence references for you. This information should be replaced by your own reference values.

Import Options

The second tab shows the various import options which can be set. The time zone and encoding can be set, prior to importing any data. It is important to establish the time zone of the target system prior to importing any data as this has a direct effect on the calculation of local time stamps. The code page default will be set to UTF-8. The **Known Passwords** box is for adding any known Master Passwords to allow NetAnalysis® to automatically decrypt username and password information.



The screenshot shows the 'New Case' dialog box with the 'Import Options' tab selected. The dialog has a title bar with a folder icon and the text 'New Case'. Below the title bar are two tabs: 'Case Information' and 'Import Options'. The 'Import Options' tab contains three sections: 'Time Zone', 'Code Page', and 'Known Passwords'. The 'Time Zone' section has a label 'Time Zone Name:' followed by a text box containing '(UTC+00:00) Dublin, Edinburgh, Lisbon, London' and a dropdown arrow. The 'Code Page' section has a label 'Encoding Name:' followed by a text box containing 'Western European (Windows)' and a dropdown arrow. The 'Known Passwords' section has a label 'Passwords:' followed by a large empty text box with a vertical scrollbar. At the bottom of the dialog is a checkbox labeled 'Remember Case Reference' and two buttons: 'OK' and 'Cancel'.

Figure 82

Time Zone

Clicking on the button next to the time zone shows the following window. This allows the user to select the appropriate time zone and see the time zone settings and dynamic daylight saving options.

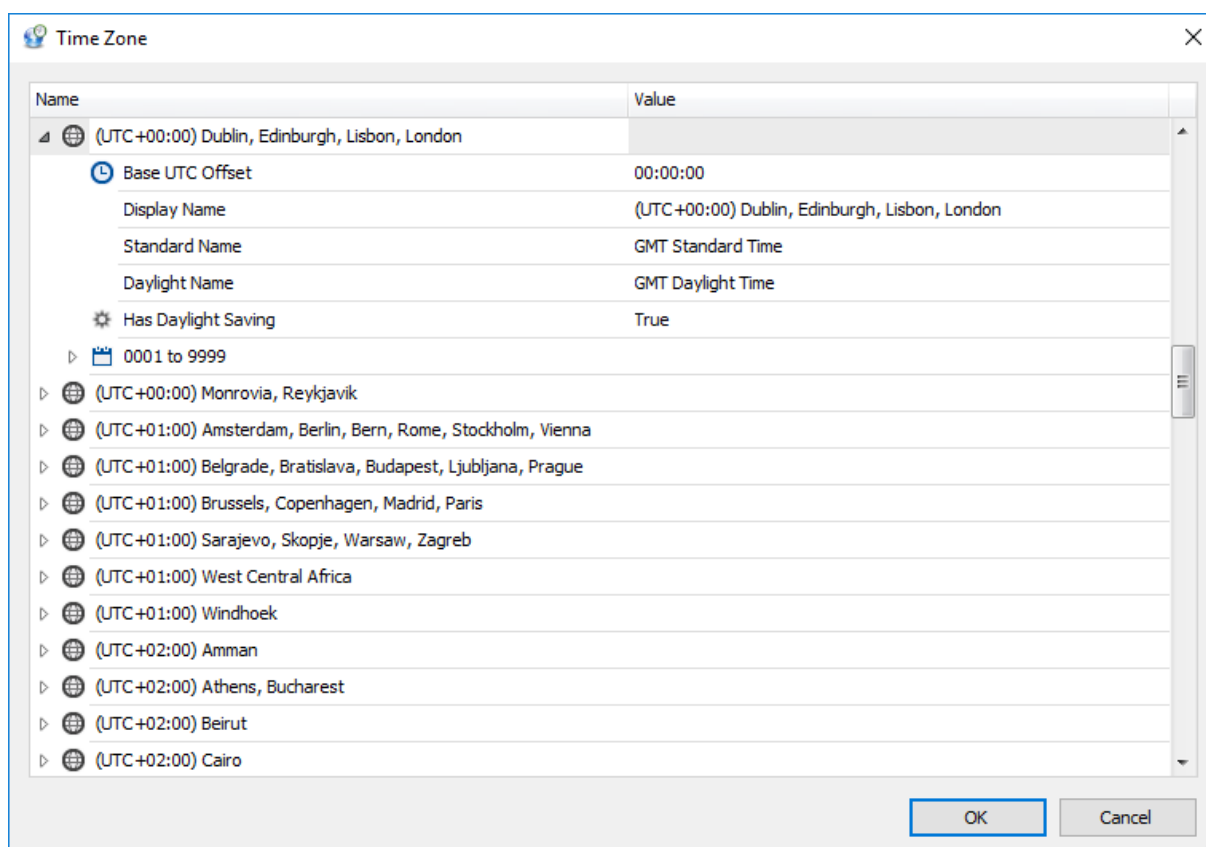


Figure 83

Code Page

Clicking the button next to the code page shows the following window (see Figure 84). This allows the user to select the appropriate code page (if required).

Please ensure you read the chapter on Character Encoding to fully understand what this means (see Encoding Configuration on Page 100).

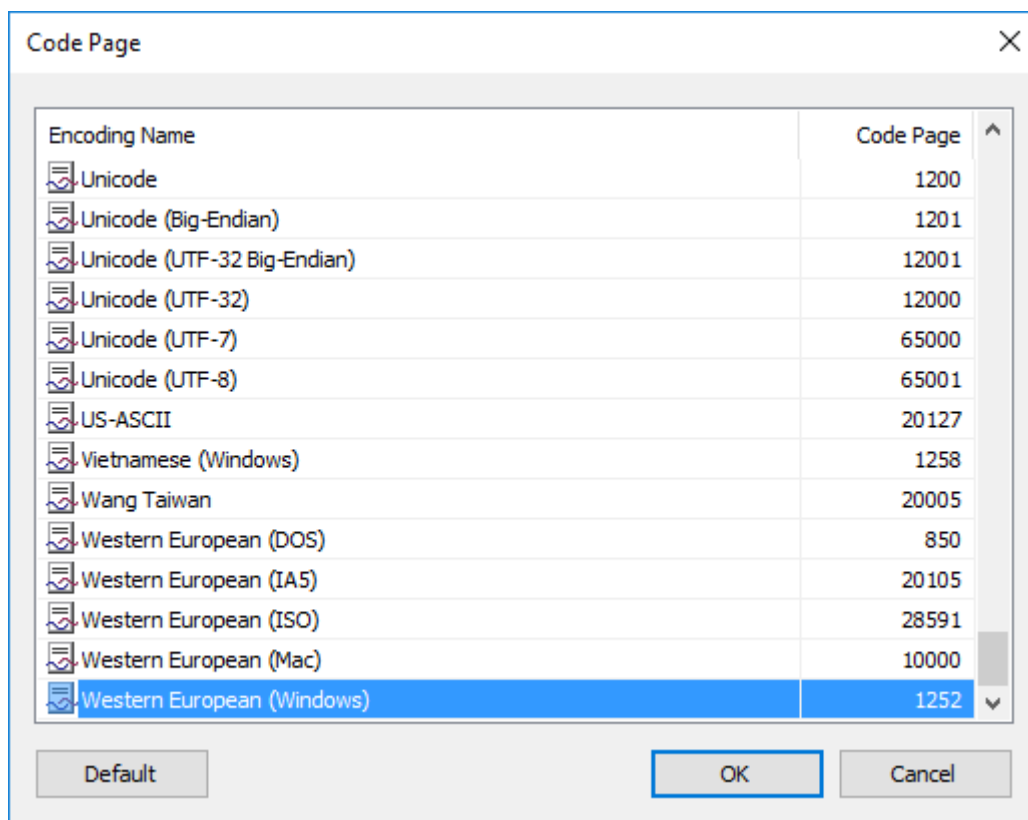


Figure 84

Importing Data

Once a new case has been created, data can be imported from an individual file, a collection of files, or recursively through a folder structure where supported file types are identified and imported. To import data, select either of the following:

- **File » Import » Data from File(s)**
- **File » Import » Data from Folder**

You can also import data by clicking on the **Import** drop-down button located on the toolbar (see Figure 85 below).

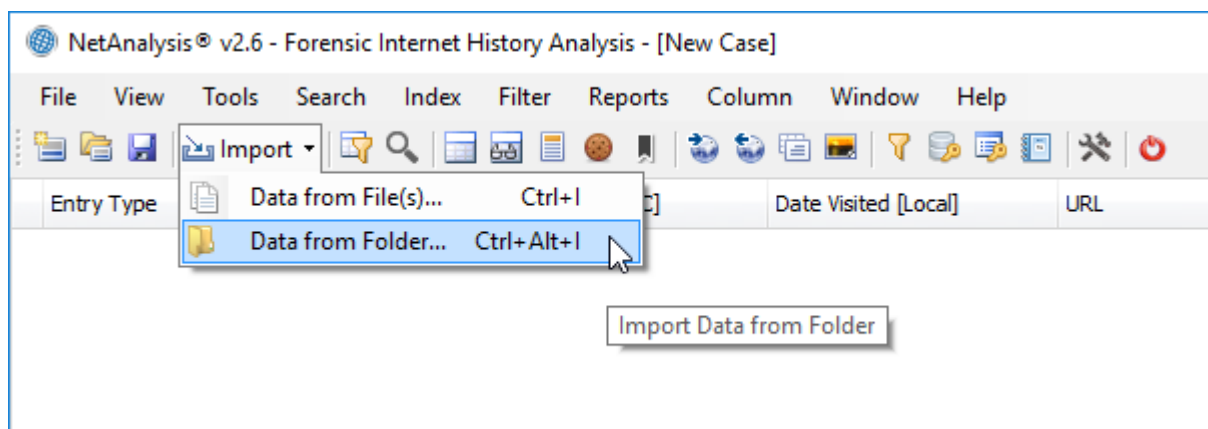


Figure 85

NetAnalysis® will then search the source looking for supported file types. Once this has completed, any identified files will be imported.

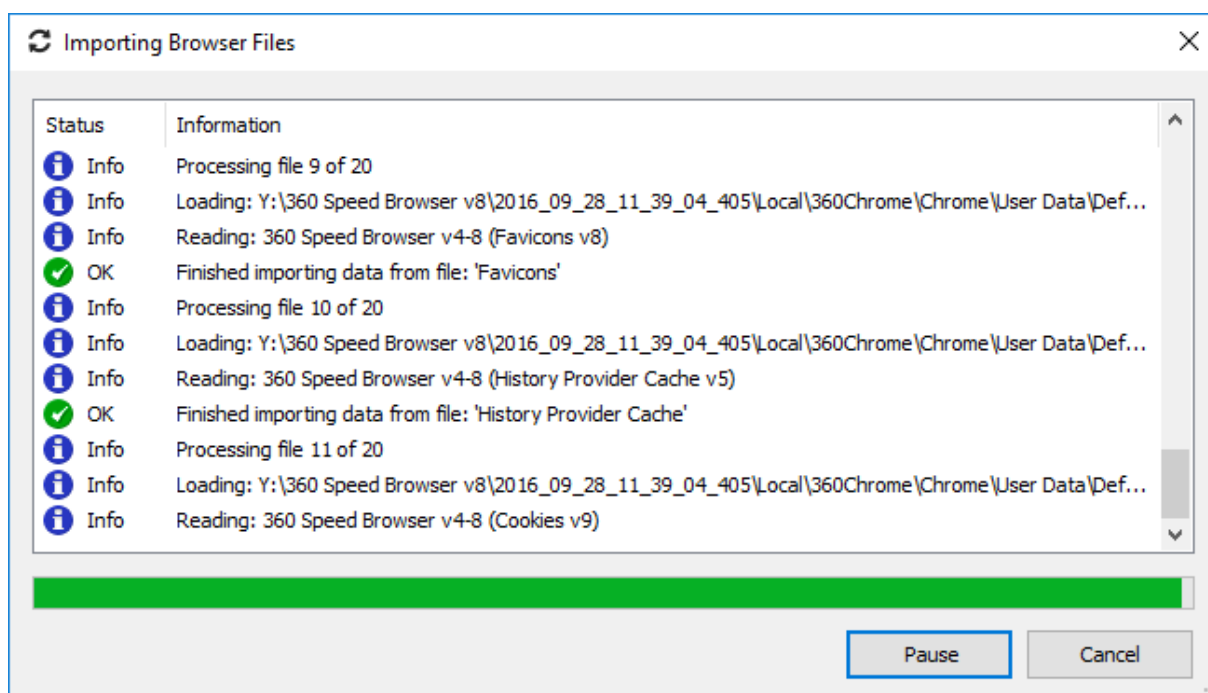
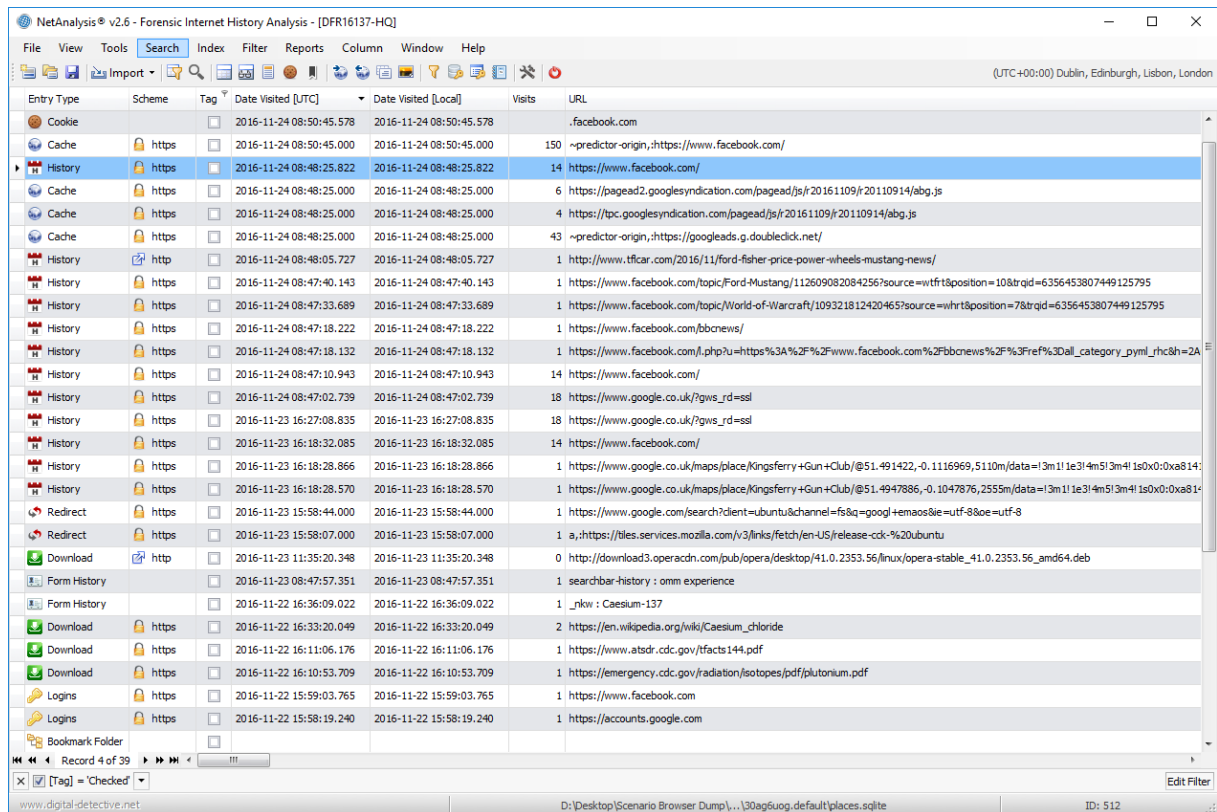


Figure 86

During the import process, NetAnalysis® displays a progress windows (as shown above in Figure 86). This window shows the progress of the import and flags to the user if any issues are encountered.

Reviewing the Imported Data

When the data has finished importing, NetAnalysis® will load the data into the main grid for review.



Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cookie			2016-11-24 08:50:45.578	2016-11-24 08:50:45.578		.facebook.com
Cache	https		2016-11-24 08:50:45.000	2016-11-24 08:50:45.000	150	~predictor-origin,https://www.facebook.com/
History	https		2016-11-24 08:48:25.822	2016-11-24 08:48:25.822	14	https://www.facebook.com/
Cache	https		2016-11-24 08:48:25.000	2016-11-24 08:48:25.000	6	https://pagead2.googlesyndication.com/pagead/js/20161109/2016110914/abg.js
Cache	https		2016-11-24 08:48:25.000	2016-11-24 08:48:25.000	4	https://tpc.googlesyndication.com/pagead/js/20161109/2016110914/abg.js
Cache	https		2016-11-24 08:48:25.000	2016-11-24 08:48:25.000	43	~predictor-origin,https://googleads.g.doubleclick.net/
History	http		2016-11-24 08:48:05.727	2016-11-24 08:48:05.727	1	http://www.tftcar.com/2016/11/ford-fisher-price-power-wheels-mustang-news/
History	https		2016-11-24 08:47:40.143	2016-11-24 08:47:40.143	1	https://www.facebook.com/topic/Ford-Mustang/112609082084256?source=wtfrt&position=10&trgid=6356453807449125795
History	https		2016-11-24 08:47:33.689	2016-11-24 08:47:33.689	1	https://www.facebook.com/topic/World-of-Warcraft/109321812420465?source=whrt&position=78&trgid=6356453807449125795
History	https		2016-11-24 08:47:18.222	2016-11-24 08:47:18.222	1	https://www.facebook.com/bbcnews/
History	https		2016-11-24 08:47:18.132	2016-11-24 08:47:18.132	1	https://www.facebook.com/.php?u=https%3A%2F%2Fwww.facebook.com%2Fbbcnews%2F%3Fref%3Dall_category_pym%3Fhrc%3D2A
History	https		2016-11-24 08:47:10.943	2016-11-24 08:47:10.943	14	https://www.facebook.com/
History	https		2016-11-24 08:47:02.739	2016-11-24 08:47:02.739	18	https://www.google.co.uk/?gws_rd=ssl
History	https		2016-11-23 16:27:08.835	2016-11-23 16:27:08.835	18	https://www.google.co.uk/?gws_rd=ssl
History	https		2016-11-23 16:18:32.085	2016-11-23 16:18:32.085	14	https://www.facebook.com/
History	https		2016-11-23 16:18:28.866	2016-11-23 16:18:28.866	1	https://www.google.co.uk/maps/place/Kingsferry+Gun+Club/@51.491422,-0.1116969,5110m/data=!3m1!1e3!4m5!3m4!1s0x0:0xa814:
History	https		2016-11-23 16:18:28.570	2016-11-23 16:18:28.570	1	https://www.google.co.uk/maps/place/Kingsferry+Gun+Club/@51.4947886,-0.1047876,2555m/data=!3m1!1e3!4m5!3m4!1s0x0:0xa814:
Redirect	https		2016-11-23 15:58:44.000	2016-11-23 15:58:44.000	1	https://www.google.com/search?client=ubuntu&channel=fs&q=googl+emaos&ie=utf-8&oe=utf-8
Redirect	https		2016-11-23 15:58:07.000	2016-11-23 15:58:07.000	1	a,https://tiles.services.mozilla.com/v3/links/fetch/en-US/release-ck-%20ubuntu
Download	http		2016-11-23 11:35:20.348	2016-11-23 11:35:20.348	0	http://download3.operacdn.com/pub/opera/desktop/41.0.2353.56/linux/opera-stable_41.0.2353.56_amd64.deb
Form History			2016-11-23 08:47:57.351	2016-11-23 08:47:57.351	1	searchbar-history : omm experience
Form History			2016-11-22 16:36:09.022	2016-11-22 16:36:09.022	1	_nlkw : Caesium-137
Download	https		2016-11-22 16:33:20.049	2016-11-22 16:33:20.049	2	https://en.wikipedia.org/wiki/Caesium_chloride
Download	https		2016-11-22 16:11:06.176	2016-11-22 16:11:06.176	1	https://www.atsdr.cdc.gov/tfacts144.pdf
Download	https		2016-11-22 16:10:53.709	2016-11-22 16:10:53.709	1	https://emergency.cdc.gov/radiation/isotopes/pdf/plutonium.pdf
Logins	https		2016-11-22 15:59:03.765	2016-11-22 15:59:03.765	1	https://www.facebook.com
Logins	https		2016-11-22 15:58:19.240	2016-11-22 15:58:19.240	1	https://accounts.google.com
Bookmark Folder						

Figure 87

Docking Panel Layout

NetAnalysis® v2 has a new docking panel layout. To view all of the available panels, select **Window » Show All Windows**. This will activate all of the docking panels as shown below in Figure 88.

The panels can be moved and docked to any desired location. They can even be pulled free from the main application and placed on a second monitor if required. Once you find a layout that you like, you can save it for later re-use. To save a layout, select **Window » Save Window Layout**.

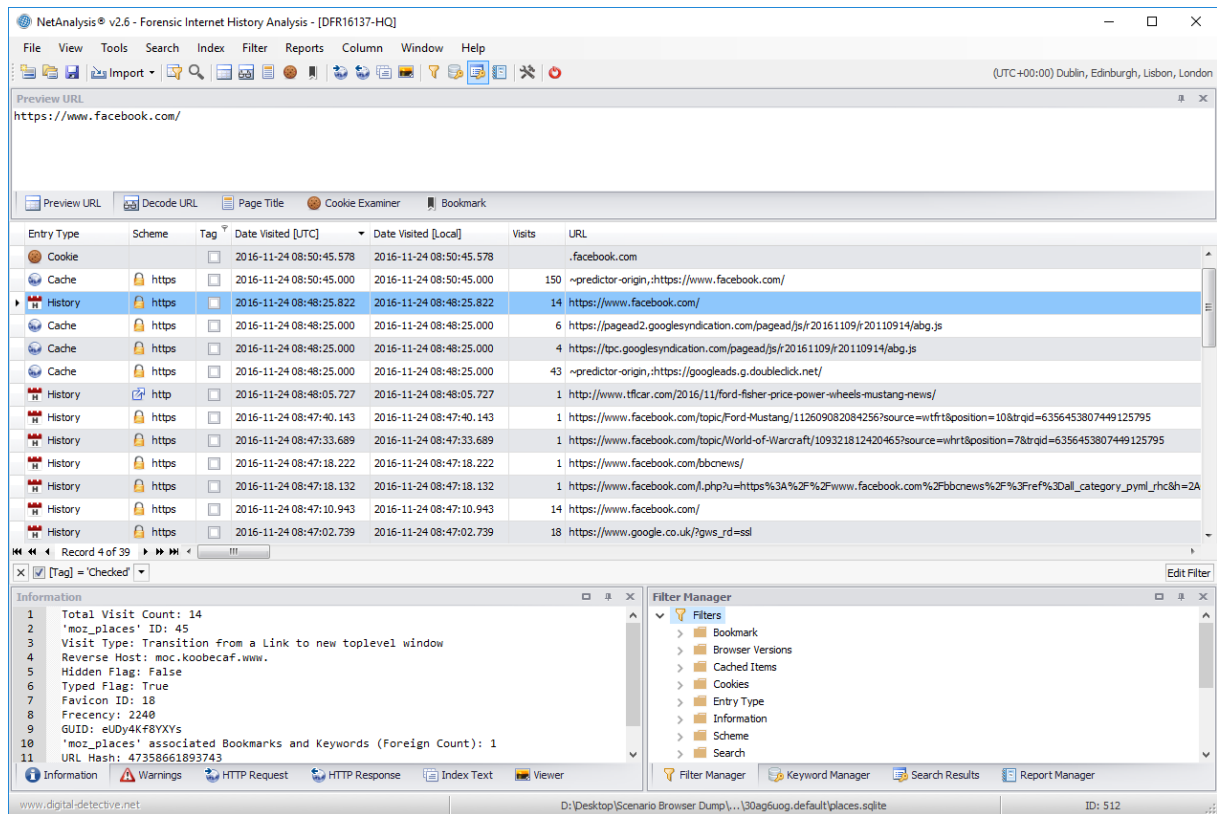


Figure 88

Quick Search

The built-in Search Panel provides an easy way of searching against multiple columns. To perform a quick search, select the following **Search » Quick Search**.

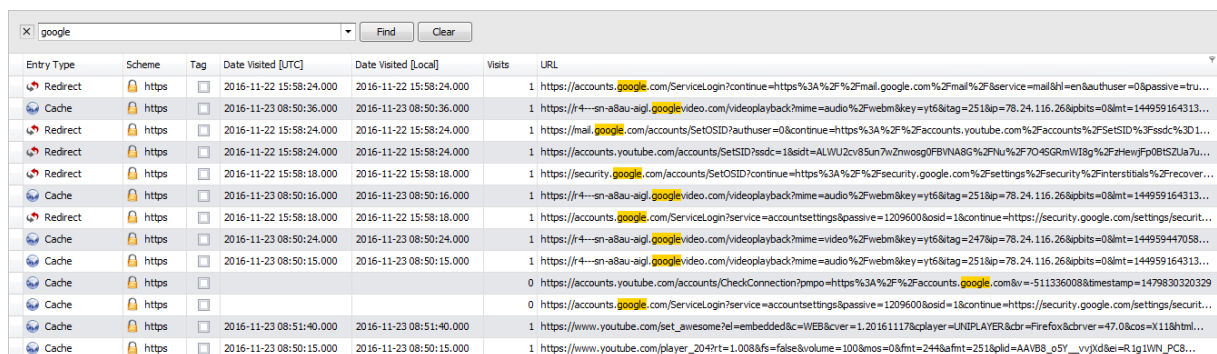


Figure 89

URL Examination and Analysis

To activate the URL Examination and Analysis window, right click on a record and select **Examine URL**. This will open the window shown below (Figure 90).

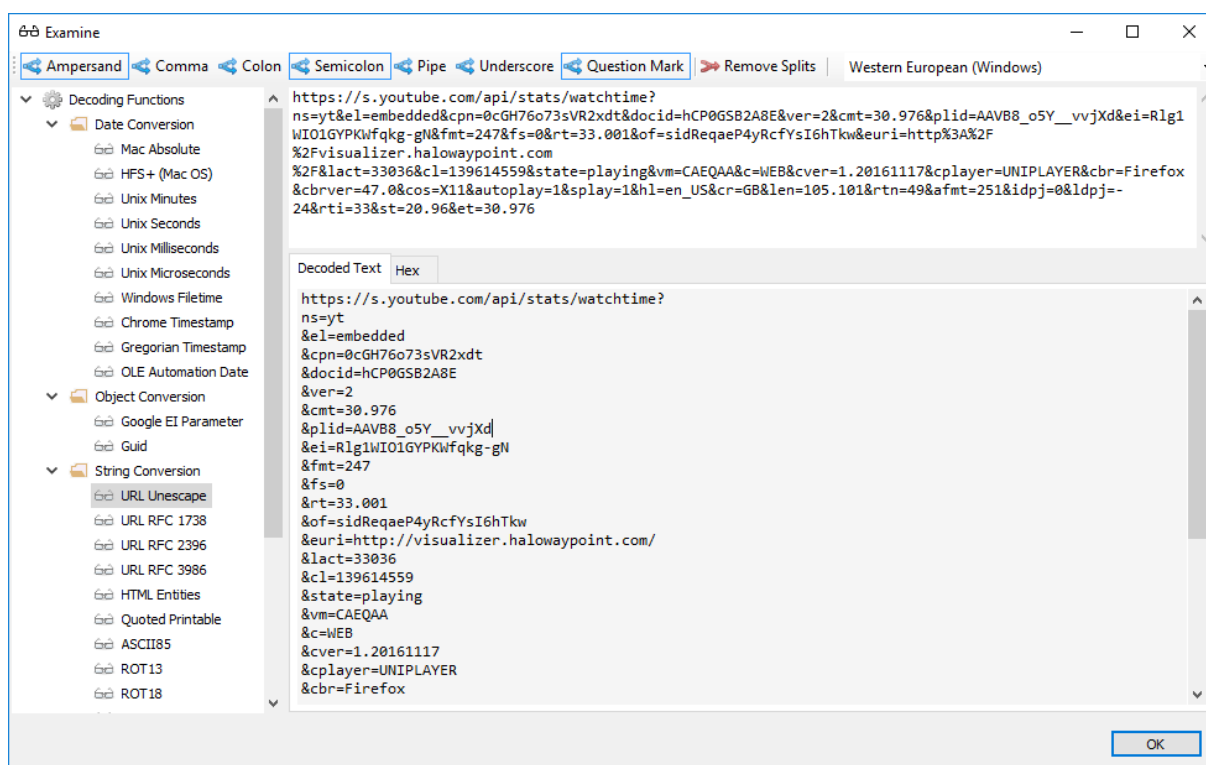


Figure 90

Cookie Examination and Analysis

An HTTP cookie is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it is used to tell if two requests came from the same browser, such as keeping a user logged in. It remembers stateful information for the stateless HTTP protocol.

To activate the Cookie Examination and Analysis window, select from the menu **View » Cookie Examiner**, or click **CTRL + Shift + C**.

When a cookie record is selected in the main grid, and there is a corresponding, existing cookie file (or cookie data), the Cookie Examiner will display one or more cookie records. Figure 91 below shows a

cookie record from Microsoft Edge. Microsoft Edge and Internet Explorer can contain multiple cookies in a single cookie file, whereas other browsers normally store cookie records individually. Some browsers encrypt the cookie values.

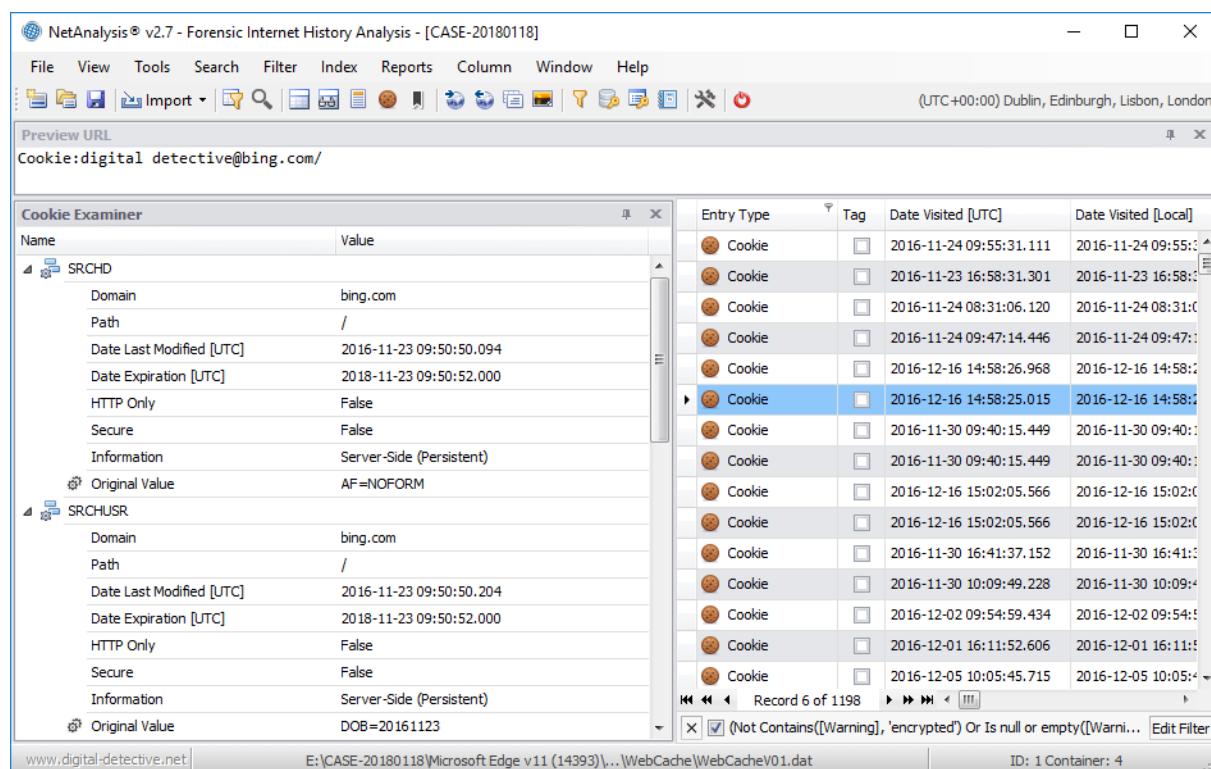


Figure 91

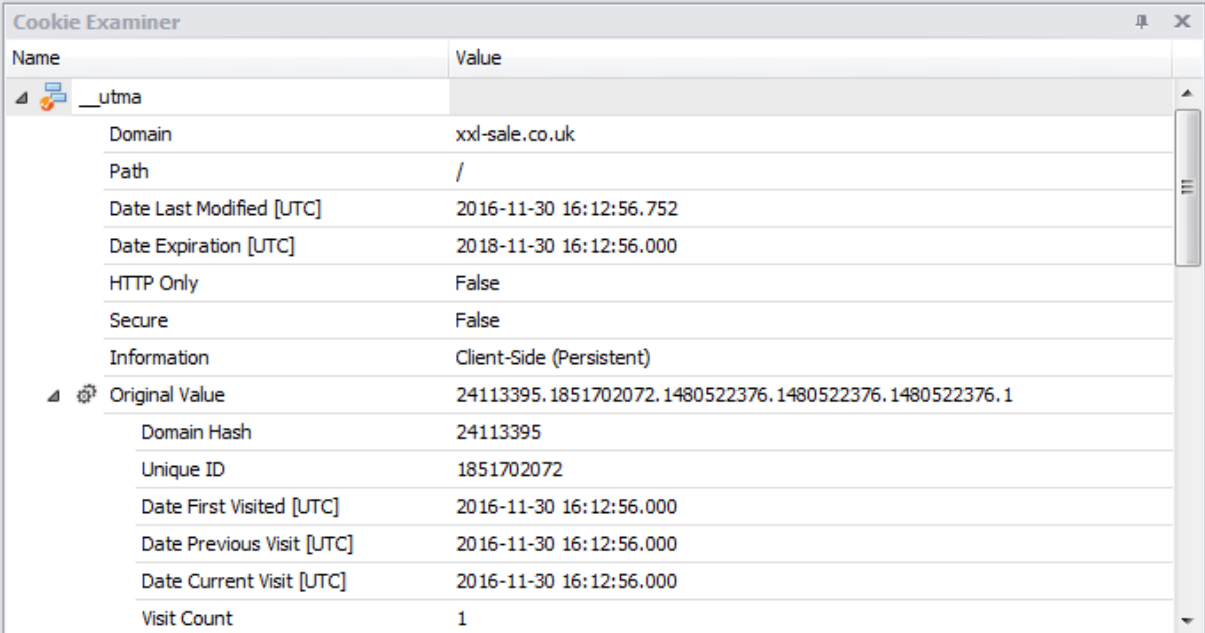
The Cookie Examiner fields are explained in Table 15 below:

Field Name	Information
Name	This field represents the name allocated by the developer for this specific cookie.
Domain	The Domain is a string which is usually the DNS host name or IP address of the server.
Path	This field indicates a URL path that must exist in the requested resource before sending the cookie header.
Date Last Accessed [UTC]	This date represents the last accessed date/time of the cookie in Coordinated Universal Time.

Field Name	Information
Date Created [UTC]	This date represents the created date/time of the cookie in Coordinated Universal Time.
Date Last Modified [UTC]	This date represents the last modified date/time of the cookie in Coordinated Universal Time.
Date Expiration [UTC]	This date represents the maximum lifetime of the cookie in Coordinated Universal Time.
HTTP Only	If the Http Only flag is included in the HTTP response header, the cookie cannot be accessed through client-side scripts.
Secure	A secure cookie is only sent to the server with an encrypted request over the HTTPS protocol.
Information	The Information field contains additional information and flags that may be present for the selected cookie.
Original Value	This field contains the Value portion of the cookie. If the cookie relates to a Google Analytics cookie, there may be a breakdown of the data contained within the Value field (as can be seen in Figure 92).

Table 15

Figure 92 shows a “__utma” Google Analytics cookie and the breakdown of the Original Value field.



Name	Value
__utma	
Domain	xxl-sale.co.uk
Path	/
Date Last Modified [UTC]	2016-11-30 16:12:56.752
Date Expiration [UTC]	2018-11-30 16:12:56.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
Original Value	24113395.1851702072.1480522376.1480522376.1
Domain Hash	24113395
Unique ID	1851702072
Date First Visited [UTC]	2016-11-30 16:12:56.000
Date Previous Visit [UTC]	2016-11-30 16:12:56.000
Date Current Visit [UTC]	2016-11-30 16:12:56.000
Visit Count	1

Figure 92

To view a Cookie Report, right click the Cookie Examiner window and select **Preview Cookie Report**. This will open a Cookie Report Preview window as shown in Figure 93.

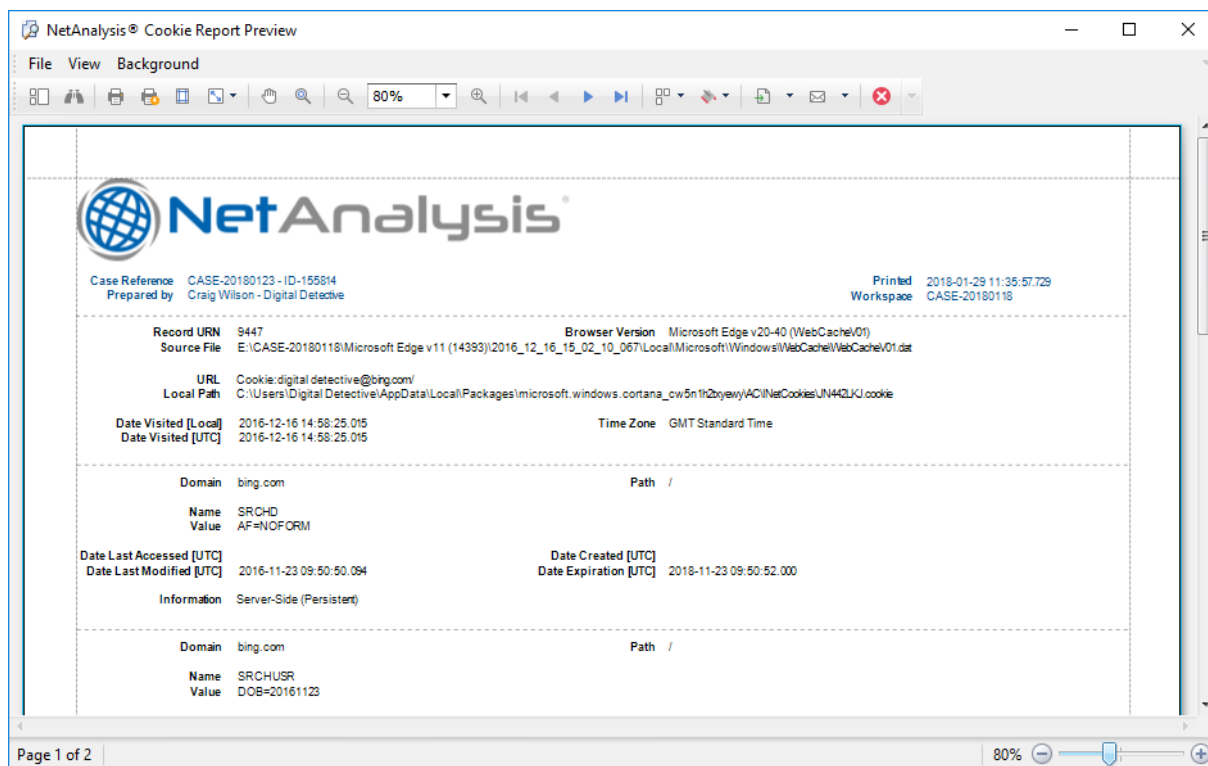


Figure 93

The report preview window allows the Cookie Report to be previewed on screen, sent to a printer or exported in a number of different formats. For further information, see Report Preview Window on Page 167.

Saving Your Workspace

At this point, you may wish to save your workspace database. This can be done by clicking on the save button or select **File » Save Workspace**.

Filtering and Searching

Introduction

It is important to be able to quickly identify the records that are relevant to your investigation. NetAnalysis® has a number of different ways to do this:

- Column Filter
- Custom Auto Filter
- Filter Editor / Filter Manager
- Searching via the Find Panel
- Auto Filter Row

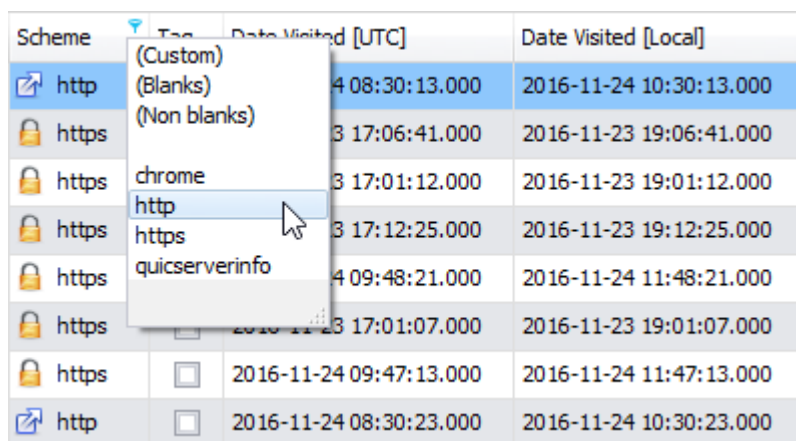
Filtering

Filtering allows you to display a subset of the records in the NetAnalysis® Workspace that meet a particular criterion. When filtering is applied to the grid, displayed records are restricted to those that meet the current filter criteria. You can filter data against single or multiple columns. You can also apply filtering by selecting a column's value from the filter dropdown, building a filter via the Filter Editor or by using the Custom Filter Dialog.

Create a Simple Filter Condition

To select records that contain a specific value in a specific column/field, do the following:

1. Invoke the filter dropdown list containing available filter values (see below on how to do this).
By default, if filtering is applied, the filter dropdown will only display the values that match the current filter criteria. If the **Shift** key is pressed while opening the filter dropdown, all values will be listed (not only those that match the current filter criteria).
2. Select the required filter value from the filter dropdown list.



Scheme	Type	Date Visited [UTC]	Date Visited [Local]
http	(Custom)	2016-11-24 08:30:13.000	2016-11-24 10:30:13.000
https	(Blanks)	2016-11-23 17:06:41.000	2016-11-23 19:06:41.000
https	(Non blanks)	2016-11-23 17:01:12.000	2016-11-23 19:01:12.000
https	chrome	2016-11-23 17:12:25.000	2016-11-23 19:12:25.000
https	http	2016-11-24 09:48:21.000	2016-11-24 11:48:21.000
https	https	2016-11-23 17:01:07.000	2016-11-23 19:01:07.000
https	quicserverinfo	2016-11-24 09:47:13.000	2016-11-24 11:47:13.000
http		2016-11-24 08:30:23.000	2016-11-24 10:30:23.000

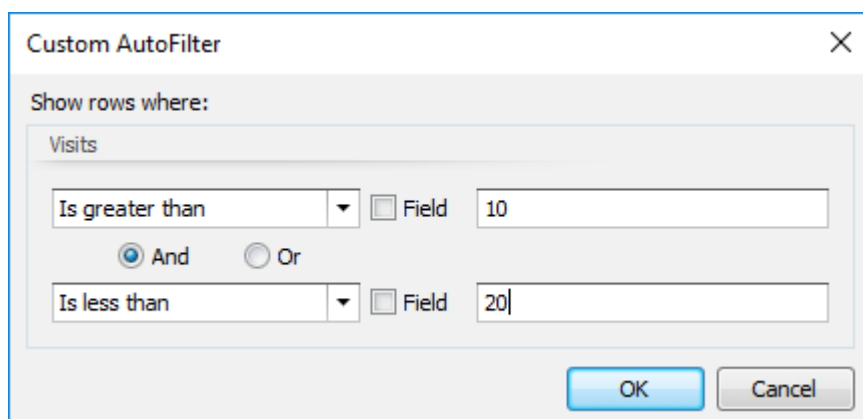
Figure 94

The filter dropdown list will be immediately closed, and the grid will display the records that contain the specified value in the specified column/field.

Create Complex Filter Criteria

To construct filter criteria involving multiple columns/fields, and using various comparison operators, do one of the following:

- Invoke the filter dropdown list and click **(Custom)**. This will invoke the Custom Filter window allowing you to compare a column with one or two values (as shown in Figure 95).
- Use the Filter Builder that allows complex filter criteria to be constructed. See Filter Editor on Page 118.



Custom AutoFilter

Show rows where:

Visits

Is greater than ☒ Field 10

☒ And ☐ Or

Is less than ☒ Field 20

OK Cancel

Figure 95

Clearing a Filter

To clear the filter applied to a specific column, do one of the following:

- Invoke the filter dropdown list and click **(All)**, see Figure 96.
- In Grid View, right click the column header and select **Clear Filter**.

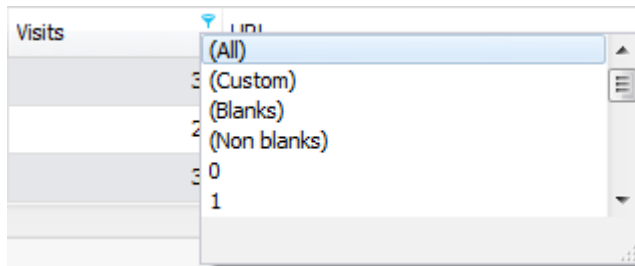


Figure 96

To clear the filter completely, click the Close Filter button within the Filter Panel (as shown in Figure 97).

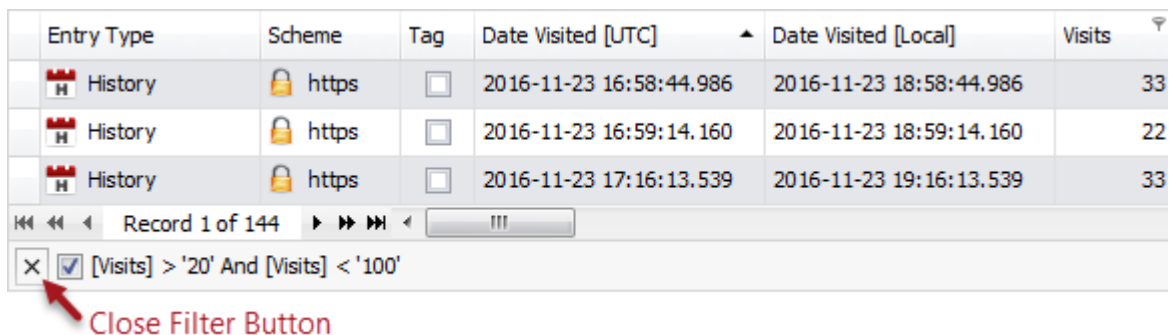


Figure 97

Disable/Enable a Filter

Click the Enable Filter button within the Filter Panel to quickly switch between enabling or disabling an existing filter; see Figure 98 below.

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits
History	https	<input type="checkbox"/>	2016-11-23 16:58:44.986	2016-11-23 18:58:44.986	33
History	https	<input type="checkbox"/>	2016-11-23 16:59:14.160	2016-11-23 18:59:14.160	22
History	https	<input type="checkbox"/>	2016-11-23 17:16:13.539	2016-11-23 19:16:13.539	33


Record 1 of 144

X ☒ [Visits] > '20' And [Visits] < '100'

Enable Filter Button

Figure 98

Invoke the Filter Dropdown List

In the grid, hover over a column header. Click the filter button  within the column header. This will show the Filter Dropdown List with the appropriate filter values.

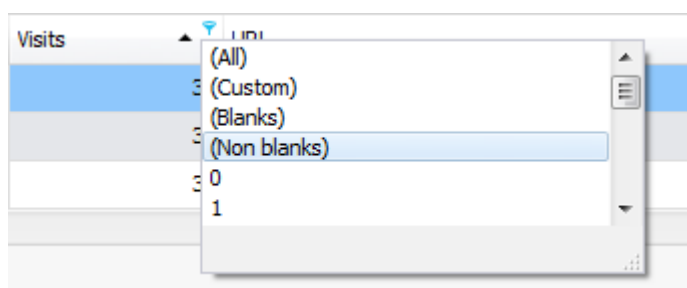




Figure 99

Filter Editor

The Filter Editor allows users to build complex filter criteria with an unlimited number of filter conditions, combined by logical operators. You can use a tree or text-based filter editing style or use both. When used in conjunction with the Filter Manager, these tools provide a powerful method of drilling down to the record(s) of interest.

To launch the Filter Editor, select **Filter » Filter Editor** from the menu (or press **F8**). To create and customise filter criteria, use the  and  buttons (as shown in Figure 100) to add or remove filter conditions.

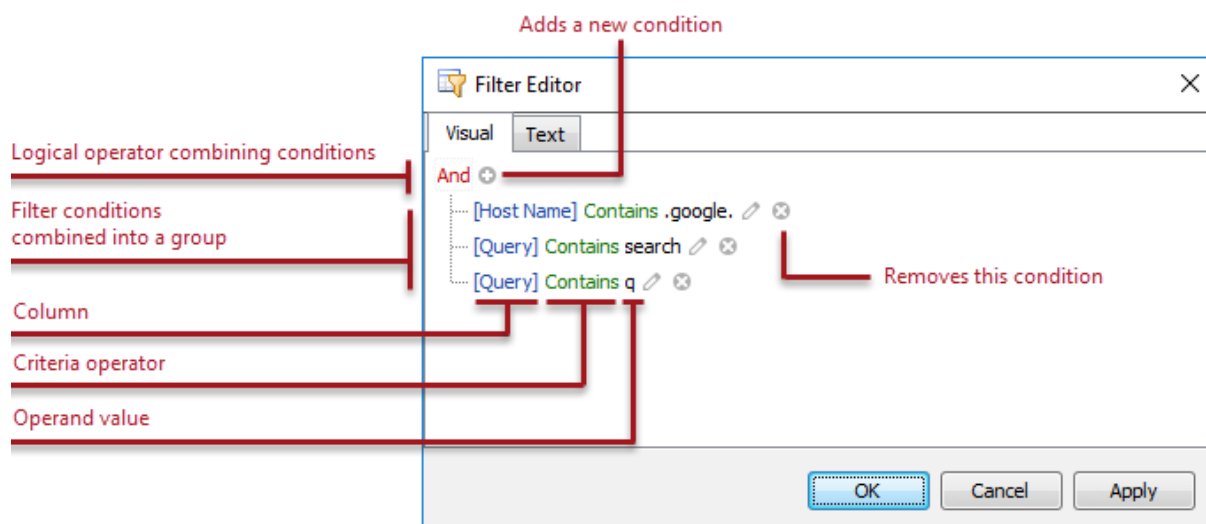


Figure 100

A filter condition group is a set of conditions combined by the same logical operator. The following filter expression contains two groups combined by the logical **OR** operator:

[Scheme] = 'https' And [Entry Type] = 'History' Or [Scheme] = 'http' And [Entry Type] = 'Download'

In the Filter Editor, it is represented as follows:

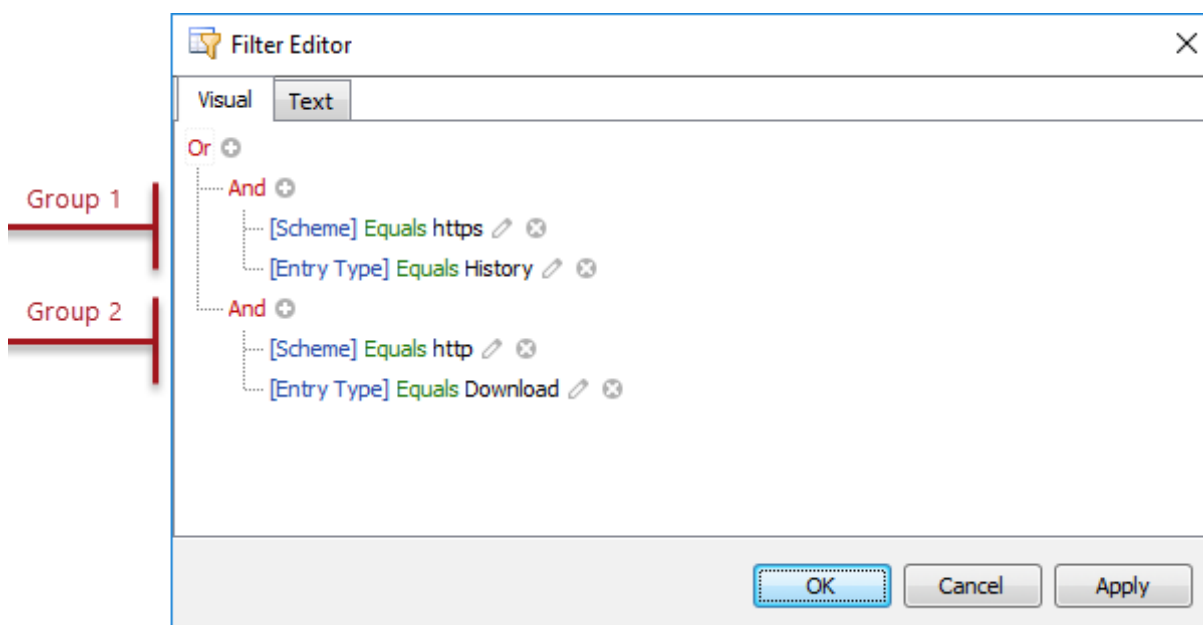



Figure 101

For step-by-step examples of creating filter criteria, see Filter Editor - Building Filter Criteria on Page 123.

Add Conditions

To add a condition to a logical group, do one of the following:

- Select any condition within the group or the group's logical operator, and then press **Insert** or **Add** on the keyboard.
- Click the  button for the group.
- Click the group's logical operator and select **Add Condition**.


To add a group of conditions to another group, do one of the following:

- Select any condition within the group or the group's logical operator, and then press **CTRL + Add** on the keyboard.
- Click the group's logical operator and select **Add Group**.

To add a condition or a group of conditions that have been copied to the Clipboard, press **CTRL + V** or **Shift + Insert**. The new condition will be added to the focused group.

Delete Conditions

To delete a condition, do one of the following:

- Select the condition and press **Delete** or **Subtract**.
- Click the  button.

To delete a group of conditions, do one of the following:

- Select the group's logical operator and press **Delete** or **Subtract**.
- Click the group's logical operator and select **Remove Group**.

To delete all conditions, do one of the following:

- Focus the topmost logical operator and press **Delete** or **Subtract**.
- Click the topmost logical operator and select **Clear All**.

To cut a condition/group of conditions to the Clipboard, focus this condition/the group's logical operator and press **CTRL + X** or **Shift + Delete**.

Change a Column in a Filter Condition

To change a condition's column, invoke the column list by doing one of the following:

- Click the current column.
- Select the current column via the keyboard and press **Space** or **ALT + Down Arrow**.

Then, choose the required column from the list.

Change an Operator in a Filter Condition

To change a condition's operator, invoke the operator list by doing one of the following:

- Click the condition's current operator.
- Focus the current operator via the keyboard and press **Space** or **ALT + Down Arrow**.

Then, choose the required operator from the list.

Edit a Condition's Value

To edit a condition's value, click the operand value and type in the edit box.

To activate the operand value's edit box without changing the value, click the value or select the operand value via the keyboard and press **F2**, **Space**, **Enter** or **ALT + Down**.

To close the active edit box, press **Enter**.

To discard changes to the value and close the active edit box, press **Esc**.

Navigation

To focus a specific filter condition or a group's operator within the Filter Editor, do one of the following:

- Click the target element.
- Use Arrow keys to move focus via the keyboard.

Launching the Filter Editor

To launch the Filter Editor, do one of the following:

- Right click any column's header and select **Filter Editor**.

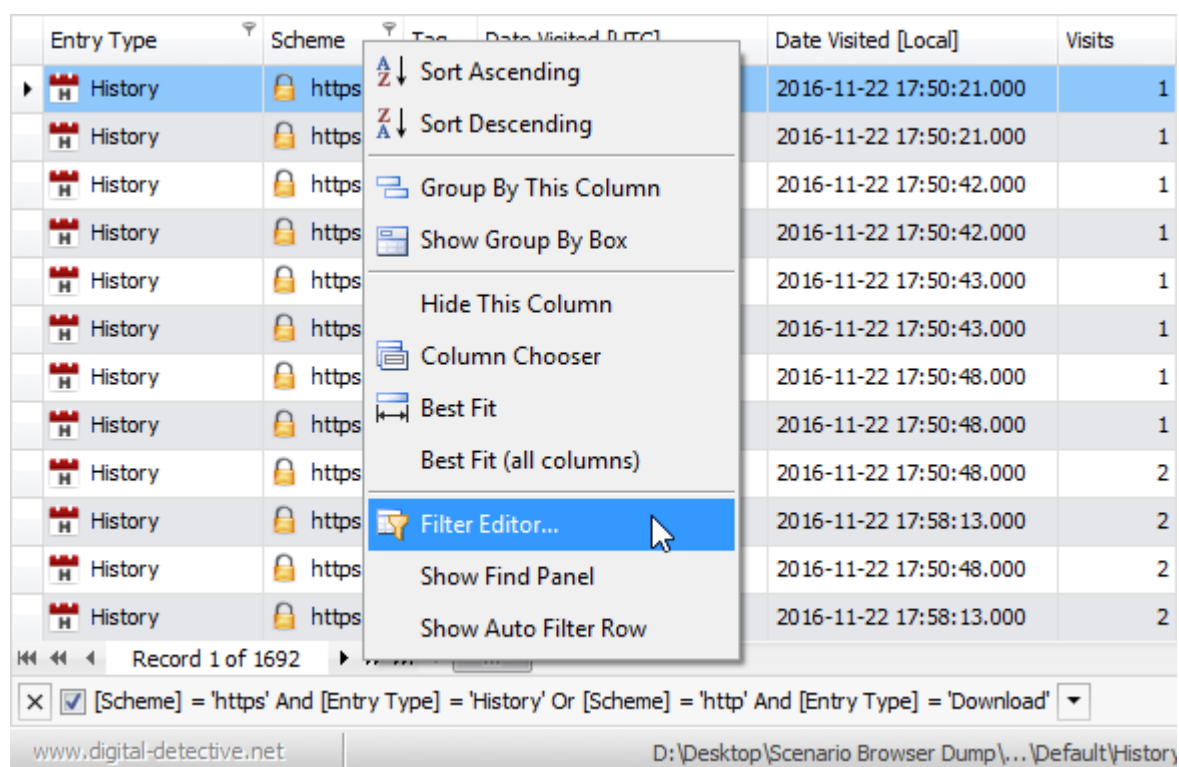


Figure 102

- If the Filter Panel at the bottom of the grid is visible, click the **Edit Filter** button.

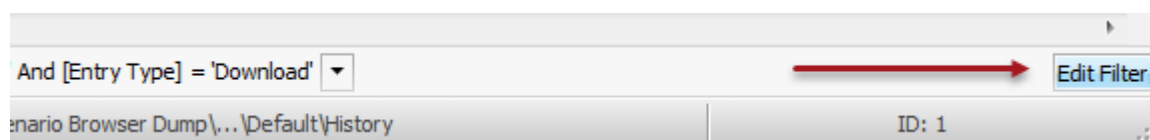

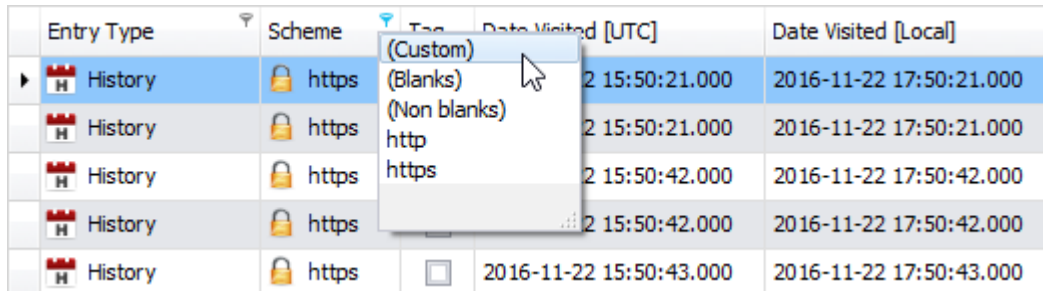


Figure 103

- Select **Filter Editor** from the **Filter** menu.
- Press the Filter Editor shortcut key **F8** when the grid has the focus.
- Press the Filter Editor button  on the main toolbar.

The Filter Editor is also launched when choosing the **(Custom)** item in a column's filter dropdown list, if the current filter criteria applied to the column consists of three or more simple filter conditions, or if the filter criteria contains advanced comparison operators such as **Is between** and **Is any of**.



Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]
History	https		2016-11-22 15:50:21.000	2016-11-22 17:50:21.000
History	https		2016-11-22 15:50:21.000	2016-11-22 17:50:21.000
History	https		2016-11-22 15:50:42.000	2016-11-22 17:50:42.000
History	https		2016-11-22 15:50:42.000	2016-11-22 17:50:42.000
History	https		2016-11-22 15:50:43.000	2016-11-22 17:50:43.000

Figure 104

Filter Editor - Building Filter Criteria

The Filter Editor allows the user to filter data (display those records that meet specific requirements) by visually constructing filter criteria in a straightforward graphical form.

The following sections demonstrate how to construct filter criteria for the grid using the Filter Editor.

Constructing Simple Filter Conditions

Filter conditions specify what data to select from the workspace and display in the grid. A typical simple filter condition consists of three parts: the column/field name, operator and value(s).

For example:

[Visits] > 20

This is a simple filter condition where **[Visits]** is the field name, **>** is an operator and **20** is a value. When this is applied to the underlying workspace data source, this condition will select records that have values in the Visits column greater than 20.

To create this condition via the Filter Editor, do the following:

1. Open the Filter Editor by right clicking on the Visits column header and selecting the **Filter Editor** option (as shown in Figure 105).

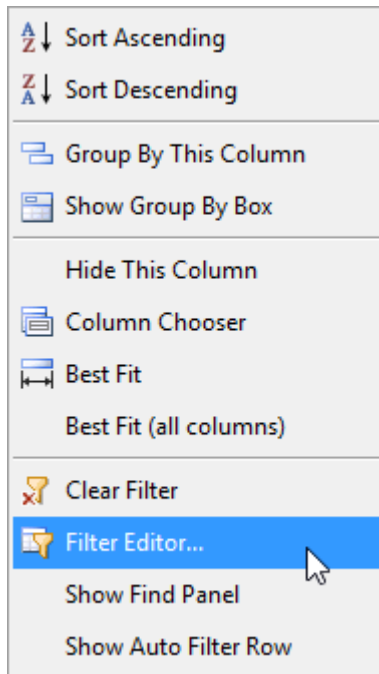


Figure 105

2. The Filter Editor will appear as shown in Figure 106. If no filtering has been applied, the Filter Editor will contain a new filter condition matching the clicked column. If filtering has been applied, the Filter Editor will contain the currently applied filter. To remove an unwanted Filter, see the section Delete Conditions on Page 120.

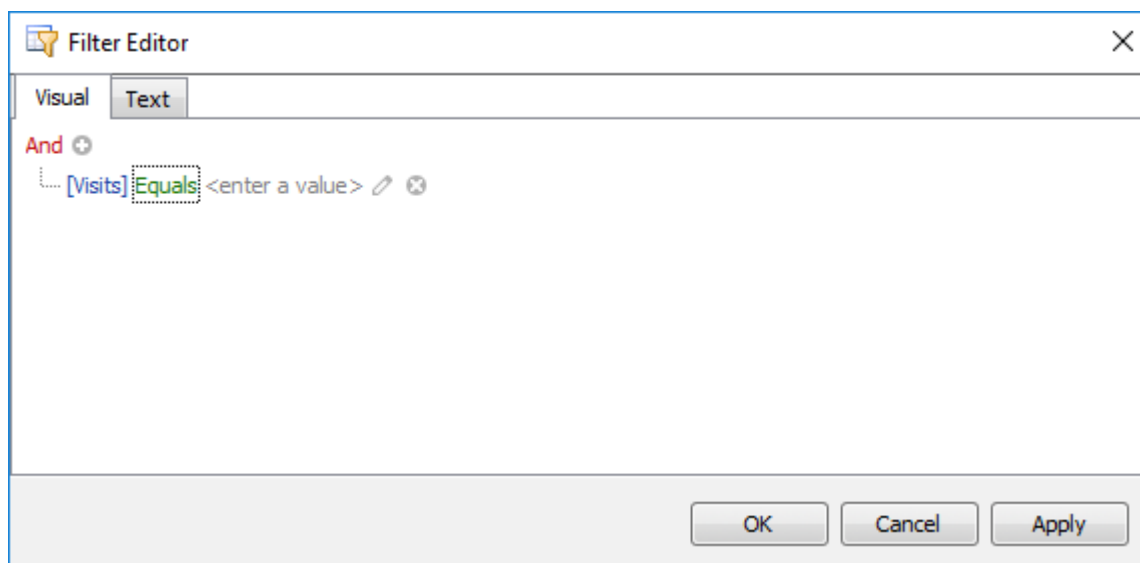


Figure 106

3. Click on the default Operator (shown as = **Equals** in Figure 107 below), and select > **Is greater than** from the dropdown list.

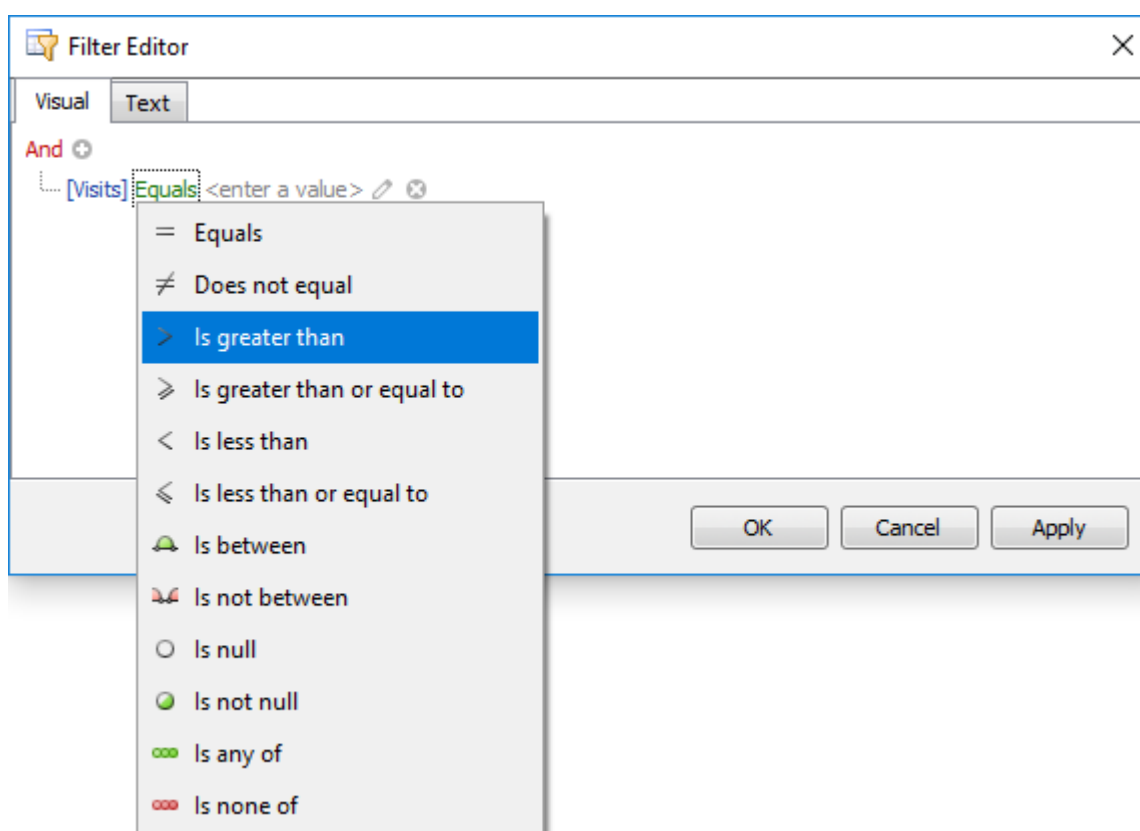


Figure 107

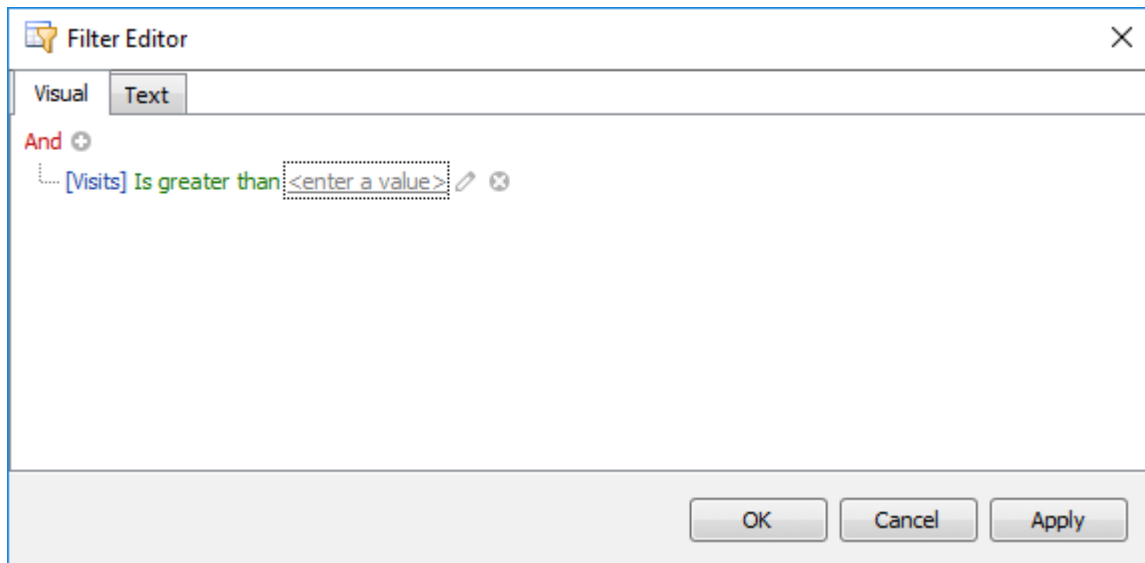


Figure 108

4. Click on the area marked **<enter a value>** (as shown in Figure 108) and type the value **20**. Your Filter Editor should now look like Figure 109 below.

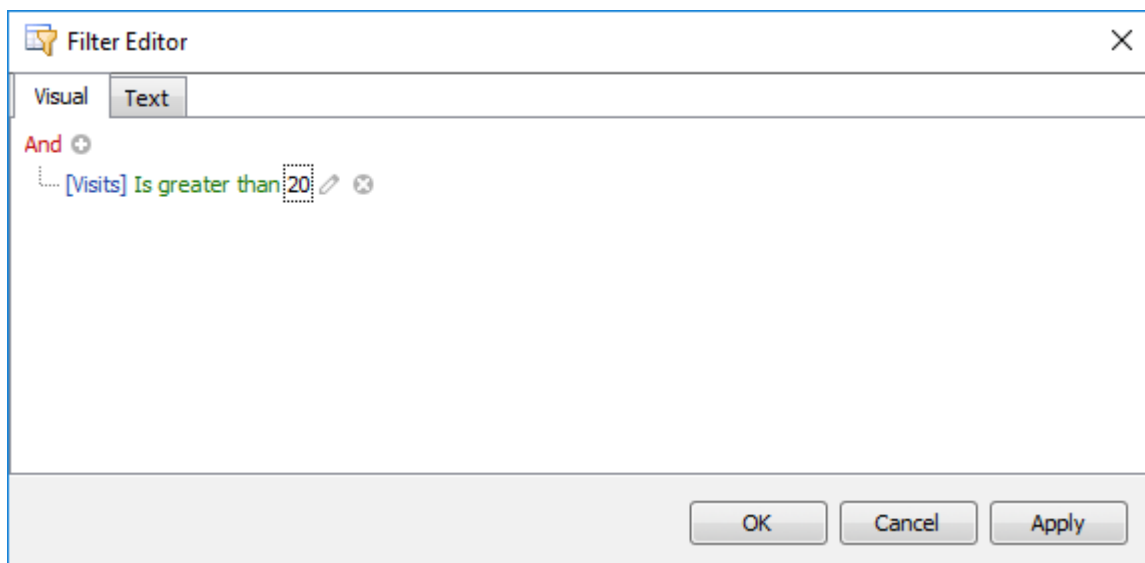


Figure 109

5. Click **OK** or **Apply** to filter data using the created filter condition. The grid will filter the records and show the filter panel displaying the current filter criteria.

- To filter against another column, click the condition link displaying a column name (see column **[Visits]** in Figure 106). This will display a list of available columns (as shown in Figure 110).

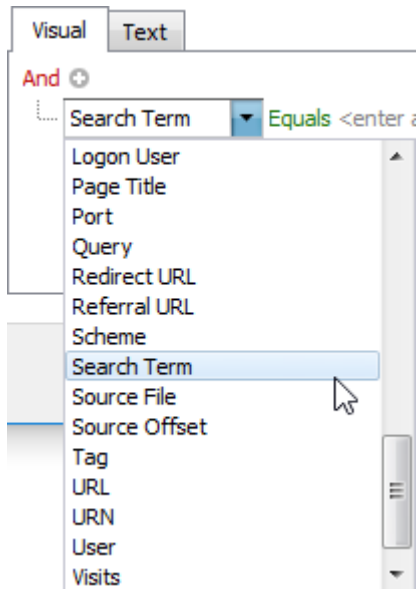


Figure 110

- Select the **[Search Term]** column from the list. The Filter Editor should now look like Figure 111.

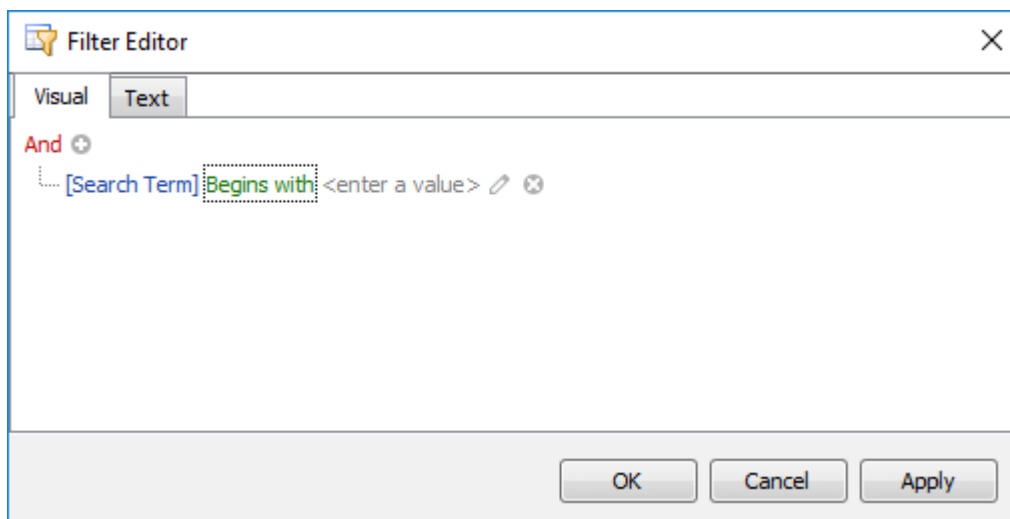


Figure 111

- To select the comparison operator, click the condition operator link to display the operator list (as shown in Figure 112 below).

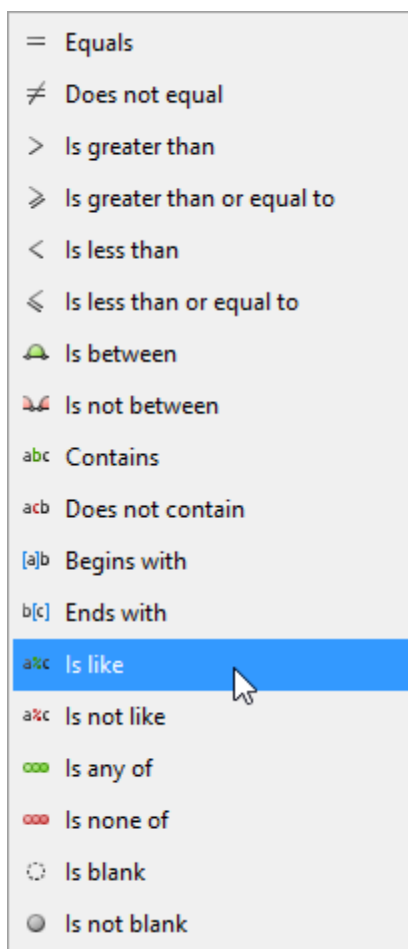


Figure 112

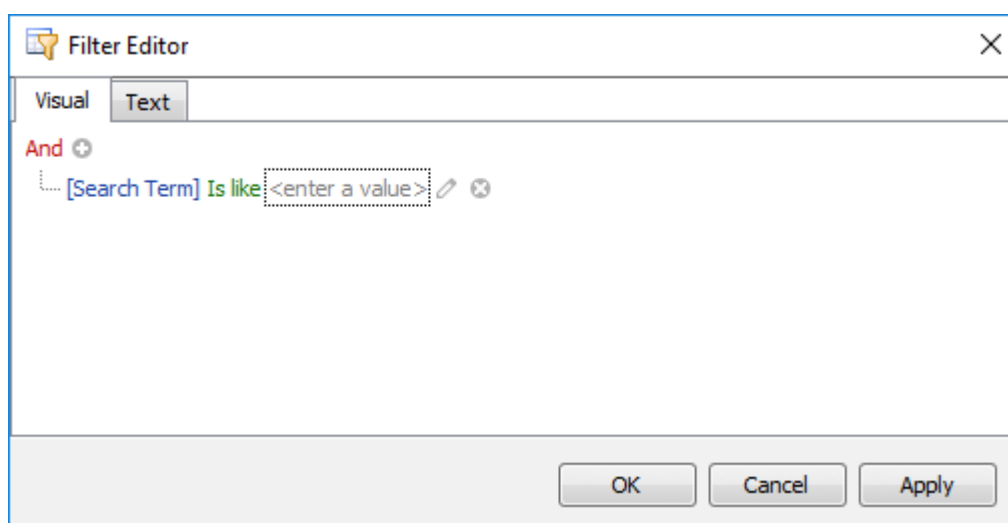


Figure 113

9. The comparison operator list displays only those operators that are supported by the current column's data type. For instance, the **[Visits]** column is a numeric type and the operator list

does not display the **Begins with** operator and other operators that are related to the string type. The field **[Search Term]** contains string data; to obtain a partial (non-case sensitive) string match, we will use the comparison operator **Is Like** (as shown in Figure 113).

10. Now click the value box and enter a comparison value **%cesium%**. When using the **Is Like** comparison operator, you must use the **%** wildcard character to perform a partial string match where the string contains text before and after the comparison value. The **Contains** comparison operator does not require the wildcard character.

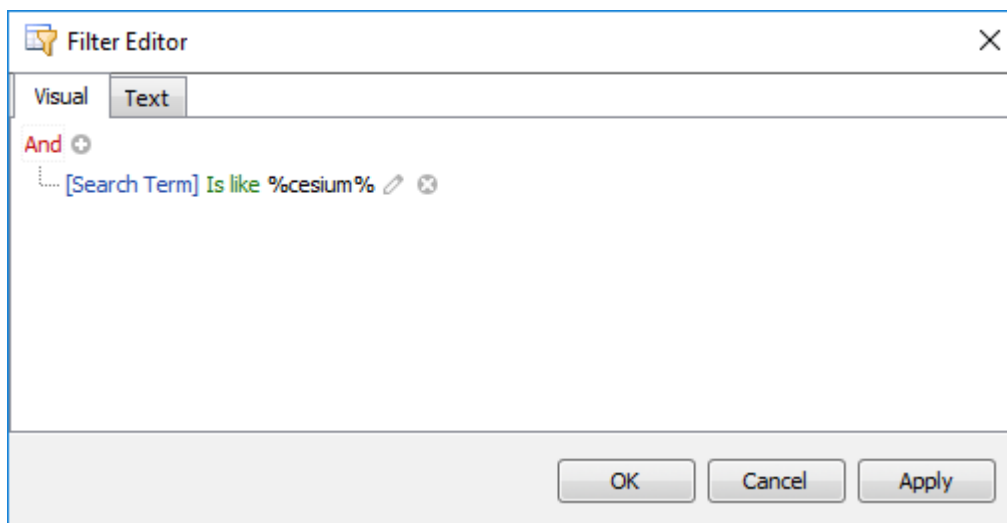


Figure 114

11. Click **OK** or **Apply** to filter data using the created filter condition. The grid will filter the records and the filter panel will display the current filter criteria (as shown in Figure 115).

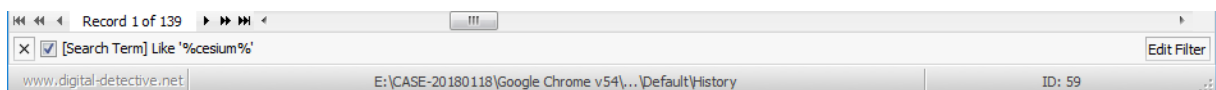


Figure 115

The filter panel will contain the **Edit Filter** button, which also allows the user to launch the Filter Editor.

Constructing Complex Filters with Logical Operators

Filter criteria typically consist of two or more simple filter conditions combined by logical operators (AND, OR, NOT AND, NOT OR). The following example shows how to construct filter criteria in the Filter Editor that consist of multiple conditions combined by one logical operator.

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

The above filter expression contains three simple filter conditions combined by the AND operator. To construct it, do the following:

1. Launch the Filter Editor by right clicking the **Entry Type** column's header and selecting the Filter Editor option. The Filter Editor will display an unfinished new filter condition referring to the clicked **Entry Type** column (as shown in Figure 116).

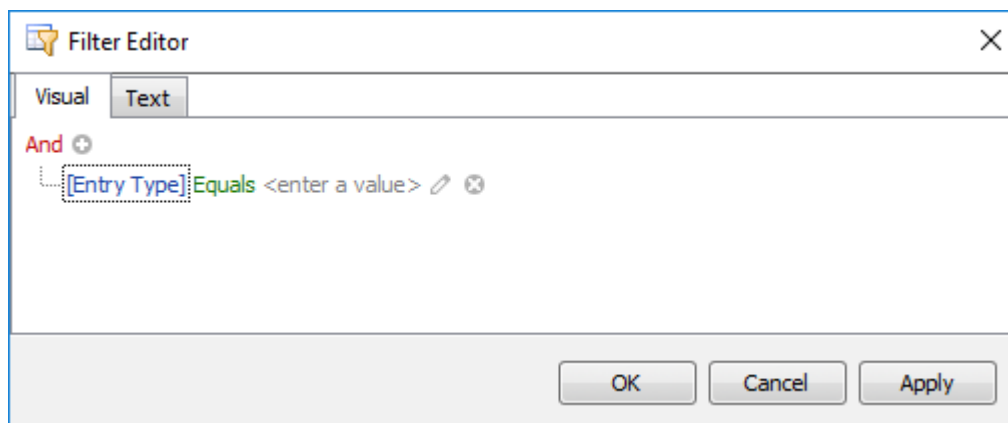


Figure 116

2. The comparison operator **Equals (=)** will already be selected as this is the default operator value for this column.
3. To complete the construction of the first filter condition, click the value box to display the list of possible values for the **Entry Type** column and select **Cache** (as shown in Figure 117).

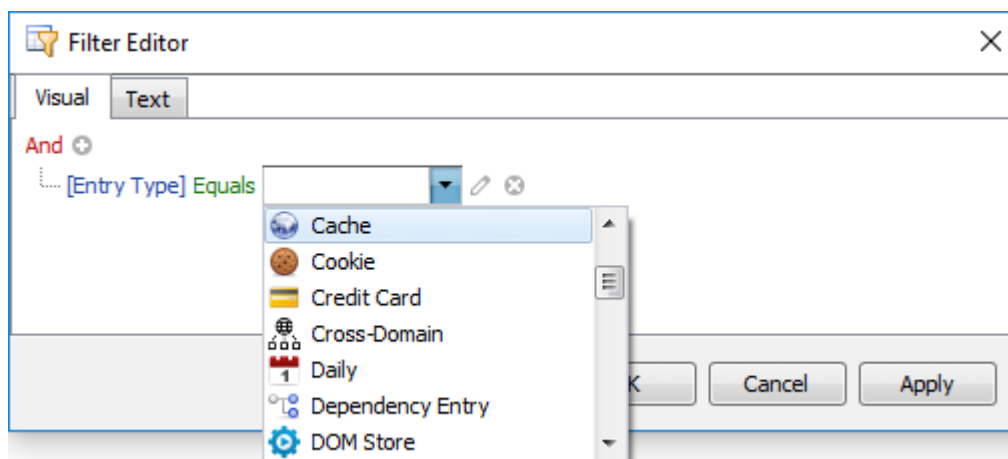


Figure 117

4. To add the second filter condition, click on the **+** button next to the **And** logical operator. The Filter Editor will now display a new, unfinished filter condition, below the first and should look like Figure 118. To combine the two filter conditions using a different logical operator, click the currently displayed **And** operator to display a list of all available logical operators and select the required one.

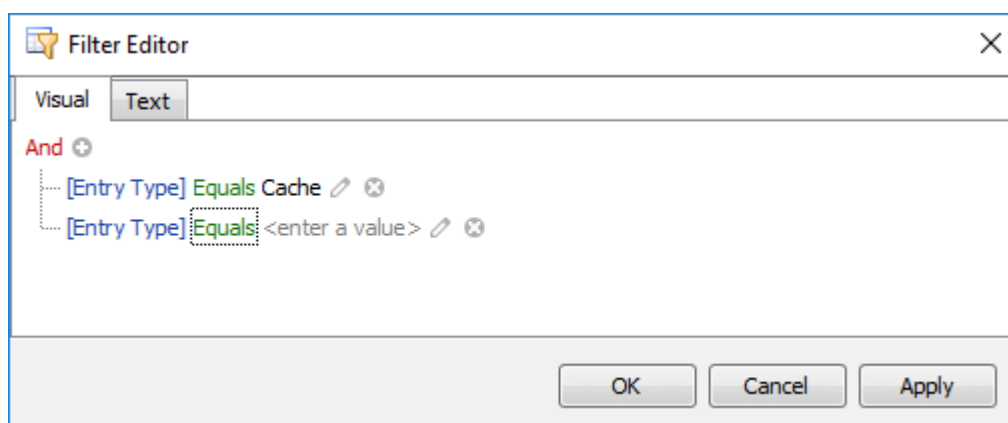


Figure 118

5. To change the second filter condition so that it filters against a different column, click the currently displayed **[Entry Type]** column name to display the list of available columns. Select the **Cache File Exists** column from the list.
6. This second filter condition also requires the default comparison operator **Equals (=)** and this should already be selected.

- Now click the value box to display the list of all possible values for the **Cache File Exists** column and select **Exists**. This step completes the construction of the second filter condition and the Filter Editor should now look like Figure 119.

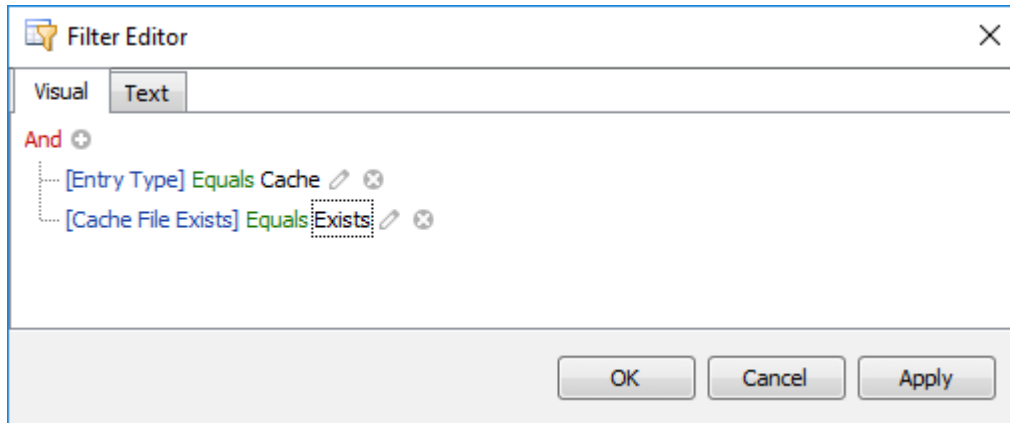


Figure 119

- To add the third and final filter condition, again click on the **+** button next to the **And** logical operator. The Filter Editor will now display a new unfinished filter condition below the second and should look like Figure 120 .

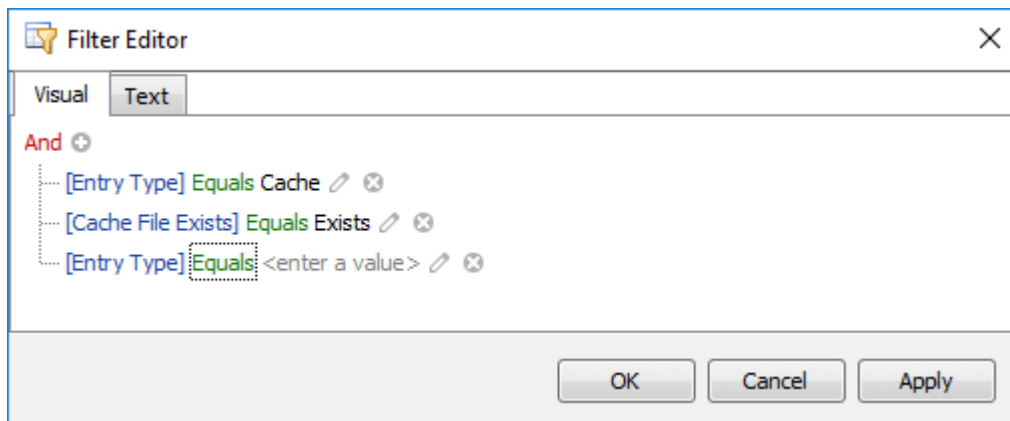


Figure 120

- To change the third filter condition so that it filters against the correct column, click the currently displayed **[Entry Type]** column name to display the list of available columns. Select the **Cache File Extension** column from the list.

10. The third filter condition will select records that have values in the **Cache File Extension** column which are either **.htm** or **.html**. To select the required comparison operator for this third filter condition, click the current operator to display the operator list and select the **Is any of** operator. The Filter Editor should now look like Figure 121.

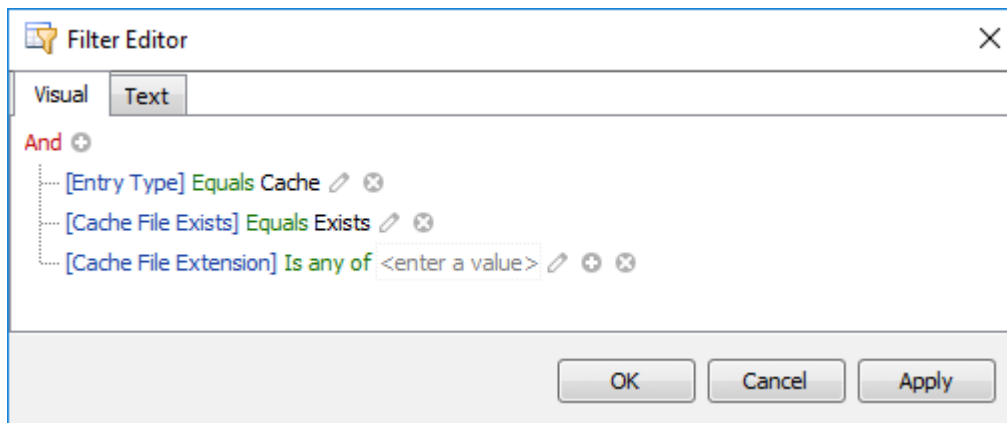


Figure 121

11. This filter condition contains two filtering values and they both need to be separately added. Click the value box and enter the first comparison value **.htm**. Click on the **+** button next to the value you have just entered and enter the second comparison value **.html**. The Filter Editor will now contain the complete filter criteria and should look like Figure 122.

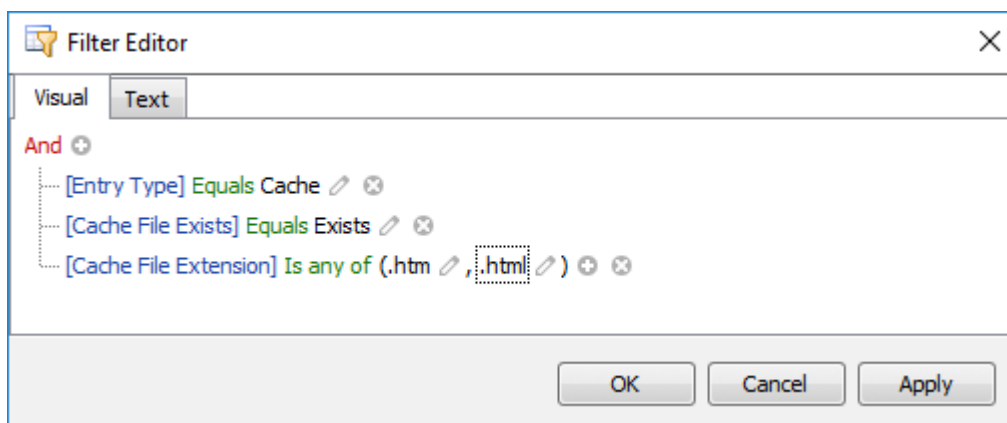


Figure 122

12. Switch from the visual editor to the text-based view by clicking on the **Text** tab and the filter criteria should look like Figure 123.

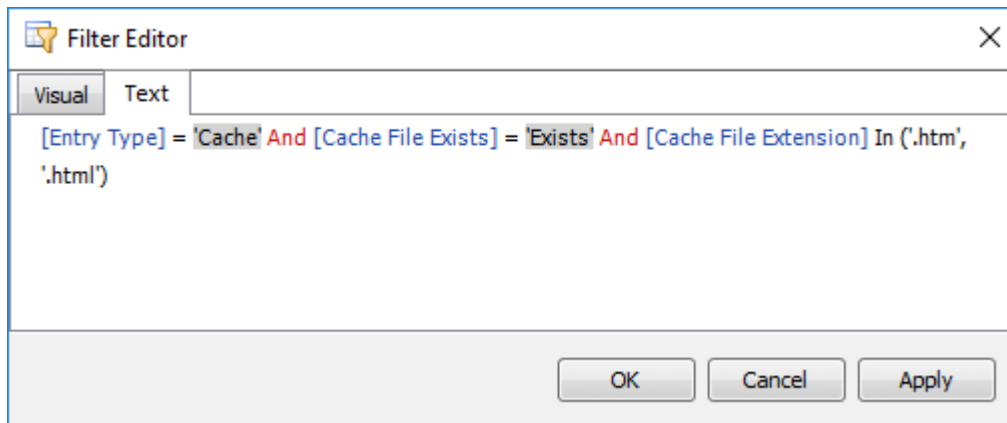


Figure 123

13. Click **OK** or **Apply** to filter data using the created filter condition. The grid will filter the records and the filter panel will display the current filter criteria (as shown in Figure 124).

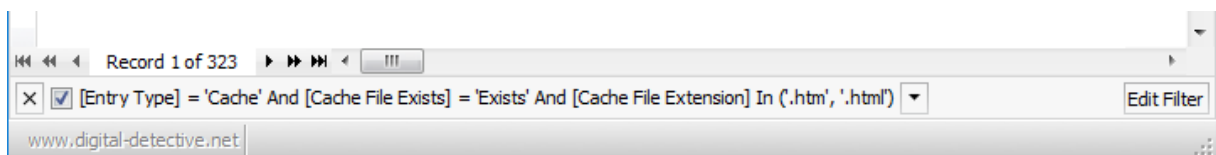


Figure 124

Constructing Filters with Multiple Logical Operators

Some filter criteria contain multiple logical (Boolean) operators combining simple filter conditions. To build such criteria via the Filter Editor, first, you need to identify groups of filter conditions.

A filter group is a set of simple filter conditions or other groups combined by the same logical operator. You can think of groups as clauses in a filter expression wrapped by round brackets.

Consider the following filter criteria:

Contains([Host Name], 'ebay') And [Visits] > 10 Or Contains([Host Name], 'amazon') And [Visits] > 10

In this expression, we'll identify groups by wrapping them with round brackets as follows:

(Contains([Host Name], 'ebay') And [Visits] > 10) Or (Contains([Host Name], 'amazon') And [Visits] > 10)

Here you see two groups of filter conditions. Within each group, filter conditions are combined by the same logical operator:

1. (Contains([Host Name], 'ebay') And [Visits] > 10)
2. (Contains([Host Name], 'amazon') And [Visits] > 10)

This expression contains two groups of filter conditions combined by the OR operator. In each group, filter conditions are combined by the AND operator.

1. Launch the Filter Editor by clicking **Filter » Filter Editor**.
2. Change the root logical operator to **Or**. To do this, click the current **And** operator and select **Or**.

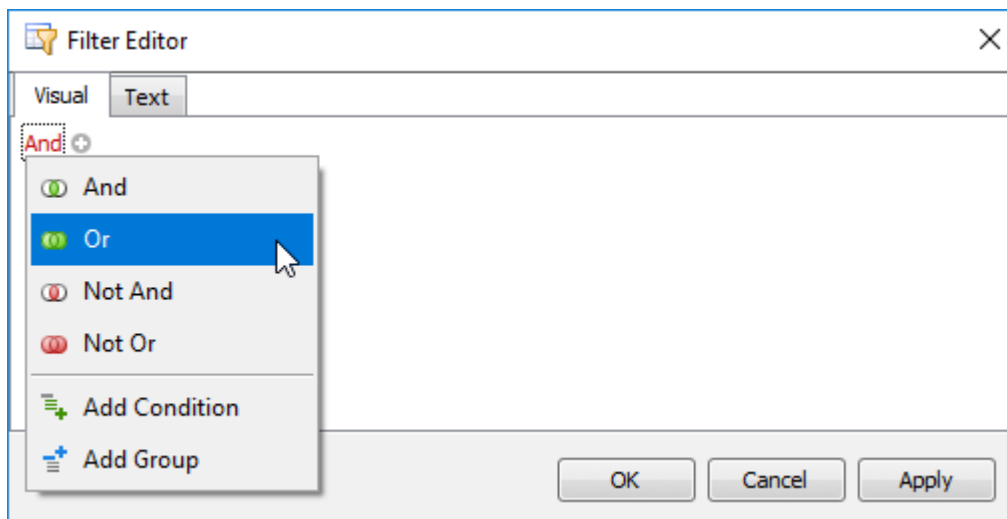


Figure 125

3. Add a new filter condition group by clicking the **Or** operator and selecting **Add Group** (as shown in Figure 126).

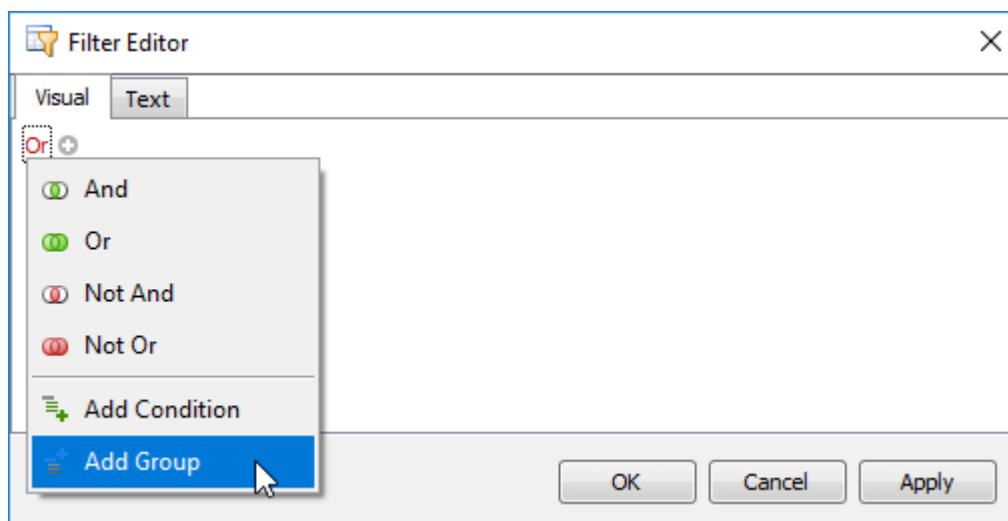


Figure 126

4. For the condition, set the column to **[Host Name]**, operator to **Contains** and operand value to **amazon**, as shown in Figure 127.

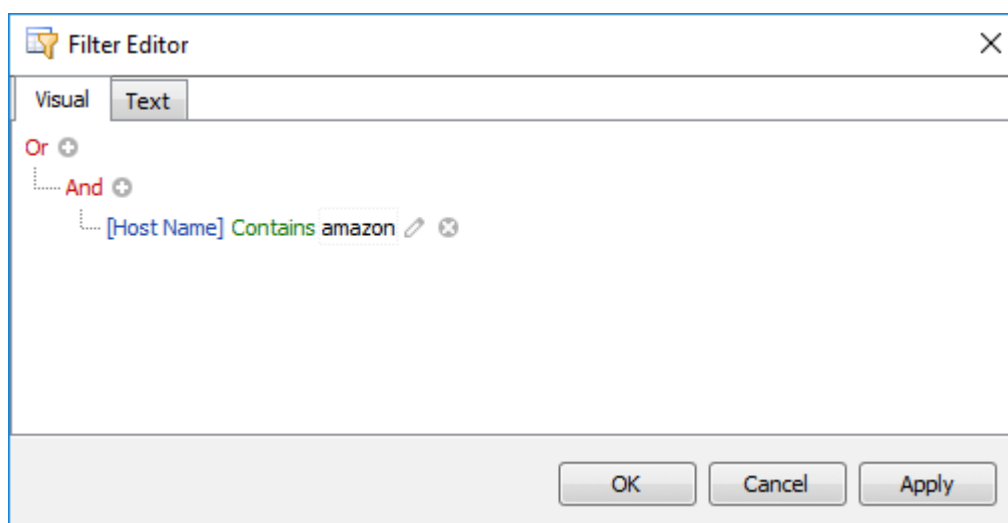


Figure 127

5. Click the + button to add a new condition to the current group (see Figure 128).

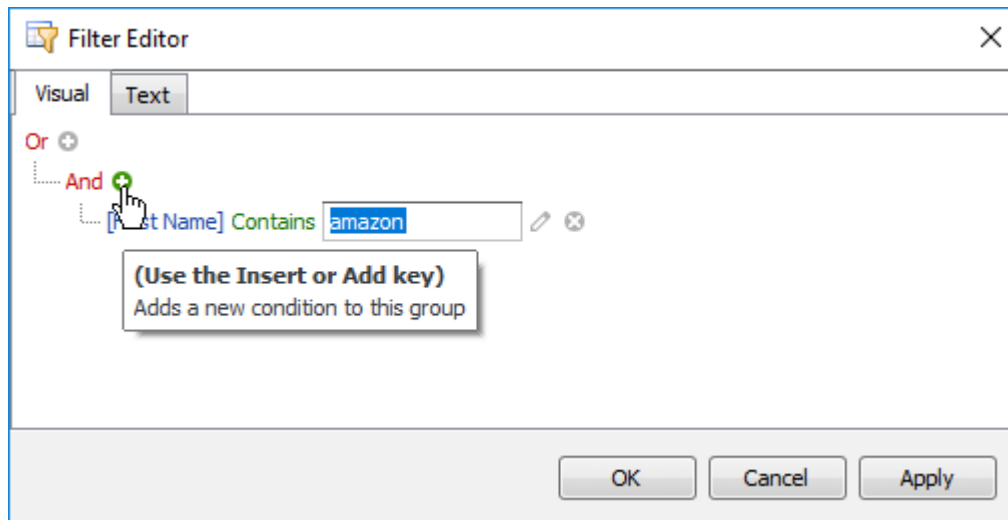


Figure 128

- For the new condition, set the column to **[Visits]**, operator to **> Is greater than** and operand value to **10** (see Figure 129).

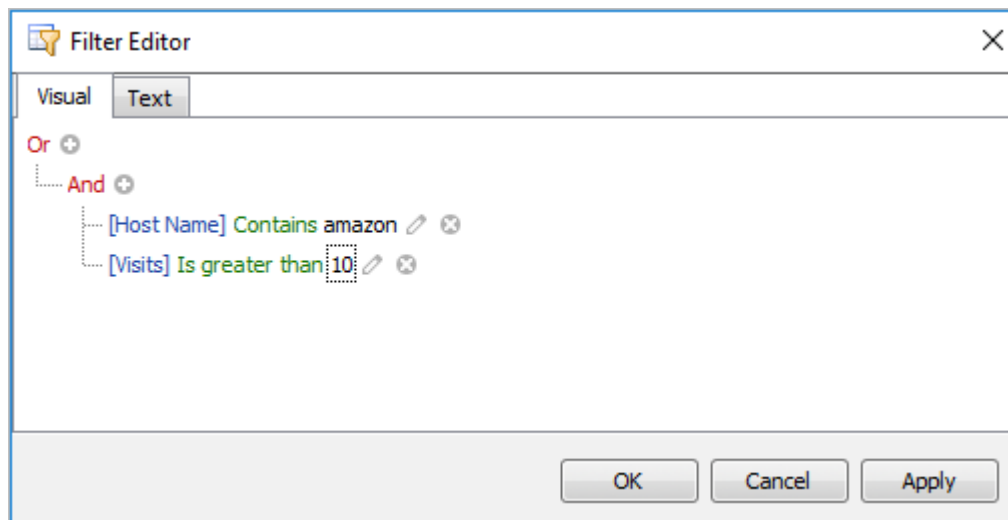


Figure 129

- Add a new filter condition group. To do this, click the root **Or** operator and select **Add Group** (see Figure 130).

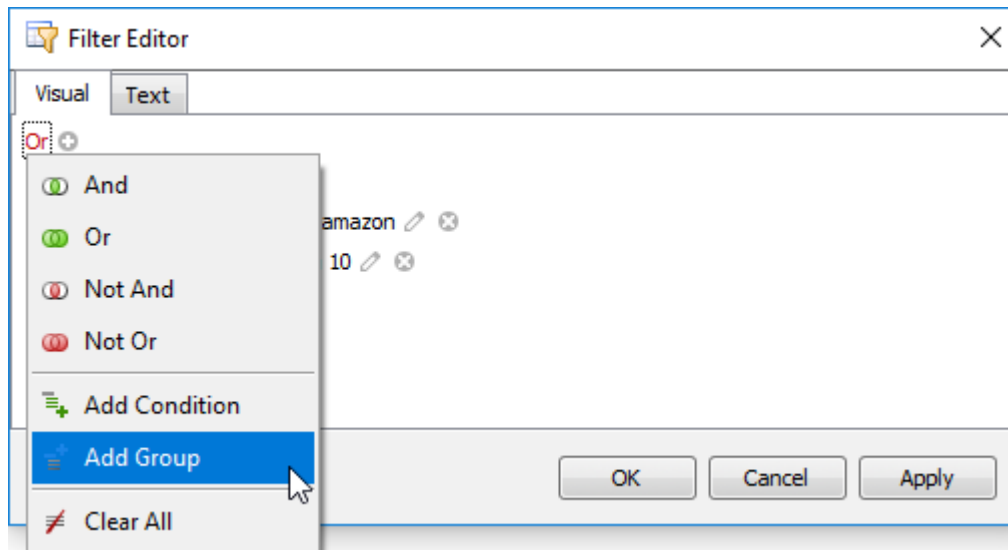


Figure 130

8. For the condition within the created group, set the column to **[Host Name]**, operator to **Contains** and operand value to **ebay** (see Figure 131).

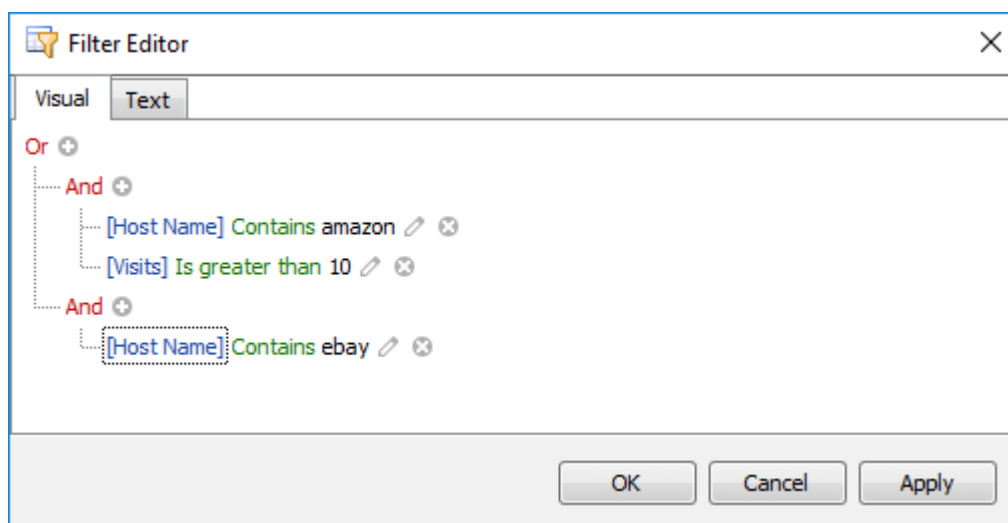


Figure 131

9. Click the **+** button to add a new condition to the new group (see Figure 132).

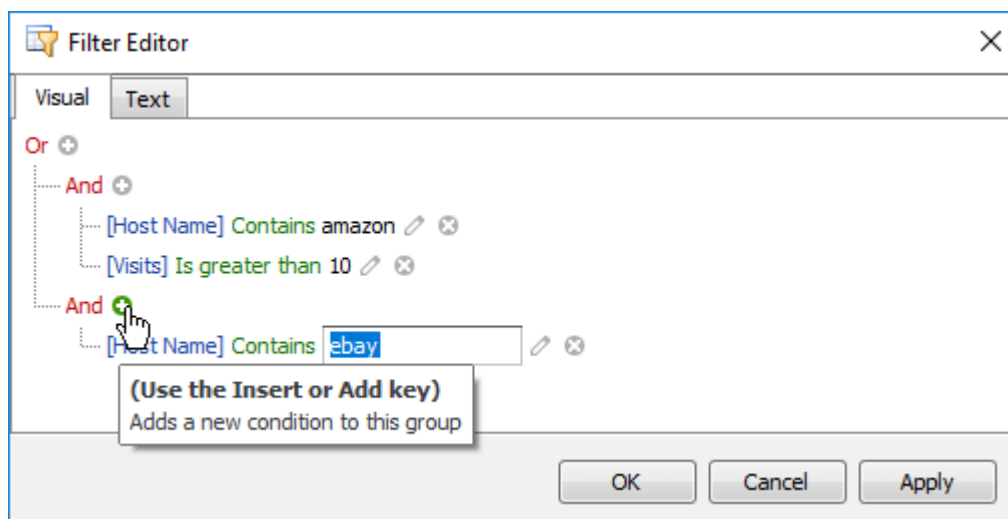


Figure 132

10. For the new condition, set the column to **[Visits]**, operator to **> Is greater than** and the operand value to **10** (see Figure 133).

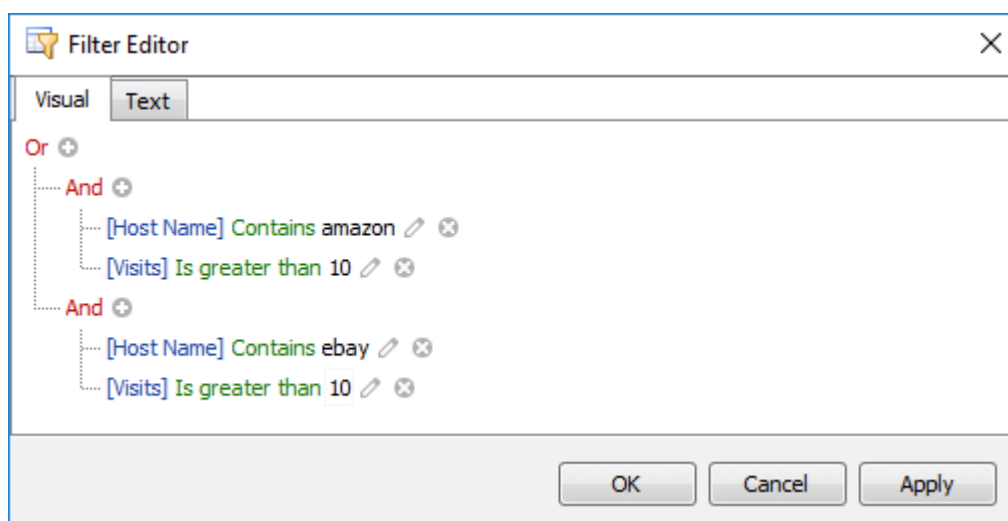
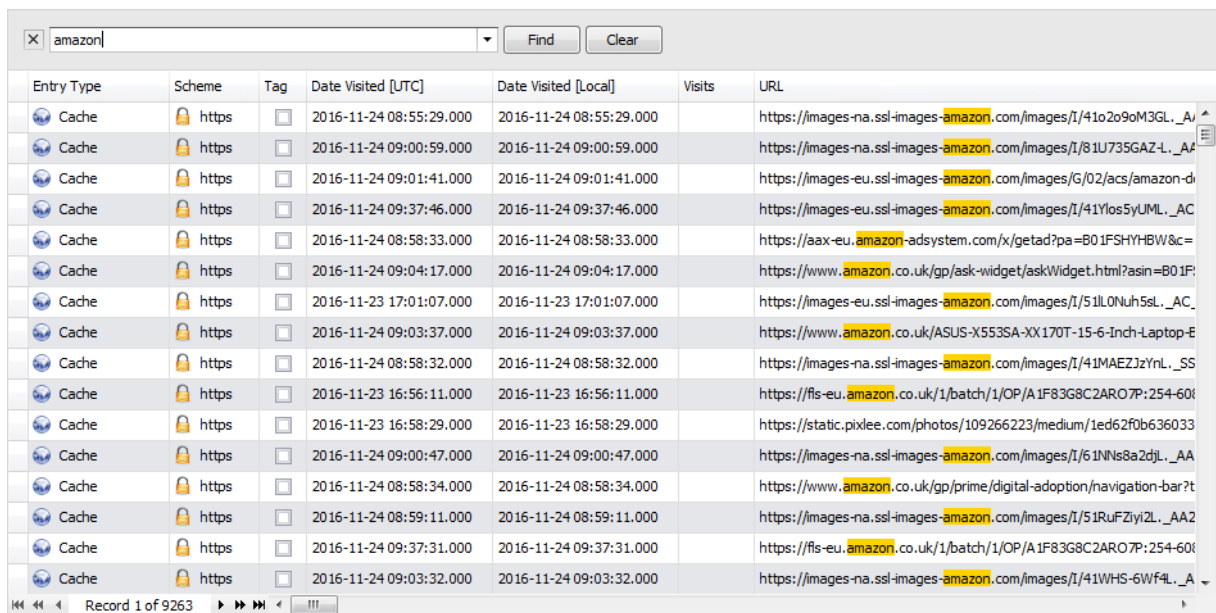


Figure 133

11. Click **OK** or **Apply** to apply the created filter criteria.
12. To Save this filter, select **Filter » Save Filter** from the menu.

Locating Rows Using Search (Find) Panel

The Find Panel provides an easy way of searching against visible columns and fields. It is displayed above the grid and contains a search box where the user can enter a search string.



Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	https		2016-11-24 08:55:29.000	2016-11-24 08:55:29.000		https://images-na.ssl-images-amazon.com/images/I/41o2o9oM3GL._AA
Cache	https		2016-11-24 09:00:59.000	2016-11-24 09:00:59.000		https://images-na.ssl-images-amazon.com/images/I/81U735GAZL._AA
Cache	https		2016-11-24 09:01:41.000	2016-11-24 09:01:41.000		https://images-eu.ssl-images-amazon.com/images/G/02/acs/amazon-d
Cache	https		2016-11-24 09:37:46.000	2016-11-24 09:37:46.000		https://images-eu.ssl-images-amazon.com/images/I/41Ylos5yUML._AC
Cache	https		2016-11-24 08:58:33.000	2016-11-24 08:58:33.000		https://aax-eu.amazon-adsystem.com/x/getad?pa=B01FSHYHBW&c=
Cache	https		2016-11-24 09:04:17.000	2016-11-24 09:04:17.000		https://www.amazon.co.uk/gp/ask-widget/askWidget.html?asin=B01F
Cache	https		2016-11-23 17:01:07.000	2016-11-23 17:01:07.000		https://images-eu.ssl-images-amazon.com/images/I/51LONuh5sL._AC
Cache	https		2016-11-24 09:03:37.000	2016-11-24 09:03:37.000		https://www.amazon.co.uk/ASUS-X553SA-XX170T-15-6-Inch-Laptop-E
Cache	https		2016-11-24 08:58:32.000	2016-11-24 08:58:32.000		https://images-na.ssl-images-amazon.com/images/I/41MAEZJzYnL._SS
Cache	https		2016-11-23 16:56:11.000	2016-11-23 16:56:11.000		https://fs-eu.amazon.co.uk/1/batch/1/OP/A1F83G8C2AR07P:254-60i
Cache	https		2016-11-23 16:58:29.000	2016-11-23 16:58:29.000		https://static.pixlee.com/photos/109266223/medium/1ed62f0b636033
Cache	https		2016-11-24 09:00:47.000	2016-11-24 09:00:47.000		https://images-na.ssl-images-amazon.com/images/I/61NNs8a2dJL._AA
Cache	https		2016-11-24 08:58:34.000	2016-11-24 08:58:34.000		https://www.amazon.co.uk/gp/prime/digital-adoption/navigation-bar?t
Cache	https		2016-11-24 08:59:11.000	2016-11-24 08:59:11.000		https://images-na.ssl-images-amazon.com/images/I/51RuFZiyi2L._AA2
Cache	https		2016-11-24 09:37:31.000	2016-11-24 09:37:31.000		https://fs-eu.amazon.co.uk/1/batch/1/OP/A1F83G8C2AR07P:254-60i
Cache	https		2016-11-24 09:03:32.000	2016-11-24 09:03:32.000		https://images-na.ssl-images-amazon.com/images/I/41WHS-6Wf4L._A

Figure 134

Open the Find Panel

To open the Find Panel, do one of the following:

- Open the Find Panel by pressing **CTRL + F**, or;
- Right click on a column header and select **Show Find Panel**.




Figure 135

- Enter a search string in the search box.
- Press **Enter** or click **Find**.

- To clear the search and reset the search box, click **Clear**.

Closing the Find Panel

To close the Find Panel, do one of the following:

- click the  button to the left of the search box, or;
- If the search box is empty, press **Esc** (the shortcut is in effect if the search box has focus), or;
- If the search box is not empty, press **Esc** twice (the shortcut is in effect if the search box has focus).

Auto Filter Row

The automatic filtering row allows data to be filtered on the fly by typing text into that row. When a user types text into this filtering row, a filter condition is automatically created based on the entered value and then applied to the focused column. The automatic filtering row is displayed at the top of the grid.

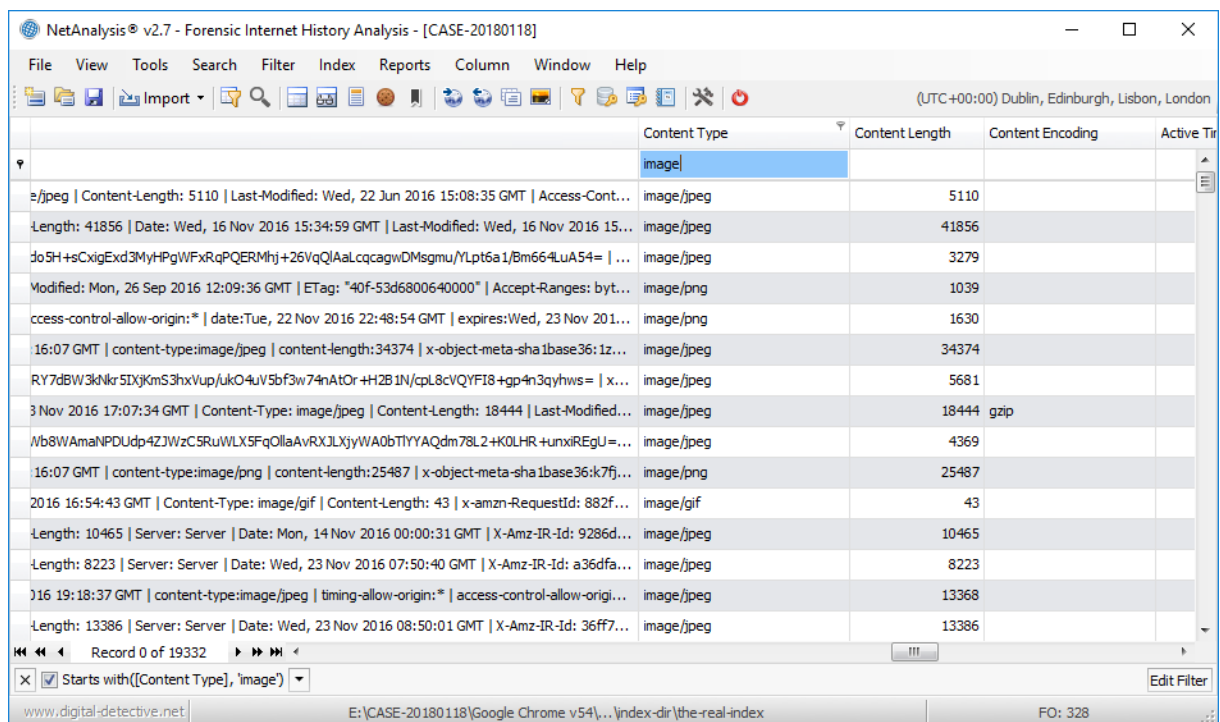
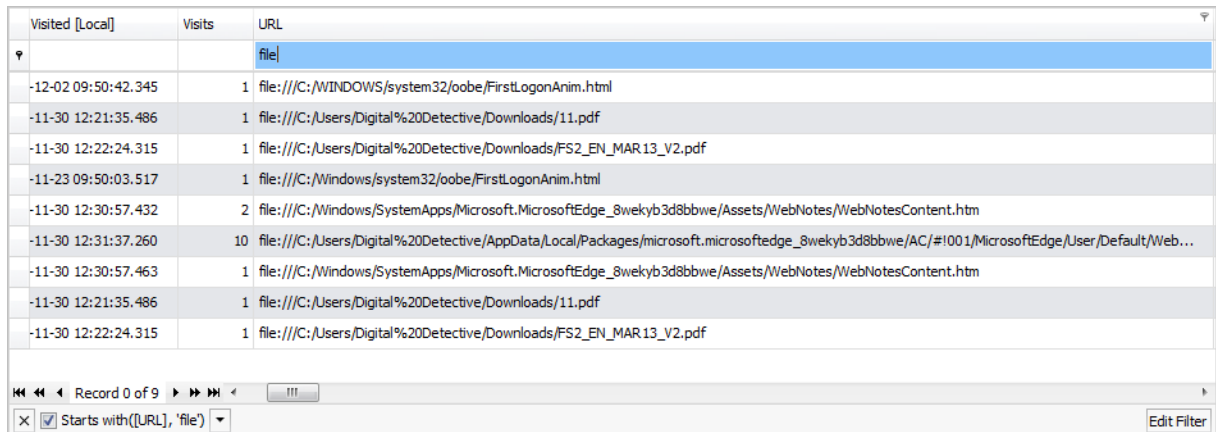


Figure 136

Opening the Auto Filter Row

To open the Auto Filter Row, do one of the following:

- From the Filter menu, select **Filter » Auto Filter Row » Show**, or;
- Right click on a column header and select **Show Auto Filter Row**.



Visited [Local]	Visits	URL
		file
-12-02 09:50:42.345	1	file:///C:/WINDOWS/system32/oobe/FirstLogonAnim.html
-11-30 12:21:35.486	1	file:///C:/Users/Digital%20Detective/Downloads/11.pdf
-11-30 12:22:24.315	1	file:///C:/Users/Digital%20Detective/Downloads/FS2_EN_MAR13_V2.pdf
-11-23 09:50:03.517	1	file:///C:/Windows/system32/oobe/FirstLogonAnim.html
-11-30 12:30:57.432	2	file:///C:/Windows/SystemApps/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/Assets/WebNotes/WebNotesContent.htm
-11-30 12:31:37.260	10	file:///C:/Users/Digital%20Detective/AppData/Local/Packages/microsoft.microsoftedge_8wekyb3d8bbwe/AC/#1001/MicrosoftEdge/User/Default/Web...
-11-30 12:30:57.463	1	file:///C:/Windows/SystemApps/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/Assets/WebNotes/WebNotesContent.htm
-11-30 12:21:35.486	1	file:///C:/Users/Digital%20Detective/Downloads/11.pdf
-11-30 12:22:24.315	1	file:///C:/Users/Digital%20Detective/Downloads/FS2_EN_MAR13_V2.pdf

Figure 137

Closing the Auto Filter Row

To close the Auto Filter Row, do one of the following:

- From the Filter menu, select **Filter » Auto Filter Row » Hide**, or;
- Right click on a column header and select **Hide Auto Filter Row**.

Showing All Records

The number of records displayed in the grid can be reduced in one of two ways:

1. By active Filter;
2. By active Search.

To quickly remove any active Filters and/or Searches, select **Tools » Show All Records** from the main menu.

Web Page Rebuilding

Introduction

Rebuilding a web page from the data contained within a suspect's Temporary Internet Files (also known as the Cache) can be one of the strongest sources of evidence available. NetAnalysis® was the first forensic software to include the functionality for rebuilding web pages from an offline cache.

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. NetAnalysis® has, by far, the most advanced and capable web page rebuilding engine available.

Exporting the Cache

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.



Note: Web pages are rebuilt from a live cache; it is not possible to rebuild cached web pages from the data recovered by HstEx®, you must import data from the live file system.

To extract the cache and rebuild web pages, make sure you have imported data containing live cached entries.

1. Select **Tools » Export and Rebuild Cache**.
2. The live cached files will be extracted to the export folder; the progress window will report on this process;

3. Once the data has been exported, NetAnalysis® will rebuild any web pages and report on the progress.
4. Once this has been completed, click **OK** to close the progress window.
5. The easiest way to review rebuilt web pages is to use the viewing layout. To load the layout, select **Window » Load Window Layout** and select the **Web Page Viewing** layout file.
6. Click the **Filter Manager** tab and double click on the **Live Cached Web Pages** filter.
7. Navigate through the list and view the rebuilt cached web page in the **Viewer** window.
8. The **Index Text** window will show the text-only version of the page.

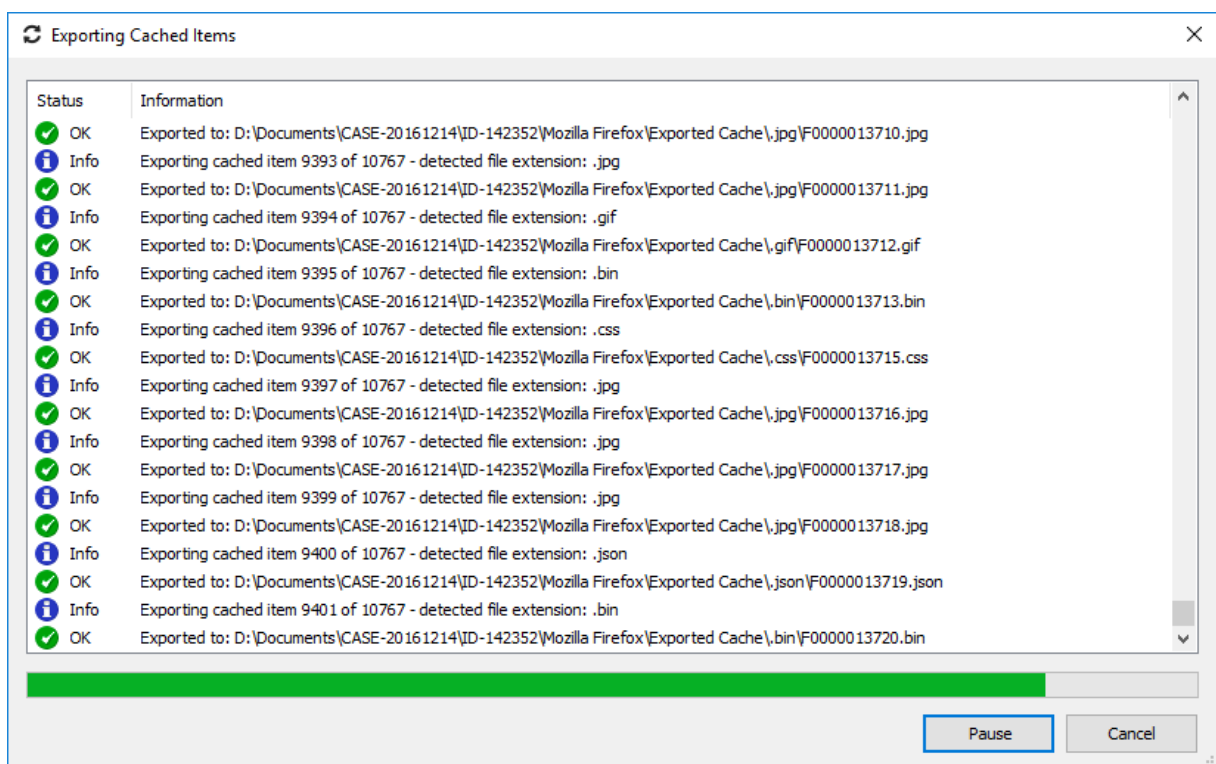


Figure 138

Figure 138 shows the progress window during the cache export process. Figure 139 and Figure 140 show examples of rebuilt web pages.

i Information: NetAnalysis® supports the automatic decompression of cached data which has been compressed using gzip, DEFLATE, Brotli, Zlib and other compression algorithms.

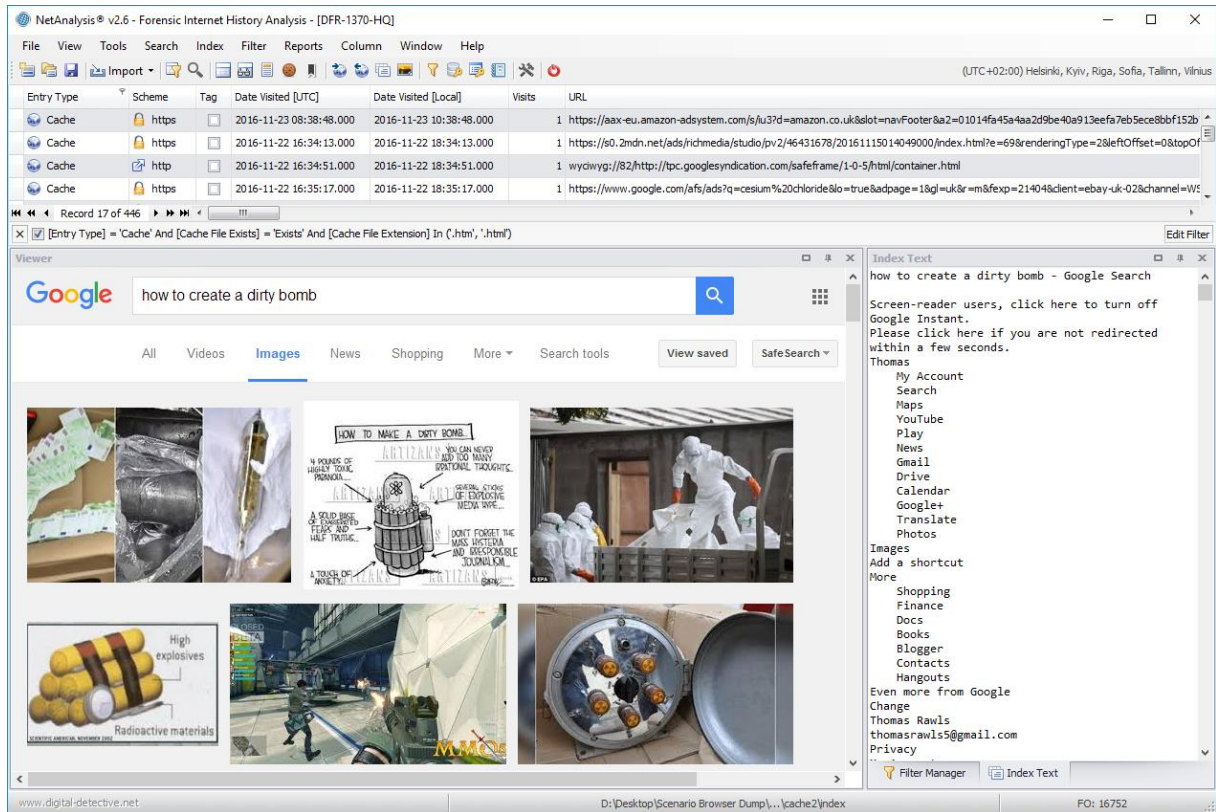


Figure 139

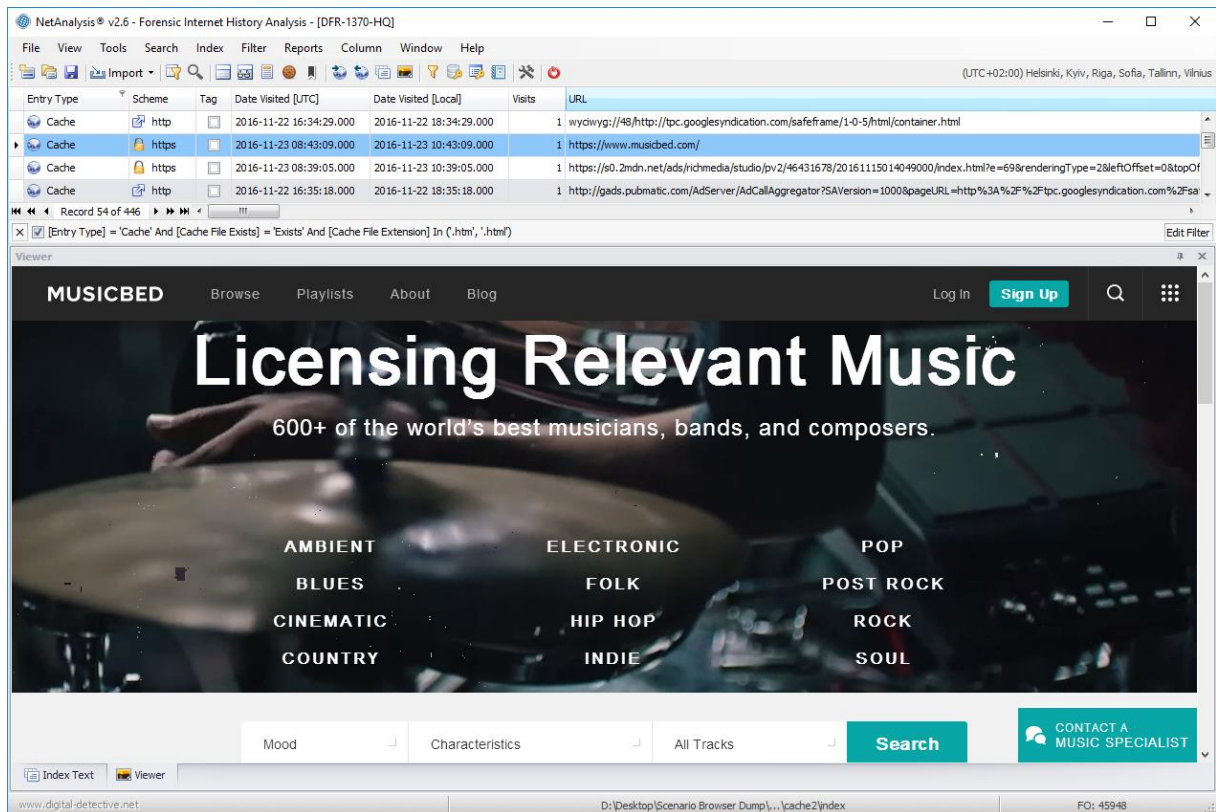


Figure 140

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.

To view a log for a specific page, right click anywhere within the Viewer and select **View Page Rebuild Log**. The HTML log will load into your default browser (as shown in Figure 141).

Source Information

Reference	CASE-20161214 / ID-142352
Page URL	http://ieer.org/resource/fissile-materials/plutonium-factsheet/
Source Path	D:\Desktop\Scenario Browser Dump\Mozilla Firefox v50\2016_11_24_10_02_03\cache\mozilla\firefox\30ag6uog.default\cache2\entries\9F6A2263227A467C32CFCD82AA2FDFD4523629F1
Output File	F0000003695.htm
Rebuild Date	2016-12-16 10:49:57.263

Rebuild Log

URL	Exists	Cache File	Output File
http://ieer.org/wp-content/themes/ieer/js/dropdown.js	✓	A495305E139C80166F59833E11CB36F5E67BDDFD (Length: 2717)	F0000007770.js
http://ieer.org/wp-content/themes/ieer/js/jquery/jquery.js?ver=1.12.4	✓	981DAD549E7C6FEC31A28996C814BC72C3165291 (Length: 97184)	F0000007538.js
http://ieer.org/wp-content/themes/ieer/js/jquery/jquery-migrate.min.js?ver=1.4.1	✓	776BC5558E7A1657DC91173A9077C286B3D5BEE7 (Length: 10056)	F0000007492.js
http://ieer.org/wp-content/themes/ieer/js/jquery.cycle.all.min.js?ver=4.6.1	✓	BF0074AE44DDF583B46323928BA507780AD7644C (Length: 23729)	F0000015031.js
http://p.jwpcdn.com/6/12/jwplayer.js?ver=4.6.1	✓	8C13F10BA8462DE350A96188388251F60B84178F (Length: 25369)	F0000005261.js
http://ieer.org/wp-content/themes/ieer/js/jquery.jplayer.min.js?ver=1.2	✓	4C19F54905BA1B9335F2166F6CAE014F47510C8D (Length: 16498)	F0000006373.js

Figure 141

The Source Information panel shows the case and item reference numbers, the original URL, source file path, output file name and hyperlink to the rebuilt web page. The number in the file name relates to a URN (Unique Reference Number). This value was allocated by NetAnalysis® as the data was imported (see Figure 142).

Source Information	
Reference	CASE-20180123 / ID-155814
Page URL	https://www.amazon.co.uk/gp/ask-widget/askWidget.html?asin=B00ZGBBVYW&askError=&askMessage=&wdg=video_games_display_on_website&requestID=WRPDFAB8QN3FCJE1B3FR&_=1479920110664
Source Path	E:\CASE-20180118\Google Chrome v54\2016_11_24_10_04_05\cache\google-chrome\Default\Cache\57c2a2f133632ca3_0
Offset	197
Length	3052
Output File	F0000000062.html
Rebuild Date	2018-01-25 10:59:22.222

Figure 142

The Rebuild Log contains a list of the elements which make up the page. The log shows the original URL and whether a corresponding cached item was found.

Rebuild Log			
URL	Exists	Cache File	Output File
https://images-na.ssl-images-amazon.com/images/G/01/x-locale/communities/discussion_boards/highlighted_up_arrow_CB320707204_.png	✓	ea5de370583223d8_0 (Offset: 153 Length: 18246)	F0000001399.png
https://images-na.ssl-images-amazon.com/images/G/01/x-locale/communities/discussion_boards/highlighted_down_arrow_CB320707210_.png	✓	b6d08a826b3066bf_0 (Offset: 155 Length: 18254)	F0000001186.png
https://images-na.ssl-images-amazon.com/images/G/01/x-locale/communities/discussion_boards/neutral_up_arrow_CB320707204_.png	✓	3b1d3d0f4464709c_0 (Offset: 149 Length: 18156)	F0000001543.png
https://images-na.ssl-images-amazon.com/images/G/01/x-locale/communities/discussion_boards/neutral_down_arrow_CB320707210_.png	✓	b1ccac4ab322748e_0 (Offset: 151 Length: 18167)	F0000003958.png

Figure 143

As with the Output File link in the Source Information panel, the Output File in the Rebuild Log (see Figure 143) relates to the exported cached item. Clicking on the hyperlink will open the item in the default viewer for that file type. The number also relates to the record URN (as generated by NetAnalysis®).

Web Page Text Content

During 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.

The extracted text can be viewed by clicking the **Index Text** tab. If the window is not visible, it can be opened by selecting **View » Index Text** (see Figure 144).

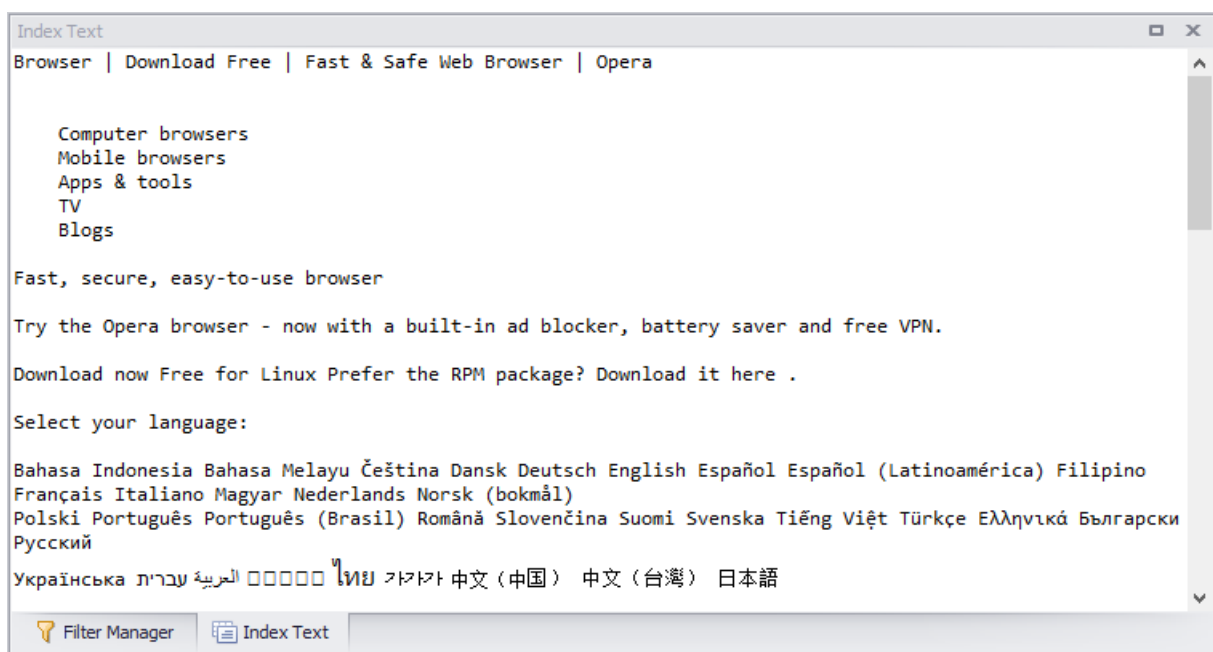


Figure 144

The extracted text can also be indexed and searched separately. For further information on the new indexing feature, please see Indexing and Searching on Page 152.

Export Folder

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. The exported content is saved to the Case Export folder.

To examine the data, select **Tools » Open Case Export Folder**.

Figure 145 shows a typical case export folder with a separate folder for each identified browser type.

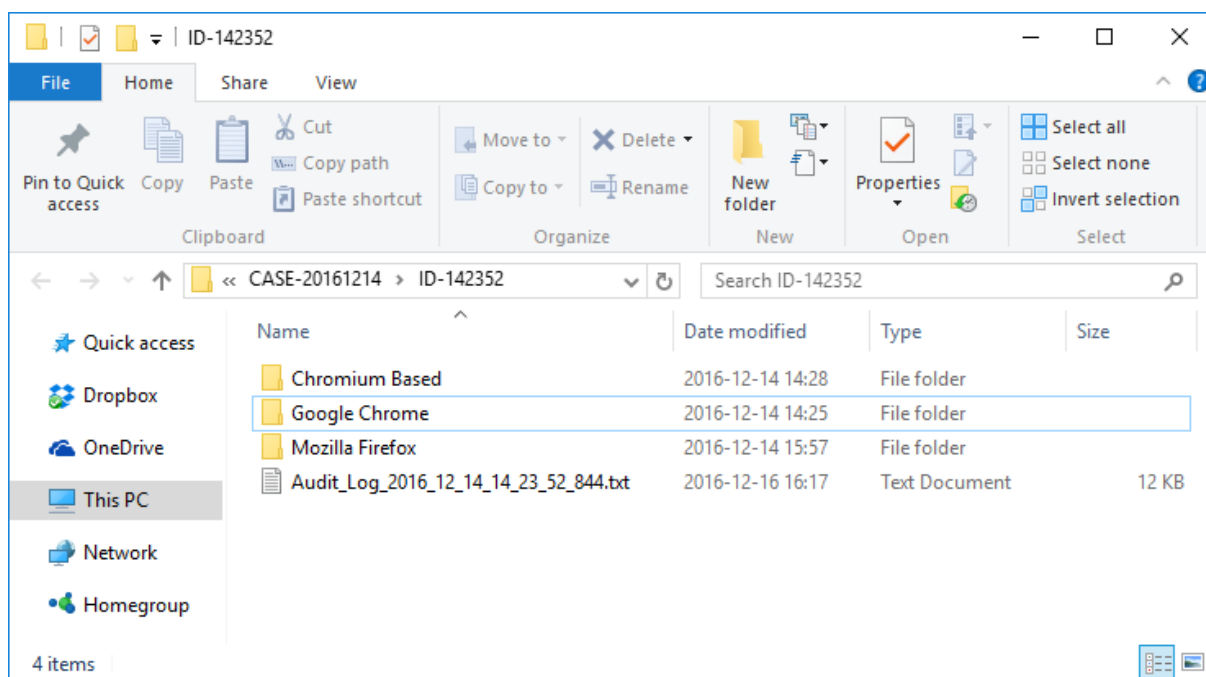


Figure 145

Figure 146 shows the export folder for Mozilla Firefox. The exported cached items can be found in the Exported Cache folder. The rebuilt web pages are stored in the Web Pages folder.

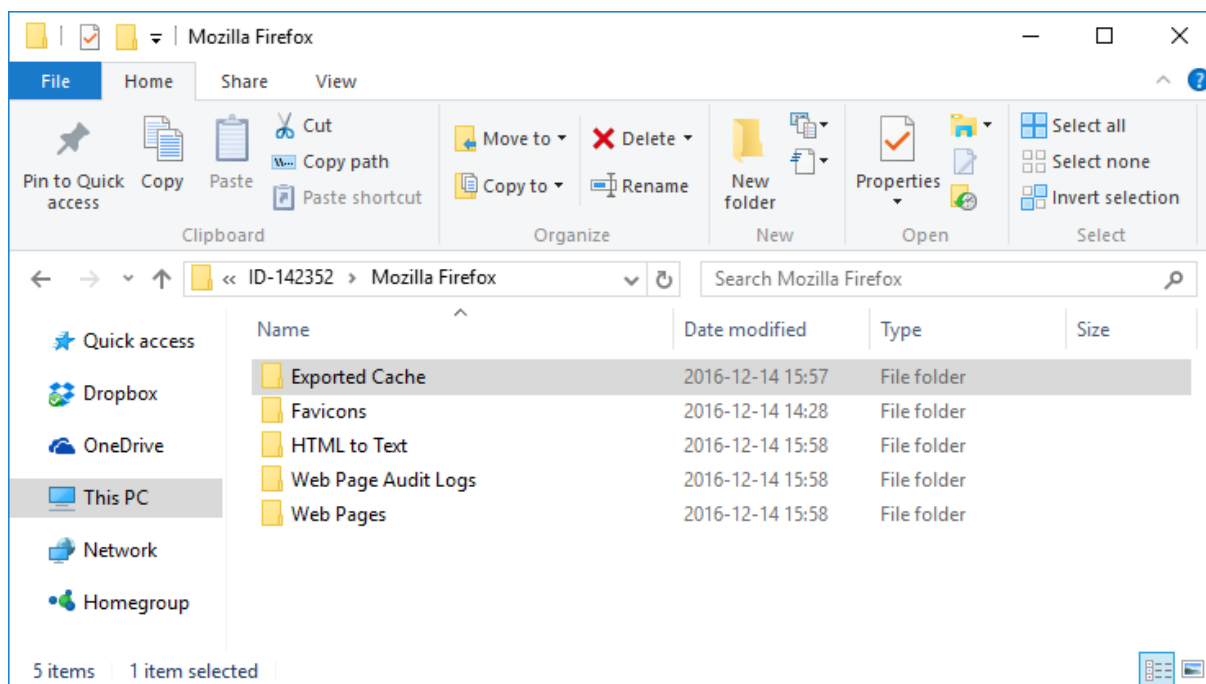


Figure 146

Built-In Viewer

In addition to displaying rebuilt web pages, the built-in viewer can also display web page previews, thumbnails and other file types. Please see Table 16 below for a full breakdown:

Browser	Information
All Browsers	Rebuilt web pages and exported cached data
Apple Safari	Favicon image data
Apple Safari	History web page previews
Apple Safari	Top sites web page previews
Chromium Based	Favicon image data
Chromium Based	History thumbnail image data
Chromium Based	Top sites thumbnail image data

Browser	Information
Microsoft Edge	"Favorite" favicon image data
Microsoft Edge	Reading view HTML page
Microsoft Edge	Reading view dominant image data
Microsoft Edge	Tab image data
Microsoft Edge	Travel Log image data
Mozilla Based	Favicon image data
Mozilla Based	History thumbnail image data
Netscape	Bookmark image data
Opera (Blink)	Bookmark page image data
Opera (Blink)	Stash web page previews
Opera (Presto)	Favicon image data
Opera	Thumbnail image data
Opera Neon	Gallery image data
Opera Neon	Page icon image data
Sleipnir	Favicon image data
Sleipnir	Tab image data

Table 16

Indexing and Searching

Introduction

To assist with rapid evidence identification, we have added a high-performance, full-featured text search engine to NetAnalysis® v2. This feature allows the user to instantly search extracted data and easily match the data back to the original source.

Data Types Added to the Search Index

The following data types can be 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.
- **Chromium Based 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.

Creating a Search Index

Prior to creating a Search Index, it is important that you Export and Rebuild the cache first. This is because, 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 written to a text file so that it can be viewed and indexed for searching.

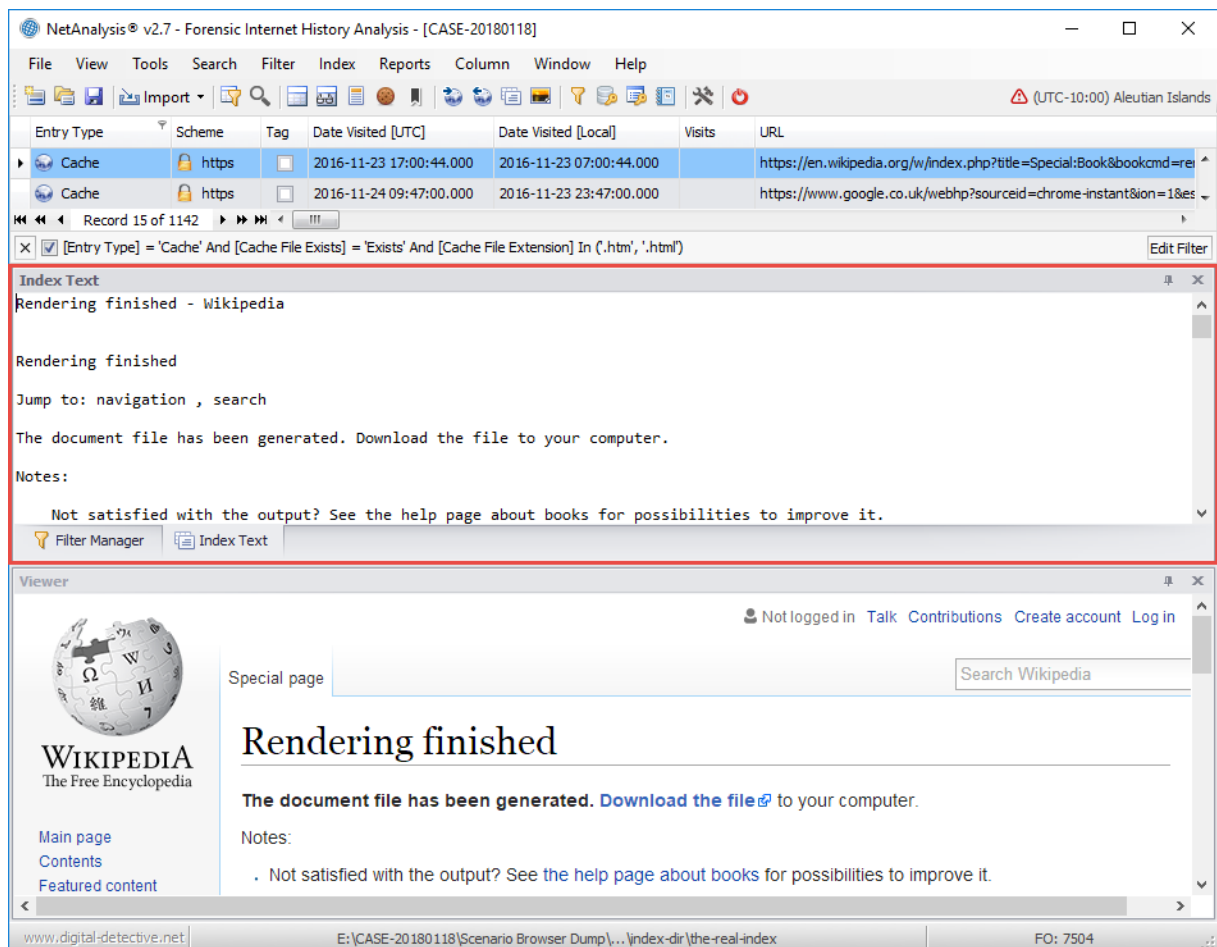


Figure 147

Figure 147 above shows the **Index Text** window displaying extracted content from a web page. This content can be quickly and easily searched once a Search Index has been created.

For further information please see Exporting the Cache on Page 143.



Tip: Always Export and Rebuild the cache prior to creating a Search Index so that web page content can be included in the Search Index Database.

To create a Search Index, please do the following:

1. From the **Index** menu, select **Create Index**.

NetAnalysis® will search through the Case Export Folder looking for supported file types; when they are found, they will be added to the Search Index. The progress window will show which folders are being processed, and will indicate how many files have been added (as shown in Figure 148).

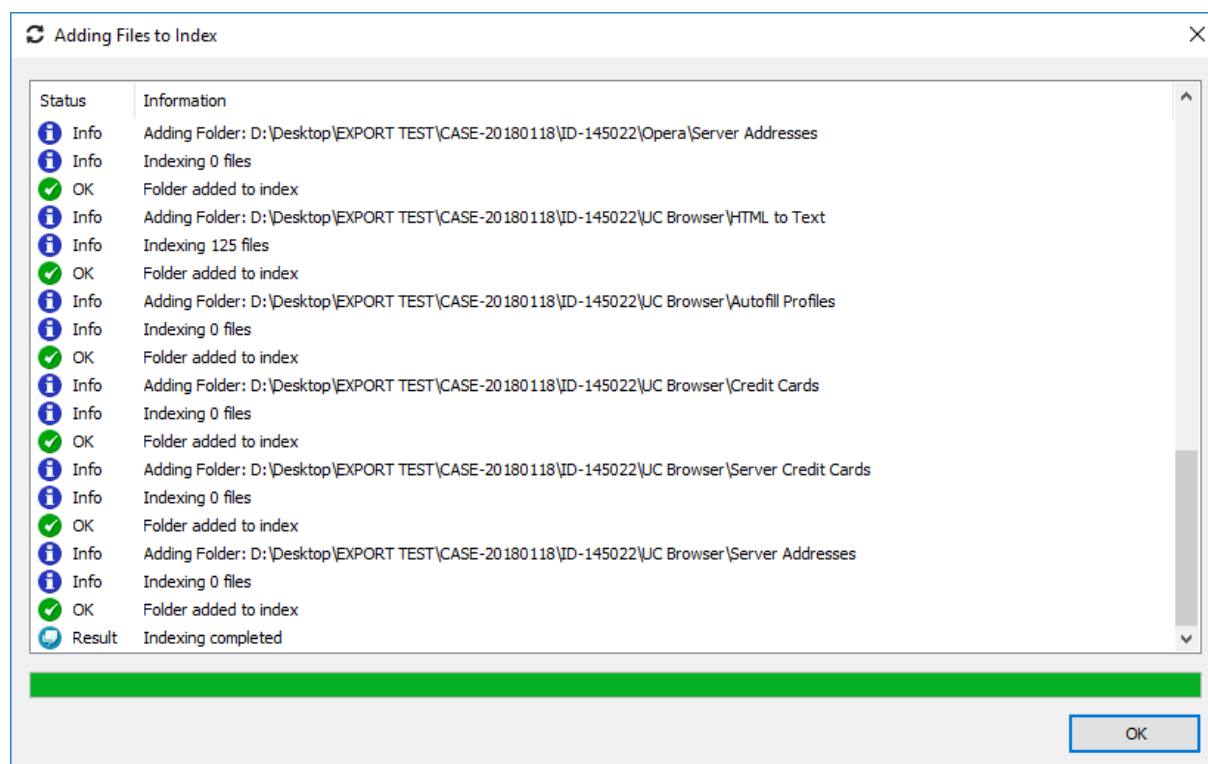


Figure 148

By default, the Search Index will be created and written to a folder called Case Index in the root of the Case Export Folder. If this folder is deleted or missing, you will need to recreate the Search Index.

How to Search

To search the Index, select the following:

1. Click **Index » Search Index** (or click **CTRL + F7**)

This will open the NetAnalysis® Search Index window as shown in Figure 149.

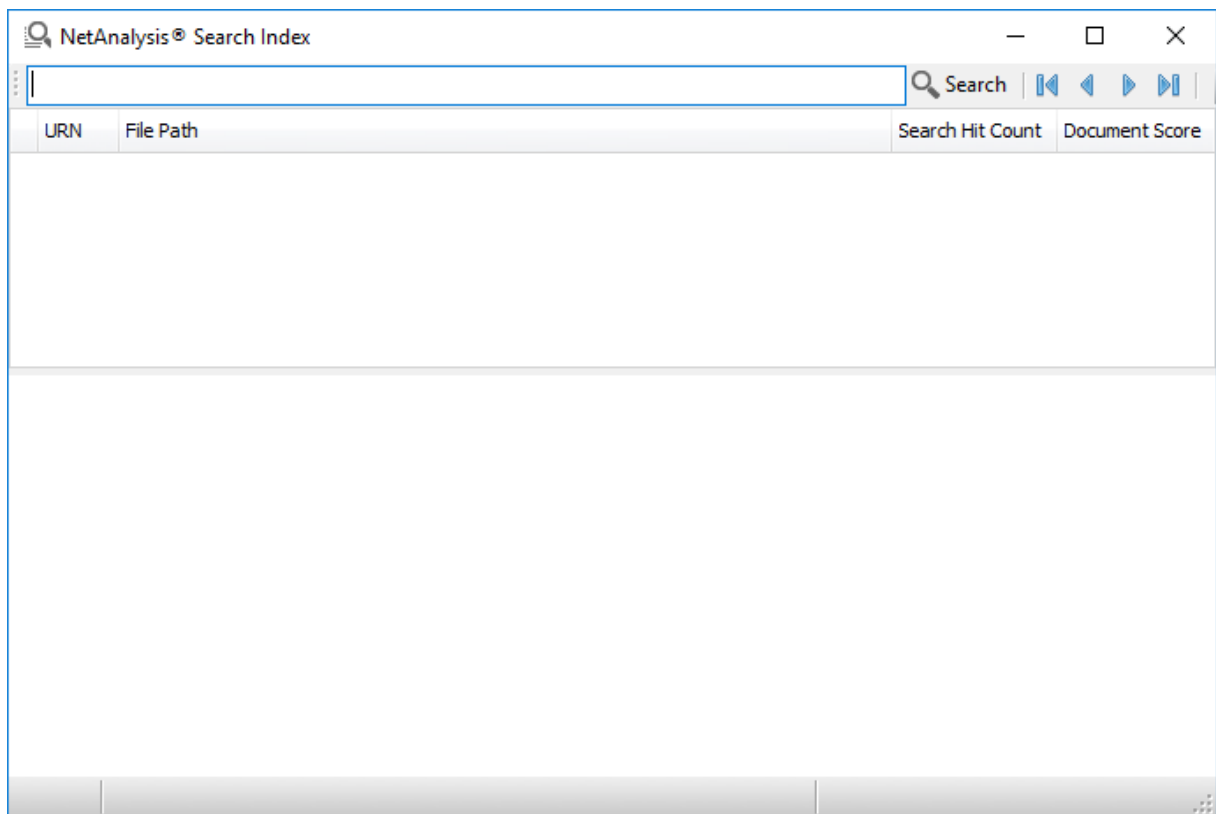


Figure 149

2. To perform a search, click inside the search box and enter some search text;
3. Hit the **Enter** key to search, or click the **Search** button to the right of the search box.

When the search has completed, the Search Index window will display the results, as can be seen in Figure 150.

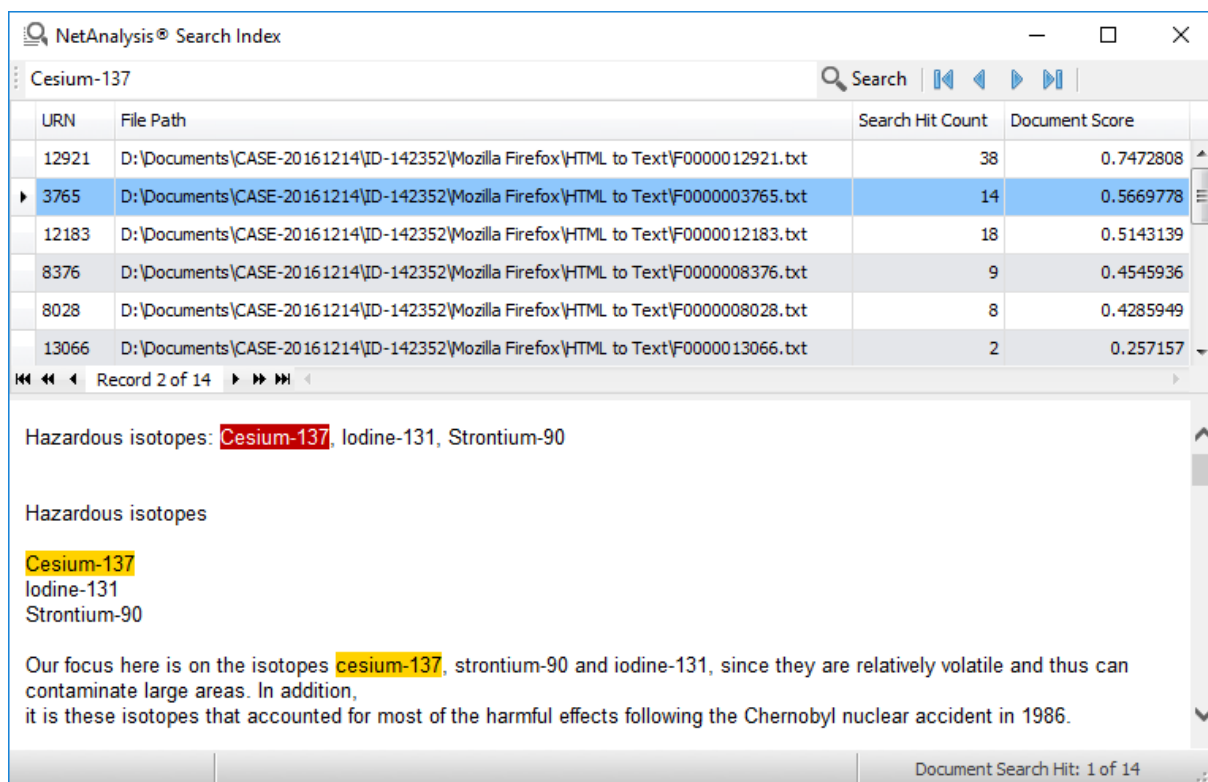


Figure 150

The Search Index result window contains a grid which shows a list of files containing the search hits along with a result view panel. The search query will be highlighted in the view panel.

To cycle through the search hits in the current document, click one of the navigation buttons on the toolbar as shown in Table 17.





Navigation		Information
	Move First	This will highlight the first search hit in the current document.
	Move Previous	This will highlight the previous search hit.
	Move Next	This will highlight the next search hit.
	Move Last	This will highlight the last search hit in the current document.

Table 17

Search Index Columns

The search results are presented in a grid list as shown in Figure 151 below.

URN	File Path	Search Hit Count	Document Score
▶ 19120	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000019120.txt	38	0.9509132
9964	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000009964.txt	14	0.721478
18382	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000018382.txt	18	0.6544633
14575	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000014575.txt	9	0.5784693
14227	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000014227.txt	8	0.5453861
1450	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Google Chrome\HTML to Text\F0000001450.txt	2	0.3272317

Record 1 of 21

Figure 151

The data contained in each column is as follows:

URN (Unique Reference Number)

NetAnalysis® generates a unique reference number for every entry added to the main grid in a workspace. URNs allow the user to quickly identify and access a specific record. In this case, the URN relates to the original record in the grid. You can easily move back to source record for this search hit. See Identifying the Original Source on Page 158.

File Path

The File Path column shows the path to the exported file containing the search hit.

Search Hit Count

This column contains a count of the number of times the search query appears in the current document.

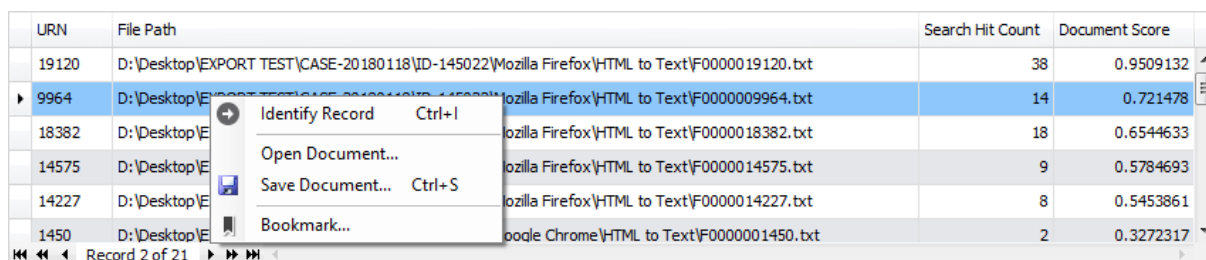
Document Score

NetAnalysis® indexed search scoring uses a combination of the Vector Space Model (VSM) of Information Retrieval and the Boolean model to determine how relevant a given document is to a specific query. In general, the idea behind the VSM is the more times a query term appears in a document relative to the number of times the term appears in all the documents in the collection, the more relevant that document is to the query.

Identifying the Original Source

From the Search Index window grid list, it is easy to identify the original source data which contains the search hit.

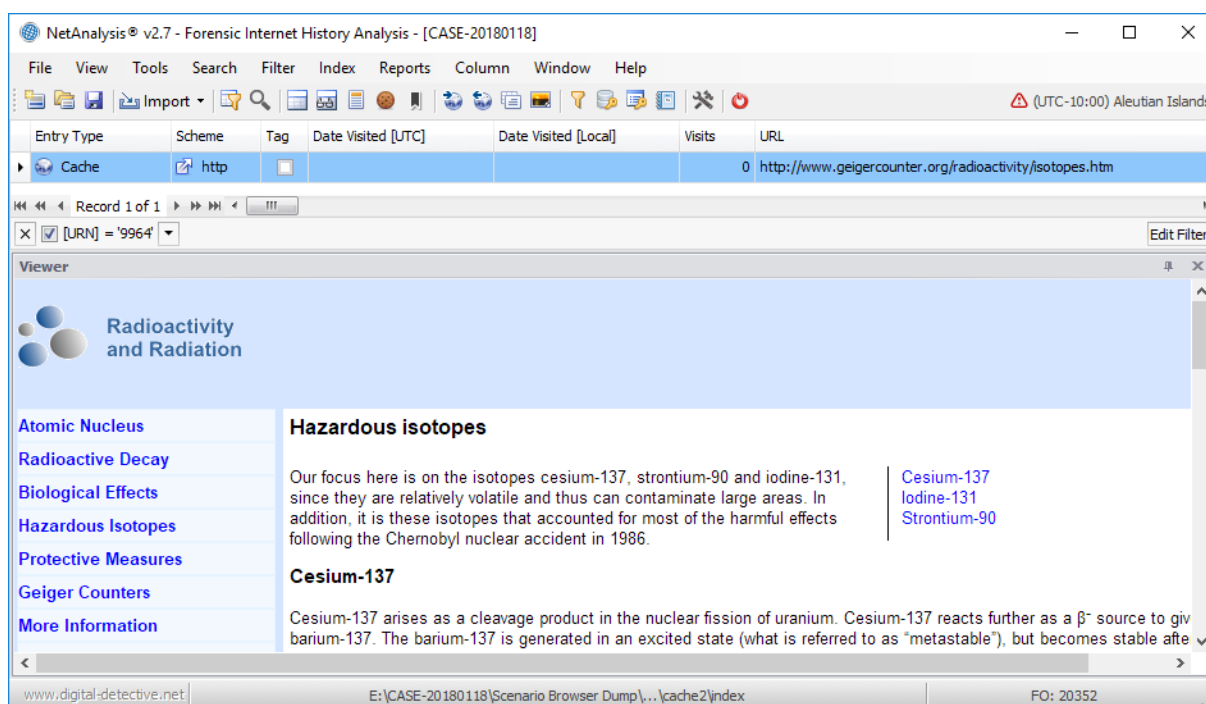
1. Right click on a search hit entry and click **Identify Record** (or **CTRL + I**) as shown in Figure 152.



URN	File Path	Search Hit Count	Document Score
19120	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000019120.txt	38	0.9509132
9964	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F000009964.txt	14	0.721478
18382	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000018382.txt	18	0.6544633
14575	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000014575.txt	9	0.5784693
14227	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Mozilla Firefox\HTML to Text\F0000014227.txt	8	0.5453861
1450	D:\Desktop\EXPORT TEST\CASE-20180118\ID-145022\Google Chrome\HTML to Text\F0000001450.txt	2	0.3272317

Figure 152

This will execute a filter in the main grid, identifying the record with the corresponding URN (as shown in Figure 153).



NetAnalysis® v2.7 - Forensic Internet History Analysis - [CASE-20180118]

File View Tools Search Filter Index Reports Column Window Help

Entry Type Scheme Tag Date Visited [UTC] Date Visited [Local] Visits URL

Cache http 0 http://www.geigercounter.org/radioactivity/isotopes.htm

Record 1 of 1

[X] [URN] = '9964'

Viewer

Radioactivity and Radiation

Atomic Nucleus
Radioactive Decay
Biological Effects
Hazardous Isotopes
Protective Measures
Geiger Counters
More Information

Hazardous isotopes

Our focus here is on the isotopes cesium-137, strontium-90 and iodine-131, since they are relatively volatile and thus can contaminate large areas. In addition, it is these isotopes that accounted for most of the harmful effects following the Chernobyl nuclear accident in 1986.

Cesium-137
Iodine-131
Strontium-90

Cesium-137

Cesium-137 arises as a cleavage product in the nuclear fission of uranium. Cesium-137 reacts further as a β^- source to give barium-137. The barium-137 is generated in an excited state (what is referred to as "metastable"), but becomes stable after...

www.digital-detective.net | E:\CASE-20180118\Scenario Browser Dump\...\cache2\index | FO: 20352

Figure 153

Viewing the Indexed Document

From the Search Index window grid list, it is easy to open the exported text document which contains the search hit:

1. Right click on a search hit entry and click **Open Document**.

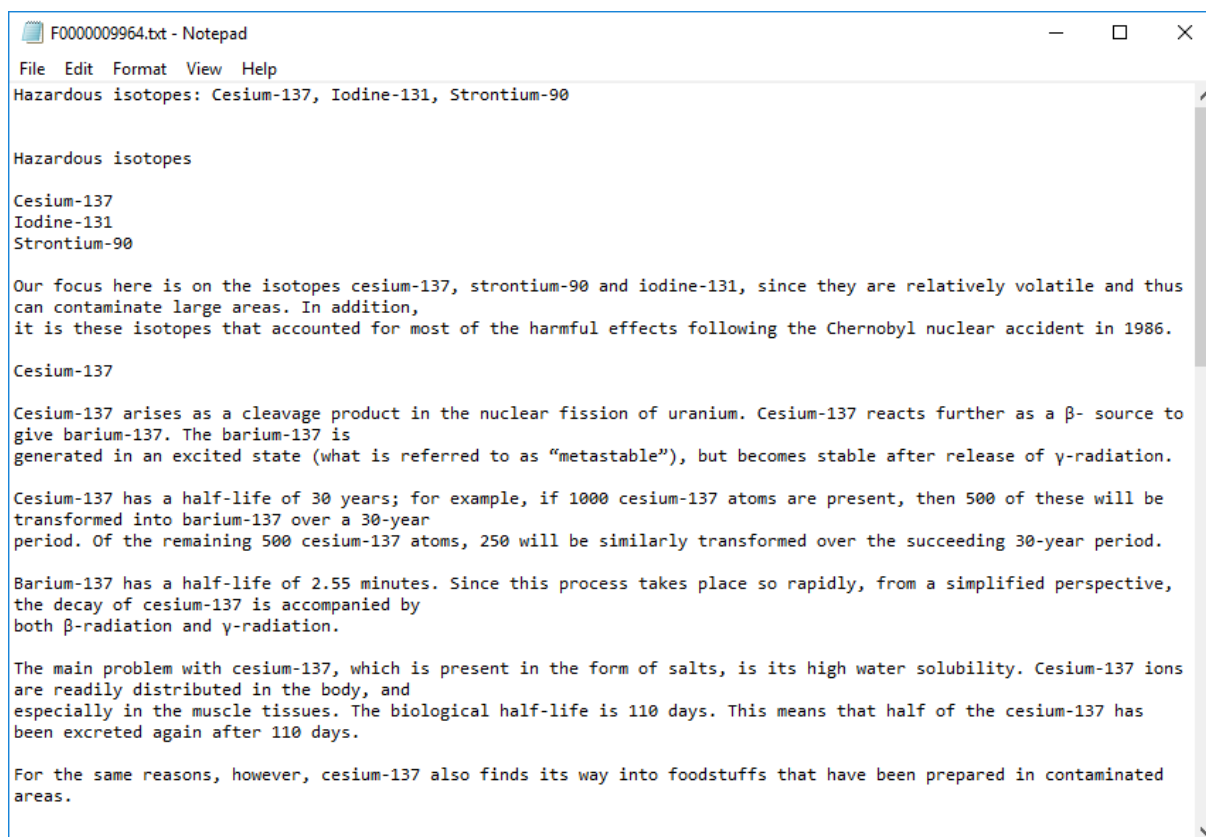


Figure 154

This will open the document in the default viewer for text files.

Saving the Indexed Document

From the Search Index window grid list, select the entry which contains the search hit:

1. Right click on a search hit entry and click **Save Document**.
2. When the Save As window opens, select a location to save the file.

3. Click the **Save** button to save the file to the selected location.

Adding a Bookmark to the Original Source

When reviewing search hits in the Search Index window, you may wish to add a bookmark to the original source record in the main grid. This can be performed easily from here. Select the entry which contains the search hit and do the following:

1. Right click on a search hit entry and click **Bookmark**.

This will open the Bookmark window as shown in Figure 155.

2. Click in the text box and enter the text for the bookmark.
3. Click **OK** to submit the bookmark.

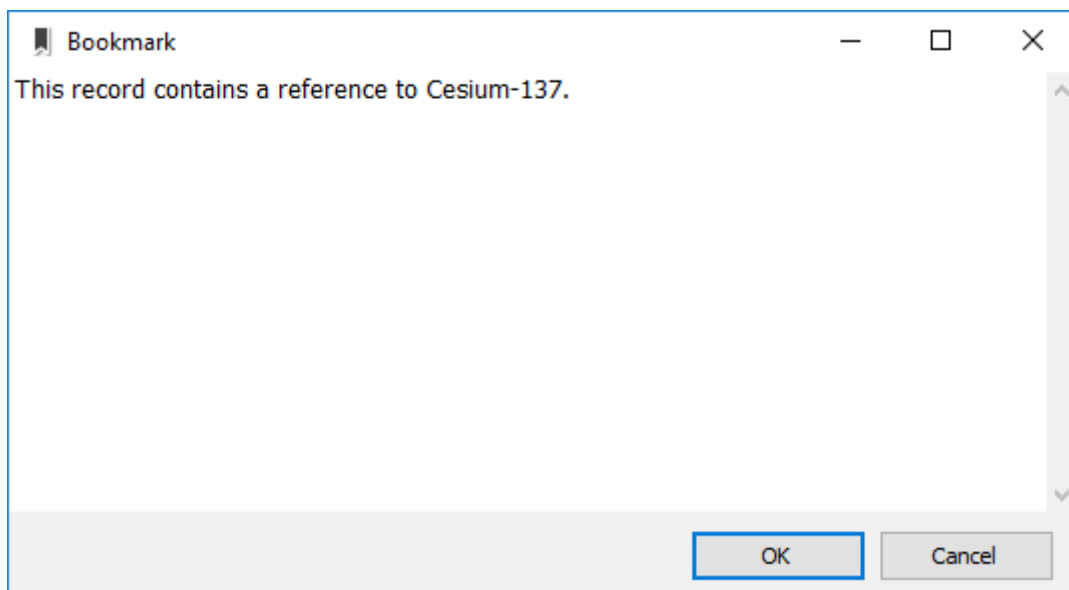


Figure 155

Query Parser Syntax

NetAnalysis® provides a rich query language through the Query Parser. This allows the search index to be queried using single terms, phrases or multiple terms combined together with Boolean operators to form more complex queries.

A query is broken up into terms and operators. There are two types of terms: Single Terms and Phrases:

- A Single Term is a single word such as "test" or "hello".
- A Phrase is a group of words surrounded by double quotes such as "credit card".

Wildcard Searches

The query parser supports single and multiple character wildcard searches within single terms (not within phrase queries).

- To perform a single character wildcard search, use the "?" symbol.
- To perform a multiple character wildcard search, use the "*" symbol.

The single character wildcard search looks for terms that match that with the single character replaced. For example, to search for "text" or "test" you can use the search:

```
te?t
```

Multiple character wildcard searches look for zero or more characters. For example, to search for test, tests or tester, you can use the search:

```
test*
```

You can also use the wildcard searches in the middle of a term.

```
te*t
```



Note: You cannot use a "*" or "?" symbol as the first character of a search.

Fuzzy Searches

The query parser also has the ability to perform fuzzy searches, which are based on the Levenshtein Distance, or Edit Distance algorithm. Fuzzy searching is the technique of finding strings that match a pattern approximately rather than exactly. This is particularly useful when looking for words that may have been misspelled or have an alternative spelling.

To perform a fuzzy search, use the tilde, "~", symbol at the end of a single word term. For example, to search for a term similar in spelling to "roam" use the following fuzzy search:

```
roam~
```

This search will find terms like foam and roams.

An additional (optional) parameter can specify the required similarity. The value should be between 0 and 1; with a value closer to 1 only terms with a higher similarity will be matched.

For example:

```
roam~0.8
```

The default that is used if the parameter is not given is 0.5.

Proximity Searches

Another feature of the query parser is the support for proximity searches. This is the ability to find words that are within a specific distance from each other. For example, to search for "caesium" and "nuclear" within 10 words of each other, use the search:

```
"caesium nuclear"~10
```

Boosting a Term

The query parser provides the relevance level of matching documents based on the terms found. To boost a term, use the caret, "^", symbol with a boost factor (a number) at the end of the term you are searching. The higher the boost factor, the more relevant the term will be.

Boosting allows the user to control the relevance of a document by boosting its term. For example, if you are searching for:

```
caesium bomb
```

and you want the term "caesium" to be more relevant, boost it using the ^ symbol along with the boost factor next to the term. You would type:

```
caesium^4 bomb
```

This will make documents with the term "caesium" appear more relevant. You can also boost Phrase Terms as in the example:

```
"caesium bomb"^4 "dirty bomb"
```

By default, the boost factor is 1. Although the boost factor must be positive, it can be less than 1 (e.g. 0.2)

Boolean Operators

Boolean operators allow terms to be combined through logic operators. The query parser supports **AND**, **+**, **OR**, **NOT** and **-** as Boolean operators.



Note: Boolean operators must contain ALL CAPITAL LETTERS.

The OR operator is the default conjunction operator. This means that if there is no Boolean operator between two terms, the OR operator is used. The OR operator links two terms and finds a matching document if either of the terms exist in a document. This is equivalent to a union using sets. The symbol **||** can be used in place of the word OR.

To search for documents that contain either "dirty bomb" or just "bomb", use the query:

```
"dirty bomb" bomb
```

or

```
"dirty bomb" OR bomb
```

AND

The AND operator matches documents where both terms exist anywhere in the text of a single document. This is equivalent to an intersection using sets. The symbol **&&** can be used in place of the word AND.

To search for documents that contain "dirty bomb" and "caesium 137" use the query:

```
"dirty bomb" AND "caesium 137"
```

+

The + or required operator requires that the term after the + symbol exists somewhere in the document.

To search for documents that must contain "fission" and may contain "bomb" use the query:

```
+fission bomb
```

NOT

The NOT operator excludes documents that contain the term after NOT. This is equivalent to a difference using sets. The symbol ! can be used in place of the word NOT.

To search for documents that contain "caesium 137" but not "dirty bomb" use the query:

```
"caesium 137" NOT "dirty bomb"
```

-

The - or prohibit operator excludes documents that contain the term after the - symbol.

To search for documents that contain "caesium 137" but not "dirty bomb" use the query:

```
"caesium 137" -"dirty bomb"
```

Grouping

The query parser supports using parentheses to group clauses to form sub queries. This can be very useful if you want to control the Boolean logic for a query.

To search for either "dirty" or "fission" and "bomb" use the query:

```
(dirty OR fission) AND bomb
```

This eliminates any confusion and makes sure that the term bomb must exist and that either term dirty or fission may exist.

Escaping Special Characters

The following special characters must be escaped if they are part of the query syntax. The following list shows all the current special characters:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

To escape these characters, use the \ before the character. For example, to search for (1+1):2 use the query:

```
\(1\+1\)\:2
```

Reporting

Introduction

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 graphical and chart 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.

As well as a built-in detailed report that can be previewed on screen, sent to a printer or exported in a number of different formats, the real power to the reporting is that the user is now able to design their own report templates. This means you can create custom reports to exactly meet your own specific requirements. A report template can be used with different NetAnalysis® Workspaces (either all records or a selected subset) and can be shared with other users.

A number of User Defined built-in report templates are included with NetAnalysis®. These can be used unmodified or can be customised by changing the layout and adding or removing data fields and text labels using the Report Designer.

The Report Designer is also used to design a custom report template, giving the end user complete control over the report content and the report layout. As well as its report editing capabilities, the Report Designer also allows the report to be previewed on screen, sent to a printer or exported to file.

Preview Detailed Report

The built-in detailed report includes all the key information you need to evidence a URL record.

The report is generated against the visible records in the main user window. To report against a subset of all records in the grid, you can first apply a filter using the Filter Editor or filter records using the Find Panel. To apply a record filter, please see Filtering and Searching on Page 115.

To generate the report, select **Reports » Preview Detailed Report**. Figure 156 shows an example Detailed Report displayed in the report preview window.

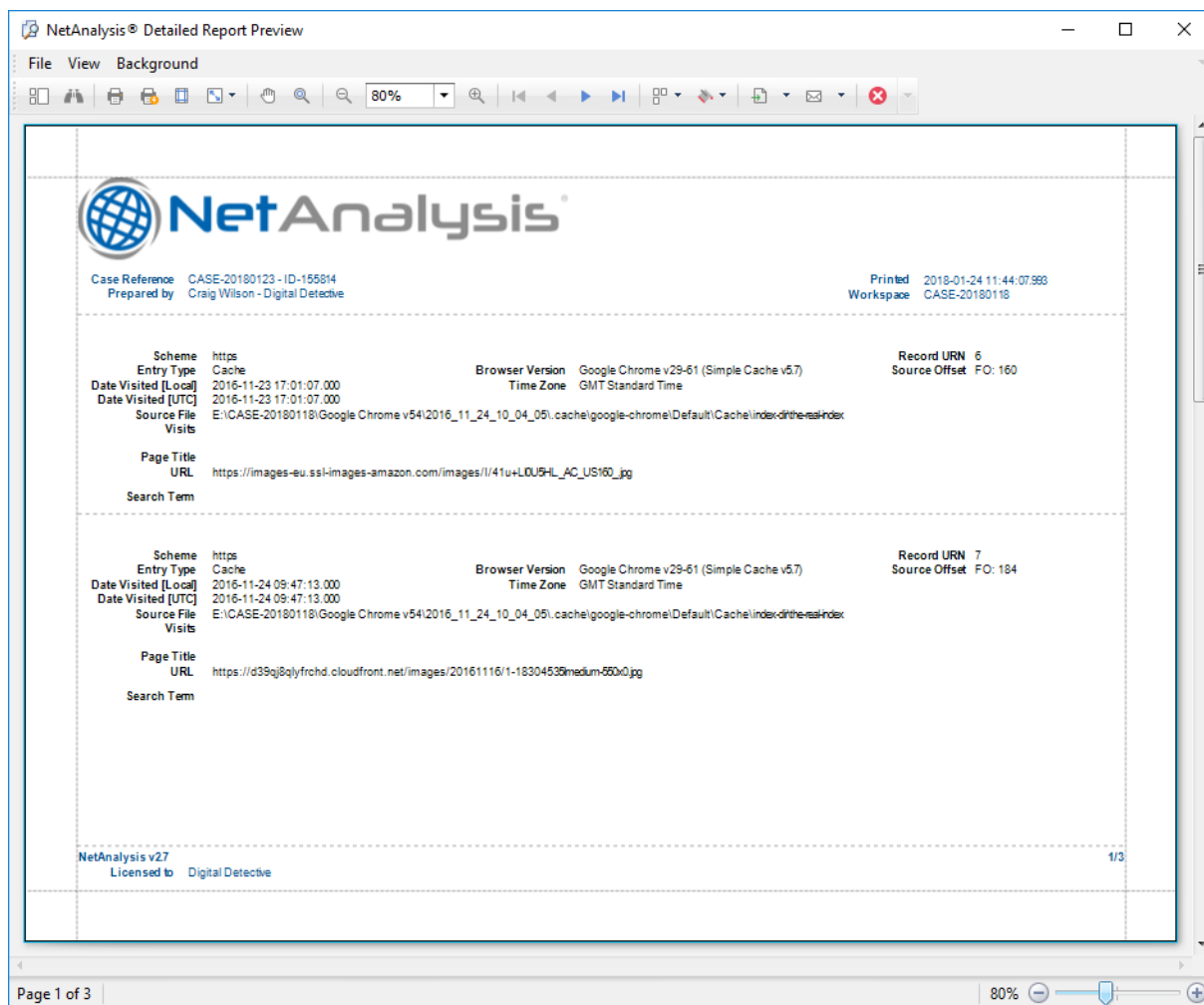


Figure 156










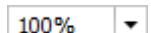






Report Preview Window

The toolbar for the Report Preview Window can be seen in Figure 157.



Figure 157

For a full description of each button in the Report Preview Window toolbar, please see Table 18 below.

Button		Information
	Thumbnails	Shows/Hides the thumbnails pane. This allows quick navigation through the report pages by clicking on a thumbnail to move to the corresponding page in the report.
	Search	Shows/Hides the search pane. The search pane allows you to search through the report for specific text (also press CTRL + F on the keyboard). Use the Next button (or press ENTER on the keyboard) and the Previous button to move between occurrences. There is also a settings button to make the search case sensitive and/or match whole words only.
	Print	Prints the current report via the Print Dialog which allows the print settings to be customised.
	Quick Print	Prints the current report to the default printer without customising any print settings.
	Page Setup	Displays the Page Setup Dialog which allows the report page orientation, paper size and page margins to be set.
	Scale	Allows the current report to be scaled to a required percentage value or to fit into a required number of pages.
	Hand Tool	Activates/Deactivates the hand tool which allows you to navigate the report using the mouse. Click and hold down the left mouse button in the report page and drag the mouse pointer to scroll through the report.
	Magnifier	Activates/Deactivates the magnifier tool which allows you to switch between 100% and fit whole page views. Toggle between views by clicking anywhere in the report page.
	Zoom Out	Changes the zoom factor by zooming out (also press CTRL + Minus key or press and hold down CTRL and rotate the mouse wheel).
	Zoom In	Changes the zoom factor by zooming in (also press CTRL + Plus key or press and hold down CTRL and rotate the mouse wheel).
	Zoom	Changes the zoom factor for the report. Either select a value from the list or enter a value into the zoom factor box.
	First Page	Moves to the first page of the current report.
	Previous Page	Navigates to the previous page of the current report.
	Next Page	Navigates to the next page of the current report.
	Last Page	Moves to the last page of the current report.
	Multiple Pages	Resizes the report so that multiple pages are shown on screen.





Button	Information	
	Background Color	Adds a background colour to the current report.
	Export Document	Export current report to a file. Select the required export format from the list and you will be prompted to set format specific export options before the Save As Dialog allows you to set the export file name. Once exported you will be prompted whether to preview the exported report file.
	Send via E-Mail	Export current report and send via email. Select the required export format from the list and you will be prompted to set format specific export options before the Save As Dialog allows you to set the export file name. Once exported, the report file will be attached to a new empty email message created in your default mail client.
	Exit	Exits out of previewing the current report and closes the report preview window.

Table 18

Working with a Report Preview Selection

As well as printing and exporting the complete report from the report preview window, you can also print and copy only a selected portion of the report.

Select the required report content by holding the left mouse button and dragging the mouse pointer to create a selection box. The selected report elements will be highlighted in blue (as shown in Figure 158).

Scheme	https	Browser Version	Google Chrome v29-61 (Simple Cache v5.7)
Entry Type	Cache	Time Zone	GMT Standard Time
Date Visited [Local]	2016-11-23 17:01:07.000		
Date Visited [UTC]	2016-11-23 17:01:07.000		
Source File Visits	E:\CASE-20180118\Google Chrome v54\2016_11_24_10_04_05\cache\google-chrome\Default\Cache\index-dir-the-real-index		
Page Title			
URL	https://images-eu.ssl-images-amazon.com/images/I/41u+LI0U5HL_AC_US160.jpg		
Search Term			

Figure 158

Right click within the highlighted area to display the context menu (as shown in Figure 159).

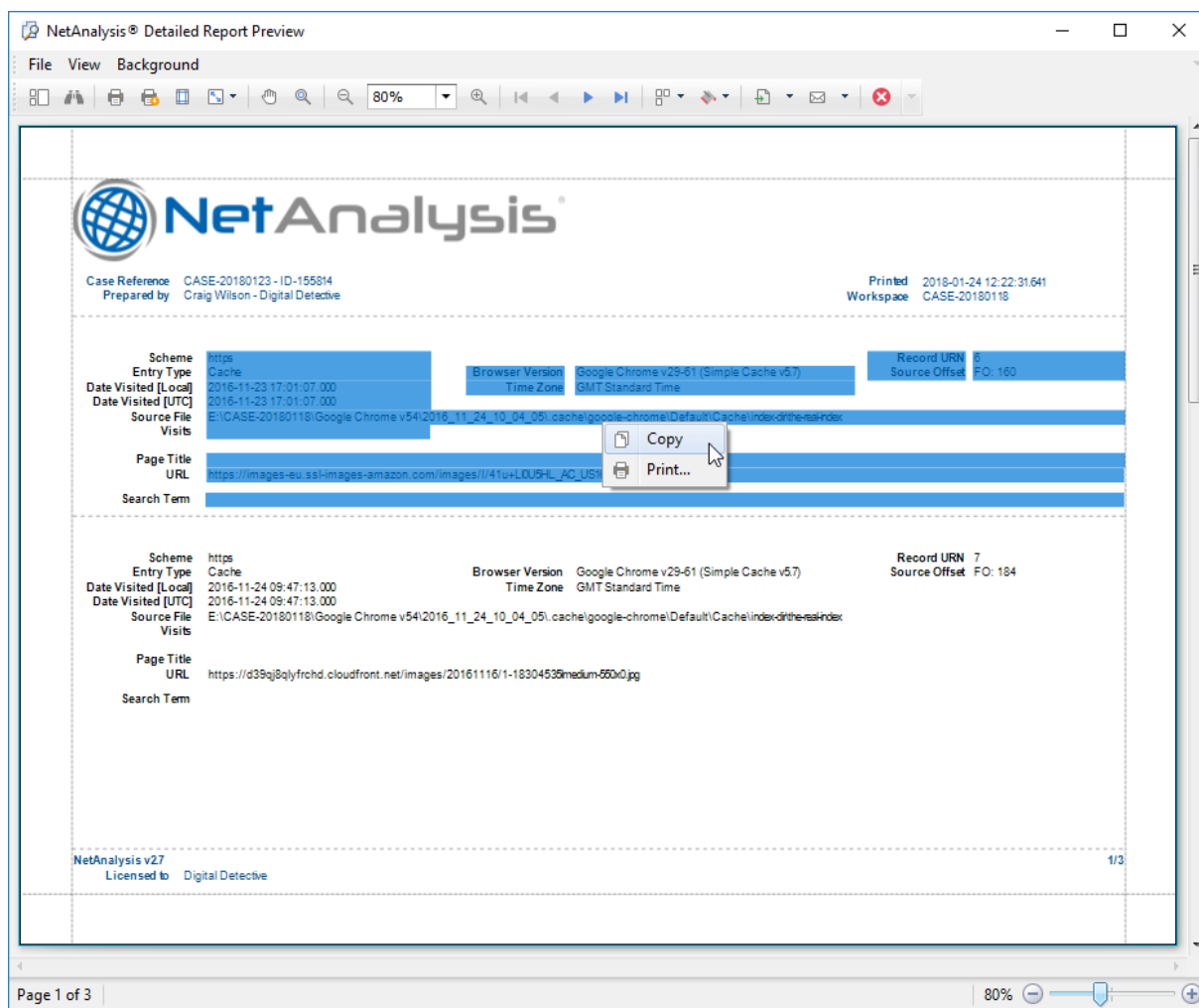


Figure 159

To print the selection, select **Print** from the context menu. The Print Dialog will be displayed to allow the print settings to be customised before sending to the printer.

To copy the selection to the clipboard, select **Copy** from the context menu (or press **CTRL + C** on the keyboard). The selection can then be pasted from the clipboard into a third-party editor compatible with one of the supported export formats. The pasted report content will automatically be converted to the target format.

Report Designer

The NetAnalysis® Report Designer provides the forensic examiner with a complete end user report designer allowing you to design a new report template or to customise an existing built-in report template.

A report template is bound to the data displayed in the grid on the main user window. To report against a subset of all records in the grid you can first apply a filter using the Filter Editor or filter records using the Find Panel. To apply a record filter, please see Filtering and Searching on Page 115.

A report template is normally designed to include data fields corresponding to the columns from the grid. For example, you could add a Label control to a report template which is bound to the **URL** column in the grid; when the report is previewed against its bound data records it will display the URL data field from every record visible in the grid.

The main capabilities of the Report Designer allow the end user to:

- Add dynamic information (data fields and report parameter fields) to a report.
- Add static information (text and images) to a report.
- Add auxiliary information (such as page numbers and current date and time) to a report.
- Change the font, colour, appearance and alignment of report elements.
- Add data grouping and sorting of the report data fields.
- Add calculated fields to a report.
- Create both tabular and chart-based reports.
- Save the report template for later reuse and sharing.
- Preview the report against the data records in the main grid while it is being designed using the built in Preview and HTML Views.
- Send the previewed report to a printer.
- Export the previewed report to a number of different formats.

Creating a New User Defined Report

To create a new report, select **Reports » User Defined Reports » New Report**. The Report Designer window will appear containing a new blank report template (as shown in Figure 160).

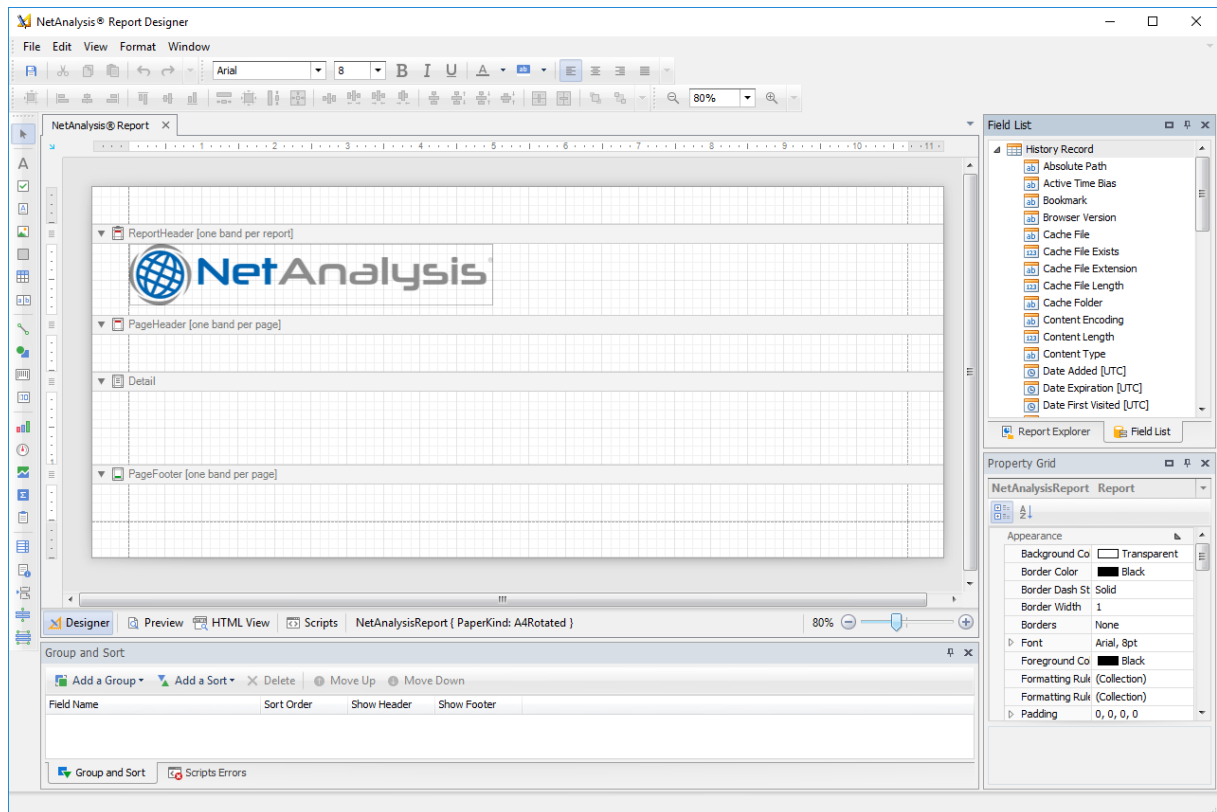


Figure 160

Report Designer Window Layout

The Report Designer window contains a number of user interface elements to allow the report template to be built. The main elements are:

- **Main menu:** Groups various commands under the categories: File, Edit, View, Format and Window. These commands largely correspond to the buttons contained in the Report Designer toolbars.
- **Design panel:** The main area of the Report Designer where the report is constructed and previewed. It provides four tabs: Designer, Preview, HTML View and Scripts to allow you to edit the report, display the report in print preview and web page preview and to manage and customise report scripts in the Scripts editor.
- **Toolbars:** Table 19 holds a detailed explanation about the function of each toolbar.
- **Dock Panels:** Table 20 holds a detailed explanation about the function of each dock panel.

Toolbar	Information
Main Toolbar	Contains commands to save the current report template; to cut, copy and paste controls, as well as undo and redo actions.
Formatting Toolbar	Contains commands related to text formatting. These commands are used when editing the text of a control using its in-place editor.
Layout Toolbar	Contains commands that manage the size and location of individual and multiple report elements.
Zoom Toolbar	Contains commands for changing the zoom factor for the report (both in the design and preview modes).
Status Bar	Displays information about the element that is currently being hovered over by the mouse pointer and also provides tips regarding the current user actions.
Toolbox Bar	Lists all available controls that can be added to the report. A control from the toolbox can be dragged and dropped onto the report's design panel.

Table 19

Dock Panel	Information
Field List	Displays the list of data fields available to the report (the list of columns from the grid on the main NetAnalysis® user window) as well as the report parameters and any calculated fields.
Report Explorer	Displays a tree-like hierarchy of report elements and allows you to manage a report's collection of formatting rules and visual styles.
Property Grid	Lists all properties available for a selected object (either the report itself or any of its elements).
Report Gallery	Stores frequently used report controls, styles and full report layouts and allows you to use them across different reports.
Group and Sort	Allows you to group and sort data in a report.
Script Errors	Displays the report scripts validating results. Click an error to navigate to the corresponding line in the Scripts editor.

Table 20

Designing a Report

The Report Designer design panel contains the Designer tab where the layout for the report is constructed and displayed. It allows you to design the report structure and content by managing the report bands and report controls and setting their properties appropriately.

A report is built upon bands, where each band represents a different section of the report (such as detail, report header and footer, page header and footer, group header and footer). The report bands allow you to select exactly where a report control should be printed and how many times. Table 21 holds details of the available report bands.

Bands	Information
Detail	This is the core part of the report and unlike other bands it cannot be deleted. The contents of this band will be repeated for each record displayed in the main NetAnalysis® grid.
Group Header and Footer	These bands are shown above and below each group in the report. The Group Header can be used to display static label headers for the group by fields. The Group Footer can be used to display group totals or group page numbers.
Report Header and Footer	These bands are rendered only once in the report. The Report Header is the first band of the report on the first page (apart from the Top Margin). It is usually used to display the report name, company logo and auxiliary information such as current system date and time. The Report Footer is placed before the Page Footer and Bottom Margin on the last page of the report. It can be used to display grand totals or conclusions.
Page Header and Footer	These bands are located at the top and bottom of every page in the report. They should be used for information that needs to be printed on every page such as a table header and footer or the page number.
Page Margin	The Top Margin and Bottom Margin bands represent the top and bottom page margins. They are intended for displaying auxiliary information such as page numbers or current system date and time.
Sub-Band	The sub-band is a band that provides a functional copy of the source band below which it is located. Using sub-bands, it is possible to create multiple versions of a band within the report and choose to display the appropriate one based on a specific condition.









Table 21

Report controls allow you to represent information of different types (such as simple or formatted text, images, tables, charts) and to arrange the layout of the report (by organising controls within panels and inserting page breaks at required positions). Both static and dynamic information can be displayed using the appropriate report controls.

Dynamic information changes through the report when viewed in preview mode, such as the data-bound fields that correspond to the columns in the main NetAnalysis® grid and auxiliary information (such as page numbers or current date and time).

Static information is text or images that do not change through the report (such as the title of the report or a company logo).

Table 22 holds details of the available report controls.

Control	Information
 Pointer	Not actually a control but it is used to reset the cursor selection.
 Label	The most basic control used to display text in the report. It can represent static or dynamic text or both. The text can only be formatted as a whole, use the Rich Text control to format parts of the text differently.
 Check Box	Intended to display true/false or checked/unchecked/indeterminate states in the report.
 Rich Text	Allows formatted text to be displayed in the report. It can represent static or dynamic text or both. Content (including images) can be loaded from an external text or RTF file and different parts formatted independently. The formatting options include font face, style, size and colour.
 Picture Box	Used to display graphics images in a number of different formats. The image can be loaded from an external file or from a web location using a URL.
 Panel	This is a container control that can be used to hold other report controls so that they can be kept together and easily moved, copied and pasted.
 Table	Designed to arrange information in a tabular layout. It can contain a number of rows comprised of individual cells. Both rows and cells can be individually customised. A cell can be a simple label or can contain other controls.
 Character Comb	Displays text so that each character is printed in an individual cell.

Control	Information
 Line	Draws a line of a specified direction, style, width and colour. Can be used for decoration or to visually separate sections of the report. It cannot cross different report bands.
 Shape	Used to embed simple graphic objects (such as rectangle, ellipse, arrow, polygon, brackets) into the report.
 Bar Code	This control transforms its content into a bar code of the specified type.
 Chart	Used to embed graphs into the report. It graphically represents a series of points using the selected 2D or 3D chart type. A chart can be populated with points either manually or dynamically.
 Gauge	Used to embed graphical gauges into the report. A gauge can be populated with values either manually or dynamically.
 Sparkline	Displays a compact chart that is commonly used to illustrate the data flow for every row in the report.
 Pivot Grid	Represents dynamic data in a cross-tabulated form to create cross-tab reports. Column headers display unique values from one data field and row headers from another field. Each cell displays a summary for the corresponding row and column values.
 Sub-Report	Allows other reports to be included in the current report.
 Table of Contents	Generates a table of contents based on bookmarks specified for report elements.
 Page Info	Used to add page numbers and other auxiliary information (such as current date and time) into the report.
 Page Break	Used to add a page delimiter at any point within the report.
 Cross-band Line	Allows a line to be drawn through several report bands. This can be useful to visually emphasize a section consisting of multiple band areas.
 Cross-band Box	Allows a rectangle to be drawn through several report bands. This can be useful to visually encompass a section consisting of multiple band areas.

Table 22

Adding Report Controls

The control toolbox bar in the Report Designer lists all available controls that can be added to a report (see Table 22). To add a control onto the report's design panel Designer tab, do one of the following:

- Double click the item for the required control in the toolbox, the control will be added to the top left corner of the report's Detail band (or whichever report band is selected).
- Drag and drop the item from the toolbox onto the required location within the report.
- Select the item in the toolbox and then click the required location within the report.
- Select the item in the toolbox and then click and hold down the left mouse button to draw the bounding rectangle for the control at the required location within the report.

Adding Static Information

By using the appropriate report control, static information can be displayed in the report. This can be text or graphics images that do not change through the report. Static information can be printed once only (by adding it to the Report Header or Footer band), can repeat on every page (by adding it to the Page Header or Footer band), or can repeat with every entry in the report's data-bound fields (by adding it to the Detail band).

To add static text information to the report (such as a Label or Rich Text control), first add the control from the toolbox and then do one of the following:

- Double click the control you have just added to activate the in-place editor and update its content.

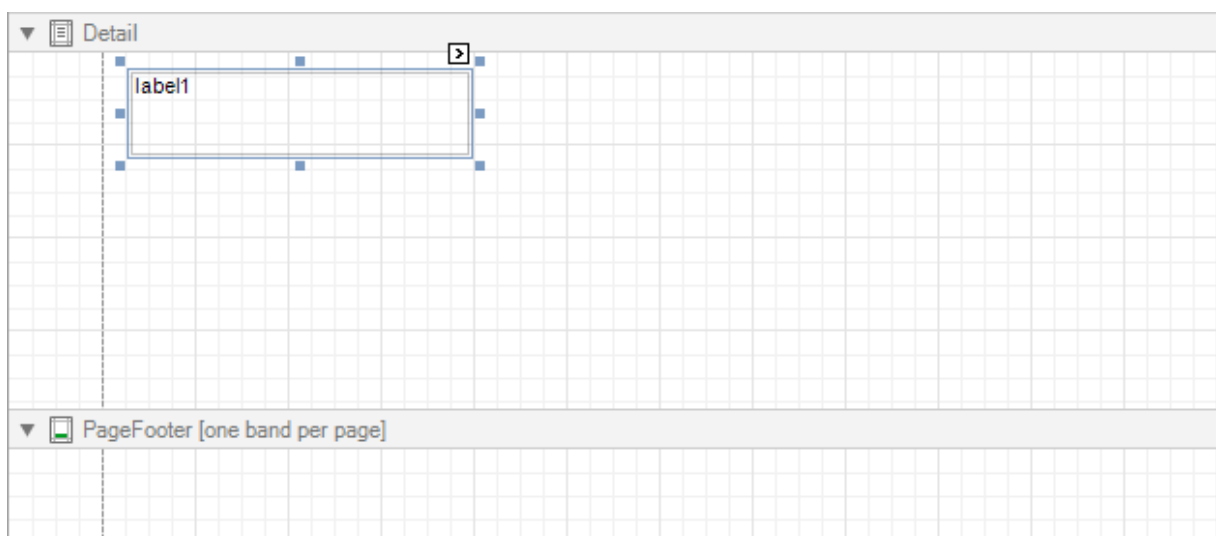



Figure 161

- Click the Smart Tag  located at the top right corner of the control. Most report elements have a Smart Tag which allows access to their most commonly used settings; when clicked a task


action list will be displayed (see Figure 162). The action list allows the control's content to be updated.

Label Tasks

Text	label1
Data Binding	(none) ▼
Format String	...
Summary	None ...
Angle	0
Formatting Rules	(Collection) ...
<input type="checkbox"/> Auto Width <input checked="" type="checkbox"/> Can Grow <input type="checkbox"/> Can Shrink <input type="checkbox"/> Multiline <input checked="" type="checkbox"/> Word Wrap	

Figure 162

To add static information to the report from an external file, first add the control from the toolbox (such as a Label, Rich Text or Picture Box control) and then do the following:


- Click the Smart Tag  located at the top right corner of the control. The displayed action list allows the file contents to be loaded into the control.

Picture Box Tasks

Image	(none) ...
Data Binding	(none) ▼
Image URL	...
Data Binding	(none) ▼
Sizing	Normal ▼
Image Alignment	Default ▼
Formatting Rules	(Collection) ...

Figure 163

Adding Dynamic Information

To display dynamic information in the report from the data-bound fields that correspond to the columns in the main NetAnalysis® grid, a report control must be added that is bound to one (or more) of these data fields. When viewed in the report's design panel Designer tab and in the Report Explorer dock panel, each data-bound control has a yellow database icon .

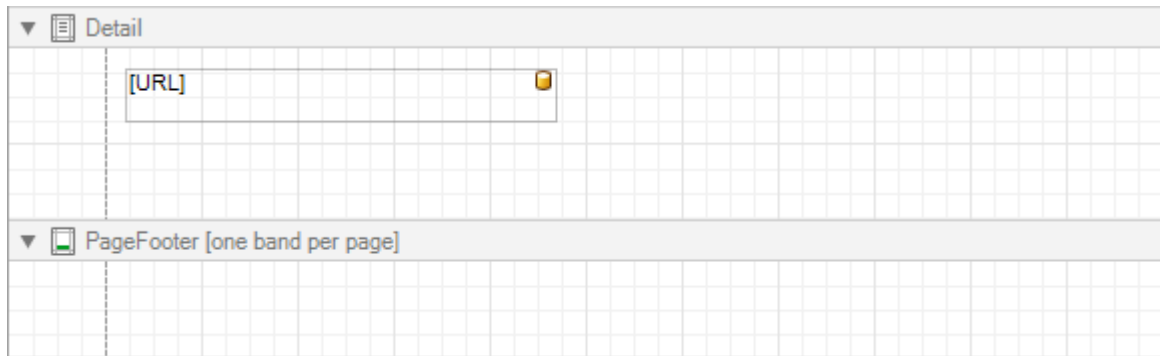


Figure 164

Figure 165 shows the Report Explorer with the Details section expanded.

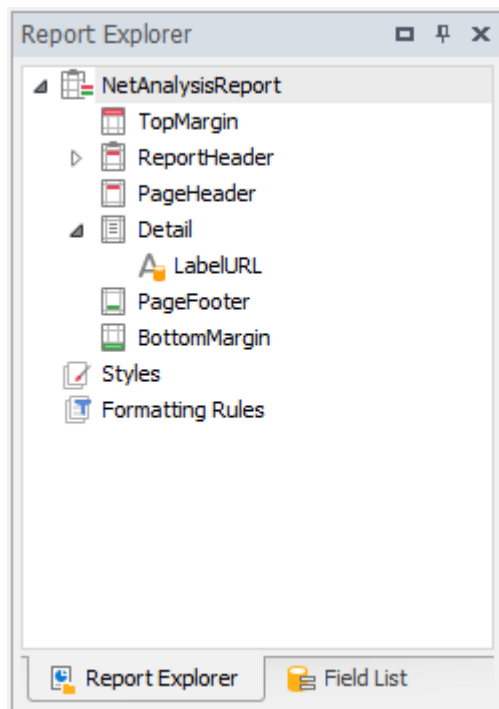


Figure 165

To add a data-bound control to the report do one of the following:

- Drag the required data field from the Field List onto the report Detail band. This will create a Label control bound to this data field.

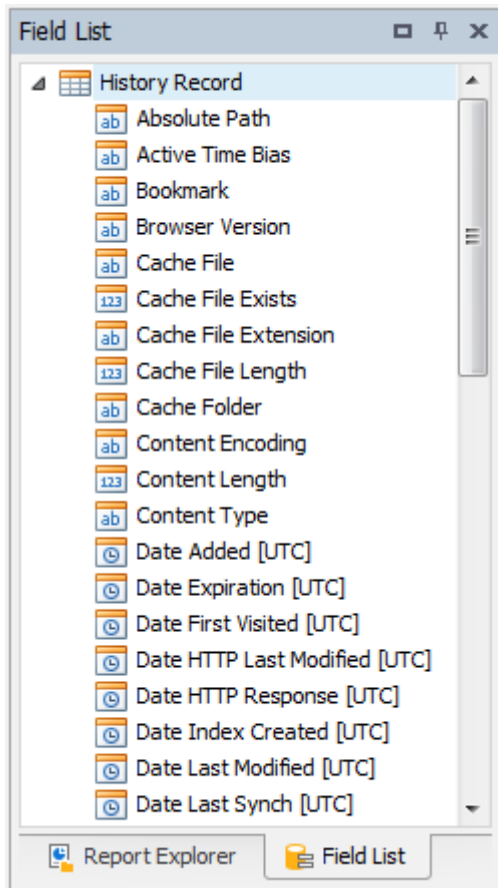


Figure 166

Figure 167 shows the Browser Version field having been dragged to the Detail section of the report.

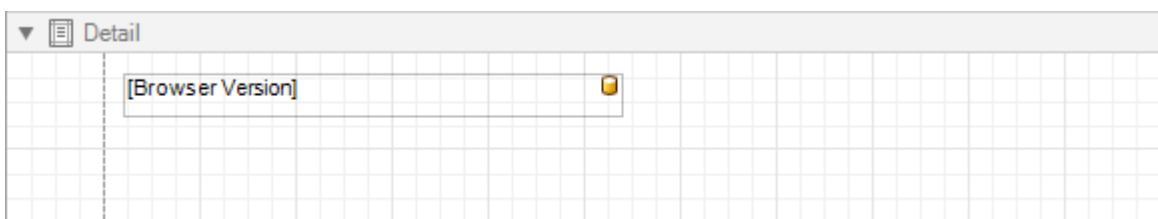


Figure 167

- An existing report control already added to the report's design panel Designer tab can also be bound to a data field. Click the required data field in the Field List and then drag and drop it onto an existing control (see Figure 168).

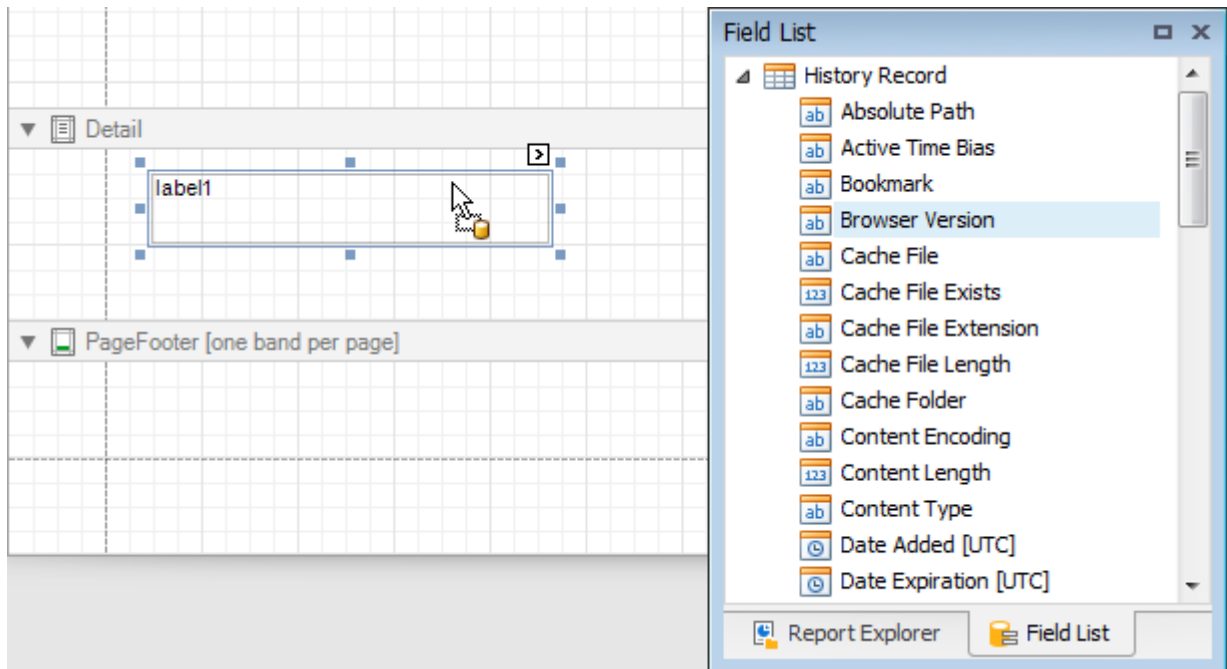


Figure 168

- Right click the required data field in the Field List and then drag and drop it onto the report Detail band. This invokes a context menu where you can choose a control item. Select an item and the control will be automatically created and bound to the data field (see Figure 169).

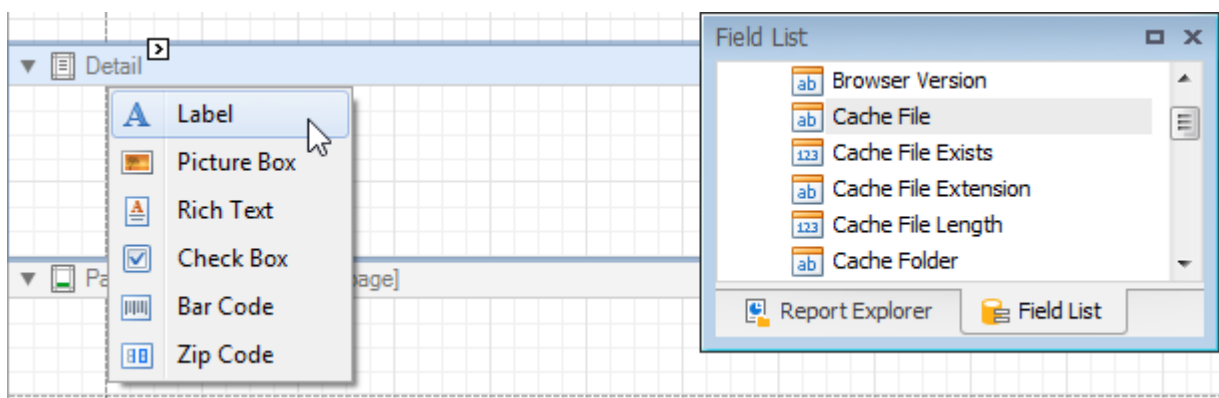



Figure 169

- For an existing control already added to the report, click its Smart Tag  located at the top right corner of the control. The displayed action list will contain a Data Binding list where the required data field can be selected (see Figure 170).

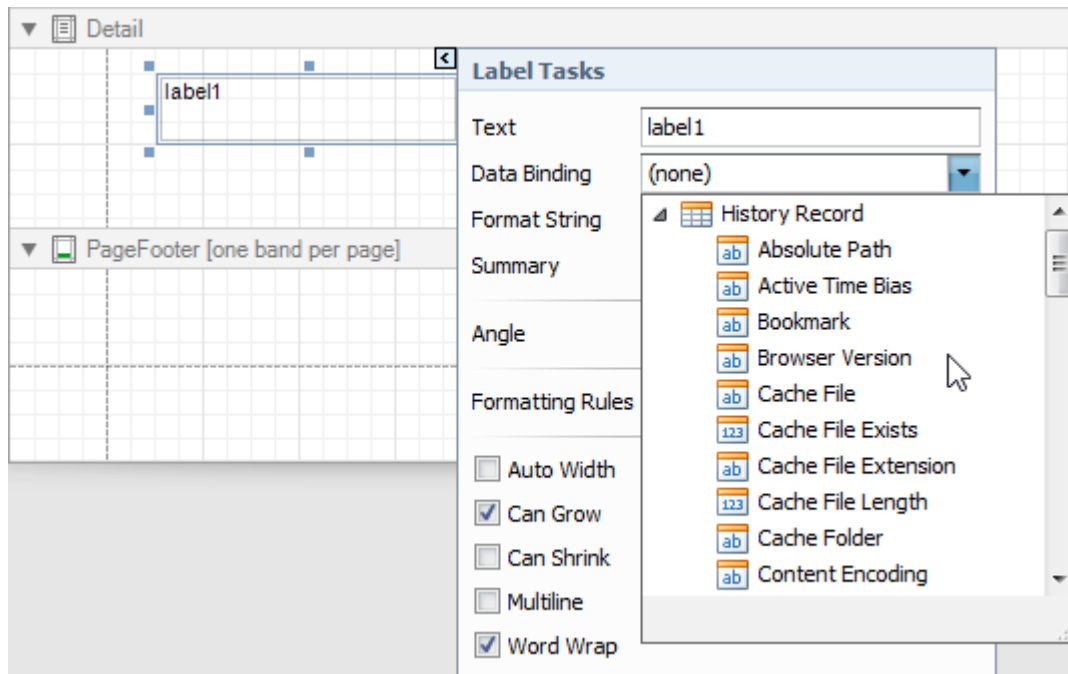


Figure 170

- For an existing control already added to the report, select the control and in the Property Grid expand the **(Data Bindings)** category that contains the binding options. Select the required data field from the list.

Data Grouping and Sorting

The bound data in the report can be grouped and sorted using the **Group and Sort** dock panel. Click the **Add a Group** button and select from the list, the data field, across which the report will be grouped.

Multiple groups can be selected and the priority for each group can be specified using the **Move Up** and **Move Down** buttons. A Group Header band will be added to the report with the specified data field set as its grouping criterion. The corresponding Group Footer band can be enabled by checking the Show Footer option in the Group and Sort dock panel.

Use the **Sort Order** list to set the sorting order of the group to Ascending, Descending or None (to disable sorting).

Preview, Printing and Exporting

To switch the report to print preview mode, click the Preview tab on the Report Designer design panel (see Figure 171). The report will now be populated with its bound data records and broken down into pages with the layout and content as specified in the Designer tab.



Figure 171

The Preview tab provides similar functionality to the report preview window used to display the built-in detailed report. It allows the report to be printed and exported to file in different formats. For further information see [Preview Detailed Report on Page 166](#).

Exporting

Introduction

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:

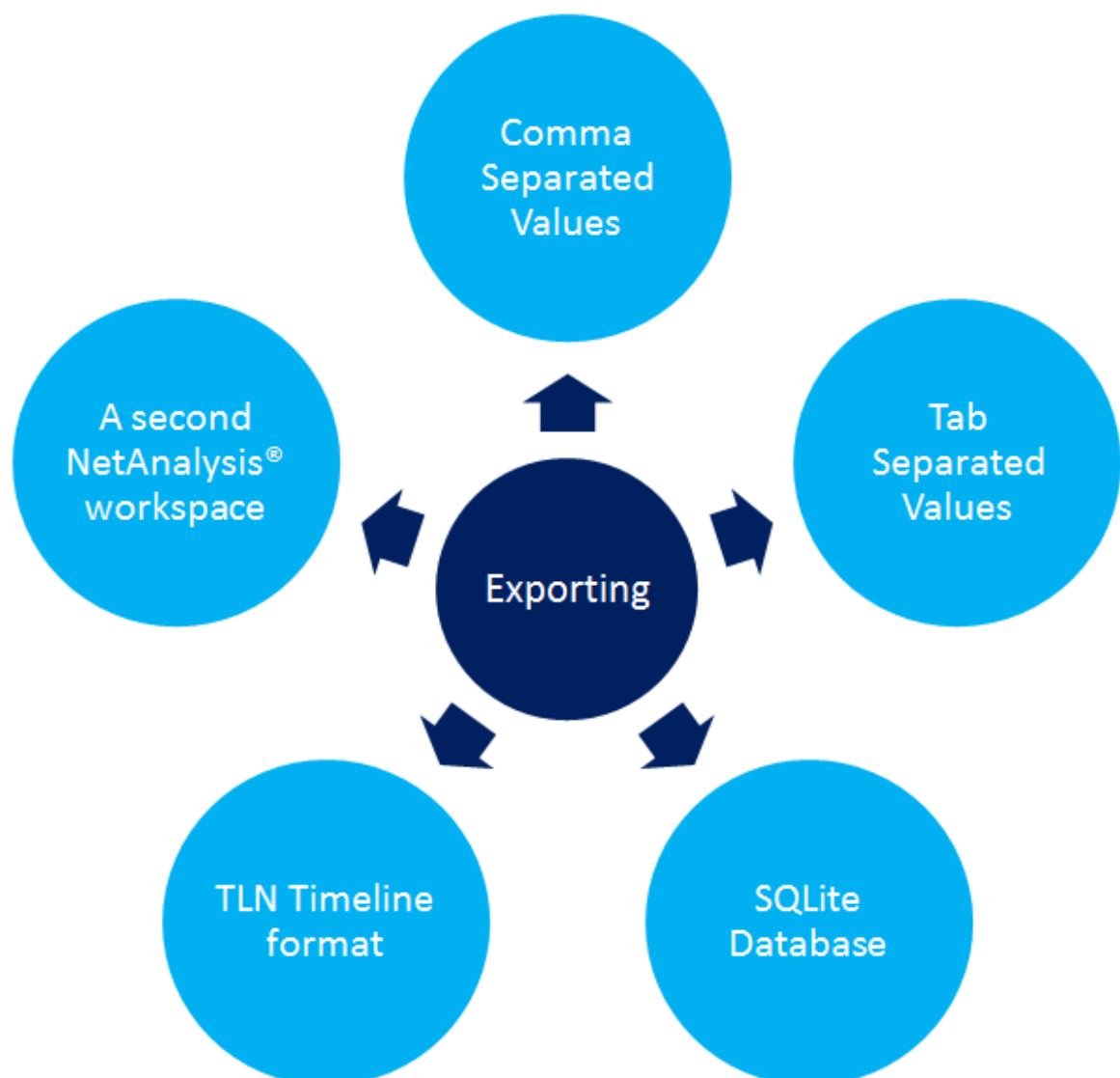


Figure 172

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.

Setting Visible Columns

With the exception of exporting records to a NetAnalysis® Workspace file and the TLN timeline format, the exporting process will only export the visible columns in the main user window. To remove or hide the columns you do not wish to export, right click on the column header and select **Hide this Column**.

To add a column back, select **Column » Column Chooser**, this will display a window containing a list of the hidden columns (as shown in Figure 173). Click on the column you wish to restore and drag it back to the position on the column header you wish the column to be placed. Releasing the mouse button will place the column at this position.

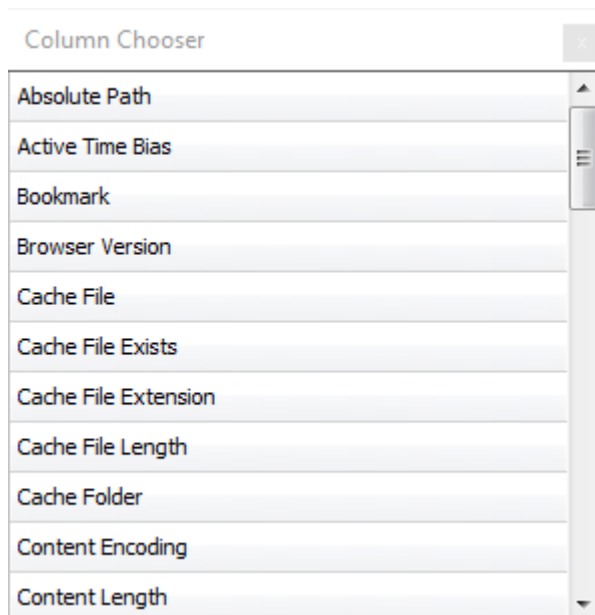


Figure 173

To reset all of the columns and place them back in their original positions, select **Column » Reset Column Layout**.

Filtering Records

Once you have the column visibility and ordering set, you are ready to either export the visible records or apply a filter.

To apply a record filter, please see Filtering and Searching on Page 115.

Exporting to CSV (Comma Separated Values)

To export your visible records to CSV, select **File » Export As » Comma Separated Values**. In the Save As window, select a file name and location for the output file.

Exporting to TSV (Tab Separated Values)

To export your visible records to TSV, select **File » Export As » Tab Separated Values**. In the Save As window, select a file name and location for the output file.

Exporting to SQLite Database

To export your visible records to an SQLite database, select **File » Export As » SQLite Database**. In the Save As window, select a file name and location for the output file.

Exporting to TLN Timeline Format

The TLN format requires that certain fields be present so will therefore ignore which columns are currently visible. To export your visible records to a TLN timeline format, select **File » Export As » TLN Timeline**. In the Save As window, select a file name and location for the output file.

Exporting to a NetAnalysis® Workspace

The NetAnalysis® Workspace format also requires a certain structure so will ignore which columns are currently visible. To export your visible records to a new NetAnalysis® Workspace, select **File » Export As » NetAnalysis® Workspace**. In the Save As window, select a file name and location for the output file.

Database

Introduction

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.

For further information on creating a workspace with SQLite, please see [Creating a New Case](#) on Page 104.



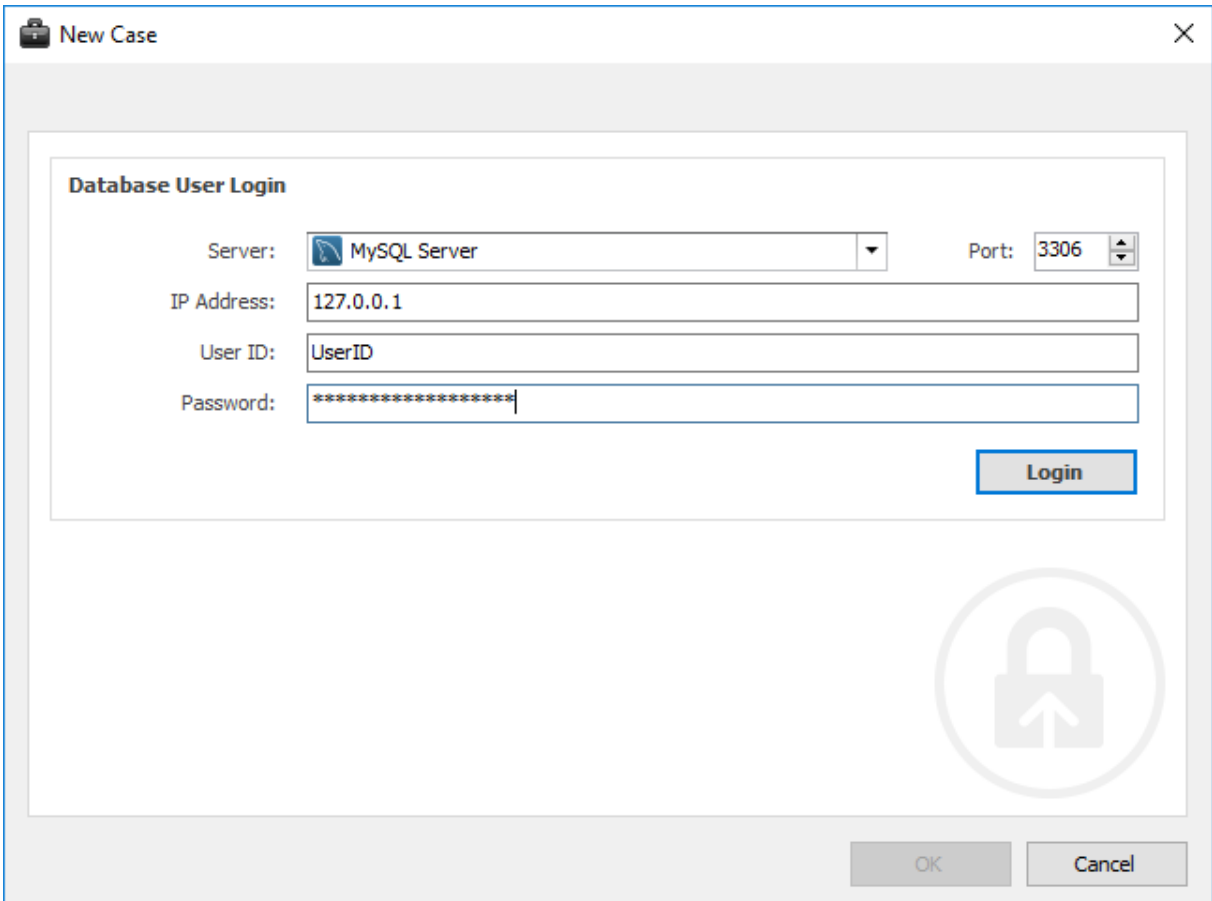
MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. This high-end solution is easy to use, includes solid data security layers that protects sensitive data as well as being scalable. It can handle almost any amount of data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

Creating a New Server Based Case

Prior to importing any data into a server-based workspace, you need to create a new MySQL Server case; this can be done by selecting **New Server Case** from the **File** menu.

First you will need to create a connection to your MySQL Server. You will need to specify the IP address and TCP/IP port number for the database server host; along with the user ID and password for the database user account that will be used to create the new workspace (as shown in Figure 174).

Please note that the database user must have previously been created using a MySQL administration tool and this account must have been granted the correct database privileges to be able to create and update the NetAnalysis® Workspace schema.



The screenshot shows a window titled "New Case" with a close button (X) in the top right corner. Inside the window, there is a section titled "Database User Login". This section contains the following fields and controls:

- Server:** A dropdown menu currently showing "MySQL Server".
- Port:** A numeric spinner box set to "3306".
- IP Address:** A text box containing "127.0.0.1".
- User ID:** A text box containing "UserID".
- Password:** A text box filled with asterisks "*****".
- Login Button:** A blue button labeled "Login" located at the bottom right of the "Database User Login" section.

Below the "Database User Login" section, there is a large, faint circular watermark containing a padlock icon with an upward-pointing arrow. At the bottom right of the "New Case" window, there are two buttons: "OK" and "Cancel".

Figure 174

Once a connection has been successfully established to the MySQL Server, the Case Information tab allows you to set the case reference and agency/company information. You can also set the location for

the export folder and temporary folders. During import, NetAnalysis® will export a number of artefacts such as web page previews, thumbnails and extracted text from search indices. The Auto-Generate option allows NetAnalysis® to create case and evidence references for you. This information should be replaced by your own reference values.

New Case

Server Authentication Case Information Import Options

Case Reference Auto-Generate ☒

Case Reference: CASE-20170110

Evidence Reference: ID-170104

Agency Information

Examiner Name: Craig Wilson

Agency Name: Digital Detective

Case Folders

Export Folder: D:\Documents ...

Temporary Folder: D:\Temp ...

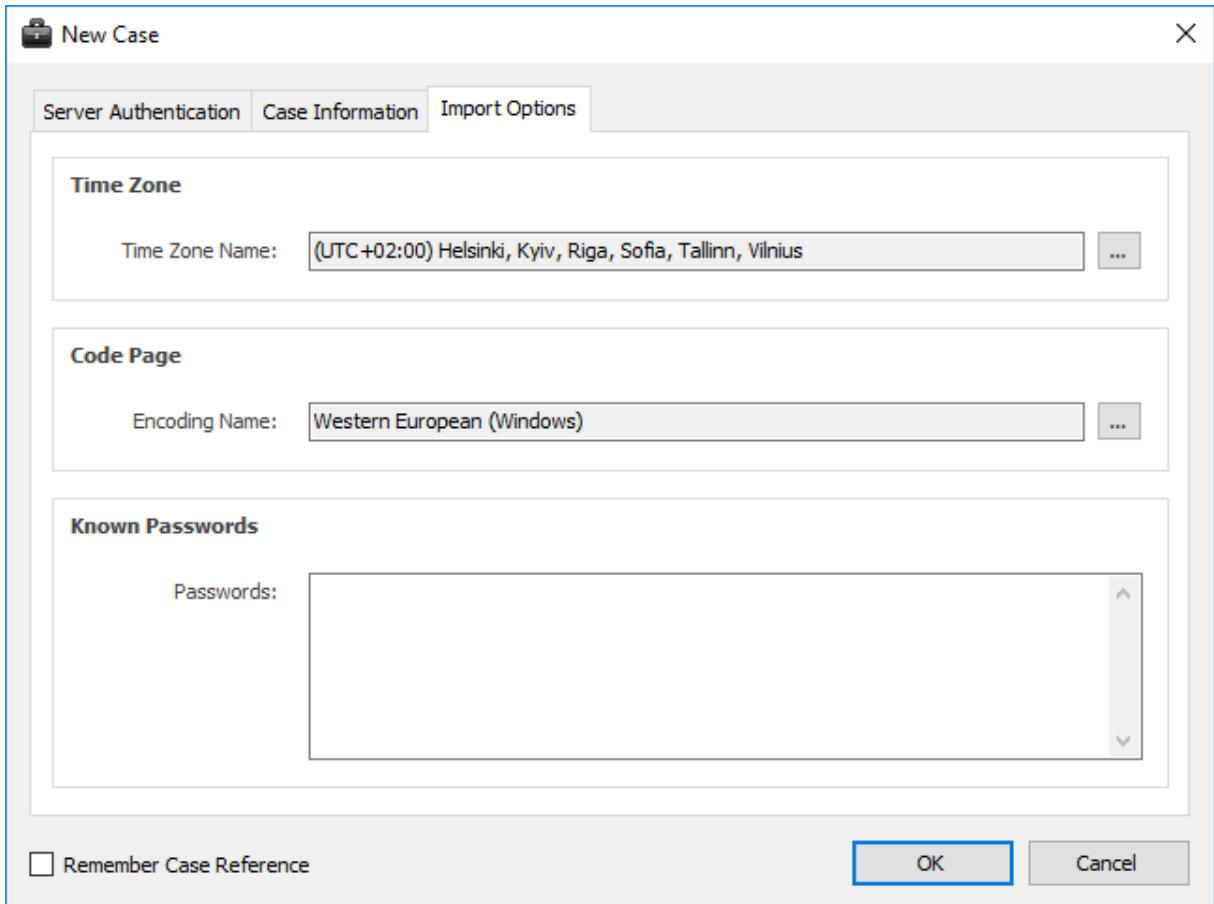
☐ Remember Case Reference

OK Cancel

Figure 175

The Import Options tab shows the various import options which can be set. The time zone and encoding can be set, prior to importing any data. It is important to establish the time zone of the target system prior to importing any data as this has a direct effect on the calculation of local time stamps. The code page default will be set to UTF-8. The **Known Passwords** box is for adding any known Master Passwords to allow NetAnalysis® to automatically decrypt username and password information.

Please ensure you read the chapters on Time Zone Configuration and Encoding Configuration to fully understand how to set the correct import options for your case (see Time Zone Configuration on Page 78 and Encoding Configuration on Page 100).



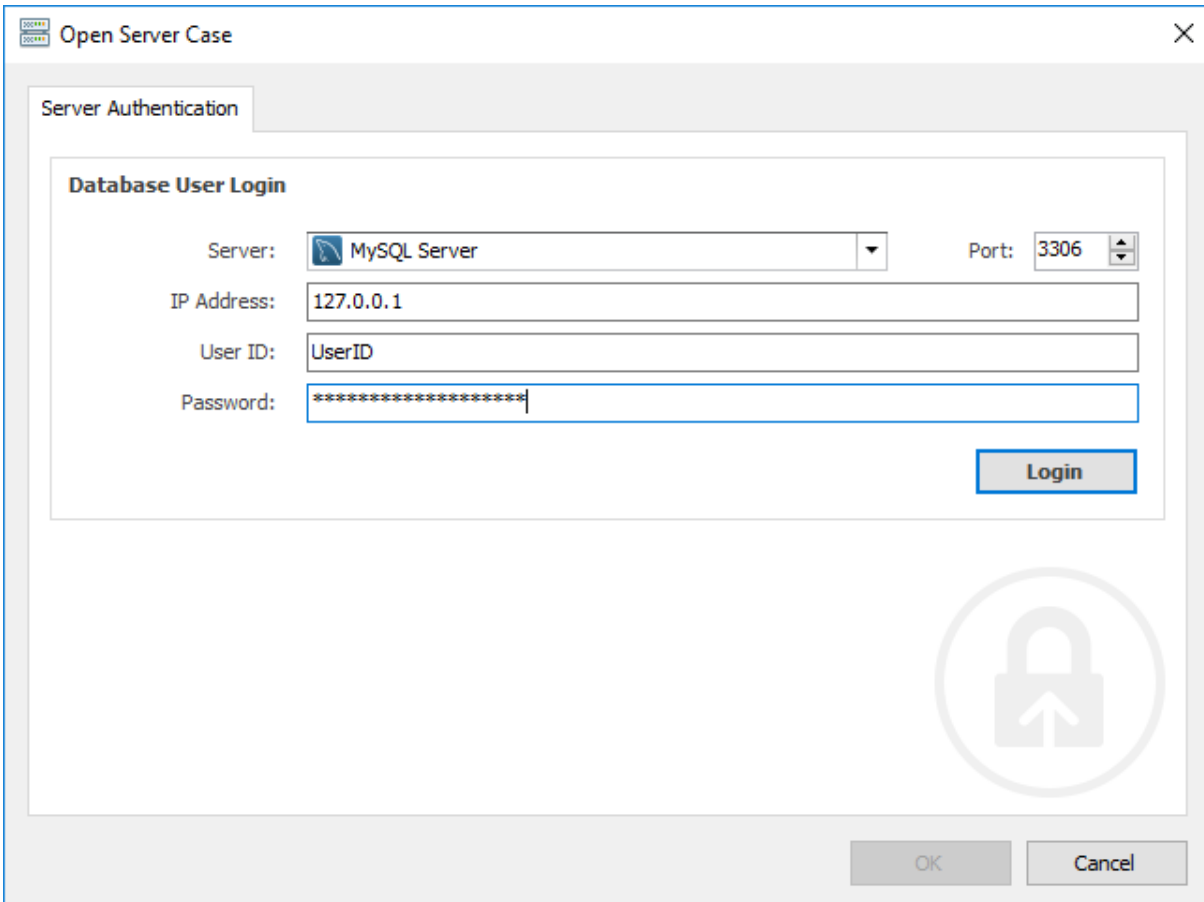
The screenshot shows the 'New Case' dialog box with the 'Import Options' tab selected. The dialog has three tabs: 'Server Authentication', 'Case Information', and 'Import Options'. The 'Import Options' tab contains three sections: 'Time Zone', 'Code Page', and 'Known Passwords'. The 'Time Zone' section has a 'Time Zone Name' field with the value '(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius' and a dropdown arrow. The 'Code Page' section has an 'Encoding Name' field with the value 'Western European (Windows)' and a dropdown arrow. The 'Known Passwords' section has a 'Passwords' label and a large empty text area with a scrollbar. At the bottom of the dialog, there is a checkbox labeled 'Remember Case Reference' which is unchecked, and two buttons: 'OK' and 'Cancel'.

Figure 176

Opening a Server Based Case

To open a previously created MySQL Server case, select **Open Server Workspace** from the **File** menu.

First you will need to create a connection to your MySQL Server. You will need to specify the IP address and TCP/IP port number for the database server host; along with the user ID and password for a database user account that has access to the NetAnalysis® Workspace that you want to open (as shown in Figure 177).



The image shows a software window titled "Open Server Case" with a close button (X) in the top right corner. Inside the window, there is a tab labeled "Server Authentication". Below this tab is a section titled "Database User Login". This section contains four input fields: "Server:" with a dropdown menu showing "MySQL Server", "Port:" with a numeric spinner set to "3306", "IP Address:" with a text box containing "127.0.0.1", and "User ID:" with a text box containing "UserID". Below these is a "Password:" field with a masked password "*****". A "Login" button is positioned to the right of the password field. At the bottom right of the window, there are "OK" and "Cancel" buttons. A large, faint watermark of a padlock with an upward arrow is visible in the background of the dialog.

Figure 177

Once a connection has been successfully established to the MySQL Server, the Case Information tab will list the NetAnalysis® Workspace databases that this database user has access to (see Figure 178). Select the workspace to open and click **OK**.

Open Server Case

Server Authentication | **Case Information**

Workspace Databases

- case-20160920_id-153728
- case-20170110_id-165833
- test01_id-142141

Case Reference

Case Reference: CASE-20160920

Evidence Reference: ID-153728

Agency Information

Examiner Name: Craig Wilson

Agency Name: Digital Detective

Case Folders

Export Folder: D:\Documents

Temporary Folder: C:\Users\Craig Wilson\AppData\Local\Temp

OK Cancel

Figure 178

HstEx®



Introduction

HstEx® v4 is a state-of-the-art, Windows-based, multi-threaded, forensic data recovery solution which has been designed to recover deleted browser artefacts 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 web browsers, whether they have been installed on Windows, Linux, Apple Mac or mobile operating 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® was designed as a separate tool from NetAnalysis® so they could be run separately. The design goal was to have an application that was capable of processing queues of evidence without unnecessarily occupying the analytical element. Further licences of HstEx® can be purchased on request.

HstEx® v4

The latest version of HstEx® is a completely new product which has been engineered from the ground up. 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.

In this new version, we have added a number of new features such as:

- Ability to add multiple recovery jobs to a queue
- Ability to select multiple recovery types for a single recovery job
- Support for a wide variety of desktop and mobile browsers
- Support for a large number of different browser artefacts
- Powerful parallel processing to make use of multi-core CPUs

Deleted Data Recovery

Introduction

As we have outlined in our introduction to HstEx® on Page 194, NetAnalysis® was designed to perform the processing and analysis of data whilst HstEx® was designed as a stand-alone application for the searching and recovery of deleted data. The following section explains how this is achieved.

Data Carving

HstEx® has been designed to process a forensic image, physical/logical disk or binary dump at sector level using a process called data carving. This term is used for extracting structured data out of raw data based on the format specific characteristics present in the structured data. In digital forensics, it is the process of extracting data from a source without the assistance of the file system that created the original file.

HstEx® will process the data source using sequential access, a block at a time, using a methodology designed to ensure that nothing is missed at block boundaries. The size of the block is determined by the value as shown in the **General Settings** tab in the **Options** Window (accessible via **Tools » Options**).

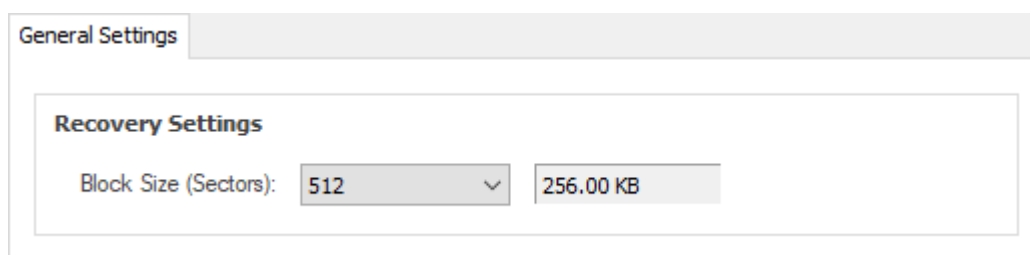


Figure 179

The default block size is 512 sectors (as shown in Figure 179). Changing the block size will affect the searching speed. The default size will provide the optimal value for searching performance.

HstEx® works in a similar way to some imager applications in that it starts at sector zero and processes all the data to the end. In many cases, it can recover individual records relating to browser activity without the entire file being present on the source image or disk.

As HstEx® ignores the file system, it can be run across many source file system types without issue. It also means that when it recovers from a disk or image, it will potentially recover the live data as well as any that is deleted. This means that it will potentially recover data from the areas outlined in Figure 180.

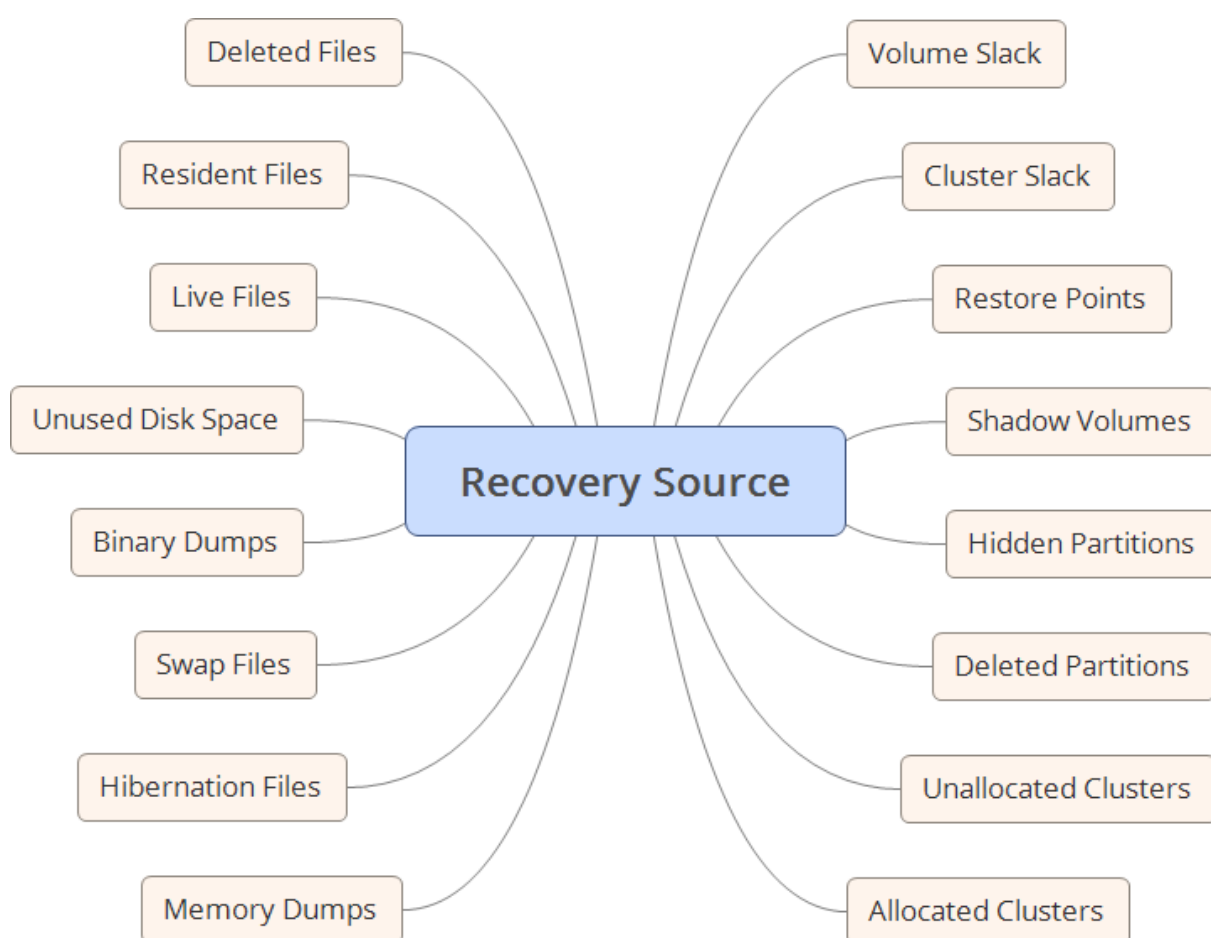


Figure 180

We recommend processing the entire data source to ensure that all potential evidence is located.

Supported Source Data Formats

HstEx® v4 natively supports a number of different image and output file formats. Table 23 lists some of the known supported file types.

HstEx® v4.8 added support for processing L01/Lx01 logical evidence files.

File Format	File Extensions
Binary Dumps	*.bin, *.dat, *.unallocated, *.rec, *.data, *.binary
EnCase® v7 - 8 Evidence File Format Version 2	*.ex01
EnCase® v1 - 8 Evidence File Format Version 1	*.e01
EnCase® v5 - 8 Logical Evidence File Format v1	*.L01
EnCase® v7 - 8 Logical Evidence File Format v2	*.Lx01
Memory Dumps	*.dmp, *.dump, *.crash, *.mem, *.vmem, *.mdmp
Mobile Phone Raw Binary Memory Dumps	*.bin
Segmented Image Unix / Linux DD / Raw Image Files	*.000, *.0000, *.00000, *.001, *.0001, *.00001
Single Image Unix / Linux DD / Raw / Monolithic	*.dd, *.img, *.ima, *.raw
SMART/Expert Witness Image File	*.s01
Virtual Hard Disk	*.vhd
VMWare Virtual Disk File	*.vmdk
X-Ways Forensics Image File	*.e01

Table 23

Understanding Data Recovery

It is important to understand the different recovery methods employed by HstEx® so that you can understand the potential weakness with each method. Applications store their data in many different ways, ranging from proprietary databases and binary formats, to industry standard formats such as SQLite databases, XML and JSON.

Record Based Extraction

With Record Based Extraction, HstEx® has the ability to identify and recover individual records from the original data source. This method is the most desirable as it is more likely to yield better results. Records tend to be relatively small and therefore are more likely to be found intact.

For example, data stored in SQLite databases can be found and recovered using this method without the need to recover the entire database.

File Based Extraction

With File Based Extraction, the full file must be recovered so that it can be read and processed. Unfortunately, due to the way some file formats have been designed, Record Based Extraction is impossible, or highly dangerous, from a forensic perspective.

Two examples of this are Mozilla's Mork database format and Apple's binary property list (Plist) format. Both formats utilise indexes which contain pointers to the objects which make up a record. In some cases, where the objects contain data already present in the database, it is not duplicated; instead, the object pointers are updated. This means that you cannot just carve out data objects that are contiguous and hope that they relate to the same record.

Intelli-Carve®

Intelli-Carve® is an intelligent data recovery and validation engine which can verify file integrity and verify data structures during the recovery process. HstEx® employs Intelli-Carve® technology for all of the current recovery profiles.

Recommended Methodology

HstEx® and NetAnalysis® have been designed to work together. The primary function of NetAnalysis® is to import live data, extract and rebuild live cache and web pages, and to provide an analytical platform for forensic analysis.

HstEx® has been designed to recover data separately from NetAnalysis® and to produce an output that can be loaded into NetAnalysis® for analysis with the live data.

HstEx® Supported Browsers



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

Apple Safari v3 - 11

- 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
- Top Site Files (Binary Plist)

Google Chrome v1 - 65

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

- 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 - 41

- 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+)

Mozilla Firefox v1 - 59

- History Entries (v3+)

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

Opera v4 - 12

- Typed History Entries
- Search Field History Entries

Opera v15 - 51

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

360 Browser v7

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

- Form History Entries
- Login Data Entries

360 Security Browser v6 - 9

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

360 Speed Browser v4 - 9

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

AOL Desktop Browser v9

- Cookie Entries
- Cache Entries

Blisk v0 - 8

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

Brave v0 - 1

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

Comodo Chromodo v36 - 52

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

- Login Data Entries
- Shortcut Entries

Comodo Dragon v4 - 60

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

Comodo Ice Dragon v13 - 57

- 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

- Form History 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

Flock v2

- Cache Entries

Flock v3

- History Entries
- Cache Entries
- Keyword Search Term Entries
- Form History 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+)
- Permission Entries (v42+)

K-Meleon v1 - 76

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

Netscape v6 - 9

- Cache Entries

Opera Neon v1

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

Pale Moon v3 - 27

- History Entries

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

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
- Form History Entries
- Login Data Entries
- 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 - 64

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

Titan Browser v1 - 33

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

Torch v1 - 55

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

UC Browser v4 - 7

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

Vivaldi v1

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries

- Keyword Search Term Entries
- Form History Entries
- Login Data Entries
- Shortcut Entries

Waterfox v4 - 56

- 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 - 18

- History Entries
- Download Entries
- Cookie Entries
- Cache Entries
- Simple Cache Entries (v2+)
- Keyword Search Term Entries
- Form History Entries
- Login Data Entries
- Shortcut Entries

Other Chromium Based Browsers

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

Other Mozilla Based Browsers

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

Installing HstEx®

Introduction

The following procedure will guide you through installing HstEx® for the first time. Please ensure that you close all other applications before starting.

Operating System Requirements

Our software has been designed to run on a Microsoft® Windows® x86/x64 platform. Please note, the following list represents the platforms which have been tested. The software may run on other platforms not listed below.

Operating System

The following Operating System versions are supported:

- Windows 10
- Windows 8
- Windows 7
- Windows Vista SP1 or later
- Windows Server 2008 (Server Core not supported)
- Windows Server 2008 R2 (Server Core not supported)

Additional Requirements

The Operating System must have the following .NET framework runtime installed:

- Microsoft .NET Framework v4

Latest Release

Prior to installing HstEx®, please ensure you have obtained the latest release. There is on-going product research and development which provides new features, important updates and bug fixes. Please check the change log for details of those changes.

The release history and change log can be found here:

[*http://kb.digital-detective.net/x/AgCQ*](http://kb.digital-detective.net/x/AgCQ)

Verification of Digital Signature

Software vendors can digitally sign and timestamp the software they distribute. The code signing process ensures the end user knows the digitally signed software is legitimate, comes from a known software vendor and the code has not been tampered with since being published. If the Authenticode Digital Signature is not valid, or the MD5 hash provided at the point of download does not match, please do not install the software.

All the software products published by Digital Detective have been digitally signed. This ensures that when you use our software, you can verify that it has not been tampered with and is a product developed and released by Digital Detective Group. The following knowledge base article explains this further and shows you how to verify the integrity of forensic grade software:

[*http://kb.digital-detective.net/x/u4EU*](http://kb.digital-detective.net/x/u4EU)

Running Setup

Now that you have verified the integrity of the setup file (all the individual executables have also been digitally signed) you can install the software. You will note that each release has been named using the version/build information (see Figure 181).



Name	Date modified	Type	Size
 HstEx-x86-EN-4.5.16321.4.exe	2016-11-16 17:01	Application	14,407 KB
 NetAnalysis-x86-EN-2.5.16321.10.exe	2016-11-16 16:56	Application	48,416 KB

Figure 181

Good forensic practice dictates that you archive each release of a software application that you use on a forensic case. This ensures that at any time in the future, you can install a specific version and replicate your results.

When you run the application setup, Windows should prompt you for permission to install the software (see Figure 182).

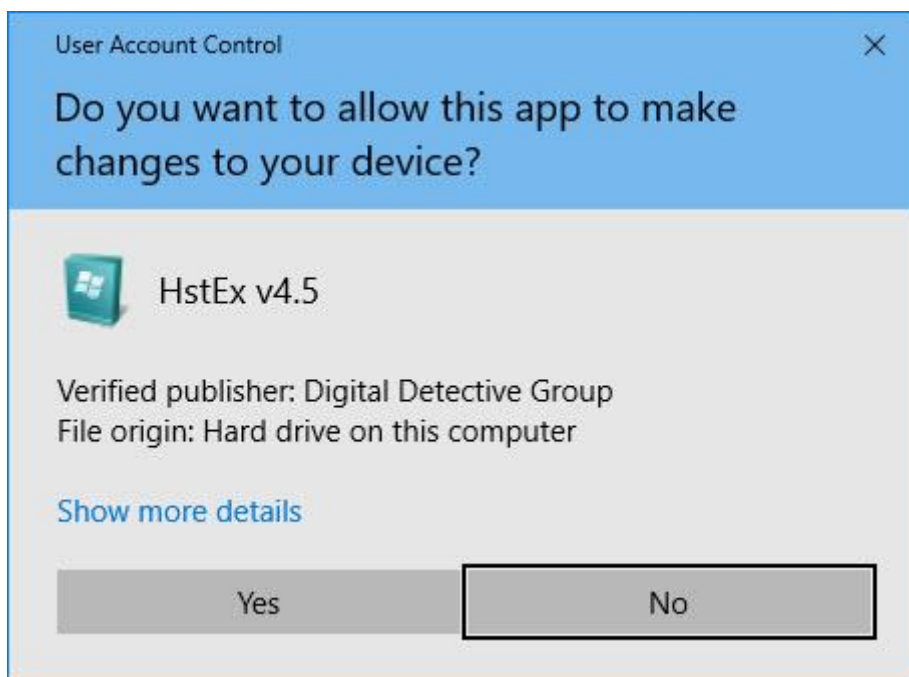


Figure 182

At this point, please ensure the prompt indicates that the publisher is Digital Detective Group and that it is verified.

Click **Yes** and move onto the next stage.

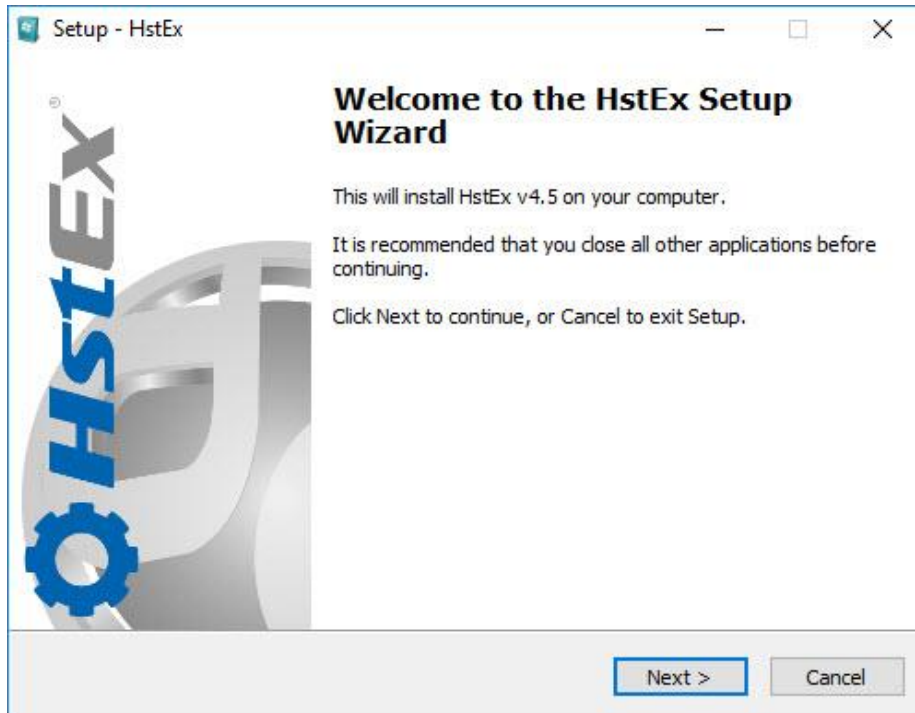


Figure 183

Please ensure that you close any other applications you may have running to prevent them interfering with the setup process.

End User Licence Agreement

The next screen (Figure 184) displays the End User Licence Agreement. Please read this carefully. If you wish to review or print a copy of this agreement, it can be found in our knowledge base at the following link:

<http://kb.digital-detective.net/x/fIUU>

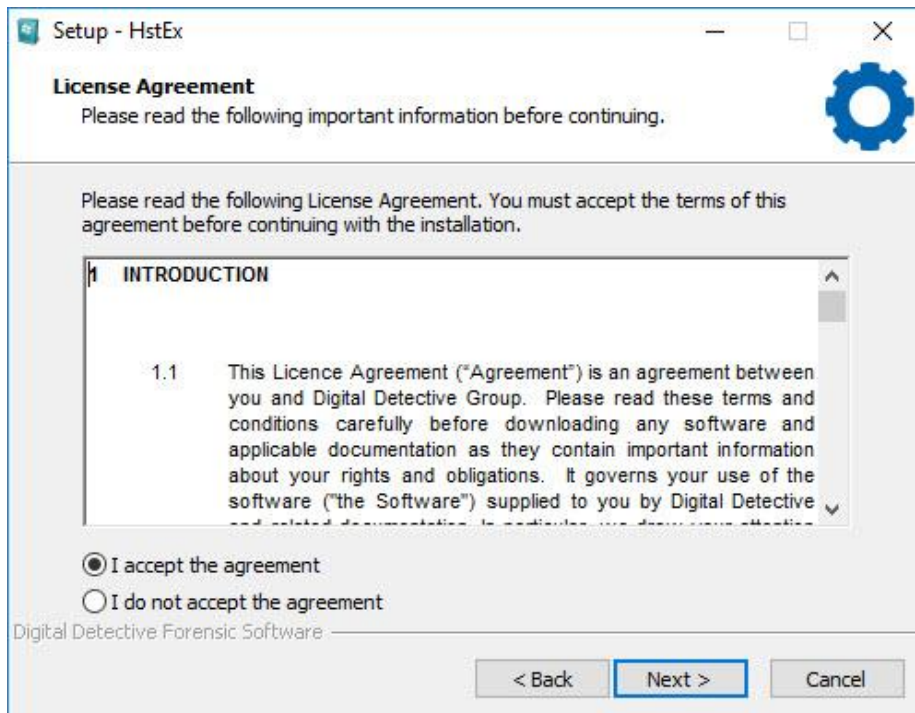


Figure 184

Click the option to accept the licence agreement and then click **Next** to move onto the next stage.

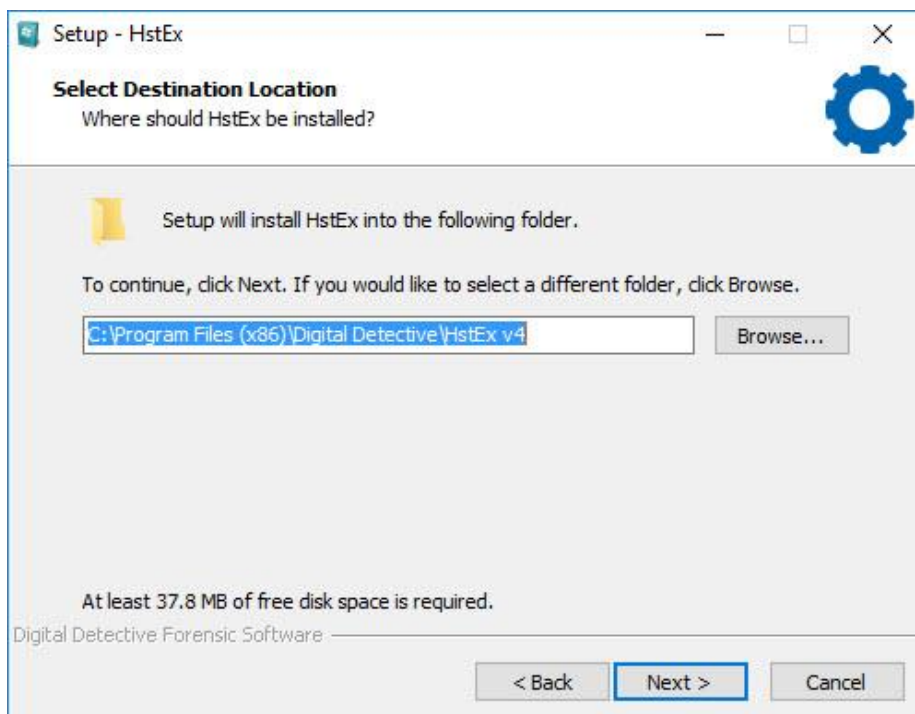


Figure 185

This window (Figure 185) allows you to configure the destination folder where the software will be installed. If this window does not appear, it means the software is already installed. In this case, the setup will use the previously selected values. Click **Next** to continue.

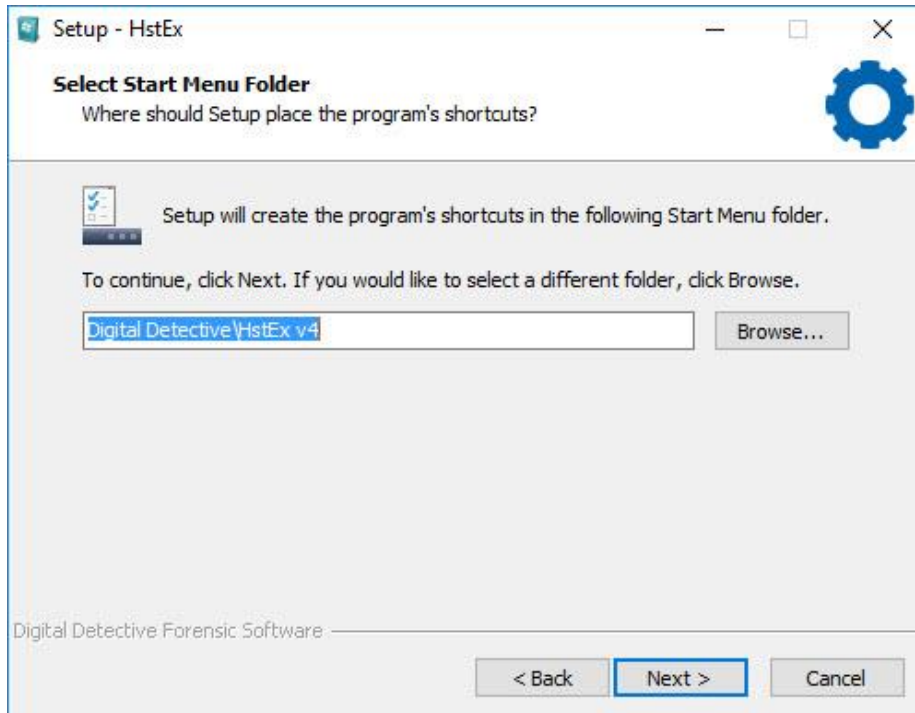


Figure 186

This window (Figure 186) allows you to configure the Start Menu folder. As with the previous window, if this option does not appear, it is because the software is already installed.

Click **Next** to continue.

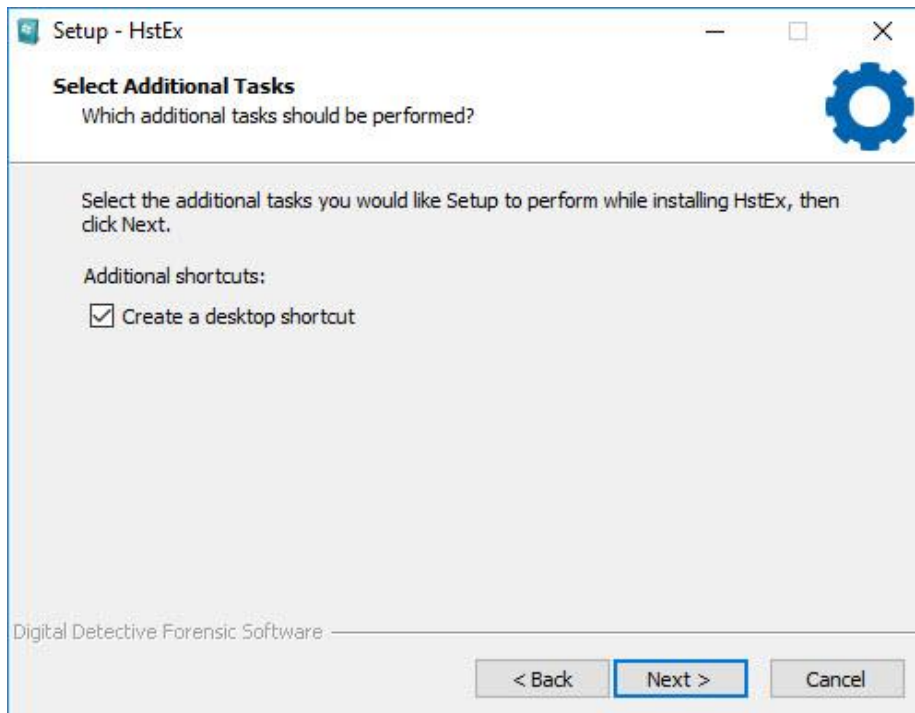


Figure 187

If you want the setup to create a desktop icon for you, select the option as shown in Figure 187. Click **Next** to continue.

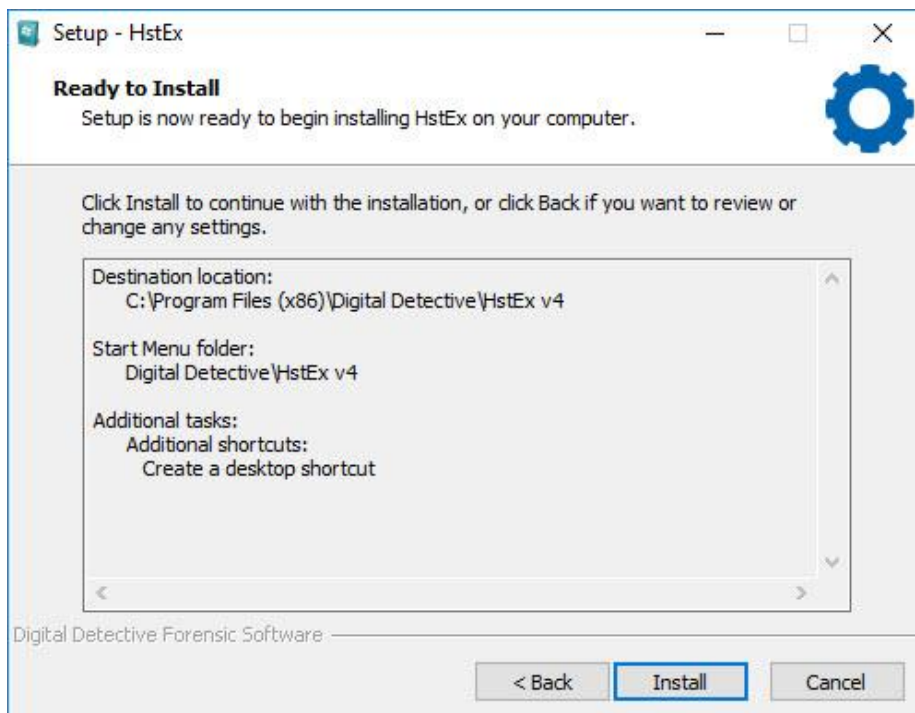


Figure 188

The next window (Figure 188) shows a summary of the installation tasks prior to launching the final installation process. If you are ready to continue, click the **Install** button.

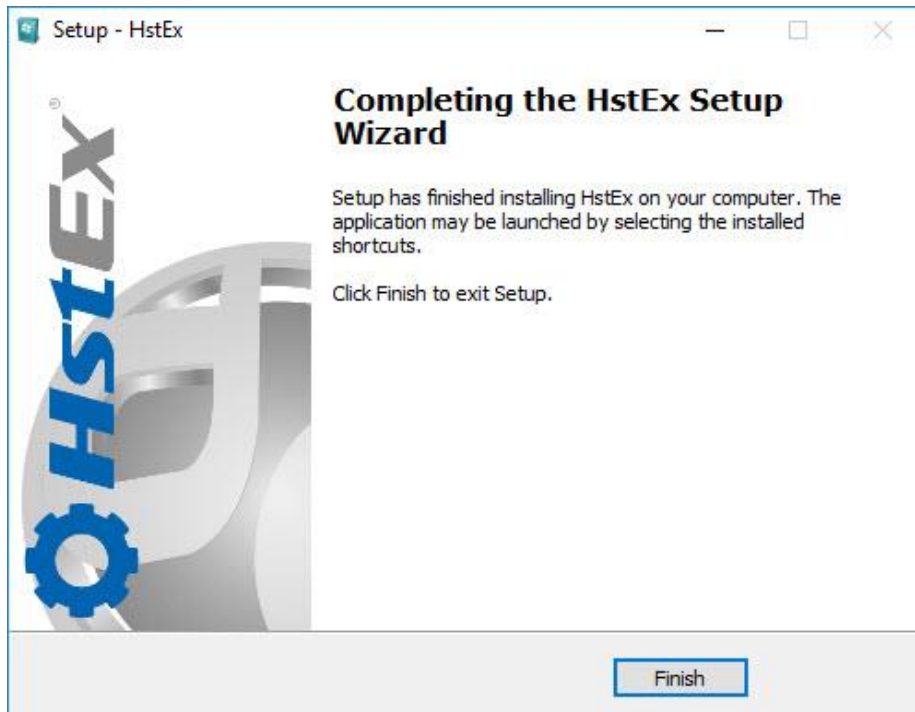


Figure 189

The final window (Figure 189) shows that the setup wizard has completed. Click **Finish** to close the Setup Wizard.

HstEx® - A Guided Tour

Introduction

To get the most from the software, it is important to understand the user interface and know what each feature does. In this chapter, we will take a brief look at the main components of the user interface and describe how they work.

The HstEx® main window can be seen in Figure 190 below. The main elements of the interface have been numbered; for a description of each user interface element, see Table 24 below.

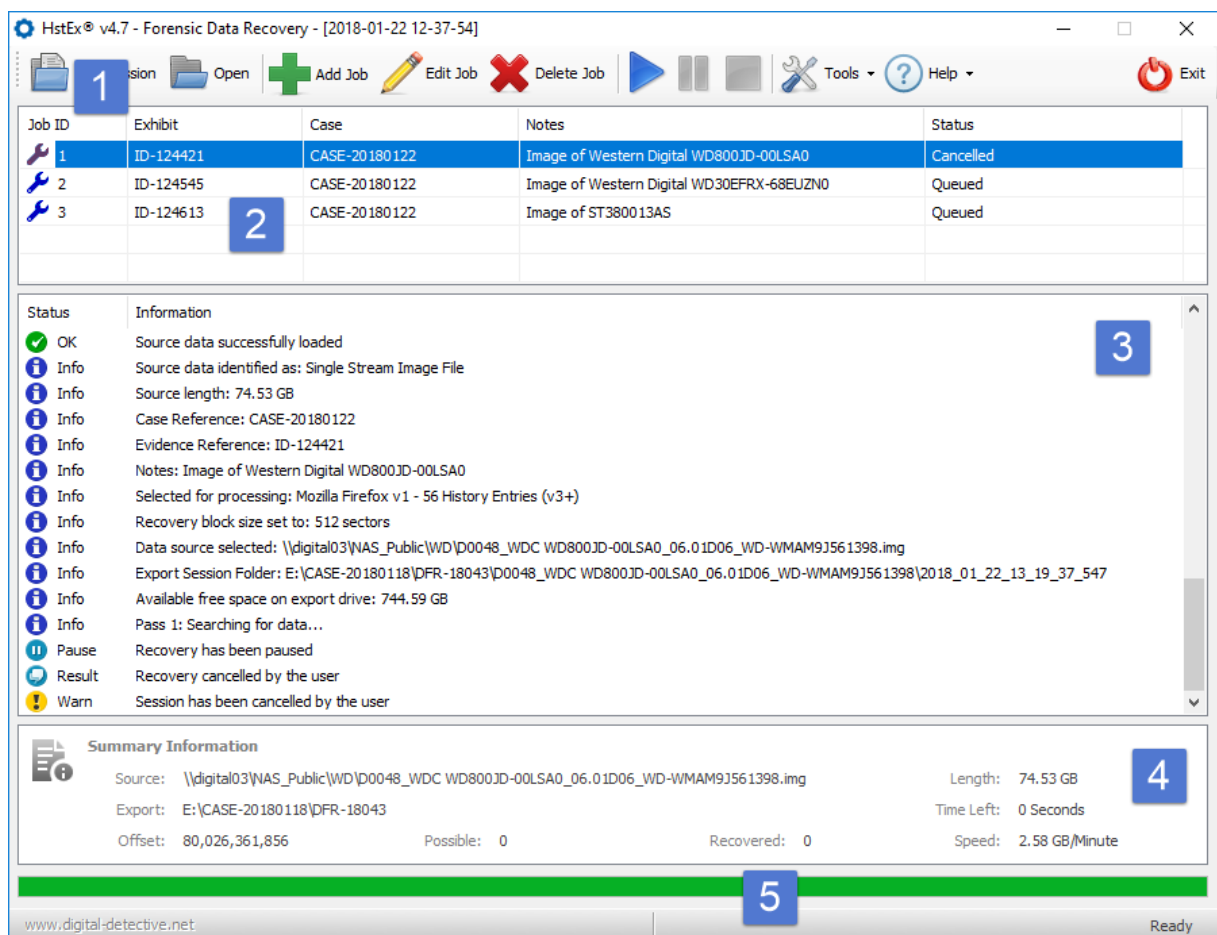


Figure 190









HstEx® Main Window	
	Toolbar For a full description of the buttons on the main toolbar, see Table 25 below.
	Job List Lists all of the jobs that have been added to this recovery session.
	Log Logs the progress of the recovery session.
	Summary Information Shows information relating to the currently selected recovery job.
	Progress and Status Bar Shows information relating to the currently selected recovery job and provides a visual representation of the status.

Table 24

Main Toolbar

The following table highlights the function of each toolbar button and dropdown menu item in the main toolbar.

HstEx® Main Toolbar	
	New Session Creates a New Recovery Session.
	Open Session Opens a previously created Recovery Session.
	Add Job Adds a new Recovery Job. See Figure 191.

HstEx® Main Toolbar**Edit Job**

Shows the Recovery Job window containing the parameters for the currently selected job.

**Delete Job**

Deleted the currently selected Job in the Job List.

**Start Recovery**

Starts or resumes a paused recovery session.

**Pause Recovery**

Pauses a running recovery session.

**Cancel Recovery**

Cancels a running recovery session.

**Tools**

Shows a dropdown menu containing the following items:

Tools » Reset Job Queue

Resets the status for all Jobs in the queue so that they will be processed.

Tools » Open Export Folder

Shows the Export Folder for the currently selected Job.

Tools » Options

Shows the Options window. Allows the user to change the current options.

**Help**

Shows a dropdown menu containing the following items:

Help » Knowledge Base

Opens a web browser with a link to the Knowledge Base.

Help » Support

Opens a web browser with a link to the Support Portal.

Help » Check for Software Update

Checks if there is an updated version of the software available, if so, the download link is provided.



HstEx® Main Toolbar	
	Help» About HstEx® Shows the About window.
	Exit Exits and closes the application.

Table 25

Recovery Job Window

The Recovery Job window can be seen in Figure 191 below. The main elements of the interface have been numbered; for a full description of each element, see Table 26.

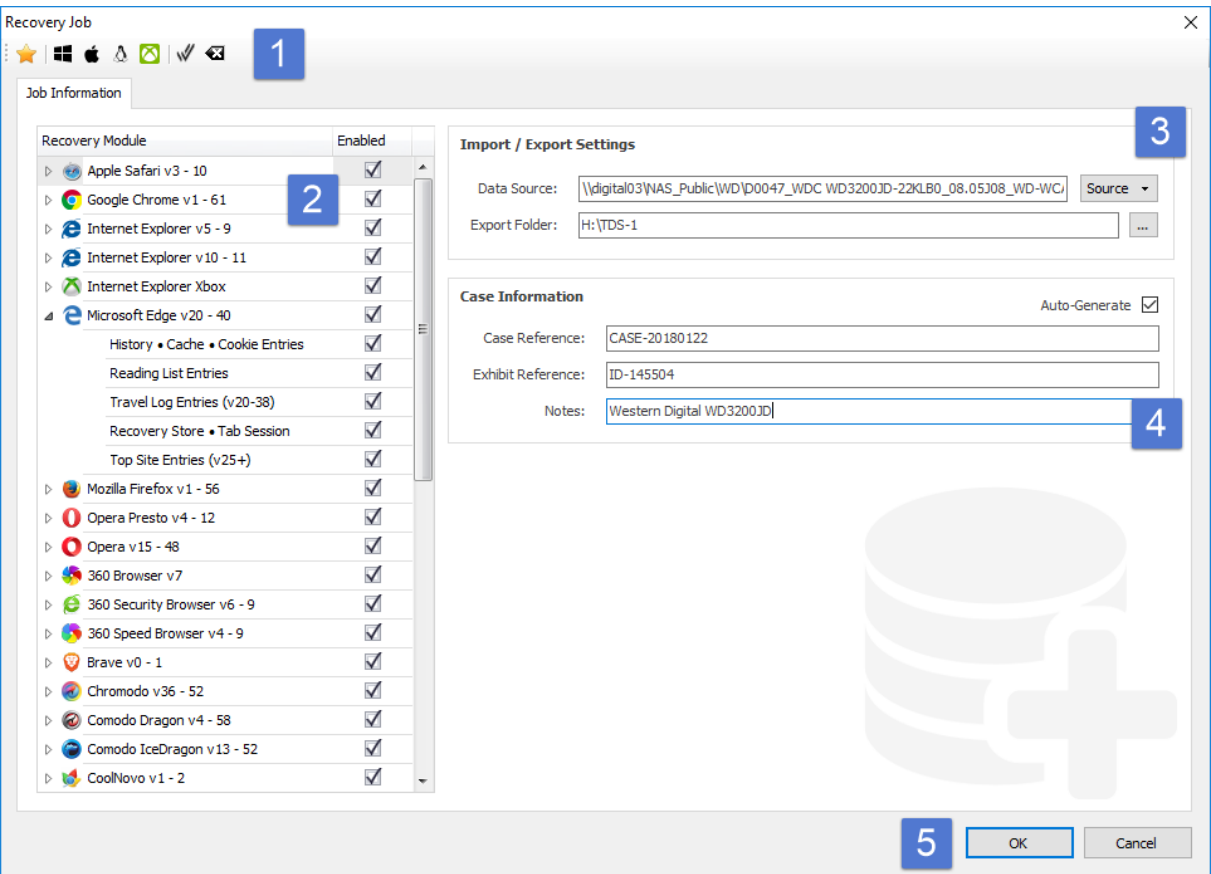


Figure 191

HstEx® Recovery Job Window

1

Main Toolbar

This toolbar contains options for the selection or deselection of recovery modules, see Table 27 below.

2

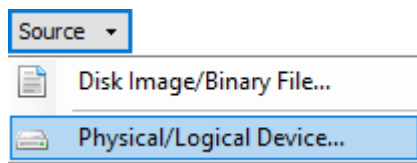
Recovery Modules

The available Recovery Modules are shown in a List. The user can select all the modules for a specific browser by clicking the tick box next to the browser name. By clicking the expansion icon ► next to the browser name, the user can view and select any of the specific recovery types.

3

Import/Export Settings

The Data Source can be selected by clicking the **Source** dropdown button:



Disk Image/Binary File

Allows a binary dump or image to be selected as the source.

Physical/Logical Device

Opens the Physical/Logical Device window containing a list of all valid devices available for processing. See Figure 192.

Export Folder

Opens a Select Folder window allowing the user to select a folder for the recovered data and logs to be written to.

4

Case Information

Contains information relating to the case the source data belongs to.

Case Reference

A mandatory text box where the case reference for the source data can be added.

Exhibit Reference

A mandatory text box where the exhibit or evidence ID for the source data can be added.

Notes

An optional text box for any relevant information to be added.

HstEx® Recovery Job Window

5

Buttons

OK will save the Recovery Job (if it contains valid parameters). **Cancel** will close the Recovery Job window without saving the Recovery Job.








The error icon  will appear against any mandatory Text Boxes or Recovery Module item should it contain invalid data or an invalid option. Hover your mouse over the icon for further information. You must rectify the issue to save the Recovery Job.


Table 26

Recovery Job Main Toolbar

The main toolbar of the Recovery Job window contains options for the selecting and deselecting of available Recovery Modules. Table 27 explains the meaning of each button.

HstEx® Recovery Job Main Toolbar	
	<div>Select Common</div> <div>Selects all common Recovery Modules.</div>
	<div>Select Windows</div> <div>Selects the Recovery Modules for browsers that can be installed on Microsoft Windows.</div>
	<div>Select OS X</div> <div>Selects the Recovery Modules for browsers that can be installed on Apple OS X.</div>
	<div>Select Linux</div> <div>Selects the Recovery Modules for browsers that can be installed on Linux.</div>
	<div>Select Xbox</div> <div>Selects the Recovery Modules for browsers that can be installed on Microsoft Xbox.</div>
	<div>Select All</div> <div>Select all Recovery Modules.</div>

HstEx® Recovery Job Main Toolbar



Clear All

Clears the selection of all Recovery Modules.

Table 27

Physical/Logical Devices Window

The Physical/Logical Devices window lists all of the attached devices that are available for processing. Select the device you wish to process and click **OK**.

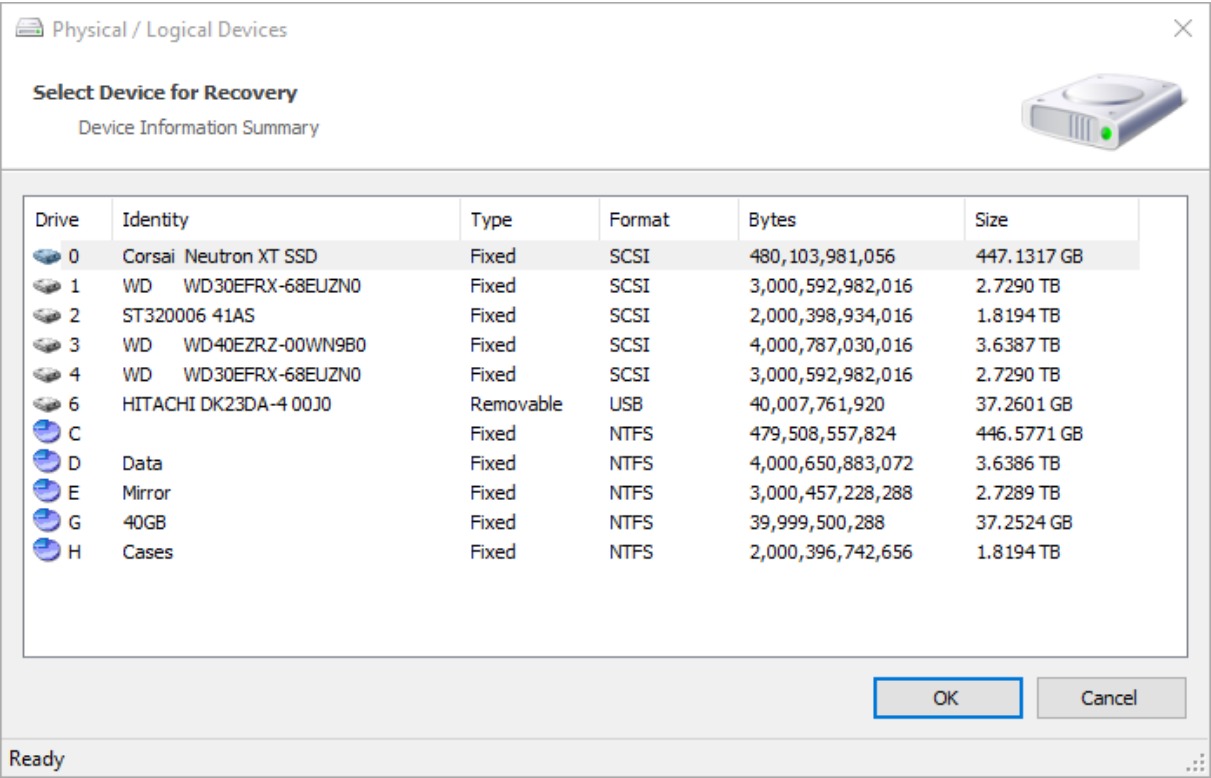


Figure 192

Options Window

The Options window (as shown in Figure 193) can be accessed from the Tools menu button: **Tools » Options**.

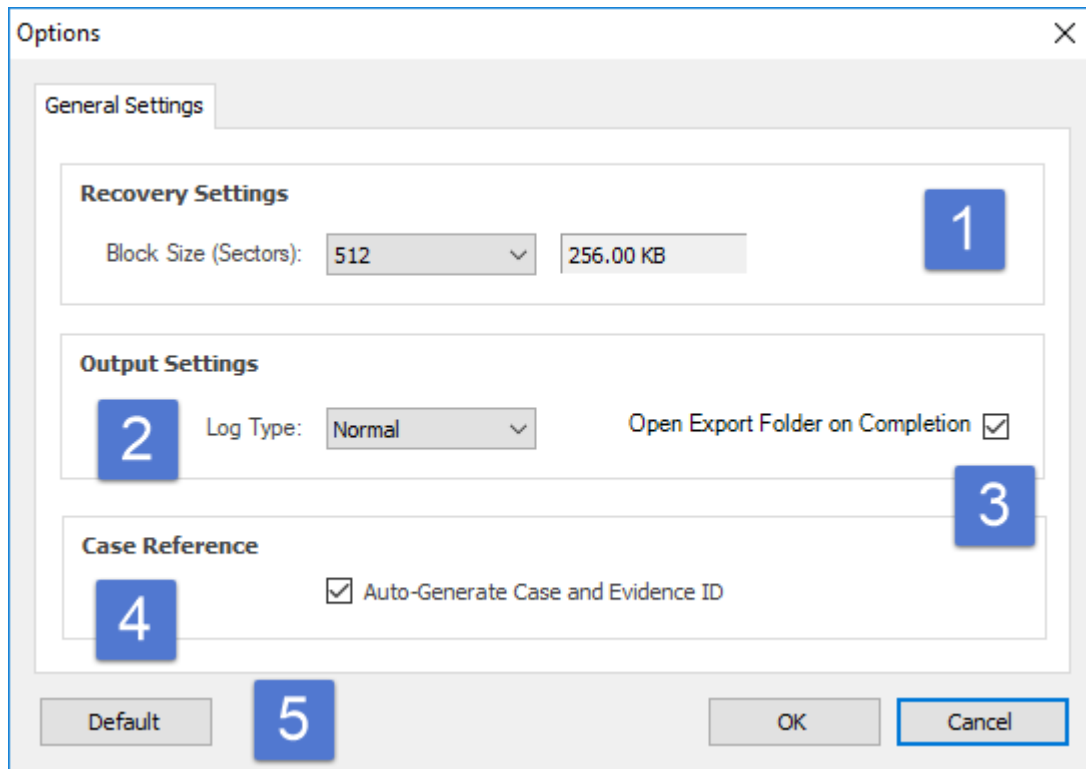


Figure 193

The main elements of the window have been numbered; for a description of each element, see Table 28 below.

HstEx® Recovery Job Window

1

Recovery Settings » Block Size

This setting changes the size of the blocks processed by HstEx® when searching for data. Changing this block size will affect the searching speed. The default value of 512 Sectors (256.00 KB) represents the optimal value for performance.

2

Output Settings » Log Type

There are two settings available, **Normal** and **Debug**. The default setting is **Normal**.

3

Output Settings » Open Export Folder on Completion

This setting will automatically open the Export Folder for the Recovery Job when it has completed.

4

Case Reference » Auto-Generate Case and Evidence ID

This setting generates Case and Exhibit IDs for mandatory fields when adding a new Recovery Job. Normally, the user would replace these values with the real values for the case.

HstEx® Recovery Job Window

5

Buttons

The **Default** button returns all settings and options to their default value. The **OK** button will save any changes that have been made. The **Cancel** button will close the options window without saving any changes.

Table 28

File Extensions

When you create and save a recovery session in HstEx®, a session database file is created with an *.hx4s extension. As recovery jobs are added to the session, they will be saved to this database. At a later date, the session database can be re-opened in HstEx® and re-run if required. The session database will also remember the state of each job, so if a session is cancelled before it has been completed, HstEx® can continue processing each outstanding job. Figure 194 shows a folder containing a number of session databases.

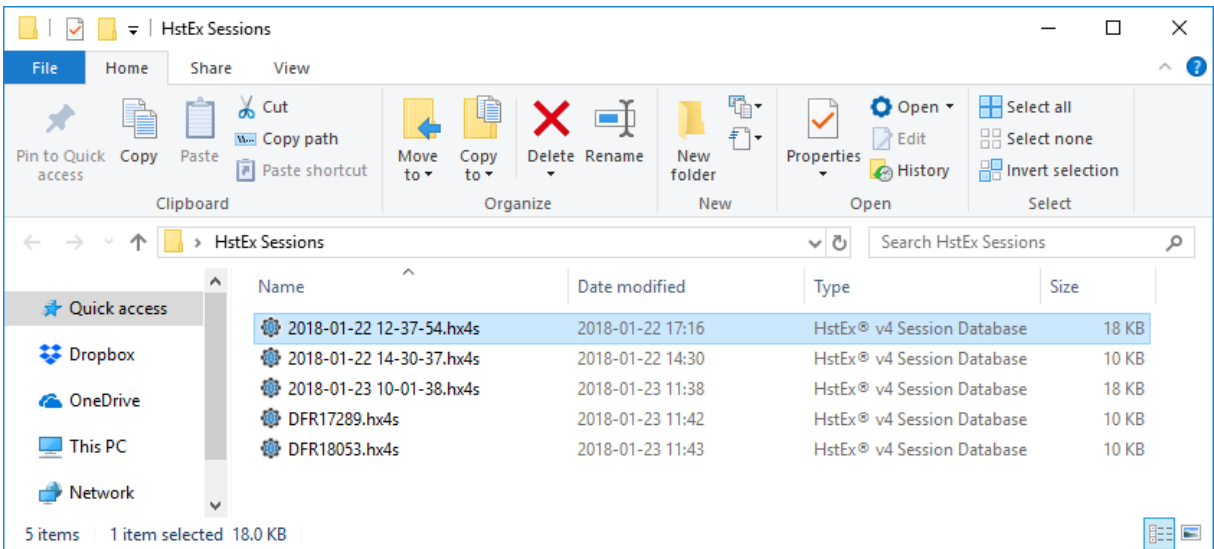


Figure 194

HstEx® Recovery File (*.hstx)

The HstEx® recovery file contains recovered data from a HstEx® recovery job. The file data is stored in a proprietary encrypted binary format which can only be read by NetAnalysis®. The recovery files are

written to the export folder for that specific job. The export folder is set when the recovery job is created in HstEx®. Figure 195 shows an export folder containing multiple recovery files.

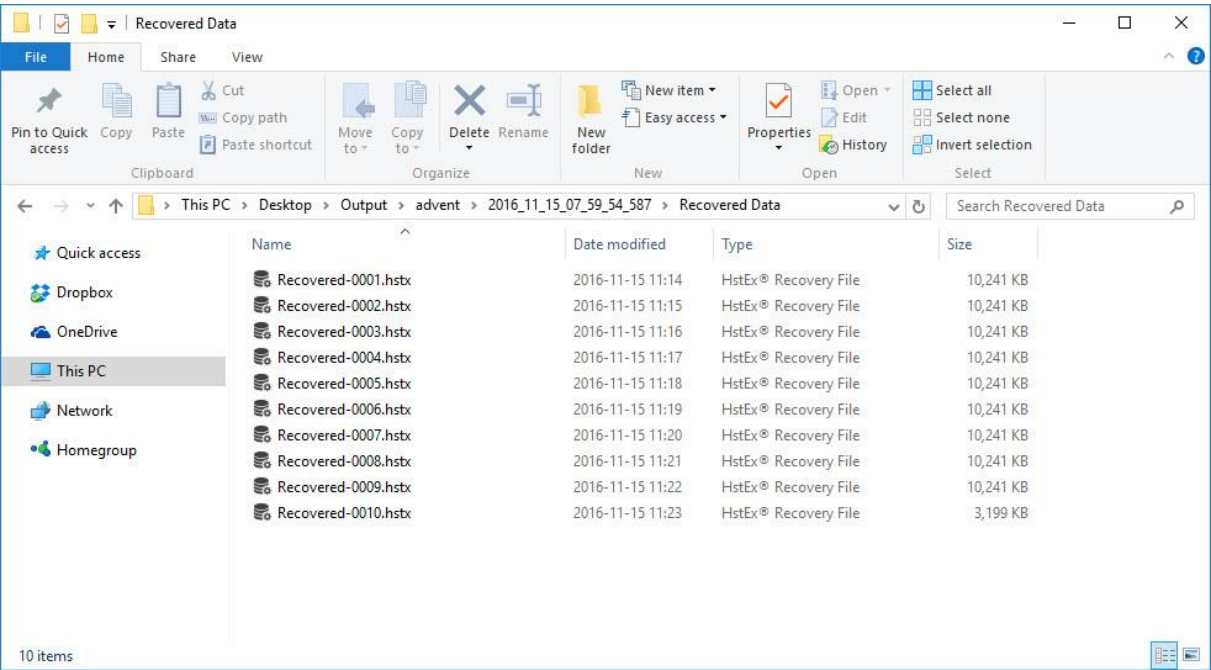


Figure 195

HstEx® Quick Start

Introduction

This chapter provides a brief introduction to working with HstEx® and explains how to create and run a recovery job.

Recovery Sessions

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.

Creating a New Session

To create a new recovery session, launch HstEx® and click on the **New Session** button. This will open the Save As window allowing you to name and select a location to save the session database file.

A session database holds information relating to the recovery job(s) you add during that session. The file has the extension **hx4s**.

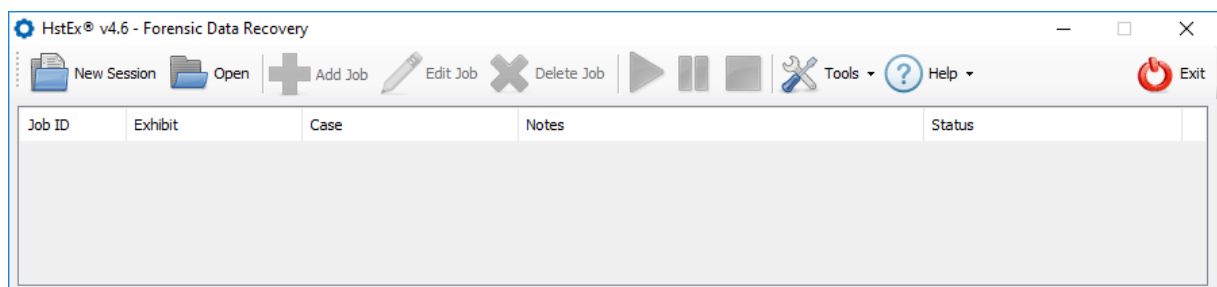


Figure 196

Adding a Recovery Job

To add a recovery job, click on the **Add Job** button. This will open the Recovery Job window (as shown in Figure 197).

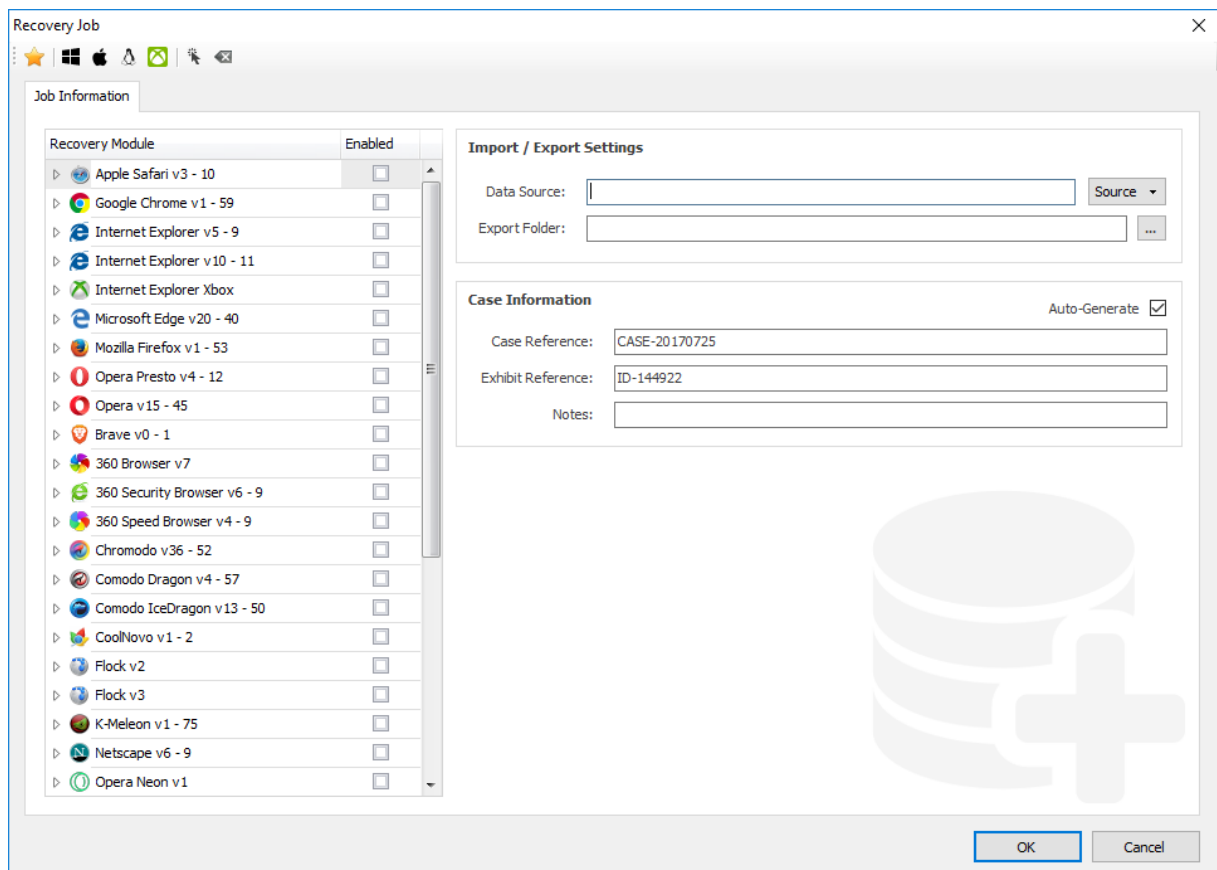


Figure 197

Recovery Module

On the left-hand side of the Recovery Job window, there is a list of Recovery Modules. Each recovery module is grouped by a specific browser and can be individually selected or deselected.

Clicking on the arrow to the left of the browser group name expands the entire group showing the individual recovery modules available.

All of the recovery modules can be shown by right clicking and selecting **Expand All**. To collapse all of the browser groups, right click and select **Collapse All**. The right click menu also has options for clearing or selecting all of the available recovery modules.

When a browser group is expanded, all of its recovery modules will be listed, as shown in Figure 198.

Recovery Module	Enabled
▶ Apple Safari v3 - 10	<input type="checkbox"/>
▲ Google Chrome v1 - 59	<input checked="" type="checkbox"/>
History Entries	<input checked="" type="checkbox"/>
Download Entries	<input checked="" type="checkbox"/>
Cookie Entries	<input checked="" type="checkbox"/>
Cache Entries	<input checked="" type="checkbox"/>
Simple Cache Entries (v29+)	<input checked="" type="checkbox"/>
Keyword Search Terms	<input checked="" type="checkbox"/>
Form History	<input checked="" type="checkbox"/>
Login Data	<input checked="" type="checkbox"/>
▶ Internet Explorer v5 - 9	<input type="checkbox"/>
▶ Internet Explorer v10 - 11	<input type="checkbox"/>
▶ Internet Explorer Xbox	<input type="checkbox"/>
▶ Microsoft Edge v20 - 40	<input type="checkbox"/>
▶ Mozilla Firefox v1 - 53	<input type="checkbox"/>
▶ Opera Presto v4 - 12	<input type="checkbox"/>
▶ Opera v15 - 45	<input type="checkbox"/>
▶ Brave v0 - 1	<input type="checkbox"/>
▶ 360 Browser v7	<input type="checkbox"/>
▶ 360 Security Browser v6 - 9	<input type="checkbox"/>
▶ 360 Speed Browser v4 - 9	<input type="checkbox"/>
▶ Chromodo v36 - 52	<input type="checkbox"/>

Figure 198

To select all of the recovery modules for a specific browser, click the check mark to the right of the browser group name.

Data Source

Each recovery job requires a single data source. HstEx® supports a number of forensic image formats, as well as direct recovery from physical and logical devices.

To select a source, click on the **Source** drop-down button. You can now select either **Disk Image/Binary File** or **Physical/Logical Device** (as shown in Figure 199).

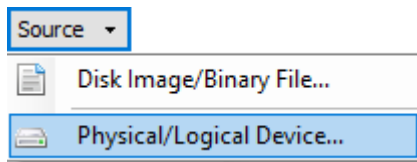


Figure 199

Clicking on **Disk Image/Binary File** will open a window allowing the user to select an image file (such as an EnCase® ex01 image) or a binary dump from a mobile phone.

Clicking on **Physical/Logical Device** will open a window allowing the user to select a device attached to the system.

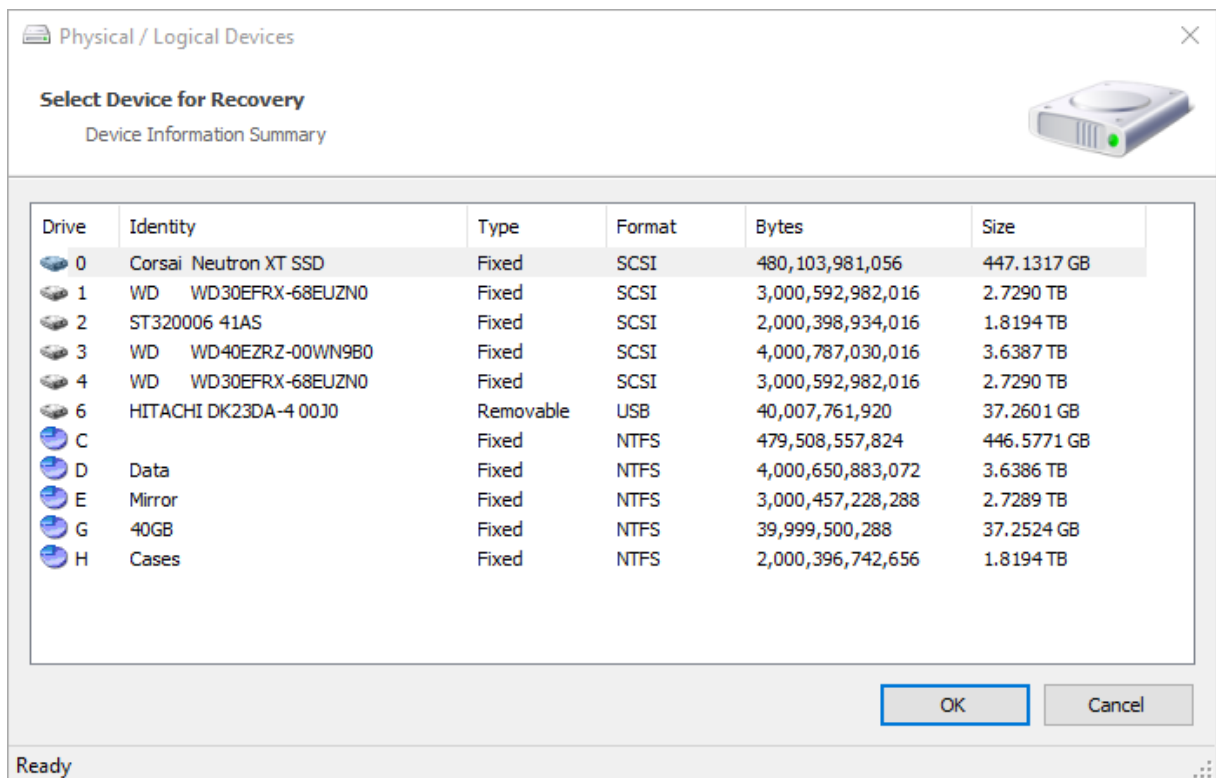


Figure 200

Export Folder

To select the export folder, Click on the '...' button to the right of the Export Folder box. This will open a window allowing the user to select a location to save the recovered data and log files.

Case Information

The Case Information section allows the user to add case specific data such as case and exhibit reference data. There is also a free text notes section.

Saving Recovery Job

Once the recovery job has been configured, click **OK** to save the job and close the Recovery Job window. This new job will now appear in the Job List as shown in Figure 201.


Job ID	Exhibit	Case	Notes	Status
 1	ID-153332	CASE-20170725	Image of TOSHIBA MK1652GSX serial number 99KBD4XZZ	Queued

Figure 201

Opening an Existing Session

If you have previously created a recovery session, click the **Open** button on the toolbar and select the *.hx4s Session Database file (as shown in Figure 202).

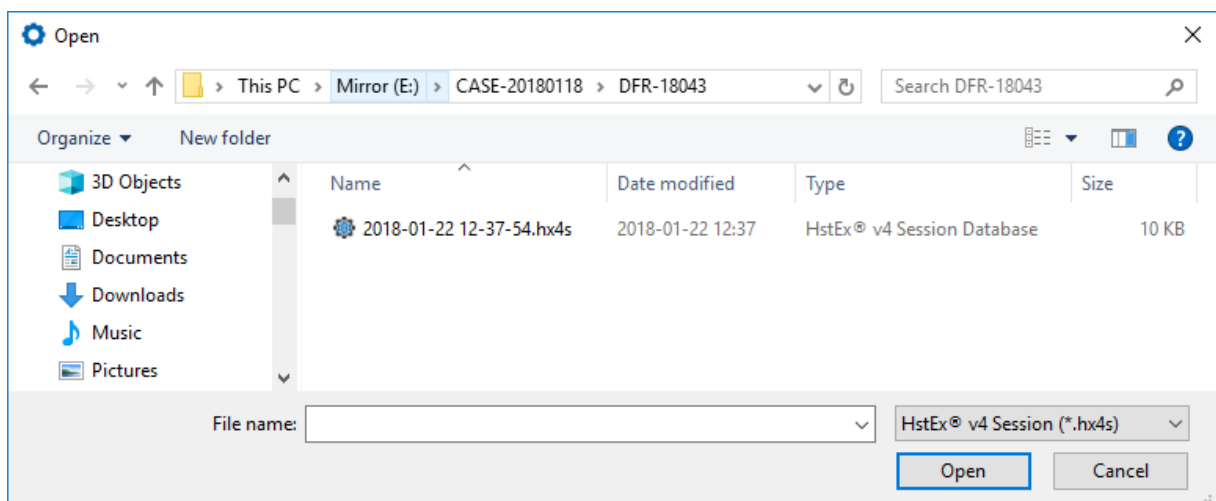


Figure 202

Running the Recovery

After one or more Recovery Jobs have been added, the recovery process can start. Click the Start Recovery button on the toolbar. The Status for the first job will change from Queued to Running as can be seen in Figure 203 below.

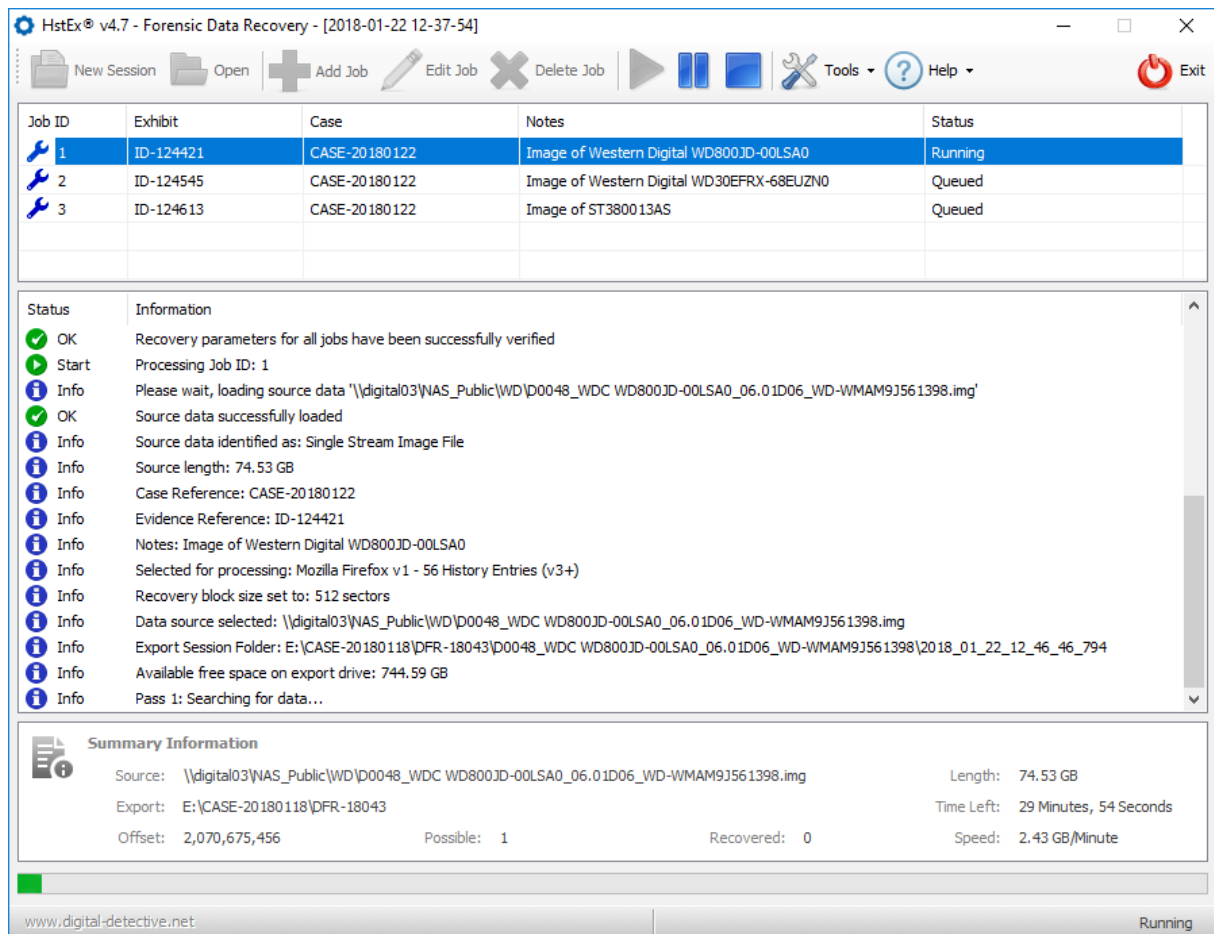


Figure 203

The first stage of the recovery process is to sequentially search, block by block, across the entire source. During this pass, the Summary Information panel will display the progress. As HstEx® searches for possible records and files (depending upon which Recovery Profiles have been selected), the count of possible search matches is displayed (as shown in Figure 204).

Summary Information			
Source:	\\digital04\NAS_Public\Imaging\D0050_SAMSUNG SP1213N_TL100-24_0777J1FWB03244.img	Length:	111.82 GB
Export:	E:\CASE-20180118\SAMSUNG SP1213N	Time Left:	25 Minutes, 38 Seconds
Offset:	74,180,198,400	Possible:	517,742
		Recovered:	0
		Speed:	1.67 GB/Minute

Figure 204

When the recovery job has completed, if there is another job in the queue, it will begin to process automatically. If the option to open the Export Folder on completion has been set in Options, the folder relating to the completed job will open (as shown in Figure 205).

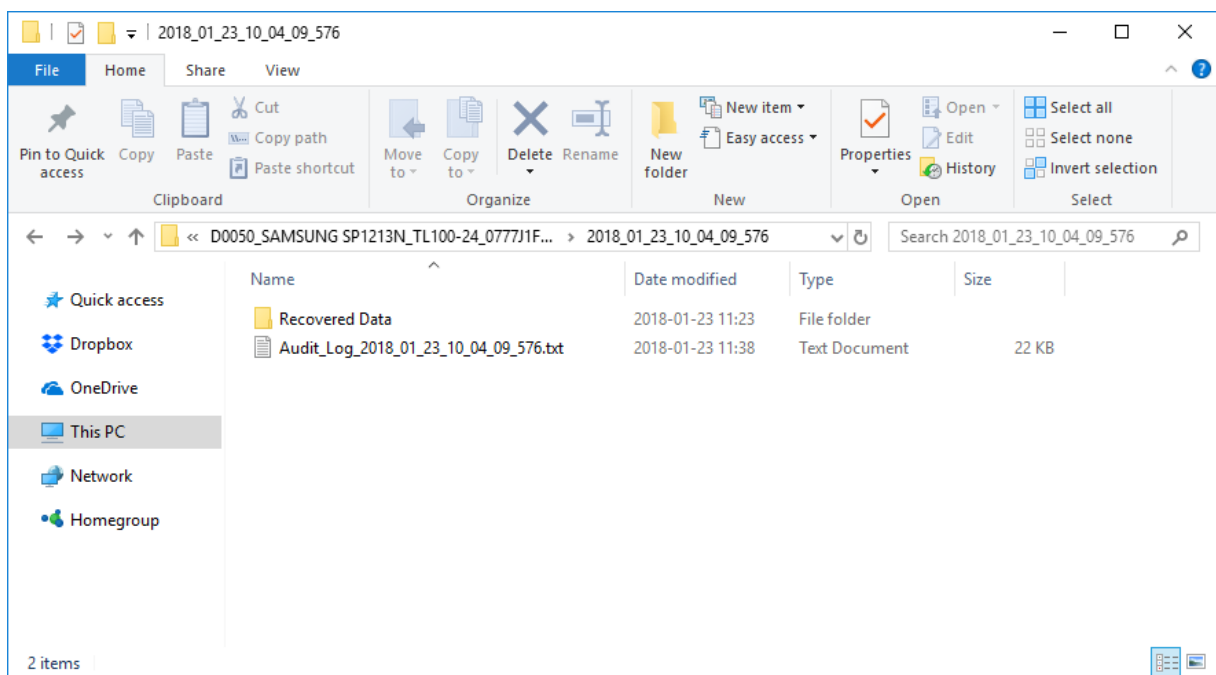


Figure 205

The recovered data for this job will be located in a folder called Recovered Data. Inside this folder will be one or more files in the following format:

Recovered-0000.hstx

See Figure 206 for an example Export folder.

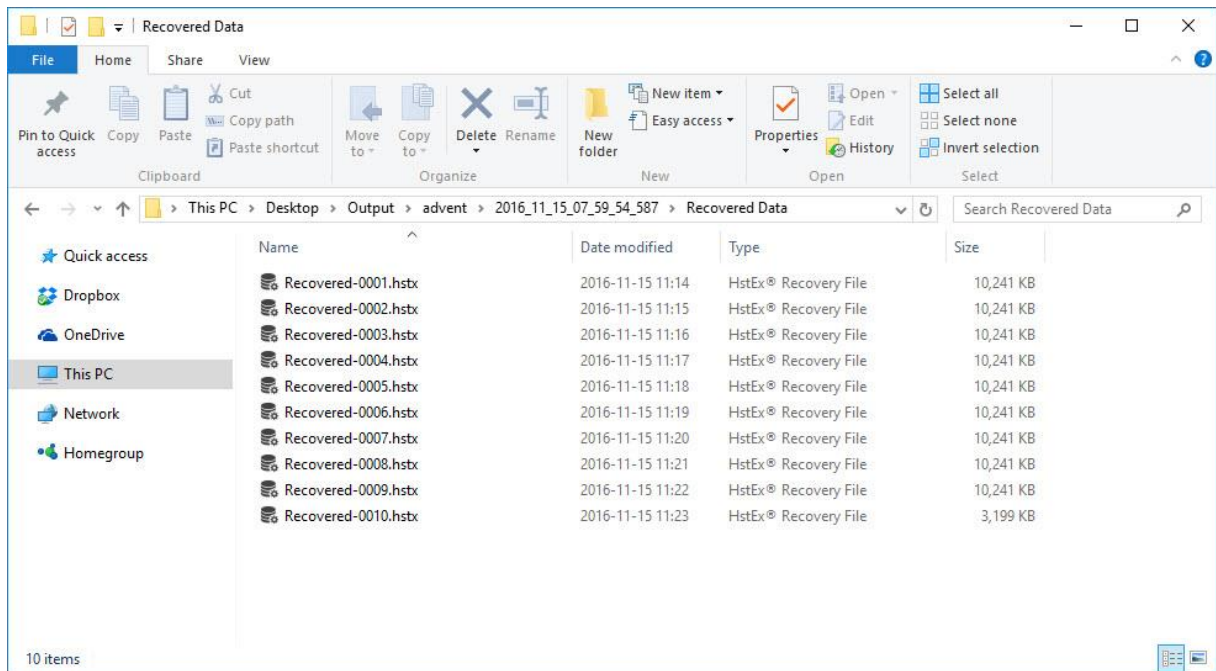


Figure 206

Importing HstEx® Recovery Files into NetAnalysis®

To import the recovered data from a HstEx® recovery session, start a new case in NetAnalysis® and select **Import » Data from Folder** from the toolbar drop down button (as shown in Figure 207). Select the folder containing the *.hstx files and click **OK**.

Selecting all of the files from **Import » Data from Files** works in exactly the same way (except you must select all *.hstx files).

You can also select **Import** from the **File** menu.

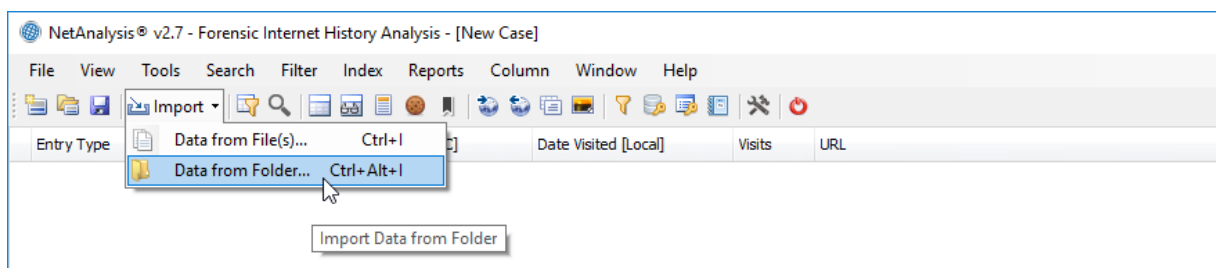


Figure 207

Technical Support

Introduction

When seeking assistance with our software, it is extremely important that you provide enough information to allow us to understand, and potentially recreate your issue. Trying to remotely diagnose a problem is extremely difficult, particularly when we cannot have access to your original data.

Please be patient, and try and provide as much information as possible. To assist in the process, please read the following section prior to submitting any support ticket. Please remember to let us know if we managed to assist you.

Identifying Software Version

Prior to submitting a support request, please open the **About** window (accessible from the **Help** menu) and note the following important information:

- Software name and Version Information;
- Operating System and Version Information;
- Licence ID and Serial Number;
- Customer ID and Licence Name;
- Expiration Date for your Software Maintenance Service (SMS).



WARNING: You must have valid SMS to be able to obtain technical support.

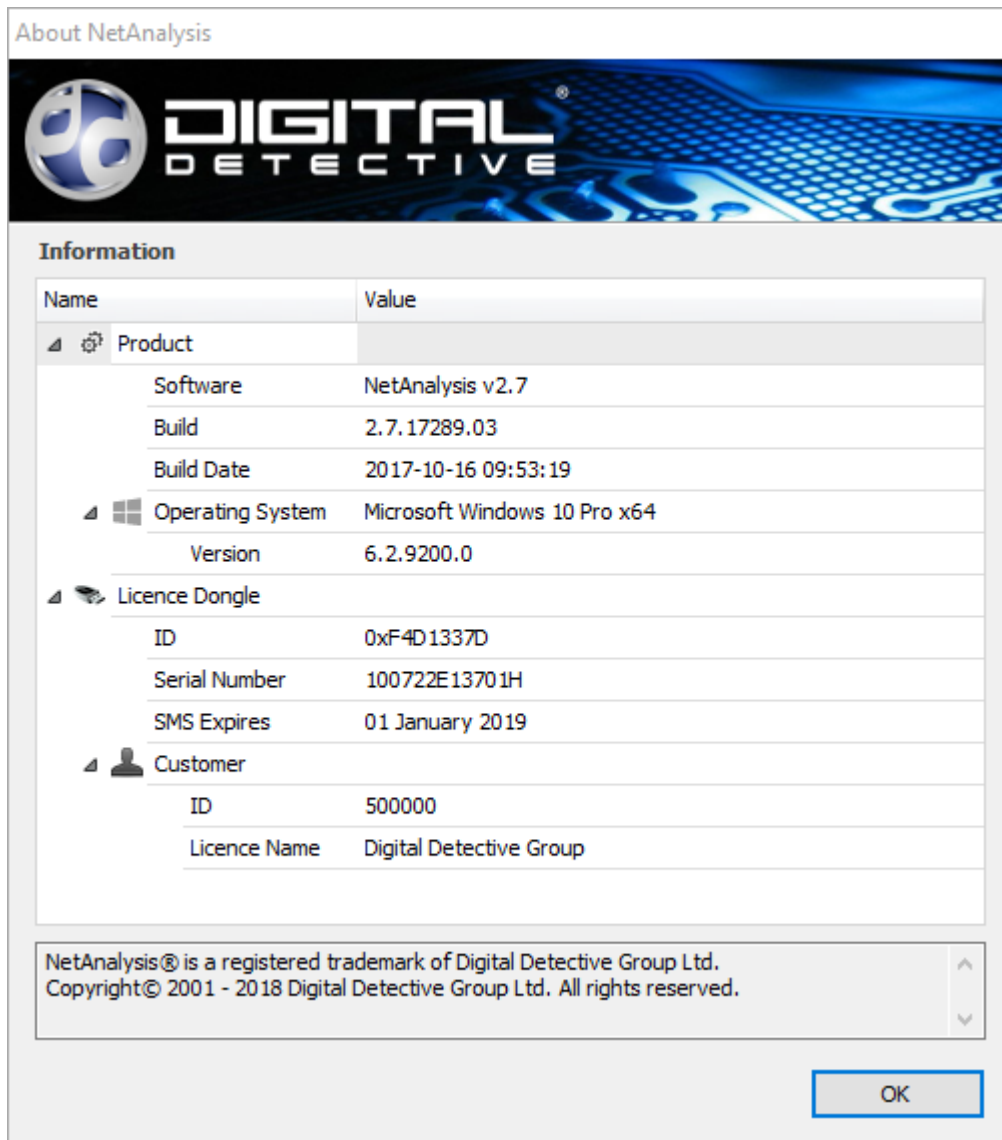


Figure 208

Figure 208 shows the About window from NetAnalysis®.

Submitting an Issue Report

The aim of an issue report is to enable a software engineer to identify a specific problem with the software and to establish what needs to be done to rectify the issue. To enable them to do this, you must provide careful and detailed instructions on how to recreate the issue.

If they cannot replicate your issue, they will try to gather extra information until they understand the cause. If they cannot make it fail, they will have to ask you to gather that information for them.

Please remember, your hardware/software setup may be completely different from our test environments and the way you use our software may also be completely different.

Background Information

There are three elements to a bug report:

- What you did;
- What you wanted to happen;
- What actually happened.

The most important element will be to provide step by step instructions to recreate the issue. This will allow us to recreate the bug, and put us in a much better position to rectify the problem and fix it in a future release. Use screen captures if you can; these will help the engineer to understand what you are trying to explain. Getting access to the data causing the issue is also very important. This is sometimes the only way to recreate a problem.

Single line submissions such as "It won't work" do not provide us with any useful information and will not allow an engineer to diagnose the problem. This will not help you in trying to get the software to work and the problem resolved as quickly as possible.

Change Log and Version History

Prior to submitting a bug report or request, please review the release history for the software. This could save you time by checking to see if the issue you have has already been identified and resolved. Please also ensure you are using the latest release of our software.

If you have encountered two bugs that don't appear to be related, create a new bug report for each one. This makes it easier for different people to help with the different bugs.

The software Release Notes can be found at the following locations:

NetAnalysis® Release Notes

<http://kb.digital-detective.net/x/VoCI>

HstEx® Release Notes

<http://kb.digital-detective.net/x/AgCQ>

Audit and Error Logs

As our software imports and/or processes data, they will write an Audit Log to the Case Export Folder. This log can be extremely helpful when trying to diagnose issues. It is important you provide this log when requesting help.


 Audit_Log_2018_01_12_15_08_14_289	12/01/2018 15:10	Text Document	7 KB
---	------------------	---------------	------

Figure 209

If NetAnalysis® or HstEx® encounters an error, they will write an error log to the root of the Case Export Folder.

The folder can be opened by selecting **Tools » Open Case Export Folder** in NetAnalysis® or **Tools » Open Export Folder** in HstEx.

Submitting a Request

To submit a support request, please visit the following page:

<http://www.digital-detective.net/support-portal/submit-support-request/>

Alternatively, an email can be submitted to:

support@digital-detective.net

List of References

Reference Index

- [1]. Microsoft, (2011). Daylight Saving Time Help and Support. Retrieved October 2011, from [*http://support.microsoft.com/gp/cp_dst*](http://support.microsoft.com/gp/cp_dst)
- [2]. Microsoft, (2006). What are Control Sets? What is CurrentControlSet? Retrieved October 2011, from [*http://support.microsoft.com/kb/100010*](http://support.microsoft.com/kb/100010)
- [3]. Microsoft, (2006). SYSTEMTIME structure. Retrieved December 2016, from [*https://msdn.microsoft.com/en-us/library/windows/desktop/ms724950\(v=vs.85\).aspx*](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724950(v=vs.85).aspx)
- [4]. Unicode® Consortium (1991 - 2017). The Unicode® Standard. Retrieved December 2016, from [*http://www.unicode.org/standard/standard.html*](http://www.unicode.org/standard/standard.html)

Appendix A

NetAnalysis® Keyboard Shortcuts

Table 29 contains a list of keyboard shortcuts for the main application window.

Shortcut Key	Action Description
Ctrl + N	New Case
Ctrl + O	Open Workspace
Ctrl + I	Import Data from File
Ctrl + Alt + I	Import Data from Folder
Ctrl + S	Save Workspace
Alt + F4	Exit
Ctrl + Shift + U	Open the Preview URL Panel
Ctrl + Shift + D	Open the Decode URL Panel
Ctrl + Shift + C	Open the Cookie Examiner
Ctrl + Shift + I	Open the Information Panel
Ctrl + Shift + W	Open the Warnings Panel
Ctrl + Shift + F	Open the Filter Manager
Ctrl + Shift + K	Open the Keyword Manager
Ctrl + Shift + R	Open the Report Manager
Ctrl + E	Open the Export Folder
Ctrl + Shift + E	Export and Rebuild Cache

Shortcut Key	Action Description
Ctrl + U	Navigate to Record URN
Space	Tag Record
Ctrl + F2	Navigate to First Tagged Record
F3	Navigate to Next Tagged Record
F2	Navigate to Previous Tagged Record
Ctrl + Shift + F2	Navigate to First Bookmarked Record
Shift + F3	Navigate to Next Bookmarked Record
Shift + F2	Navigate to Previous Bookmarked Record
Ctrl + H	Open Source in Hex Viewer
F7	Open the Quick Search Panel
Ctrl + F5	Clear Search
Ctrl + F7	Show the Search Index Window
F8	Open the Filter Editor
Ctrl + F8	Open the Auto Filter Row
F9	Filter Tagged Records
F5	Remove the Currently Active Filter
Ctrl + Shift + A	Display All Panels
Ctrl + L	Load Window Layout
F10	Enables Hotkey Functionality
Ctrl + A	Selects All Records

Table 29

Appendix B

HstEx® Keyboard Shortcuts

Table 30 contains a list of keyboard shortcuts for the main application window.

Shortcut Key	Action Description
Ctrl + Shift + R	Reset Job Queue
Ctrl + E	Open Export Folder

Table 30

Appendix C

Extended ASCII Table

Table 31 below shows the extended ASCII character set.

DEC	OCT	HEX	BIN	Symbol	Description
0	000	00	00000000	NUL	Null Character
1	001	01	00000001	SOH	Start of Heading
2	002	02	00000010	STX	Start of Text
3	003	03	00000011	ETX	End of Text
4	004	04	00000100	EOT	End of Transmission
5	005	05	00000101	ENQ	Enquiry
6	006	06	00000110	ACK	Acknowledgment
7	007	07	00000111	BEL	Bell
8	010	08	00001000	BS	Back Space
9	011	09	00001001	HT	Horizontal Tab
10	012	0A	00001010	LF	Line Feed
11	013	0B	00001011	VT	Vertical Tab
12	014	0C	00001100	FF	Form Feed
13	015	0D	00001101	CR	Carriage Return
14	016	0E	00001110	SO	Shift Out / X-On
15	017	0F	00001111	SI	Shift In / X-Off
16	020	10	00010000	DLE	Data Line Escape

DEC	OCT	HEX	BIN	Symbol	Description
17	021	11	00010001	DC1	Device Control 1 (oft. XON)
18	022	12	00010010	DC2	Device Control 2
19	023	13	00010011	DC3	Device Control 3 (oft. XOFF)
20	024	14	00010100	DC4	Device Control 4
21	025	15	00010101	NAK	Negative Acknowledgement
22	026	16	00010110	SYN	Synchronous Idle
23	027	17	00010111	ETB	End of Transmit Block
24	030	18	00011000	CAN	Cancel
25	031	19	00011001	EM	End of Medium
26	032	1A	00011010	SUB	Substitute
27	033	1B	00011011	ESC	Escape
28	034	1C	00011100	FS	File Separator
29	035	1D	00011101	GS	Group Separator
30	036	1E	00011110	RS	Record Separator
31	037	1F	00011111	US	Unit Separator
32	040	20	00100000		Space
33	041	21	00100001	!	Exclamation mark
34	042	22	00100010	"	Double quotes (or speech marks)
35	043	23	00100011	#	Hash (or pound)
36	044	24	00100100	\$	Dollar
37	045	25	00100101	%	Percent
38	046	26	00100110	&	Ampersand
39	047	27	00100111	'	Single quote

DEC	OCT	HEX	BIN	Symbol	Description
40	050	28	00101000	(Open parenthesis (or open bracket)
41	051	29	00101001)	Close parenthesis (or close bracket)
42	052	2A	00101010	*	Asterisk
43	053	2B	00101011	+	Plus
44	054	2C	00101100	,	Comma
45	055	2D	00101101	-	Hyphen
46	056	2E	00101110	.	Period, dot or full stop
47	057	2F	00101111	/	Slash or divide
48	060	30	00110000	0	Zero
49	061	31	00110001	1	One
50	062	32	00110010	2	Two
51	063	33	00110011	3	Three
52	064	34	00110100	4	Four
53	065	35	00110101	5	Five
54	066	36	00110110	6	Six
55	067	37	00110111	7	Seven
56	070	38	00111000	8	Eight
57	071	39	00111001	9	Nine
58	072	3A	00111010	:	Colon
59	073	3B	00111011	;	Semicolon
60	074	3C	00111100	<	Less than (or open angled bracket)
61	075	3D	00111101	=	Equals
62	076	3E	00111110	>	Greater than (or close angled bracket)

DEC	OCT	HEX	BIN	Symbol	Description
63	077	3F	00111111	?	Question mark
64	100	40	01000000	@	At symbol
65	101	41	01000001	A	Uppercase A
66	102	42	01000010	B	Uppercase B
67	103	43	01000011	C	Uppercase C
68	104	44	01000100	D	Uppercase D
69	105	45	01000101	E	Uppercase E
70	106	46	01000110	F	Uppercase F
71	107	47	01000111	G	Uppercase G
72	110	48	01001000	H	Uppercase H
73	111	49	01001001	I	Uppercase I
74	112	4A	01001010	J	Uppercase J
75	113	4B	01001011	K	Uppercase K
76	114	4C	01001100	L	Uppercase L
77	115	4D	01001101	M	Uppercase M
78	116	4E	01001110	N	Uppercase N
79	117	4F	01001111	O	Uppercase O
80	120	50	01010000	P	Uppercase P
81	121	51	01010001	Q	Uppercase Q
82	122	52	01010010	R	Uppercase R
83	123	53	01010011	S	Uppercase S
84	124	54	01010100	T	Uppercase T
85	125	55	01010101	U	Uppercase U

DEC	OCT	HEX	BIN	Symbol	Description
86	126	56	01010110	V	Uppercase V
87	127	57	01010111	W	Uppercase W
88	130	58	01011000	X	Uppercase X
89	131	59	01011001	Y	Uppercase Y
90	132	5A	01011010	Z	Uppercase Z
91	133	5B	01011011	[Opening bracket
92	134	5C	01011100	\	Backslash
93	135	5D	01011101]	Closing bracket
94	136	5E	01011110	^	Caret - circumflex
95	137	5F	01011111	_	Underscore
96	140	60	01100000	`	Grave accent
97	141	61	01100001	a	Lowercase a
98	142	62	01100010	b	Lowercase b
99	143	63	01100011	c	Lowercase c
100	144	64	01100100	d	Lowercase d
101	145	65	01100101	e	Lowercase e
102	146	66	01100110	f	Lowercase f
103	147	67	01100111	g	Lowercase g
104	150	68	01101000	h	Lowercase h
105	151	69	01101001	i	Lowercase i
106	152	6A	01101010	j	Lowercase j
107	153	6B	01101011	k	Lowercase k
108	154	6C	01101100	l	Lowercase l

DEC	OCT	HEX	BIN	Symbol	Description
109	155	6D	01101101	m	Lowercase m
110	156	6E	01101110	n	Lowercase n
111	157	6F	01101111	o	Lowercase o
112	160	70	01110000	p	Lowercase p
113	161	71	01110001	q	Lowercase q
114	162	72	01110010	r	Lowercase r
115	163	73	01110011	s	Lowercase s
116	164	74	01110100	t	Lowercase t
117	165	75	01110101	u	Lowercase u
118	166	76	01110110	v	Lowercase v
119	167	77	01110111	w	Lowercase w
120	170	78	01111000	x	Lowercase x
121	171	79	01111001	y	Lowercase y
122	172	7A	01111010	z	Lowercase z
123	173	7B	01111011	{	Opening brace
124	174	7C	01111100		Vertical bar
125	175	7D	01111101	}	Closing brace
126	176	7E	01111110	~	Equivalency sign - tilde
127	177	7F	01111111		Delete
128	200	80	10000000	€	Euro sign
129	201	81	10000001		
130	202	82	10000010	,	Single low-9 quotation mark
131	203	83	10000011	f	Latin small letter f with hook

DEC	OCT	HEX	BIN	Symbol	Description
132	204	84	10000100	„	Double low-9 quotation mark
133	205	85	10000101	...	Horizontal ellipsis
134	206	86	10000110	†	Dagger
135	207	87	10000111	‡	Double dagger
136	210	88	10001000	^	Modifier letter circumflex accent
137	211	89	10001001	‰	Per mille sign
138	212	8A	10001010	Š	Latin capital letter S with caron
139	213	8B	10001011	‹	Single left-pointing angle quotation
140	214	8C	10001100	Œ	Latin capital ligature OE
141	215	8D	10001101		
142	216	8E	10001110	Ž	Latin capital letter Z with caron
143	217	8F	10001111		
144	220	90	10010000		
145	221	91	10010001	‘	Left single quotation mark
146	222	92	10010010	’	Right single quotation mark
147	223	93	10010011	“	Left double quotation mark
148	224	94	10010100	”	Right double quotation mark
149	225	95	10010101	•	Bullet
150	226	96	10010110	–	En dash
151	227	97	10010111	—	Em dash
152	230	98	10011000	~	Small tilde
153	231	99	10011001	™	Trade mark sign
154	232	9A	10011010	š	Latin small letter S with caron

DEC	OCT	HEX	BIN	Symbol	Description
155	233	9B	10011011	›	Single right-pointing angle quotation mark
156	234	9C	10011100	œ	Latin small ligature oe
157	235	9D	10011101		
158	236	9E	10011110	ž	Latin small letter z with caron
159	237	9F	10011111	ÿ	Latin capital letter Y with diaeresis
160	240	A0	10100000		Non-breaking space
161	241	A1	10100001	¡	Inverted exclamation mark
162	242	A2	10100010	¢	Cent sign
163	243	A3	10100011	£	Pound sign
164	244	A4	10100100	¤	Currency sign
165	245	A5	10100101	¥	Yen sign
166	246	A6	10100110		Pipe, Broken vertical bar
167	247	A7	10100111	§	Section sign
168	250	A8	10101000	¨	Spacing diaeresis - umlaut
169	251	A9	10101001	©	Copyright sign
170	252	AA	10101010	ª	Feminine ordinal indicator
171	253	AB	10101011	«	Left double angle quotes
172	254	AC	10101100	¬	Not sign
173	255	AD	10101101	­	Soft hyphen
174	256	AE	10101110	®	Registered trade mark sign
175	257	AF	10101111	¯	Spacing macron - overline
176	260	B0	10110000	°	Degree sign
177	261	B1	10110001	±	Plus-or-minus sign

DEC	OCT	HEX	BIN	Symbol	Description
178	262	B2	10110010	²	Superscript two - squared
179	263	B3	10110011	³	Superscript three - cubed
180	264	B4	10110100	´	Acute accent - spacing acute
181	265	B5	10110101	μ	Micro sign
182	266	B6	10110110	¶	Pilcrow sign - paragraph sign
183	267	B7	10110111	·	Middle dot - Georgian comma
184	270	B8	10111000	,	Spacing cedilla
185	271	B9	10111001	¹	Superscript one
186	272	BA	10111010	º	Masculine ordinal indicator
187	273	BB	10111011	»	Right double angle quotes
188	274	BC	10111100	¼	Fraction one quarter
189	275	BD	10111101	½	Fraction one half
190	276	BE	10111110	¾	Fraction three quarters
191	277	BF	10111111	¿	Inverted question mark
192	300	C0	11000000	À	Latin capital letter A with grave
193	301	C1	11000001	Á	Latin capital letter A with acute
194	302	C2	11000010	Â	Latin capital letter A with circumflex
195	303	C3	11000011	Ã	Latin capital letter A with tilde
196	304	C4	11000100	Ä	Latin capital letter A with diaeresis
197	305	C5	11000101	Å	Latin capital letter A with ring above
198	306	C6	11000110	Æ	Latin capital letter AE
199	307	C7	11000111	Ç	Latin capital letter C with cedilla
200	310	C8	11001000	È	Latin capital letter E with grave

DEC	OCT	HEX	BIN	Symbol	Description
201	311	C9	11001001	É	Latin capital letter E with acute
202	312	CA	11001010	Ê	Latin capital letter E with circumflex
203	313	CB	11001011	Ë	Latin capital letter E with diaeresis
204	314	CC	11001100	Ì	Latin capital letter I with grave
205	315	CD	11001101	Í	Latin capital letter I with acute
206	316	CE	11001110	Î	Latin capital letter I with circumflex
207	317	CF	11001111	Ï	Latin capital letter I with diaeresis
208	320	D0	11010000	Ð	Latin capital letter ETH
209	321	D1	11010001	Ñ	Latin capital letter N with tilde
210	322	D2	11010010	Ò	Latin capital letter O with grave
211	323	D3	11010011	Ó	Latin capital letter O with acute
212	324	D4	11010100	Ô	Latin capital letter O with circumflex
213	325	D5	11010101	Õ	Latin capital letter O with tilde
214	326	D6	11010110	Ö	Latin capital letter O with diaeresis
215	327	D7	11010111	×	Multiplication sign
216	330	D8	11011000	Ø	Latin capital letter O with slash
217	331	D9	11011001	Ù	Latin capital letter U with grave
218	332	DA	11011010	Ú	Latin capital letter U with acute
219	333	DB	11011011	Û	Latin capital letter U with circumflex
220	334	DC	11011100	Ü	Latin capital letter U with diaeresis
221	335	DD	11011101	Ý	Latin capital letter Y with acute
222	336	DE	11011110	Þ	Latin capital letter THORN
223	337	DF	11011111	ß	Latin small letter sharp s - ess-zed

DEC	OCT	HEX	BIN	Symbol	Description
224	340	E0	11100000	à	Latin small letter a with grave
225	341	E1	11100001	á	Latin small letter a with acute
226	342	E2	11100010	â	Latin small letter a with circumflex
227	343	E3	11100011	ã	Latin small letter a with tilde
228	344	E4	11100100	ä	Latin small letter a with diaeresis
229	345	E5	11100101	å	Latin small letter a with ring above
230	346	E6	11100110	æ	Latin small letter ae
231	347	E7	11100111	ç	Latin small letter c with cedilla
232	350	E8	11101000	è	Latin small letter e with grave
233	351	E9	11101001	é	Latin small letter e with acute
234	352	EA	11101010	ê	Latin small letter e with circumflex
235	353	EB	11101011	ë	Latin small letter e with diaeresis
236	354	EC	11101100	ì	Latin small letter i with grave
237	355	ED	11101101	í	Latin small letter i with acute
238	356	EE	11101110	î	Latin small letter i with circumflex
239	357	EF	11101111	ï	Latin small letter i with diaeresis
240	360	F0	11110000	ð	Latin small letter eth
241	361	F1	11110001	ñ	Latin small letter n with tilde
242	362	F2	11110010	ò	Latin small letter o with grave
243	363	F3	11110011	ó	Latin small letter o with acute
244	364	F4	11110100	ô	Latin small letter o with circumflex
245	365	F5	11110101	õ	Latin small letter o with tilde
246	366	F6	11110110	ö	Latin small letter o with diaeresis

DEC	OCT	HEX	BIN	Symbol	Description
247	367	F7	11110111	÷	Division sign
248	370	F8	11111000	ø	Latin small letter o with slash
249	371	F9	11111001	ù	Latin small letter u with grave
250	372	FA	11111010	ú	Latin small letter u with acute
251	373	FB	11111011	û	Latin small letter u with circumflex
252	374	FC	11111100	ü	Latin small letter u with diaeresis
253	375	FD	11111101	ý	Latin small letter y with acute
254	376	FE	11111110	þ	Latin small letter thorn
255	377	FF	11111111	ÿ	Latin small letter y with diaeresis

Table 31

Digital Detective Group

Innovation House
Discovery Park
Innovation Way
Sandwich, Kent, CT13 9FF
United Kingdom



©2018 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.