NetAnalysis v2.11

- Introduction
- New Browser Support
  - Avast Secure Browser
  - CCleaner Browser
- New Features
  - Apple Safari
- Improvements
  - Property Set Information
  - Filter Functions
- Change Log

Introduction

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

New Browser Support

We have added support for the following browsers:

Avast Secure Browser

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

CCleaner Browser

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

New Features

Apple Safari

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

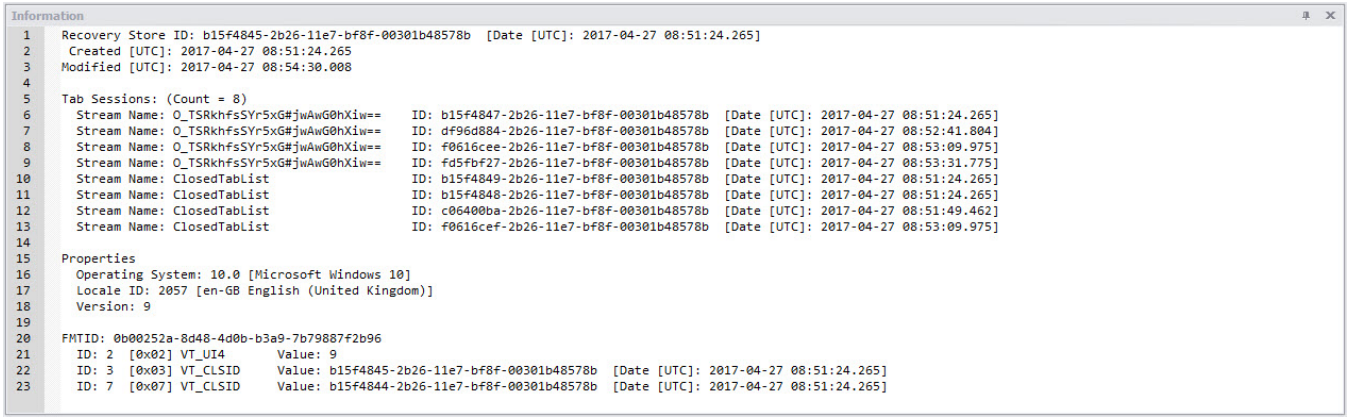
Improvements

Property Set Information

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

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

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



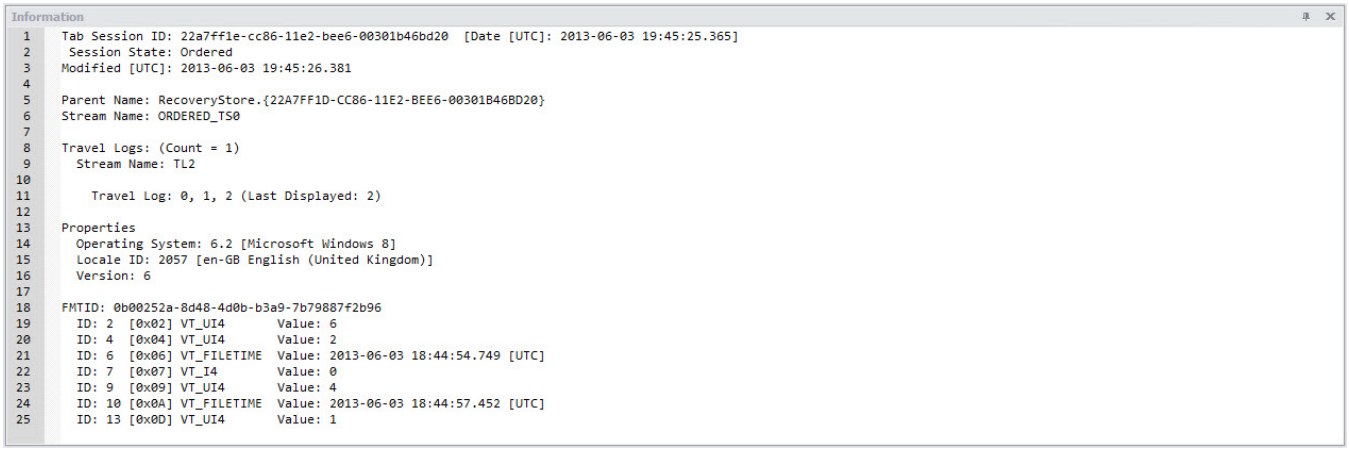
Information

```
Recovery Store ID: 16cf0cbe-98d9-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 09:43:06.266]
 Created [UTC]: 2015-12-02 09:39:02.172
Modified [UTC]: 2015-12-04 17:31:27.787

Tab Sessions: (Count = 28)
  Stream Name: O_TSiktRhdiY5RGCd#yqFAY+cw==    ID: 81498986-98db-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:00:23.900]
  Stream Name: O_TSiktRhdiY5RGCd#yqFAY+cw==    ID: 81498987-98db-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:00:23.900]
  Stream Name: O_TSiktRhdiY5RGCd#yqFAY+cw==    ID: 81498988-98db-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:00:23.900]
  Stream Name: O_TSiktRhdiY5RGCd#yqFAY+cw==    ID: 81498989-98db-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:00:23.900]
  Stream Name: O_TSiktRhdiY5RGCd#yqFAY+cw==    ID: 8149898a-98db-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:00:23.900]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad11c-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad11d-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad11e-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad11f-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad120-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad121-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad122-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad123-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad124-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad125-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad126-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad127-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad128-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad129-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TStdUsr9uY5RGCd#yqFAY+cw==    ID: d0aad12a-98dd-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:16:56.071]
  Stream Name: O_TSu3+k+t2Y5RGCd#yqFAY+cw==    ID: 8149cc81-98de-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:21:52.392]
  Stream Name: O_TSVUpZk96Y5RGCd#yqFAY+cw==    ID: 4e7a9bcd-98e0-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:34:46.142]
  Stream Name: O_TSVUpZk96Y5RGCd#yqFAY+cw==    ID: 4e7a9bce-98e0-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:34:46.142]
  Stream Name: O_TSNejZVm6a5RGCd#yqFAY+cw==    ID: 78d1fa96-9a6e-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-04 10:04:56.877]
  Stream Name: O_TSVHzByqKa5RGCd#yqFAY+cw==    ID: 577538eb-9aa4-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-04 16:30:33.728]
  Stream Name: O_TSVHzByqKa5RGCd#yqFAY+cw==    ID: 577538ec-9aa4-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-04 16:30:33.728]
  Stream Name: O_TSVHzByqKa5RGCd#yqFAY+cw==    ID: 577538ed-9aa4-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-04 16:30:33.728]
  Stream Name: O_TStqQE2aqa5RGCd#yqFAY+cw==    ID: ea44a478-9aaa-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-04 17:17:37.015]

Properties
  Operating System: 6.3 [Microsoft Windows 8.1]
  Locale ID: 2057 [en-GB English (United Kingdom)]
  Version: 9

FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
  ID: 2  [0x02] VT_UI4       Value: 9
  ID: 3  [0x03] VT_CLSID     Value: 16cf0cbe-98d9-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 09:43:06.266]
  ID: 7  [0x07] VT_CLSID     Value: 85514b88-98d8-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 09:39:02.172]
```

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

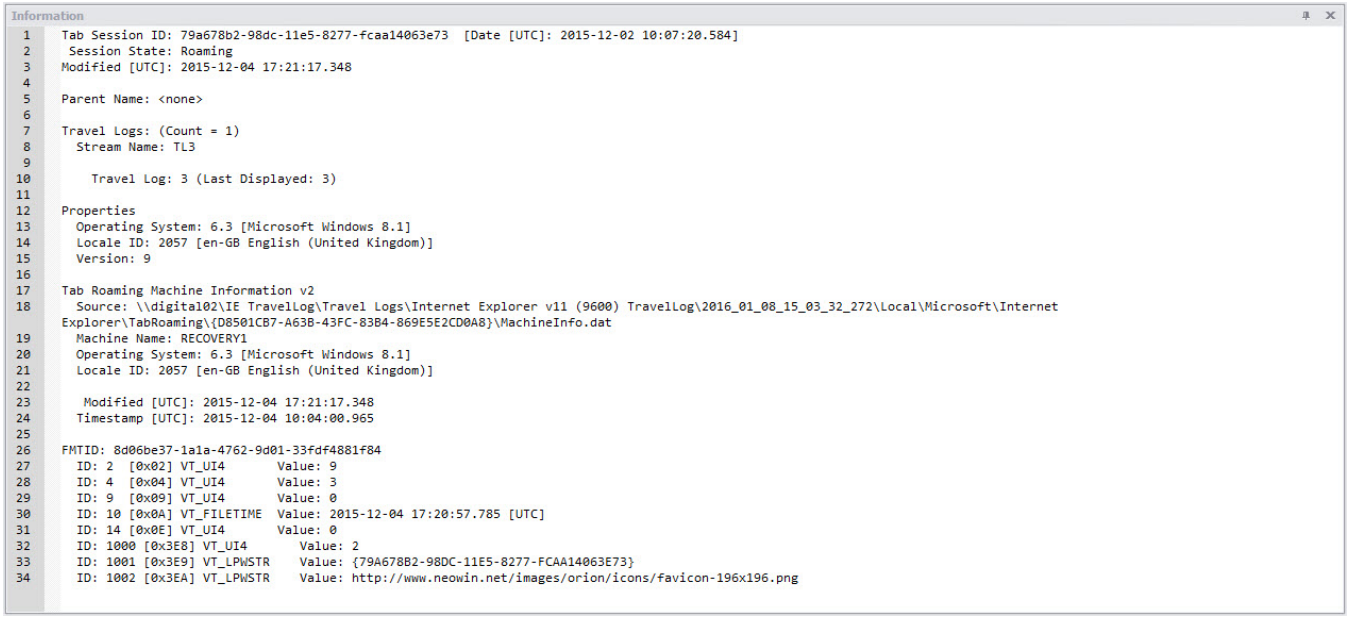
Information

```
Tab Session ID: b15f4847-2b26-11e7-bf8f-00301b48578b  [Date [UTC]: 2017-04-27 08:51:24.265]
 Session State: Ordered
Modified [UTC]: 2017-04-27 08:53:44.751

Parent Name: RecoveryStore.{B15F4845-2B26-11E7-BF8F-00301B48578B}
Stream Name: O_TSRkhfsSYr5xG#jwAwG0hXiw==

Travel Logs: (Count = 6)
  Stream Name: TL1
  Stream Name: TL2
  Stream Name: TL3
  Stream Name: TL4
  Stream Name: TL5
  Stream Name: TL6

    Travel Log: 0, 1, 2, 3, 4, 5, 6 (Last Displayed: 6)

Properties
  Operating System: 10.0 [Microsoft Windows 10]
  Locale ID: 2057 [en-GB English (United Kingdom)]
  Version: 9

FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
  ID: 2  [0x02] VT_UI4       Value: 9
  ID: 4  [0x04] VT_UI4       Value: 6
  ID: 6  [0x06] VT_FILETIME  Value: 2017-04-27 08:52:47.833 [UTC]
  ID: 7  [0x07] VT_I4        Value: 0
  ID: 9  [0x09] VT_UI4       Value: 1
  ID: 10 [0x0A] VT_FILETIME  Value: 2017-04-27 08:53:11.955 [UTC]
  ID: 13 [0x0D] VT_UI4       Value: 1
  ID: 14 [0x0E] VT_UI4       Value: 0
  ID: 17 [0x11] VT_UI4       Value: 0
```

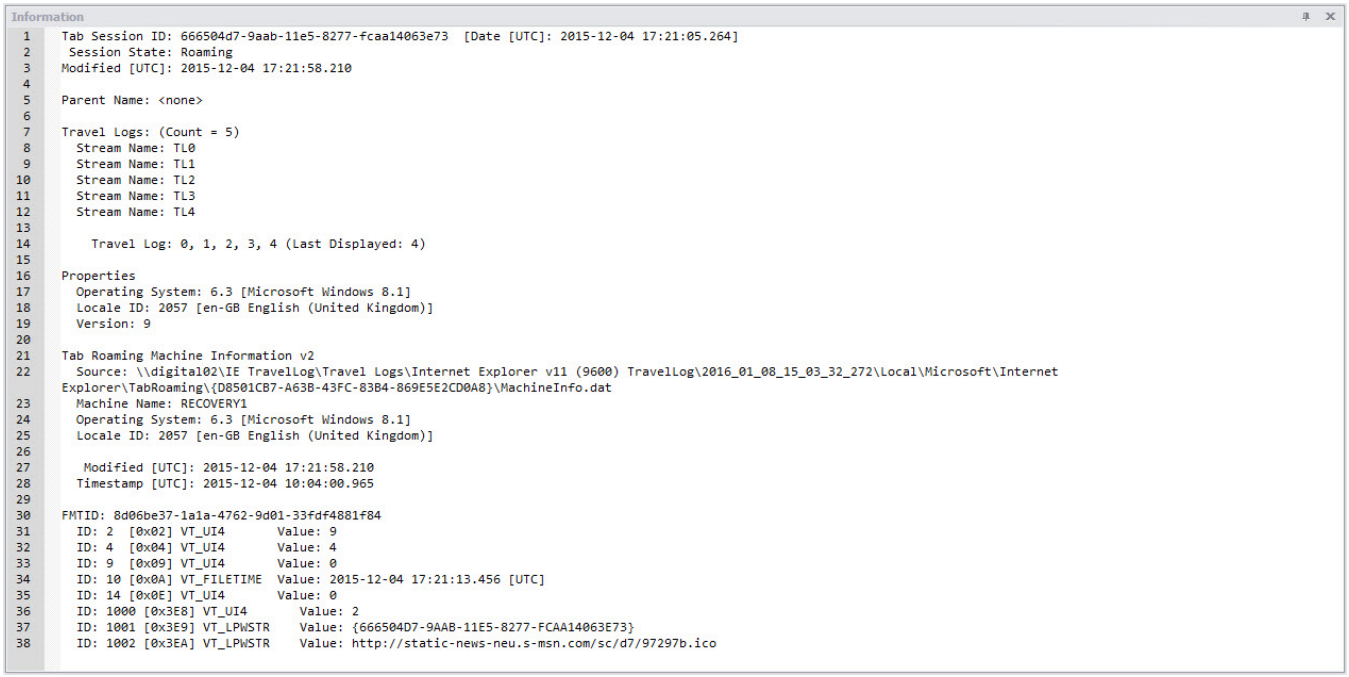


```
Information
Tab Session ID: 22a7ff1e-cc86-11e2-bee6-00301b46bd20  [Date [UTC]: 2013-06-03 19:45:25.365]
 Session State: Ordered
Modified [UTC]: 2013-06-03 19:45:26.381

Parent Name: RecoveryStore.{22A7FF1D-CC86-11E2-BEE6-00301B46BD20}
Stream Name: ORDERED_TS0

Travel Logs: (Count = 1)
  Stream Name: TL2

    Travel Log: 0, 1, 2 (Last Displayed: 2)

Properties
  Operating System: 6.2 [Microsoft Windows 8]
  Locale ID: 2057 [en-GB English (United Kingdom)]
  Version: 6

FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
  ID: 2  [0x02] VT_UI4       Value: 6
  ID: 4  [0x04] VT_UI4       Value: 2
  ID: 6  [0x06] VT_FILETIME  Value: 2013-06-03 18:44:54.749 [UTC]
  ID: 7  [0x07] VT_I4        Value: 0
  ID: 9  [0x09] VT_UI4       Value: 4
  ID: 10 [0x0A] VT_FILETIME  Value: 2013-06-03 18:44:57.452 [UTC]
  ID: 13 [0x0D] VT_UI4       Value: 1
```

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



```
Information
Tab Session ID: 79a678b2-98dc-11e5-8277-fcaa14063e73  [Date [UTC]: 2015-12-02 10:07:20.584]
 Session State: Roaming
Modified [UTC]: 2015-12-04 17:21:17.348

Parent Name: <none>

Travel Logs: (Count = 1)
  Stream Name: TL3

    Travel Log: 3 (Last Displayed: 3)

Properties
  Operating System: 6.3 [Microsoft Windows 8.1]
  Locale ID: 2057 [en-GB English (United Kingdom)]
  Version: 9

Tab Roaming Machine Information v2
  Source: \\digital02\IE TravelLog\Travel Logs\Internet Explorer v11 (9600) TravelLog\2016_01_08_15_03_32_272\Local\Microsoft\Internet
Explorer\TabRoaming\{D8501CB7-A63B-43FC-83B4-869E5E2CD0A8}\MachineInfo.dat
  Machine Name: RECOVERY1
  Operating System: 6.3 [Microsoft Windows 8.1]
  Locale ID: 2057 [en-GB English (United Kingdom)]

   Modified [UTC]: 2015-12-04 17:21:17.348
  Timestamp [UTC]: 2015-12-04 10:04:00.965

FMTID: 8d06be37-1a1a-4762-9d01-33fdf4881f84
  ID: 2  [0x02] VT_UI4       Value: 9
  ID: 4  [0x04] VT_UI4       Value: 3
  ID: 9  [0x09] VT_UI4       Value: 0
  ID: 10 [0x0A] VT_FILETIME  Value: 2015-12-04 17:20:57.785 [UTC]
  ID: 14 [0x0E] VT_UI4       Value: 0
  ID: 1000 [0x3E8] VT_UI4       Value: 2
  ID: 1001 [0x3E9] VT_LPWSTR    Value: {79A678B2-98DC-11E5-8277-FCAA14063E73}
  ID: 1002 [0x3EA] VT_LPWSTR    Value: http://www.neowin.net/images/orion/icons/favicon-196x196.png
```

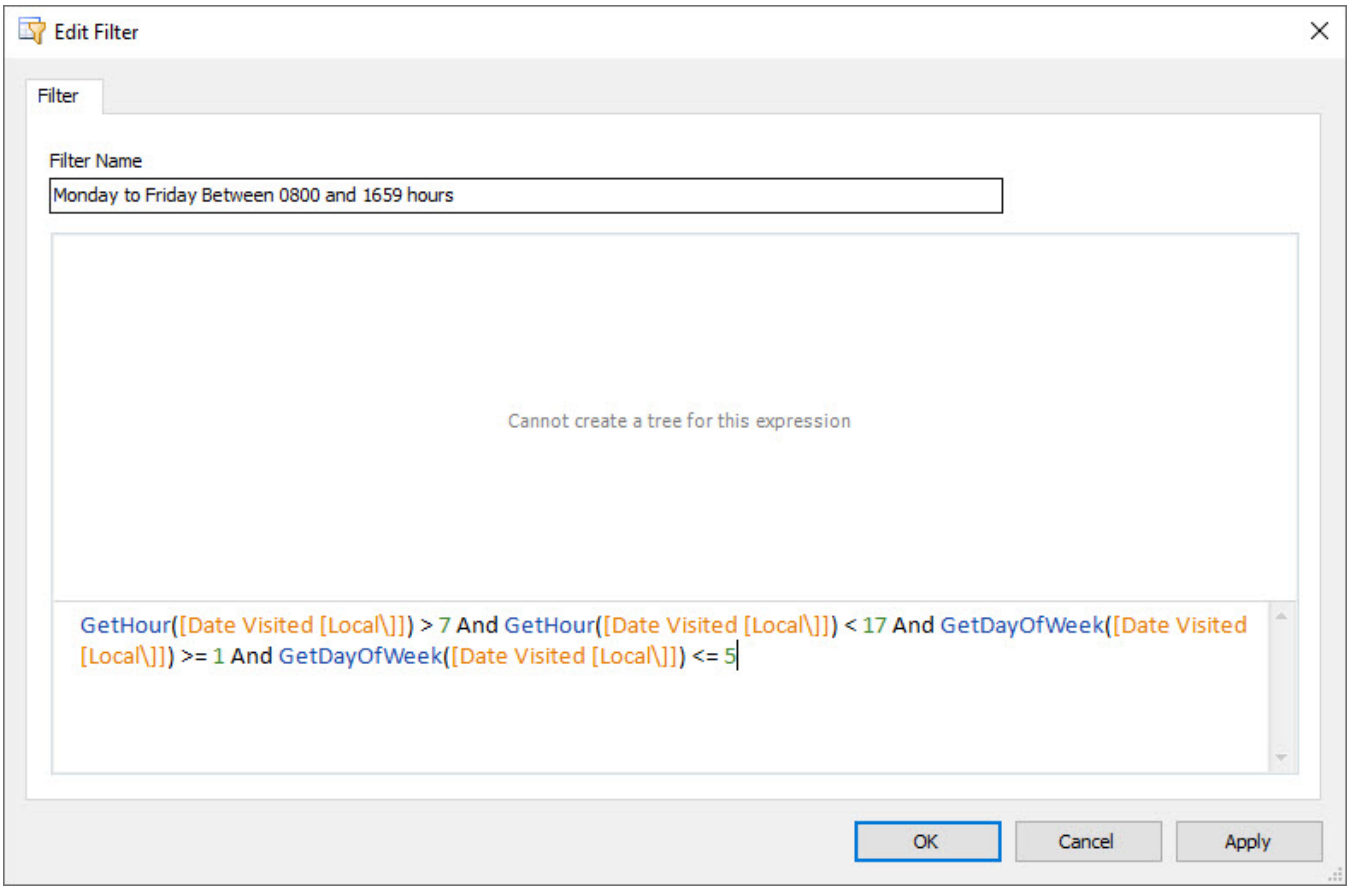


Filter Functions

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

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

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



Change Log

To review the full list of changes for this release, please see: Change Log v2.11.