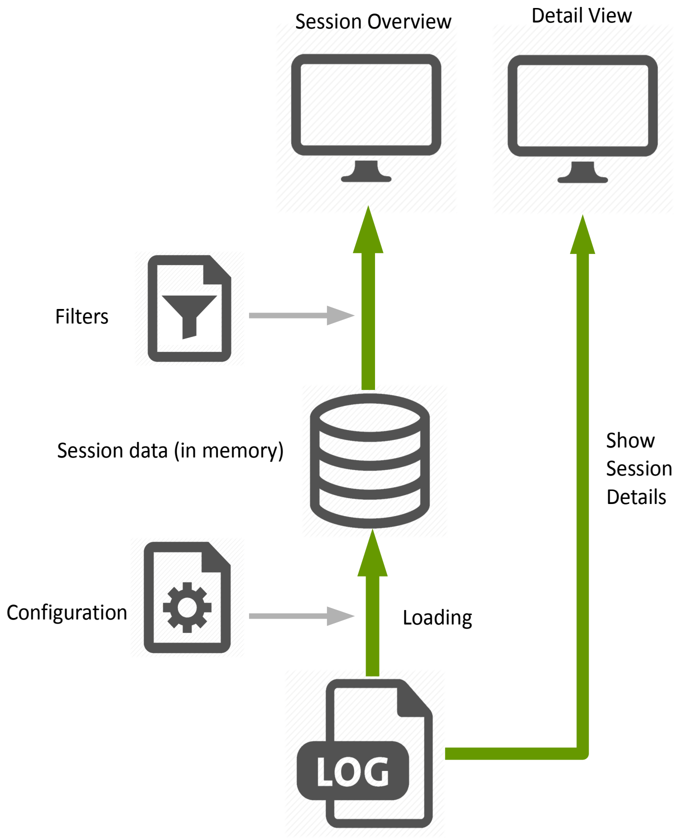
LogViewPro 3.5.5
Manual

Contents

1 How it works

Web server logfiles can get really huge and are usually difficult to handle. It's even more difficult to get useful information out of the millions of log entries. LogViewPro offers a solution to this problem. It makes it easy to open even huge logfiles and offers an interactive and visual approach to the desired information.



So this is how it works:

- Before we load the first logfile, we have to define a configuration per website. This configuration contains information about where the logfiles are stored, how to identify user sessions, what is a page etc.
  In this configuration we also can define counters for specific events.
- Using this configuration, the session data is loaded into memory
- Using filters we can select the sessions we want to display
- To display detailed information about each session, LogViewPro retrieves the data directly from the original logfile.

Like this, we get access to all the information inside the logfile very intuitively and quickly.

2 Installation

To install LogViewPro and get advantage of the full functionality, just follow these steps:

- **Run the Setup** program. The software is now already functional, but the country information for each IP and session is still missing.
- **Download an IP-to-country database**. Such can be downloaded for free here: https://db-ip.com/db/download/country
  We recommend this version, as it is still relatively small and ensures good performance.
- **Extract** the file to any location on your local hard drive.
- Start LogViewPro and go to **Tools / Import Country database**. Choose the extracted CSV file and import it

Now LogViewPro is ready to analyse your logfiles.

3 Preparing your logfiles

For better performance, we recommend to copy the web server logfiles to your local hard drive, except if the logfiles are still quite small (< 100 MB) or you have a really fast connection to the storage with throughput comparable to local hard drives.

- Create a **separate folder** for each of your websites you want to analyse.
- **Download** the log files to these folders

If you are analysing logfiles frequently, you can automate this process.

If you use a **load balancing**, usually each web server is writing its own log files. So, if you want to analyse the complete traffic, you have to merge the log files first:

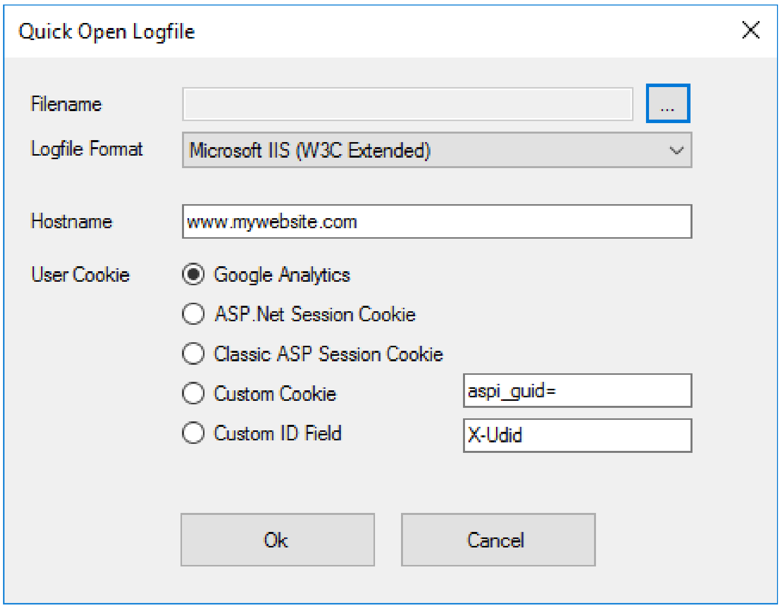
- Create **separate folders** for each server and one for the merged files
- Use the function **Tools / Merge Logfiles** to merge all the balanced server log files to a single one. Currently this function only supports IIS formats. For other formats you have to use another tool or convert the files first.

The detailed functionality of the merge function is described later.

4 Open log file

For a deeper analysis in log files, it is recommended to make a configuration as described in the next chapter. The most interesting features of LogViewPro are only available if you define your own counters and make a precise definition of the log file contents.

Anyway, if you just want to have a first look, you can use the quick open function. In the menu, go to **File / Quick Open**:



Quick Open Logfile

Filename

Logfile Format: Microsoft IIS (W3C Extended)

Hostname: www.mywebsite.com

User Cookie:
- ● Google Analytics
- ○ ASP.Net Session Cookie
- ○ Classic ASP Session Cookie
- ○ Custom Cookie: aspi_guid=
- ○ Custom ID Field: X-Udid

Here you just can make the most important settings:

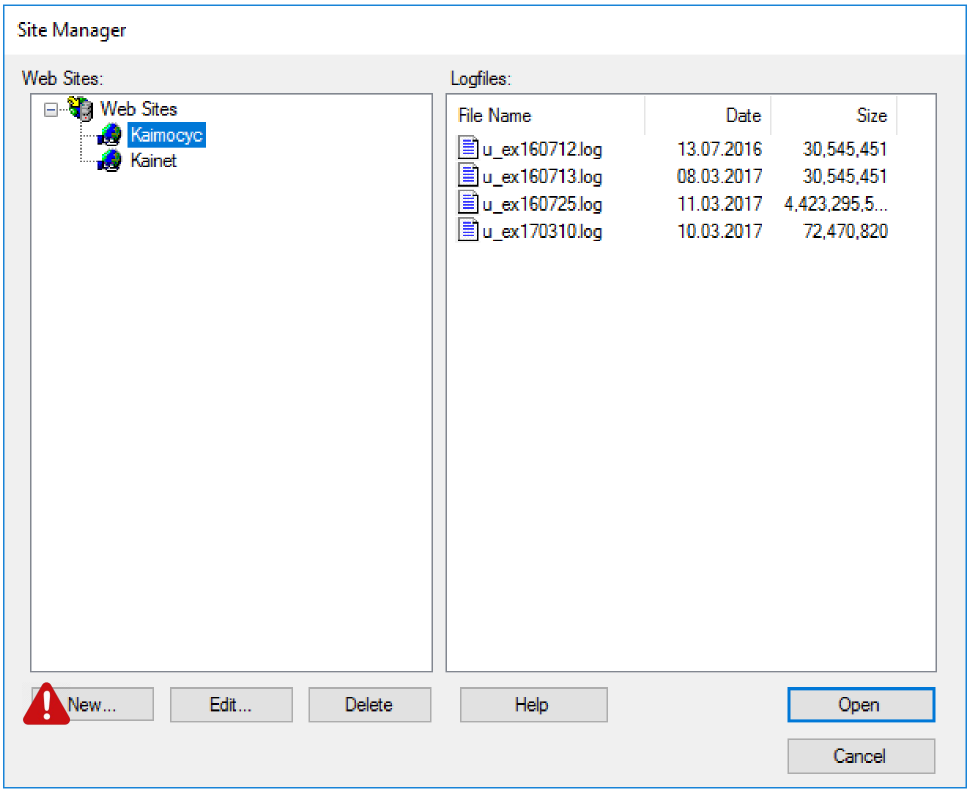
Filename	Choose the file you want to load
Logfile Format	Choose the right log file format.
Hostname	If you want the links in the request details to be click-able, enter the host name of your server here. The other functions also work without this setting.
User Cookie	To identify the user sessions more precisely, LogViewPro uses cookies, if they are logged. Choose the type of cookie which is identifying users or sessions on your server. You can use standard cookies, as written by Google Analytics, or the ASP.NET or ASP session management. The Custom ID field only works if the web server is logging the User IDs in a custom field using the Advanced Logging Module

5 Website Configuration

5.1 Adding a new website

For quick results, you can skip most of the settings and just do the most important (with ⚠). For the rest of the settings, you can leave the default values and do it later.

Before you can open a logfile, LogViewPro requires some information about the logfiles and the web server configuration. This configuration is done in the Site Manager, which you open using ⚠**File / Open Logfile**:



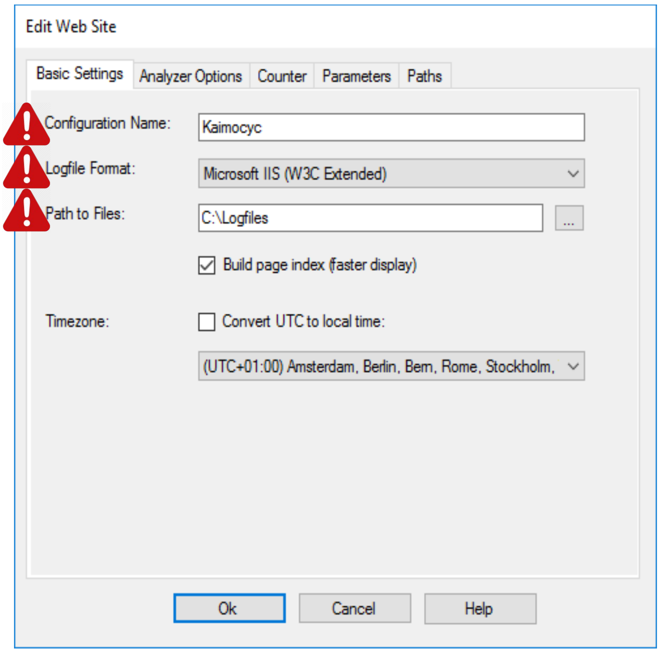
File Name	Date	Size
u_ex160712.log	13.07.2016	30,545,451
u_ex160713.log	08.03.2017	30,545,451
u_ex160725.log	11.03.2017	4,423,295,5...
u_ex170310.log	10.03.2017	72,470,820

On the left side you see the list of the websites you already have configured. Initially, this list is empty. On the right side you will see the list of all logfiles locally available.

⚠To create a new configuration, just press **New...**

5.2 Basic settings

The basic settings contain information about where the log files are stored and in which format.



⚠ Configuration Name: Kaimocyc

⚠ Logfile Format: Microsoft IIS (W3C Extended)

⚠ Path to Files: C:\Logfiles

☑ Build page index (faster display)

Timezone: ☐ Convert UTC to local time:

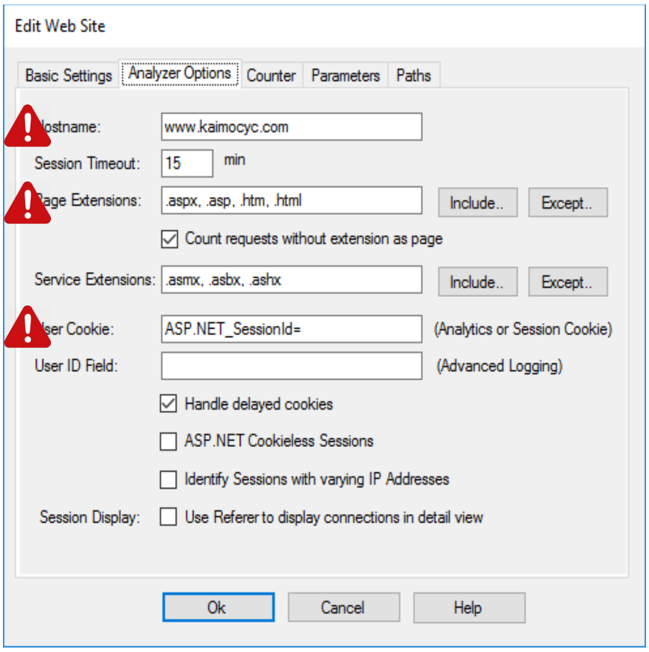
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm,

⚠ Configuration Name	Name of the configuration. Can bee chosen freely.
⚠ Logfile Format	Web server log format. Formats currently supported are: - Microsoft IIS (W3C Extended) for the Microsoft Internet Information Server - IIS Advanced Logging module - Apache Log Format - W3C Extended (Compatible) for W3C formats other than Microsoft's implementation. Parsing this format is a little bit slower
⚠ Path to files	Physical path to logfiles.
Build Page index	This option is activated by default. That way every single request will be referenced, so the access when displaying will be much faster. But reading the logfile will take more time (about 20%).
Convert UTC to local time	If your web server uses UTC for log file entries, you can select this option to convert the time codes to local time. Do not check this option, if logging in local time is enabled.
Time zone	The time zone to use when converting UTC to local time.

5.3 Analyzer Options

These settings are very important. They define:

- How user sessions are identified
- What is a page, what a service request



Edit Web Site

ostname: www.kaimocyc.com

Session Timeout: 15 min

age Extensions: .aspx, .asp, .htm, .html

☑ Count requests without extension as page

Service Extensions: .asmx, .asbx, .ashx

ser Cookie: ASP.NET_SessionId= (Analytics or Session Cookie)

User ID Field: (Advanced Logging)

☑ Handle delayed cookies

□ ASP.NET Cookieless Sessions

□ Identify Sessions with varying IP Addresses

Session Display: □ Use Referer to display connections in detail view

⚠Hostname	Host name of the web site (for example **www.company.com**). This setting is only required if the host name is not contained in the logfile, and if you want to be able to click on the links in the request information window.
Session Timeout	Requests from the same IP address with the same user agent (and optionally same Session Cookie) are counted as single session until this duration of inactivity
⚠Page extensions	Extensions of requests that are displayed on the client browser as pages. Usually it is useful to define Exceptions or Includes, as certain resources (web services, dynamic images) are generated dynamically and have the same extension as web pages.
Count Requests without Extension as Page	In certain web applications, for example **ASP.NET MVC,** or when using **URL rewriting**, requests like *http://www.mycompany.com/order* are possible. If these requests are also should be considered as web page, select this option.

Service Extensions	Web service calls, for example AJAX requests. Such requests are logged too and you can count and diyplay them. Here you can define Exceptions or Includes too. For **ASP.NET MVC** sites, web pages and service requests usually have the same url format. To correctly count and display web services, you have to do the following: ◆ Enable the option **Count Requests without extension as page** ◆ Define **Exceptions** for all service requests under **Page extensions** ◆ Define **Includes** for the same requests here
⚠User Cookie	If you are logging the cookies too, it is possible to identify and separate sessions sessions using a session or user cookie. This is useful as there are networks where every computer has the same ip address towards the internet. The session cookie depends on the technology and the application configuration. Common cookie setting are: ◆ **ASP.NET_SessionId=** for ASP.NET applications, ◆ **ASPSESSIONID** for Classic ASP (where also the second part of the cookie name, before **=** can vary. ◆ **_ga=** If you are using Google Analytics, the cookie **_ga=** can also be used for session identification.
User ID Field	When using the **Advanced Logging Module**, custom fields (or columns) can be defined. If you have defined a special column for the user or session cookie, the **column name** can be defined here. Use this option then **instead** of defining a user cookie.
Handle delayed cookies	LogViewPro identifies sessions based on the cookie, as soon as a client session contains one, usually starting at the second page. But sometimes some requests still containing no cookie are following. To map these entries to the right session, this option should be chosen.
ASP.NET cookieless sessons	With ASP.NET it is possible to run an session based application without using cookies. In this case, the session id is inserted as part of the path. This id is not logged, but it will be part of the Referer header. To display sessions correctly, this setting has to be activated when cookieless sessions are used.

Identify Sessions with varying IP addresses	There are some proxy server around (for example AOL's), which change the IP address from request to request. It is possible to merge together such sessions, but this works fine only when cookies are logged. Otherwise the result is not really perfect.
Use Referer to display connections	In the graphical session detail, the entries are connected based on the referrer of each entry. This lets you to follow the flow of the user session more easily. However, this option should only be checked, if the browser url corresponds to the logged URI. So, this option should **not** be used for **ASP.NET MVC** applications or if URL rewrite is used very often. Otherwise the session detail can be displayed incorrectly and performance could be bad.

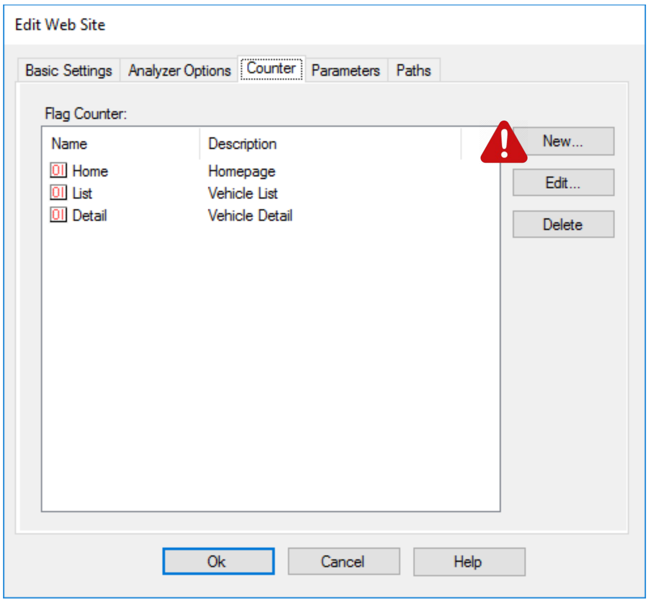
⚠ If you have done the most important settings so far, you can now open your first logfile and skip the rest of this chapter.

It's not necessary to do all the settings in the first attempt. Just do the most important settings first, then open a part of a logfile. You will find out easily, which settings still have to be done.

5.4 Counters

If you want to know, how often certain pages are requested, you can define counters. You will get a summary and you also can filter the sessions by the number of times a user requested a certain page.

For example you can count all requests for total product pages (not for specific products)

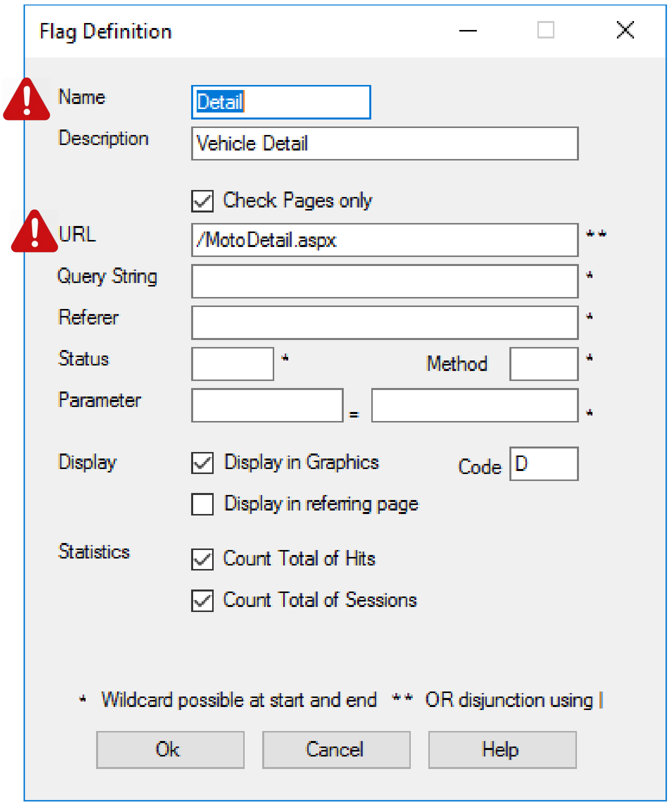


Flag Counter:

Name	Description
Home	Homepage
List	Vehicle List
Detail	Vehicle Detail

To define a new counter, just press **New**...

The flag definition contains all the criteria which have to apply for a certain log entry (request) to be counted:



Flag Definition

⚠ Name: Detail

Description: Vehicle Detail

☑ Check Pages only

⚠ URL: /MotoDetail.aspx **

Query String: *

Referer: *

Status: * Method: *

Parameter: = *

Display: ☑ Display in Graphics Code: D

☐ Display in referring page

Statistics: ☑ Count Total of Hits

☑ Count Total of Sessions

* Wildcard possible at start and end ** OR disjunction using |

Flag information:

⚠Name	Choose a name for the counter
Description	The description of the filter will be displayed in the flag list in the Edit Website window

Criteria:

Check pages only	If you check this option, during the analysis of the logfile, only pages will be checked if they match the criteria of this flag. By checking this flag you can improve the loading performance
⚠URL	Pattern for the URL, the script name
Query String	Pattern that occurs at any place of the query string
Referer	Pattern for the referer
Status	Pattern for the status code
Method	Method of the request: **GET / POST / HEAD** etc.
Parameter	Here you can define a pattern that must appear in a certain parameter. The patameter name itself must not contain any wildcards

All the criteria that are not left empty are combined using the **AND** operator.

In the search patterns, **wildcards** (*) are allowed at the beginning and the end of the expressions. Examples:

```
/MyApplication/*
*/Detail.aspx
*id=1*
20*
```

All expressions are not case sensitive.

For the URL field you can use | do combine different patterns using an OR operation. Example for a homepage:

```
/|/Default.aspx|/Home*
```

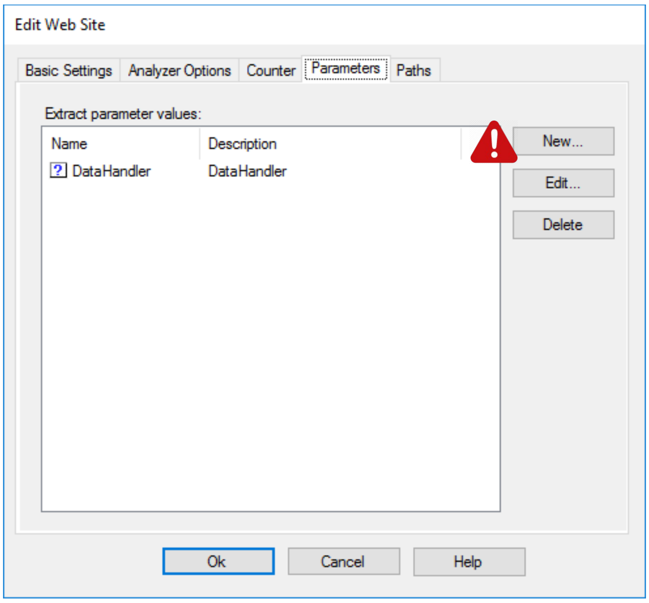
Options:

Display in Graphics	If this option is selected, a label will be displayed in the visualization of the sessions. By default, the first character of the script name will be taken. But optionally you can define your own Label, up to three characters long, by typing it into the field **Code**.
Display in referring page	If the flag matches to an image (or resource), by default an asterisk will be displayed besides the rectangle symbolizing the image. By choosing this option, the label will be displayed on the referring page.
Count total of hits	When displaying the Summary of the logfile, the total sum of occurrences in all the selected sessions will be calculated.
Count total of sessions	When displaying the Summary of the logfile, the number of sessions containing this flag will be calculated.

5.5 Parameters

If you want to know, how often certain object was requested, you can define parameter counters. You will get a summary and you also can filter the sessions by the number of times a user requested a certain object.

For example you can count all requests for a specific product



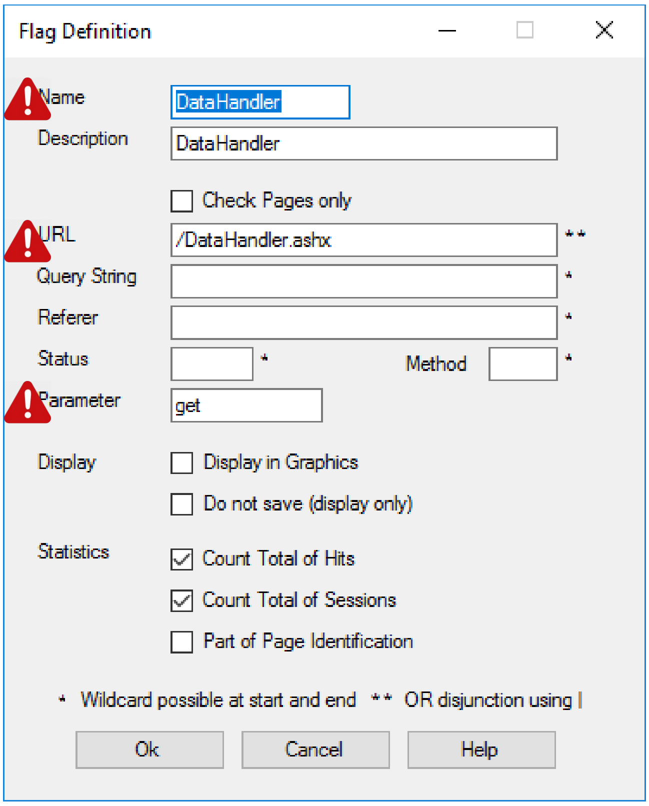
Name	Description
DataHandler	DataHandler

To define a new parameter counter, just press **New**...

Note: To use this feature, the ID of an object has to be logged as URL parameter, which is a part of the query string. With URL rewriting, this is usually no problem (at least with IIS), as not the requested URL is logged, but the rewritten one.

In future versions we will also support extracting ids from the URL path (stem).

The flag definition contains all the criteria which have to apply for a certain log entry (request) to be counted:


Flag Definition

⚠ Name: DataHandler

Description: DataHandler

□ Check Pages only

⚠ URL: /DataHandler.ashx **

Query String: *

Referer: *

Status: *   Method: *

⚠ Parameter: get

Display: □ Display in Graphics

□ Do not save (display only)

Statistics: ☑ Count Total of Hits

☑ Count Total of Sessions

□ Part of Page Identification

* Wildcard possible at start and end ** OR disjunction using |

Flag information:

⚠ Name	Choose a name for the parameter counter
Description	The description of the filter will be displayed in the flag list in the Edit Website window

Criteria:

Check pages only	If you check this option, during the analysis of the logfile, only pages will be checked if they match the criteria of this flag. By checking this flag you can improve the loading performance
⚠ URL	Pattern for the URL
Query String	Pattern that occurs at any place of the query string
Referer	Pattern for the referer
Status	Pattern for the status code
Method	Method of the request: **GET / POST / HEAD** etc.
⚠ Parameter	The name of the parameter you want to extract. Wildcards are not possible here

All the criteria that are not left empty are combined using the **AND** operator.

In the search patterns, **wildcards** (*) are allowed at the beginning and the end of the expressions. Examples:

```
/MyApplication/*
*/Detail.aspx
*id=1*
20*
```

All expressions are not case sensitive.

For the URL field you can use | do combine different patterns using an OR operation. Example for a homepage:

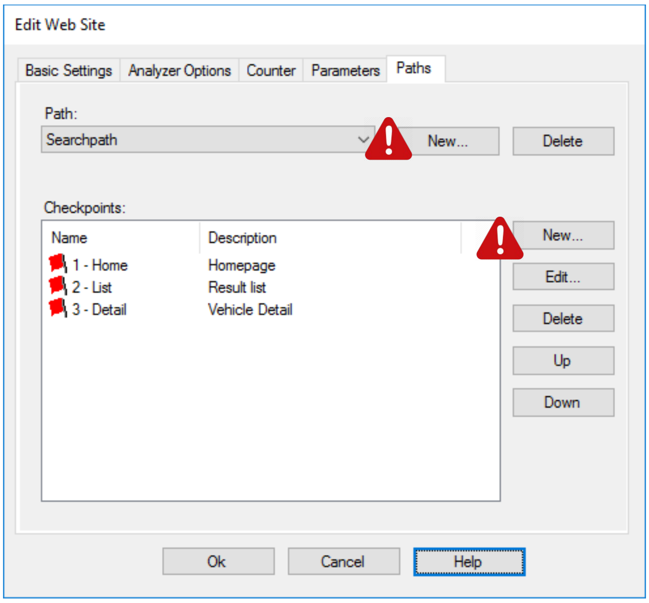
```
/|/Default.aspx|/Home*
```

Options:

Display in Graphics	Only this single parameter will be displayed in the visualization instead of the entire query string
Do not save	If you don't need the parameter for filtering purposes, you can save memory by checking this option
Count total of hits	When displaying the Summary of the logfile, the total sum of occurences of the values in all the selected sessions will be calculated. If more than 25 different values are found, just the top 25 are displayed.
Count total of sessions	When displaying the Summary of the logfile, the number of sessions containing the values will be calculated. If more than 25 different values are found, just the top 25 are displayed.
Part of page identification	In Web Statistics, the parameter is used as part of the page identificator. That means that a page like " **Page.aspx?id=.."** is counted as separate page for each id. This can be useful if you use a database based content management system and you want to know, what content pages are viewed how often.

5.6 Paths (Funnels)

If you are defining Paths (or funnels), each step has to be identified by a checkpoint. The definition of checkpoints is similar to the definition of Counters and Parameters.



To define a new counter, just press **New**... and choose a name for your path (funnel)

After this, you can define multiple checkpoints for this funnel.

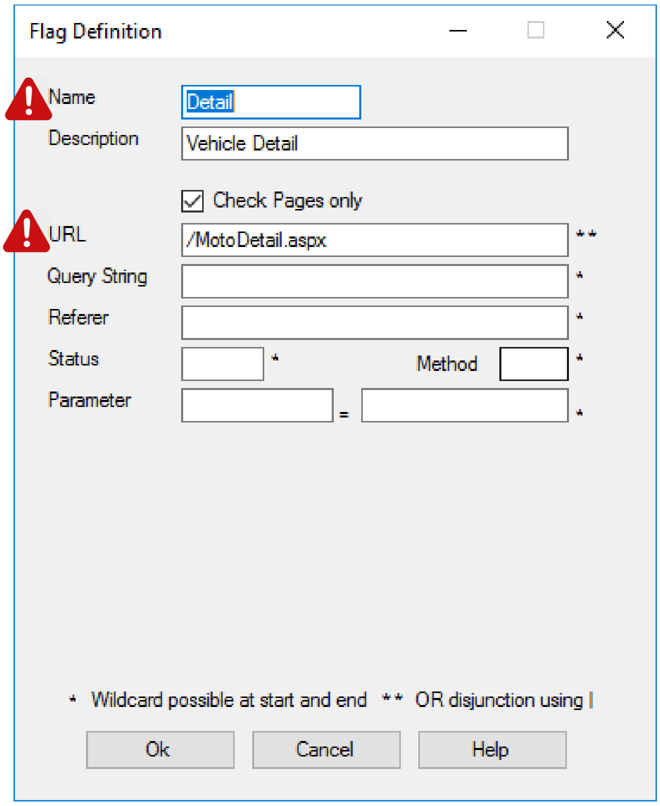
You will get the result under **Display / Path**:

```
Paths
-----

Searchpath
    2,712   100.0%          Home
    1,050    38.7%   38.7%  List
      653    24.1%   62.2%  Detail
```

You can also search for sessions which stopped at one of the checkpoints of this path.

The path definition contains all the criteria which have to apply for a certain log entry (request) to be counted as checkpoint:



Name: Detail

Description: Vehicle Detail

☑ Check Pages only

URL: /MotoDetail.aspx **

Query String: *

Referer: *

Status: * Method: *

Parameter: = *

* Wildcard possible at start and end ** OR disjunction using |

Flag information:

⚠Name	Choose a name for the counter
Description	The description of the filter will be displayed in the flag list in the Edit Website window

Criteria:

Check pages only	If you check this option, during the analysis of the logfile, only pages will be checked if they match the criteria of this flag. By checking this flag you can improve the loading performance
⚠URL	Pattern for the URL, the script name
Query String	Pattern that occurs at any place of the query string
Referer	Pattern for the referer
Status	Pattern for the status code
Method	Method of the request: **GET / POST / HEAD** etc.
Parameter	Here you can define a pattern that must appear in a certain parameter. The patameter name itself must not contain any wildcards

All the criteria that are not left empty are combined using the **AND** operator.

In the search patterns, **wildcards** (*) are allowed at the beginning and the end of the expressions. Examples:

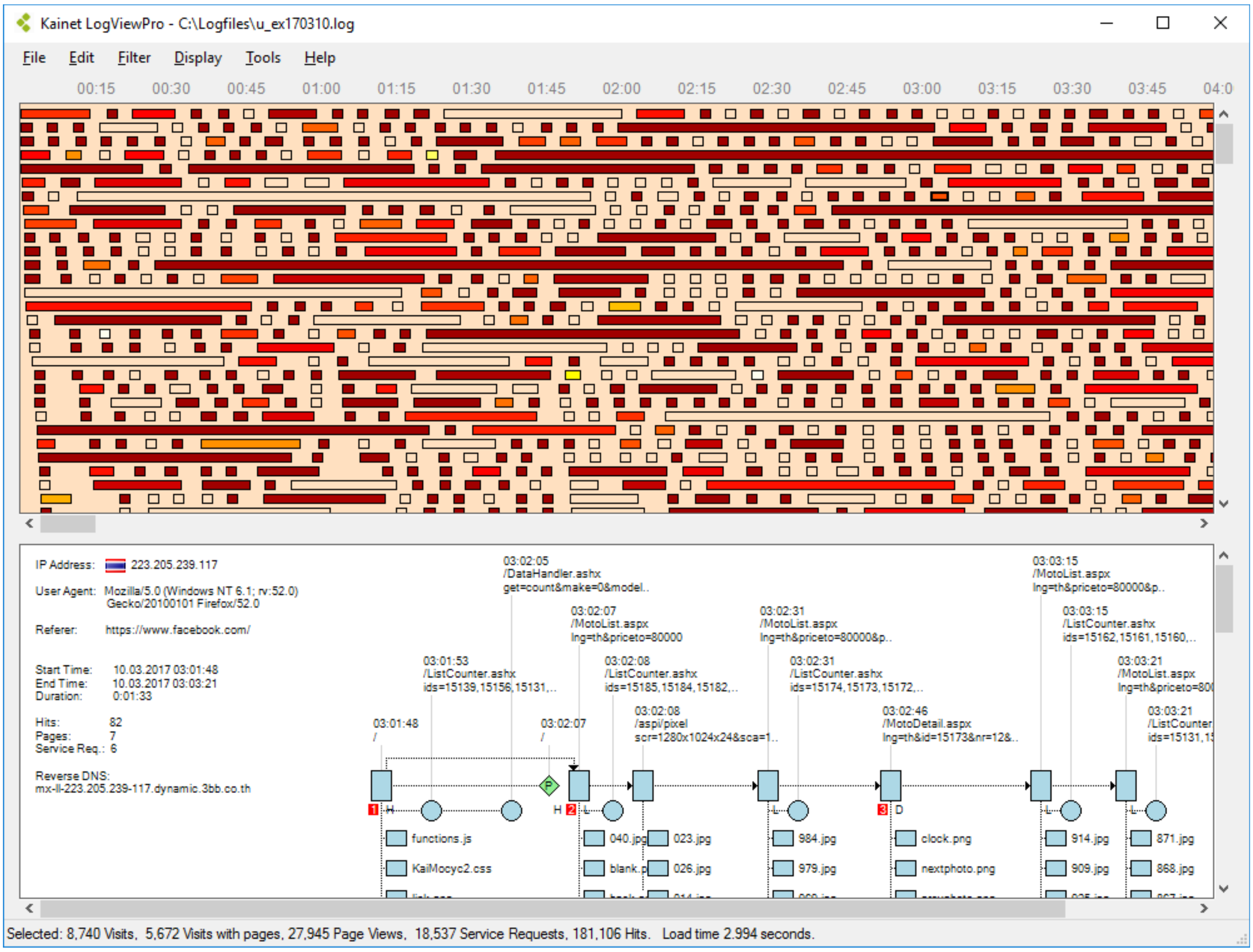
```
/MyApplication/*
*/Detail.aspx
*id=1*
20*
```

All expressions are not case sensitive.

For the URL field you can use | do combine different patterns using an OR operation. Example for a homepage:

```
/|/Default.aspx|/Home*
```

6 Main Window



IP Address: 223.205.239.117

User Agent: Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0

Referer: https://www.facebook.com/

Start Time: 10.03.2017 03:01:48
End Time: 10.03.2017 03:03:21
Duration: 0:01:33

Hits: 82
Pages: 7
Service Req.: 6

Reverse DNS:
mx-ll-223.205.239-117.dynamic.3bb.co.th

Selected: 8,740 Visits, 5,672 Visits with pages, 27,945 Page Views, 18,537 Service Requests, 181,106 Hits. Load time 2.994 seconds.

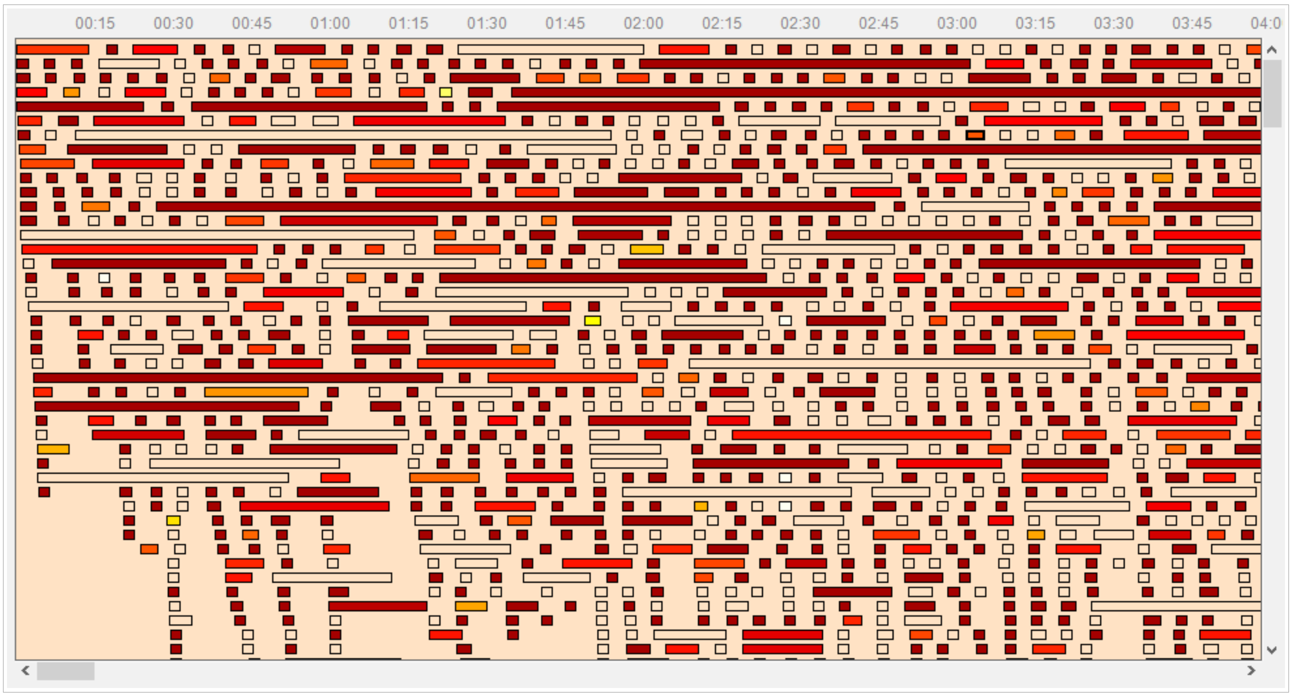
The main window is split into two views:

- The session overview where all the loaded sessions are displayed
- The session detail view where you will find the details about the currently selected session.

To select a single session, just click the bar which represents a user session

6.1 Session Overview

All the currently active sessions are rendered as clickable bars. First after loading a logfile, all the sessions in the logile are visible. Because this can be really a lot, it is useful to define a filter, so only the sessions you are interested in are displayed. For more details see Filtering.



The **colour** depends on the click speed of the session, that means the number of pages per minute. Sessions with e very high rate are displayed in white, the slowest in dark red.

You can compare the colours of the bars with the colours of hot glowing metal. The hotter, the faster.

Bars **without fill colour** represent sessions without requests identified as pages (so for example only images). It is normal that you will find a lot of these in your traffic.

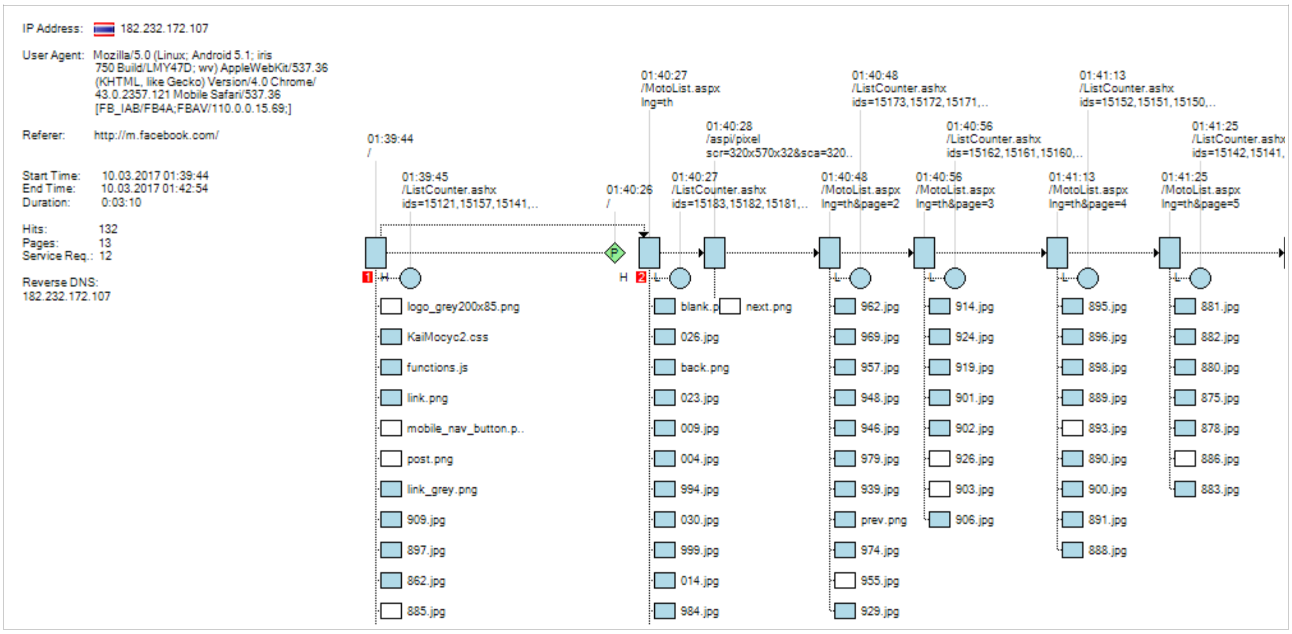
6.2 Session Detail Views

To have the details of a session displayed here, just click it in the overview. Here different types of views are possible, which you can select in the Display menu.

Using the menu Display or by clicking one of the function keys from F5 to F12, you can select the view for the session details.

6.2.1 Graphical view (F5, default)

Graphical representation of the selected session. The horizontal axis represents the time, all the pages are displayed on the same level.



IP Address: 182.232.172.107

User Agent: Mozilla/5.0 (Linux; Android 5.1; iris 750 Build/LMY47D; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/43.0.2357.121 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/110.0.0.15.69;]

Referer: http://m.facebook.com/

Start Time: 10.03.2017 01:39:44
End Time: 10.03.2017 01:42:54
Duration: 0:03:10

Hits: 132
Pages: 13
Service Req.: 12

Reverse DNS:
182.232.172.107

Symbols:

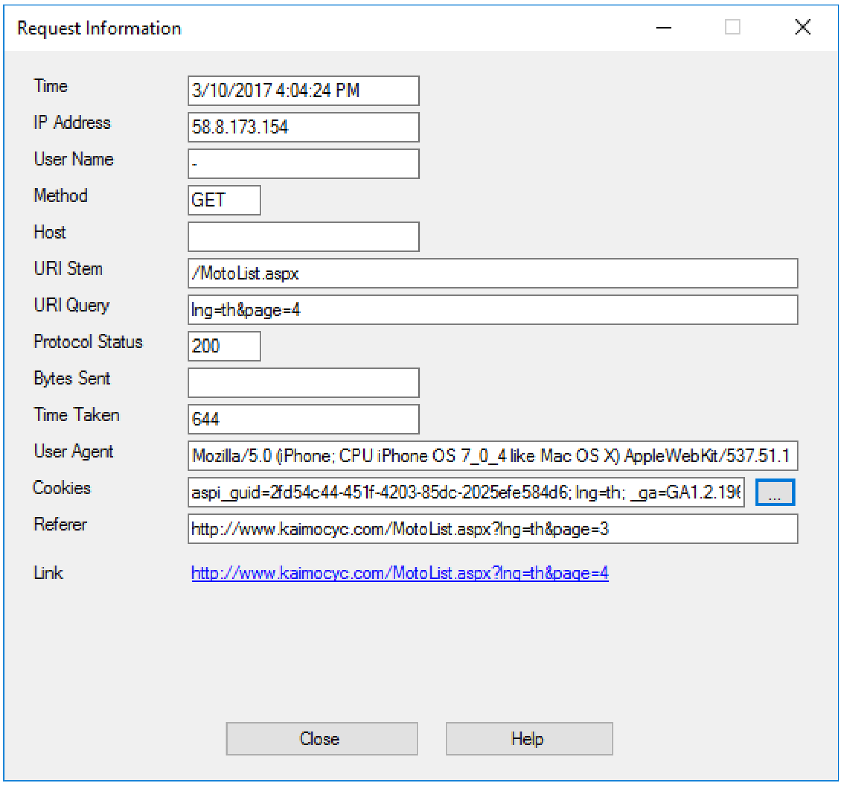
▭	Web Page
◇	Redirect (page extension requested)
○	Asynchronous request
▭	Image or other resource defined as non-script
→	Catenation identified by the referer header
⇢	Assumed Catenation, no matching referer found

Blue	Successful request
Green	Redirect
Red	Server or user error
White	Status 304 (not modified)

The Method of the request is displayed as letter inside the symbol if different from GET: P for POST, H for HEAD

6.2.2 Request details

To see the detail data of a request, just simply click onto the symbol:



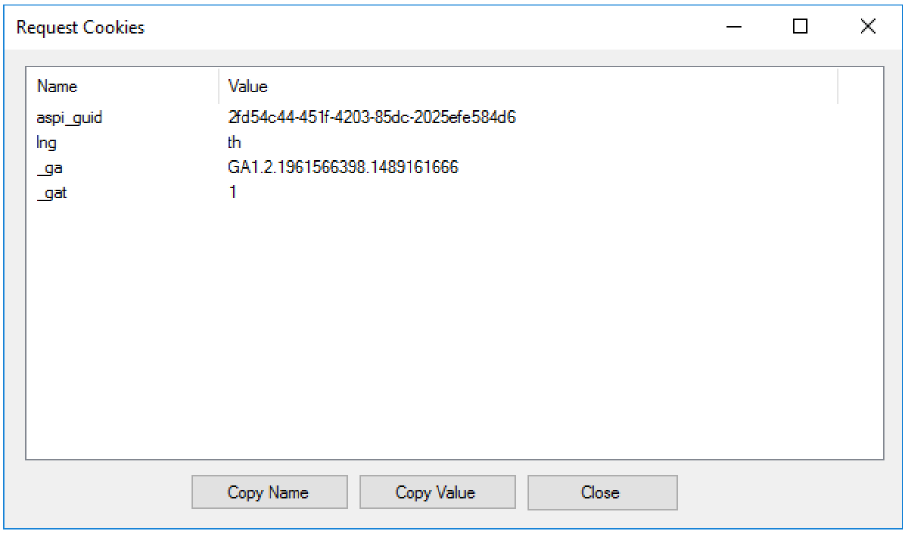
Time	3/10/2017 4:04:24 PM
IP Address	58.8.173.154
User Name	-
Method	GET
Host	
URI Stem	/MotoList.aspx
URI Query	lng=th&page=4
Protocol Status	200
Bytes Sent	
Time Taken	644
User Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 7_0_4 like Mac OS X) AppleWebKit/537.51.1
Cookies	aspi_guid=2fd54c44-451f-4203-85dc-2025efe584d6; lng=th; _ga=GA1.2.19(
Referer	http://www.kaimocyc.com/MotoList.aspx?lng=th&page=3
Link	http://www.kaimocyc.com/MotoList.aspx?lng=th&page=4

You see all the information that is logged and used by LogViewPro.

Clicking onto the link will open a browser and directly open the URL. This only works if

- The host name is logged or configured correctly
- The page is publicly accessible
- The page is accessible under the logged URL, which sometimes is not the case when using URL rewriting

Clicking onto the button between cookies displays a list of all cookies sent with that request:



Request Cookies

Name	Value
aspi_guid	2fd54c44-451f-4203-85dc-2025efe584d6
lng	th
_ga	GA1.2.1961566398.1489161666
_gat	1

You can copy the name or the value of the cookie.

6.2.3 General information (F6)

All the collected information about the session, including IP Address, User Agent, Entry Page, Start Time, End Time, Duration, Hits, Pages, Referrer of the first page (if available). The IP Address will be resolved to a host name if possible.

```
Session 557
    IP Address:     171.99.47.86  TH
    User Agent:     Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X)
      AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/56.0.2924.79 Mobile/14D27
      Safari/602.1
    Entry Page:     /
    Start Time:     10.03.2017 01:55:03
    End Time:       10.03.2017 01:59:06
    Duration:       0:4:3
    Hits:           153
    Pages:          15
    Service Req.:   22
    Referer:        https://www.google.co.th/

Reverse DNS Lookup:
    Hostname:       wf-171-99-47-86.revip9.asianet.co.th

Flag Counter:
    Home:           2
    List:           10
    Detail:         3

DataHandler:
    count           2

Paths:
    Searchpath:     completed.
```

All the flag counters and collected parameters are listed.

6.2.4 Pages (F7)

All the pages of the session are listed.

```
Session 557
    IP Address:     171.99.47.86  TH
    User Agent:     Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X)
      AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/56.0.2924.79 Mobile/14D27
      Safari/602.1
    Referer:        https://www.google.co.th/

10.03.2017 01:55:03       /
10.03.2017 01:55:15 P --> /
10.03.2017 01:55:15       /MotoList.aspx?lng=th&ccmfrom=230
```

```
10.03.2017 01:55:16       /aspi/pixel?scr=375x667x32&sca=375x667&win=375x591
10.03.2017 01:55:22       /MotoList.aspx?lng=th&ccmfrom=230&page=2
10.03.2017 01:55:29       /MotoList.aspx?lng=th&ccmfrom=230&page=3
10.03.2017 01:55:37       /MotoDetail.aspx?lng=th&id=15026&nr=21&tot=3
10.03.2017 01:56:54       /MotoList.aspx?lng=th&ccmfrom=230&page=4
10.03.2017 01:57:01       /MotoDetail.aspx?lng=th&id=15008&nr=34&tot=328
10.03.2017 01:57:57       /MotoList.aspx?lng=th&ccmfrom=230&page=5
10.03.2017 01:58:05       /MotoList.aspx?lng=th&ccmfrom=230&page=6
10.03.2017 01:58:11       /MotoList.aspx?lng=th&ccmfrom=230&page=7
10.03.2017 01:58:16       /MotoList.aspx?lng=th&ccmfrom=230&page=8
10.03.2017 01:58:22       /MotoList.aspx?lng=th&ccmfrom=230&page=9
10.03.2017 01:58:30       /MotoDetail.aspx?lng=th&id=14383&nr=9
10.03.2017 01:59:06       /MotoList.aspx?lng=th&ccmfrom=230
```

-->	Redirect
P	Post

6.2.5 Pages and Hits (F8)

All the pages and images of the session are listed:

```
Session 557
    IP Address:     171.99.47.86  TH
    User Agent:     Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X)
      AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/56.0.2924.79 Mobile/14D27
      Safari/602.1
    Referer:        https://www.google.co.th/

10.03.2017 01:55:03       /
                          /Photos/Small/0058/851.jpg
10.03.2017 01:55:03    A  /ListCounter.ashx?ids=15125,15167,15111
                          /Photos/Small/0058/866.jpg
                          /Photos/Small/0058/948.jpg
                          /Photos/Small/0058/886.jpg
                          /Photos/Small/0058/880.jpg
                       .  /Images/post.png
                       .  /Images/link.png
                       .  /Images/link_grey.png
                          /Photos/Small/0058/878.jpg
                       .  /Images/address.png
                       .  /Images/selector.png
10.03.2017 01:55:15    A  /DataHandler.ashx?get=count&make=0&model=0
10.03.2017 01:55:15 P --> /
10.03.2017 01:55:15       /MotoList.aspx?lng=th&ccmfrom=230
10.03.2017 01:55:15    A  /ListCounter.ashx?ids=15183,15174,15169,15159
                          /Photos/Small/0058/984.jpg
                          /Photos/Small/0059/030.jpg
                          /Photos/Small/0058/957.jpg
                       .  /Images/blank.png
                          /Photos/Small/0058/919.jpg
                          /Photos/Small/0058/897.jpg
                          /Photos/Small/0058/891.jpg
                          /Photos/Small/0058/847.jpg
```

6.2.6 WHOIS (F9)

A WHOIS query is performed. The WHOIS servers defined under **File /Settings** are queried one by one until a useful result is returned:

```
Session 557
    IP Address:     171.99.47.86
    User Agent:     Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X)
    Referer:        https://www.google.co.th/

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '171.99.0.0 - 171.99.127.255'

inetnum:        171.99.0.0 - 171.99.127.255
netname:        TRUENET-WIFI
descr:          TRUE INTERNET CO.LTD.
country:        TH
admin-c:        TIA6-AP
tech-c:         TIA6-AP
status:         ASSIGNED NON-PORTABLE
remarks:        Abusing network please contact : ipadmin@trueinternet.co.th
mnt-by:         MAINT-AP-TRUEINTERNET
mnt-irt:        IRT-TRUEINTERNET-TH
mnt-lower:      MAINT-AP-TRUEINTERNET
mnt-routes:     MAINT-AP-TRUEINTERNET
changed:        ipadmin@trueinternet.co.th 20120111
source:         APNIC

irt:            IRT-TRUEINTERNET-TH
address:        14th,27 th, floor ,Fortune Town
address:        1 Ratchadaphisek Road, Din Daeng
address:        Bangkok 10400
e-mail:         abuse@trueinternet.co.th
abuse-mailbox:  abuse@trueinternet.co.th
admin-c:        TIA6-AP
tech-c:         TIA6-AP
auth:           # Filtered
mnt-by:         MAINT-AP-TRUEINTERNET
changed:        abuse@trueinternet.co.th 20101108
source:         APNIC


% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r0
(UNDEFINED)
```

6.2.7 Traceroute (F10)

LogViewPro contains a traceroute function which is much faster than the command line version shipped with Windows, but still can take a few seconds

The IP address of the selected session is traced. Additionally, if the country database is installed, the country for each hop is displayed.

```
   IP Address:     171.99.47.86   TH
   User Agent:     Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X)
   Referer:        https://www.google.co.th/

 1   13 ms  ZZ 192.168.1.1
 2  123 ms  ZZ 10.121.47.241
 3   31 ms  ZZ 10.121.47.242
 4   35 ms  ZZ 10.33.34.237
 5   41 ms  ZZ 10.254.254.35
 6   43 ms  ZZ 10.254.254.28
 7   46 ms  ZZ 10.254.253.26
 8   54 ms  ZZ 10.255.255.196
 9   38 ms  TH mx-ll-110.164.0-138.static.3bb.co.th [110.164.0.138]
10   41 ms  TH 218.100.66.41
11   36 ms  TH TIG-Net31-213.trueintergateway.com [122.144.31.213]
12   40 ms  TH TIG-Net30-220.trueintergateway.com [122.144.30.220]
13   50 ms  TH 122.144.30.234
14   38 ms  TH ppp-171-102-254-129.revip18.asianet.co.th [171.102.254.129]
15   54 ms  TH 203-144-128-50.static.asianet.co.th [203.144.128.50]
16   43 ms  TH ppp-171-102-254-68.revip18.asianet.co.th [171.102.254.68]
17   38 ms  TH 119-46-42-74.static.asianet.co.th [119.46.42.74]
18   *         Timed out
19   *         Timed out
```

6.2.8 Logfile Details (F12)

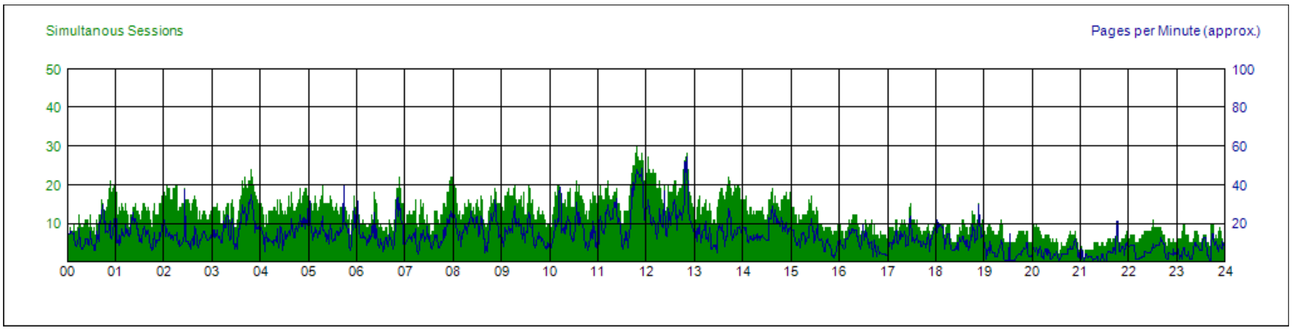
The original Logfile data lines for the current session are listed.

6.3 Global views

These views don't depend on a single session, but on the complete and filtered - data.

6.3.1 Day statistics (F1)

he traffic of the entire day (only of the selected sessions) is visualized. Note: The indicator for pages per minutes is only approximated.



6.3.2 Summary (F2)

Display summary of counters over all the selected sessions.

```
Total
-----
   Hits:                        153330
   Pages:                        23431
   Service Requests:             16937
   Sessions:                      1563

Hit Counter
-----------
   Home                3718    15.9%     Homepage
   List               10822    46.2%     Vehicle List
   Detail              7329    31.3%     Vehicle Detail

Session Counter
---------------
   Home                1095    70.1%     Homepage
   List                1392    89.1%     Vehicle List
   Detail              1080    69.1%     Vehicle Detail

Parameter Hit Counter
---------------------
DataHandler (DataHandler)
   count               3343
   models               940
   userok                43
```

6.3.3 Paths (F3)

Display summary of the paths (funnels) over all the loaded sessions.

```
Paths
-----

Searchpath
    1,279   100.0%          Home
    1,014    79.3%   79.3%  List
      653    51.1%   64.4%  Detail
```

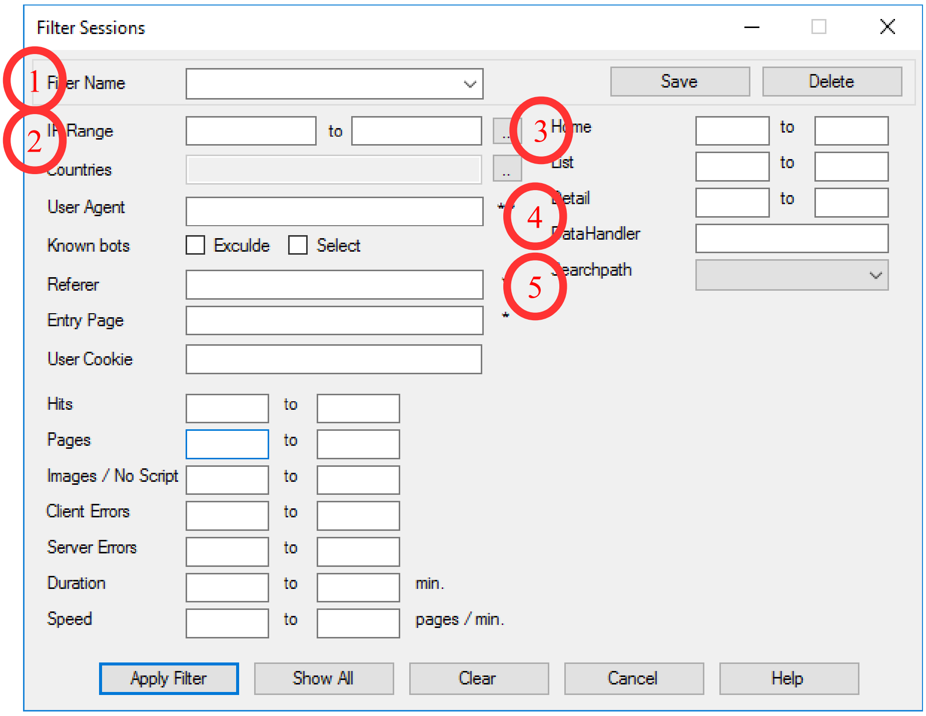
7 Filtering

Web server logfiles can grow very big and contain thousands, or even millions of visitor sessions. So the concept of filtering is getting very important. You can limit the sessions which are displayed on the main window according to criteria you define.

So it will be easy to find and select the certain visitors you are searching among the big mass of visitors. For example special groups of users, spiders, hackers or attackers or even one special single user.

7.1 The main filter form

The filters are defined in the filter window, you get there by klicking **Filter / Filter visits..** or just **Ctrl+F.**



Here you can directly define and apply a filter.

You also can optionally save a filter under a name you choose. The saved filters will be available directly in the main menu.

Saving and Loading (1)

Filter name	Assign a filter name to your filter. It will appear under this name in the Filter Menu. In the dropdown menu you can choose filter definitions you have made before.
Save	Save the current filter definition under the name you chose. The filters are saved per configuration.
Delete	Delete the selected filter. It will also be removed from the Filter Menu

Fixed filter criteria (2)

IP Range	Select an IP address or range. You can enter it directly or use the IP range selector tool (see below)
Countries	List of countries which should be selected. You can select the countries by picking them using the country selector tool (see below). Note: This function only works when a country database has been imported. To do this, use the Country Database Import tool.
User Agent	User agent. Wildcards (asterisk *) at the beginning and the end of the expression are allowed
Known Bots	Include or exclude known bots based on their user agent. The list of patterns used for filtering is defined under **Settings** Note: Evil spiders can easily fake their user agent. So you cannot rely on this function when searching for unwanted bots.
Referer	Referer of the session. The referer is captured together with the first web page in the session. Wildcards are allowed.
Entry Page	First page of the session. Wildcards allowed.
User Cookie	Filter the sessions by their user cookie. This can be useful to track a user. Of course this option only works when using permanent cookies (like Google Analytics), and the session cookie is configured in the current website configuration.
Hits	Range of Number of hits (includes all kinds of requests) **For all range selectors:** To select sessions with no matches, write **0** into the **to-**field. For sessions with at least one match, write **1** into the **from-**field.
Pages	Range of Number of pages (identified by the script endings as defined, without the exceptions)
Images / No Script	Range of Number of all hits that are **not** pages or services

Client Errors	Range of Number of client errors (Status 4xx)
Server Errors	Range of Number of server errors (Status 5xx)
Duration	Range of Duration of the session, time between first and last request
Speed (pages / min)	Range of Click speed in the session.

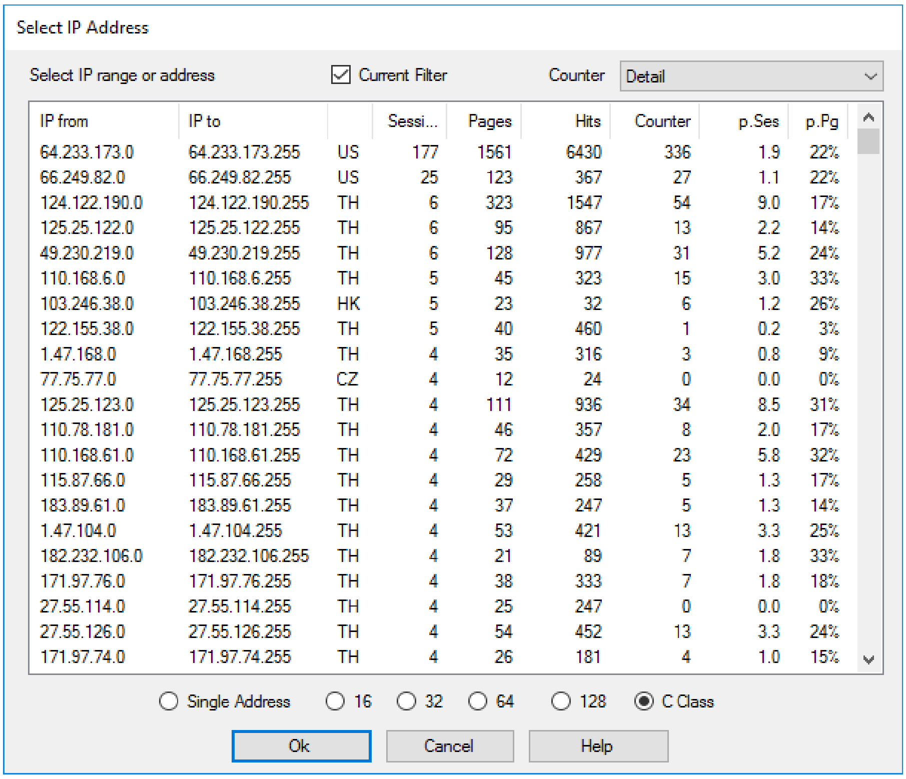
Dynamic filter criteria

Counter (3)	You can filter the sessions by the number of occurrences of flag counters you have defined in the website configuration
Parameters(4)	If you have captured parameter values in the website configuration, you can select the values here. This is probably one of the strongest features of the entire application. It allows you to find visitors who have requested specific items.
Paths / Funnels(5)	You can search for users who stopped the visit at a certain point of the funnel process

7.2 IP selector tool

In this window you see all the IP addresses or ranges of your visitors listed by Sessions, Pages, Hits or Counter counts. Just click the column header to change the sort order.

This tool is very useful if you are searching for abnormal traffic coming from single IP addresses or whole C-Classes.



Select IP Address

Select IP range or address ☑ Current Filter Counter Detail

IP from	IP to		Sessi...	Pages	Hits	Counter	p.Ses	p.Pg
64.233.173.0	64.233.173.255	US	177	1561	6430	336	1.9	22%
66.249.82.0	66.249.82.255	US	25	123	367	27	1.1	22%
124.122.190.0	124.122.190.255	TH	6	323	1547	54	9.0	17%
125.25.122.0	125.25.122.255	TH	6	95	867	13	2.2	14%
49.230.219.0	49.230.219.255	TH	6	128	977	31	5.2	24%
110.168.6.0	110.168.6.255	TH	5	45	323	15	3.0	33%
103.246.38.0	103.246.38.255	HK	5	23	32	6	1.2	26%
122.155.38.0	122.155.38.255	TH	5	40	460	1	0.2	3%
1.47.168.0	1.47.168.255	TH	4	35	316	3	0.8	9%
77.75.77.0	77.75.77.255	CZ	4	12	24	0	0.0	0%
125.25.123.0	125.25.123.255	TH	4	111	936	34	8.5	31%
110.78.181.0	110.78.181.255	TH	4	46	357	8	2.0	17%
110.168.61.0	110.168.61.255	TH	4	72	429	23	5.8	32%
115.87.66.0	115.87.66.255	TH	4	29	258	5	1.3	17%
183.89.61.0	183.89.61.255	TH	4	37	247	5	1.3	14%
1.47.104.0	1.47.104.255	TH	4	53	421	13	3.3	25%
182.232.106.0	182.232.106.255	TH	4	21	89	7	1.8	33%
171.97.76.0	171.97.76.255	TH	4	38	333	7	1.8	18%
27.55.114.0	27.55.114.255	TH	4	25	247	0	0.0	0%
27.55.126.0	27.55.126.255	TH	4	54	452	13	3.3	24%
171.97.74.0	171.97.74.255	TH	4	26	181	4	1.0	15%

○ Single Address ○ 16 ○ 32 ○ 64 ○ 128 ● C Class

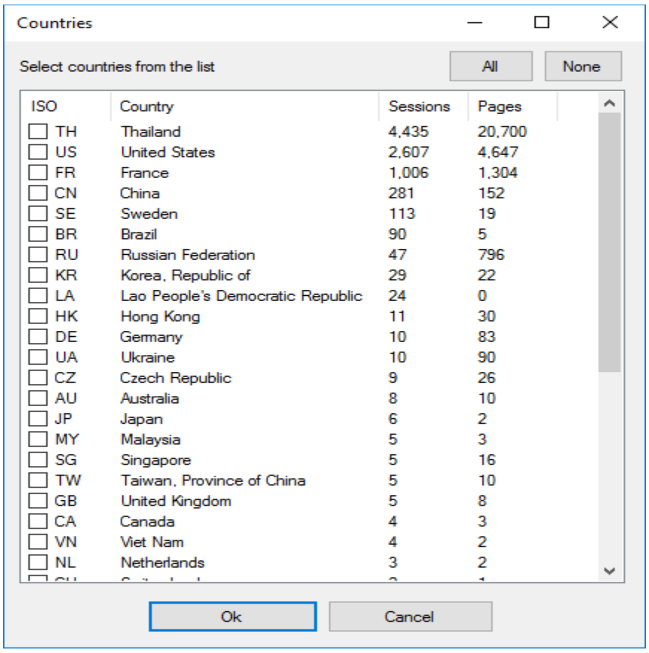
Options

Current Filter	If this option is checked, the current filter (except IP address/range) is applied before filling the data table. The columns will only countain the totals within the current result set. IP addresses which are not included in the current filter will not be displayed.
Counter	If you have defined Flag Counters, then you can choose one for display and sort in the data table.
Range size	You can change the IP range size by choosing it below ◆ Single IP Address ◆ 16 Addresses (subnet mask 255.255.255.240) ◆ 32 Addresses (subnet mask 255.255.255.224) ◆ 64 Addresses (subnet mask 255.255.255.192) ◆ 128 Addresses (subnet mask 255.255.255.128) ◆ Entire C-Class, 256 Addresses (subnet mask 255.255.255.0)

Displayed columns	
IP From	Start address of the range.
IP To	End address of the range
Country	Country of the IP range/address. If the range contains Addresses of different countries, only ** is displayed. Only works, if a country database is installed.
Sessions (sortable)	Number of sessions coming from that range
Pages (sortable)	Number of pages coming from that range
Hits (sortable)	Total number of requests coming from that range
Counter (sortable)	Number of Flag Counter occurrences from that range
p.Ses	Average number of occurrences of Flag counters per session.
p.Pg.	Avarage number of occurences of Flag Counters in relation to the total number of pages (in percent)

7.3 Country selector tool

With this tool you can select one or more countries from a list:



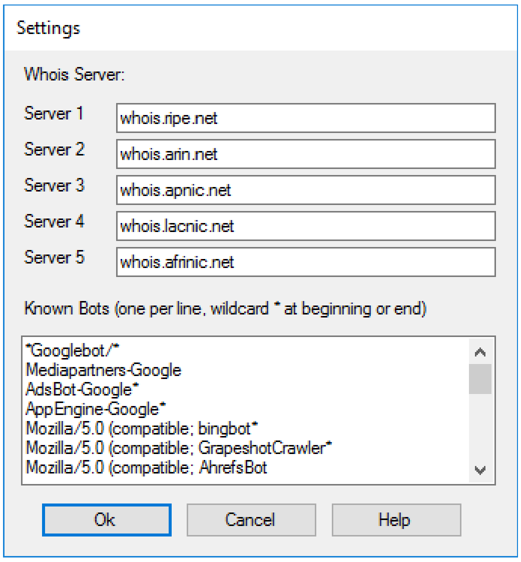
Select countries from the list

ISO	Country	Sessions	Pages
□ TH	Thailand	4,435	20,700
□ US	United States	2,607	4,647
□ FR	France	1,006	1,304
□ CN	China	281	152
□ SE	Sweden	113	19
□ BR	Brazil	90	5
□ RU	Russian Federation	47	796
□ KR	Korea, Republic of	29	22
□ LA	Lao People's Democratic Republic	24	0
□ HK	Hong Kong	11	30
□ DE	Germany	10	83
□ UA	Ukraine	10	90
□ CZ	Czech Republic	9	26
□ AU	Australia	8	10
□ JP	Japan	6	2
□ MY	Malaysia	5	3
□ SG	Singapore	5	16
□ TW	Taiwan, Province of China	5	10
□ GB	United Kingdom	5	8
□ CA	Canada	4	3
□ VN	Viet Nam	4	2
□ NL	Netherlands	3	2

The country list can be sorted by Country Code, Country, Number of Sessions, Number of Pages by clicking on the column header. The numbers are always the total of all sessions, independent of other search criteria.

8 Application settings

These settings are application wide for all website configurations and are applied immediately:



Settings

Whois Server:

Server 1 whois.ripe.net
Server 2 whois.arin.net
Server 3 whois.apnic.net
Server 4 whois.lacnic.net
Server 5 whois.afrinic.net

Known Bots (one per line, wildcard * at beginning or end)

```
*Googlebot/*
Mediapartners-Google
AdsBot-Google*
AppEngine-Google*
Mozilla/5.0 (compatible; bingbot*
Mozilla/5.0 (compatible; GrapeshotCrawler*
Mozilla/5.0 (compatible; AhrefsBot
```

Whois servers

Here you can define up to five WHOIS servers. These servers will be queried when the WHOIS view is selected. One by one is queried, until the IP address could be resolved

Known Bots

This list contains user agent patterns for known bots, such as search engines. When filtering sessions, you can select or exclude these known bots from the set of selected sessions based on these patterns.

The default configuration contains the following know bots:

```
*Googlebot/*
Mediapartners-Google
AdsBot-Google*
AppEngine-Google*
Mozilla/5.0 (compatible; bingbot*
Mozilla/5.0 (compatible; GrapeshotCrawler*
Mozilla/5.0 (compatible; AhrefsBot
Mozilla/5.0 (compatible; Baiduspider*
Mozilla/5.0 (compatible; bingbot*
Mozilla/5.0 (compatible; YandexBot*
Mozilla/5.0 (compatible; Yahoo*
Mozilla/5.0 (compatible; AhrefsBot*
Mozilla/5.0 (compatible; MJ12bot*
Mozilla/5.0 (compatible; proximic*
Mozilla/5.0 (compatible; DotBot*
Mozilla/5.0 (compatible; BLEXBot*
ia_archiver
msnbot*
Pingdom*
rogerbot*
Nutch*
```

Notes:

- This list is not complete. You can extend it depending on the bots which are crawling your website, and which bots you consider as “good”
- When filtering the traffic based on this list, you might also exclude “bad” robots, as these sometimes use a fake user agent of well-known search engines, such as google.
- Entering too many patterns can slow down the function of applying filters. Especially patterns with two wildcards (at beginning AND end, like *google*) can cause more load for the CPU.

9 Tools

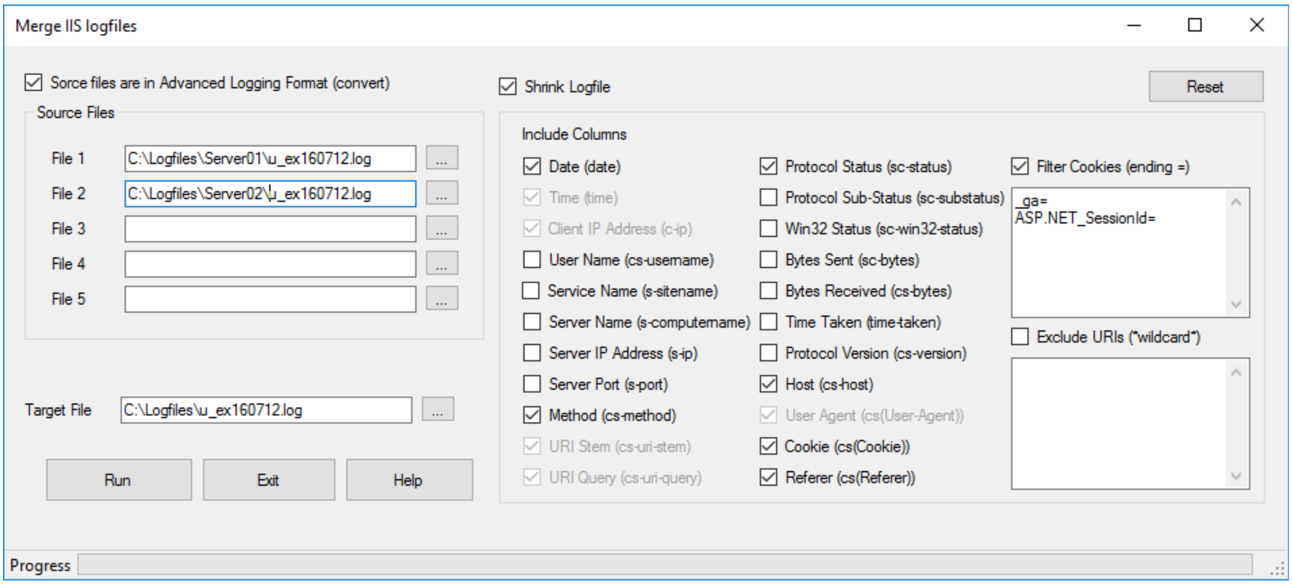
9.1 Merge / Shrink logfiles

As LogViewPro can only work with a single logfile, we have a problem when load balancing is used. Using this tool you can merge several web server logfiles in IIS format or Advanced Logging format into a single one. The output will always be in standard IIS format.

This function reads all the files in parallel and creates a new logfile containing the common columns that are contained in all source files. The entries in the resulting logfile will be in correct chronological order.

Additionally you can also shrink a log file, that means you can exclude certain columns, cookies, or lines containing specific uri paths. This is helpful when your logfiles are really huge (> 10GB). So you can reduce the files to the data needed for your analysis.

This function can also be used for a single logfile if you just want to shrink a file.



Merge IIS logfiles

☑ Sorce files are in Advanced Logging Format (convert)

Source Files

File 1 C:\Logfiles\Server01\u_ex160712.log
File 2 C:\Logfiles\Server02\u_ex160712.log
File 3
File 4
File 5

Target File C:\Logfiles\u_ex160712.log

☑ Shrink Logfile

Include Columns

☑ Date (date)
☑ Time (time)
☑ Client IP Address (c-ip)
□ User Name (cs-username)
□ Service Name (s-sitename)
□ Server Name (s-computername)
□ Server IP Address (s-ip)
□ Server Port (s-port)
☑ Method (cs-method)
☑ URI Stem (cs-uri-stem)
☑ URI Query (cs-uri-query)
☑ Protocol Status (sc-status)
□ Protocol Sub-Status (sc-substatus)
□ Win32 Status (sc-win32-status)
□ Bytes Sent (sc-bytes)
□ Bytes Received (cs-bytes)
□ Time Taken (time-taken)
□ Protocol Version (cs-version)
☑ Host (cs-host)
☑ User Agent (cs(User-Agent))
☑ Cookie (cs(Cookie))
☑ Referer (cs(Referer))

☑ Filter Cookies (ending =)

_ga=
ASP.NET_SessionId=

□ Exclude URIs (*wildcard*)

Options

Source files are in advanced Logging format	If the logfile(s) had been written using the Advanced Logging module, this option has to be checked. The output file will be in standard IIS format.
File 1 - File 5	The input files. At least one has to be selected
Target file	The output file in standard IIS format.
Shrink logfile	Using this option, the logfiles can be made smaller for faster processing. Do not use this option, if you are using the Advanced Logging Module whith a custom user id field. Otherwise, this information, which is very useful for precise session identification, will be lost.
Data columns	You can choose the data columns you want to keep. Some options cannot be deselected as they are required by LogViewPro. By default, only the columns are selected which are useful for LogViewPro.
Shrink cookies	Sometimes quite a lot of cookies are logged, which results in really huge logfiles. With this option you can choose the cookies you really want to keep. Usually, these cookies are used for session identification. By default the Google Analytics cookie, and the ASP.NET session cookies are listed here.
Exculde URIs	If the resulting logfile is still too big, you also can exclude certain URIs, like Images. You can use * as wildcard at the beginning or end of the term.

Important Note: If you use a custom field for the user cookie (usually using the advanced logging module) then you must **not** shrink the logfile, because custom columns are always removed when shrinking.

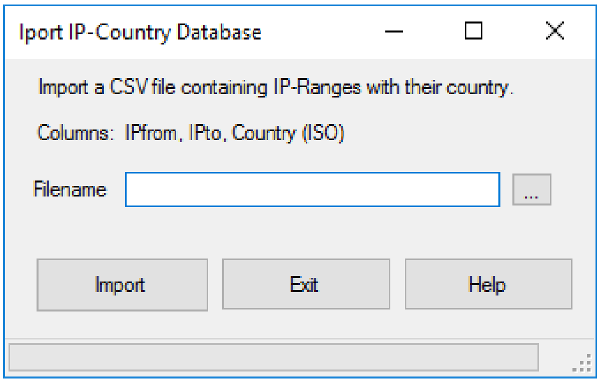
9.2 Import IP-Country-Database

For quick resolving of the originating country of each IP address, LogViewPro needs a database mapping IP address ranges to their country.

This import requires a **CSV** file, containing at least three columns, where the first three must contain:

- Start IP address of range
- End IP address of range
- 2-Letter ISO country code

We recommend to use the free database of **DB-IP.com**. Choose the smallest product, **IP address to country**. This file can be imported directly.



Import a CSV file containing IP-Ranges with their country.

Columns: IPfrom, IPto, Country (ISO)

Filename

Importing the database just takes some seconds. After this, a local copy of the data will always be loaded on startup.

10 Useful information

10.1 Logging basics

10.1.1 What is a web server logfile

A web server log maintains a history of all requests, this can be web pages, scripts, images or any type of resource that is provided by the web server. The W3C maintains a standard format for web server log files, but other proprietary formats exist. LogView Pro supports the W3C format as it is written by the **Microsoft Internet Information Server IIS**, the format of the **IIS Advanced Logging Module** and the **Apache log format**.

More recent entries are typically appended to the end of the file. Information about the request, including client IP address, request date/time, page requested, HTTP code, bytes served, user agent, and referer are typically added.

10.1.2 Logfile fields / columns

If you are using the W3C extended format, all the following fields are logged:

W3C	*Name*	*Description*	
date	Date	The date on which the activity occurred.	*
time	Time	The time the activity occurred.	**
c-ip	Client IP Address	The IP address of the client that accessed your server.	**
cs-username	Username	The name of the user who accessed your server, if he was not connected anonymously	
s-sitename	Service Name	The Internet service that was running on the client computer.	
s-computername	Server Name	The name of the server on which the log entry was generated.	
s-ip	Server IP	The IP address of the server on which the log entry was generated.	
s-port	Server Port	The port number the client is connected to. The standard port for HTTP is port 80.	
cs-method	Method	The action the client was trying to perform, usually GET or POST (see below)	*

cs-uri-stem	URI Stem	The resource accessed: for example, an HTML page, a CGI program, a script, an image, a media file.	**
cs-uri-query	URI Query	The query string, if any. The query string is separated from the Stem part or the URL by a question mark. The query string usualy consists of one or more name-value pairs (see below)	**
sc-status	HTTP Status	The status of the action, in HTTP terms (see below)	*
sc-win32-status	Win32 Status	The status of the action, in terms used by Windows.	
sc-bytes	Bytes Sent	The number of bytes sent by the server.	
cs-bytes	Bytes Received	The number of bytes received by the server.	
time-taken	Time Taken	The length of time the action took.	
cs-version	Protocol Version	The protocol (HTTP, FTP) version used by the client. For HTTP this will be either HTTP 1.0 or HTTP 1.1.	
cs-host	Host	The hostname requested in the url. As there is possible to run several web sites on the same IP address, the host name is used to make the differentation	*
cs(User-Agent)	User Agent	The browser used on the client. It contains information about the browser manufacturer, the browser version and the operating system. Very often the user agent is manipulated or fake.	**
cs(Cookie)	Cookie	The cookies sent from the browser to the server, if any. The cookie which identifies a user session is found here.	*
cs(Referer)	Referer	The full url that directed the user to the current site.	*

** Required by LogView Pro

* Useful / Recommended

10.1.3 Methods

There are different HTTP request methods:

GET	By far the most common method used to request for a specified URL. When using GET, all the values sent to the server are part of the query string.
HEAD	Identical to GET, except that the page content is not returned; just the headers are. Useful for retrieving meta-information.
POST	Similar to GET, except that a message body, typically containing key-value pairs from an HTML form submission, is included in the request data, not as part of the URL. While all the get parameters can be found in the logfile, the post data is not logged. Typically POST is used for complex forms.
TRACE	Echoes back the received request, so that a client can see what intermediate servers are adding or changing in the request.
OPTIONS	Returns the HTTP methods that the server supports. This can be used to check the functionality of a web server.
CONNECT	For use with a proxy that can change to being an SSL tunnel
PUT	Used for uploading files to a specified URI on a web-server.
DELETE	Rarely implemented, deletes a resource (i.e. a file).

10.1.4 Query Strings

When data is sent to the server as part of the URL, then this is done using query strings. These can contain these special characters:

?	Separates the resource from the query string
&	Delimiter between name-value pairs
=	Delimiter between name and value
+	Replacement for space character in query string (for details look for URL Encoding)
%nn	Encoded character

Example query string:

make=RENAULT&modellike=M%C3%A9gane&submit=Search+Car

Post data is encoded the same way, but not logged. Submiting a GET-Form also generates a url with a query string

10.1.5 Status Codes

The status code is returned by the server as result of each request:

Code	*Definition*
1xx	**Informational**
100	CONTINUE - the client should continue with request.
101	SWITCHING PROTOCOLS - the server will switch protocols as necessary.
2xx	**Successful**
200	OK - the request was fulfilled.
201	CREATED - following a *POST* command.
202	ACCEPTED - accepted for processing, but processing is not completed.
203	NON-AUTHORITATIVE INFORMATION - the returned metainformation is not the definitive set from the original server.
204	NO CONTENT - request received but no information exists to send back.
205	RESET CONTENT - the server has fulfilled the request and the user agent should reset the document view.
206	PARTIAL CONTENT - the server has fulfilled the partial GET request.
3xx	**Redirection**
300	MULTIPLE CHOICES - the requested resource has many representations.
301	MOVED PERMANENTLY - the data requested has a new location and the change is permanent.
302	FOUND - the data requested has a different URL temporarily.
303	SEE OTHER - a suggestion for the client to try another location.
304	NOT MODIFIED - the document has not been modified as expected.
305	USE PROXY - The requested resource must be accessed through the specified proxy.
306	UNUSED
307	TEMPORARY REDIRECT - the requested data resides temporarily at a new location.
4xx	**Client Errors**
400	BAD REQUEST - syntax problem in the request or it could not be satisfied.
401	UNAUTHORIZED - the client is not authorized to access data.
402	PAYMENT REQUIRED - indicates a charging scheme is in effect.
403	FORBIDDEN - access not required even with authorization.
404	NOT FOUND - server could not find the given resource.
405	METHOD NOT ALLOWED
406	NOT ACCEPTABLE
407	PROXY AUTHENTICATION REQUIRED - the client must first authenticate with the proxy for access.

408	REQUEST TIMEOUT - the client did not produce a request within the time the server was prepared to wait.
409	CONFLICT - the request could not be completed due to a conflict with the current state of the resource.
410	GONE - the requested resource is no longer available.
411	LENGTH REQUIRED - the server refused to accept the request without a defined *Content Length*.
412	PRECONDITION FAILED
413	REQUESTED ENTITY TOO LARGE - the server is refusing to process a request because it is larger than the server is willing or able to process.
414	REQUEST-URI TOO LONG - the server is refusing to process a request because the *URI* is longer than the server is willing or able to process.
415	UNSUPPORTED MEDIA TYPE - requested resource format is not supported.
416	REQUESTED RANGE NOT SATISFIABLE
417	EXPECTATION FAILED
5xx	**Server Errors**
500	INTERNAL ERROR - the server could not fulfill the request because of an unexpected condition.
501	NOT IMPLEMENTED - the sever does not support the facility requested.
502	BAD GATEWAY - received an invalid response from an upstream sever.
503	SERVICE UNAVAILABLE - the server is currently unable to handle a request.
504	GATEWAY TIMEOUT - The server, acting as a gateway/proxy, did not receive a timely response from an upstream server.
505	HTTP VERSION NOT SUPPORTED

10.1.6 Cookies

A HTTP magic cookie (usually called simply a cookie) is a packet of information sent by a server to a World Wide Web browser and then sent back by the browser each time it accesses that server (but not to other servers).

Cookies are often used to identify user sessions, because it is common that many computers share the same IP address towards the internet and there is no other way to differentiate them.

10.1.7 Sessions (Visits)

Every request is logged separately in the logfiles in chronological order, just as they get in. As a result, the requests of different users that are accessing a web server simultaneously, are completely mixed up.

LogViewPro tries to get these requests together again build sessions (or visits, as you like) by identifying the originator by some characteristics:

- IP Address
- User Agent
- Session Cookie (if available)

As the session cookie is not always available, and as there are very homogenous networks where many identical computers share the same IP Address, it is possible, that more than one session are counted and displayed as a single one. This is a problem that all the logfile analysis tools have to fight with.

10.1.8 DNS

The Domain Name System is a system that stores information about hostnames and domain names in a type of distributed database on the Internet. Of the many types of information that can be stored, most importantly it provides a physical location (IP address) for each domain name.

10.1.9 WHOIS

WHOIS is a TCP-based protocol which is widely used for querying a database in order to determine the owner of a domain name, an IP address, or an autonomous system number, on the Internet.

10.2 Backup and copy configurations and filters

LogViewPro stores all its data in the local Application Data Folder, usually found at:

```
C:\ProgramData\LogViewPro
```

Here you find the following types of files:

```
(config).lvs              Configuration files
(config)_(filter).xml     Filter files
IPCountries.xml           IP-Country-Database
Shrink.xml                Configuration of Merge / Shrink tool
```

You can copy these files to another computer.

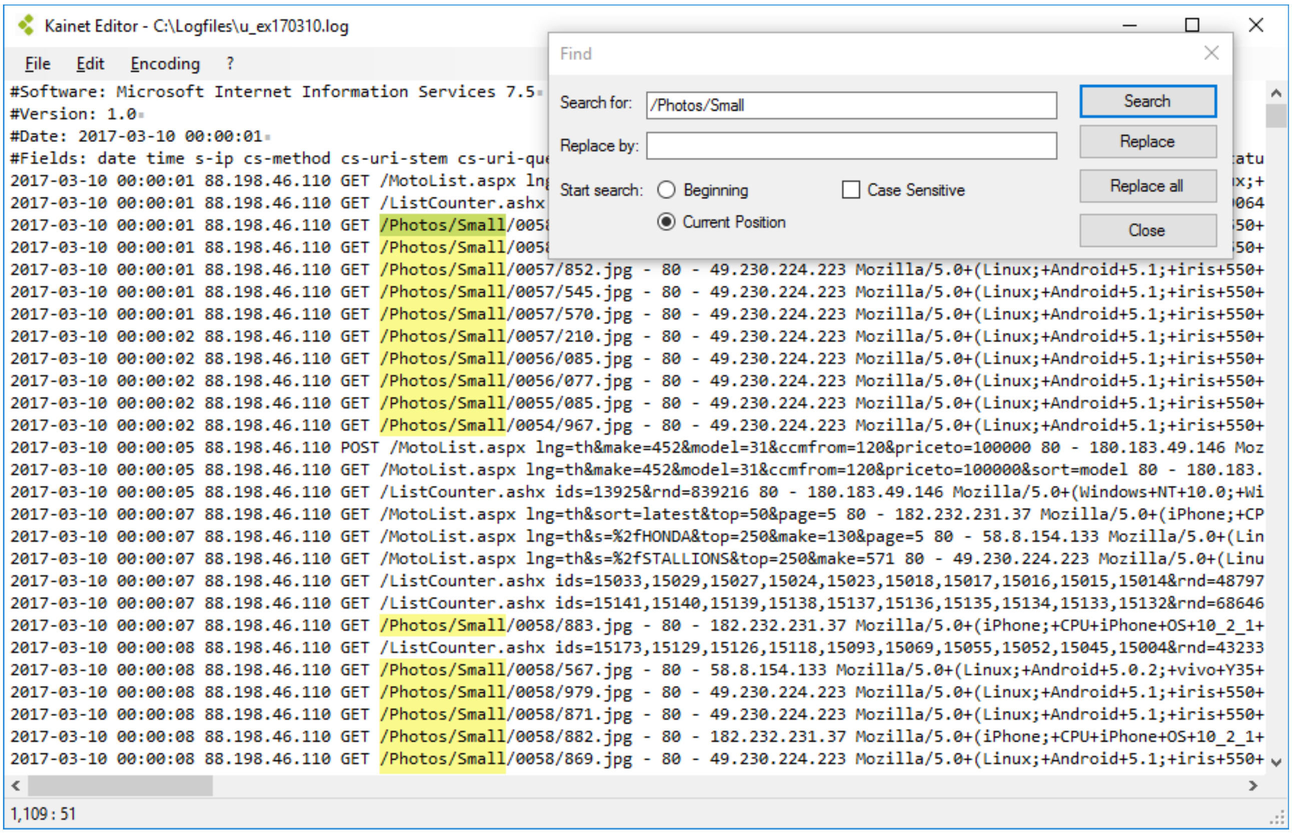
If you store your logfiles in another folder, an error message will appear, as soon as you choose the website. Then you have to edit the configuration and change the logfiles folder.

11 Other useful software

11.1 Kainet Editor

If you want to have a look at your log files, for example to see what fields are logged or what format it is, you need an editor or viewer which is able to open huge files without loading them completely into memory.

Kainet editor not only lets you open huge files, you can also do changes or replacements in files of any size:



Search for: /Photos/Small

Replace by:

Start search: ○ Beginning ● Current Position

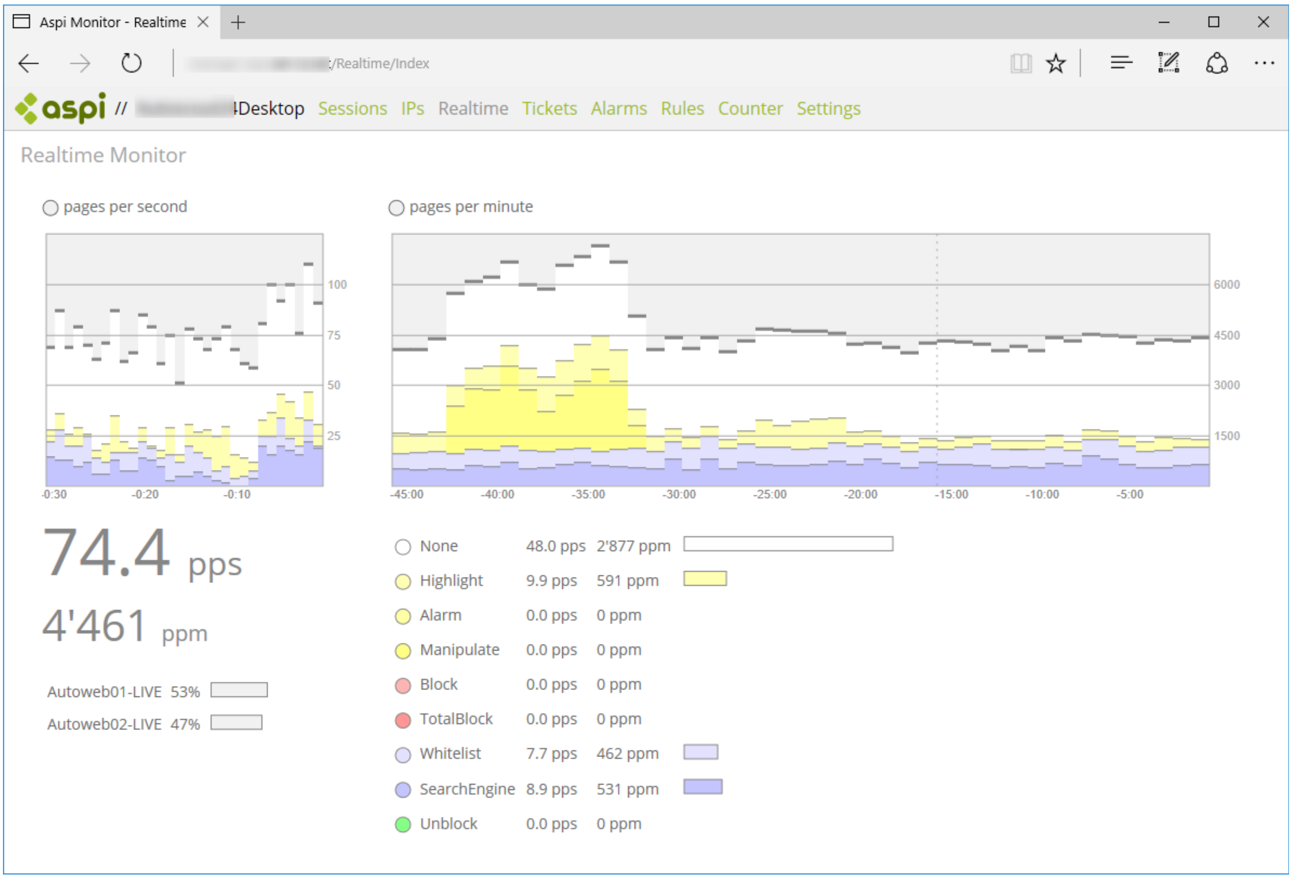
□ Case Sensitive

```
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2017-03-10 00:00:01
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-que                                                     atu
2017-03-10 00:00:01 88.198.46.110 GET /MotoList.aspx lng                                                     x;+
2017-03-10 00:00:01 88.198.46.110 GET /ListCounter.ashx                                                      064
2017-03-10 00:00:01 88.198.46.110 GET /Photos/Small/005                                                      50+
2017-03-10 00:00:01 88.198.46.110 GET /Photos/Small/005                                                      50+
2017-03-10 00:00:01 88.198.46.110 GET /Photos/Small/0057/852.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:01 88.198.46.110 GET /Photos/Small/0057/545.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:01 88.198.46.110 GET /Photos/Small/0057/570.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:02 88.198.46.110 GET /Photos/Small/0057/210.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:02 88.198.46.110 GET /Photos/Small/0056/085.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:02 88.198.46.110 GET /Photos/Small/0056/077.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:02 88.198.46.110 GET /Photos/Small/0055/085.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:02 88.198.46.110 GET /Photos/Small/0054/967.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:05 88.198.46.110 POST /MotoList.aspx lng=th&make=452&model=31&ccmfrom=120&priceto=100000 80 - 180.183.49.146 Moz
2017-03-10 00:00:05 88.198.46.110 GET /MotoList.aspx lng=th&make=452&model=31&ccmfrom=120&priceto=100000&sort=model 80 - 180.183.
2017-03-10 00:00:05 88.198.46.110 GET /ListCounter.ashx ids=13925&rnd=839216 80 - 180.183.49.146 Mozilla/5.0+(Windows+NT+10.0;+Wi
2017-03-10 00:00:07 88.198.46.110 GET /MotoList.aspx lng=th&sort=latest&top=50&page=5 80 - 182.232.231.37 Mozilla/5.0+(iPhone;+CP
2017-03-10 00:00:07 88.198.46.110 GET /MotoList.aspx lng=th&s=%2fHONDA&top=250&make=130&page=5 80 - 58.8.154.133 Mozilla/5.0+(Lin
2017-03-10 00:00:07 88.198.46.110 GET /MotoList.aspx lng=th&s=%2fSTALLIONS&top=250&make=571 80 - 49.230.224.223 Mozilla/5.0+(Linu
2017-03-10 00:00:07 88.198.46.110 GET /ListCounter.ashx ids=15033,15029,15027,15024,15023,15018,15017,15016,15015,15014&rnd=48797
2017-03-10 00:00:07 88.198.46.110 GET /ListCounter.ashx ids=15141,15140,15139,15138,15137,15136,15135,15134,15133,15132&rnd=68646
2017-03-10 00:00:07 88.198.46.110 GET /Photos/Small/0058/883.jpg - 80 - 182.232.231.37 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+10_2_1+
2017-03-10 00:00:08 88.198.46.110 GET /ListCounter.ashx ids=15173,15129,15126,15118,15093,15069,15055,15052,15045,15004&rnd=43233
2017-03-10 00:00:08 88.198.46.110 GET /Photos/Small/0058/567.jpg - 80 - 58.8.154.133 Mozilla/5.0+(Linux;+Android+5.0.2;+vivo+Y35+
2017-03-10 00:00:08 88.198.46.110 GET /Photos/Small/0058/979.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:08 88.198.46.110 GET /Photos/Small/0058/871.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
2017-03-10 00:00:08 88.198.46.110 GET /Photos/Small/0058/882.jpg - 80 - 182.232.231.37 Mozilla/5.0+(iPhone;+CPU+iPhone+OS+10_2_1+
2017-03-10 00:00:08 88.198.46.110 GET /Photos/Small/0058/869.jpg - 80 - 49.230.224.223 Mozilla/5.0+(Linux;+Android+5.1;+iris+550+
```

Kainet Editor can be downloaded from our web page. It is free for private users, self-employed persons and small companies.

11.2 Kainet Aspi

Kainet has developed a complete solution for blocking spiders. It is a http module which can easily be integrated into ASP.NET web sites.



Realtime Monitor

○ pages per second

○ pages per minute

74.4 pps

4'461 ppm

Autoweb01-LIVE	53%	▭
Autoweb02-LIVE	47%	▭

○ None	48.0 pps	2'877 ppm	▭
○ Highlight	9.9 pps	591 ppm	▭
○ Alarm	0.0 pps	0 ppm	
○ Manipulate	0.0 pps	0 ppm	
● Block	0.0 pps	0 ppm	
● TotalBlock	0.0 pps	0 ppm	
○ Whitelist	7.7 pps	462 ppm	▭
● SearchEngine	8.9 pps	531 ppm	▭
● Unblock	0.0 pps	0 ppm	

Please visit our web page or contact us to get more information about the solution.