The attached tip sheet presents the most common regular expressions and queries used in the creating report and running search queries.

Example Regular Expression	Result
Website Domain Name Field	***"Matches regexp"***
windows	Websites that contain *"windows"* in their URL
^windows	Websites that have URLs starting with *"windows"*
windows.com$	*Websites that have URLs ending with "windows.com"*
^windows.com$	Websites that exactly match *"windows.com"*
Logon Name Field	***"Matches regexp"***
laura.ashton	The user *"laura.ashton"*
laura.ashton|robert.schmidt	The users "laura.ashton" and "robert.schmidt"
Resource Field	***"Matches regexp"***
\.*mp3*	All MP3 downloads
\.mp3|\.wma	All MP3 or WMA audio file downloads
File/Folder Name Field	***"Matches regexp"***
sales|profit|loss	All filenames or directory names that contain "sales", "profit", or "loss"
\.pptx$	All file activity involving .pptx files
\.docx|\.xlsx	All file activity involving Microsoft Word or Excel files
\.zepto|\.locky|\.help_decrypt	All file activity involving file extensions .zepto, .locky and .help_decrypt
\\private\\	All file activity involving a directory named *"private"*

Example of Search bar entries	Result
IP Address	
192.168.127.1	A single IP address 192.168.127.1
192.168.127.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254
192.168.127.1,192.168.127.2	The IP addresses 192.168.127.1 and 192.168.127.2
192.168.127.0/24,192.168.128.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254 and 192.168.128.1 to 192.168.128.254
192.168.0.0/16,!192.168.127.0/24	All IP addresses in the range 192.168.0.1 to 192.168.127.254 but excludes IP addresses in the range 192.168.127.1 to 192.168.127.254
Report variables can be used in place of IPs/Ports/Subnets	
Dublin	A single IP which matches the report variable “Dublin”. Filter box will autofill on typing.
Dublin,NewYork,Berlin	The IP addresses which correspond to the report variables (subnets) *“Dublin”* and *“NewYork”* and *“Berlin”* separated by a comma

User Name	
laura.ashton	The user "laura.ashton"
laura.ashton|robert.schmidt	The users "laura.ashton" or "robert.schmidt"
Website	
youtube.com	Web activity associated with youtube.com
Face	Web activity associated with any website that contains *"Face"* in the URL
youtube.com|googlevideo.com	Websites that contain "youtube.com" or *"googlevideo.com"* in the URLs

Syntax help with lguser commands	**Command explained**
lguser credentials	**Login: lguser** **Password: netfort**
cat	Concatenate and print files
ifconfig	Configure network interface parameters
ls	List directory contents
nslookup	Query Internet name servers interactively
rm	Remove directory entries
sh	Command interpreter (shell)
tail	Display the last part of a file
df	Display free disk space
ping	Send ICMP ECHO_REQUEST packets to network hosts
scp	Secure copy (remote file copy program)
ssh	OpenSSH SSH client (remote login program)
tcpdump	Dump traffic on a network

BPF traffic filter for IDS and for the Traffic Monitor	**BPF filter explained**
Ignore traffic from a network range and a few singular hosts:	not net xx.xx.xx.0/20 and not host x.x.x.x and not host x.x.x.x
To exclude one host:	not host xx.xx.xx.xx
To exclude multiple hosts:	not host xx.xx.xx.xx and not host xx.xx.xx.xx and not host xx.xx.xx.xx
To exclude one port:	not port x

If you have any queries regarding regular expressions and queries used in the creating report and running search queries, please contact the NetFort support team who will be delighted to assist you https://www.netfort.com/about-netfort/contact/