## **Filtering and Searching**

The filtering and searching capabilities have been considerably enhanced. The user can filter records via column filters, the auto-filter row, filter editor, filter manager and quick search panel. The filter manager allows the user to store, order and configure any number of filters.

0						NetAnal	ysis ®	v2.0	- Fo	rensi	ic Inter	net History Analysis - [lan Richardson]
File View	Tools Sea	rch l	Index Filter Reports	Co	lumn	Window	v H	elp				
1 🔁 🕞 🔁	🖢 Import 🝷	🕎 Q	. 🖃 🔜 🗏 🧶 📕	٢	<b>)</b> 🗉	) 🔜   🏹	5	3 🗈	13	t   C		
Entry Type	Scheme	Tag	Date Visited [UTC]			od Docoll		Visit	-	uni		
Redirect	🛃 http		2014-05-14 14:50:08.000		Show	/ all by a speci	fic date					t-survey.co.uk/s.asp?i=107455hxljo&x=drinkand
😡 Cache	🚰 http		2014-05-14 14:50:08.000		4	by a spea		mber 2	014			tsurvey.co.uk/_cdn/jquery/min.js
😡 Cache	🛃 http		2014-05-14 14:50:08.000				J-ph					tsurvey.co.uk/s.asp?i=107455hxljo&x=drinkando
le Cache	🛃 http		2014-05-14 14:50:08.000			Mon Tue	Wed	Thu	Fri	Sat		ite.org/newsite/survey/fancybox_loading.gif
le Cache	🛃 http		2014-05-14 14:50:08.000			25 26 1 2	27 3	28 4	29 5	30 6	31 7	ite.org/newsite/survey/fancybox_sprite.png
Cookie			2014-05-14 14:50:08.485			8 9	10	11	12	13	14	
Cookie			2014-05-14 14:50:08.991			15 16	17	18	19	20	21	y.co.uk
😡 Cache	🛃 http		2014-05-14 14:50:09.000			22 23 29 30	24 1	25 2	26 3	<b>27</b> 4	28 5	tsurvey.co.uk/s/jc/ss.default.min.js
le Cache	🛃 http		2014-05-14 14:50:09.000		Faste							ple-analytics.com/collect?v=1&_v=j21&a=762611
le Cache	🚰 http		2014-05-14 14:50:09.000			er this year to this yea	r					tsurvey.co.uk/s/jc/ss.survey.min.3.js
le Cache	🛃 http		2014-05-14 14:50:09.000			is valid						tsurvey.co.uk/_files/cabinet/30027/140_Thesite_
😡 Cache	🛃 http		2014-05-14 14:50:09.000	×								tsurvey.co.uk/_cdn/jquery/ui.css
Cookie			2014-05-14 14:50:09.364	20	14-05-	14 15:50:0	9.364			.sm	artsurvey	y.co.uk
😡 Cache	🛃 http		2014-05-14 14:50:18.000	20	14-05-	14 15:50:1	8.000		1	L http	://listing:	s07.skiddlecdn.co.uk/1/d/4/448314_2_tynedale-beer-
Redirect	🛃 http		2014-05-14 14:50:18.000	20	14-05-	14 15:50:1	8.000		1	1 http	)://r9sr	n-aiglInel.googlevideo.com/videoplayback?c=web&cler
😡 Cache	🛃 http		2014-05-14 14:50:18.000	20	14-05-	14 15:50:1	8.000		1	L http	)://r7sr	n-cg07luer.googlevideo.com/videoplayback?c=web&cl

Each column header has a small filter icon; clicking on this icon allows the user to select filter criteria for that column. In the case above, the user has selected a date filter.

۵ (۱	NetAnalysis® v2.0 - Forensic Int	ernet History Analysis - [l	an Richardson]
File View Tools Search Index Filter Reports Column	Window Help		
🔚 🖶 🛃   🚵 Import 🗸   🟹 🔍   📰 👪 🗐 🧶 📕   😻 😂 🗐	) 🔜   7 🥪 尋 🗊   🔆 🛛		
Search Term  Searc	Personant         idols         jag xf         jaguar xf         mass         mdma cost per gram         mdma crystals         most expensive tablet         news: mdma         omega         plant nutrients         plant pots         raves around swansea         raves around swansea         raves around swansea wales	Dect Lloor	E Cogon User
		80	
		80	
		80	

In the screen above, the user has selected a column filter for the Search Term column, if a specific term is selected, all the records which contained that search term will be filtered.

۲	NetAnalysis® v2.0 - Forensic Internet History Analysis - [lan	Richardson]
File	View Tools Search Index Filter Reports Column Window Help	
1	🛅 🛃 🔤 Import 🗸 🔄 🖓 🔍 🔄 🔜 🗏 🧶 則 🗳 🤤 🖼 💌 🦓 🦻 🔜 🛠 😓	
	Page Title	Absolute Path
۴	green	
	greenhouse foundations pdf - Bing	/search
	greenhouse pdf - Bing	/search
	greenhouse sunlight lamps - Bing	/search
	greenhouses - Bing	/search
	Greenhouses   eBay	/sch/Greenhouses-/
	Greenhouses for sale from Greenhouses Direct	1
	Greenhouses for Sale from Greenhouse Stores	1
	Greenhouse Staging   Greenhouse Stores	/Greenhouse-Stagin
	Greenhouse Base Preparation Guide	/greenhouse-base-h
	Greenhouse  Halls Greenhouses   Greenhouses For Sale   southwestgreenhouses.co.uk	1

The auto-filter row, when activated, appears under the column header. This allows the user to filter rows based on the search string. In the example above, the user is searching for Page Titles which start with the text "green".

0				Not A polycic ®	20 Eor	ensic Internet History Analysis - [Ian Richardson]	
-						ensic internet history Analysis - [ian Kichardson]	
File View	Tools Sear		Index Filter Reports	Column Window He	lp		
1 🖆 🛱 🛃 1 🖻	🔄 Import 🝷	<b>7</b> Q	. 🖃 🖽 🗏 🧶 📕 🕻	ə 🗟 🖹 🔜   🎖 😼 🏾	> 🖸 🔆	0	
× google	X google Find Clear						
Entry Type	Scheme	Tag	Date Visited [UTC] •	Date Visited [Local]	Visits	URL	
🛞 Cookie			2014-05-21 11:17:32.282	2014-05-21 12:17:32.282		.google.com	
🍛 Cache	🔒 https		2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	58	https://apis. <mark>google</mark> .com/js/plusone.js	
🍛 Cache	🔒 https		2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	17	https://apis. <mark>google</mark> .com/js/api.js	
🈡 Cache	🛃 http		2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	38	http://www.google-analytics.com/analytics.js	
😡 Cache	📝 http		2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	1	http://www.google-analytics.com/collect?v=1&_v=j21&a=933818&	
😡 Cache	🔒 https		2014-05-21 11:17:32.000	2014-05-21 12:17:32.000	28	https://oauth.googleusercontent.com/gadgets/js/core:rpc:shindig.r	
le Cache	🛃 http		2014-05-21 11:15:03.000	2014-05-21 12:15:03.000	1	http://www.google-analytics.com/utm.gif?utmwv=5.5.1&utms=1	
🦦 Cache	🛃 http		2014-05-21 11:15:02.000	2014-05-21 12:15:02.000	142	http://www. <mark>google</mark> -analytics.com/ga.js	
le Cache	🛃 http		2014-05-21 11:14:59.000	2014-05-21 12:14:59.000	1	http://ajax.googleapis.com/ajax/libs/jquery/1.2.6/jquery.min.js	
le Cache	🛃 http		2014-05-21 11:14:56.000	2014-05-21 12:14:56.000	1	http://ad.uk.doubleclick.net/N4215/adj/amzn.uk.sr.aps;sz=160x600	
le Cache	🛃 http		2014-05-21 11:14:56.000	2014-05-21 12:14:56.000	1	http://www.google-analytics.com/utm.gif?utmwv=1.4&utmn=138	
🥪 Cache	🛃 http		2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	10	http://www.google-analytics.com/urchin.js	
😡 Cache	🛃 http		2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	1	http://pubads.g.doubleclick.net/activity;dc_iu=/7369/nreaudience;c	
🥪 Cache	📝 http		2014-05-21 11:14:55.000	2014-05-21 12:14:55.000	1	http://ad.doubleclick.net/activity;src=3401595;dcnet=7194;boom=	

In the example above, the user has searched for the text "google" across all rows and columns. NetAnalysis® automatically filters and highlights the hits so the user can easily review the matches.

<b>\$</b>	Edit Filter			×
Filter Nan Live Cad Visual And O				
		ОК	Cancel	Apply .::

The visual filter editor is extremely powerful and makes it a simple task for the user to build complex queries which can be saved for later re-use. The user no longer has to have an understanding of SQL to create powerful queries.



The filter manager is located in a docking panel and allows the user to easily create, edit, save and categorise all the filters they would need during a forensic investigation.

Keyword Manager		щ	х			
🔺 🧓 Keyword List						
Adult						
Child Protection						
🖌 🚄 Computer Crime						
🧓 Cyber Security						
🧓 Virus						
🧓 Worm						
Drugs						
Financial						
Social Media						
Terrorism						
Weapons						
🏹 Filter Manager 🛛 😓 Keyword Manager 👔 Report Manager 😜 HTTP Response 📑 Search Results						

The keyword manager is also located in a docking panel and 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.

5		Edit Keyword List	-	. 🗆	×
	Keywords				
	Keyword Li	st Name			
	Cutting Ag				
	Keyword Li				
	1	acetylsalicylic acid			<u>^</u>
	2	amphetamine atropine			
	4	benzocaine			
	5	boric acid			
	6	caffeine			
	7	creatine			
	8	dextrose			
	9	dihydrochloride			
	10	diltiazem			
	11	dimethylterephthalate			
	12	ephedrine			
	13	glucose			
	14	hydroxyzine			
	15	inositol			
	16	lactose			
	17	lidocaine			
	18	lidocaine			
	19	lignocaine			
	20	mannitol			
	21	methamphetamine			
	22	monohydrate			
	23	paracetamol			
	24	paracetamol			
	25	phenacetine			<b>~</b>
				C	
		OK		Cancel	
					.::

Keyword lists can be easily maintained via the keyword manager. The above example shows a list of keywords relating to drugs.

Search Results	д	х
A C Keyword Hits		^
🔑 acid (6)		
🔑 amphetamine (2)		
🔑 base (1941)		
🔑 blast (4)		
🤌 bonsai (3)		
🤌 bounce (2)		
🤌 brown (3)		
🤌 brownies (1)		
🥬 bubble (23)		
🔑 cannabis (7)		
🔑 chang (92)		
🔑 charge (6)		
🤌 cocaine (2)		
🔑 codeine (1)		4
Search Results √ Filter Manager		

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

	NetAnalysis® v2.0 - Forensic Internet History Analysis - [lan Richardson]	- 🗆 ×
File View Tools Search Index Filter Reports	Column Window Help	
🗄 🔚 🛃 🚵 Import 🗸 🕎 🔍 🔚 🔜 🗐 🧶 🔳 🕇	کا 😒 🖬 🔜 🦷 🥪 🔯 🕹 🕹	(UTC) Dublin, Edinburgh, Lisbon, London
	Date Visited [Local] Visits URL	() <u>-</u>
		"
	2014-05-21 12:15:08.000 1 http://tss.mm.bing.net/th/q=Marguana +Hant +Nutrientsaw=508n=508n=508n=508n=508n=508n=508n=508n	lit=moderate&t=1
H4 44 4 Record 0 of 1 + H+ HH 4		•
Keyword Manager 🗖 🖪 🗴	Search Results	□ # X
a 😼 Keyword List	🔑 herb (5)	^
Adult	🤌 heroin (1)	
Child Protection	🔑 hog (1)	
<ul> <li>Computer Crime</li> <li>Grugs</li> </ul>	Phorse (3)	
Cutting Agents	🔑 ice (3486)	
brugs A-Z	🔑 juice (1)	
B Hazardous Substances	🔑 ketamine (1)	
> 🧮 Financial	🔑 killer (4)	
b Gocial Media	🔑 kix (2)	
Terrorism	🔑 lsd (12)	
Weapons		
	🔑 marijuana (1)	
	🔑 mdat (2)	
	🔑 mdma (244)	
	🤌 meow meow (1)	~
🤯 Keyword Manager 🛛 🏹 Filter Manager	S Report Manager Search Results	
www.digital-detective.net	C: \Users\Joseph\\wx4agie7.default\cookies.sqlite	ID: 12314 ,;;

To review the search results, the user double clicks on a keyword from the list and the corresponding hits are automatically filtered and highlighted in the grid.