

While users are surfing the web, listening to music, and writing documents, the kernel and various background daemons write information to logfiles. KSystemLog, Gnome System Log Viewer, and MultiTail will help you read and process logfile data. *By Andrej Fink* 

f some piece of hardware or software refuses to work, you can't log in, or a file, print or web server isn't responding, the logfiles on a Linux system very often give you the hints you need to solve the problem. Logs such as /var/log/messages or /var/log/auth. log keep a watchful eye, but they do so slowly enough for users to be able to investigate their content using standard tools (e.g., tail, less, cut, grep, etc.).

Other logfiles explode into impenetrable text jungles and make it difficult for mere mortals to see what's relevant. The access logs on a public web server, for example, contain details of the date and time, the contacting IP address, and the requested URL for each request. Also, the web server logs the status code (e.g., 200 0K or 404 Not Found), the traffic volume, and, depending on the configuration, much more. All told, whenever a browser accesses a website with images, JavaScript, and stylesheets, several lines of logfile content will be created.

#### Foresters

When you are exploring the logfile jungle, you can't just rely on having good eyesight. Instead, you need a guide in the shape of a logfile viewer. These tools look for certain strings and filter out irrelevant information. Additionally, you will probably want the viewer to show you new entries automatically because logfiles are often fairly meaningless unless you view them in real time. After all, if you just wanted to view the content, you could use a text editor or a pager. Color highlighting of keywords is also a neat feature, although not strictly necessary. Just like syntax highlighting in an editor, this feature can facilitate a search for certain information.

In our lab, I put three logfile viewers through their paces: KSystemLog [1] is part of the KDE Software Compilation and tries to help users through the logfile maze with a graphical interface. Its Gnome counterpart, the Gnome System Log Viewer [2], follows the same approach, but with a more spartan interface that tries to entice the user into exploring. MultiTail [3] is a very different beast – this text-based application is an extension of the tail command and simply displays interwoven or horizontally or vertically separated logs.

# KSystemLog

By default, the KDE logfile viewer begins with a view of the system logfile (/var/ log/syslog). The entries in the logfile are organized like a spreadsheet, in which you can view, hide, and change the order of the columns. KSystemLog



🤊 📀 🗙	lorg Log - Ks	Systemlog				
File Ec	lit Logs <u>W</u> indo	w <u>S</u> ettings <u>H</u> elp				
0	0	2 9				
U	G R	Evetom Log Korp	llog Au	bentication log Doomens' logs Verg log		
Stop	Reload Details	system Log Kern	a Log Au	mentication Log Daemons Logs X.org Log		
<u> </u>	🕺 X.org Log 🛛	👮 System Log (6)	🔊 🦳 Au	thentication Log (4)		
Y Filter:	Enter your searc	h here				All V
Line 🔹	<ul> <li>Type</li> </ul>	Message				<u>^</u>
8	Error	open /dev/fb0: No suc	h file or dir	ectory		
0	Information	resource ranges after	probing:			
0	Information	[4] 0	0	0x000a0000 - 0x000affff (0x10000) MS[B]		
0	Information	[5] 0	0	0x000b0000 - 0x000b7fff (0x8000) MS[B]		
0	Information	[6] 0	0	0x000b8000 - 0x000bffff (0x8000) MS[B]		
0	Information	[7] -1	0	0x0000ffff - 0x0000ffff (0x1) IX[B]		
0	Information	[8] -1	0	0x00000000 - 0x00000000 (0x1) IX[B]		
0	Information	[9] 0	0	0x000003b0 - 0x000003bb (0xc) IS[B]		
0	Information	[10] 0	0	0x000003c0 - 0x000003df (0x20) IS[B]		
0	Information	Loading sub module "	vgahw"			
0	Information	LoadModule: "vgahw"	1.1			
0	Information	Loading /usr/lib/xorg/n	nodules//lib	vgahw.so		
0	Information	Module vgahw: vendo	="X.Org Fo	undation"		
0	Information	compiled	for 1.6.4, r	nodule version = 0.1.0		
0	Information	CIRRUS(0): vgaHWGet	OBase: hw	o->IOBase is 0x03d0, hwp->PI00ffset is 0x0000		U
0	Information	Loading sub module "	int10"			
	Information	LoadModule: "int10"	1.1. 401			
U	Information	Loading /usr/lib/xorg/n	nodules//lib	Int10.so		
	Information	Module Intit: vendor	="x.org Fou	indation"		
•	Information	CIRRUS(U): Initializing	ntio	- 1/700-		
	warning	System lacks support	for changin	IG MIRRS		
	Information	CIRRUS(U): Primary V	sios segme	int is: 0xc000		
	Information	CIRRUS(U): Creating d	efault displ	ay subsection in Screen section		
2	Drohod	CIDDUC(0): Depth 24	erault cirru	s Screen 0° for depth/fbbpp 24/24		
1000	Probed Default action	CIRRUS(0): Depth 24,	(==) frame	builer bpp 24		
649	Default setting	CIRRUS(0): RGB weigh	uol in Truc	alar		
690 619	Default setting	CIRROS(0): Default VIS				
1	Brohod	14:47:27: Log file 'Na			<b>^</b>	
1	Probed	14:46:25: Log file '/va				
	Probed	14:45:55: Log file '/va				
ä	Information	14:45:38: Log succe				
ă	Information	14:45:38: Log file '/va			~	<u>.</u>
-	ation	14:45:38: Log file '/va	inilog/auth.	log" loaded successfully	· · · ·	•
384 lines.		14:47:27: Log file '/va	r/log/syslo	g' has changed.	~	Last updated: 14:23:56

Figure 1: If the display in a tab changes, KSystemLog updates the new message count in the brackets. To view the changes, you simply drop down the menu at the bottom.

runs the logfiles through a parser when it is loaded to construct the correct columns for the files. The KDE tool automatically refreshes the view and highlights new logfile entries in bold type. By default, the viewer also jumps to the new lines, although you can disable this feature in the context menu.

KSystemLog will normally show you the last 1,000 lines in a logfile, although the program settings let you expand this to 30,000 entries. You can click to highlight a line or multiple lines, copy the selection to the clipboard, store it in a text file, print it, or mail it. KSystemLog will only work with the content of the highlighted lines; you do not get the name of the logfile or other useful metadata.

The toolbar and the Logs menu give you quick access to other logfiles. If the logfiles defined by the program are not sufficient for your purposes, you can open a file browser to find the required log. KSystemLog will automatically try to apply the syslog schema. This might not be a perfect solution, however, in that many programs have their own ideas of how to organize things and do not pass things on to syslog.

Pressing Ctrl + F displays a search box below the log table that you can use to look for keywords. As an alternative to this, a filter bar above the table lets you restrict the display to specific entries. The detailed view shows selected lines in a separate dialog, which contains the full entry along with additional information, such as the date, logfile, or process name.

KSystemLog can open multiple logfiles at the same time and organize them in tabs. For this to happen, you first need to press Ctrl + T and create a new tab; then you select the required log. When the viewer refreshes a logfile in the background, it shows you the number of new lines in brackets next to the tab name. Additionally, the tool displays a dropdown menu at the bottom of the window telling you which log was updated and displaying the new lines with color high-

lighting (see Figure 1). Unfortunately, the program doesn't remember which tabs you opened with which logfiles. So, the next time you launch KSystemLog, you have to reopen the tabs and logfiles and set them up again.

One of KSystem-Log's neatest gimmicks is its support for multiple date formats. You can use the program's general settings to choose between a short or long display format. And, for both variants, you replace the numerical date with *Today* or *Yesterday* (as opposed to "long names").

At this point, a minor weakness in KSystemLog is revealed: If it runs without interruption beyond midnight, you need to reload the logfiles to avoid confusion.

#### Gnome System Log Viewer

This viewer follows the general philosophy of the Gnome desktop environment: More is not always better. When it comes up, the tool is spartan but fast and functional. The logfile name is shown in the sidebar on the left, with the content displayed on the right. In this text box, users can scroll and highlight to their heart's content without being distracted by cryptic menu entries or garish icons. Pressing F9 hides the sidebar, giving the Gnome System Log Viewer the feel of a text editor.

The selection in the area on the left is huge, but if your favorite logfile is missing, you can use the file browser to locate it. The Gnome tool remembers the logs you added manually when restarted, making it worthwhile to customize. You can close logfile views by pressing Ctrl + W, but don't look for a setup dialog for organizing or editing existing entries. The approach here is via the Gconf editor, in which the /apps/ gnome-system-log section gives you access to the various keys (see Figure 2).

The Gnome System Log Viewer also gives you a live view that automatically

Configurat			on Editor - gnome-system-log			
File Edit Bookmarks Help						
Image:	^	Name	✓ Value			
i gnect		1 fonts	tsize 10			
<ul> <li>imig gnibbles</li> <li>imig gnobots2</li> <li>imig gnome-dictionary</li> <li>imig gnome-keyring</li> </ul>		1 heig	ght 554			
		🗟 logfi	ile /var/log/messages			
		🗈 logfi	iles [/var/log/daemon.log,/var/log/kern.log,/var/log/us	ser.lc		
		1 widt	th 733			
gnome-power-manager		-				
<ul> <li>□ gnome-screensaver</li> <li>□ gnome-screenshot</li> <li>▷ □ gnome-search-tool</li> <li>▷ □ gnome-session</li> </ul>		1	🗙 💶 🛛 Edit Key			
		<		>		
		Key Doc	Name: /apps/gnome-system-log/logfiles			
			Type: List			
gnome-settings		Key na				
gnome_settings_daemo		Key ov	List type: String			
gnome-sound-recorder		Short	Values			
📄 gnome-sudoku		Long d	/var/log/aptitude			
🦲 gnome-system-log			/var/log/messages	iy /		
▶ <u>anome-system-tools</u> ▼			/var/log/debug <u>R</u> emove			
			/var/log/pm-powersave.lo			
×			/var/log/iockey.log.1			
			/var/log/mail.log			
			/var/log/mail.info			
			<u>Down</u>			
3			Cancel OK			
/apps/gpome-system-log/logfiles			guiler gr			

Figure 2: To organize or edit existing entries, use the Gconf editor.



<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>F</u> ilters	<u>H</u> elp						
Xora 0 log	Арг	7 13:08:18 UDUNTU ANCLIENT: DHCPACK OT 10.0.0.154 TROM 10.0.0.1					
Add g.o.log	Apr	7 13:08:18 ubuntu dhclient: bound to 10.0.0.154 renewal in 1422 seconds.					
aptitude	Apr	7 13:32:00 ubuntu dhclient: DHCPREQUEST of 10.0.0.154 on eth0 to 10.0.0.1 port 67					
auth.log	Apr	7 13:32:00 ubuntu dhclient: DHCPACK of 10.0.0.154 from 10.0.0.1					
boot	Apr	7 13:32:00 ubuntu dhclient: bound to 10.0.0.154 renewal in 1456 seconds.					
srap log	Apr	7 13:55:16 ubuntu decient: DHCPHEQUEST of 10.0.0.154 on etho to 10.0.0.1 port 6/					
cronilog	Apr	7 13:56:16 ubuntu dhellent: bhend to 10.0.0.154 renewal in 1403 seconds					
daemon.log	Apr	7 14:14:57 ubuntu gnore-session[1558]: WARNEG: Client '/org/one/SessionManager/Client9' fail					
◊ debug	Apr	7 14:14:57 ubuntu gnome-session[1558]: WARNING: Client '/org/gnome/SessionManager/Client8' fail					
dmesg	Apr	7 14:14:57 ubuntu gnome-session[1558]: WARNING: Unable to find desktop file 'evolution-exchange					
dmesa 0	Apr	7 14:14:57 ubuntu gnome-session[1558]: WARNING: Unable to find desktop file 'gnome-evolution-ex					
N I I I	Apr	7 14:17:20 ubuntu gdm-binary[32]: WARNING: Unable to find users: no seat-id found					
и аркд.юд	Apr	7 14:17:21 ubuntu acpid: client 1428[0:0] has disconnected					
fontconfig.log	Apr	7 14:17:21 ubuntu acpid: client connected from 3208[0:0]					
jockey.log	Apr	7 14:21:09 ubuntu dhclient: DHCPHEQUEST of 10.0.0.154 on etho to 10.0.0.1 port 6/					
▷ kern.log	Apr	7 14:21:09 ubuntu ductient: DHCPACK 01 10:0.0.154 From 10:0.0.1					
b lorlog	Apr	7 14-21.09 ubuntu dhellent. DHCPBEQUEST of 10.0.0154 or renewat in 1578 seconds.					
r ipiliog	Apr	7 14:47:27 ubuntu dhclient: DHCPACK of 10.0.0.154 from 10.0.0.1					
mail.err	Apr	7 14:47:27 ubuntu dhclient: bound to 10.0.0.154 renewal in 1622 seconds.					
mail.info	Apr	7 15:14:29 ubuntu dhclient: DHCPREQUEST of 10.0.0.154 on eth0 to 10.0.0.1 port 67					
mail.log	Apr	7 15:14:29 ubuntu dhclient: DHCPACK of 10.0.0.154 from 10.0.0.1					
mailwarn	Apr	7 15:14:29 ubuntu dhclient: bound to 10.0.0.154 renewal in 1250 seconds.					
N massages	Apr	7 15:35:19 ubuntu dhelient: DHCPREQUEST of 10.0.0.154 on eth0 to 10.0.0.1 port 67					
v messages	Apr	/ 15:35:10 ubuntu docteor: DHCPACK of 10.0.0.154 from 10.0.0.1					
pm-powersave.log	Apr	7 15:57:52 uburtu dictient: DWCDREC 10:00:154 - Tenewar in 155 seconds.					
pm-suspend.log	Apr	7 15:57:52 ubuntu dhelient: DHCPACK of 10.0.0.154 from 10.0.0.1					
pycentral.log	Apr	7 15:57:52 ubuntu dhclient: bound to 10.0.0.154 renewal in 1306 seconds.					
b syslog	Apr	7 15:59:31 ubuntu gdm-binary[3845]: WARNING: Unable to find users: no seat-id found					
, systeg	Apr	7 15:59:32 ubuntu acpid: client 3208[0:0] has disconnected					
udev	Apr	7 15:59:32 ubuntu acpid: client connected from 3850[0:0]					
▶ user.log	Apr	7 16:00:18 ubuntu gdm-session-worker[3951]: WARNING: Unable to open session: Did not receive a					
	Apr	/ 16:03:28 ubuntu avahi-daemon[614]: Got SlGHUP, reloading.					
	Apr	/ 10:00:20 upuntu avanz-daemon[014]: No service file found in /etc/avahi/services.					
	Apr	7 10.07.72 upuntu upus-uachion. Recoaueu configuration					
2200 l' (00 0 (0)   .							
1132 IIIIes (98,0 KB) - Iasc update: Mit APF / 16:00:18 2010							

Figure 3: Gnome System Log Viewer does without colorful icons and offers very unobtrusive highlighting.

refreshes the display. When new entries reach the logfile you are viewing, the tool jumps to the lines in question and highlights them in bold type. In contrast to KSystemLog, you cannot disable this behavior. If something happens in one of the logfiles, the Gnome tool discreetly draws your attention to it by highlighting the log name in the sidebar. The label doesn't revert to the normal display until you have checked the updated log.

The Ctrl + F shortcut displays a search bar below the text box. Additionally, you can define some filters in the filter menu. In the dialog this displays, you can then define rules to highlight (Figure 3) or hide individual lines. Regular expressions are supported here. Once set up, the filter rules can be enabled individually as subitems in the *Filter* menu.

Working with the Gnome System Log Viewer is enjoyable because the tool only highlights the date in the area on the right and otherwise displays the logfiles as is. This rules out incorrect pars-

ing of some logs. Logfiles whose timestamps the tool has identified will appear in the bar on the left as expandable entries. Then you can click to sort the entries by day.

### MultiTail

The logfile viewer for the command line might ap-

pear hard to use at first glance, but it soon reveals itself as a powerful tool that gives admins unlimited possibilities for log analytics. When launched, MultiTail expects you to pass in a number of details, such as the log name (multitail /var/log/messages). The tool will then show you the latest entries from the selected file. The viewer highlights some keywords (see Figure 4).

Hitting F1, *H*, or Ctrl + H will display a window in the terminal with details of the available shortcuts. *B* opens a subwindow for scrolling. In this view, you can press *B*, the arrow keys, or use the mouse wheel to navigate. While you are doing so, the log display continues to run in the main window, keeping Multi-Tail up to date at all times. Pressing Q quits the subwindow, as well as the program itself.

The keyboard shortcut / (that's simply a slash) opens MultiTail's search function. Again, the viewer gives you a separate window for this so that the display

#### LISTING 1: Script weekday.rb

```
01 #!/usr/bin/env ruby
02 require 'date'
03
04 STDOUT.sync = true
05
06 STDIN.each_line do |date|
07 puts DateTime.parse(date).strftime
  ('W%W %A %T') + "\n"
08 end
```

will continue to update in the background.

MultiTail color codes logfiles for ease of viewing with color schemes defined in /etc/multitail.conf. If you don't like the program defaults, you can either define the color scheme in the setup file at run time (press C) or when launching the program (-cS scheme). Also, you can combine multiple schemes, which makes sense for logs like /var/log/messages that contain messages from various services.

#### Versatility

If you find the huge range of options described by the man page daunting, check out the examples on the website [4]. The "MultiTail Hands On" box also gives you two examples of advanced use. After setting up MultiTail to meet your requirements, you can press *W* to generate a one-line shell script that automatically sets the tool to your preferred state when launched.

As mentioned earlier, MultiTail can display multiple logfiles simultaneously. The viewer is flexible and will also accommodate messages from external programs like ping, tcpdump, or strace. You can also mix the displays (merge function) or tile the main window horizontally or vertically (Figure 5).

Combinations of these view options are allowed. This makes it possible to

```
Terminal
                                                                                                                                                                                                                                                                                                                                                                                                                                      - • ×
            16 10:34:28 karmic avahi-daemon[600]
                                                                                                                                    New relevant interface eth0.IPv4 for mDNS
 Apr
                                                                                                                                    Registering new address record for 10.0.2.15 on eth0.IPv4.
            16 10:34:28 karmic avahi-daemon[600]
                                                                                                                                  Kegistering new address record for 10.0.2.15 on eth0.1PV4.
Withdrawing address record for 10.0.2.15 on eth0.
Leaving mDNS multicast group on interface eth0.1Pv4 with address 10.0.2.15.
Interface eth0.1Pv4 no longer relevant for mDNS.
Joining mDNS multicast group on interface eth0.1Pv4 with address 10.0.2.15.
New relevant interface eth0.1Pv4 for mDNS.
 Apr
Apr
Apr
            16 10:34:28 karmic avahi-daemon[600]
            16 10:34:28 karmic avahi-daemon[600]
16 10:34:28 karmic avahi-daemon[600]
16 10:34:28 karmic avahi-daemon[600]
 Apr
 Apr
            16 10:34:28 karmic avahi-daemon[600]
            16 10:34:28 karmic avahi-daemon[600]: New relevant interface eth0.IPv4 for mNNS.
16 10:34:28 karmic avahi-daemon[600]: Registering new address record for 10.0.2.15 on eth0.IPv4.
16 10:34:28 karmic declient: bound to 10.0.2.15 -- renewal in 41345 seconds.
16 10:35:21 karmic decimal: [197517.88323] usb 1-1: USB disconnect, address 6
16 10:35:21 karmic dernel: [19759.128128] atkbd.c: Spurious NAK on isa0060/serio0. Some program might be trying access hardware directly.
16 10:36:37 karmic kernel: [197637.198274] atkbd.c: Spurious NAK on isa0060/serio0. Some program might be trying access hardware directly.
16 10:36:37 karmic kernel: [197657.198274] atkbd.c: Spurious NAK on isa0060/serio0. Some program might be trying access hardware directly.
16 10:37:38 karmic kernel: [197696.475287] atkbd.c: Spurious NAK on isa0060/serio0. Some program might be trying access hardware directly.
16 10:37:38 karmic kernel: [197696.475287] atkbd.c: Spurious NAK on isa0060/serio0. Some program might be trying access hardware directly.
 Ap
 Apr
 Apr
Apr
00] /var/log/syslog
                                                                                                                                                                                                                                                                                                                                                                             34KB - 2010/04/16 10:40:03
```

Figure 4: Red alert: MultiTail color highlights keywords on the basis of custom color schemes.



O Termin	
83.142.228.14 [14/Apr/2010:12:19:40 +0100] "GET	[Wed Apr 14 20:01:14 2010] [error] [client 83.142.228.
/robots.txt HTTP/1.0" 404 362 "-" "msnbot/2.0b (+htt	<pre>14] File does not exist: /var/www/prx2.php</pre>
p://search.msn.com/msnbot.htm)"	[Wed Apr 14 20:01:16 2010] [error] [client 83.142.228.
83.142.228.14 [14/Apr/2010:12:42:43 +0100] "GET	<pre>14] File does not exist: /var/www/virtual/debian.org/i</pre>
<pre>/picture archive/irland/irland sommer2001/0917/0917</pre>	nternational/l10n/po-debconf/ast.en.html/phpmyadmin/se
063_thumb.jpg HTTP/1.0" 404 416 "-" "Googlebot-Image	rver_status.php
/1.0"	[Wed Apr 14 20:01:16 2010] [error] [client 83.142.228.
83.142.228.14 [14/Apr/2010:13:15:49 +0100] "GET	<pre>14] File does not exist: /var/www/virtual/debian.org/i</pre>
<pre>/picture_archive/irland/irland_sommer2001/0914/0914_</pre>	nternational/l10n/po-debconf/phpmyadmin
001.jpg HTTP/1.0" 404 410 "-" "Googlebot-Image/1.0"	[Wed Apr 14 20:01:17 2010] [error] [client 83.142.228.
83.142.228.14 [14/Apr/2010:13:32:24 +0100] "GET	14] File does not exist: /var/www/virtual/debian.org/i
<pre>/picture_archive/irland/irland_sommer2001/0914/0914_</pre>	nternational/l10n/phpmyadmin
060_thumb.jpg HTTP/1.0" 404 416 "-" "Googlebot-Image	[Wed Apr 14 20:01:17 2010] [error] [client 83.142.228.
/1.0"	14] File does not exist: /var/www/virtual/debian.org/i
83.142.228.14 [14/Apr/2010:13:48:55 +0100] "GET	nternational/phpmyadmin
<pre>/picture_archive/irland/irland_sommer2001/0917/0917_</pre>	[Wed Apr 14 20:01:17 2010] [error] [client 83.142.228.
047.jpg HTTP/1.0" 404 410 "-" "Googlebot-Image/1.0"	14] File does not exist: /var/www/virtual/debian.org/p
83.142.228.14 [14/Apr/2010:14:22:02 +0100] "GET	hpmyadmin
<pre>/picture_archive/irland/irland_sommer2001/0917/0917_</pre>	01] /var/log/apache2/error.log
023_thumb.jpg HTTP/1.0" 404 416 "-" "Googlebot-Image	51.241.22: hostname 190-51-241-22.speedy.com.ar verifi
/1.0"	cation failed: Name or service not known
83.142.228.14 [14/Apr/2010:14:48:18 +0100] "GET	Apr 14 20:04:36 free postfix/smtpd[319]: connect from
/robots.txt HTTP/1.0" 404 362 "-" "msnbot/2.0b (+htt	unknown[190.51.241.22]
p://search.msn.com/msnbot.htm)"	Apr 14 20:04:38 free postfix/smtpd[319]: NOQUEUE: reje
83.142.228.14 [14/Apr/2010:14:51:39 +0100] "GET	ct: RCPT from unknown[190.51.241.22]: 504 5.5.2 <santi< th=""></santi<>
/picture_archive/irland/lbw2002/0830/0830_088.jpg HT	ago-5d8ce0>: Helo command rejected: need fully-qualifi
TP/1.0" 404 400 "http://maennerseiten.de/harry_potte	ed hostname; from=<@gmail.com> to=<=doingflumed
r/yabbse/index.php?topic=42628.0" "Mozilla/5.0 (Wind	s.com> proto=ESMTP helo= <santiago-5d8ce0></santiago-5d8ce0>
ows; U; Windows NT 5.1; de; rv:1.9.1.3) Gecko/200908	Apr 14 20:04:38 free postfix/smtpd[319]: lost connecti
24 Firefox/3.5.3"	on after DATA (0 bytes) from unknown[190.51.241.22]
83.142.228.14 [14/Apr/2010:15:08:36 +0100] "GET	Apr 14 20:04:38 free postfix/smtpd[319]: disconnect fr
/robots.txt HTTP/1.0" 404 362 "-" "msnbot/2.0b (+htt	om unknown[190.51.241.22]
p://search.msn.com/msnbot.htm)"	Apr 14 20:04:42 free postfix/smtpd[485]: warning: 190.
83.142.228.14 - [14/Apr/2010:15:09:15 +0100] "GET	51.241.22: hostname 190-51-241-22.speedy.com.ar verifi
/picture_archive/irland/uk_eire_april2003/index.php	cation failed: Name or service not known
HTTP/1.0" 404 402 "-" "msnbot/2.0b (+http://search.m	Apr 14 20:04:42 free postfix/smtpd[485]: connect from
sn.com/msnbot.htm)"	unknown[190.51.241.22]
00] /var/log/apache2/huhnix_access.log	02] /var/log/syslog 8MB - 2010/04/14 20:04:42

Figure 5: MultiTail can track multiple logfiles at the same time. Users can arrange the subwindows to meet their own needs.

combine logs and related program output. If you plan to modify the system and want to monitor the effect quickly and easily in the logfiles, pressing the Enter key gives you an additional overview. MultiTail then creates a thick red line with the date and time in all of its windows – a useful dividing line between the before and after states. Critics might argue that MultiTail is overkill, in that most of its functions are covered by legacy Unix tools, but the flexible view options are impressive when you have found the perfect setup.

# Good Wood

All three of the programs investigated fulfill their tasks satisfactorily. If you just

### **MULTITAIL HANDS ON**

The following two examples show how MultiTail can quickly help administrators with analysis and troubleshooting. In the first case, the administrator uses the viewer to investigate a web server that seems to be having problems accessing various pages. The administrator launches MultiTail in a large terminal window for a better overview with the use of the following command:

```
multitail -sw 100,20 /var/log/apache2/access_log -I /var/log/apache2/error_log
    -L "tcpdump -q -i lo port http" -kS 'TCP (.*:http.*)$'
    -ev '^COMMAND' -l "lsof -r l -i TCP:http"
```

The larger part of the window now displays the web server messages combined with the TCP packets that are sent. The narrow column on the right shows whether the web server is actually listening on its assigned port. You can easily see that the web server doesn't send any data if a certain page is in the referrer. The admin can now check the referrer's spam settings to see if they are restrictive.

The second example shows MultiTail using a script to include a filter. The script tells the viewer to display the calendar week and the weekday name. The script itself (weekday . rb) is given as Listing 1. The MultiTail command line for this is:

multitail -o 'convert:weekday:script:./weekday.rb:^([[:space:]]\*[[:alnum:]]{,3}
+[[:alnum:]]{,3} +..:..)' -cv weekday /var/log/syslog

Of course, MultiTail will work with Bash, Perl, or other scripting languages, as long as they are executable.

need a quick view of your logs, the Gnome System Log Viewer would be the right choice. The viewer focuses on the bare necessities, without cluttering the screen with needless colorful icons or too much information. The only drawback is the extended launch times, which is a factor because the tool updates the view between each change.

KSystemLog has useful highlighting and, above all, the ability to organize multiple logfiles in tabs. However, it is a pity that the tool doesn't remember the logfile tabs after quitting. This actually makes it useless for power users, but it will provide good service if you simply want to take a closer look behind the drapes from time to time.

MultiTail closes this gap and combines the frugality of

the Gnome tool with the flexibility of the KDE viewer. Its interactive controls take some getting used to, but the tool impresses with the ability to store settings, a choice of view modes, and its ability to cooperate with external programs and scripts.

### INFO

- [1] KSystemLog: http://ksystemlog. forum-software.org
- [2] Gnome System Log Viewer: http:// library.gnome.org/users/ gnome-system-log
- [3] MultiTail: http://www.vanheusden. com/multitail/
- [4] Examples of MultiTail command lines: http://www.vanheusden.com/ multitail/examples.html

# AUTHOR

Andrej Fink lives in Vienna, where he is studying mathematics at the Vienna University of Technology. Linux has been his choice of operating system since 1999. He is the sys admin for various organizations and is currently exploring virtualization, configuration management, and behavior-driven infrastructure, all of which generate a huge number of logs.