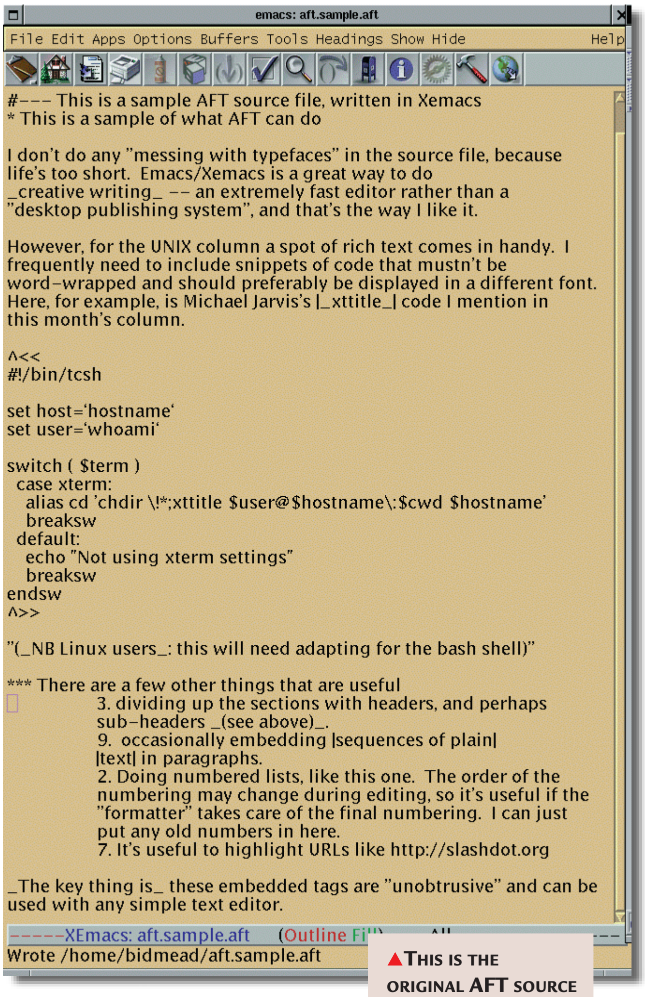
Mad as hatters

Everyone's wearing Red Hat these days, from BestCrypt to the Queen herself, says Chris Bidmead.


emacs: aft.sample.aft
File Edit Apps Options Buffers Tools Headings Show Hide Help

```
#--- This is a sample AFT source file, written in Xemacs
* This is a sample of what AFT can do

I don't do any "messing with typefaces" in the source file, because
life's too short.  Emacs/Xemacs is a great way to do
_creative writing_ -- an extremely fast editor rather than a
"desktop publishing system", and that's the way I like it.

However, for the UNIX column a spot of rich text comes in handy.  I
frequently need to include snippets of code that mustn't be
word-wrapped and should preferably be displayed in a different font.
Here, for example, is Michael Jarvis's |_xttitle_| code I mention in
this month's column.

^<<
#!/bin/tcsh

set host=`hostname`
set user=`whoami`

switch ( $term )
 case xterm:
  alias cd 'chdir \!*;xttitle $user@$hostname\:$cwd $hostname'
  breaksw
 default:
  echo "Not using xterm settings"
  breaksw
endsw
^>>

"(_NB Linux users_: this will need adapting for the bash shell)"

*** There are a few other things that are useful
            3. dividing up the sections with headers, and perhaps
            sub-headers _(see above)_.
            9.  occasionally embedding |sequences of plain|
            |text| in paragraphs.
            2. Doing numbered lists, like this one.  The order of the
            numbering may change during editing, so it's useful if the
            "formatter" takes care of the final numbering.  I can just
            put any old numbers in here.
            7. It's useful to highlight URLs like http://slashdot.org

_The key thing is_ these embedded tags are "unobtrusive" and can be
used with any simple text editor.
-----XEmacs: aft.sample.aft      (Outline Fi
Wrote /home/bidmead/aft.sample.aft
```

▲This is the original AFT source as written in Emacs

Having installed Mandrake Linux version 6, Adam Webb <oddweb@clara.co.uk> reports that he's 'perplexed and disappointed at just how difficult it is to work with'.

His ire seems to be directed against Linux in general – it's actually a tribute to Mandrake that after trying other distributions this is the one he's managed to install. His chief problem seems to be running into 'access denied' error messages while trying to install new KDE themes. 'Personally I wouldn't mess with any of this stuff until you've covered the fundamentals,' I suggested. Tweaking the GUI can be a lot of fun, but not if file and directory permissions are a hurdle you don't know how to leap.

If you're having similar problems you might like to take a look at http://perlfect.com/articles/chmod.shtml, which gives a useful overview of how permissions for users and groups apply to files and directories.

■ Samba: a footnote

By the way, within hours of filing my last column I discovered the solution to my problems getting the Samba Web Administration Tool (SWAT) up and running on my system. For some reason not mentioned in the documentation, it doesn't like you to have an /etc/smb.conf file in place already, and insists that you start afresh.

■ Name that terminal

I always seem to end up working with a large number of different Xterminals scattered around my workspace, some iconised, some open, some invisibly inhabiting other virtual screens. Finding the one that's running, say, Telnet to my router, can take a while.

Most X implementations on Unix allow you to pop up some kind of window selection menu, to let you bring any particular running program into focus. But the menu entries for your various Xterms are normally all the same, because all the windows are called 'Terminal' or 'Xterm'.

You can get round this by naming each new window as you create it. The command xterm -name PerlDev will create a new window called 'PerlDev' which should turn out to be named as such on any workspace menu you pop up. Other terminal emulators, such as Gnome Terminal, have a similar command.

But in real life you often don't know in advance what you're going to end up doing in an Xterm window at the time you create it. You can rename an already created window, but it means sending a nasty string of unmemorable escape codes, and it's generally too much trouble.

This tiny utility – named xttitle – allows you to rename an Xterm on the fly

To the rescue comes Michael Jarvis <michael@jarvis.com> with a snippet of C code you can download from his website at www.jarvis.com/xttitle. This tiny utility – named xttitle – makes it easy to rename an Xterm on the fly. One simple use for xttitle that Michael suggests is to create an alias for the cd command that also runs xttitle with $PWD as a parameter, thus embedding the current directory name into the window title.

■ Linux gets girls (or vice versa)

My experiences of attending various Linux and Unix IRL (In Real Life) meetings suggest that this isn't necessarily a great way to meet girls. There's a lot of long hair about (balding Bid notes enviously), but 99 per cent of it sprouts from decidedly male techheads.

But that may be changing. Of course there have long been some key women activists on the Unix front – the valuable general Unix resource site at www.geekgirl.com, run by Jennifer Myers, has been around for over half a decade. And of course there's Nitrozac who does the Y2K comic strip at www.geekculture.com. Now there's a new (Linux-specific) distaff site at www.linuxchix.org. A #linuxchix IRC channel has also been set up on irc.gimp.org.

But the biggest story under this heading has to be the news that a Very Important Person of the female persuasion has switched from Solaris to Linux as the engine behind Her Royal Website. Yes, the Queen's running Apache on Red Hat. The story comes from Netcraft, which regularly sweeps the web to determine who's using what in the way of operating systems and web servers. Web users can also use Netcraft's site to check individual systems – try: www.netcraft.com/whats/?host=www.royal.gov.uk.

■ Creep into the crypts

A year has gone by since I talked about CFS, the cryptographic filesystem developed by AT&T Labs employee Matt Blaze. Meanwhile the absurd US restrictions on crypto software have been reviewed by Congress, but it's still all a real mess as far as I can make out. However, you can download CFS freely from Replay's Amsterdam site at www.replay.com. The site seems to have had a heavy attack of RedHatness since I visited it last year, and is now called Red Hat Crypto, which is a bit alarming, because CFS is cross-platform Unix code. It remains so, but it looks as though you now need a Red Hat Linux system, or at least a system that supports RPM packages, to get at the source code. Nice one, Red Hat.

Since I last covered this subject, an interesting newcomer has popped up on the crypto filesystem scene. BestCrypt, devised by the Finnish company Jetico at www.jetico .com is a commercial product, but Linux users can download and use it for free if they observe the rather liberal licence terms.

A female VIP has switched to Linux as the engine behind Her Royal Website

While Windows users have to pay around $90 (£56.25) for the package, the software is freely available on Linux as easy-to-compile source (you don't need to be a programmer as long as you can type 'make' at the command line).

Whereas CFS keeps its encrypted data as a directory and so can expand dynamically as you add more files (up to the physical limitations of your partition, of course), BestCrypt's filesystem is built inside a single file. This means you need to decide in advance how much data space to set aside. The advantage is that BestCrypt is easier to set up and manage, and the encrypted data can easily be backed up, or even sent by email or filed on an FTP site, readable only by someone who has the key.

Files are attached as filesystems using loop devices that the BestCrypt installation creates automatically for you when you run make (take a look inside the Makefile to get an idea how this is done). It's sometimes useful to use loop device filesystems without crypto – as a way of putting an ext2 filesystem inside a dedicated DOS partition, for example. In fact, Andrew Bishop, <amb@gedanken .demon.co.uk>, has written a Loopback Root Filesystem mini-HOWTO about exactly this, which I found included with my Mandrake 6 distribution, and is also available online at, for example, www.gedanken.demon.co.uk/linux/looproot.html.

Preparing the file for encryption, as well as mounting and unmounting it as a loopback device, is all taken care of by the BestCrypt utility bctool. You create the initial file with a command line something like this:

```
bctool new -a blowfish -s ↙
20M -d 'Mind your own ↙
business' /crypt/encrypted
```

The file now needs to be formatted using the filesystem of your choice:

```
bctool format -t ext2 ↙
/crypt/encrypted
```

(*Key: ↙ code string continues*)

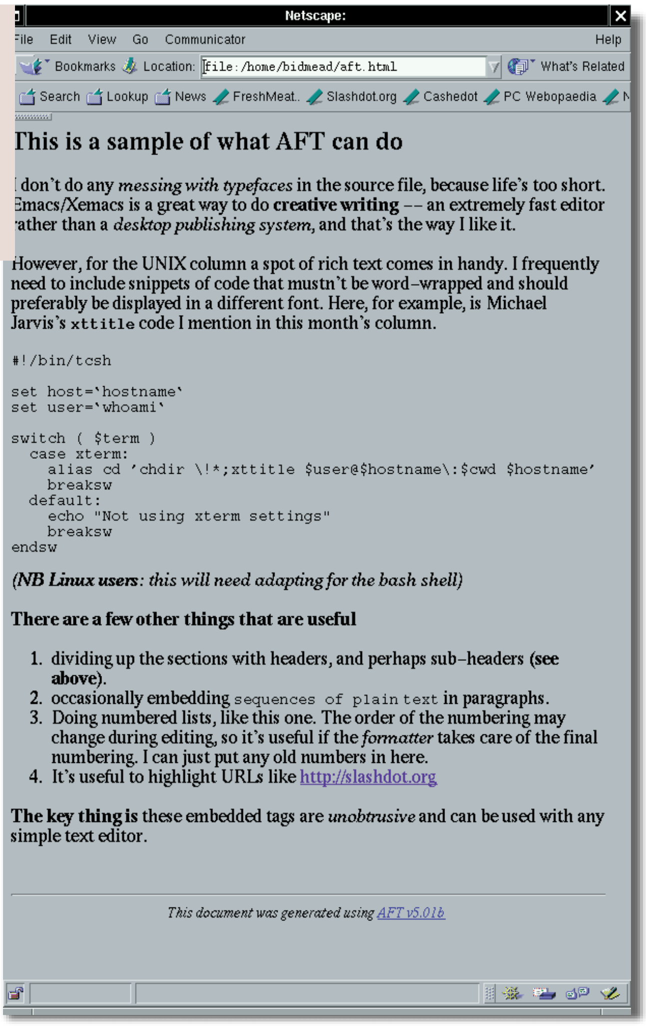
It's a good idea to choose ext2, as the default -t msdos restricts any files you subsequently write to the filesystem to the usual 8.3 DOS file format. But be aware that in some circumstances – for example, if you exit from Linux without unmounting the BestCrypt file – you can corrupt the filesystem, and there's no encrypted equivalent of fsck to repair it, at least not at the time of writing.

Now it's time to mount the encrypted filesystem for use. Assuming you've created an empty mountpoint at, say ~/bc, the command is:

```
bctool mount ↙
/crypt/encrypted ~/bc
```

At each of these last two stages bctool will ask you to repeat the passphrase you

▶This is the HTML version of the AFT source displayed using Netscape. The key point is that the AFT source is readily legible, but contains minimal tags that AFT uses to create the HTML


Netscape:
File Edit View Go Communicator Help
Bookmarks Location: file:/home/bidmead/aft.html What's Related
Search Lookup News FreshMeat.. Slashdot.org Cashedot PC Webopaedia

This is a sample of what AFT can do

I don't do any *messing with typefaces* in the source file, because life's too short. Emacs/Xemacs is a great way to do **creative writing** –– an extremely fast editor rather than a *desktop publishing system*, and that's the way I like it.

However, for the UNIX column a spot of rich text comes in handy. I frequently need to include snippets of code that mustn't be word–wrapped and should preferably be displayed in a different font. Here, for example, is Michael Jarvis's `xttitle` code I mention in this month's column.

```
#!/bin/tcsh

set host=`hostname`
set user=`whoami`

switch ( $term )
  case xterm:
    alias cd 'chdir \!*;xttitle $user@$hostname\:$cwd $hostname'
    breaksw
  default:
    echo "Not using xterm settings"
    breaksw
endsw
```

*(**NB Linux users**: this will need adapting for the bash shell)*

There are a few other things that are useful

1. dividing up the sections with headers, and perhaps sub–headers (**see above**).
2. occasionally embedding `sequences of plain text` in paragraphs.
3. Doing numbered lists, like this one. The order of the numbering may change during editing, so it's useful if the *formatter* takes care of the final numbering. I can just put any old numbers in here.
4. It's useful to highlight URLs like http://slashdot.org

The key thing is these embedded tags are *unobtrusive* and can be used with any simple text editor.

This document was generated using AFT v5.01b were invited to enter when you ran ‘bctool new’. If you get this passphrase wrong bctool shrugs you off. The only unguarded command bctool accepts is:

```
bctool info /crypt/encrypted
```

This returns details of the filesystem type, the encryption method and the -d description string you entered when you created the file. As anyone can collect these interesting details without a password, security is compromised to some extent.

BestCrypt offers three block encryption options: Blowfish, DES and GOST. DES is the standard invented by IBM in the 1970s – in those days it was virtually uncrackable, but today its 56bit key size is vulnerable to a brute force attack if you found yourself on the wrong side of a government with a lot of resources, and is now officially limited to ‘unclassified information’. GOST is the Russian Federal standard, with a 128bit key that is thought to be pretty-well bullet-proof. Blowfish was devised in the mid-1990s as a secure, unpatented, and freely-available encryption algorithm.

Like GOST, the BestCrypt implementation of Blowfish uses a 128bit key, and it too is thought to be virtually uncrackable, with the advantage that it's considerably faster than both GOST and DES.

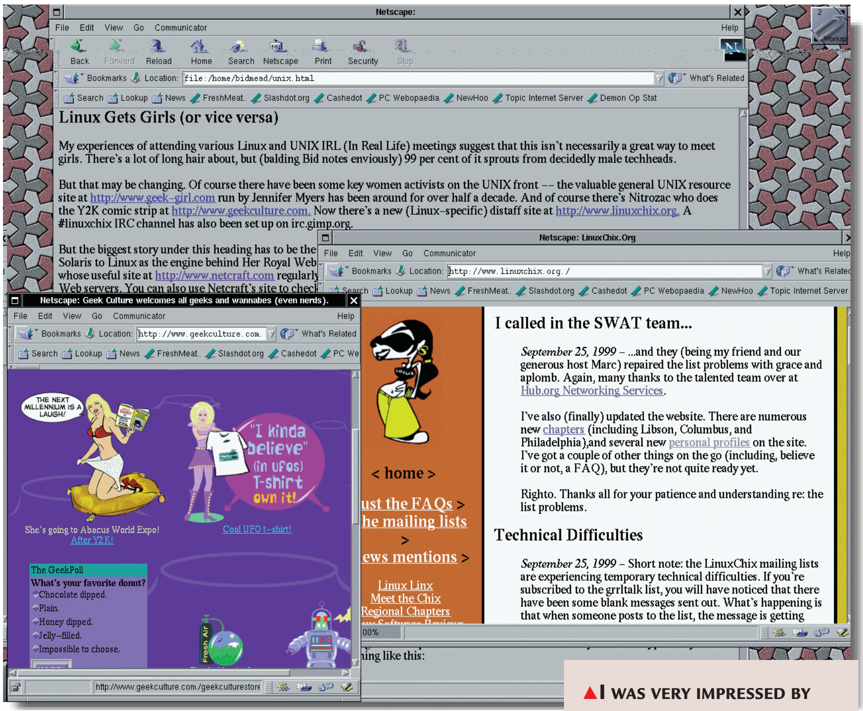
Almost Free Text

I've just stumbled across a very exciting piece of software that, it turns out, has been hanging around the Internet for ages. It's very simple stuff, so I need to explain why I'm so exited about it.

What you want is a way of using easily-written tags that don't offend the eye

I write this column in the same way as I write features and other articles, using the Emacs text editor. I've explained in previous columns why I keep coming back to Emacs after messing with a range of different word processors, so I won't go into that again here (but do write in if you're curious). The plain text that Emacs creates is fine for pretty much everything except this column, where I do need a certain amount of font changing for things such as examples and snatches of code.

So I've been filing this column in Microsoft .rtf format, using Edit on my NeXTStep machine to add the final touches of rich text. This kind of formatting by hand is a bit tedious, and I've been meaning to write an awk or Perl script to automate some of it. For example, I begin section headers with a couple of asterisks and it would be nice to turn these automatically into bold, larger text. And when I need a chunk of code that must be protected against word-wrapping it would be nice to put a tag in the text stream to indicate this. Emphasis, indicated in a plain text file _like this_ should automatically be translated into real bold text.


Netscape:
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: file:/home/bidmead/unix.html What's Related
Search Lookup News FreshMeat.. Slashdot.org Cashedot PC Webopaedia NewHoo Topic Internet Server Demon Op Stat

Linux Gets Girls (or vice versa)

My experiences of attending various Linux and UNIX IRL (In Real Life) meetings suggest that this isn't necessarily a great way to meet girls. There's a lot of long hair about, but (balding Bid notes enviously) 99 per cent of it sprouts from decidedly male techheads.

But that may be changing. Of course there have been some key women activists on the UNIX front –– the valuable general UNIX resource site at http://www.geek–girl.com run by Jennifer Myers has been around for over half a decade. And of course there's Nitrozac who does the Y2K comic strip at http://www.geekculture.com. Now there's a new (Linux–specific) distaff site at http://www.linuxchix.org. A #linuxchix IRC channel has also been set up on irc.gimp.org.

But the biggest story under this heading has to be the Solaris to Linux as the engine behind Her Royal Web whose useful site at http://www.netcraft.com regularly Web servers. You can also use Netcraft's site to check

Netscape: LinuxChix.Org
File Edit View Go Communicator Help
Bookmarks Location: http://www.linuxchix.org/ What's Related
Search Lookup News FreshMeat.. Slashdot.org Cashedot PC Webopaedia NewHoo Topic Internet Server
< home >
ust the FAQs >
he mailing lists >
ews mentions >
Linux Linx
Meet the Chix
Regional Chapters

I called in the SWAT team...

September 25, 1999 – ...and they (being my friend and our generous host Marc) repaired the list problems with grace and aplomb. Again, many thanks to the talented team over at Hub.org Networking Services.

I've also (finally) updated the website. There are numerous new chapters (including Libson, Columbus, and Philadelphia),and several new personal profiles on the site. I've got a couple of other things on the go (including, believe it or not, a FAQ), but they're not quite ready yet.

Righto. Thanks all for your patience and understanding re: the list problems.

Technical Difficulties

September 25, 1999 – Short note: the LinuxChix mailing lists are experiencing temporary technical difficulties. If you're subscribed to the grrltalk list, you will have noticed that there have been some blank messages sent out. What's happening is that when someone posts to the list, the message is getting

Netscape: Geek Culture welcomes all geeks and wannabes (even nerds).
File Edit View Go Communicator Help
Bookmarks Location: http://www.geekculture.com. What's Related
Search Lookup News FreshMeat.. Slashdot.org Cashedot PC We
THE NEXT MILLENNIUM IS A LAUGH!
"I kinda believe" (in ufos) T-shirt own it!
She's going to Abacus World Expo!
After Y2K!
Cool UFO t–shirt!
The GeekPoll
What's your favorite donut?
Chocolate dipped.
Plain.
Honey dipped.
Jelly–filled.
Impossible to choose.
Fresh Air
http://www.geekculture.com./geekculturestore

▲I WAS VERY IMPRESSED BY THE FEATURE IN TODD CORAM'S AFT THAT HIGHLIGHTS URLS AND CONVERTS THEM INTO LIVE LINKS. THIS ALLOWS ME ACTIVELY TO CHECK EACH LINK IN MY COPY BEFORE I FILE IT

One way would be to write the column in SGML, or, more likely, HTML. Emacs has a mode to help you with this, but the tags look a bit ugly (although Emacs allows you to hide them) and it can get messy. What you want is a way of using very minimal, easily-written tags that don't offend the eye, but can be converted by a filter utility into full-blown HTML.

Todd Coram has written just such a filter. It's called Almost Free Text (AFT). A line beginning with one or more asterisks is converted into a header (the more asterisks the lower value the header) – which is great for me, because I've been doing headers like this for years, as Emacs uses the same indicators for its outlining feature. A line beginning with a tab is a literal, not-to-be-wrapped line and gets converted into a non-proportional font, which is perfect for code snippets. Emphasis is indicated by opening and closing the section with the underline character, just as I suggested above. Italics are similarly marked using a pair of single quote marks like this: ‘’.

There are a number of other (configurable) tag conventions, including an elementary way of doing tables. The AFT tags are all designed to intrude minimally on the visual appearance of the plain text source file. My favourite is that web addresses, like Todd's at www.pobox.com/˜tcoram automatically get converted into live anchors. Brilliant stuff, Todd.

PCW CONTACTS

Chris Bidmead welcomes your comments on the Unix column. Contact him via the PCW editorial office or email ***unix@pcw.co.uk***