Bitflipped

Blair Harrison
Kiwicon 666
November 2012

@trogs

Whoami

- Twitter.com/trogs
- http://jedi.school.nz

- Kiwicon 4 - Fibre optics talk
- Random internet research as and when I feel like it
- Not a security professional

What is bitflipping

- When 1s turn into 0s and vice versa inside computer memory probably due to cosmic rays
- Probably the cause of all those random crashes you've had and just shrugged off
- Consequences for DNS resolution, if your browser corrupts a page with domain names in it, or if you are served up a corrupted page, you could end up loading content from a different site
- DNS requests could also be corrupted on the way to the DNS server (any server in the chain)

DNS (is hard)

- DNS query (PC) ->
- -> DNS Forwarder (Router) ->
- -> Recursive DNS Server (ISP DNS Servers) ->
- -> Authoritative DNS Server (ns1.example.com)

Example

- trademe.co.nz
- t2ademe.co.nz
- tbademe.co.nz
- tzademe.co.nz
- tvademe.co.nz
- tpademe.co.nz
- tsademe.co.nz

- r 72 hex 01110010
- 2 32 hex 00110010

- r 72 hex 01110010
- R 52 hex 01010010

- r 72 hex 01110010
- b 62 hex 01100010

- r 72 hex 01110010
- z 7A hex 01111010

- r 72 hex 01110010
- v 76 hex 01110110

- r 72 hex 01110010
- p 70 hex 01110000

- r 72 hex 01110010
- s 73 hex 01110011

Trademe

- I bitflipped trademe.co.nz
- Got a few hits

- Set up DNS server and web server to also serve results for trademe.co.nz
- Got more hits

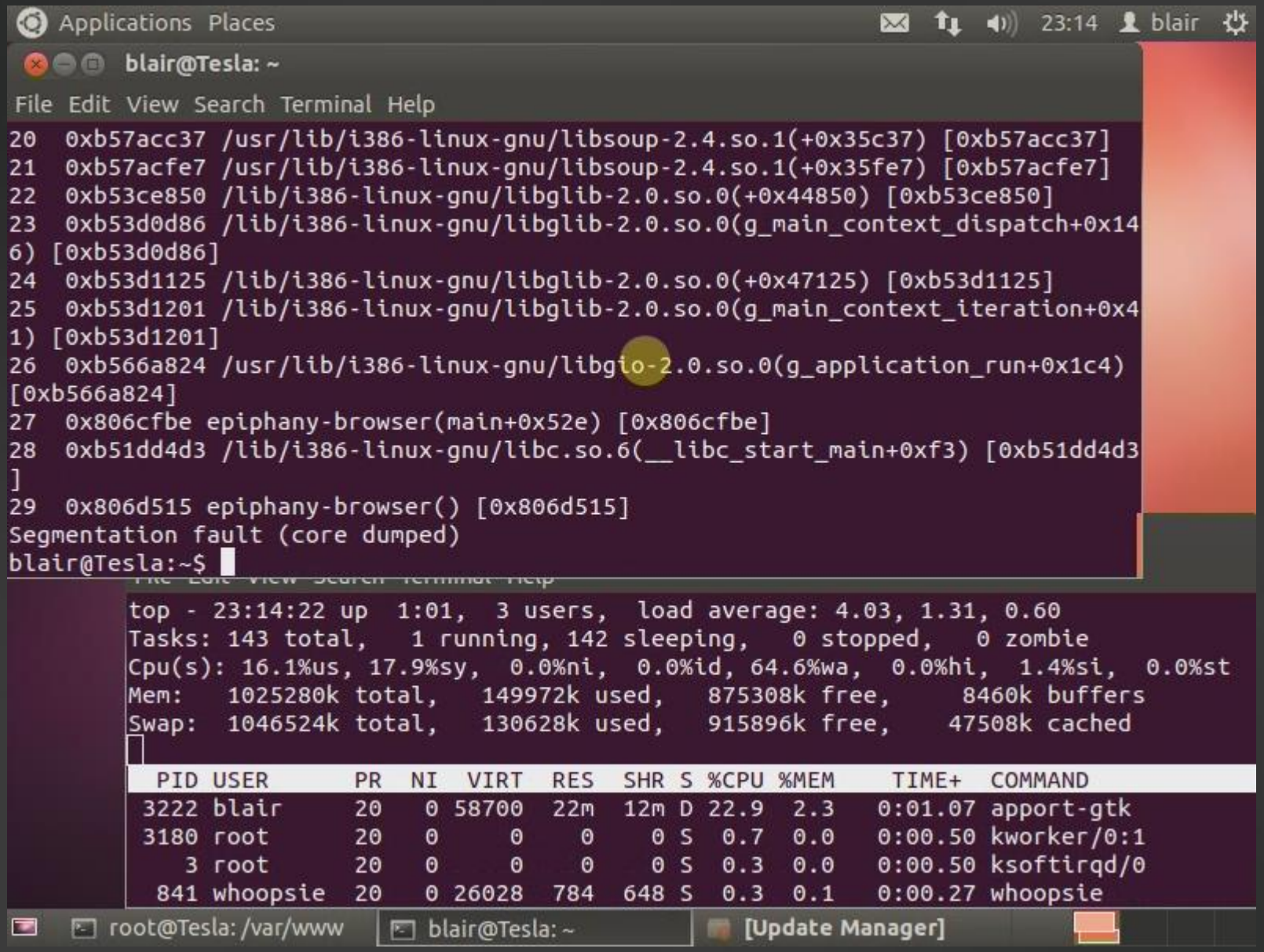
wtf

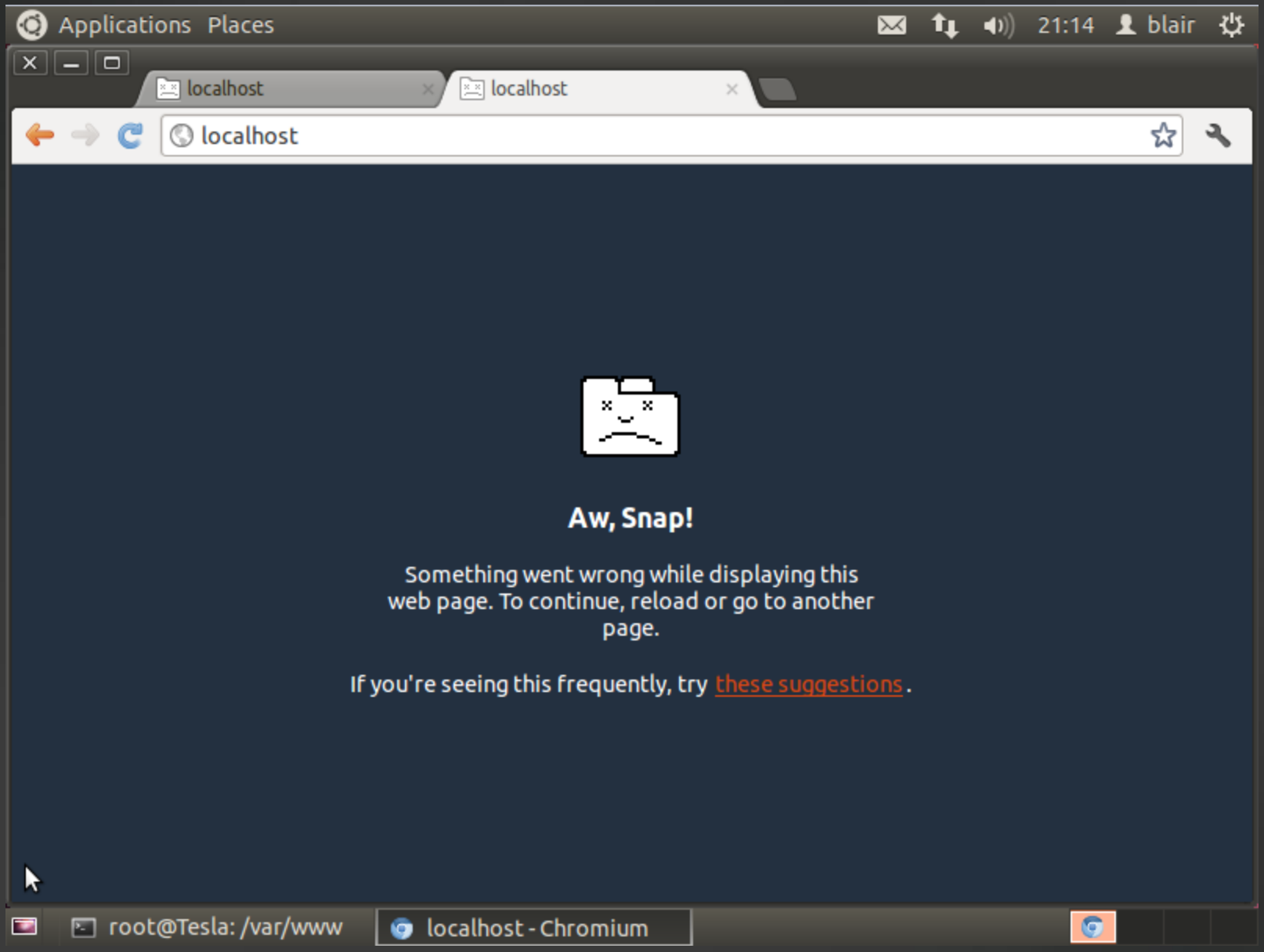
- The bitflipped domains have now expired
- Still getting hits on trademe.co.nz
- From 3 different IPs

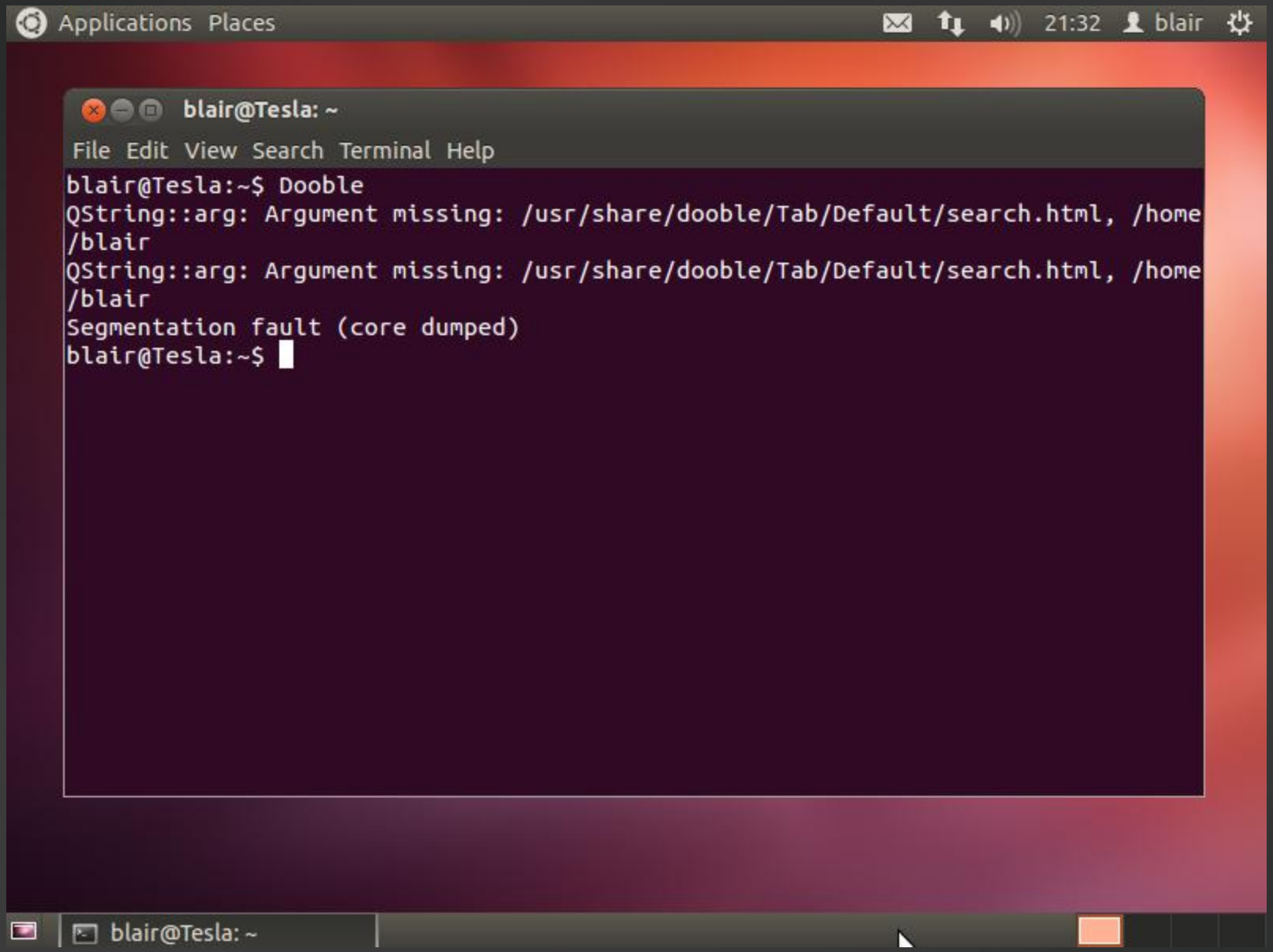
38	203.167.188.xxx
40	58.28.153.xxx
1707	203.109.198.xxx

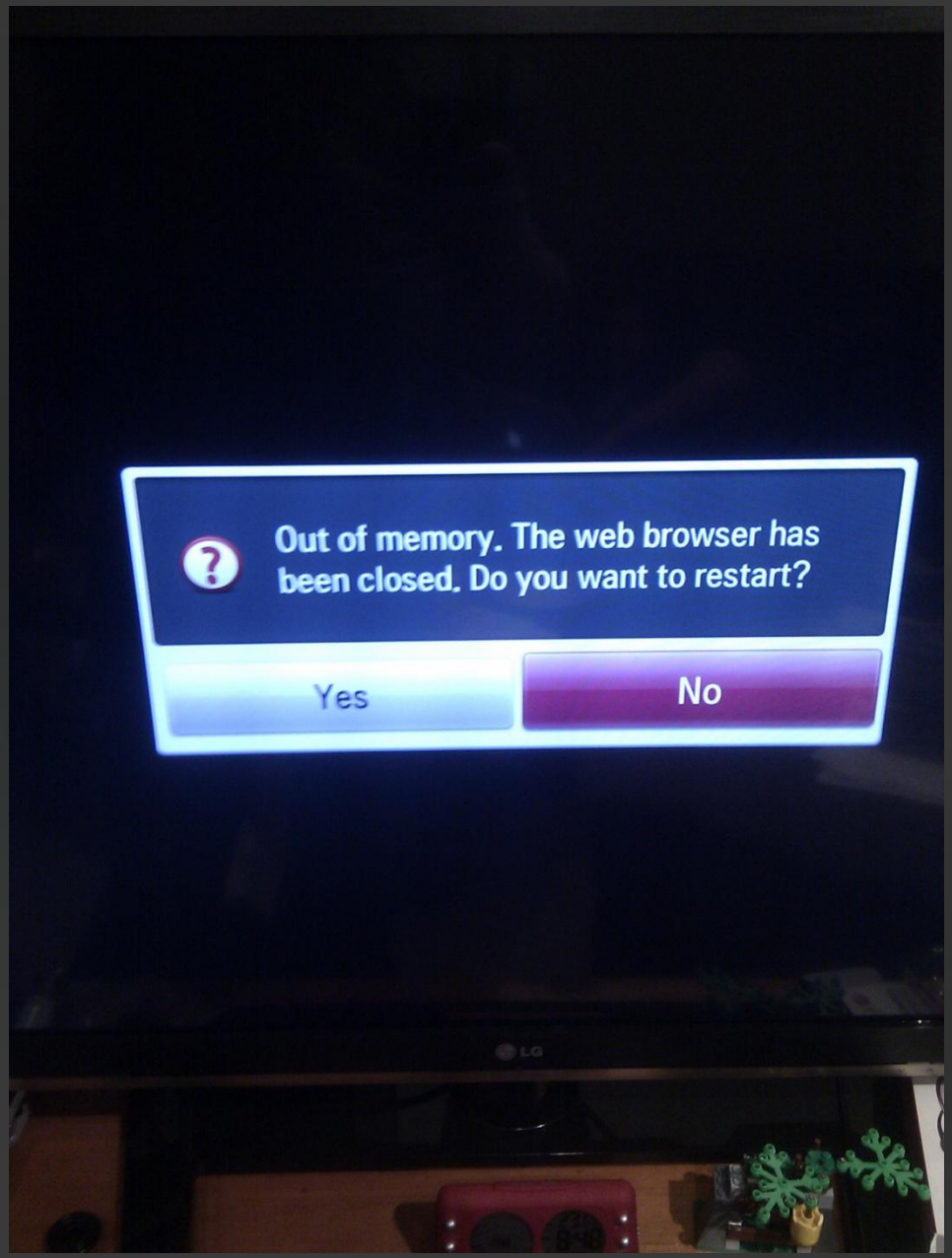
Favicon.ico

- As an aside, while I was looking at these logs I noticed everything seems to try and get favicon.ico
- Wonder if there's some fun to be had?
- Lets make favicon.ico 2GB in size. Surely the browser wouldn't download that much?


Applications Places
23:14
blair
blair@Tesla: ~
File Edit View Search Terminal Help
20 0xb57acc37 /usr/lib/i386-linux-gnu/libsoup-2.4.so.1(+0x35c37) [0xb57acc37]
21 0xb57acfe7 /usr/lib/i386-linux-gnu/libsoup-2.4.so.1(+0x35fe7) [0xb57acfe7]
22 0xb53ce850 /lib/i386-linux-gnu/libglib-2.0.so.0(+0x44850) [0xb53ce850]
23 0xb53d0d86 /lib/i386-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x14
6) [0xb53d0d86]
24 0xb53d1125 /lib/i386-linux-gnu/libglib-2.0.so.0(+0x47125) [0xb53d1125]
25 0xb53d1201 /lib/i386-linux-gnu/libglib-2.0.so.0(g_main_context_iteration+0x4
1) [0xb53d1201]
26 0xb566a824 /usr/lib/i386-linux-gnu/libgio-2.0.so.0(g_application_run+0x1c4)
[0xb566a824]
27 0x806cfbe epiphany-browser(main+0x52e) [0x806cfbe]
28 0xb51dd4d3 /lib/i386-linux-gnu/libc.so.6(__libc_start_main+0xf3) [0xb51dd4d3
]
29 0x806d515 epiphany-browser() [0x806d515]
Segmentation fault (core dumped)
blair@Tesla:~$
top - 23:14:22 up 1:01, 3 users, load average: 4.03, 1.31, 0.60
Tasks: 143 total, 1 running, 142 sleeping, 0 stopped, 0 zombie
Cpu(s): 16.1%us, 17.9%sy, 0.0%ni, 0.0%id, 64.6%wa, 0.0%hi, 1.4%si, 0.0%st
Mem: 1025280k total, 149972k used, 875308k free, 8460k buffers
Swap: 1046524k total, 130628k used, 915896k free, 47508k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
3222 blair 20 0 58700 22m 12m D 22.9 2.3 0:01.07 apport-gtk
3180 root 20 0 0 0 0 S 0.7 0.0 0:00.50 kworker/0:1
3 root 20 0 0 0 0 S 0.3 0.0 0:00.50 ksoftirqd/0
841 whoopsie 20 0 26028 784 648 S 0.3 0.1 0:00.27 whoopsie
root@Tesla: /var/www
blair@Tesla: ~
[Update Manager]


Applications Places
21:14
blair
localhost
localhost
localhost
Aw, Snap!
Something went wrong while displaying this web page. To continue, reload or go to another page.
If you're seeing this frequently, try these suggestions.
root@Tesla: /var/www
localhost - Chromium

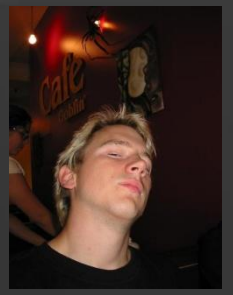

Applications Places
21:32 blair
blair@Tesla: ~
File Edit View Search Terminal Help
blair@Tesla:~$ Dooble
QString::arg: Argument missing: /usr/share/dooble/Tab/Default/search.html, /home
/blair
QString::arg: Argument missing: /usr/share/dooble/Tab/Default/search.html, /home
/blair
Segmentation fault (core dumped)
blair@Tesla:~$
blair@Tesla: ~


Out of memory. The web browser has been closed. Do you want to restart?
Yes
No

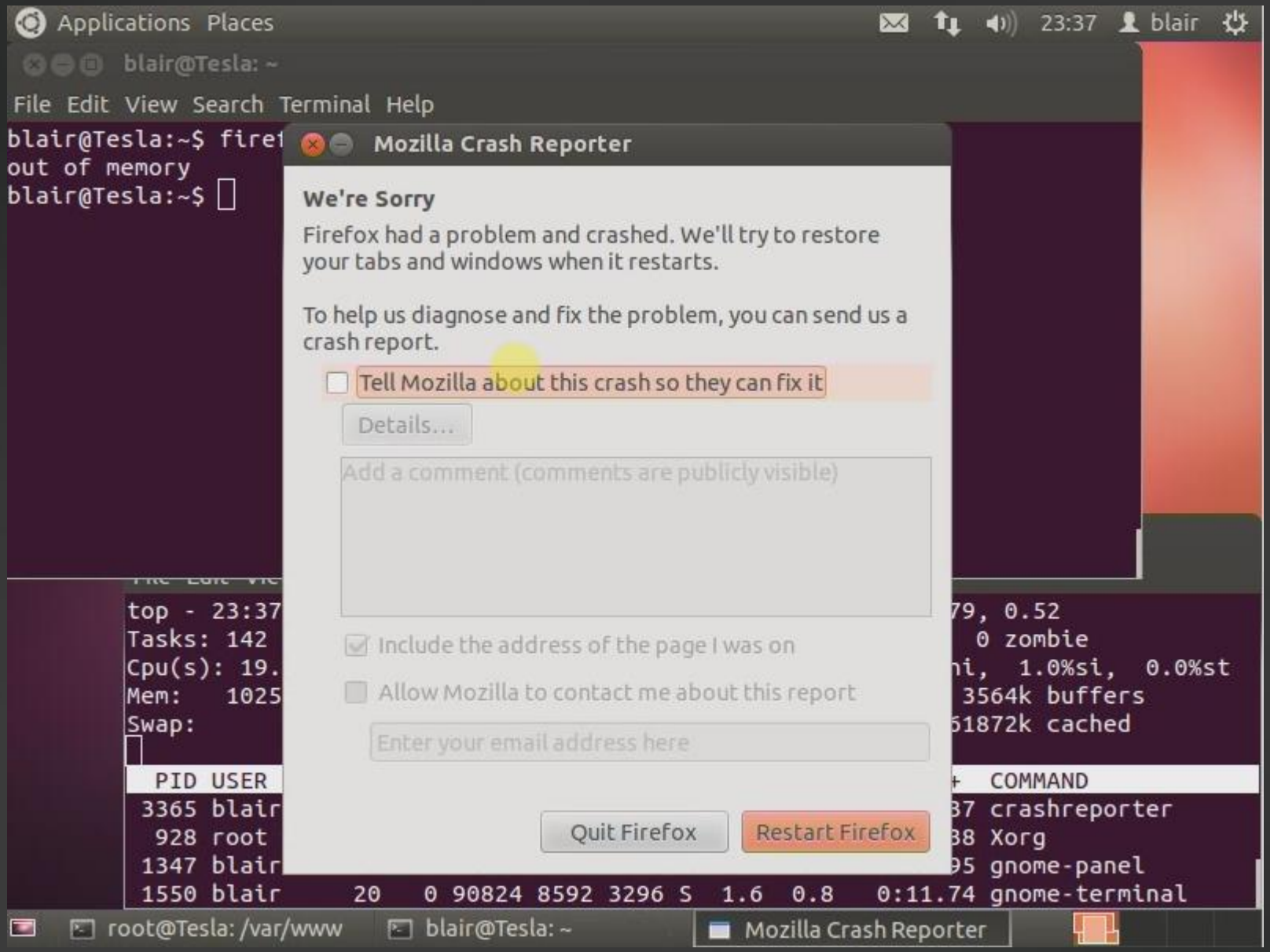
summary

- Epiphany browser segfaulted (oops)
- Chromium downloaded about 400MB of the file repeatedly then sadface'd the tab
- Dooble Segfaulted
- My LG TV ran out of memory

What about wpad.dat?



- So, surely after the wpad debacle everyone would have reviewed their wpad code, right?
- Lets make a 1GB wpad.dat file and point the browser configuration at it
- Surely the browser would ignore a broken 1GB wpad.dat?


Applications Places
23:37
blair
blair@Tesla: ~
File Edit View Search Terminal Help
blair@Tesla:~$ firef
out of memory
blair@Tesla:~$
Mozilla Crash Reporter
We're Sorry
Firefox had a problem and crashed. We'll try to restore your tabs and windows when it restarts.
To help us diagnose and fix the problem, you can send us a crash report.
Tell Mozilla about this crash so they can fix it
Details...
Add a comment (comments are publicly visible)
Include the address of the page I was on
Allow Mozilla to contact me about this report
Enter your email address here
Quit Firefox
Restart Firefox
top - 23:37
Tasks: 142
Cpu(s): 19.
Mem: 1025
Swap:
PID USER
3365 blair
928 root
1347 blair
1550 blair 20 0 90824 8592 3296 S 1.6 0.8 0:11.74 gnome-terminal
0 zombie
3564k buffers
51872k cached
COMMAND
crashreporter
Xorg
gnome-panel
root@Tesla: /var/www
blair@Tesla: ~
Mozilla Crash Reporter

IE

- IE will happily download about 1GB worth of wpad.dat with no issues
- It might use up a lot of ram, so your computer might end up being quite slow for a bit. Or lock up for a few minutes.
- Doesn’t seem to try re-downloading the file each launch like Firefox after it’s got it, at least not in the time period of my testing

Summary

- Browsers suck
- Some suck more than others
- Use Chrome
- Disable favicon support in your browser if possible
- Defcon 19 : Bitsquatting – Artem Dinaburg
- SSH timeouts due to broken router doing bitflipping - http://mina.naguib.ca/blog/2012/10/22/the-little-ssh-that-sometimes-couldnt.html

The End

- Thanks to everyone!