

Supporting Debian machines for friends and family

Notes and tricks from an amateur sysadmin

The logo for Debian 8, featuring the text "debian 8" in a white, sans-serif font. To the right of the text is a stylized white swirl or spiral graphic. The entire logo is set against a dark teal background with faint, light-colored geometric lines (circles and a vertical line) that create a grid-like pattern.

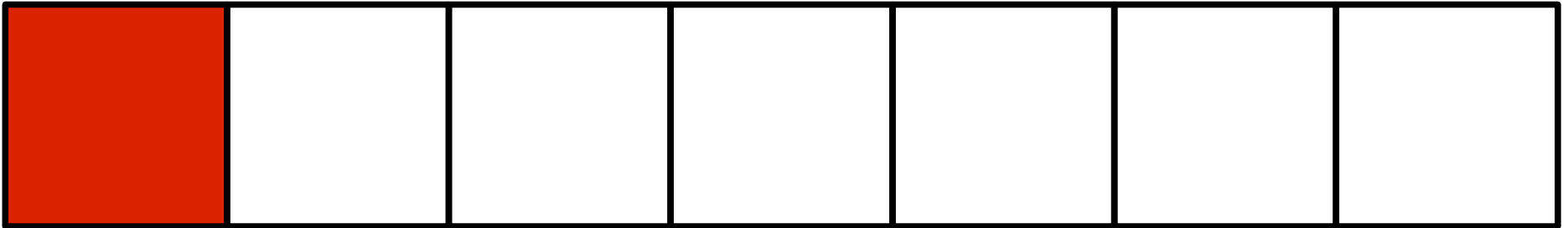
debian⁸

François Marier @fmarier
francois@debian.org

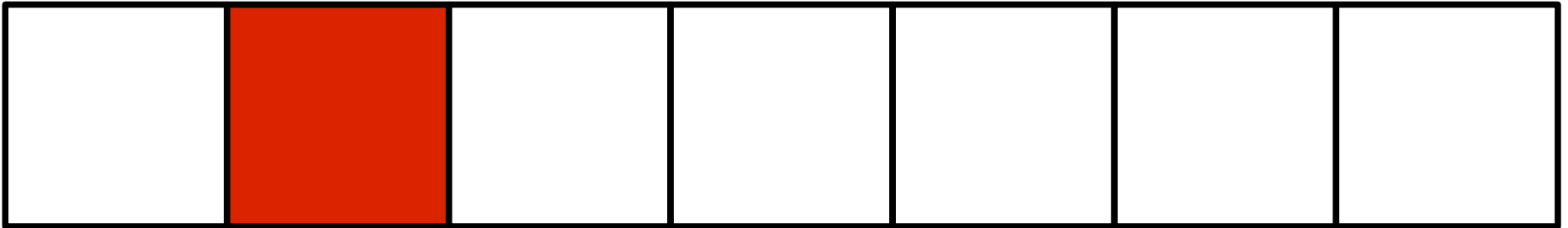
“providing an enjoyable computing environment so that they can fully experience the benefits of Free Software...”

“... without using up
all of our precious
spare time”

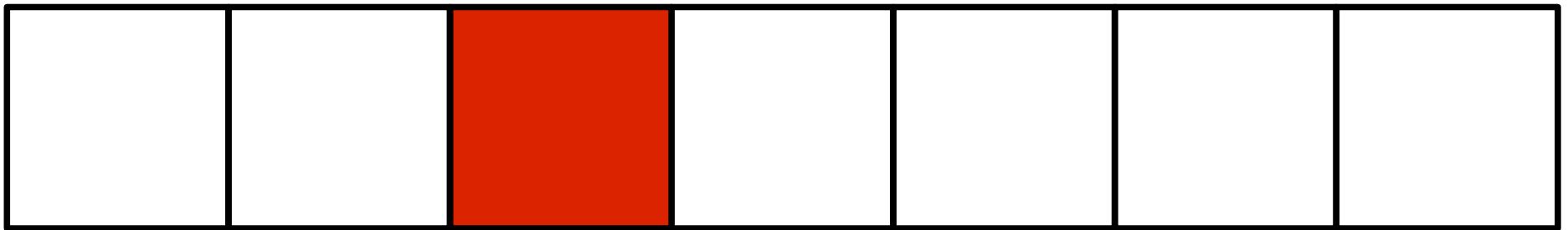
hardware



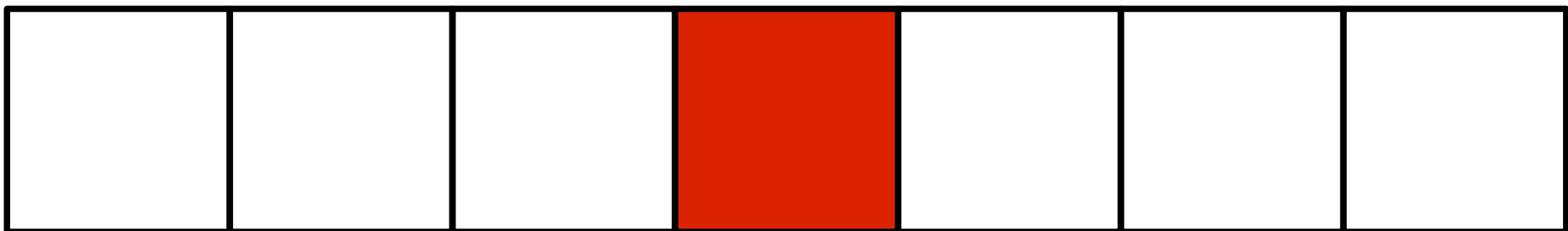
package updates



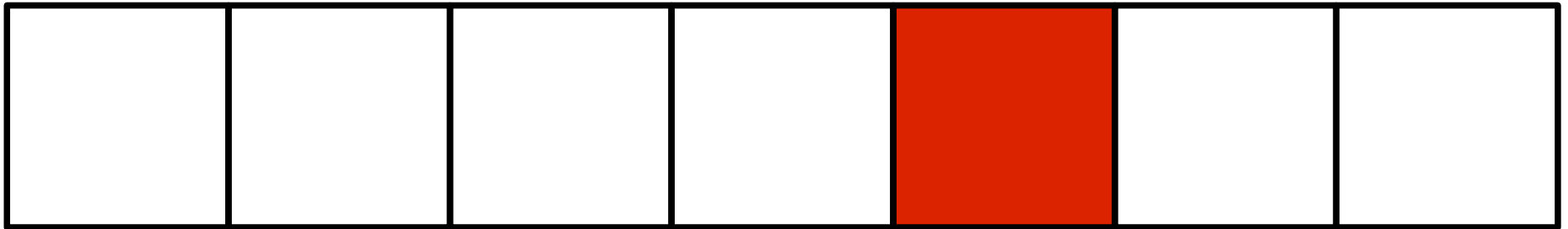
monitoring



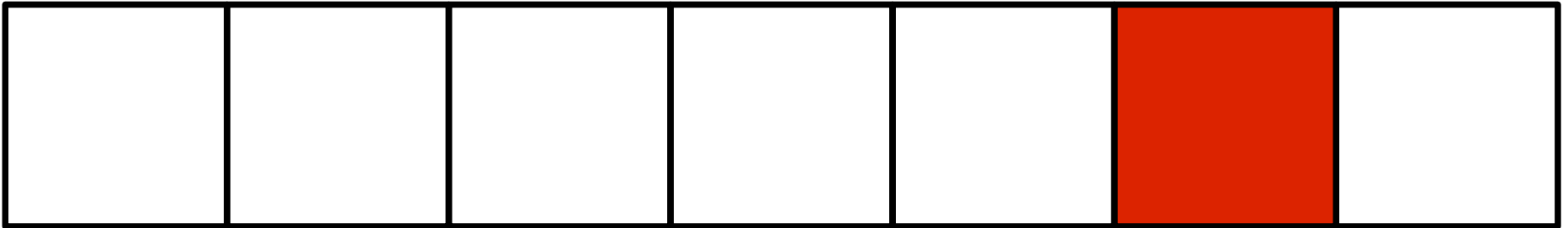
safety



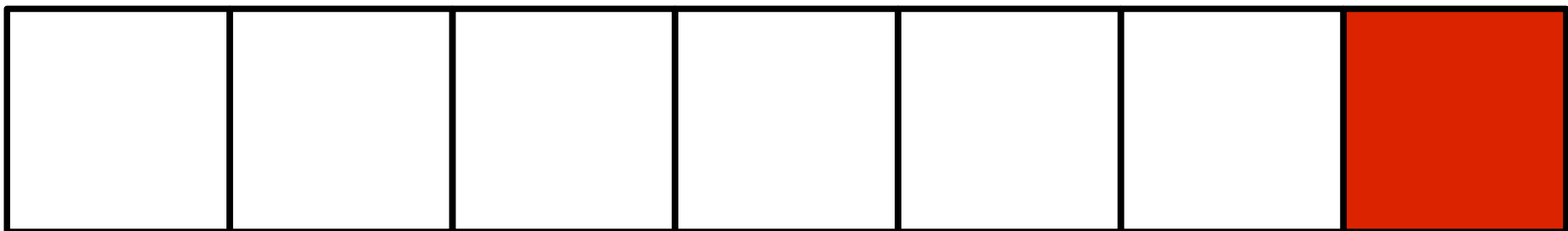
security



remote access



backups



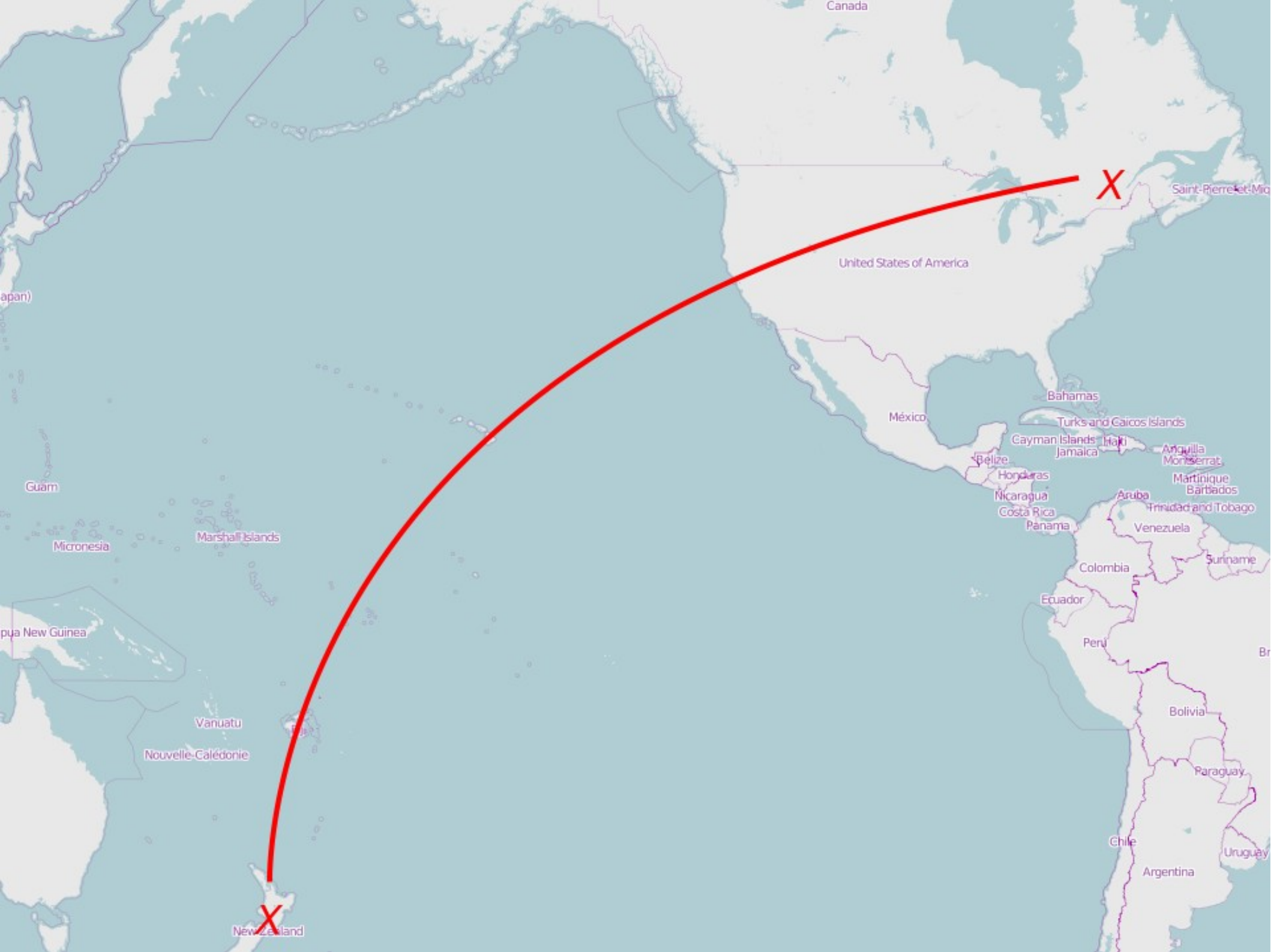
example

[

]







United States of America



Saint-Pierre-et-Mic

Bahamas

México

Turks and Caicos Islands

Gayman Islands

Jamaica

Haiti

Anguilla

Montserrat

Martinique

Barbados

Belize

Honduras

Nicaragua

Costa Rica

Panama

Aruba

Trinidad and Tobago

Venezuela

Colombia

Suriname

Ecuador

Perú

Bolivia

Paraguay

Chile

Argentina

Uruguay

New Zealand

Guam

Micronesia

Marshall Islands

Vanuatu

Nouvelle-Calédonie

Papua New Guinea

keflavik







akureyri

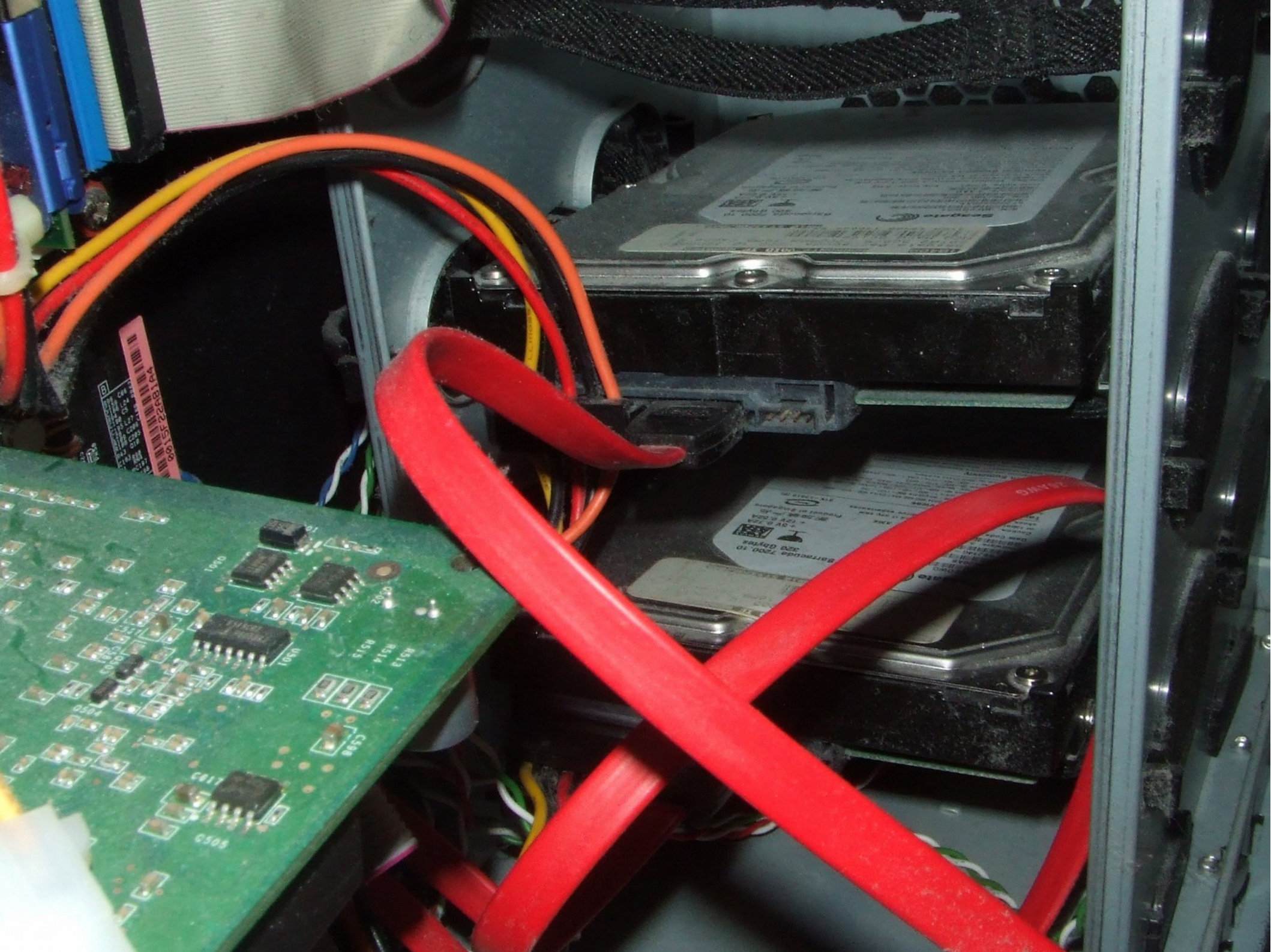




hardware

[====]

]





memtest86+

`badblocks -swo out /dev/sdX`

package updates

[=====

]

apticron

unattended-upgrades



deborphan

debfooster

debian-security-support

monitoring

[=====]

]

logcheck



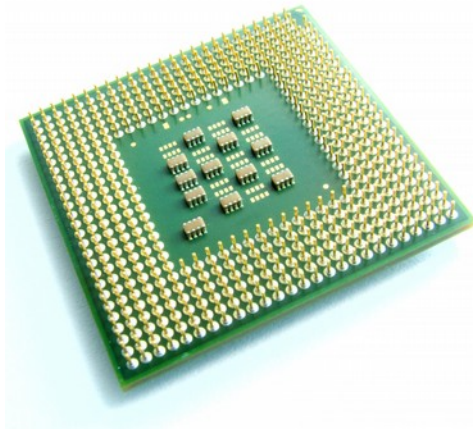
smartmontools



smartmontools



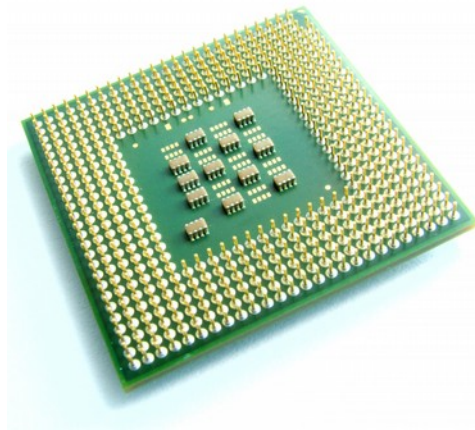
mcelog



smartmontools



mcelog



lm-sensors




```
$ sar -A
```

```
Linux 2.6.32-23-generic
```

```
2010-07-08
```

```
_x86_64_
```

00:00:01	CPU	%usr	%nice	%sys	%iowait	%steal
00:05:01	0	44,23	1,07	4,20	9,74	0,00
00:15:01	0	40,83	0,18	1,85	0,61	0,00
00:25:01	0	39,14	0,18	2,26	0,68	0,00
00:35:02	0	46,30	4,86	9,16	11,44	0,00
00:45:01	0	43,13	2,19	7,26	6,30	0,00
00:55:01	0	36,73	0,22	2,12	0,75	0,00
01:05:01	0	24,21	9,15	19,56	5,90	0,00
01:15:02	0	1,17	14,03	38,30	11,95	0,00
01:25:02	0	1,22	8,72	22,72	8,75	0,00
01:35:01	0	1,11	0,31	2,19	0,28	0,00
01:45:01	0	1,09	0,25	2,16	0,21	0,00
01:55:01	0	1,03	0,40	2,17	0,23	0,00
02:05:01	0	1,19	1,86	3,28	0,99	0,00
02:15:01	0	1,03	0,28	2,15	0,25	0,00
02:25:01	0	1,13	0,43	2,26	0,27	0,00
02:35:01	0	0,98	0,41	2,09	0,46	0,00
02:45:01	0	1,07	0,25	2,04	0,21	0,00
02:55:01	0	1,01	0,27	2,25	0,24	0,00
03:05:01	0	1,92	2,28	2,76	1,13	0,00
03:15:01	0	1,02	0,26	2,19	0,22	0,00
03:25:01	0	1,12	0,26	2,14	0,27	0,00
03:35:01	0	1,06	0,28	2,34	0,28	0,00
03:45:01	0	1,08	0,26	2,26	0,26	0,00
03:55:01	0	1,06	0,39	2,15	0,22	0,00
04:05:01	0	1,04	1,75	2,70	0,40	0,00
	0	1,10	0,30	2,33	0,26	0,00
	0	1,09	0,31	2,29	0,21	0,00
	0	1,16	9,76	13,21	6,99	0,00
	0	1,24	8,52	15,61	8,20	0,00

sysstat

safety

[=====]

molly-guard



```
***: via eth1 at 0x00000000, 00:03:11:11:11:11, IRQ 7
eth0: MII PHY found at address 29, status 0x7829 advertising Gbit Link <Gel.
netrom dg252x driver, version 1.07-181 0.17, Sep 27, 2002
originally by Donald Becker <becker@nyu.edu>
http://www.cygwin.com/projects/custom1.html
2.4.x kernel port by Jeff Garzik, Jgarzik@redhat.com
netrom eth1: Realtek RV8811561 at 0x00000000 (0000-00-00-00), FF:FF:FF:FF:FF:FF
- IRQ 10, port FF
supnet probe start
PCI: Enabling device 0000-00-02.0 (0000 -> 0003)
mm region start add 0x00000000 size == 0x000000
rv region start add 0x00000000 size == 0x000000
io region start add 0x0000 size == 0x00
mm ioremap add 0x00000000
rv ioremap add 0x00000000
supnet probe exit
Device Multi-Platform E-IDE driver Revision: 7.0bhigh2
ide: assuming IDE0: option bus speed for PIO mode: override with idebus=xx
HP_IDE: IDE controller at PCI slot 0000-00:11.1
HP_IDE: chipset revision 6
HP_IDE: not 100% native mode: will probe irq later
HP_IDE: VIA 82C35 (rev 00) IDE UDMA33 controller on pci0000-00:11.1
ide0: BM-200 at 0x0000-0x0007, BIOS settings: hM:pio, hM:pio
ide1: BM-200 at 0x0000-0x0007, BIOS settings: hM:pio, hM:pio
```

safe-rm

```
$ rm -rf /usr/lib/libfoo.so
```

safe-rm

```
$ rm -rf /usr/lib /libfoo.so
```

safe-rm

```
$ rm -rf /usr/lib /libfoo.so  
/bin/rm: cannot remove `/libfoo.so':  
No such file or directory
```

safe-rm

```
$ rm -rf /usr/lib /libfoo.so  
/bin/rm: cannot remove `/libfoo.so':  
No such file or directory
```

```
$ ls /usr/lib  
ls: cannot access /usr/lib: No such  
file or directory
```

/
/etc
/usr
/var/lib

...

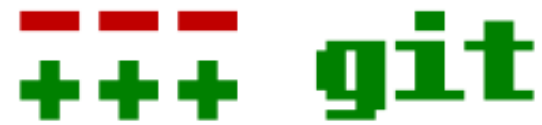
safe-rm

```
$ rm -rf /usr/lib  
safe-rm: skipping /usr/lib
```

etckeeper



mercurial



mythtv-status

```
andrew@cerberus
MythTV status for localhost
=====
Status.....: Fri Dec 14 2007, 6:29 AM
Total Disk Space.: Total space is 102,350 GB, with 83,290 GB used (81.4%)
Next Recording In: 11 Hours, 30 Minutes

Encoders:
cerberus (9) - Idle
cerberus (12) - Idle

Scheduled Recordings:
2007-12-14 18:00:00 - 3 News (TV3)
2007-12-15 18:00:00 - 3 News (TV3)
2007-12-15 19:30:00 - Grand Designs (TV3)

Schedule Conflicts:
2007-12-14 18:30:00 - Friends (TV2)

Disk Space:
Total space for group 2 is 20,746 GB, with 20,101 GB used (96.9%)

cerberus:~$ █
```


security

[=====]





LOCKWOOD

120/50

apparmor

apparmor-profiles

apparmor-profiles-extra

debsums

fcheck

chkrootkit

checksecurity



rkhunter

tiger

remote access

[=====]

openssh-server

mosh

<http://feeding.cloud.geek.nz/posts/hardening-ssh-servers/>

iptables

```
$ cat /etc/network/iptables.up.rules
```

```
*filter
```

```
:INPUT DROP [0:0]
```

```
:FORWARD DROP [0:0]
```

```
:OUTPUT DROP [0:0]
```

```
-A OUTPUT -j ACCEPT
```

```
-A INPUT -i lo -j ACCEPT
```

```
-A INPUT -p icmp -j ACCEPT
```

```
-A INPUT -m conntrack --ctstate RELATED,  
ESTABLISHED -j ACCEPT
```

```
:LOGDROP - [0:0]
```

```
-A LOGDROP -j LOG --log-level 6
```

```
-A LOGDROP -j DROP
```

```
-A INPUT -j LOGDROP
```

```
COMMIT
```



```
$ cat /etc/network/iptables.up.rules
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

-A OUTPUT -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,
    ESTABLISHED -j ACCEPT

-A INPUT -s 192.168.1.0/24
    -p tcp --dport 22 -j ACCEPT

:LOGDROP - [0:0]
-A LOGDROP -j LOG --log-level 6
-A LOGDROP -j DROP
-A INPUT -j LOGDROP
COMMIT
```

fwknop



fwknop



ipcheck



x11vnc

ssvnc

<http://feeding.cloud.geek.nz/posts/high-latency-vnc-tech-support/>

backups

[=====]

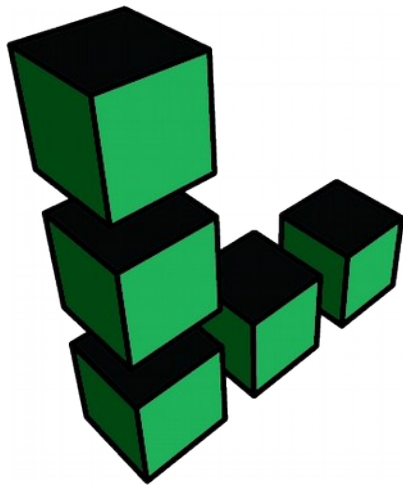
1. config files

2. important documents

3. non-critical data

1. config files

duplicity



linode

1. config files

all of /etc

installed packages

Myth TV DB dump

2. important documents

~/documents/safe

emails

bookmarks

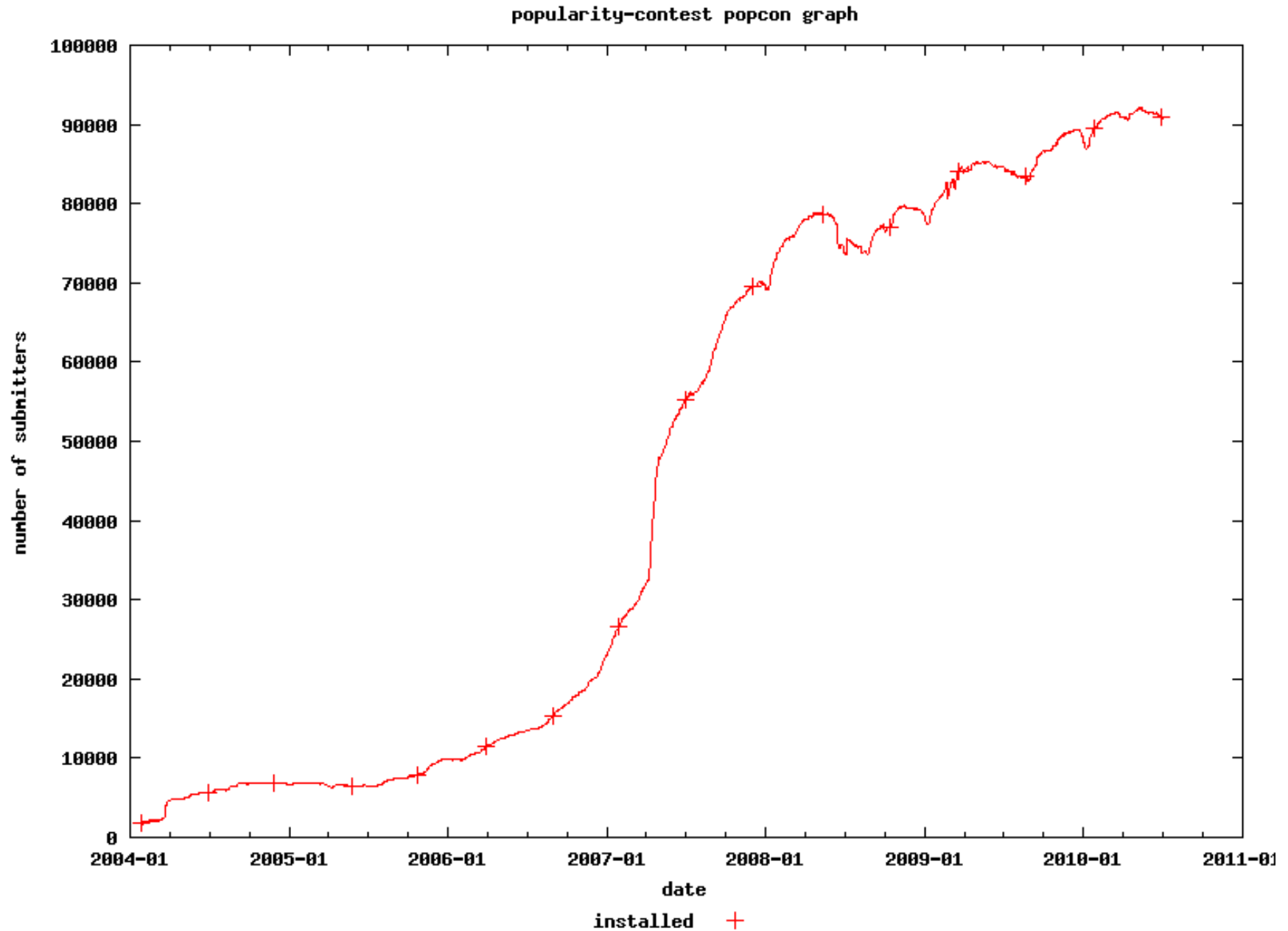
3. non-critical data



“giving back”
















[=====]

popularity-contest


















kerneloops

921 oopses reported

run_timer_softirq		45
intel_opregion_video_event		32
lirc_register_driver		26
drm_ioctl		19
audit_inc_name_count		17
tmm_tt_swapout		16
radeon_set_pcigart		16
hiddev_ioctl		15
__do_softirq		15
fb_release		14
list_del		13
firegl_trace (P)		11
_nv005370rm		10
tmm_bo_pci_offset		10
nouveau_gem_ioctl_pushbuf		9

919 BUG/BUG_ON's reported

__slab_alloc		329	
b43_dma_handle_txstatus		181	
acpi_idle_enter_bm		133	Dell Laptops oops in idle
acpi_idle_enter_simple		51	
shrink_dcache_for_umount_subtree		36	
_raw_spin_unlock		32	
__do_softirq		7	
ext4_get_blocks		7	
mntput_no_expire		5	
mwait_idle		5	
synchronize_irq		4	
_spin_unlock_irqrestore		4	
iput		4	
inode_reserved_space		4	
ext4_da_get_block_prep		4	



hardware

package updates

monitoring

safety

security

remote access

backups

Photos credits:

blue lagoon: <http://www.flickr.com/photos/benhusmann/4467839635/>

in-flight entertainment: <http://www.flickr.com/photos/kalleboo/2473197800/>

ssd and hdd: <http://www.flickr.com/photos/28771658@N03/3377026684/in/photostream/>

igloo: <http://www.flickr.com/photos/zuc123/426508881/>

canadian flag: <http://www.flickr.com/photos/webhamster/2914086018/>

broom: <http://www.flickr.com/photos/jrigol/2821450325/>

intel cpu: <http://www.flickr.com/photos/andresrueda/3274875773/>

thermometer: <http://www.flickr.com/photos/andresrueda/3407340937/>

open harddrive: <http://www.flickr.com/photos/uwehermann/2994944961/>

ram: <http://www.flickr.com/photos/detodounpoquito/2481060491/>

baby hay stack: <http://www.flickr.com/photos/nerdcoregirl/2959701240/>

safe: <http://www.flickr.com/photos/pong/288491653/>

padlock: <http://www.flickr.com/photos/shelleygibb/3396463409/>

tiger: <http://www.flickr.com/photos/auburnnewyork/4439937219/>

old modem: <http://www.flickr.com/photos/rexroof/3302978710/>

red door: <http://www.flickr.com/photos/romdos/8846131/>

dvd on cat: <http://www.flickr.com/photos/suzanneandsimon/84038024/>

uncle sam: <http://www.flickr.com/photos/notionscapital/2942067553/>

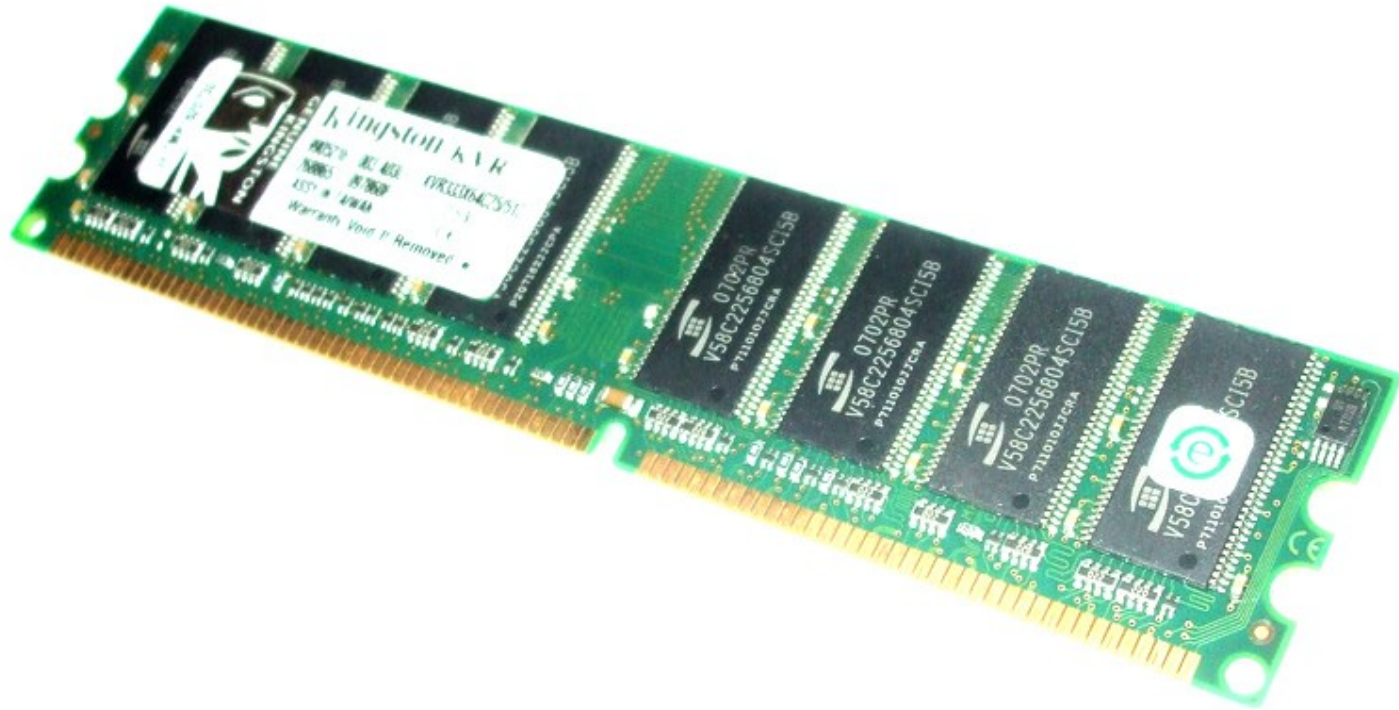


This presentation is © 2015 François Marier and released under the terms of the Creative Commons Attribution Share-Alike 4.0 license

`/* TODO */`

[=====]

ECC memory



https://blogs.oracle.com/ksplice/entry/attack_of_the_cosmic_rays1