Trying To Not Use All Your Memory

Robert O'Callahan
Mozilla Corporation

Please be interactive.

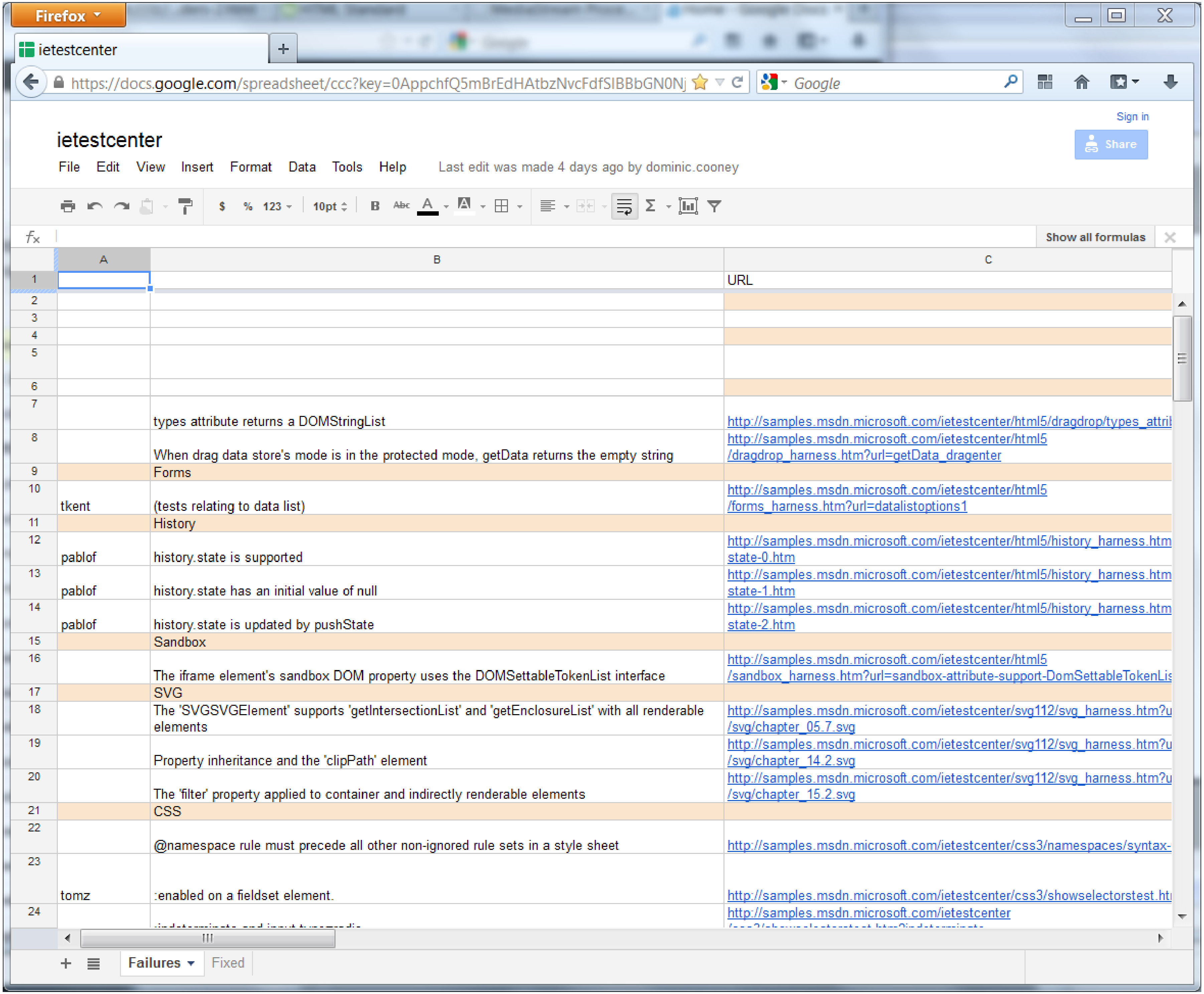
Credit to Nick Nethercote and many others.

- Our problem space
- A glimpse into Firefox memory management
- What we haven't figured out yet

Once upon a time, Web browsers were simple.

THE COMPANY PAYS ME TEN DOLLARS FOR EVERY BUG I FIX IN MY CODE, RATBERT.
I WANT YOU TO DO YOUR LITTLE RAT DANCE ON MY KEYBOARD SO I'LL HAVE LOTS OF BUGS TO FIX.
HOW AM I DOING?
NOT SO GOOD. YOU JUST AUTHORED A WEB BROWSER.
S. ADAMS E-mail: SCOTTADAMS@AOL.COM
11/14 © 1995 United Feature Syndicate, Inc.(NYC)

Things have changed.

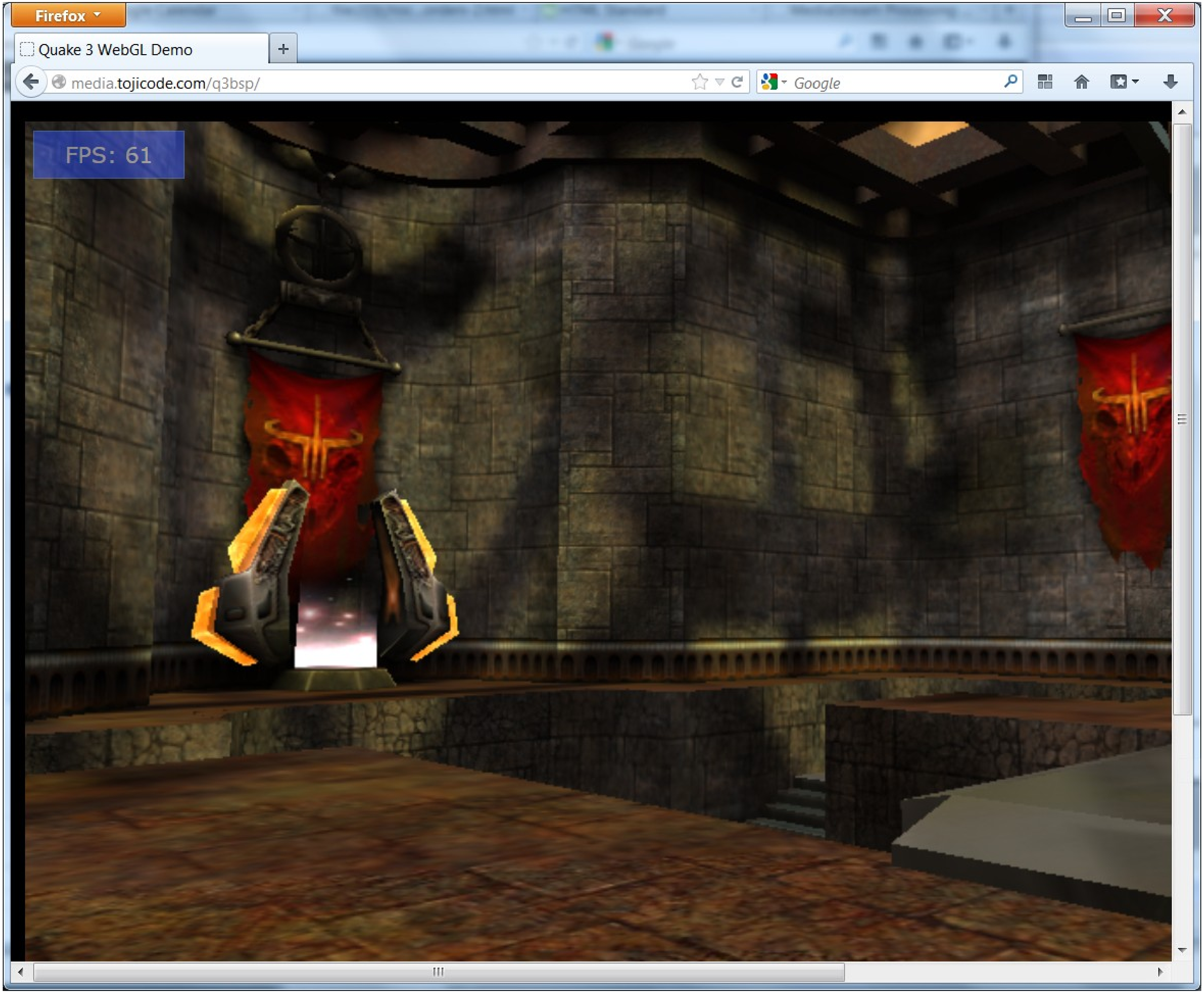


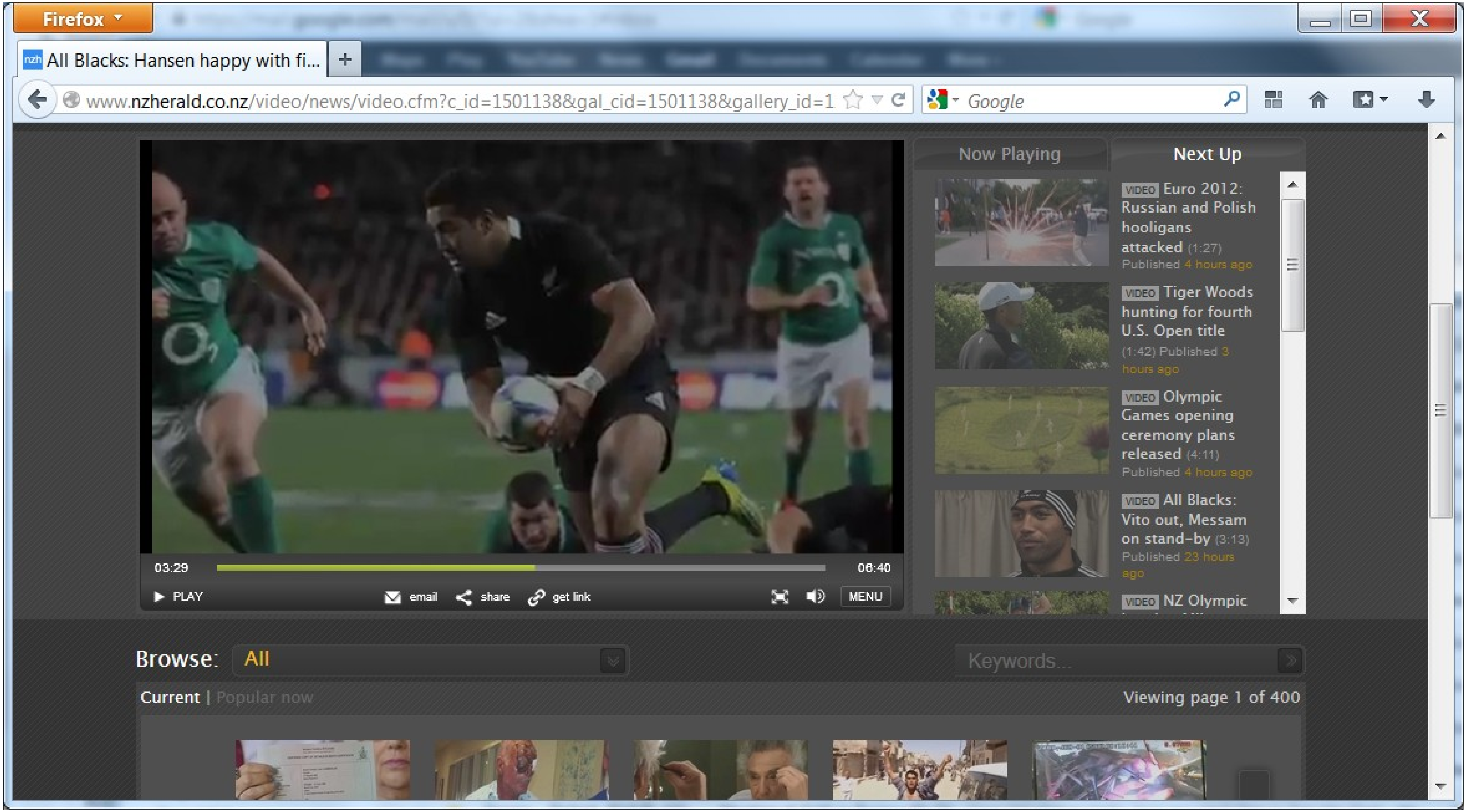
https://docs.google.com/spreadsheet/ccc?key=0AppchfQ5mBrEdHAtbzNvcFdfSlBBbGN0Nj

ietestcenter

Last edit was made 4 days ago by dominic.cooney

	A	B	C
1			URL
2			
3			
4			
5			
6			
7		types attribute returns a DOMStringList	http://samples.msdn.microsoft.com/ietestcenter/html5/dragdrop/types_attri
8		When drag data store's mode is in the protected mode, getData returns the empty string	http://samples.msdn.microsoft.com/ietestcenter/html5 /dragdrop_harness.htm?url=getData_dragenter
9		Forms	
10	tkent	(tests relating to data list)	http://samples.msdn.microsoft.com/ietestcenter/html5 /forms_harness.htm?url=datalistoptions1
11		History	
12	pablof	history.state is supported	http://samples.msdn.microsoft.com/ietestcenter/html5/history_harness.htm state-0.htm
13	pablof	history.state has an initial value of null	http://samples.msdn.microsoft.com/ietestcenter/html5/history_harness.htm state-1.htm
14	pablof	history.state is updated by pushState	http://samples.msdn.microsoft.com/ietestcenter/html5/history_harness.htm state-2.htm
15		Sandbox	
16		The iframe element's sandbox DOM property uses the DOMSettableTokenList interface	http://samples.msdn.microsoft.com/ietestcenter/html5 /sandbox_harness.htm?url=sandbox-attribute-support-DomSettableTokenLis
17		SVG	
18		The 'SVGSVGElement' supports 'getIntersectionList' and 'getEnclosureList' with all renderable elements	http://samples.msdn.microsoft.com/ietestcenter/svg112/svg_harness.htm?u /svg/chapter_05.7.svg
19		Property inheritance and the 'clipPath' element	http://samples.msdn.microsoft.com/ietestcenter/svg112/svg_harness.htm?u /svg/chapter_14.2.svg
20		The 'filter' property applied to container and indirectly renderable elements	http://samples.msdn.microsoft.com/ietestcenter/svg112/svg_harness.htm?u /svg/chapter_15.2.svg
21		CSS	
22		@namespace rule must precede all other non-ignored rule sets in a style sheet	http://samples.msdn.microsoft.com/ietestcenter/css3/namespaces/syntax-
23	tomz	:enabled on a fieldset element.	http://samples.msdn.microsoft.com/ietestcenter/css3/showselectorstest.ht
24		:indeterminate and input type=radio	http://samples.msdn.microsoft.com/ietestcenter /css3/showselectorstest.htm?indeterminate


Firefox
Quake 3 WebGL Demo
media.tojicode.com/q3bsp/
Google
FPS: 61



All Blacks: Hansen happy with fi...

www.nzherald.co.nz/video/news/video.cfm?c_id=1501138&gal_cid=1501138&gallery_id=1

VIDEO Euro 2012: Russian and Polish hooligans attacked (1:27) Published 4 hours ago

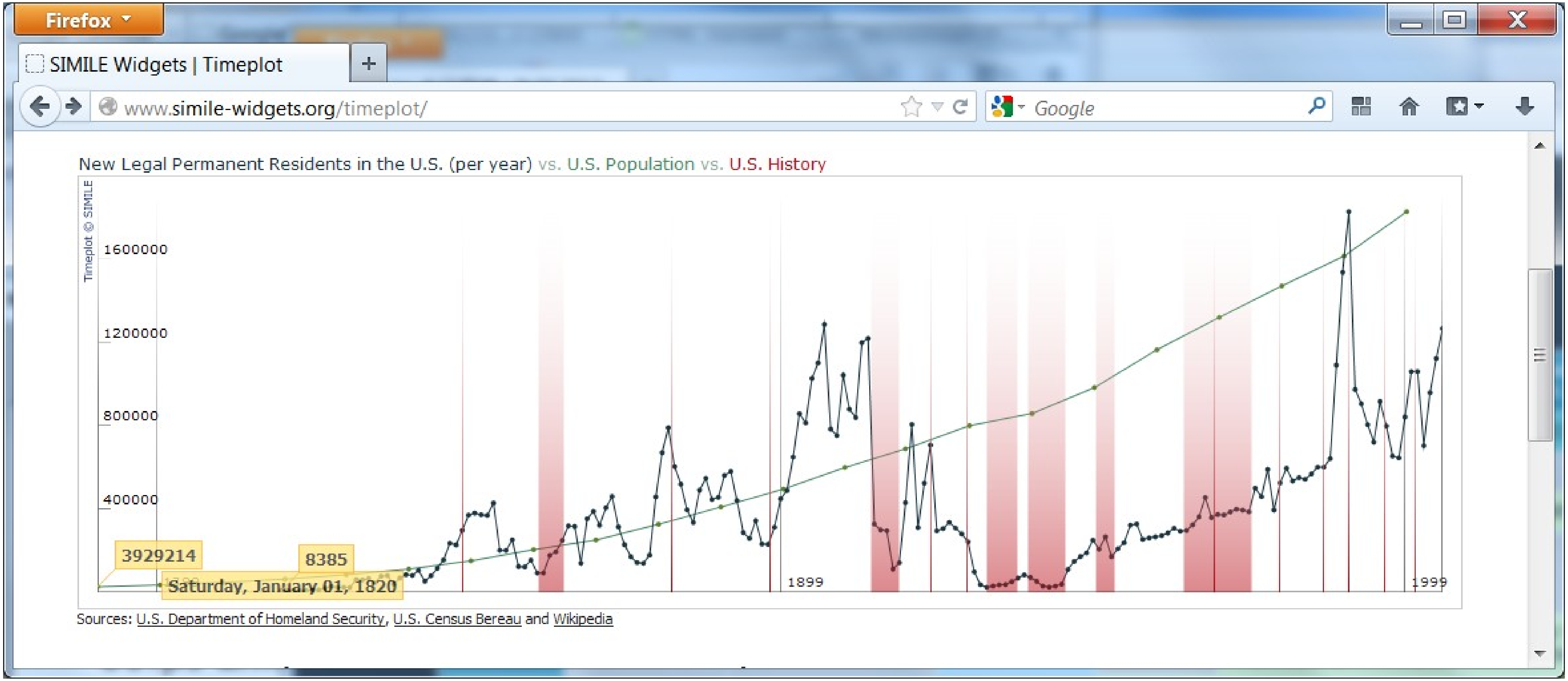
VIDEO Tiger Woods hunting for fourth U.S. Open title (1:42) Published 3 hours ago

VIDEO Olympic Games opening ceremony plans released (4:11) Published 4 hours ago

VIDEO All Blacks: Vito out, Messam on stand-by (3:13) Published 23 hours ago

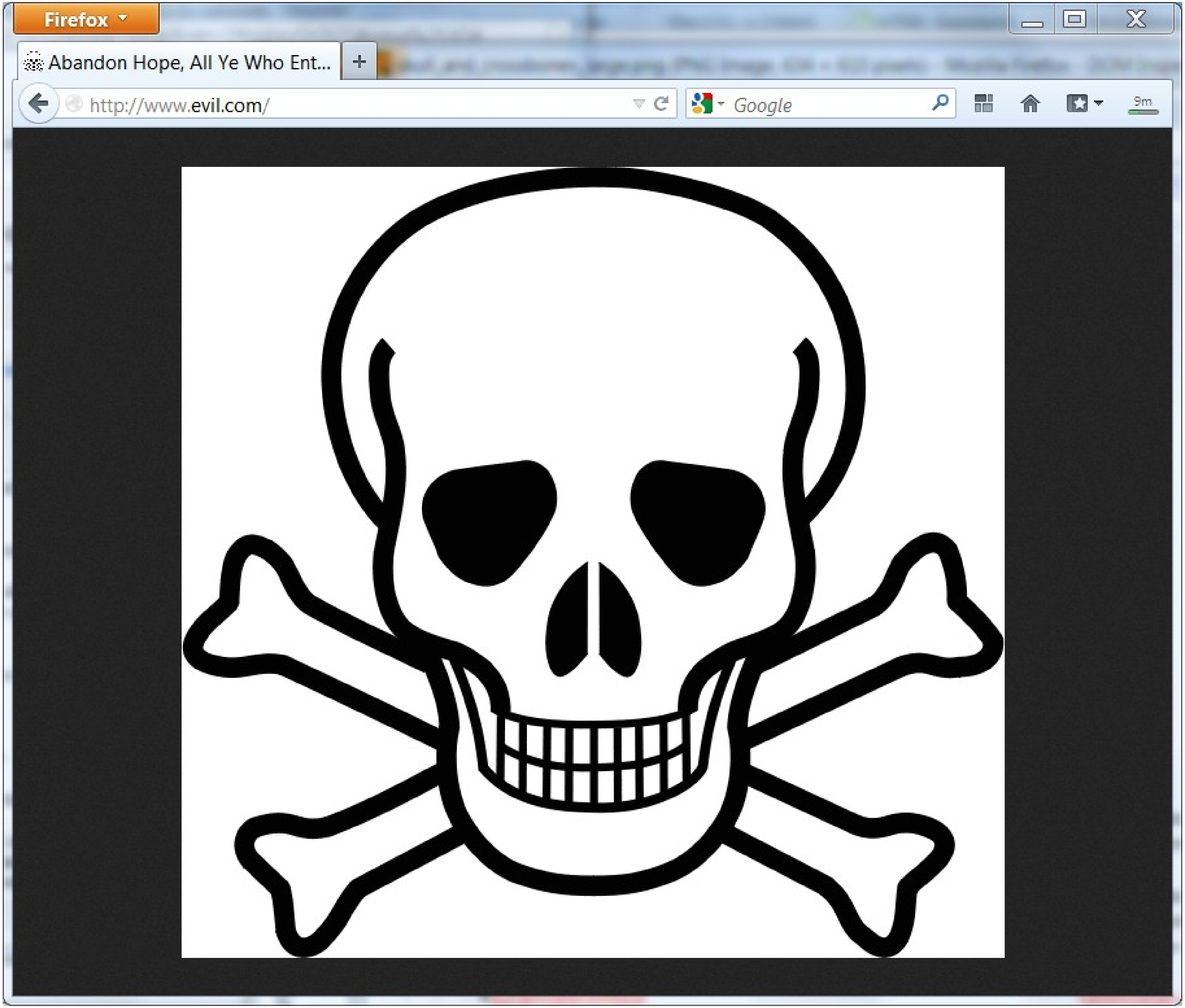
VIDEO NZ Olympic

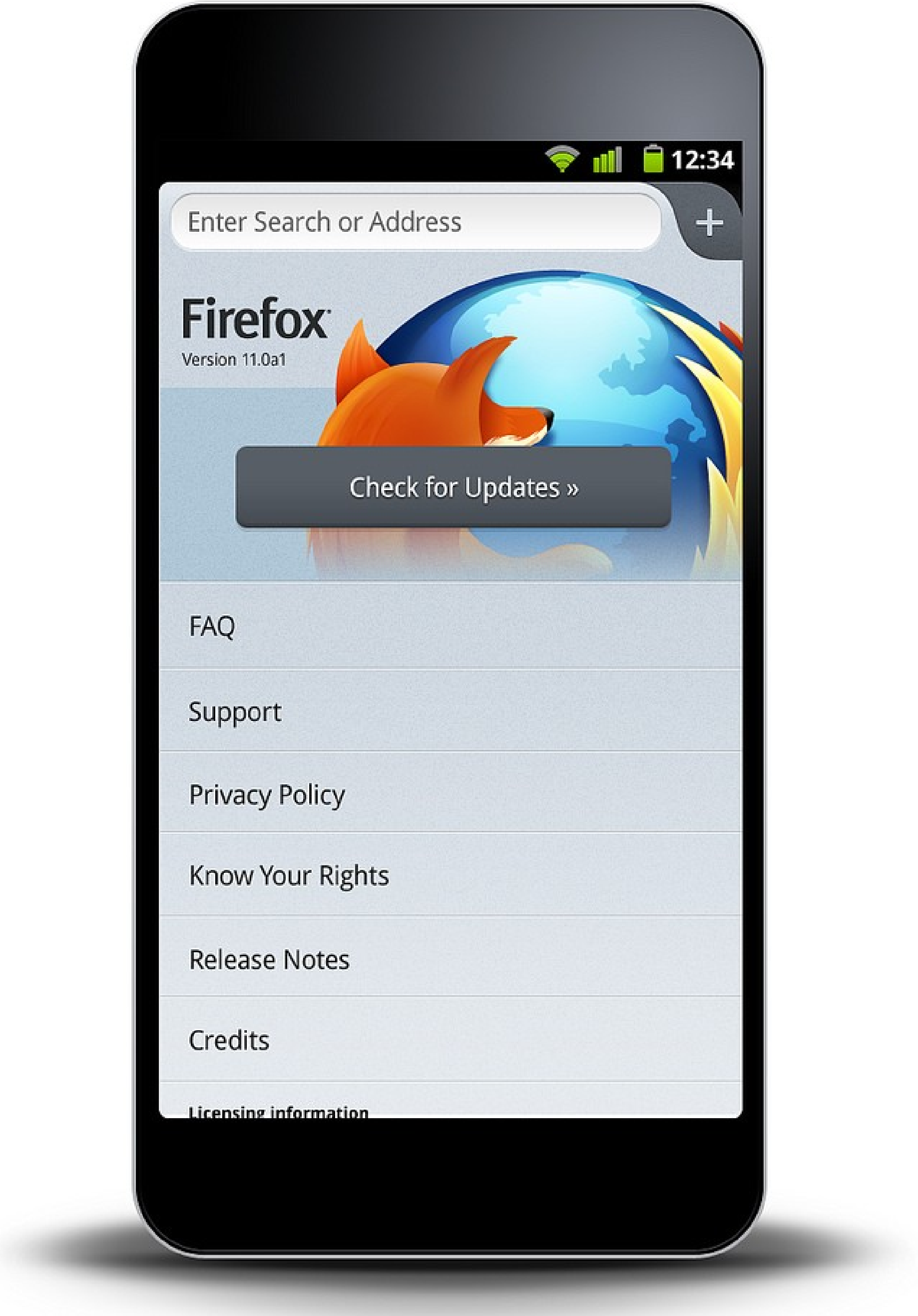
Viewing page 1 of 400


Firefox
SIMILE Widgets | Timeplot
www.simile-widgets.org/timeplot/
Google
Timeplot © SIMILE
1600000
1200000
800000
400000
3929214
8385
Saturday, January 01, 1820
1899
1999

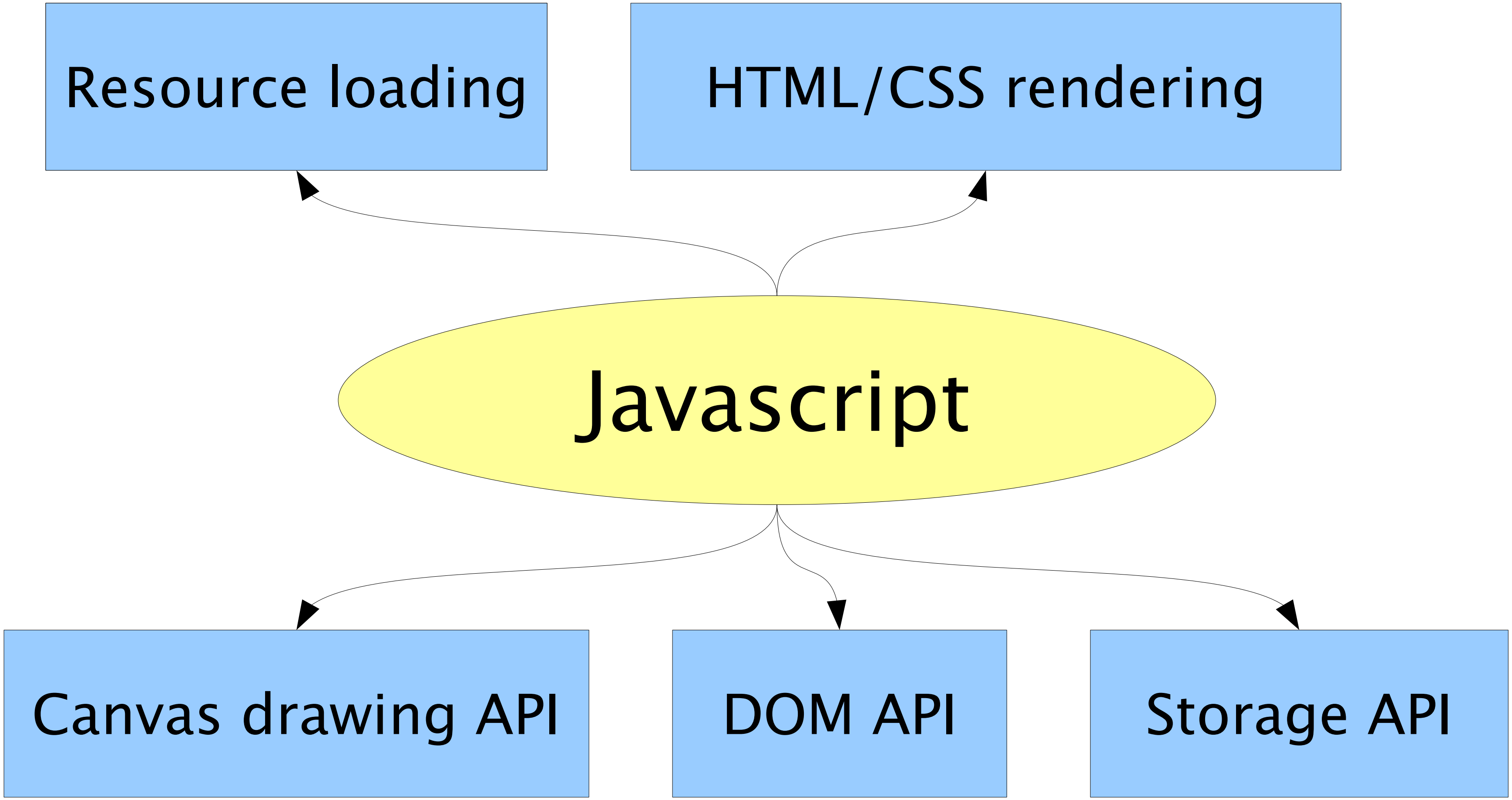
New Legal Permanent Residents in the U.S. (per year) vs. U.S. Population vs. U.S. History

Sources: U.S. Department of Homeland Security, U.S. Census Bereau and Wikipedia


Firefox
Abandon Hope, All Ye Who Ent...
http://www.evil.com/
Google


12:34
Enter Search or Address
+
Firefox
Version 11.0a1
Check for Updates »
FAQ
Support
Privacy Policy
Know Your Rights
Release Notes
Credits
Licensing information

One Point Of View



Host Objects

- DOM API objects implemented by browser in C++
- FFI/“DOM bindings” very important
- Memory management across language boundary very important
  - Especially cycles

Additional Constraints

- 100s of tabs
- KB to GB per tab
- Page load/unload churn
- 60FPS
- “The Web” is difficult to characterize and evolves rapidly

Commodity Software

- Users compare browser memory usage, share impressions, and switch browsers
- Reducing memory usage matters even if it has **no impact** on performance
- Must release memory ASAP when closing tabs while user is watching Task Manager
- Must be competitive even on **extremely poorly designed** Web sites
- Worst-case performance matters

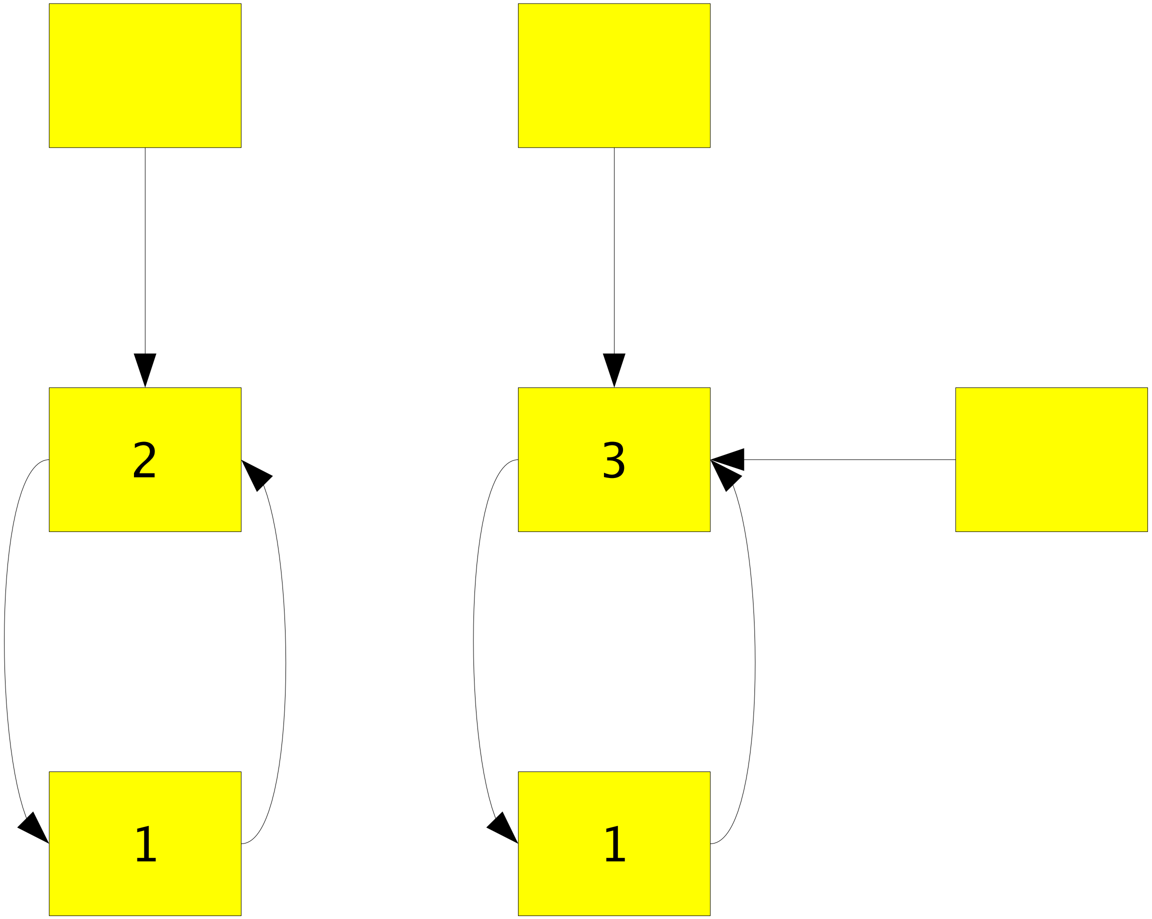
Memory Management In Firefox

- JS heap: incremental mark and sweep collector
  - WIP: Moving generational
- C++ objects: reference counting with smart pointers
- Everything: cycle collector [Bacon+Rajan, ECOOP01]

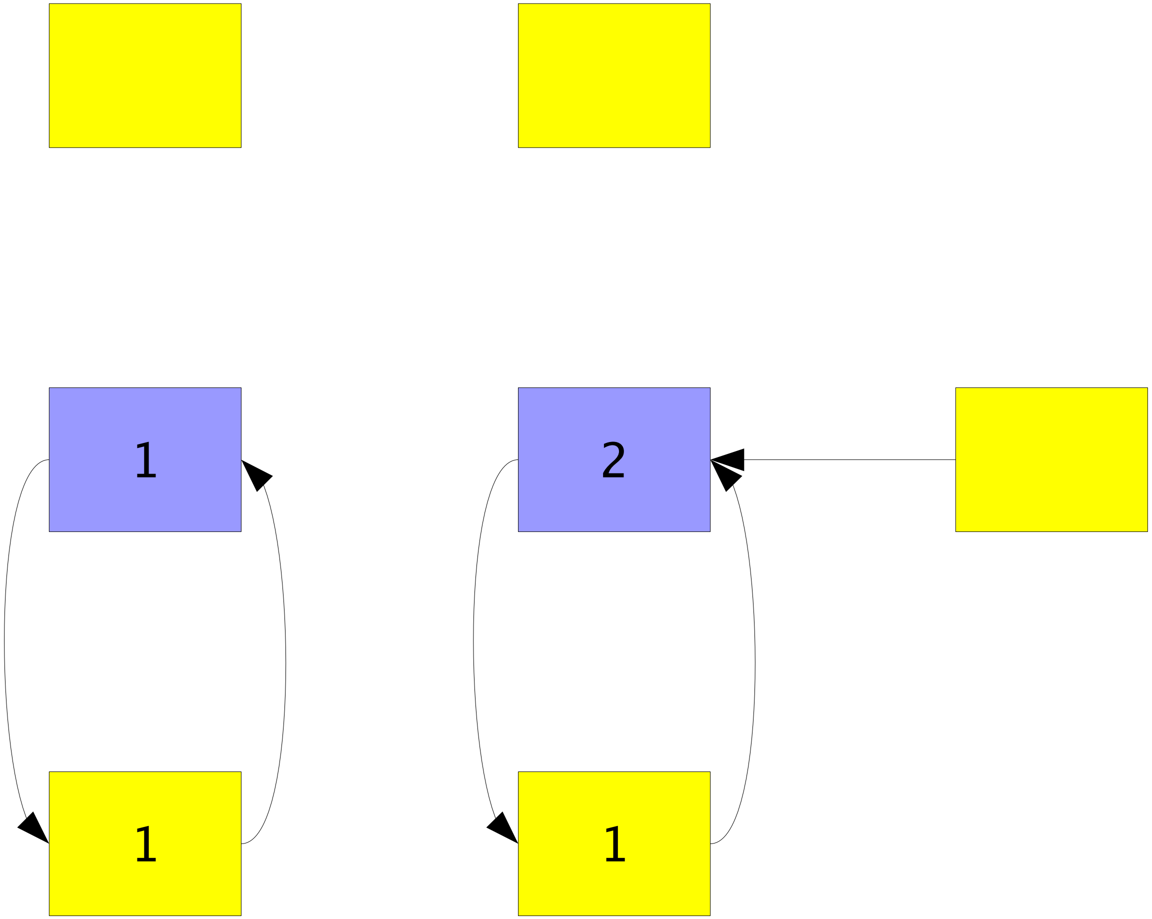
"It [reference counting] ... is unused by mature high performance systems."

— An ISMM 2012 paper

Cycle Collection



Cycle Collection

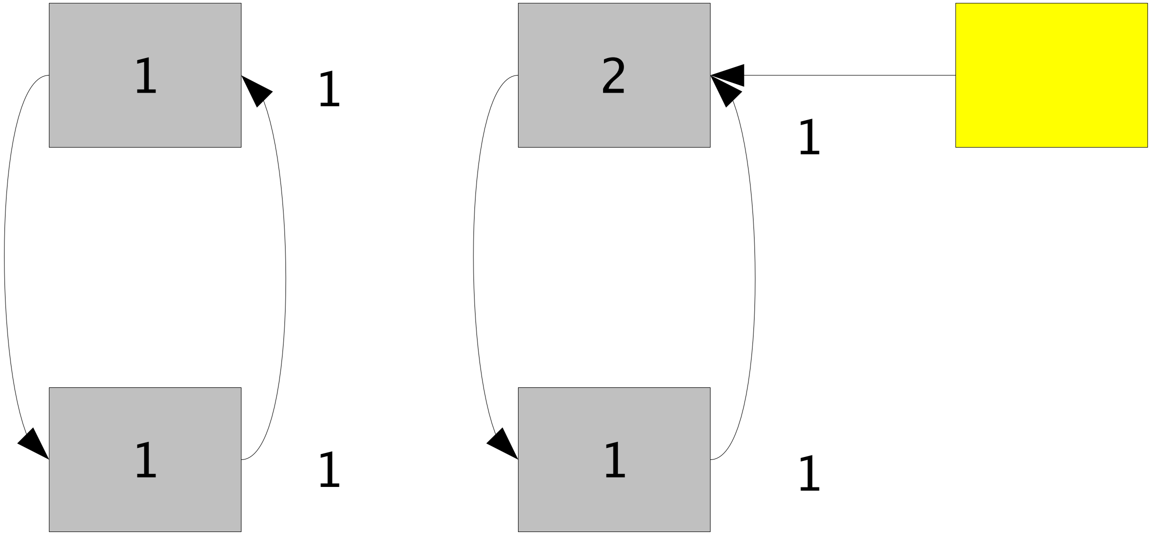


Node marked purple/"suspect" when refcount decremented

Live purple nodes are “roots” of potential cycles. CC does not require explicit knowledge of root set (win!)

Cycle Collection

Mark purple nodes and those reachable from purple as “gray”. Count number of incoming edges found for each node.

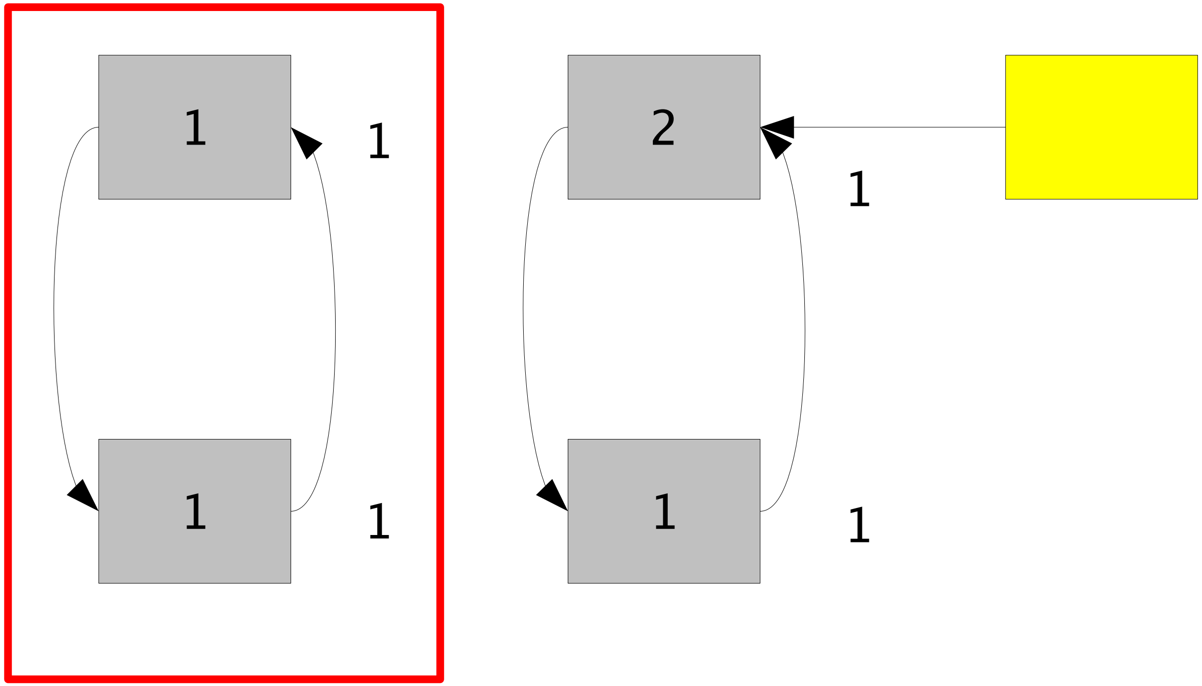


Cycle Collection

Traverse gray nodes breadth-first, starting with the former purple nodes:

If all references found, then it's garbage; release it later.

Otherwise it's live: preserve it and all gray nodes reachable from it.



Cycle Collector

✓ Works with C++ (albeit manual tracing)

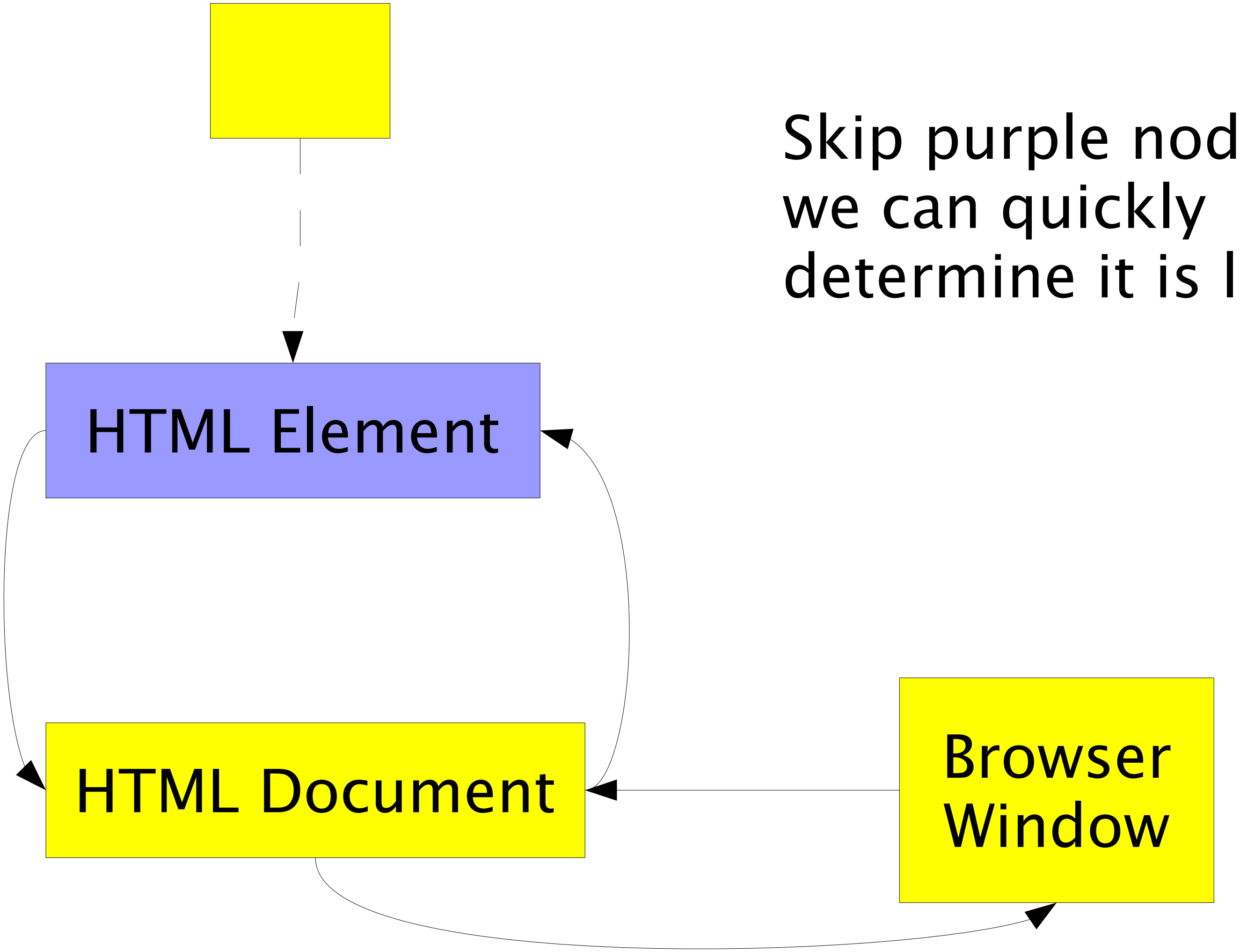
✓ Edges and objects that can't be involved in cycles don't need tracing

✓ Only looks at potential garbage not already released by reference counting

  - “Everything live” is a common steady state
  - Can delay CC until a certain amount of potential garbage exists

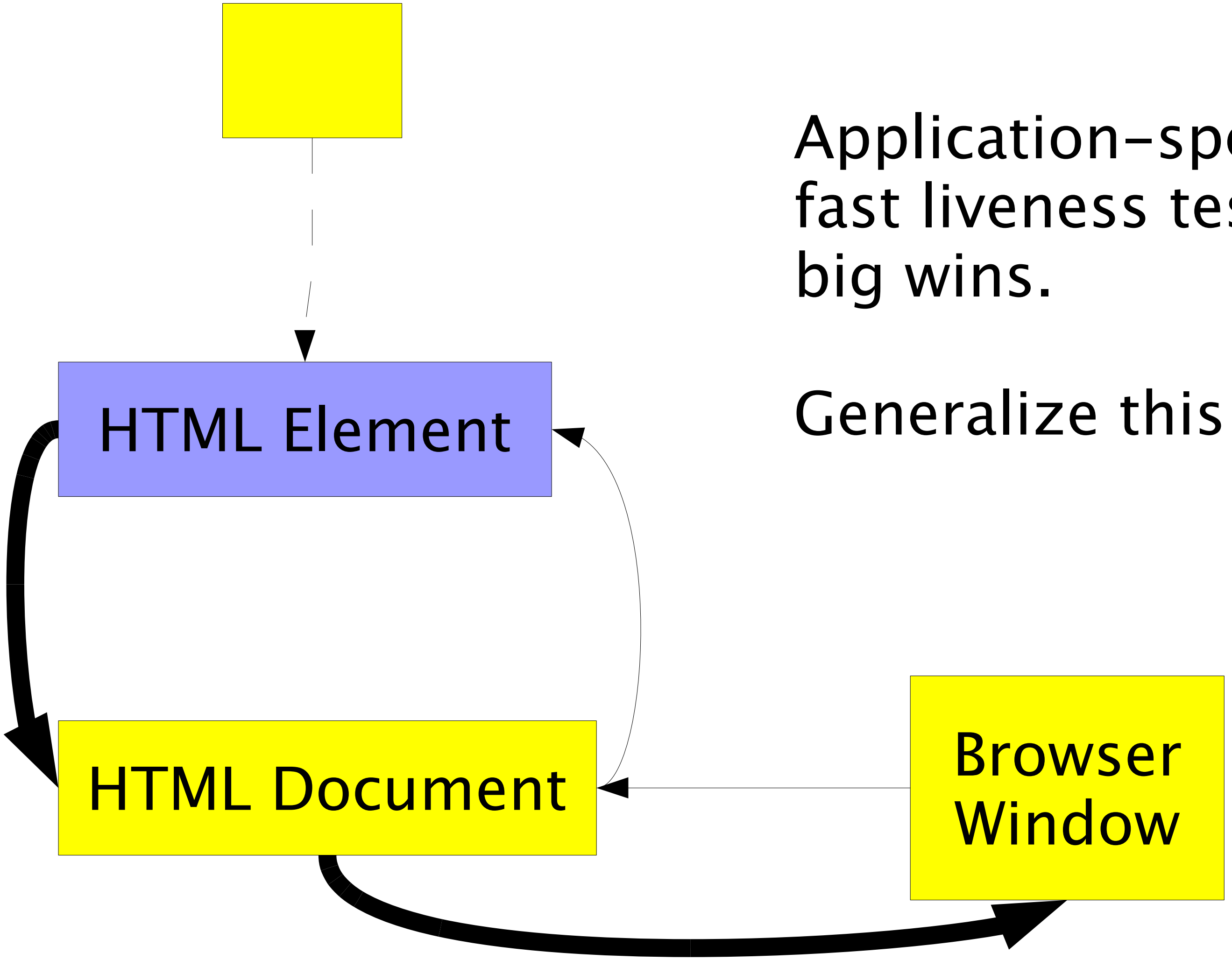
X Not fully generational/incremental (yet)

Optimizing Cycle Collection



Skip purple node if we can quickly determine it is live

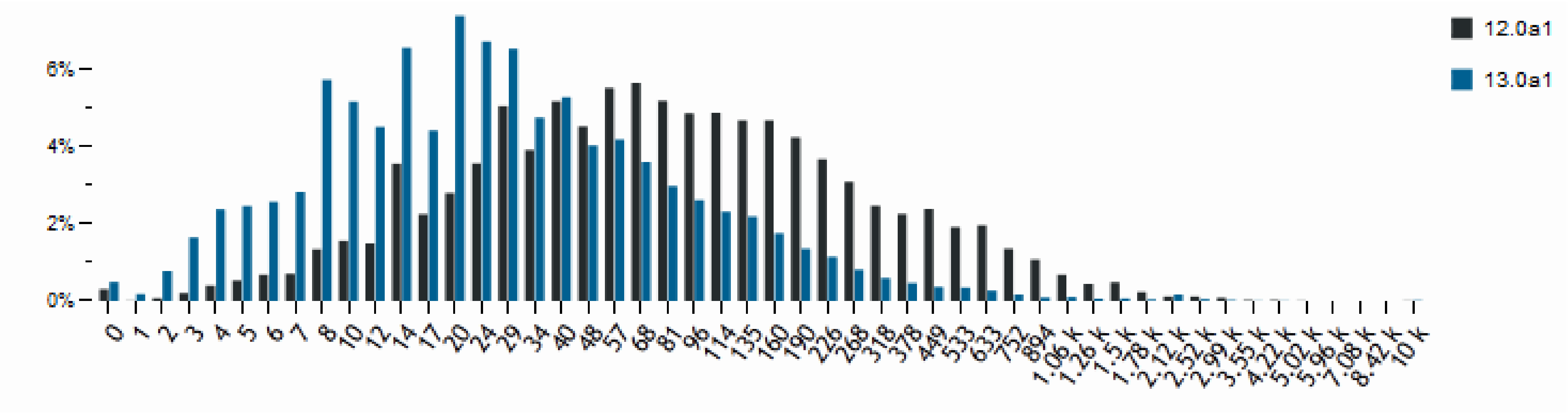
Optimizing Cycle Collection



Application-specific fast liveness test for big wins.

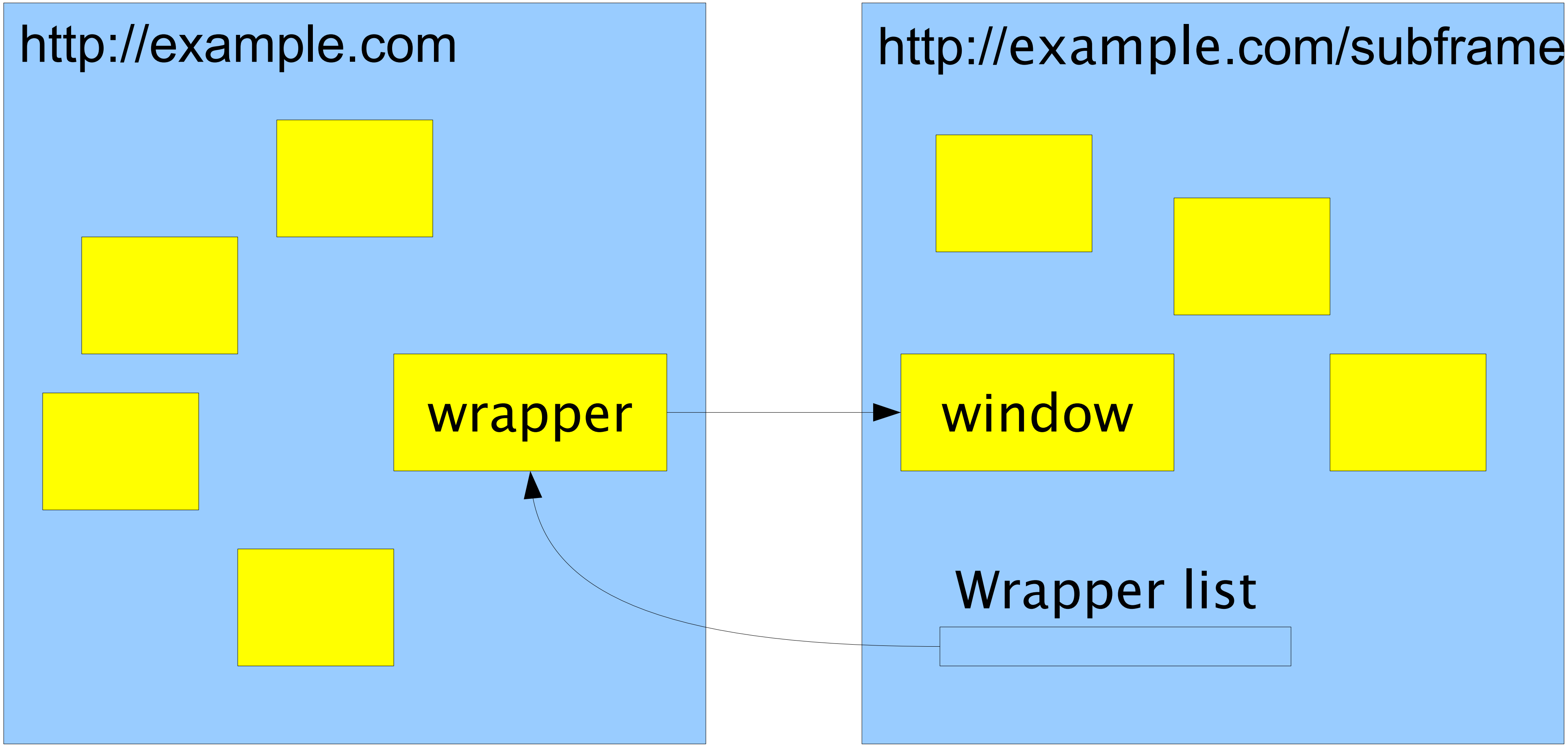
Generalize this!

Root!



12.0a1
13.0a1
6%
4%
2%
0%
0
1
2
3
4
5
6
7
8
10
12
14
17
20
24
29
34
40
48
57
68
81
96
114
135
160
190
226
268
318
378
449
533
633
752
894
1.06 k
1.26 k
1.5 k
1.78 k
2.12 k
2.52 k
2.99 k
3.55 k
4.22 k
5.02 k
5.96 k
7.08 k
8.42 k
10 k

Javascript Compartments



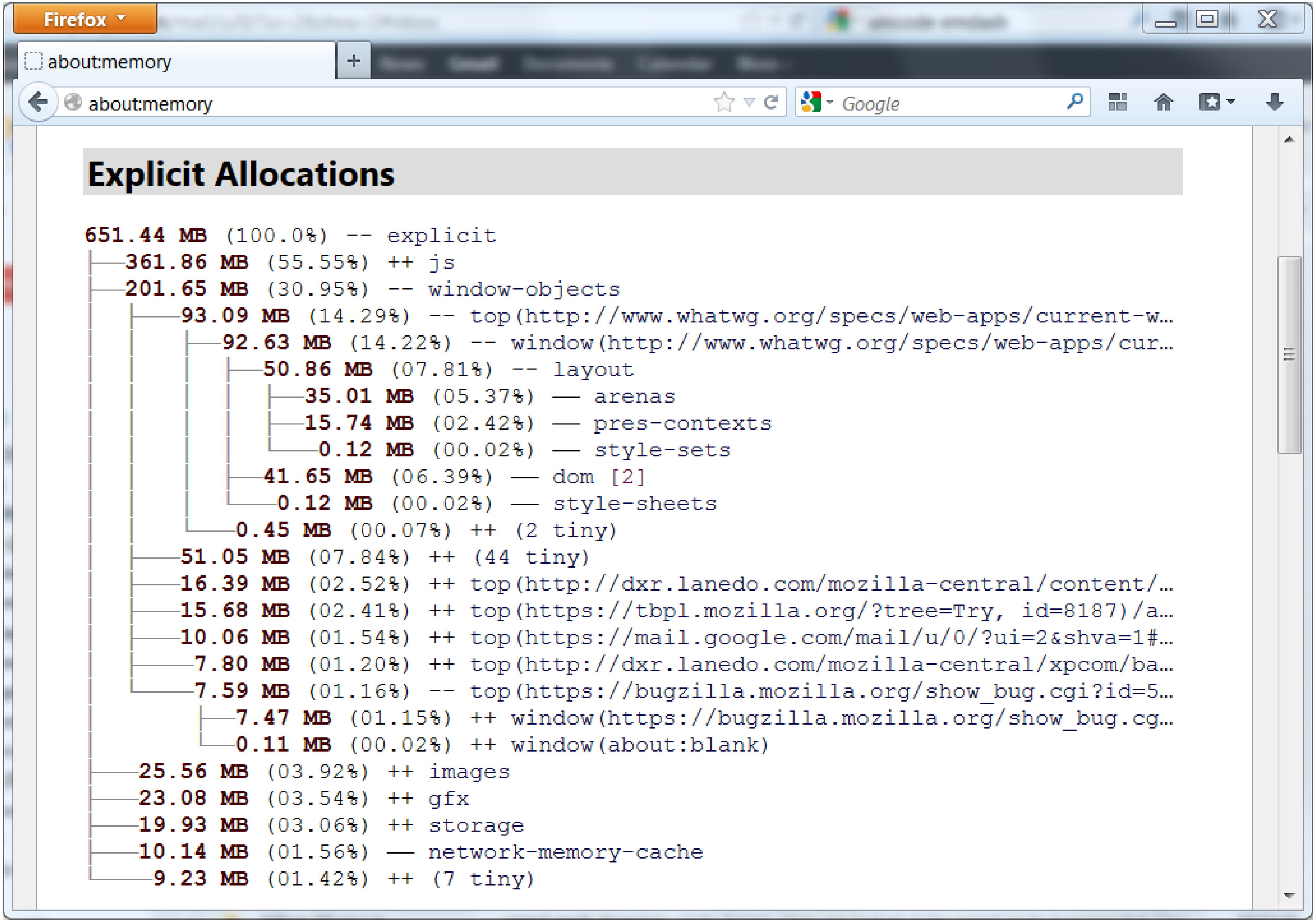
Security, accounting, GC, CPG

Firefox had a reputation for memory usage.

MemShrink

Nick Nethercote

Built better measurement tools.



Explicit Allocations

```
651.44 MB (100.0%) -- explicit
├──361.86 MB (55.55%) ++ js
├──201.65 MB (30.95%) -- window-objects
│  ├───93.09 MB (14.29%) -- top(http://www.whatwg.org/specs/web-apps/current-w…
│  │   ├──92.63 MB (14.22%) -- window(http://www.whatwg.org/specs/web-apps/cur…
│  │   │  ├──50.86 MB (07.81%) -- layout
│  │   │  │  ├──35.01 MB (05.37%) — arenas
│  │   │  │  ├──15.74 MB (02.42%) — pres-contexts
│  │   │  │  └───0.12 MB (00.02%) — style-sets
│  │   │  ├──41.65 MB (06.39%) — dom [2]
│  │   │  └───0.12 MB (00.02%) — style-sheets
│  │   └───0.45 MB (00.07%) ++ (2 tiny)
│  ├───51.05 MB (07.84%) ++ (44 tiny)
│  ├───16.39 MB (02.52%) ++ top(http://dxr.lanedo.com/mozilla-central/content/…
│  ├───15.68 MB (02.41%) ++ top(https://tbpl.mozilla.org/?tree=Try, id=8187)/a…
│  ├───10.06 MB (01.54%) ++ top(https://mail.google.com/mail/u/0/?ui=2&shva=1#…
│  ├────7.80 MB (01.20%) ++ top(http://dxr.lanedo.com/mozilla-central/xpcom/ba…
│  └────7.59 MB (01.16%) -- top(https://bugzilla.mozilla.org/show_bug.cgi?id=5…
│         ├──7.47 MB (01.15%) ++ window(https://bugzilla.mozilla.org/show_bug.cg…
│         └──0.11 MB (00.02%) ++ window(about:blank)
├───25.56 MB (03.92%) ++ images
├───23.08 MB (03.54%) ++ gfx
├───19.93 MB (03.06%) ++ storage
├───10.14 MB (01.56%) — network-memory-cache
└────9.23 MB (01.42%) ++ (7 tiny)
```

Found and fixed many bugs.

Bugs Found

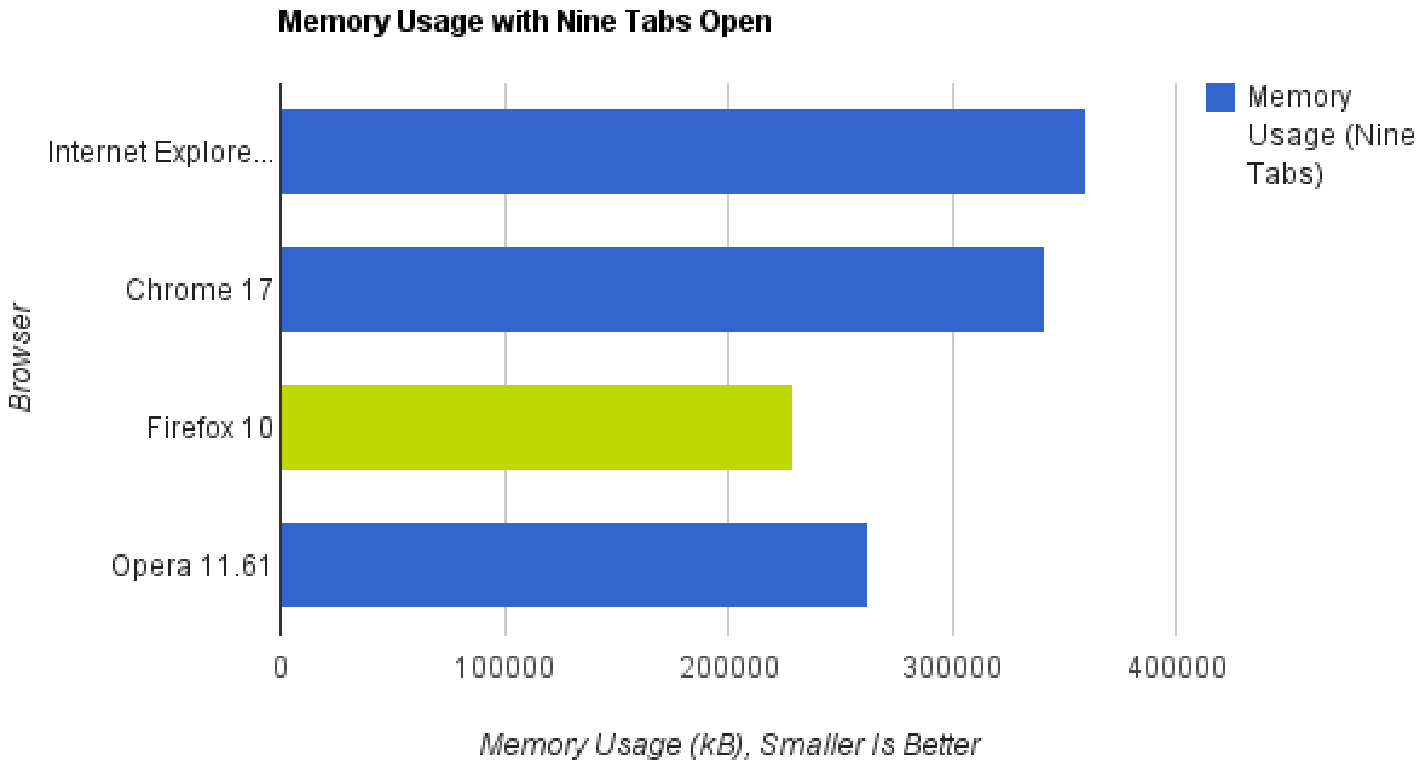
- Actual leaks
- Bloated data structures
- Space allocated but never used
- Non–Firefox issues: leaky addons and sites

```
sqlite3_int64 *p;
nByte = ROUND8(nByte);
p = malloc( nByte+8 );
if( p ){
  p[0] = nByte;
  p++;
}
```

nByte is normally an SQLite page size,
a power of 2…

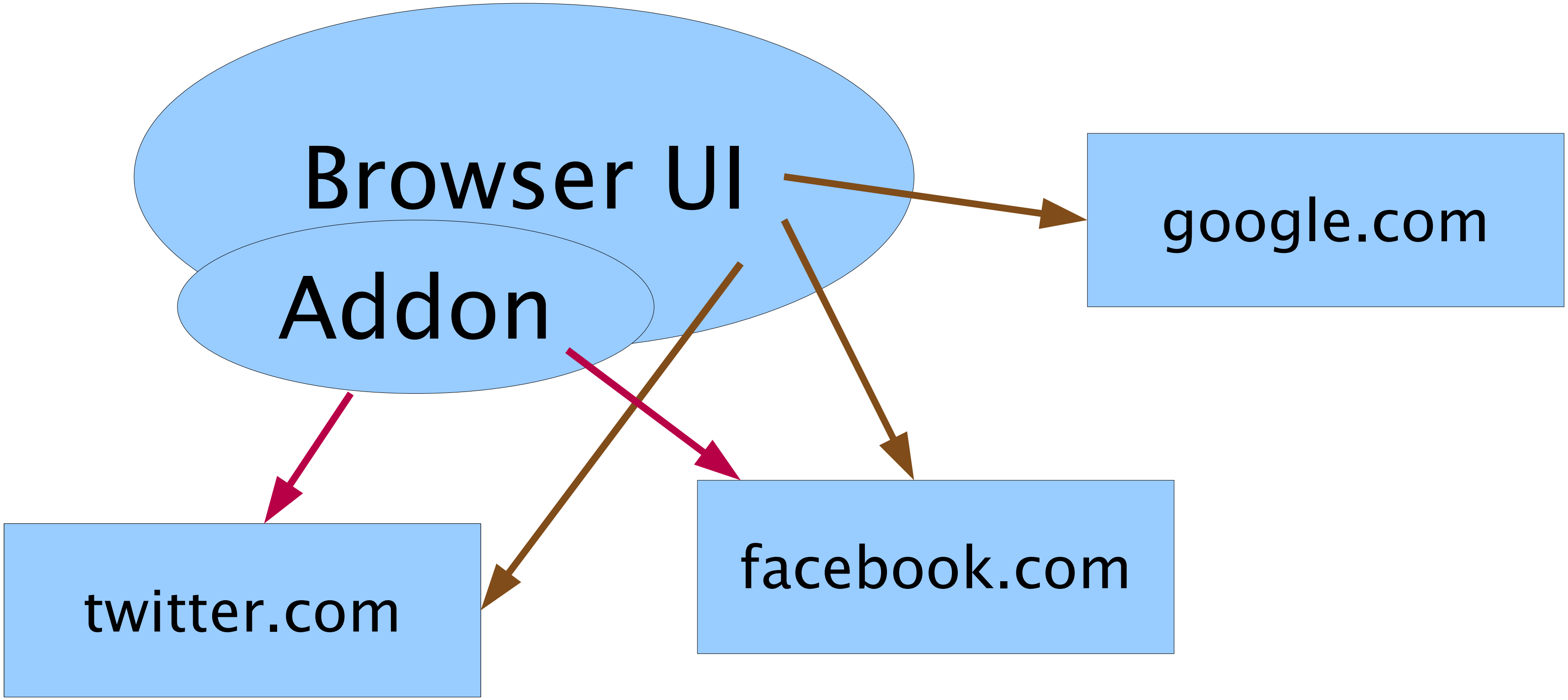
- Nick used instrumentation to find and fix **many** such issues

Unscientific Benchmark

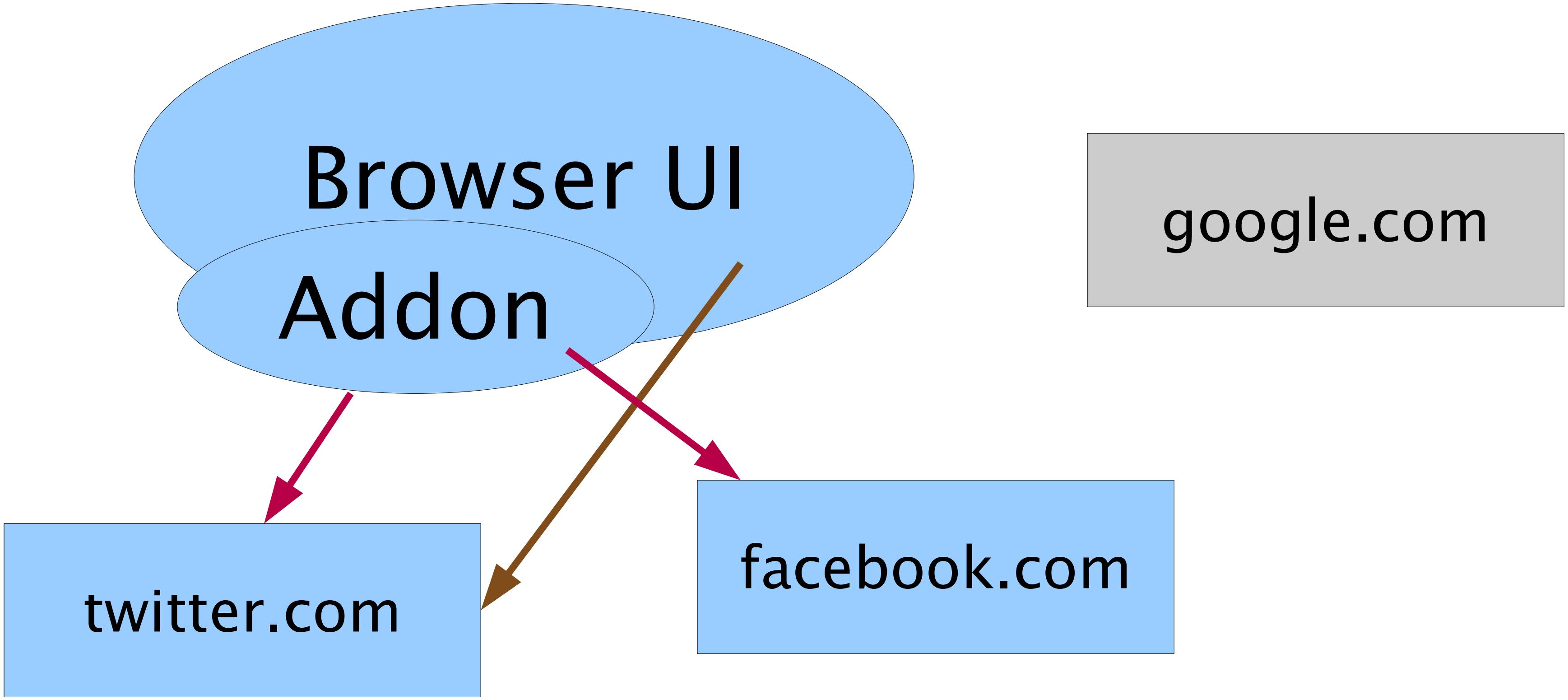


Lifehacker, Feb 2012

Blocking Addon-related Leaks



Blocking Addon-related Leaks



Browser UI

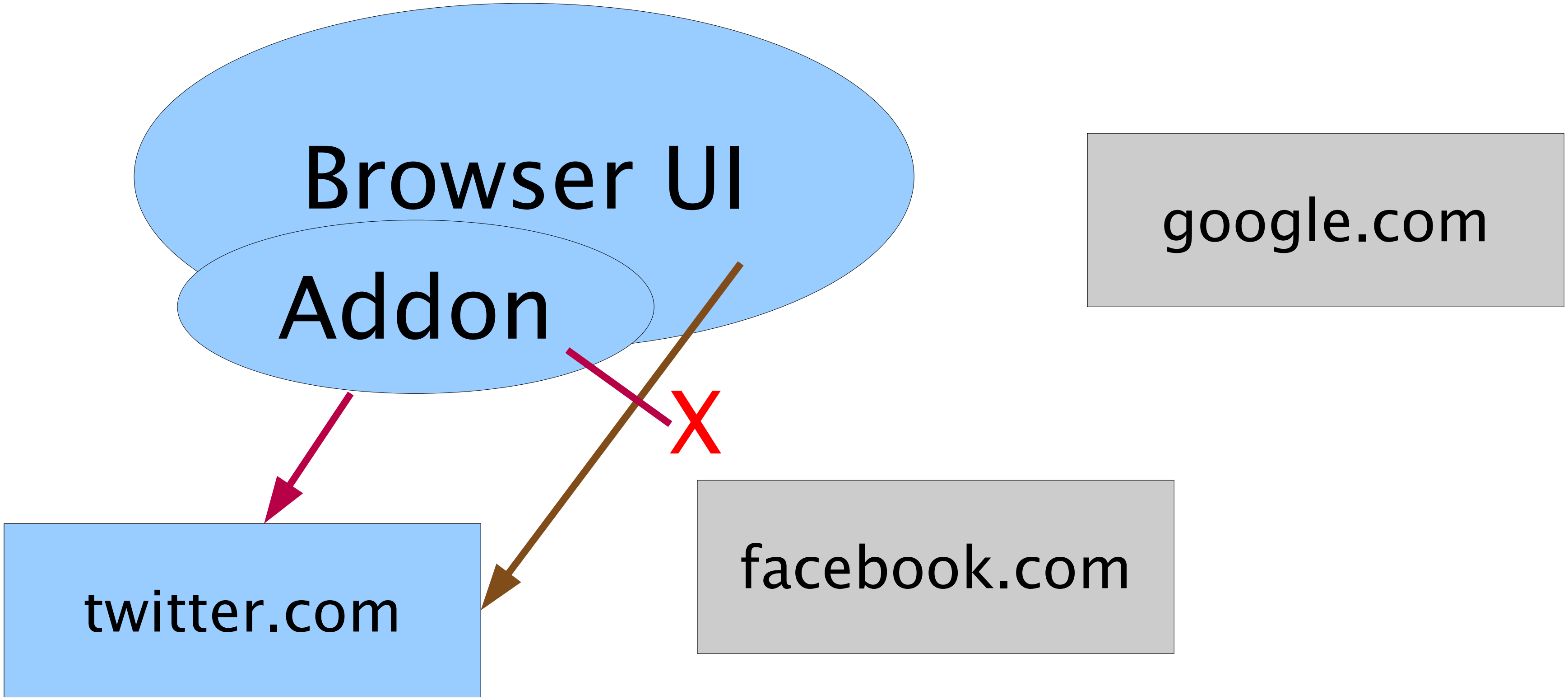
Addon

google.com

facebook.com

twitter.com

Blocking Addon-related Leaks



Lessons Learned

- Need measurement tools users can run
- Need good tools for Web developers and Firefox addon developers
- Still difficult to debug some bugs:

  “I ran Firefox for a week and leaked some memory”

Thoughts for the future:

How far can you push refcounting + cycle collection?

Interactive applications demand 60fps.

Not much time for GC pauses or VM page-in.

End of virtual memory?

Divergence between client and server workloads.

Without virtual memory, how should apps cooperate to optimize memory usage?

“OOM killing” is popular, but suboptimal. “ashmem” difficult to use.

Applications make isolated caching decisions based on little data and less principle.

Foolproof abstractions that Web developers can use to optimize memory usage across a pool of apps?

Valuable negative results:
Solutions that should work
but don't.

Questions?

Clownshoes: http://www.flickr.com/photos/29233640@N07/5131195458/

Pig: http://www.flickr.com/photos/22864665@N06/5082987037/