A Browser Developer's Research Wish List

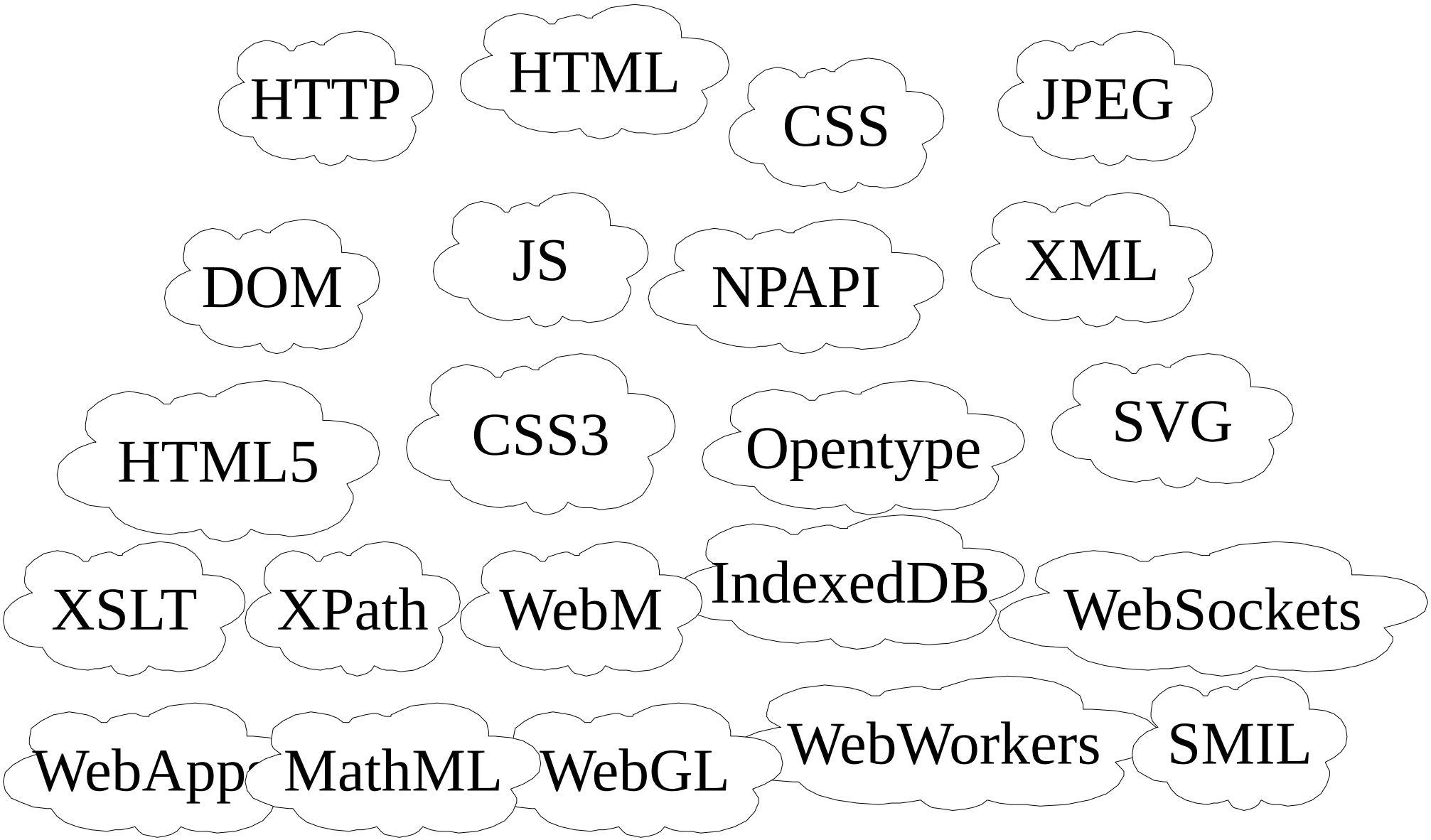
Robert O'Callahan
Mozilla Corporation

About Me

- Research career
- Mozilla career
  - Contributor
  - Developer
  - Manager

- A very quick overview of Mozilla development
- Problems that need research attention

Browsers Are Hard



```
<html>

<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 1</title>

<LINK REL=stylesheet HREF="soccer.css" TYPE="text/css">

</head>

<body style="background-attachment: fixed" background="images/puysl_08.gif">
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"><svg width="100%"
height="100%" version="1.1"
xmlns="http://www.w3.org/2000/svg"><defs>
<linearGradient id="orange_red" x1="0%" y1="0%" x2="100%" y2="0%">
<stop offset="0%" style="stop-color:rgb(255,255,0);
stop-opacity:1"/>
<stop offset="100%" style="stop-color:rgb(255,0,0);
stop-opacity:1"/>
</linearGradient>
</defs><ellipse cx="200" cy="190" rx="85" ry="55"
style="fill:url(#orange_red)"/>
<p> </p>
<p><font size="3" face="Tahoma">Welcome To <b> </b></font><b>
<font color="#FF0066" size="5" face="Tahoma">POMONA UNITED YOUTH SOCCER
LEAGUE</font></b></p>
<p><font size="3" face="Tahoma">Weekly news : Updated AGOSTO 26, 2008 </
font><b>
<font face="Tahoma" size="6" color="#FFFF00"> </font></b></p>
<p><span style="background-color: #000000"><b>
<font face="Tahoma" size="6" color="#FF00FF">NO HABRA JUEGOS PARA LABOR DAY
WEEKEND!!!!!</font></b></span></p>
<p><u><span style="background-color: #000000"><b>
<font face="Tahoma" size="6" color="#FFFF00">****ENTRENAMIENTO DE LA SELECCION
DEL 98</font></b></span></u></p>
```

HTML

You're doing it wrong.

Browsers Are Hard

- Severe performance requirements
- Severe security challenges

Browsers Are Hard

Mozilla

- Nonprofit
- Relatively small (~300 FTE)
- Large community
- > 300M users (~25% worldwide)
- Long-ish history (to 1998 and earlier)

Code

- C: 0.88M lines (many third party libs)
- C++: 1.5M lines
- .h: 0.98M lines
- JS: 0.19M lines

Being Open

- Making it easy for anyone to contribute to any level means opening everything online
  - Code
  - Data, e.g.
    - Bugs
    - Crash data
    - Test farm data
  - Decision-making
- Need to be distributed
- Need low barriers to entry

Distributed Version Control

- Mercurial (hg)
  - Like git
- Mercurial Queues (mq)
- Make it easy to factor work into many logically separate changes

Patch Lifecycle

- Bug filed in bugzilla.mozilla.org (including for new features)
- Patch attached, discussed, and formally reviewed
- Checkin, close bug

Automated Tests

- Multiple test frameworks
- Correctness and performance
- Run on every “push”

Firefox – Tinderboxpushlog

http://tests.themasta.com/tinderboxpushlog/

Google

Firefox – Tinderboxpushlog

Firefox | Firefox3.6 | MozillaTry | more...

Timezone: **local** | MVT

tnikkel@gmail.com – Sat Jun 5 16:46:55 2010 (compare:)

fdb1e4bc853d Timothy Nikkel – Bug 563878. Part 4. Add AppUnitsPerDevPixel c
83d0cd161be2 Timothy Nikkel – Bug 563878. Part 3. Fix FindViewContaining. r=
5702bf7ea7eb Timothy Nikkel – Bug 563878. Part 2. Some view/ cleanup. r=ma
2c4a36b7e9ea Timothy Nikkel – Bug 563878. Part 1c. Misc layout cleanup. r=ma
d5ca465f4238 Timothy Nikkel – Bug 563878. Part 1b. Make nsIPresShell::Render
f2991bf41c20 Timothy Nikkel – Bug 563878. Part 1a. Make nsThebesRegion hol
b2d0bd7761a1 Timothy Nikkel – Bug 8253. Part 1. Disable first-letter and first-li

Linux Bo Bd Mo (1* 1 2 2 3 3 4 4 5 5 oth oth) Md (1 1 2 2 3 3 4 4 5 5 oth oth) Co Co Cd Cd Ro Ro Rd Rd Jo Jo Jd Jd Xo Xo Xd Xd T T T T T T T

Linux64 Bo Bd Mo (1* 2 3 4* 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T

OS X Bo Bd Mo (1 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T

OS X 64 Bo Bd* Mo (2 3 4 oth) Md (2 3 4 oth) Co Cd Ro Rd T T T T T T T T

Windows Bo Bd Mo (1* 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T T T T T T T

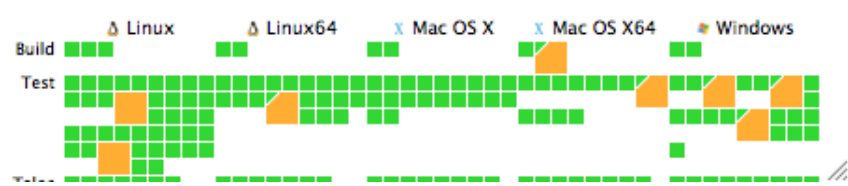
[tnikkel@gmail.com – 2010/06/05 14:51:30]
Bug 513558

s: talos-r3-fed64-037
1089 ERROR TEST-UNEXPECTED-FAIL | /tests/browser/base/content/test/test_contextmenu.html | checking item #10 (context-selectall) enabled state – got false, expected true

Rev3 Fedora 12x64 mozilla-central opt test mochitests-1/5 [test failed] Started 17:37, finished 17:44, took 7mins

- mochitest-plain-1: 63404/1/815

View Brief Log
View Full Log
Add a comment



Try-server

- “Push to try”
- Very heavily used

MozillaTry – Tinderboxpushlog

http://tests.themasta.com/tinderboxpushlog/?tree=MozillaTry

Google

MozillaTry – Tinderboxpushlog

Firefox | Firefox3.6 | **MozillaTry** | more...

Timezone: **local** | MVT

8a81c5776cad Jeff Muizelaar – imported patch cairo-update

Linux Bo Bd Mo (1 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T

OS X Bo Bd Md (1 5 oth) Cd Jd Xd T T T T T

Windows Bo Bd Mo (1 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T T T T T T T

me@kylehuey.com – Sun Jun 6 00:06:55 2010 (compare: ☐)

fb8399c7685a Kyle Huey – Bug 511648: Kill Packager.pm, replace with Package

46670e907036 Kyle Huey – Bug 231062: Part 3 – Capture self-registration infor

a4d31ad1fd8f Kyle Huey – Bug 231062: Part 2a – Fix comments in branding inf

eef6ea8c2fc3 Kyle Huey – Bug 231062: Part 2 – Provide branding information t

a0a83fc9d2d9 Kyle Huey – Bug 231062: Part 1 – Clean up the cruft from last tir

Linux Bo Bd

OS X Bo Bd

Windows Bo Bd

eakhgari@mozilla.com – Sat Jun 5 23:48:59 2010 (compare: ☐)

8d694381b4c1 Ehsan Akhgari – Bug 570350 – Crash [@ nsTextServicesDocumer

ae87e93b7483 Ehsan Akhgari – Bug 570321 – spell-check-dictionary name is n

9db47018dc05 Ehsan Akhgari – Bug 519928 – IFRAME inside designMode disabl

222978576730 Ehsan Akhgari – Bug 570192 – Make sure that XUL textbox's con

36644d587a48 Ehsan Akhgari – Bug 535490 – Intermittent timeout: browser_pri

533cb1b378ce Ehsan Akhgari – imported patch certexcep-button-madness.patc

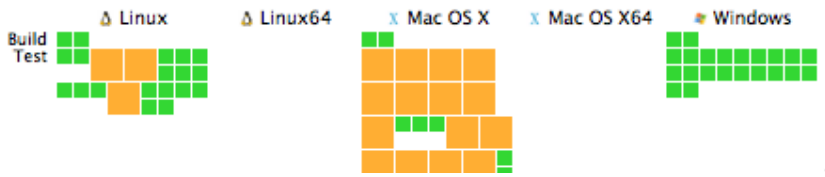
79f73867474a Ehsan Akhgari – Bug 529922 – Make sure that delayedStartup ha

ce4ba20bb13b Ehsan Akhgari – Bug 567708 – Intermittent crashtest 378325-1.

Linux Bo Bd Mo (1 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T

OS X Bo Bd Md (1 2 3 4 5 oth) Cd Rd Jd Xd T T T T T T T T

Windows Bo Bd Mo (1 2 3 4 5 oth) Md (1 2 3 4 5 oth) Co Cd Ro Rd Jo Jd Xo Xd T T T T T T T T T T T T T



Fuzz Testing

- Best bug-finding methodology so far
- Skilled operators
- Automated reduction

Adding Value To Tests

- Assertions
  - Debug only
- Leak detection
- Valgrind
- Race detection (hasn't worked?)
- Combined concrete/symbolic execution?

Crash-Stats

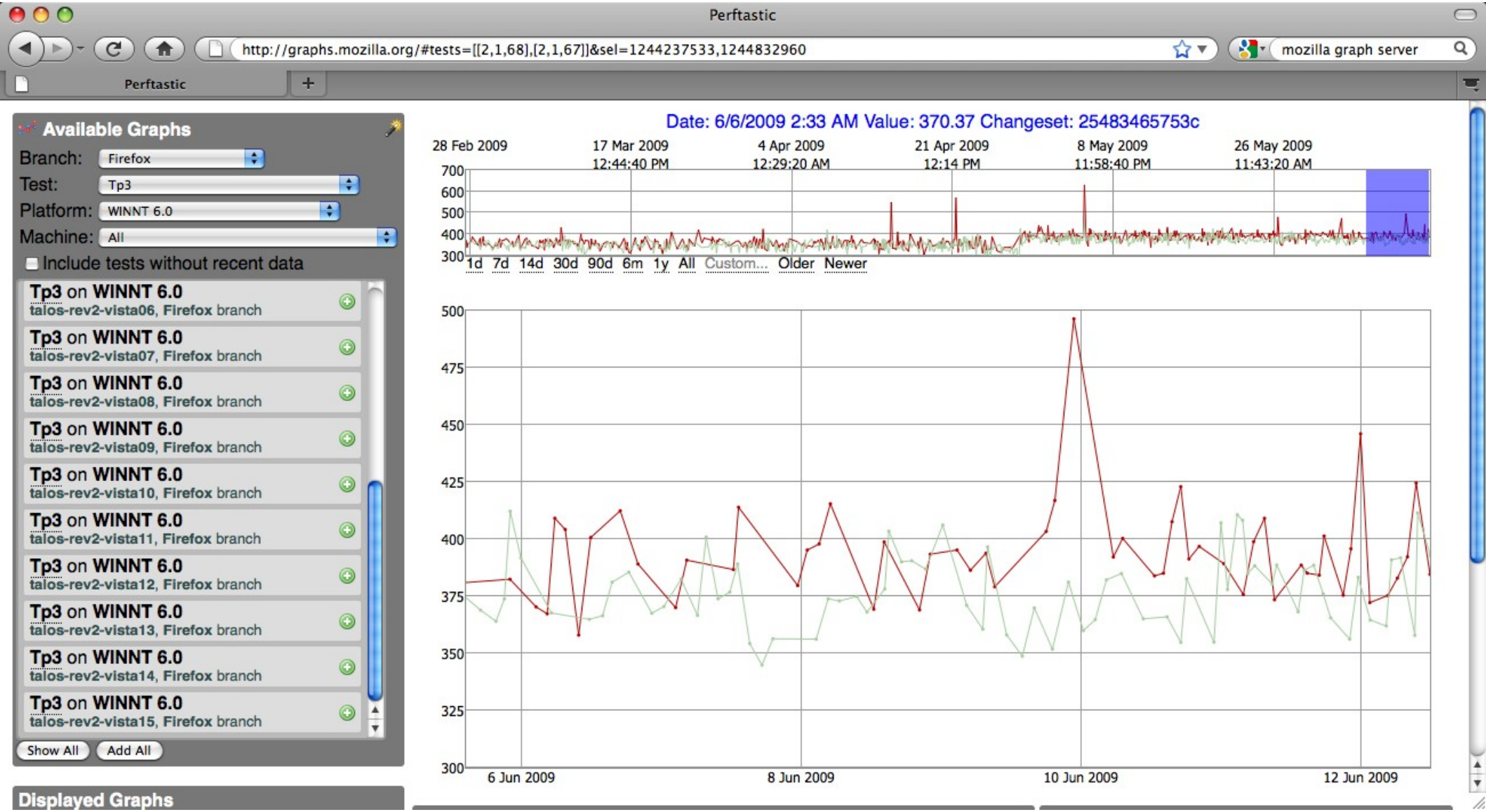
- Google Breakpad
- http://crash-stats.mozilla.org
- Long tail of low frequency, non-reproducible, inexplicable crashes
  - Sometimes due to environmental differences
  - Correlate environmental factors with crashes
    - E.g., list of loaded DLLs
  - Malware

Dehydra

- GCC plugin for AST-level access
  - Custom checkers written in JS
    - e.g. “override”
  - Dead code detection
  - Syntax-aware source code browsing (DXR)
- Refactoring using Pork (based on Elsa)
  - Renaming
  - Not much used

A Wish List

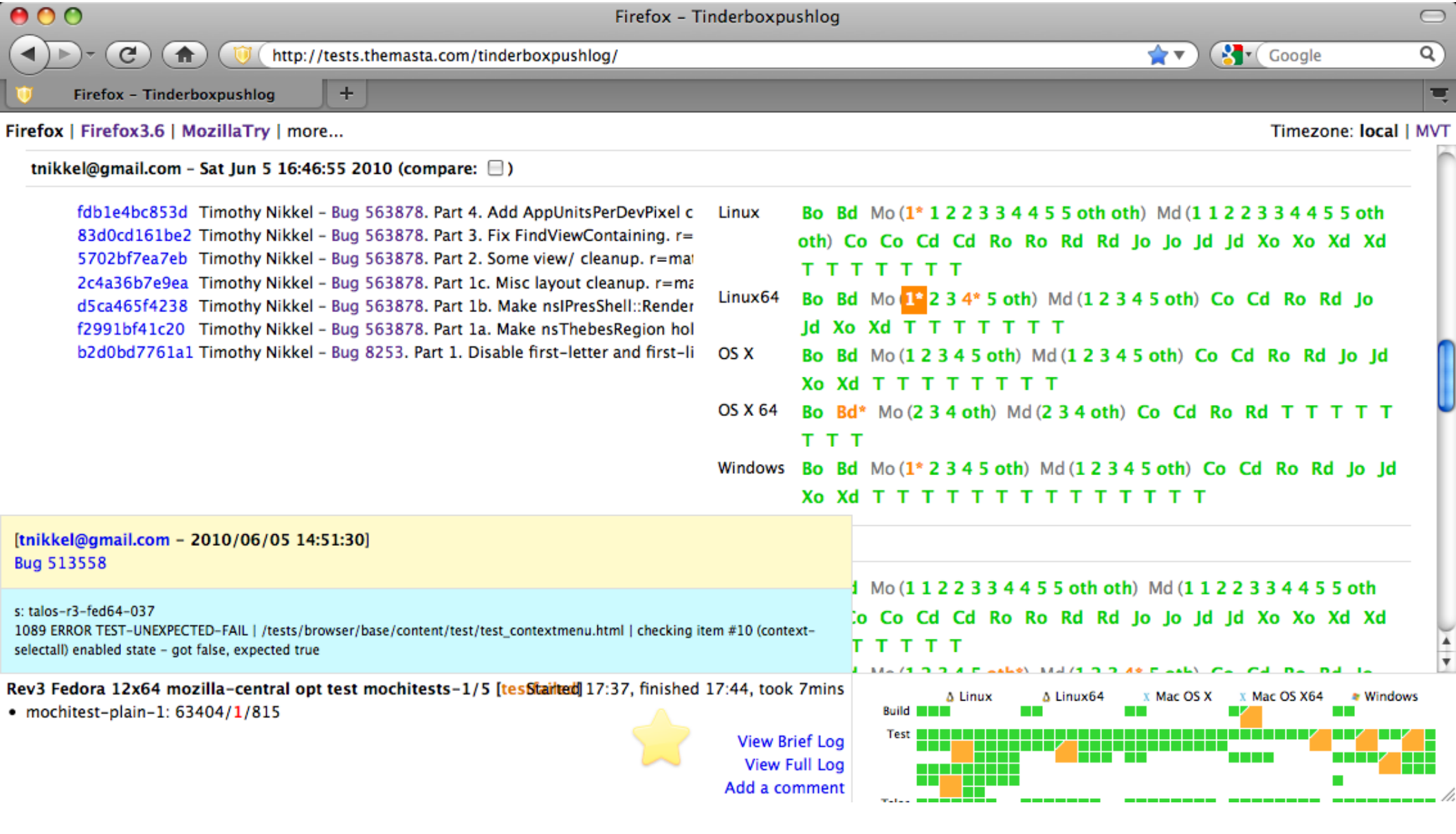
Performance Analysis



Performance Analysis

- Reduce noise
- Find significant metrics
  - e.g. instruction counts, cache misses
- Intelligent profile diffing

Nondeterministic Test Failures



VM Record And Replay

- It really works
- Best advance in debugging since …
- Need improvements
  - Overhead and reliability
  - “Always On”
  - Easy sharing
  - Application-specific extensibility (e.g. DumpJSStack())
- Combine with finer-grained R&R?

Static Analysis

- So far, no useful advanced generic analysis
- sixgill looks promising
  - Brian Hackett's PhD thesis
  - Low-annotation array bounds checking for C++
  - Works on Firefox
  - http://sixgill.org

Program Analysis And Code Review

- Unreported bugs in shipped code: low priority
- Bugs in new code: high priority
  - Regression bugs: highest priority!
- Code review is the one time we look at code to try to find bugs!
  - Use analyses to assist code review
  - Add analyses to try-server
  - Even false positives could improve review quality
  - Reviewer more likely to believe results?

Bug Finding

- Code review is a cheap time to fix bugs
- Finding a bug too late may mean it's not worth fixing
- Bug finding is not our bottleneck
  - Need to reduce cost of fixing bugs
  - (Potential) regressions are a big part of that cost

Verifying Refactorings

- DVCSs enable breaking up changes into small patches
  - Facilitates code review
  - Facilitates bisection search
  - We could use better tools for this!
- Many patches are (intended to be) behaviour-preserving refactorings

Verifying Refactorings

- Verify operational equivalence for refactoring patches
  - Check for performance effects?
- Tremendously useful because these patches consume review time
- Easy incremental research progress
- Easier and more important than automated refactoring

Code Complexity

- Simple, buggy code is better than complex, less buggy code
  - All code will need to be fixed and improved, and that will be easier for the simple code
- Less skilled developers write overcomplex code
- “Is this patch the simplest possible change?”
- Depends on entire system
  - E.g. failure to reuse existing code

Programming Languages

- Finding and fixing mountains of bugs is not sustainable
- Need approaches that prevent classes of bugs
- At some point we will need to change to better languages
- Lots to say, but out of scope

Final Plea

- Do problem-driven research, not solution-driven research
- Help!
- Thanks for inviting me :-)