



# Bringing P2P to the Web: Security and Privacy in the Firecoral Network

Jeff Terrace

Sean Stern



Hao Eric Liu

Harold Laidlaw

Michael Freedman

# Slashdot Effect



Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://box4.mercumaya.net/suspended.page/

Slashdot - Main Stories (20) x http://box4.m...pended.page/ x

## This Account Has Been Suspended

Please contact the billing/support department as soon as possible.

Views (red) / Downloads (blue)

## Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request. Please contact the server administrator, support@supportwebsite.com and inform them of the time of the error. More information about this error may be available in the server error log.

*Apache/1.3.33 Server at www.gocfr.com Port 80*

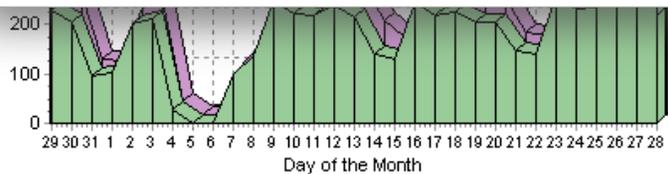
**Network Timeout**

The server at rickmahn.com is taking too long to respond.

The requested site did not respond to a connection request and the browser has stopped waiting for a reply.

- Could the server be experiencing high demand or a temporary outage? Try again later.
- Are you unable to browse other sites? Check the computer's network connection.
- Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.
- Still having trouble? Consult your network administrator or Internet provider for assistance.

Try Again



Untitled - Galeon

File Edit View Tab Settings Go Bookmarks Tools Help

Back Forward Reload Home Stop 100 http://www.armadillo

Google » Google » Google GROUPS » Google IMAGES

Search Daily BLOGs Weekly Linux TV Guide SpellCheck

Too many users... blah blah blah

Probable cause: <http://www.slashdot.org>

Try again in a few seconds...

-xian@idsoftware.com

Done.

# Existing Commercial CDNs



- Build your own solution
  - Expensive to set up
  - Only cost effective at massive scale
  
- Purchase from provider
  - Expensive
  - Requires prior knowledge of demand

The Google logo, consisting of the word "Google" in its signature multi-colored font.

The Facebook logo, featuring the word "facebook" in white lowercase letters on a blue rectangular background.

The Microsoft logo, featuring the word "Microsoft" in a bold, black, sans-serif font.

The Akamai logo, featuring a blue circular graphic with white lines and the word "Akamai" in a bold, orange, sans-serif font.

The Limelight Networks logo, featuring a green and blue graphic and the text "Limelight NETWORKS" in a sans-serif font.

The Amazon Web Services logo, featuring a stack of orange cubes and the text "amazon web services" in a sans-serif font.



- Peer-to-peer CDNs
  - Easy to use
  - Free!
  - Automatic redirection



- Unfortunately...
  - Over-subscribed
  - Under-provisioned
  - Scalability limited due to trust

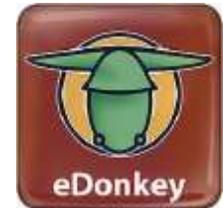
# Existing P2P Networks



- Leverage file-sharing networks
  - Demonstrated to provide scalability, fairness, and high-performance
- Design Mismatch
  - Not easily integrated into web browsers
  - High latency cost for small files



gnutella2



DC++



# Introducing Firecoral



- **What is Firecoral?**
  - A peer-to-peer network for the web
  - Integrates directly into a user's web browser
  - Ensures authenticity of content
  - Preserves user privacy
  - Backwards compatible
- **This talk's focus**
  - Security
  - Privacy
  - Usability
- **Not focused on**
  - P2P Algorithms
  - Incentives
  - Evaluation



- **Content Providers**

- Easily integrate into existing web servers
- Backwards compatibility
- Not interfere with advertisements and analytics

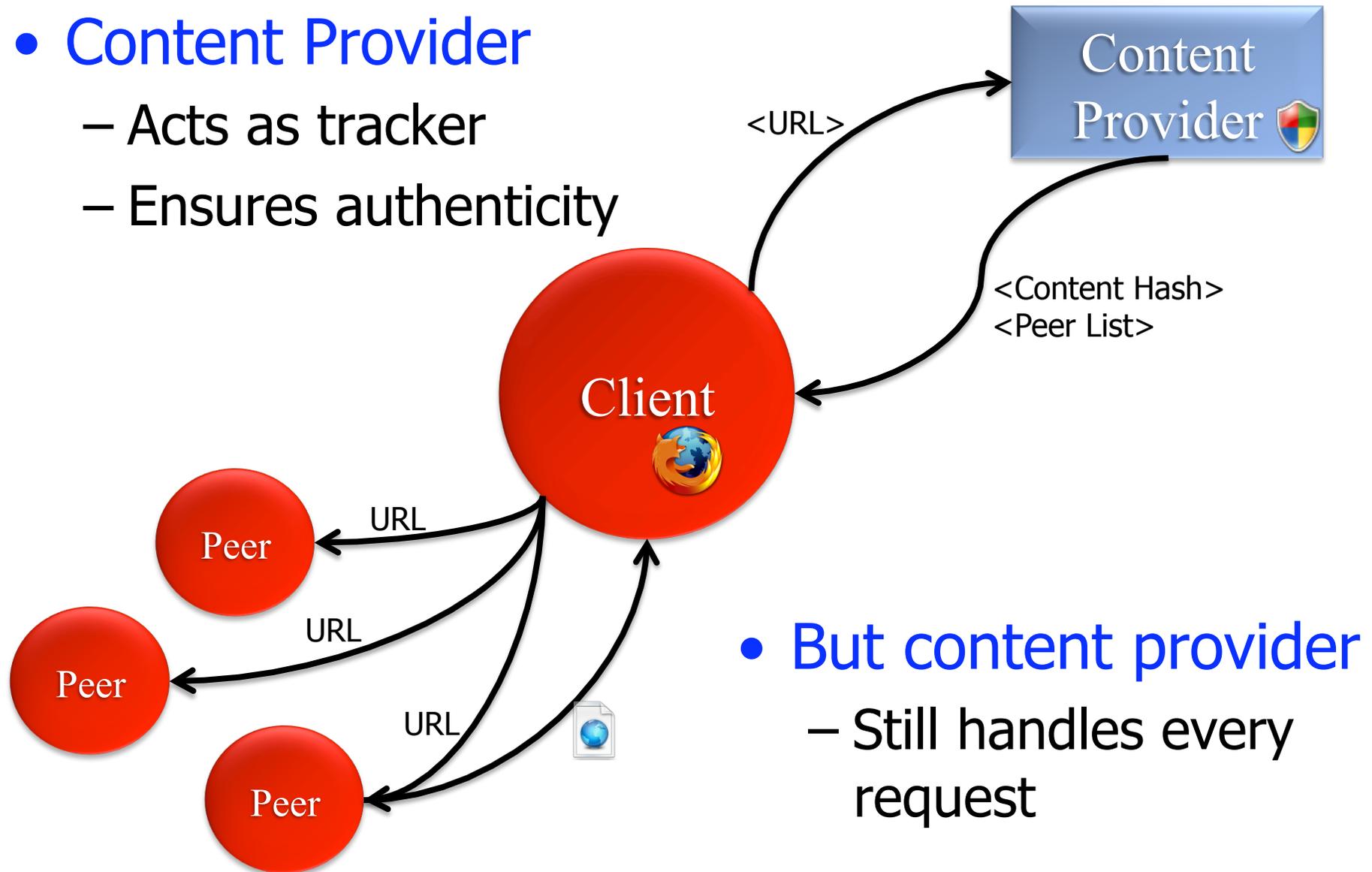
- **End Users**

- Easy to install and transparent to use
- Provide content integrity
- Respect privacy/sharing policies

# Modified Content Provider

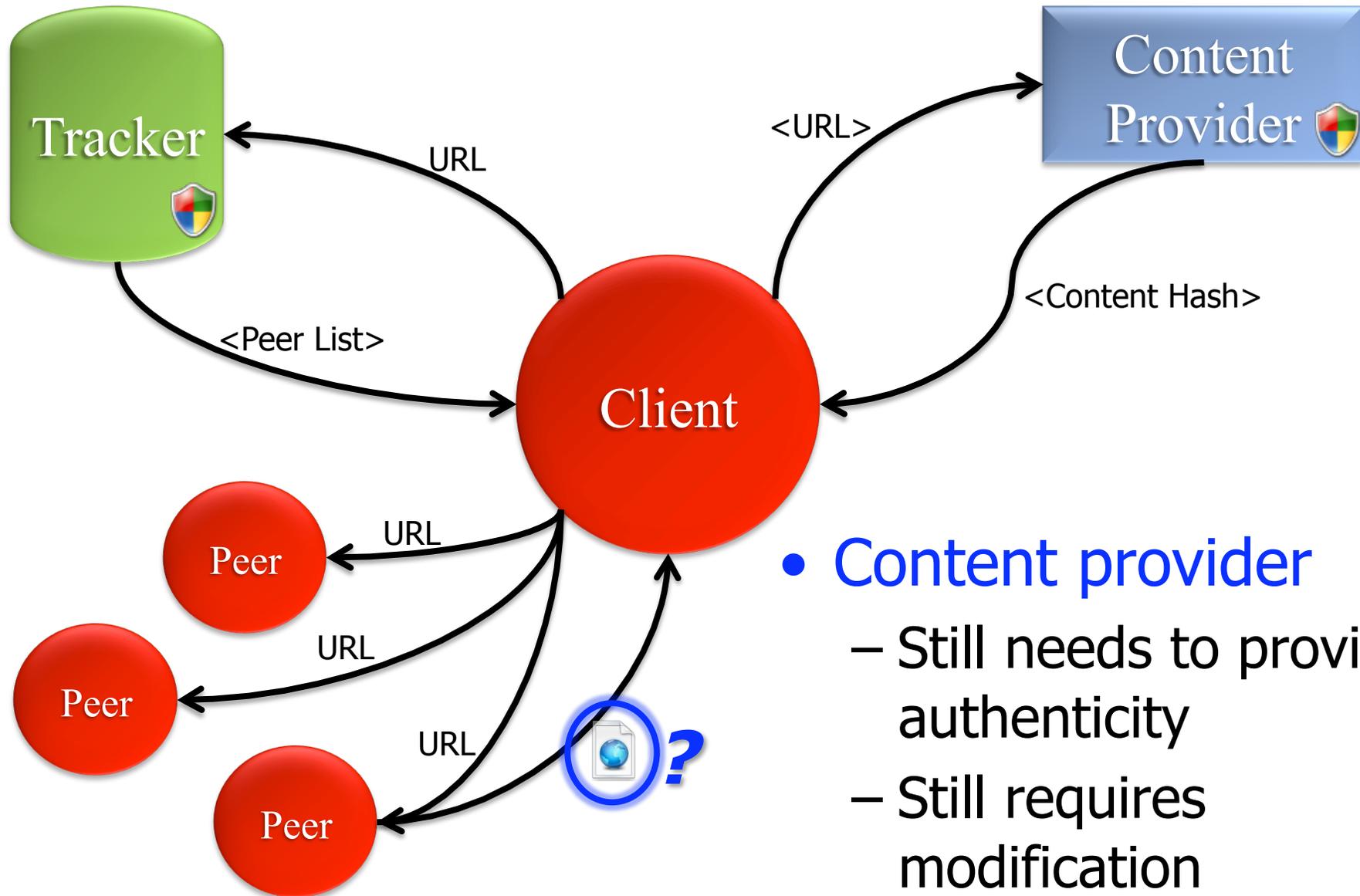


- Content Provider
  - Acts as tracker
  - Ensures authenticity



- But content provider
  - Still handles every request

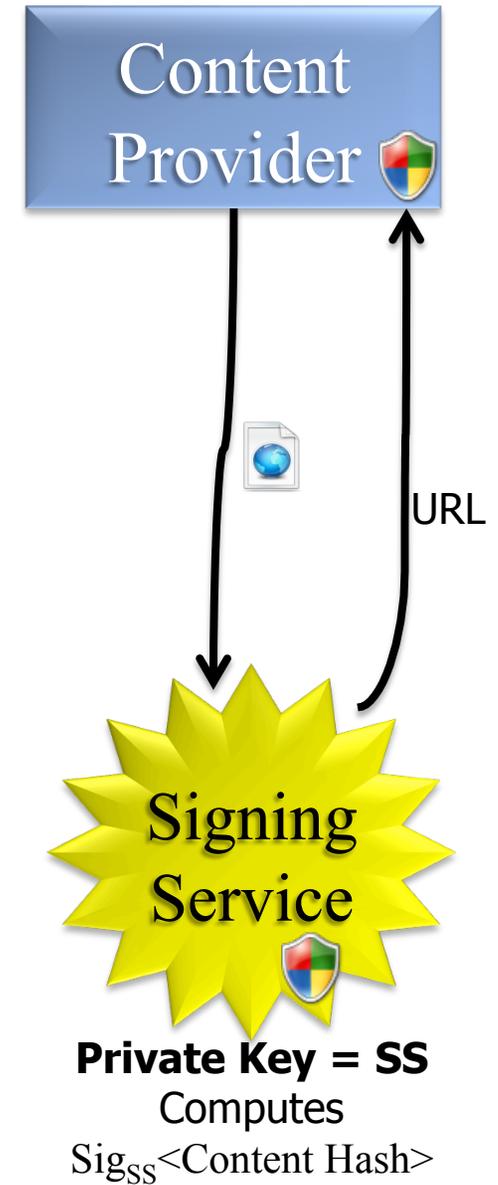
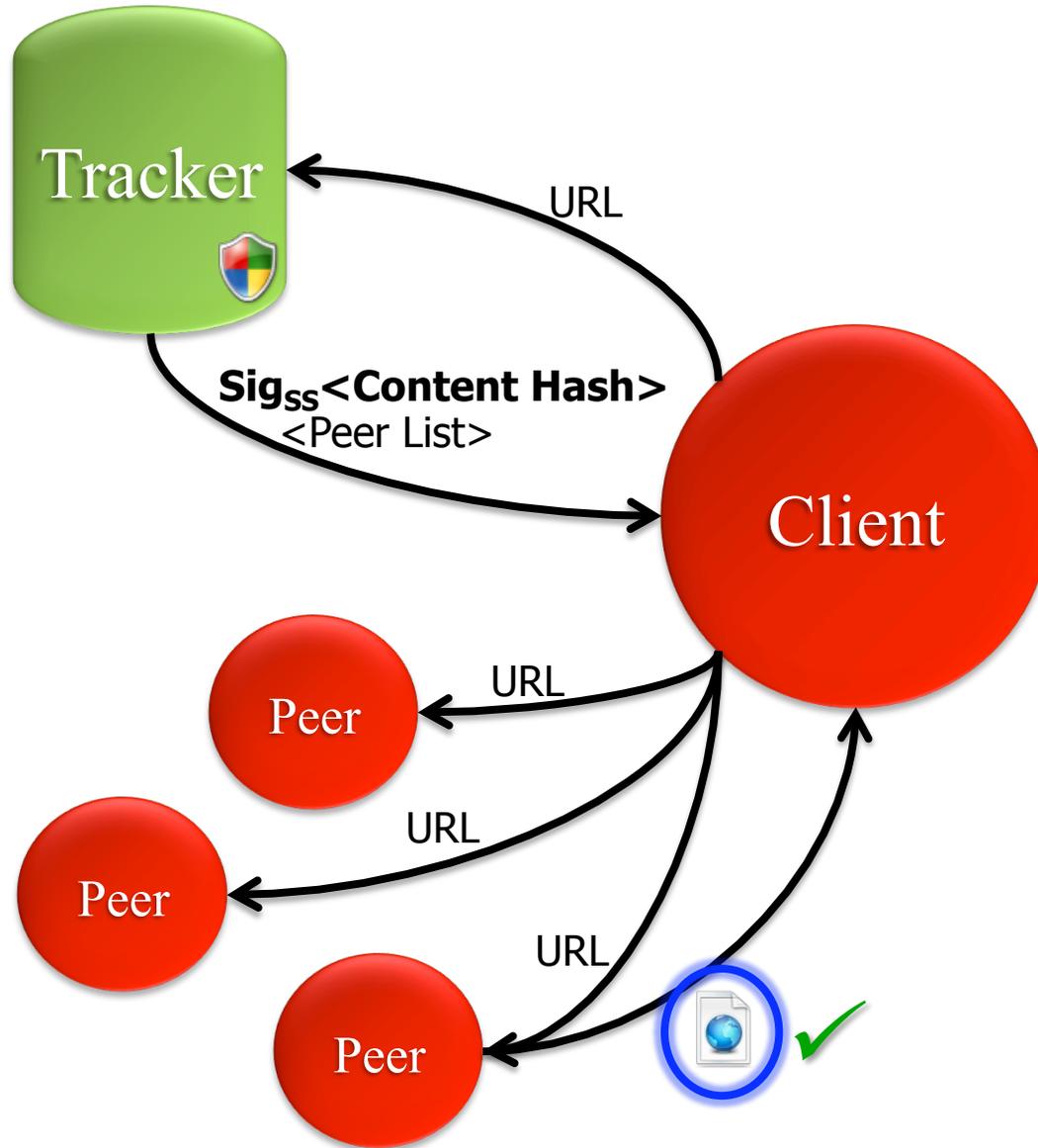
# External Tracker



- **Content provider**

- Still needs to provide authenticity
- Still requires modification

# Signing Service





- Content to avoid

- HTTPS

- Banking
    - Online Shopping

- POST Requests

- Web mail
    - Feedback forms

- Other private content?



# When to Use Firecoral

---



- **Simply list domains**
  - Too coarse grained
  - Requires site lists be known
  
- **Use HTTP referrer header**
  - Captures 3rd party advertisements
  - Interferes with analytics

# Configuration Example



Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

[Log In](#) | [Create Account](#) | [Help](#) | [Subscribe](#) | [Firehose](#)
[Why Log In?](#) | [Why Subscribe?](#)

**Sections**

- [Main](#)
- [Apple](#)
- [AskSlashdot](#)
- [Books](#)
- [Developers](#)
- [Games](#)
- [Hardware](#)
- [IT](#)
- [Idle](#)
- [Index](#)
- [Interviews](#)
- [Linux](#)
- [Mobile](#)
- [Politics](#)
- [Science](#)
- [Technology](#)
- [YRO](#)
- Help**
- [FAQ](#)
- [Bugs](#)
- Stories**
- [Old Stories](#)
- [Old Polls](#)
- [Topics](#)
- [Hall of Fame](#)

Slashdot is powered by your submissions, so send in your scoop

+ -
**Hardware: New AMD Processors Aiming Between Laptops and Netbooks**

Posted by Soulskill on Saturday November 15, @02:04AM from the not-too-big-not-too-small dept.

An anonymous reader writes with an article about AMD's Conesus chip, suggesting that it is intended to compete with Intel's Nano for the netbook market. However, CNET reports that AMD is eschewing that form factor in favor of something larger, yet still more portable than a traditional laptop. Quoting:

"AMD's strategy seems solid, in my opinion. Go for a segment that is bigger and better than Netbooks. The ultraportable category (the MacBook Air being the best example) is full of attractive but expensive designs. Why not work with PC makers to offer an ultrathin, ultralight, full-featured 13-inch notebook that is priced a lot less than \$1,800? Why not \$600 or \$700? In addition to the conventional criticism of Netbooks (small screens, tiny keyboards), an underrated fact is that many users eventually get the feeling that they're stuck with an underpowered laptop."

[Read More](#) | [5 comments](#) ▶ portables netbook hardware amd

+ -
**Games: Independent Dev Reports Over 80% Piracy Rate On DRM-Free Game**

Posted by Soulskill on Saturday November 15, @12:19AM from the trust-rewarded dept.

An anonymous reader writes

"Developer 2D Boy has written that they are seeing an 82% piracy rate for everyone's favorite DRM-free physics puzzler World of Goo. Surprisingly, this rate is in-line with what they were expecting. The article also features a fascinating comparison with the piracy rate of another game that was shipped complete with DRM, at 92%. There seemed to be no major difference in the outcomes or the rate regardless of whether DRM was used or not well no difference other than the cost to implement such nonsense "

**Interviews**

- [Blizzard Answers Your Questions. From Blizzcon](#)
- [Ask Blizzard Employees About Things That Matter](#)
- [Be Part of the 2008 Presidential Youth Debate](#)
- [Answers from Harald Welte, "VIA's Open Source Representative"](#)
- [Ask Harald Welte, "VIA's open source representative"](#)

**Slashdot Poll**

**Of childhood "building" toys, my favorite is ...**

- Tinker Toys
- Capsela
- Erector Set
- Lego
- Construx
- Lincoln Logs
- Plain old blocks
- (Something else, described below)

[ [Results](#) | [Polls](#) ]

Comments:735 | Votes:50983

**Recent Tags**

- [correlationisnotcausation](#)
- [suddenoutbreakofcommonsense](#)
- [amd](#)
- [hardware](#)
- [portables](#)



- **HTML Text**
  - Difficult to parse
  - Requires maintenance
- **Web standards!**
  - XML Path Language (XPath)
  - Queries can select XML nodes from HTML
  - XPath rules are simple and easy to write
  - Firefox executes XPath very quickly

# XPath Example



- Query for digg.com used to be:

```
//div[@class='news-summary']  
/descendant::a[starts-with(@href, 'http://')  
and not(contains(@class, 'thumb'))]/@href
```

- Digg releases “DiggBar” feature which changes HTML
- New query only changes one word:

```
//div[@class='news-summary']  
/descendant::a[starts-with(@href, 'http://')  
and not(contains(@class, 'thumb'))]/@title
```



- List of Domain/XPath pairs
- Whitelist
  - Use Firecoral
  - Contains popular news aggregators
- Blacklist
  - Don't use Firecoral
  - Contains known well-provisioned sites



- **Tracker**
  - 1000 lines of PHP running on Apache
  - Uses MySQL, Memcachedb, and Memcached
- **Signing Service**
  - 700 lines of Python
- **Firefox Extension**
  - 7000 lines of JavaScript, XUL, and CSS
  - Runs an HTTP proxy server within Firefox
  - Uses Mozilla XPConnect API for access to low-level network functions
  - Cross platform



Slashdot - News for nerds, stuff that matters (16) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://slashdot.org/ Google

Most Visited Getting Started Latest Headlines

**Slashdot** NEWS FOR NERDS. STUFF THAT MATTERS. [Submit Story](#) [Help](#) [Log In](#)

Log In Help Subscribe Firehose [Create Account](#) 14:38

Sections

- Main
- [Apple](#)
- [Ask Slashdot](#)
- [Book Reviews](#)
- [Games](#)
- [Hardware](#)
- [Idle](#)
- [Interviews](#)
- [Linux](#)

Slashdot is powered by **your submissions**, so send in your scoop

**Your Rights Online: Conviction of Sen. Ted Stevens Is Thrown Out**

Posted by [kdawson](#) on Tuesday April 07, @02:08PM from the [up-from-down-the-tubes](#) dept.

A federal judge has [thrown out the conviction](#) of the senator who educated us all about the true nature of the Internet. Ted Stevens had been [convicted last fall](#) of lying about free home renovations that he received from an oil contractor, 8 days before he lost his Senate re-election bid. The judge blasted the US Department of



**ASUS**  
Inspiring Innovation - Persistent Perfection

THE PERFORMANCE AND POWER OF A DESKTOP. MINUS THE NEED FOR A DESK.

Click Here

Powered by Intel® Core™2 Quad processor

Look for Intel Inside®

Downloads Uploads Transfer History Proxy URL List Proxying Log Parsing Log Firecoral

Time	Base	XPath	Extracted
02:40:20 PM	http://slashdot.org/	1	38
	*.slashdot.org	//div[@class='body' or @class='com...	http://www.washingtonpost.com/wp-dyn/c...
	*.slashdot.org	//div[@class='body' or @class='com...	http://www.alternativebrowseralliance.com/
	*.slashdot.org	//div[@class='body' or @class='com...	http://patft.uspto.gov/netacgi/nph-Parser...
	*.slashdot.org	//div[@class='body' or @class='com...	http://my.opera.com/haavard/blog/2009/...
	*.slashdot.org	//div[@class='body' or @class='com...	http://www.w3.org/2009/03/widgets-pag-c...
	*.slashdot.org	//div[@class='body' or @class='com...	http://www.nvtimes.com/2009/04/07/opini...

Done



- Firecoral brings P2P to the web
- Firecoral provides
  - Security
  - Privacy
  - Usability
- Allows content providers to easily support Firecoral
- Allows users to easily configure sharing and privacy policy



- **Implementation**

- NAT traversal
- Apache plug-in for signing and redirection

- **Design**

- Incentives
- Peer selection
- Measurement study

# Thank You

---



Questions?



<http://firecoral.net/>