Privacy

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

March 31, 2010

Announcements

- Reminder: on Friday go to 1 Pimental, not here, for Midterm #2
  - 5:10-6:30PM
  - You can bring a single page "cheat sheet"
    - Plus you can also bring the cheat-sheet from Midterm #1
- Note: **no section next week**

Defining Privacy

- Privacy = right to control who knows certain aspects about you / your communications / your activities
  - Control over disclosure
  - And ideally over subsequent use

- How much of an issue is this?
  E.g., how much information about you do web sites learn as you surf?

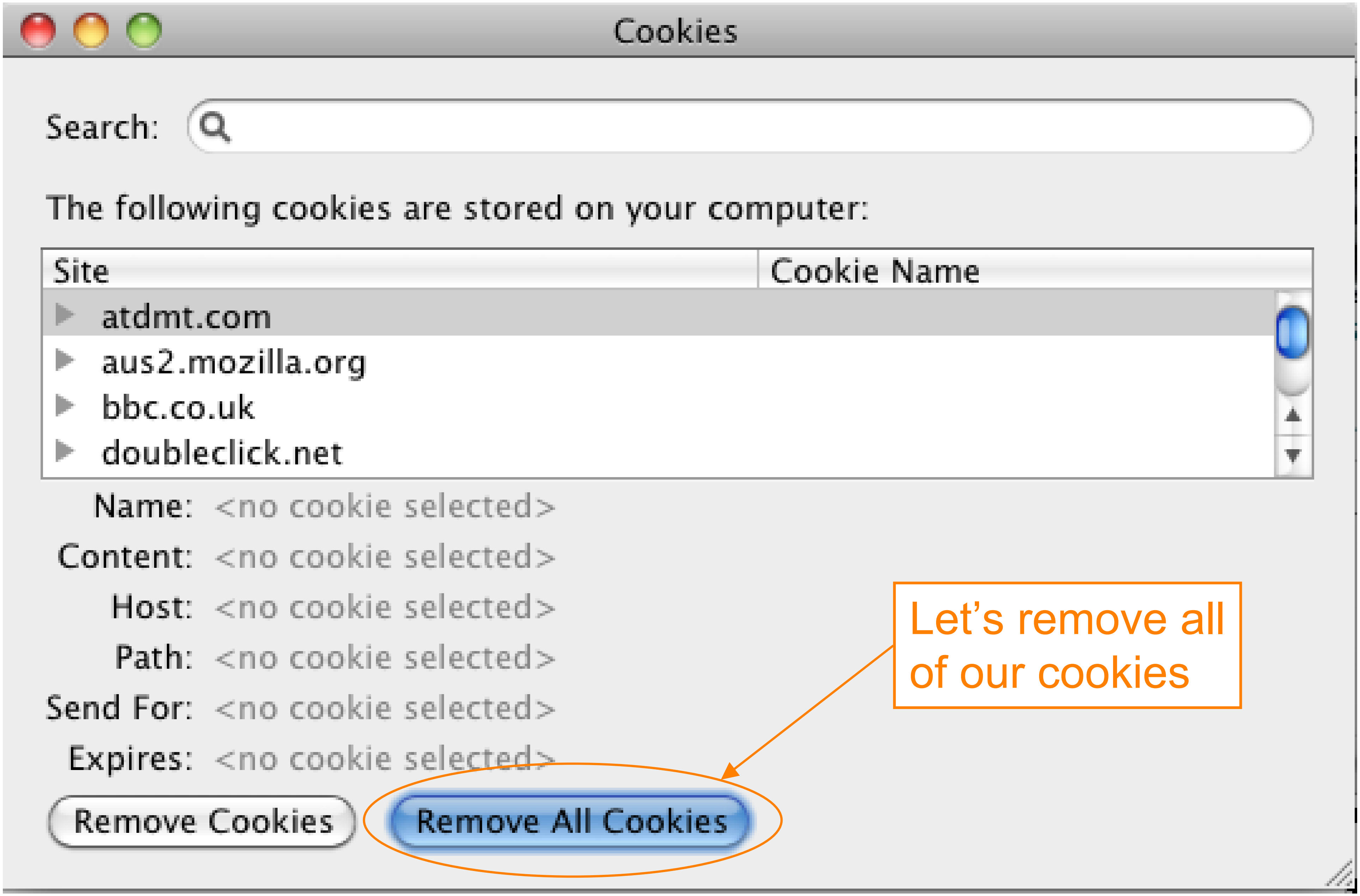
Privacy & Web Surfing

- The sites you visit learn:
  - The URLs you’re interested in
    - Google/Bing also learns *what you’re searching for*
  - Your IP address
    - Thus, your service provider & geo-location
    - Can often link you to other activity including at other sites
  - Your browser’s capabilities, which OS you run, which language you prefer
  - Which URL you looked at that took you there
    - Via “`Referer`” header

Privacy & Web Surfing, con’t

- Oh and also cookies.
- Cookies = state that server tells browser to store locally
  - Name/value pair, plus expiration date
- Browser returns the state any time visiting the same site

- Where’s the harm in that?
  And are these used much anyway?



Cookies

Search:

The following cookies are stored on your computer:

Site	Cookie Name
atdmt.com	
aus2.mozilla.org	
bbc.co.uk	
doubleclick.net	

Name: <no cookie selected>

Content: <no cookie selected>

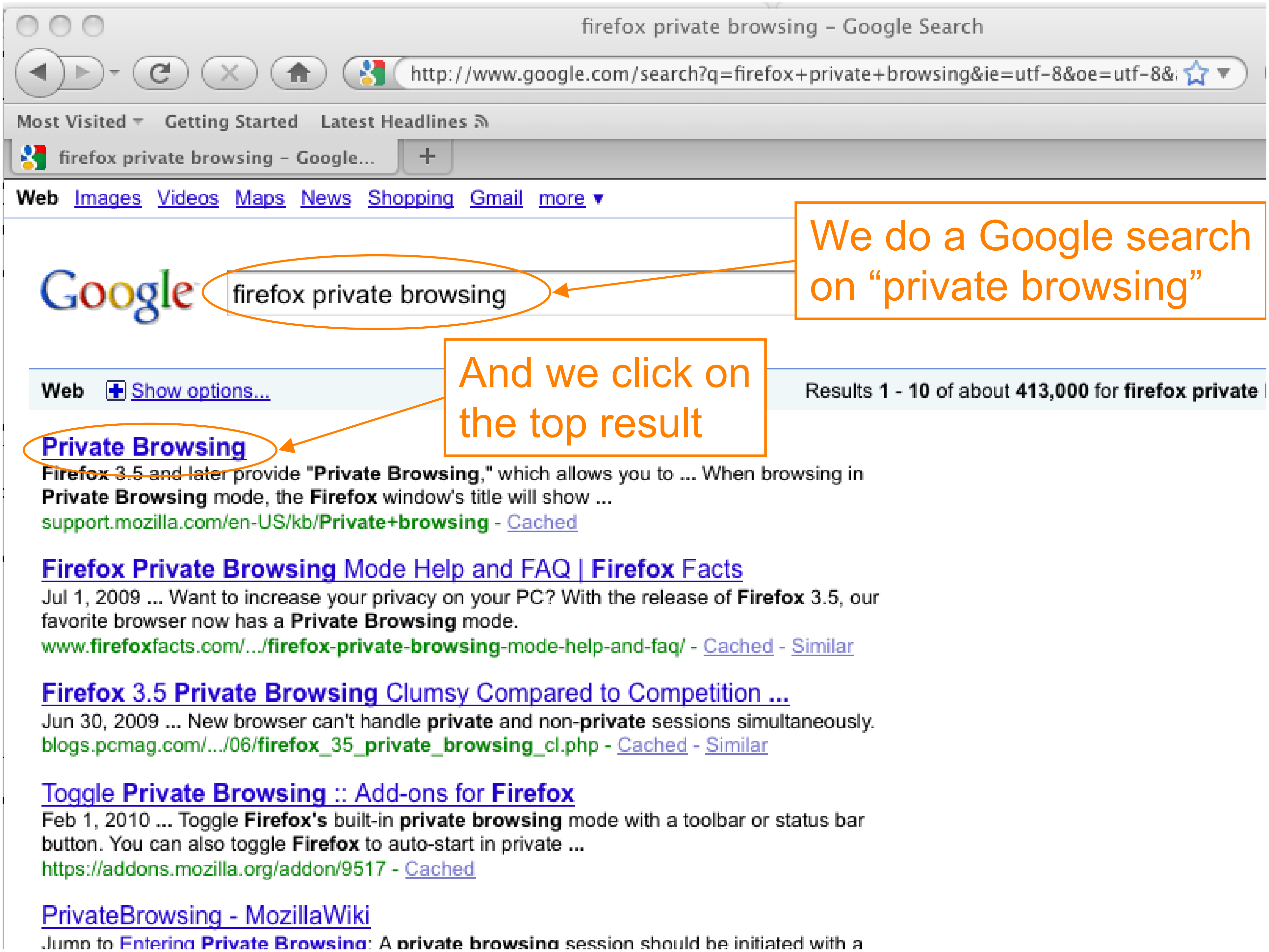
Host: <no cookie selected>

Path: <no cookie selected>

Send For: <no cookie selected>

Expires: <no cookie selected>

Let’s remove all of our cookies


firefox private browsing – Google Search
http://www.google.com/search?q=firefox+private+browsing&ie=utf-8&oe=utf-8&
Most Visited
Getting Started
Latest Headlines
firefox private browsing – Google...
Web
Images
Videos
Maps
News
Shopping
Gmail
more ▾
Google
firefox private browsing
Web
Show options...

We do a Google search on “private browsing”

And we click on the top result

Results **1** - **10** of about **413,000** for **firefox private**

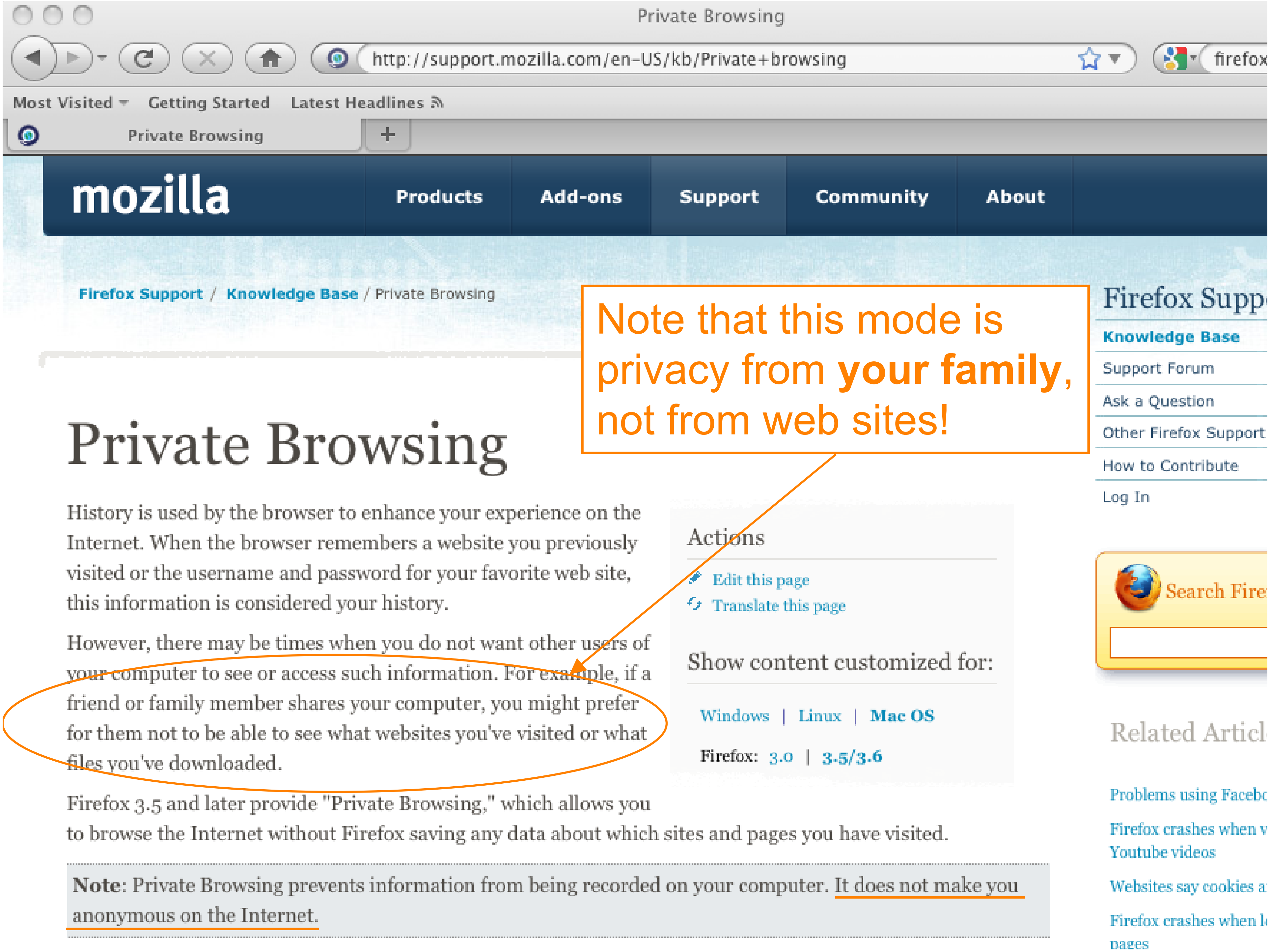
Private Browsing
Firefox 3.5 and later provide "**Private Browsing**," which allows you to ... When browsing in **Private Browsing** mode, the **Firefox** window's title will show ...
support.mozilla.com/en-US/kb/**Private+browsing** - Cached

Firefox Private Browsing Mode Help and FAQ | **Firefox** Facts
Jul 1, 2009 ... Want to increase your privacy on your PC? With the release of **Firefox** 3.5, our favorite browser now has a **Private Browsing** mode.
www.**firefox**facts.com/.../**firefox-private-browsing**-mode-help-and-faq/ - Cached - Similar

Firefox 3.5 **Private Browsing** Clumsy Compared to Competition ...
Jun 30, 2009 ... New browser can't handle **private** and non-**private** sessions simultaneously.
blogs.pcmag.com/.../06/**firefox**_35_**private**_**browsing**_cl.php - Cached - Similar

Toggle **Private Browsing** :: Add-ons for **Firefox**
Feb 1, 2010 ... Toggle **Firefox's** built-in **private browsing** mode with a toolbar or status bar button. You can also toggle **Firefox** to auto-start in private ...
https://addons.mozilla.org/addon/9517 - Cached

PrivateBrowsing - MozillaWiki
Jump to Entering **Private Browsing**: A **private browsing** session should be initiated with a



Note that this mode is privacy from **your family**, not from web sites!

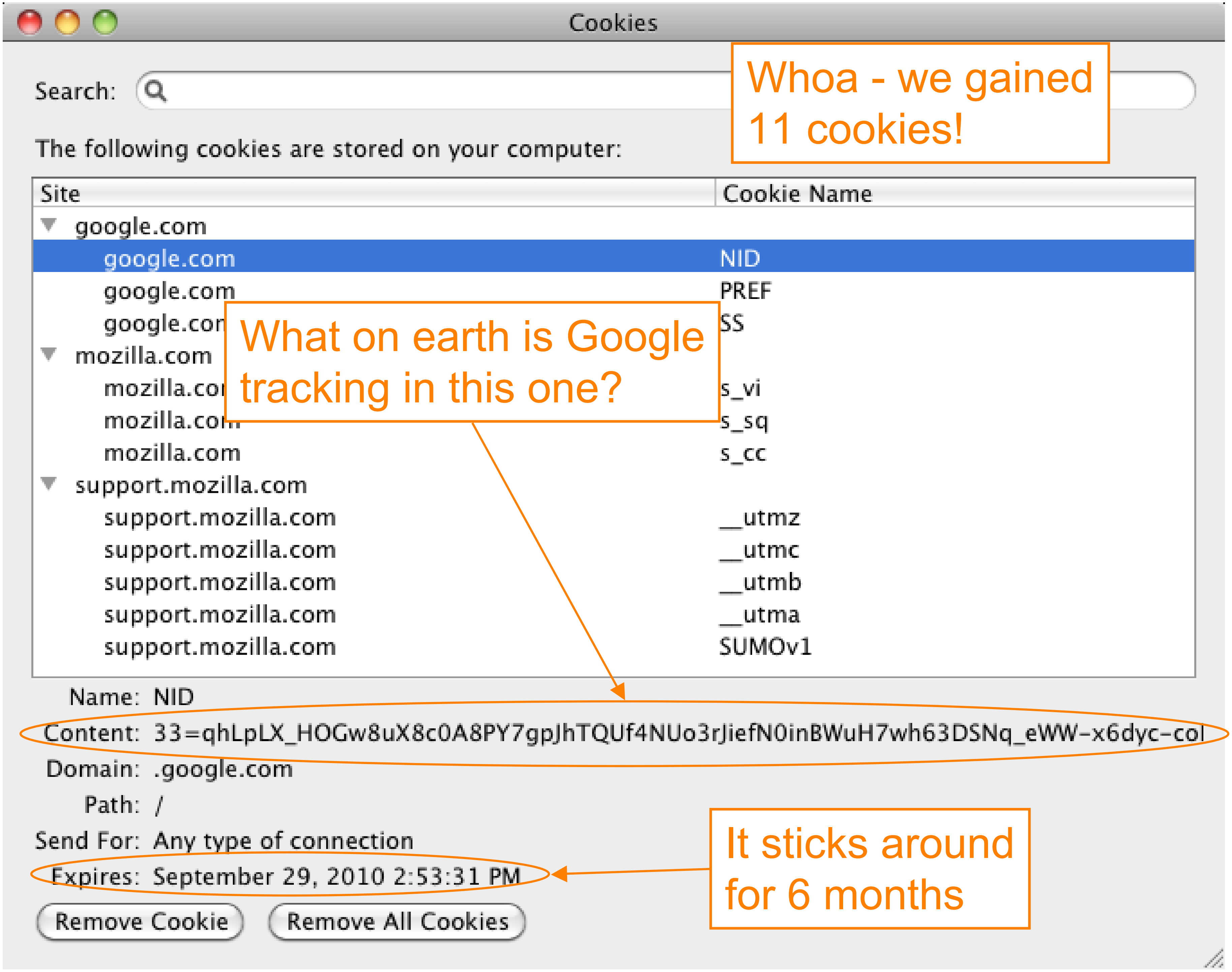
Private Browsing

History is used by the browser to enhance your experience on the Internet. When the browser remembers a website you previously visited or the username and password for your favorite web site, this information is considered your history.

However, there may be times when you do not want other users of your computer to see or access such information. For example, if a friend or family member shares your computer, you might prefer for them not to be able to see what websites you've visited or what files you've downloaded.

Firefox 3.5 and later provide "Private Browsing," which allows you to browse the Internet without Firefox saving any data about which sites and pages you have visited.

Note: Private Browsing prevents information from being recorded on your computer. It does not make you anonymous on the Internet.



The following cookies are stored on your computer:

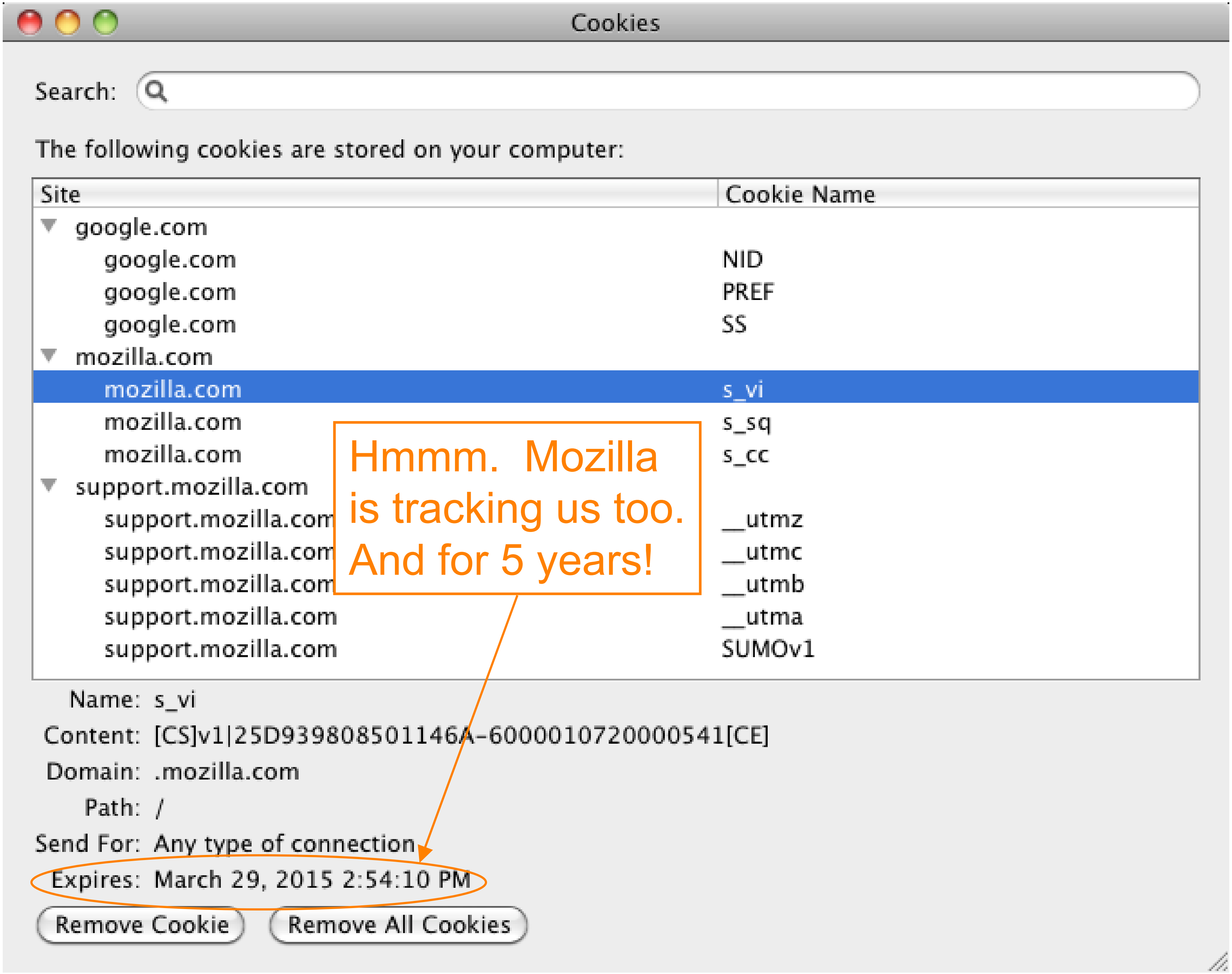
Site	Cookie Name
google.com	
google.com	NID
google.com	PREF
google.co	SS
mozilla.com	
mozilla.co	s_vi
mozilla.co	s_sq
mozilla.com	s_cc
support.mozilla.com	
support.mozilla.com	__utmz
support.mozilla.com	__utmc
support.mozilla.com	__utmb
support.mozilla.com	__utma
support.mozilla.com	SUMOv1

Name: NID
Content: 33=qhLpLX_HOGw8uX8c0A8PY7gpJhTQUf4NUo3rJiefN0inBWuH7wh63DSNq_eWW-x6dyc-col
Domain: .google.com
Path: /
Send For: Any type of connection
Expires: September 29, 2010 2:53:31 PM

Whoa - we gained 11 cookies!

What on earth is Google tracking in this one?

It sticks around for 6 months

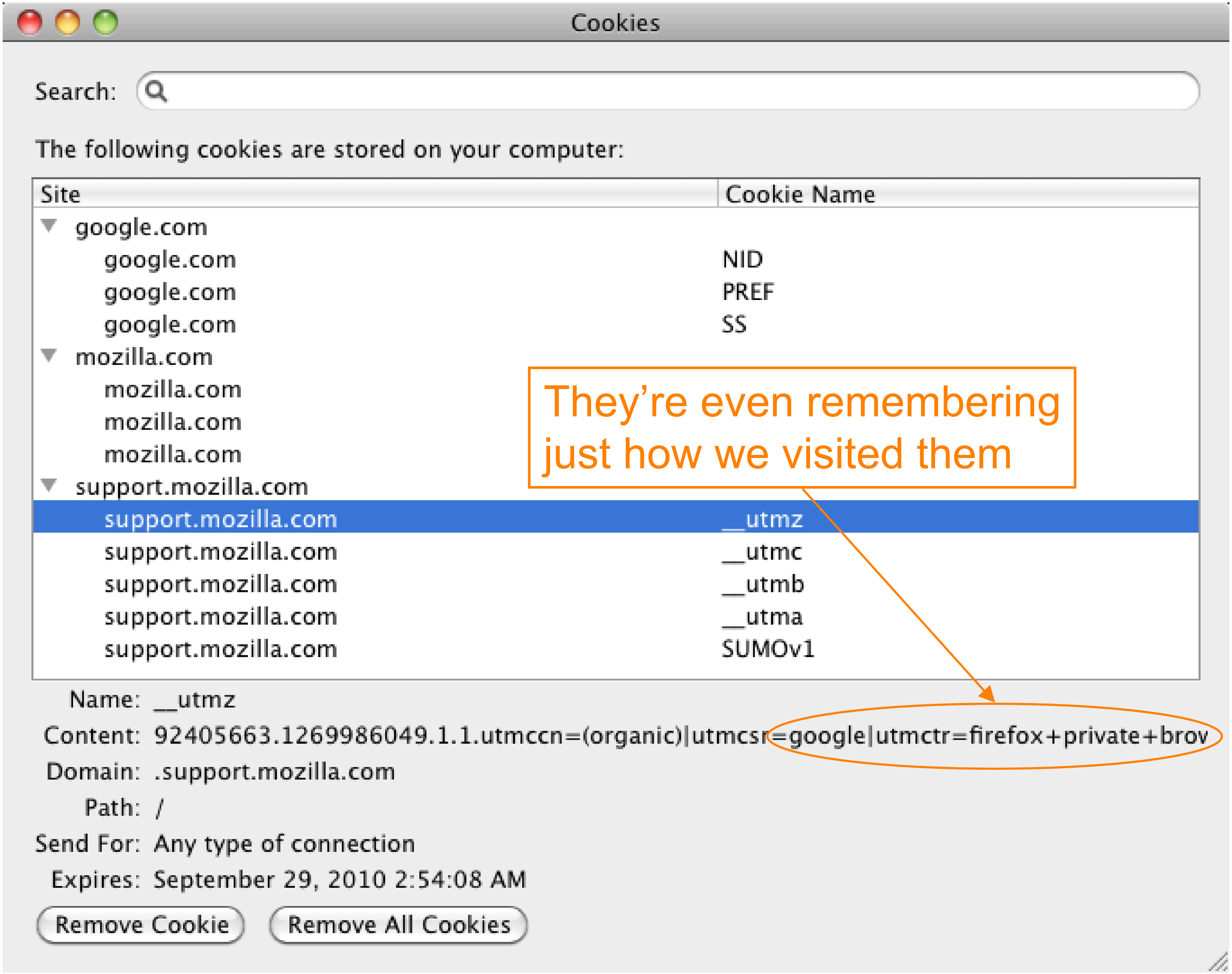


The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	NID
google.com	PREF
google.com	SS
▼ mozilla.com	
mozilla.com	s_vi
mozilla.com	s_sq
mozilla.com	s_cc
▼ support.mozilla.com	
support.mozilla.com	__utmz
support.mozilla.com	__utmc
support.mozilla.com	__utmb
support.mozilla.com	__utma
support.mozilla.com	SUMOv1

Name: s_vi
Content: [CS]v1|25D939808501146A-6000010720000541[CE]
Domain: .mozilla.com
Path: /
Send For: Any type of connection
Expires: March 29, 2015 2:54:10 PM

Hmmm. Mozilla is tracking us too. And for 5 years!

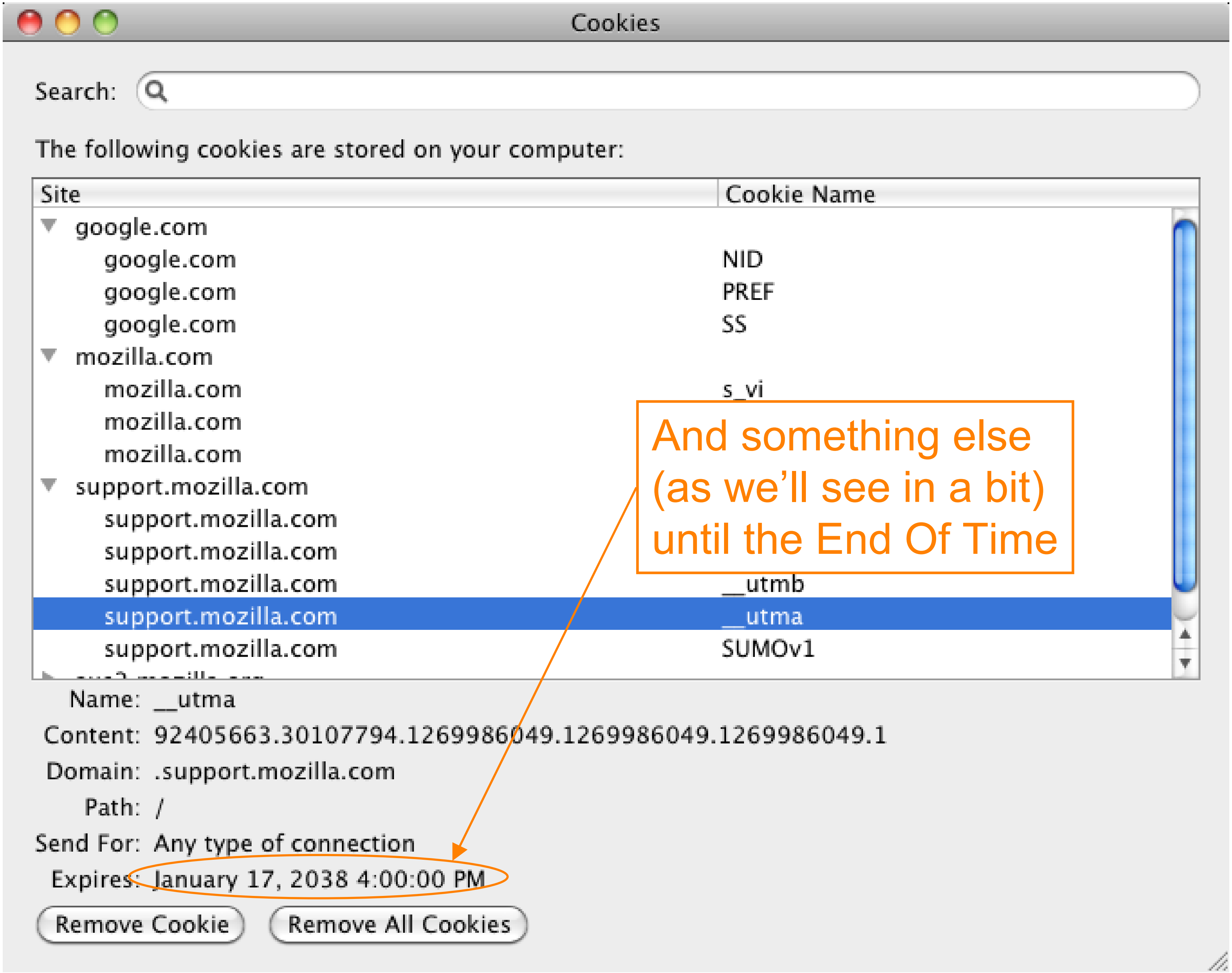


The following cookies are stored on your computer:

Site	Cookie Name
google.com	
google.com	NID
google.com	PREF
google.com	SS
mozilla.com	
mozilla.com	
mozilla.com	
mozilla.com	
support.mozilla.com	
support.mozilla.com	__utmz
support.mozilla.com	__utmc
support.mozilla.com	__utmb
support.mozilla.com	__utma
support.mozilla.com	SUMOv1

Name: __utmz
Content: 92405663.1269986049.1.1.utmccn=(organic)|utmcsr=google|utmctr=firefox+private+brov
Domain: .support.mozilla.com
Path: /
Send For: Any type of connection
Expires: September 29, 2010 2:54:08 AM

They're even remembering just how we visited them

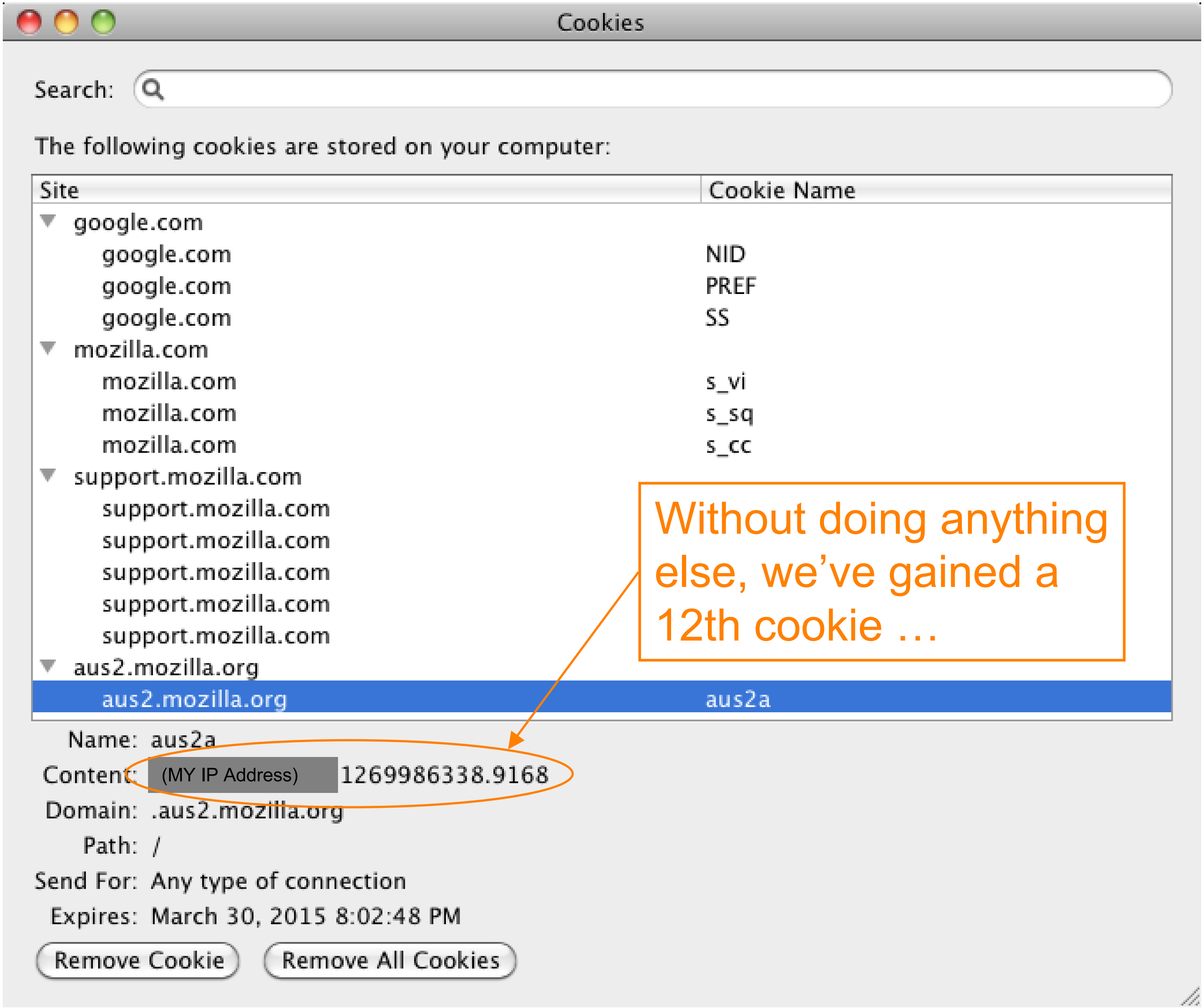


The following cookies are stored on your computer:

Site	Cookie Name
google.com	
google.com	NID
google.com	PREF
google.com	SS
mozilla.com	
mozilla.com	s_vi
mozilla.com	
mozilla.com	
support.mozilla.com	
support.mozilla.com	
support.mozilla.com	
support.mozilla.com	__utmb
support.mozilla.com	__utma
support.mozilla.com	SUMOv1

Name: __utma
Content: 92405663.30107794.1269986049.1269986049.1269986049.1
Domain: .support.mozilla.com
Path: /
Send For: Any type of connection
Expires: January 17, 2038 4:00:00 PM

And something else (as we'll see in a bit) until the End Of Time



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	NID
google.com	PREF
google.com	SS
▼ mozilla.com	
mozilla.com	s_vi
mozilla.com	s_sq
mozilla.com	s_cc
▼ support.mozilla.com	
support.mozilla.com	
support.mozilla.com	
support.mozilla.com	
support.mozilla.com	
support.mozilla.com	
▼ aus2.mozilla.org	
aus2.mozilla.org	aus2a

Name: aus2a

Content: (MY IP Address) 1269986338.9168

Domain: .aus2.mozilla.org

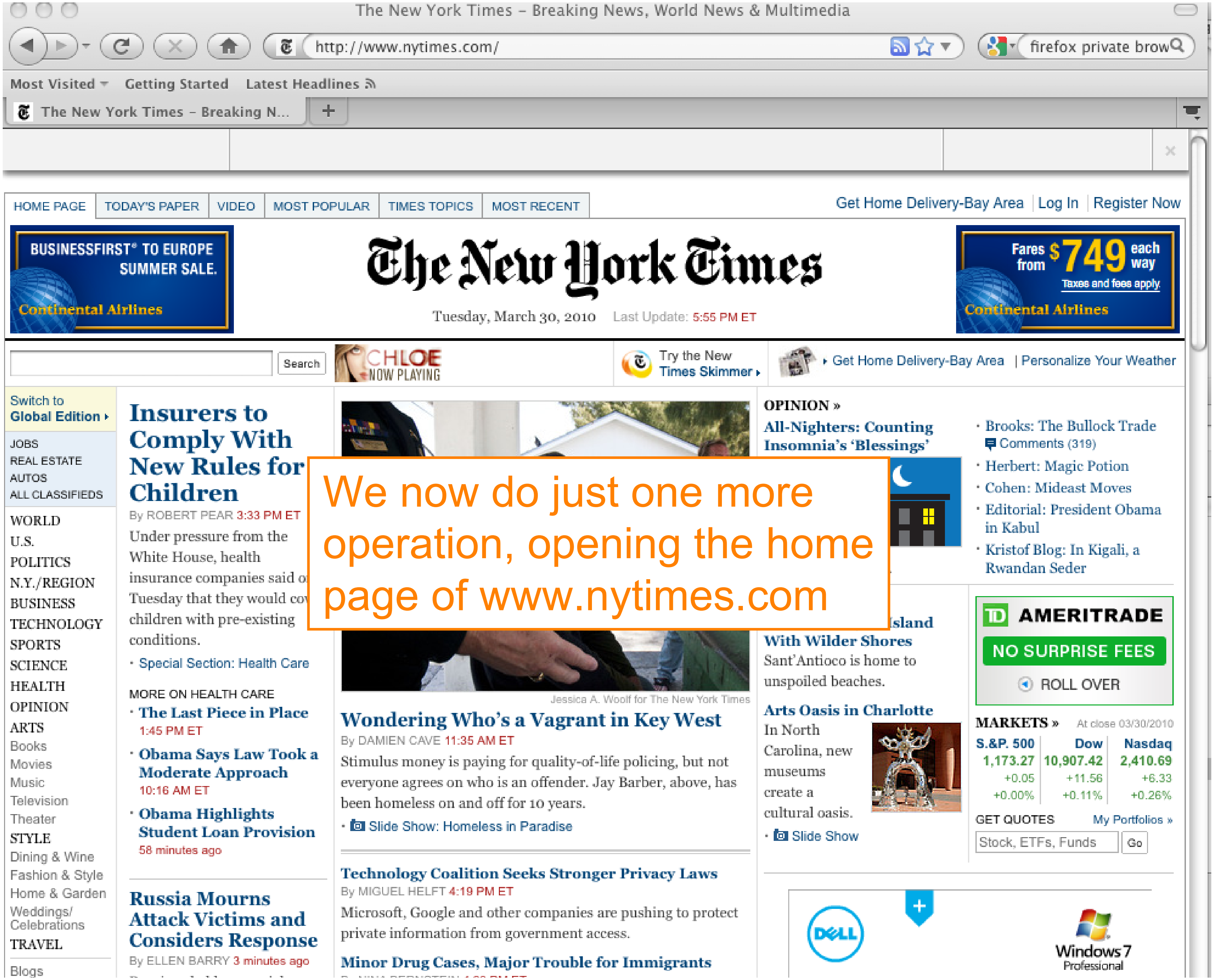
Path: /

Send For: Any type of connection

Expires: March 30, 2015 8:02:48 PM

Without doing anything else, we've gained a 12th cookie …

We now do just one more operation, opening the home page of www.nytimes.com



The New York Times - Breaking News, World News & Multimedia

http://www.nytimes.com/

firefox private brow

Most Visited | Getting Started | Latest Headlines

The New York Times - Breaking N...

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS | MOST RECENT

Get Home Delivery-Bay Area | Log In | Register Now

BUSINESSFIRST® TO EUROPE SUMMER SALE. Continental Airlines

The New York Times

Tuesday, March 30, 2010 Last Update: 5:55 PM ET

Fares from $749 each way Taxes and fees apply Continental Airlines

Search

CHLOE NOW PLAYING

Try the New Times Skimmer

Get Home Delivery-Bay Area | Personalize Your Weather

Switch to Global Edition

JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/ Celebrations
TRAVEL
Blogs

Insurers to Comply With New Rules for Children

By ROBERT PEAR 3:33 PM ET

Under pressure from the White House, health insurance companies said o Tuesday that they would cov children with pre-existing conditions.

- Special Section: Health Care

MORE ON HEALTH CARE

- The Last Piece in Place 1:45 PM ET
- Obama Says Law Took a Moderate Approach 10:16 AM ET
- Obama Highlights Student Loan Provision 58 minutes ago

Russia Mourns Attack Victims and Considers Response

By ELLEN BARRY 3 minutes ago

Jessica A. Woolf for The New York Times

Wondering Who's a Vagrant in Key West

By DAMIEN CAVE 11:35 AM ET

Stimulus money is paying for quality-of-life policing, but not everyone agrees on who is an offender. Jay Barber, above, has been homeless on and off for 10 years.

- Slide Show: Homeless in Paradise

Technology Coalition Seeks Stronger Privacy Laws

By MIGUEL HELFT 4:19 PM ET

Microsoft, Google and other companies are pushing to protect private information from government access.

Minor Drug Cases, Major Trouble for Immigrants

OPINION »

All-Nighters: Counting Insomnia's 'Blessings'

- Brooks: The Bullock Trade Comments (319)
- Herbert: Magic Potion
- Cohen: Mideast Moves
- Editorial: President Obama in Kabul
- Kristof Blog: In Kigali, a Rwandan Seder

Island With Wilder Shores

Sant'Antioco is home to unspoiled beaches.

Arts Oasis in Charlotte

In North Carolina, new museums create a cultural oasis.

- Slide Show

TD AMERITRADE NO SURPRISE FEES ROLL OVER

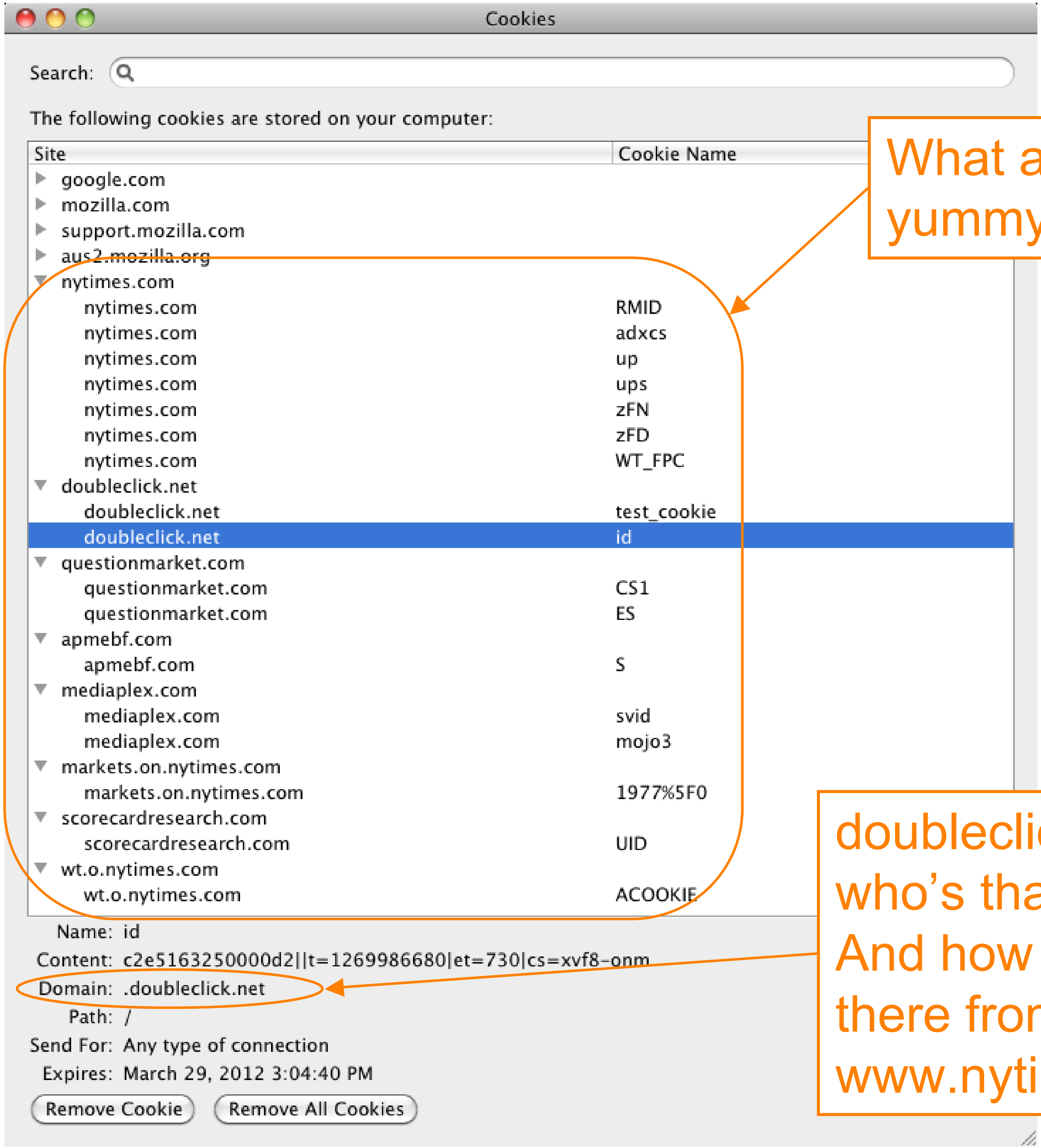
MARKETS » At close 03/30/2010

S.&P. 500	Dow	Nasdaq
1,173.27	10,907.42	2,410.69
+0.05	+11.56	+6.33
+0.00%	+0.11%	+0.26%

GET QUOTES My Portfolios »

Stock, ETFs, Funds Go

DELL Windows 7 Professional



The following cookies are stored on your computer:

Site	Cookie Name
google.com	
mozilla.com	
support.mozilla.com	
aus2.mozilla.org	
nytimes.com	
nytimes.com	RMID
nytimes.com	adxcs
nytimes.com	up
nytimes.com	ups
nytimes.com	zFN
nytimes.com	zFD
nytimes.com	WT_FPC
doubleclick.net	
doubleclick.net	test_cookie
doubleclick.net	id
questionmarket.com	
questionmarket.com	CS1
questionmarket.com	ES
apmebf.com	
apmebf.com	S
mediaplex.com	
mediaplex.com	svid
mediaplex.com	mojo3
markets.on.nytimes.com	
markets.on.nytimes.com	1977%5F0
scorecardresearch.com	
scorecardresearch.com	UID
wt.o.nytimes.com	
wt.o.nytimes.com	ACOOKIE

Name: id
Content: c2e5163250000d2||t=1269986680|et=730|cs=xvf8-onm
Domain: .doubleclick.net
Path: /
Send For: Any type of connection
Expires: March 29, 2012 3:04:40 PM

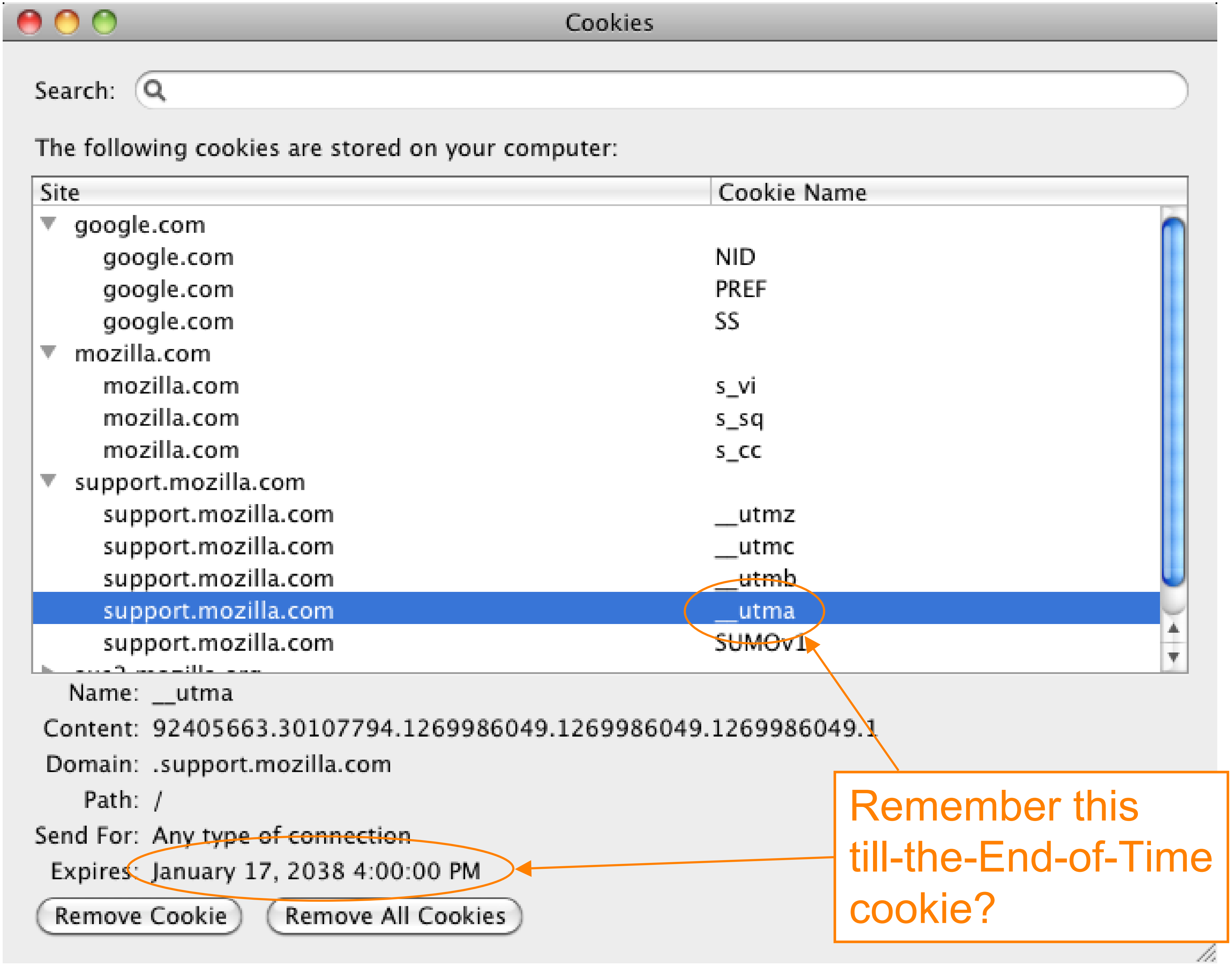
What a lot of yummy cookies!

doubleclick.net - who’s that?
And how did it get there from visiting www.nytimes.com?

Third-Party Cookies

- How can a web site enable a third party to plant cookies in your browser & later retrieve them?
  - Answer: using a “web bug”
  - Include on the site’s page (for example):
    - `<img src="http://doubleclick.net/ad.gif" width=1 height=1>`
- Why would a site do that?
  - Site has a business relationship w/ DoubleClick*
  - Now DoubleClick sees all of your activity that involves their web sites (each of them includes the web bug)
    - Because your browser dutifully sends them their cookies for any web page that has that web bug
    - Identifier in cookie ties together activity as = YOU

* Owned by Google, by the way



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	NID
google.com	PREF
google.com	SS
▼ mozilla.com	
mozilla.com	s_vi
mozilla.com	s_sq
mozilla.com	s_cc
▼ support.mozilla.com	
support.mozilla.com	__utmz
support.mozilla.com	__utmc
support.mozilla.com	__utmb
support.mozilla.com	__utma
support.mozilla.com	SUMOv1

Name: __utma
Content: 92405663.30107794.1269986049.1269986049.1269986049.1
Domain: .support.mozilla.com
Path: /
Send For: Any type of connection
Expires: January 17, 2038 4:00:00 PM

Remember this till-the-End-of-Time cookie?

Google Analytics

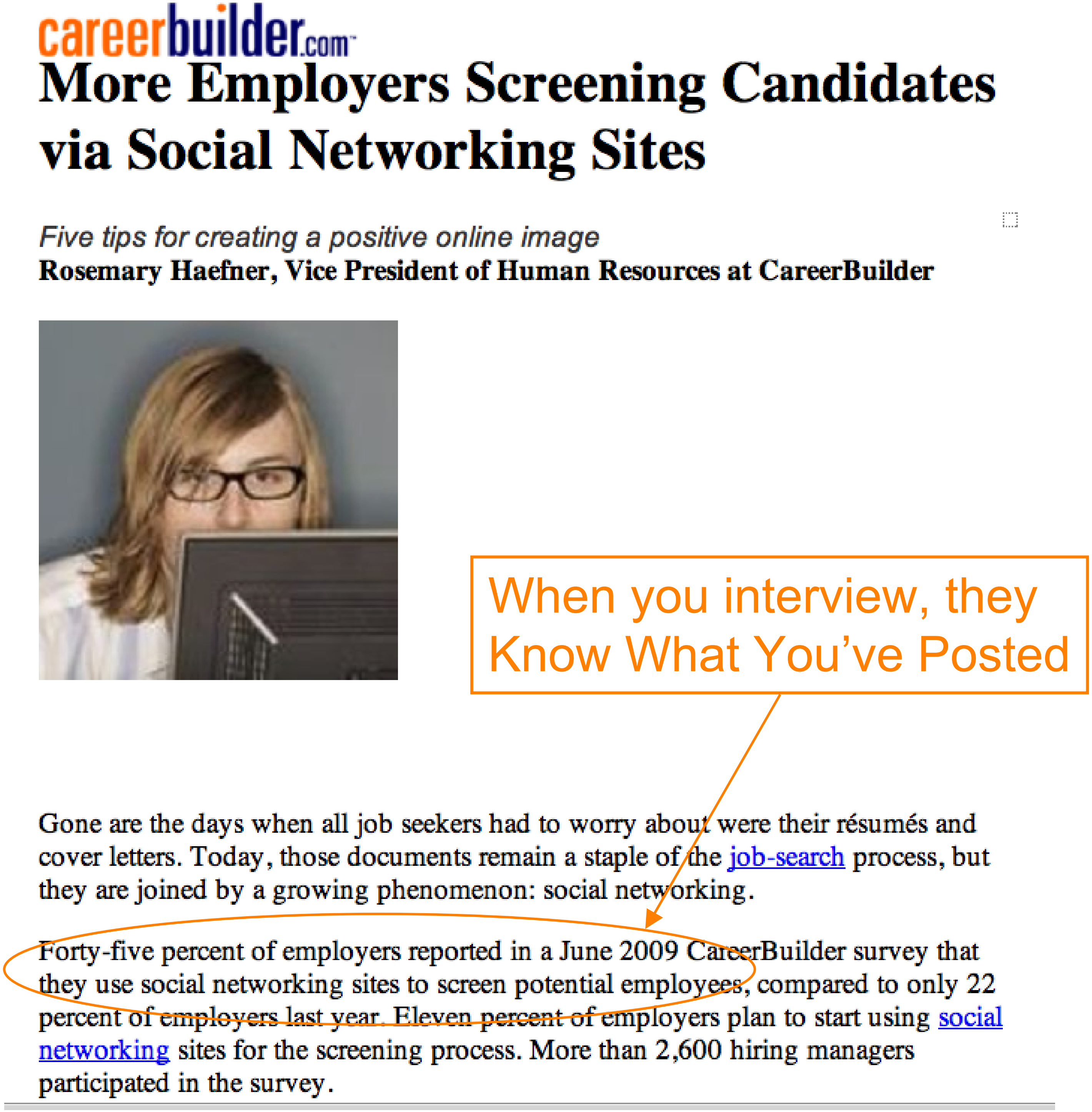
- Any web site can (anonymously) register with Google to instrument their site for *analytics*
  - Gather information about who visits, what they do when they visit
- To do so, site adds a small Javascript snippet that loads http://www.google-analytics.com/ga.js
  - You can see sites that do this because they introduce a "`__utma`" cookie
- Code ships off to Google information associated with your visit to the web site
  - Shipped by fetching a GIF w/ values encoded in URL
  - Web site can use it to analyze their ad “campaigns”
  - Not a small amount of info …

Values Reported via Google Analytics

Affiliation
Billing City
Billing Country
Billing Region
Browser Lang.
Complete URL
Cookie Values
Current Page
Event Tracking
Flash Version
Grand Total
Host Name
Java-enabled
Language Encoding
Order ID
Page Title
Product Code
Product Name
Profile Number
Repeat Campaign Visit
Quantity
Screen Color Depth
Screen Resolution
Shipping Cost
Special Event
Start Campaign Sess.
Tax
Tracking Code Version
Unique GIF ID
Unit Price
User Defined Var
Variations on an Item

Privacy - What’s the Big Deal?

- Cookies form the core of how Internet advertising works today
  - Without them, arguably you’d have to pay for content up front a lot more
    - (and payment would mean you’d lose anonymity anyway)
  - A “better ad experience” is not necessarily bad
    - Ads that reflect your interests; not seeing repeated ads
- But: ease of gathering so much data so easily ⇒ concern of losing control how it’s used
  - Mission creep …
    - Consider how ordering a pizza in the near future might work (http://www.aclu.org/ordering-pizza)
  - Content shared with friends doesn’t just stay with friends …



careerbuilder.com

More Employers Screening Candidates via Social Networking Sites

Five tips for creating a positive online image

Rosemary Haefner, Vice President of Human Resources at CareerBuilder

Gone are the days when all job seekers had to worry about were their résumés and cover letters. Today, those documents remain a staple of the job-search process, but they are joined by a growing phenomenon: social networking.

Forty-five percent of employers reported in a June 2009 CareerBuilder survey that they use social networking sites to screen potential employees, compared to only 22 percent of employers last year. Eleven percent of employers plan to start using social networking sites for the screening process. More than 2,600 hiring managers participated in the survey.

When you interview, they Know What You've Posted

Why employers disregard candidates after screening online

Thirty-five percent of employers reported they have found content on social networking sites that caused them not to hire the candidate, including:

- Candidate posted provocative or inappropriate photographs or information -- 53 percent
- Candidate posted content about them drinking or using drugs -- 44 percent
- Candidate bad-mouthed their previous employer, co-workers or clients -- 35 percent
- Candidate showed poor communication skills -- 29 percent
- Candidate made discriminatory comments -- 26 percent
- Candidate lied about qualifications -- 24 percent
- Candidate shared confidential information from previous employer -- 20 percent

How To Gain Better Privacy?

- Force of law
  - Example #1: web site privacy policies
    - US sites that violate them commit false advertising
    - But: policy might be “*Yep, we sell everything about you, Ha Ha!*”
  - Example #2: SB 1386
    - *Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)*
    - Quite effective at getting sites to pay attention to securing personal information

Gaining Privacy Through Technical Means

- How can we surf the web truly anonymously?
- Step #1: remove browser leaks
  - Delete cookies (oops - also "Flash cookies"!)
  - Turn off Javascript (so Google Analytics doesn't track you)
- Step #2: how do we hide our IP address?
- One approach: trusted third party
  - E.g. anonymizer.com
    - You set up an encrypted VPN to their site
    - All of your traffic goes via them
  - Issues?
    - Performance
    - ($80/year)
    - "*rubber hose cryptanalysis*" (cf. `anon.penet.fi` & Scientologists)

Anonymous Web Surfing, con't

- Idea: remove single point of trust failure by chaining together a series of servers
- Suppose Alice wants to send a message X anonymously with Bob
- And there are N servers, M_1 … M_N ("mixes"), available, each with a public key K_1 …. K_N
  - Each mix will accept a (message, next-hop) pair encrypted w/ its key and forward message to the mix (or end system) given by the next hop
- Approach: Alice bounces her message among the mixes to mask its origin ("onion routing")

Peeling the Onion

- Alice picks some mixes at random, say M_i, M_h & M_k
- She sends to M_i the following:
  $\{ \{ \{ X, B \}_{K_k}, M_k \}_{K_h}, M_h \}_{K_i}$
- M_i receives $\{ \{ \{ X, B \}_{K_k}, M_k \}_{K_h}, M_h \}_{K_i}$, decrypts
  – Message inside is $\{ \{ X, B \}_{K_k}, M_k \}_{K_h}$, next hop is M_h
- M_h receives $\{ \{ X, B \}_{K_k}, M_k \}_{K_h}$, decrypts
  – Message inside is $\{ X, B \}_{K_k}$, next hop is M_k
- M_k receives $\{ X, B \}_{K_k}$, decrypts
  – Message inside is X, next hop is B
- B receives X; has no idea who sent, nor does M_h/M_k
- Note: this is what the industrial-strength Tor anonymizing service uses
  – It also provides bidirectional communication

Onion Routing Issues/Attacks?

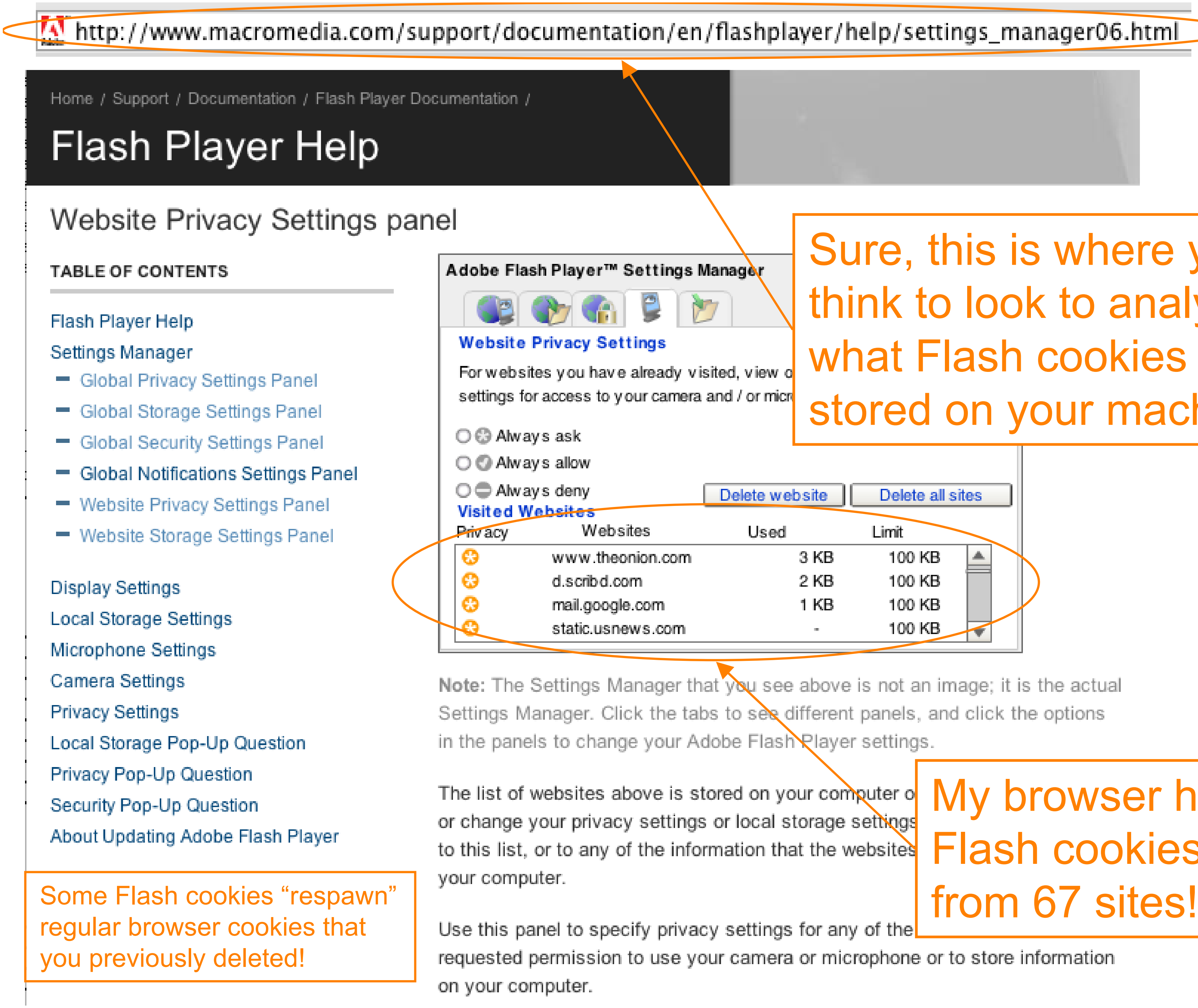
- Performance: message bounces around a lot
- Key management: the usual headaches
- Attack: rubber-hose cryptanalysis of mix operators
  - Defense: use mix servers in different countries
    - Though this makes performance worse :-(
- Attack: adversary operates M_i
  - Defense: have lots of mix servers (Tor today: ~2,000)
- Attack: adversary observes when Alice sends and when Bob receives, links the two together
  - A “confirmation” attack
  - Defenses: pad messages, introduce significant delays
    - Tor does the former, but notes that it’s not enough for defense

Onion Routing Attacks, con't

- Issue: **leakage**
- Suppose all of your HTTP/HTTPS traffic goes through Tor, but the rest of your traffic doesn't
  - Because you don't want it to suffer performance hit
- How might the operator of `sensitive.com` deanonymize your web session to their server?
- Answer: they inspect the logs of their DNS server to see who looked up `sensitive.com` just before your connection to their web server arrived
- **Hard**, general problem: anonymity often at risk when adversary can correlate separate sources of information

Dataset Privacy

- Difficult issues of anonymity arise when releasing database records
- Recent example: Netflix released a portion of their customer records in a contest to improve their recommendation system
  - Data included anonymized user ID, some of the movies user rated, how much the user liked them, and when user rated them
- How could (some) users be deanonymized?
- Attackers (researchers) cross-correlated with non-anonymous IMDB movie reviews
  - Looked for rarely-reviewed movies for which same movie was reviewed in Netflix & IMDB at about the same time
- General finding: in datasets with modest level of details, *individuals tend to be in some way unique*
- Related finding: birthdate + gender + zip code = **unique** for 60+% of US population! (*note, P&P quotes older 87% figure*)



http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html

Home / Support / Documentation / Flash Player Documentation /

Flash Player Help

Website Privacy Settings panel

TABLE OF CONTENTS

Adobe Flash Player™ Settings Manager

Website Privacy Settings

For websites you have already visited, view o
settings for access to your camera and / or micr

○ Always ask

○ Always allow

○ Always deny

Visited Websites

Privacy	Websites	Used	Limit
✻	www.theonion.com	3 KB	100 KB
✻	d.scribd.com	2 KB	100 KB
✻	mail.google.com	1 KB	100 KB
✻	static.usnews.com	-	100 KB

Note: The Settings Manager that you see above is not an image; it is the actual Settings Manager. Click the tabs to see different panels, and click the options in the panels to change your Adobe Flash Player settings.

The list of websites above is stored on your computer o
or change your privacy settings or local storage settings
to this list, or to any of the information that the websites
your computer.

Use this panel to specify privacy settings for any of the
requested permission to use your camera or microphone or to store information on your computer.

Sure, this is where you'd think to look to analyze what Flash cookies are stored on your machine

My browser had Flash cookies from 67 sites!

Some Flash cookies "respawn" regular browser cookies that you previously deleted!

THE NEW YORKER’s Privacy Policy (when you buy their archives)

7. *Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.*