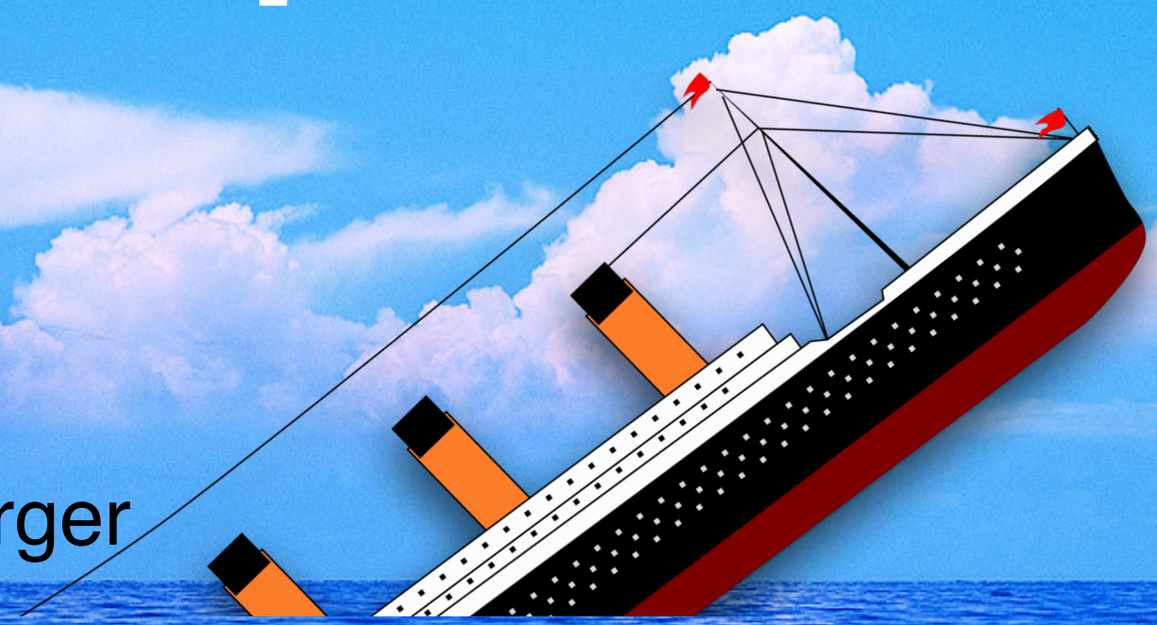
Righting Web Development



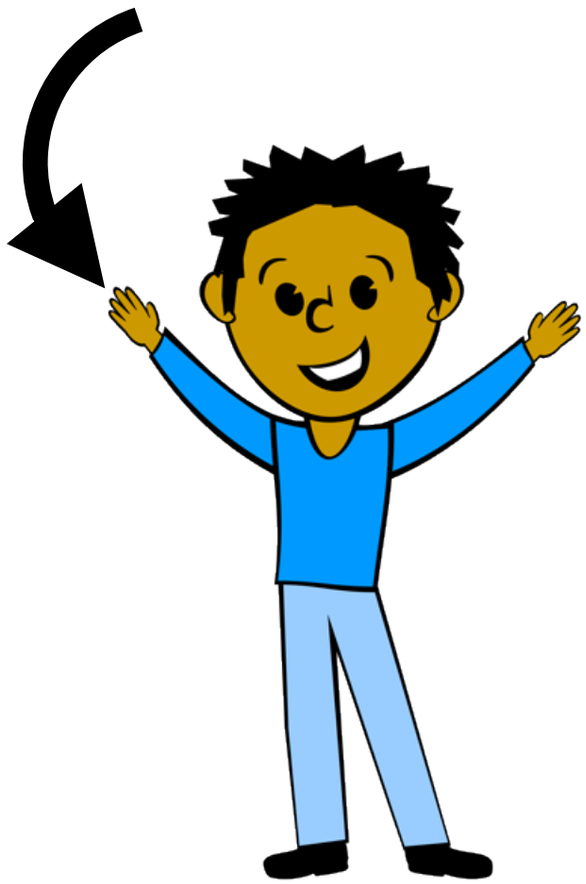
Advisor
Emery D. Berger

Dissertation Defense
John Vilk

August 2nd, 2018
2:00PM
Room 151, CS Building

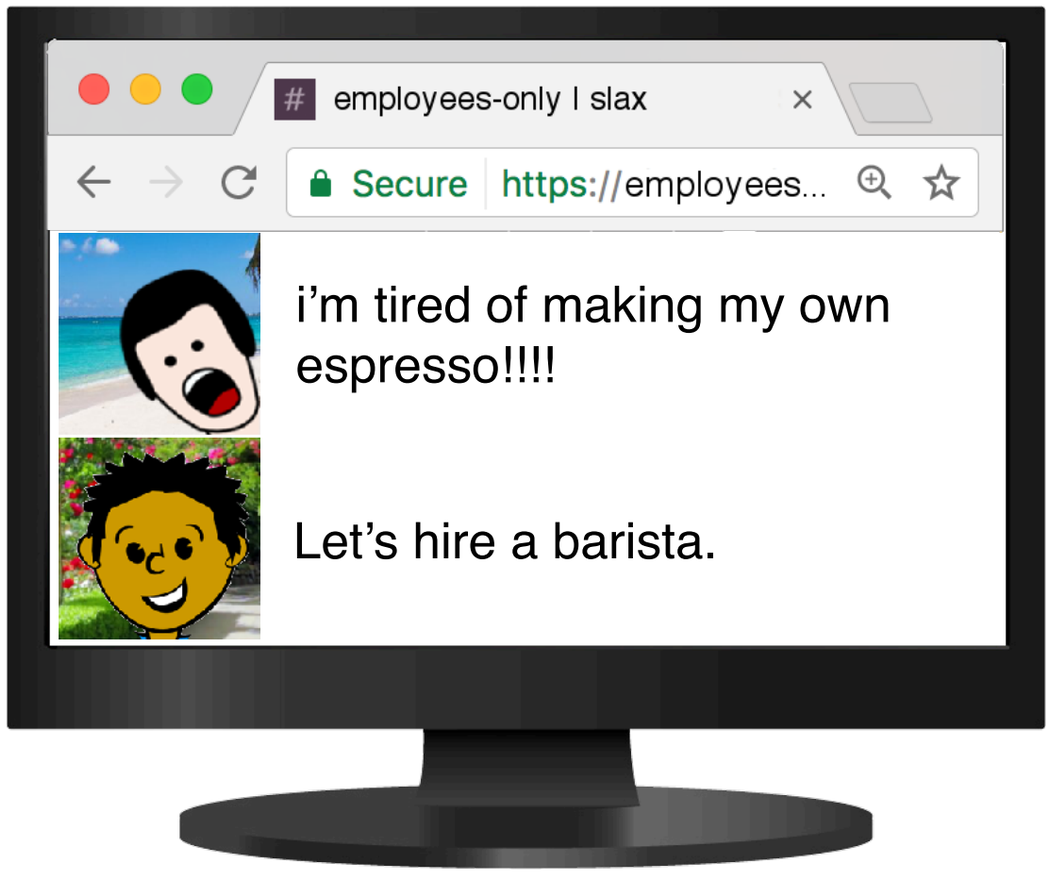
programming languages and systems at massachusetts
PLASMA
http://plasma.cs.umass.edu

Bret, lead developer

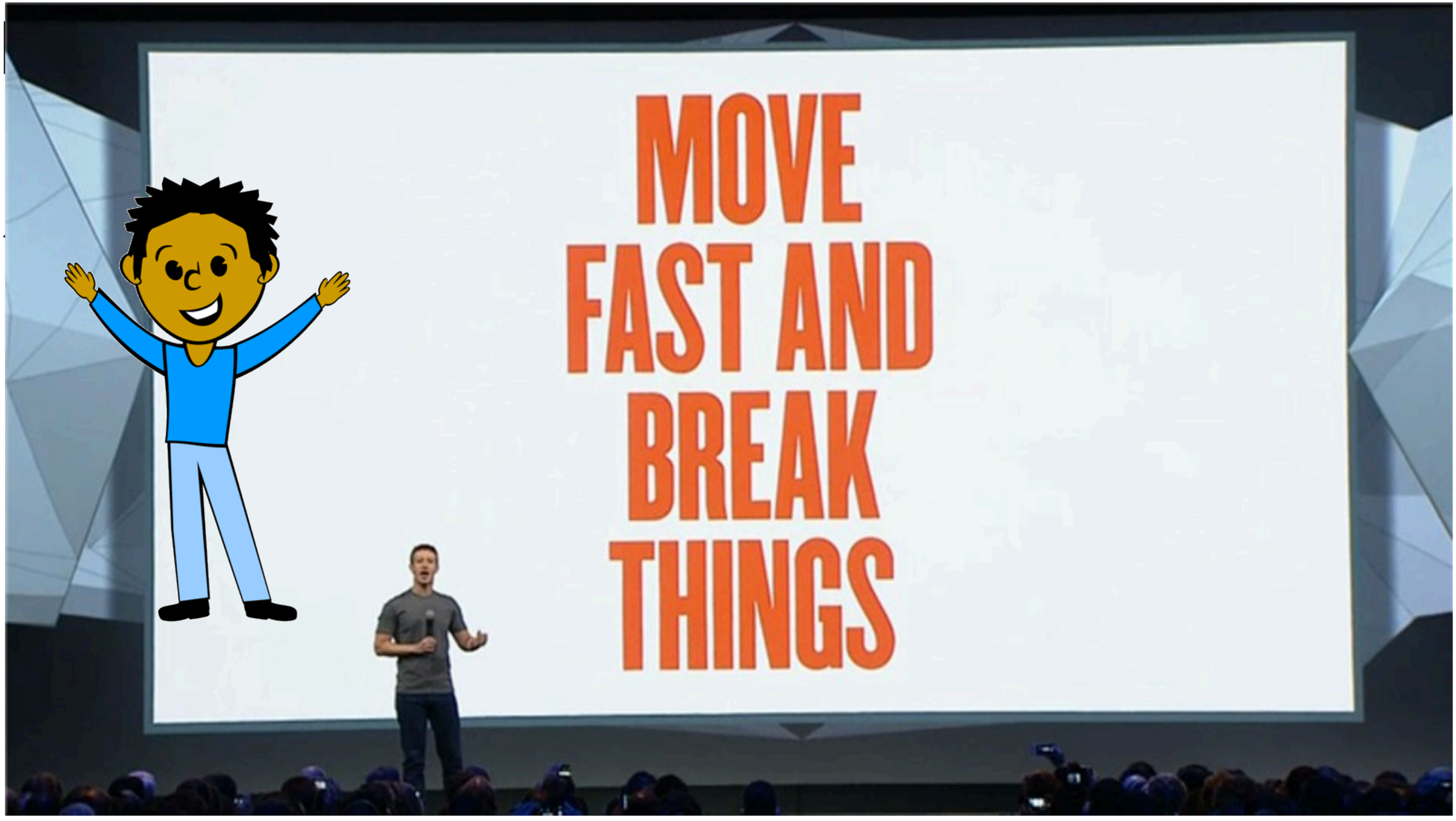


slax

Bret, lead developer

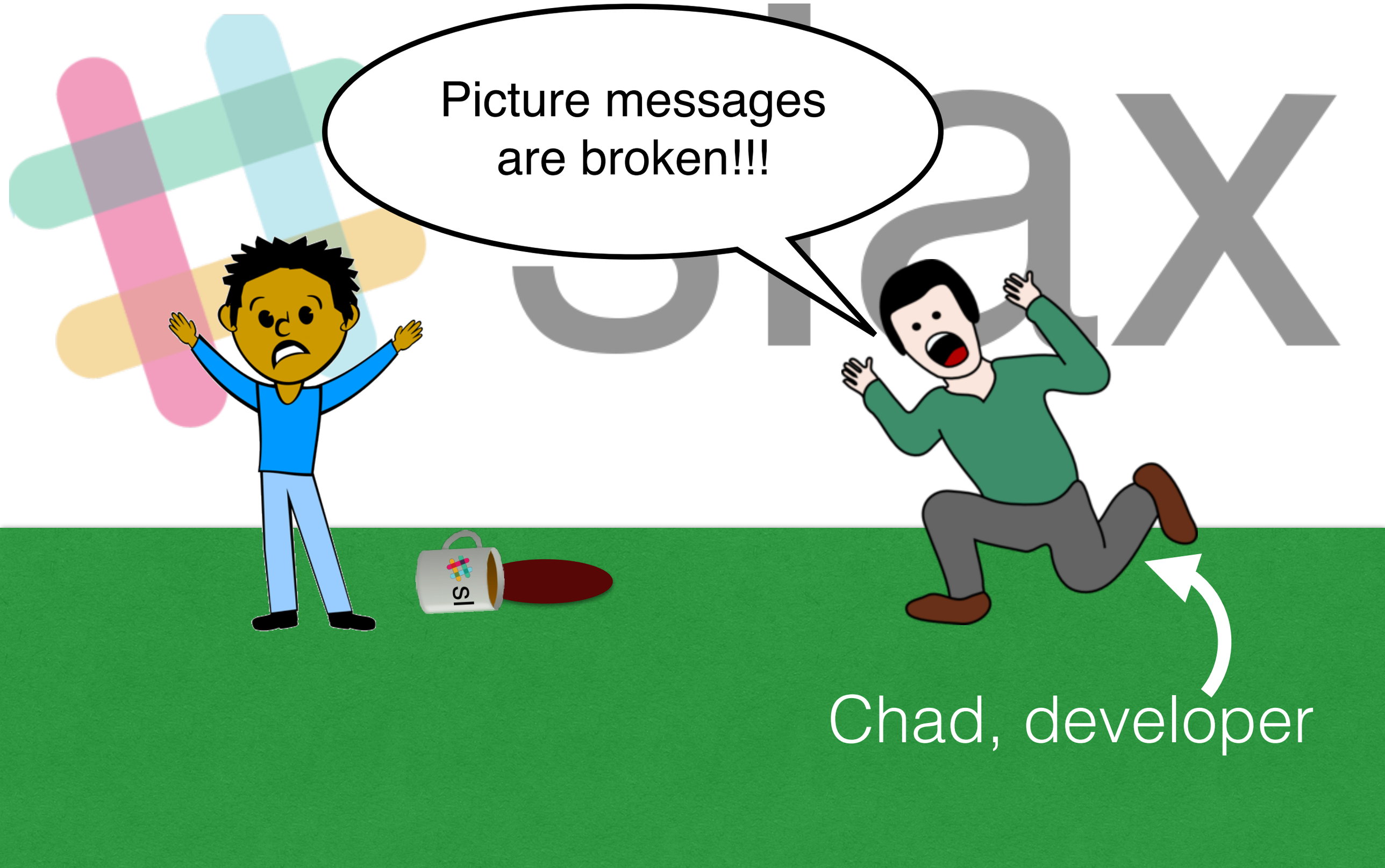


slax



slax

slax
sl


Picture messages are broken!!!
Chad, developer

Picture Message Bug

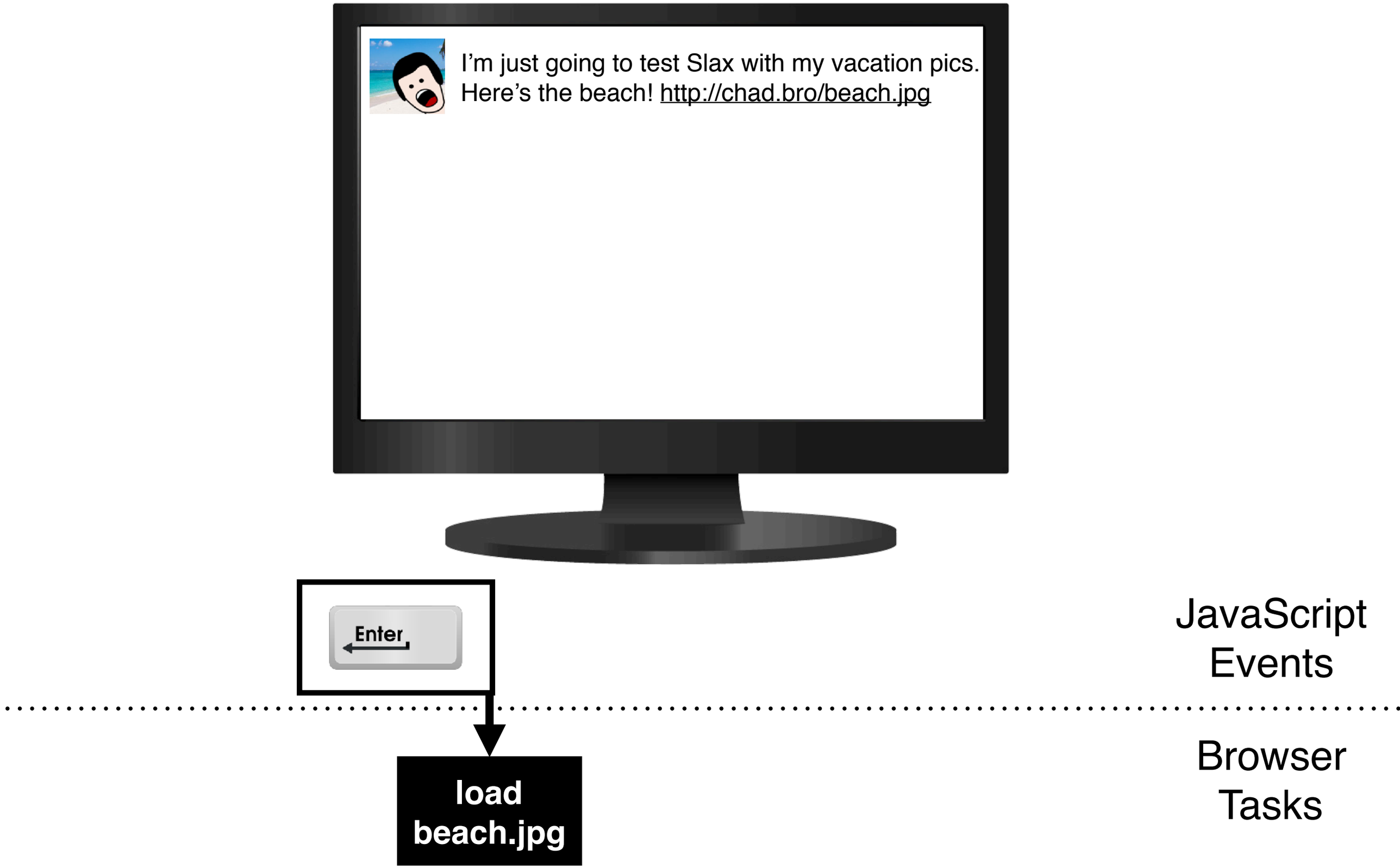
Picture Message Bug

Intended Behavior

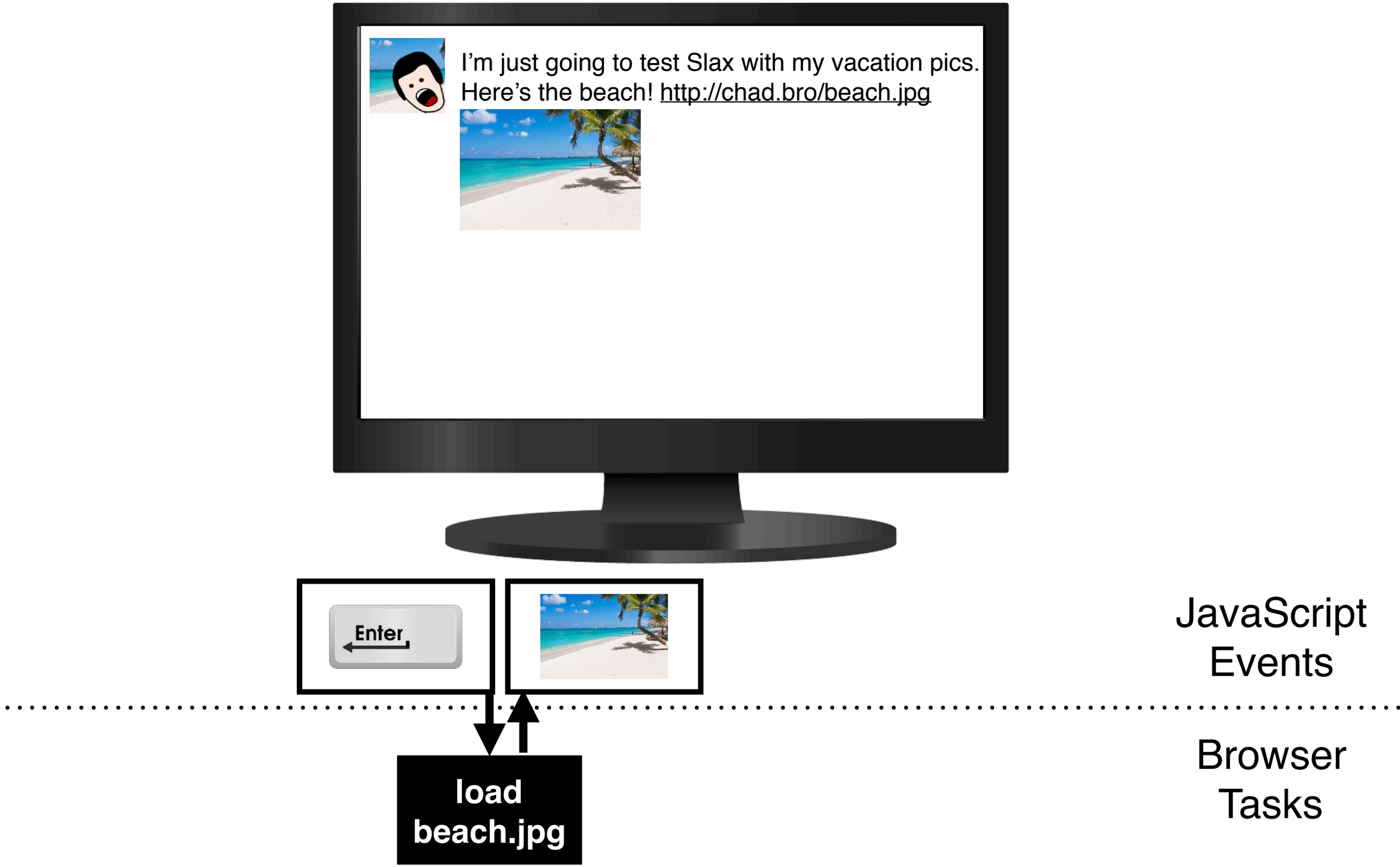
JavaScript
Events

Browser
Tasks

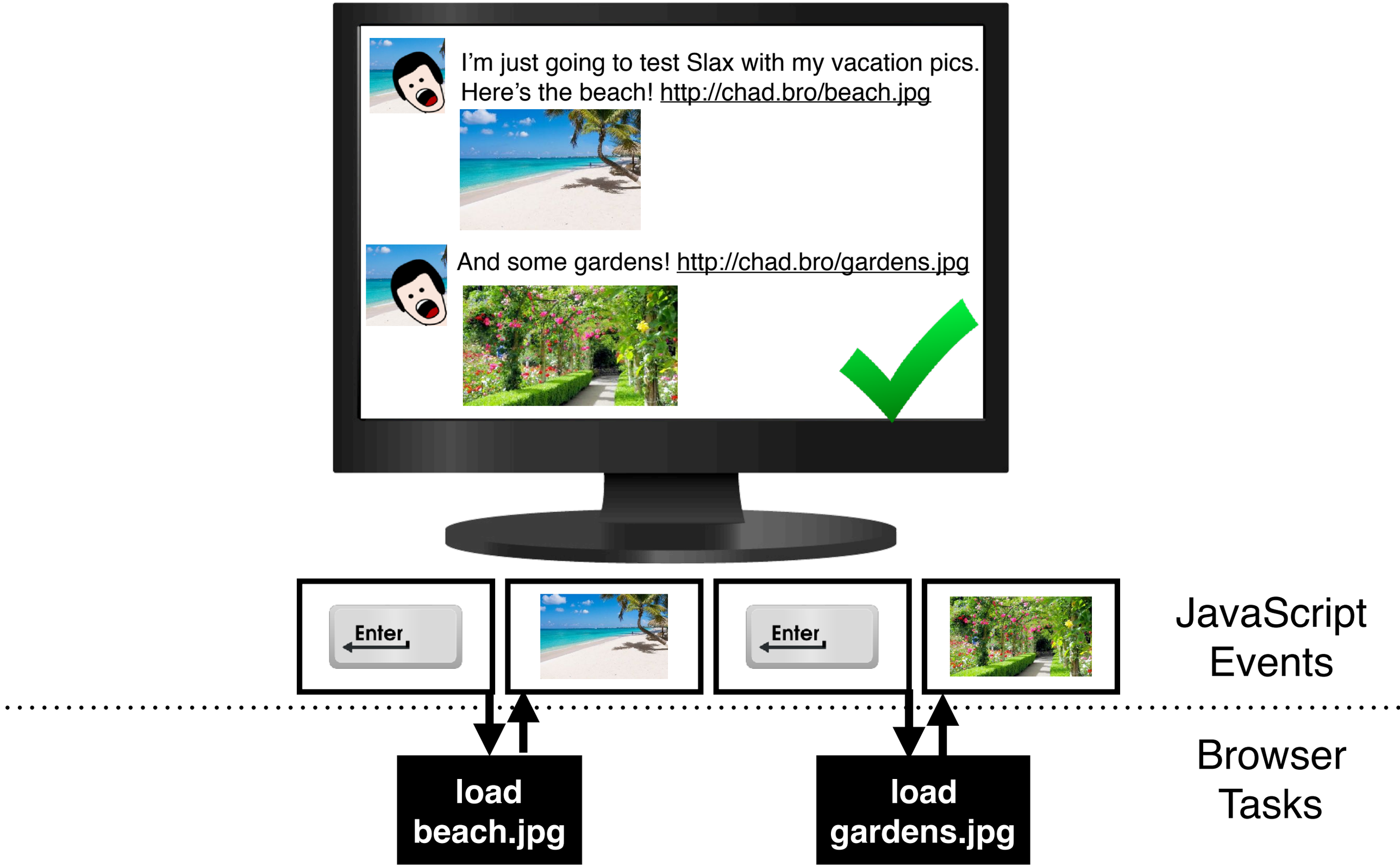
Intended Behavior



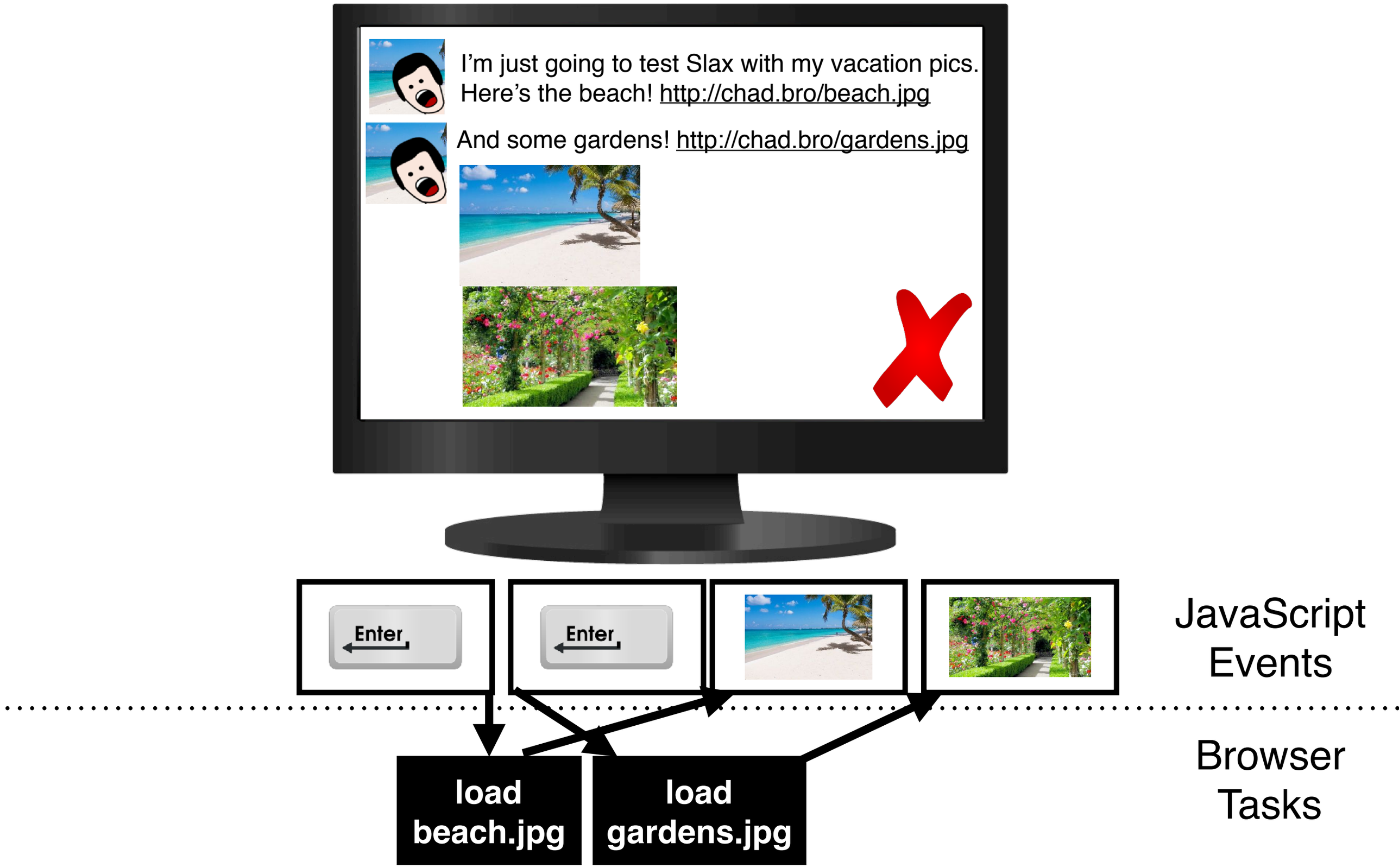
Intended Behavior



Intended Behavior



Intended Behavior



Intended Behavior

RACE CONDITION!

load beach.jpg

load gardens.jpg

Browser Tasks

Standard Stepping Debugger

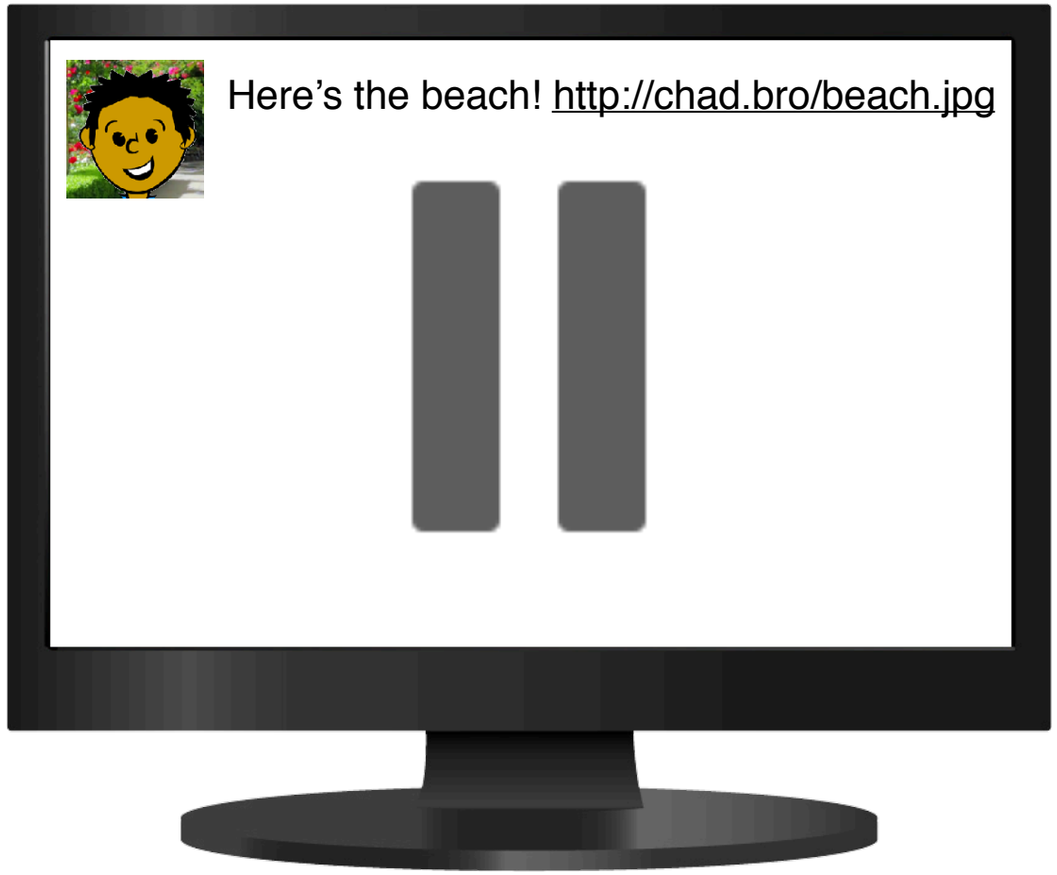
Browser

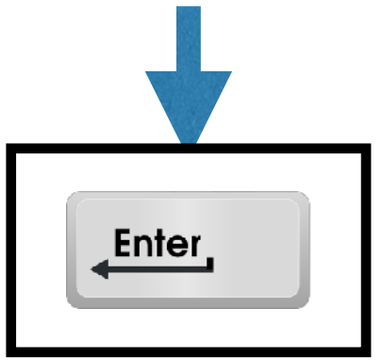
Standard Stepping Debugger

JavaScript

Browser

Standard Stepping Debugger

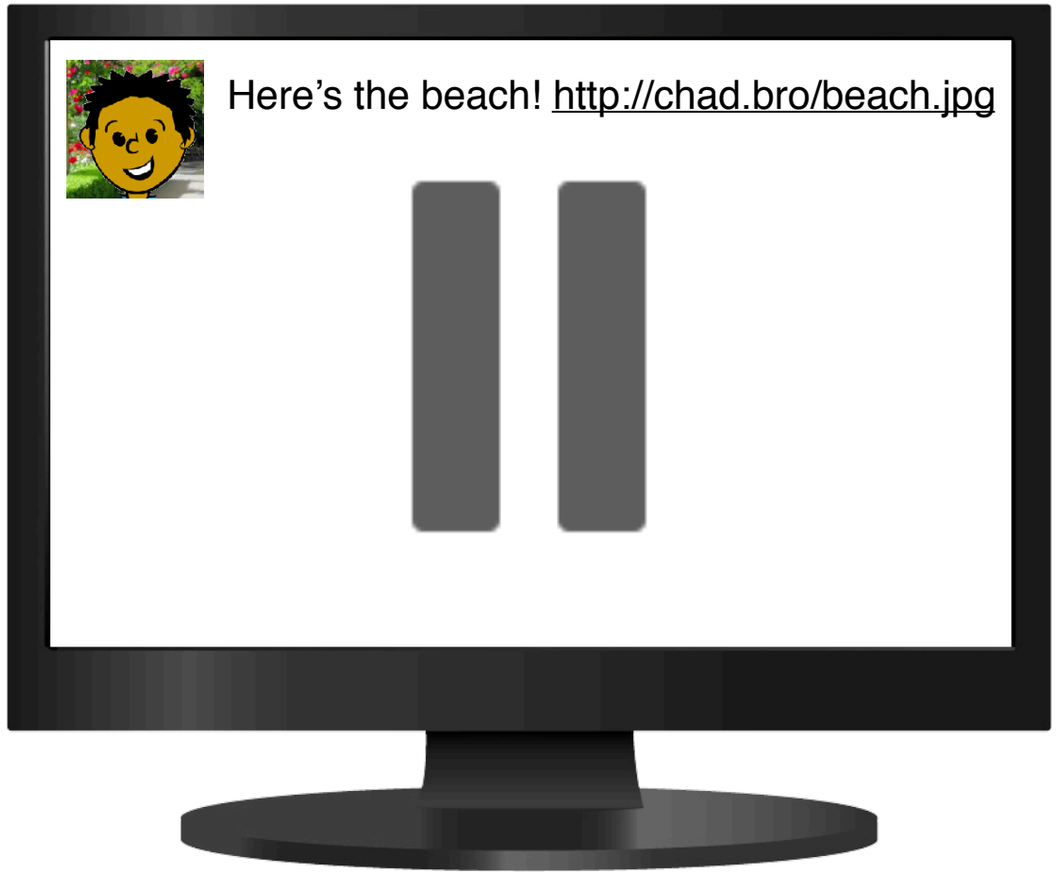


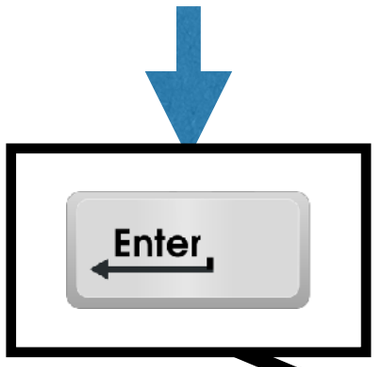


JavaScript

Browser

Standard Stepping Debugger





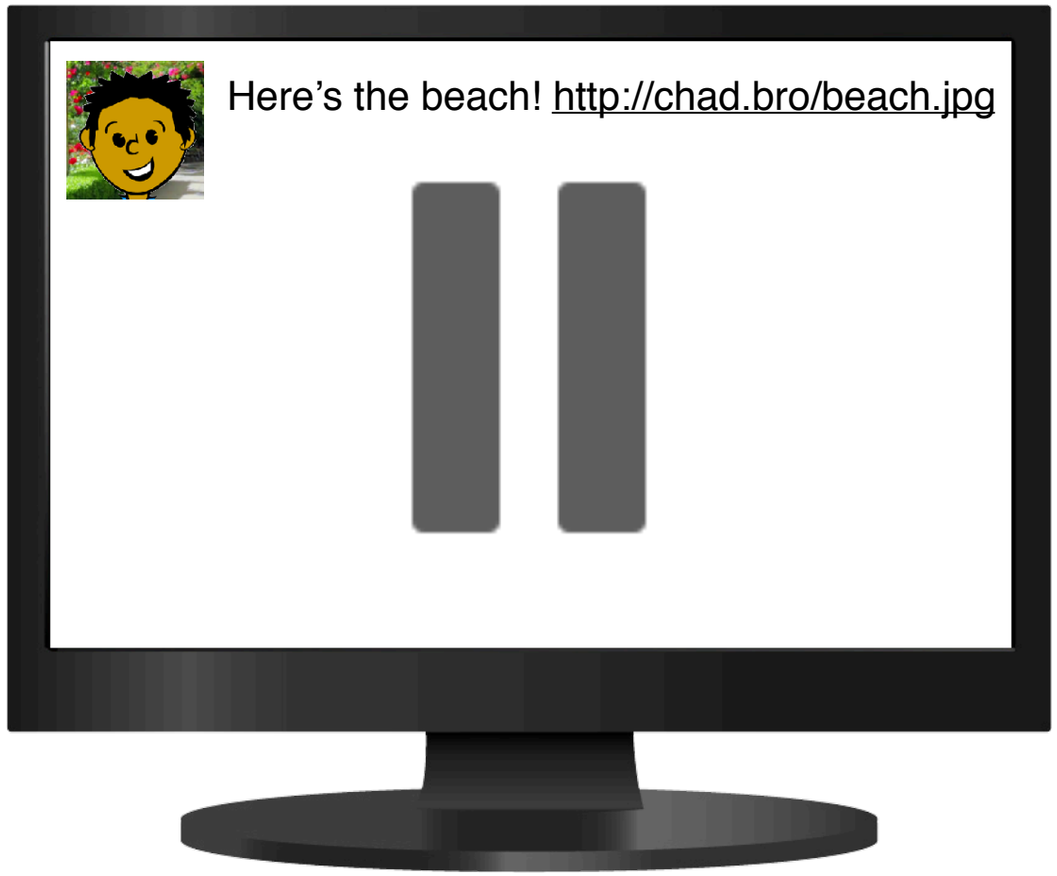
JavaScript

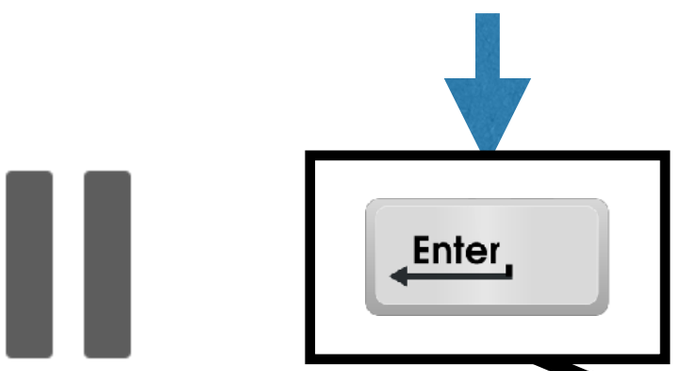
Active Tasks

download beach.jpg

Browser

Standard Stepping Debugger





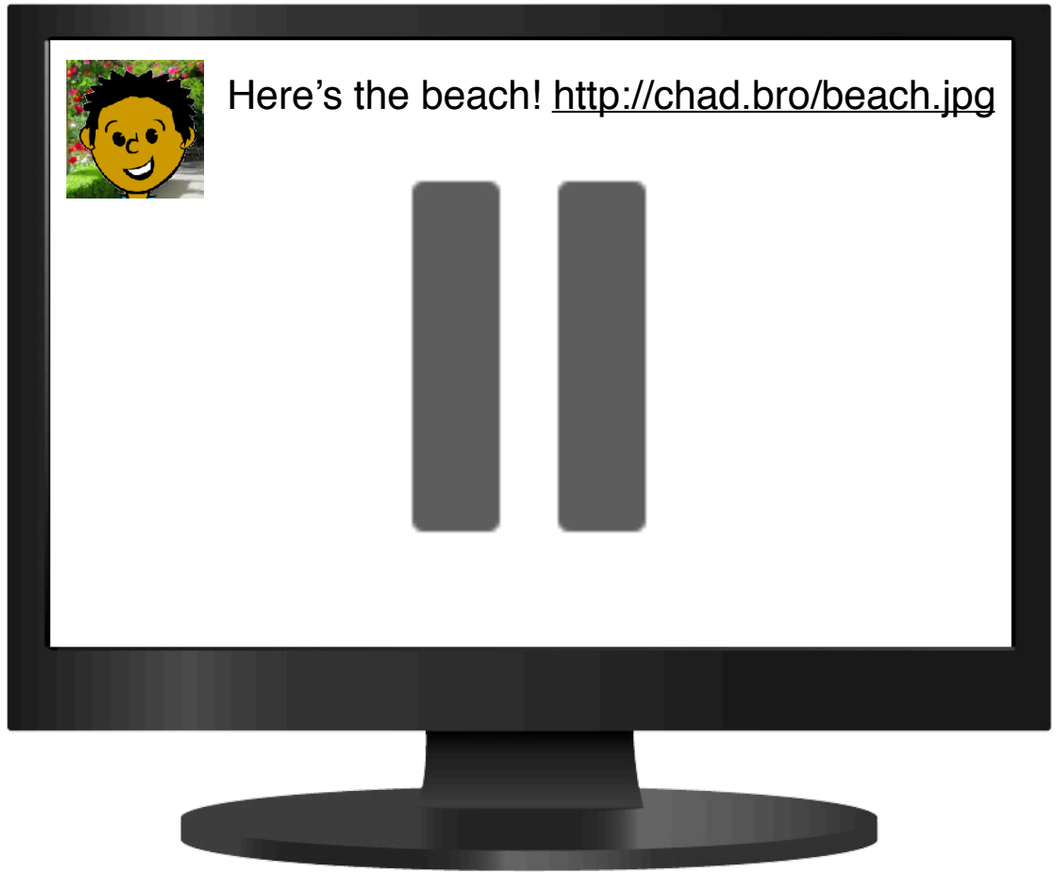
JavaScript

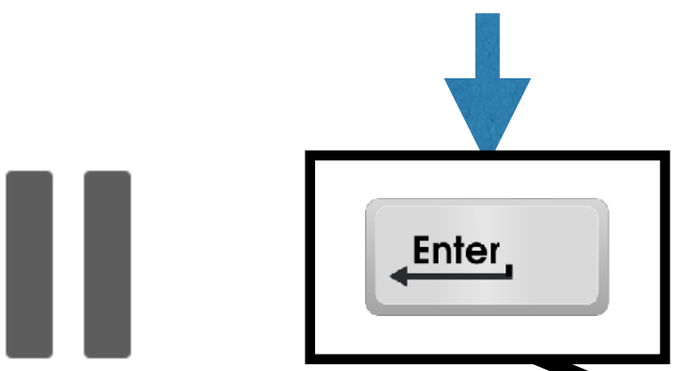
Active Tasks

download beach.jpg

Browser

Standard Stepping Debugger

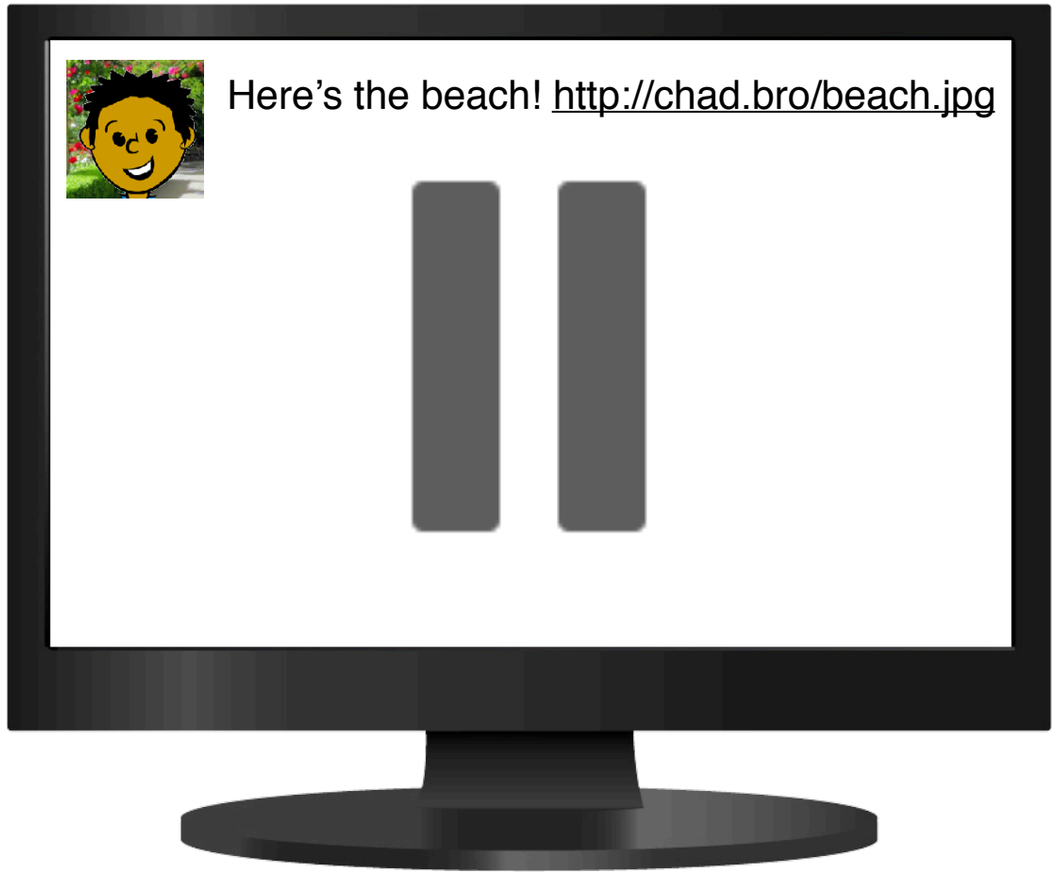


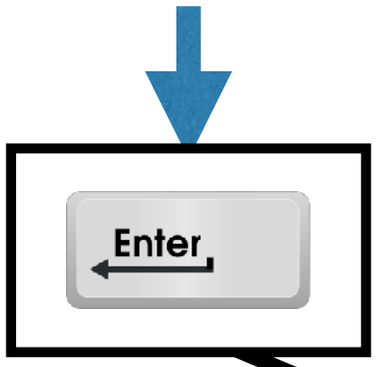


JavaScript

Browser

Standard Stepping Debugger





JavaScript

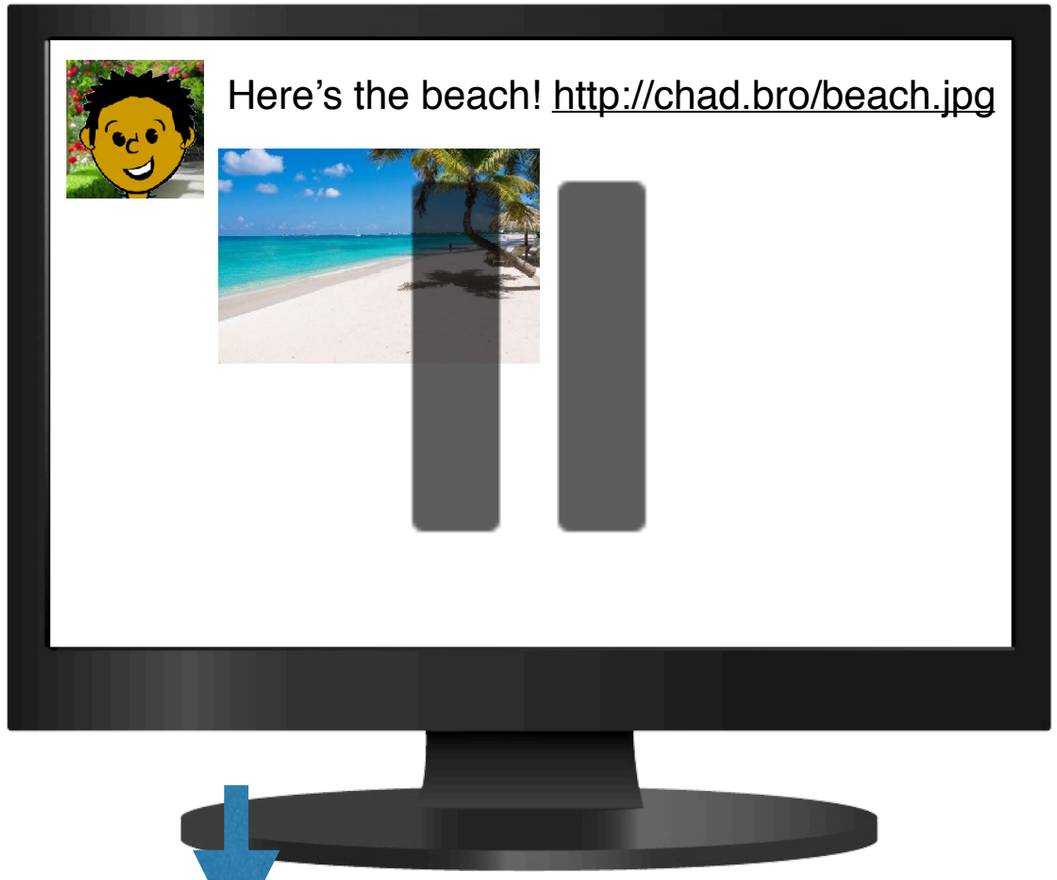
Active Tasks

download beach.jpg

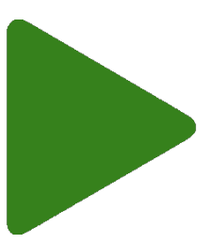
Event Queue

Browser

Standard Stepping Debugger



JavaScript



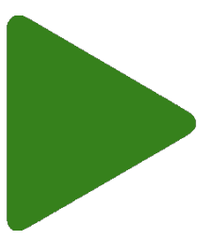
Active Tasks

Event Queue

Browser

Standard Stepping Debugger

JavaScript

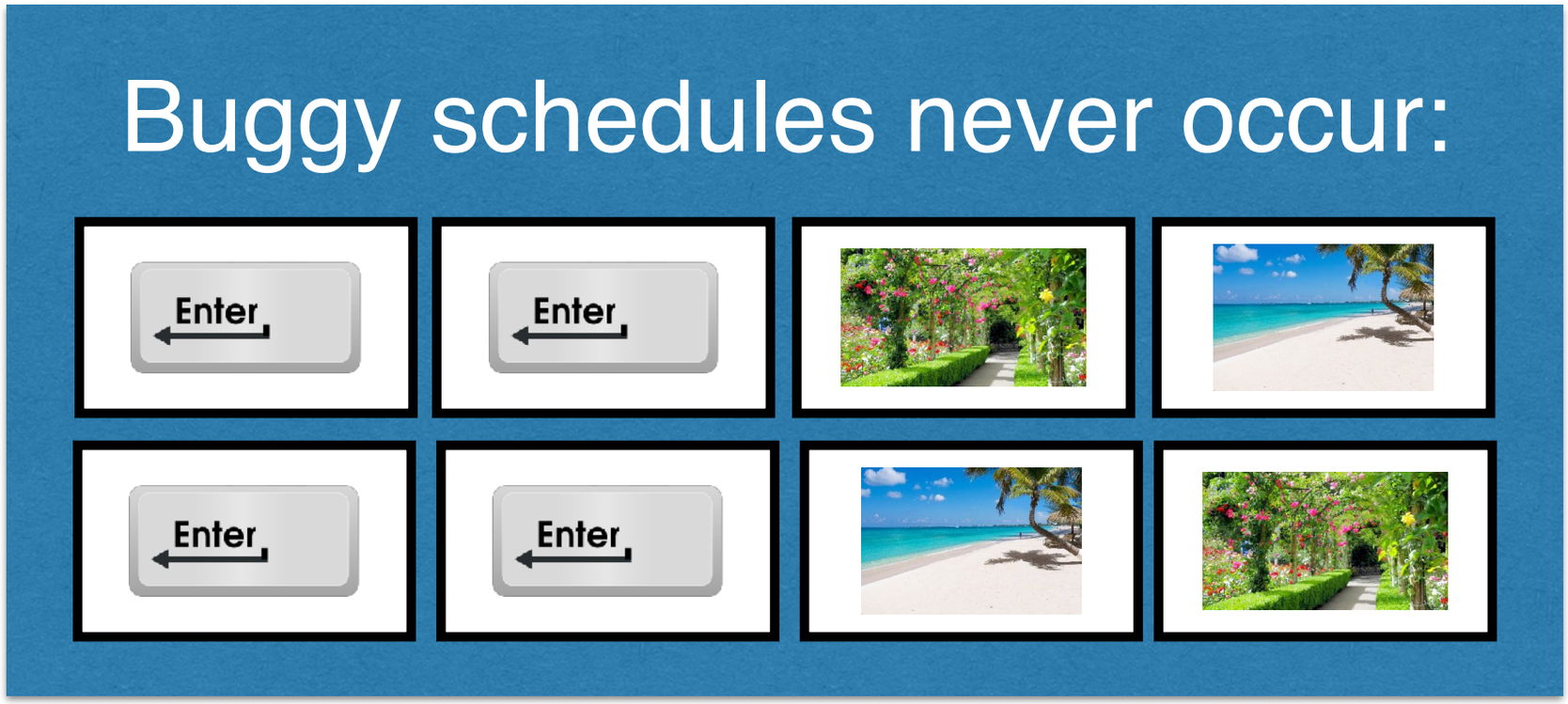


Active Tasks

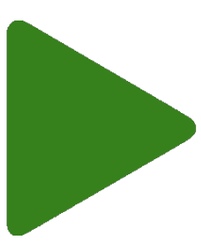
Event Queue

Browser

Standard Stepping Debugger



JavaScript

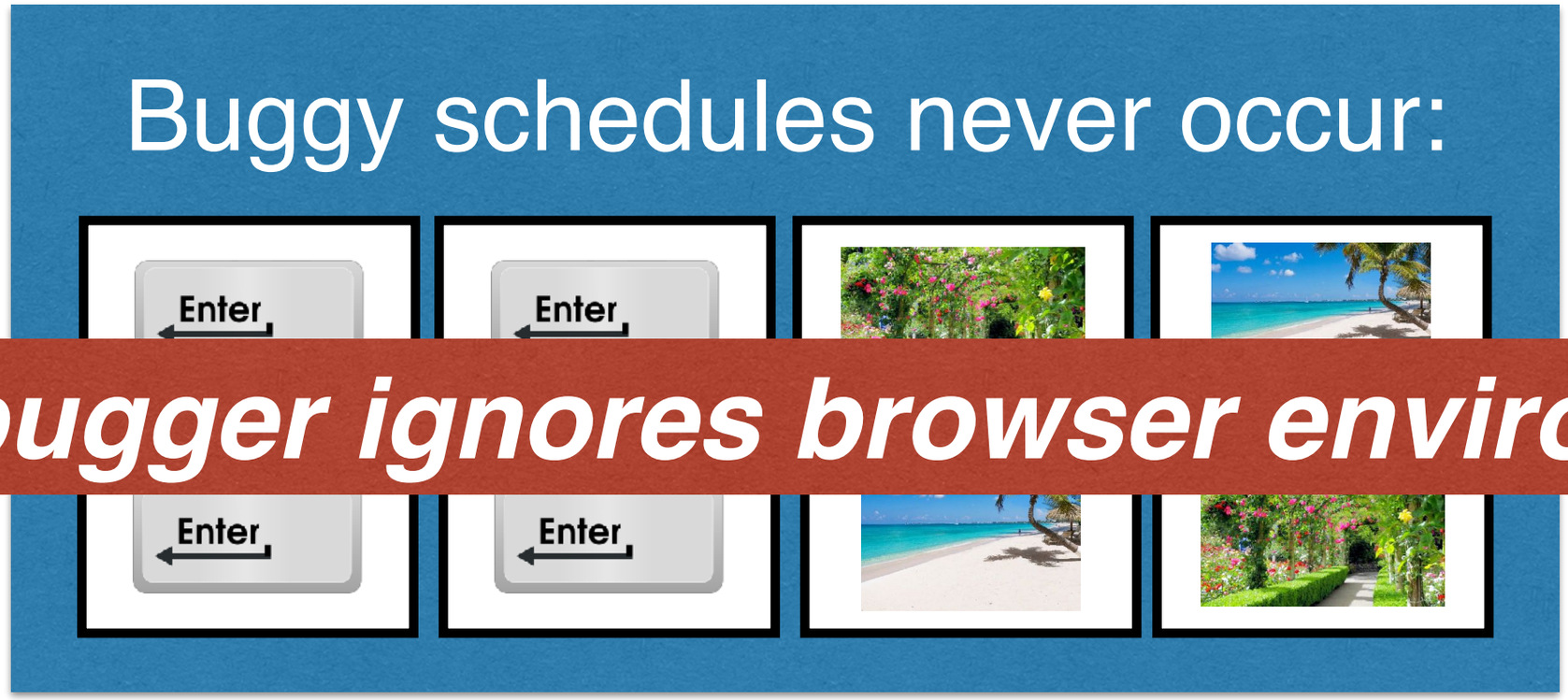


Active Tasks

Event Queue

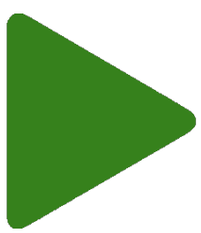
Browser

Standard Stepping Debugger



Debugger ignores browser environment!

JavaScript

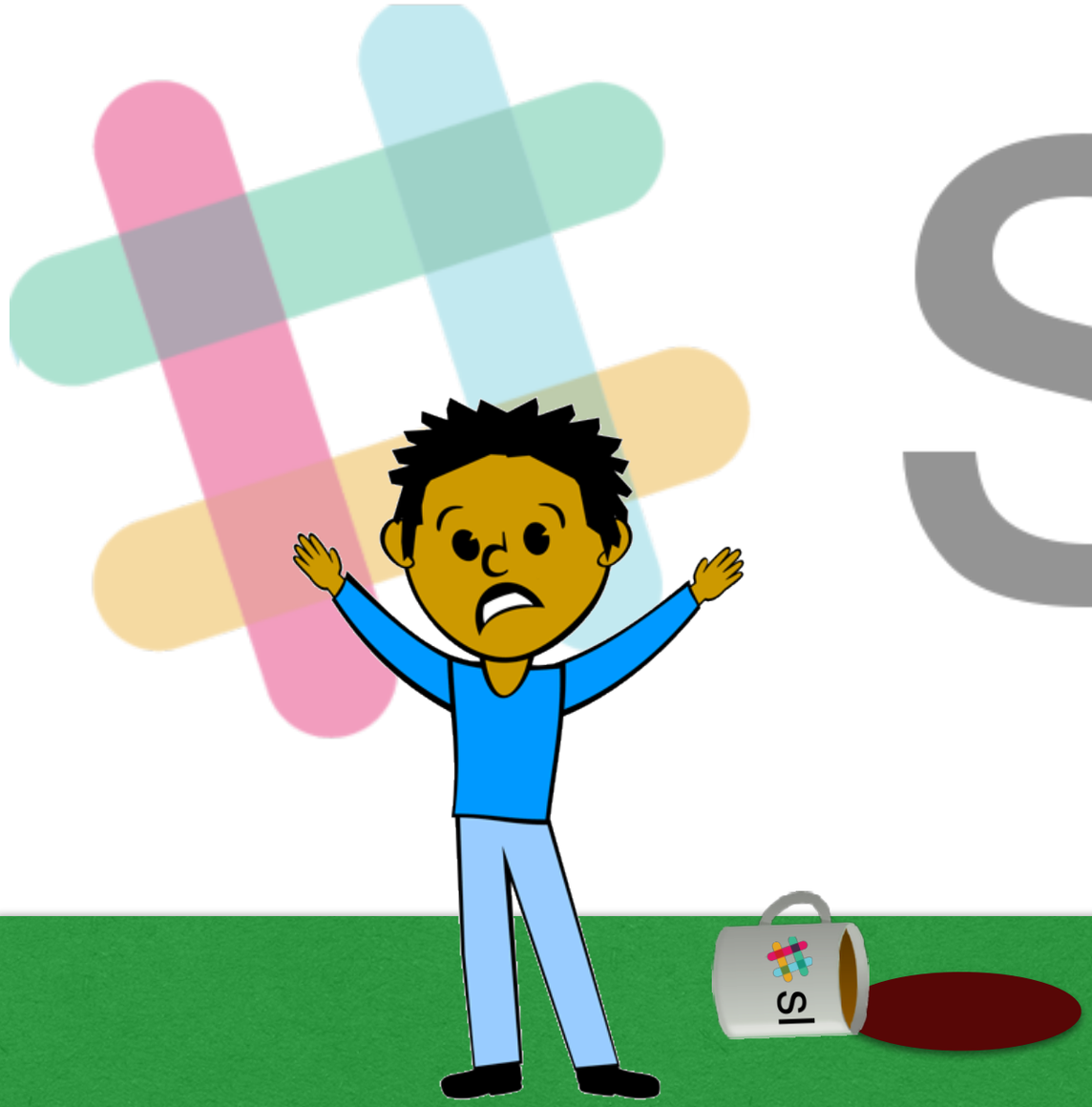


Active Tasks

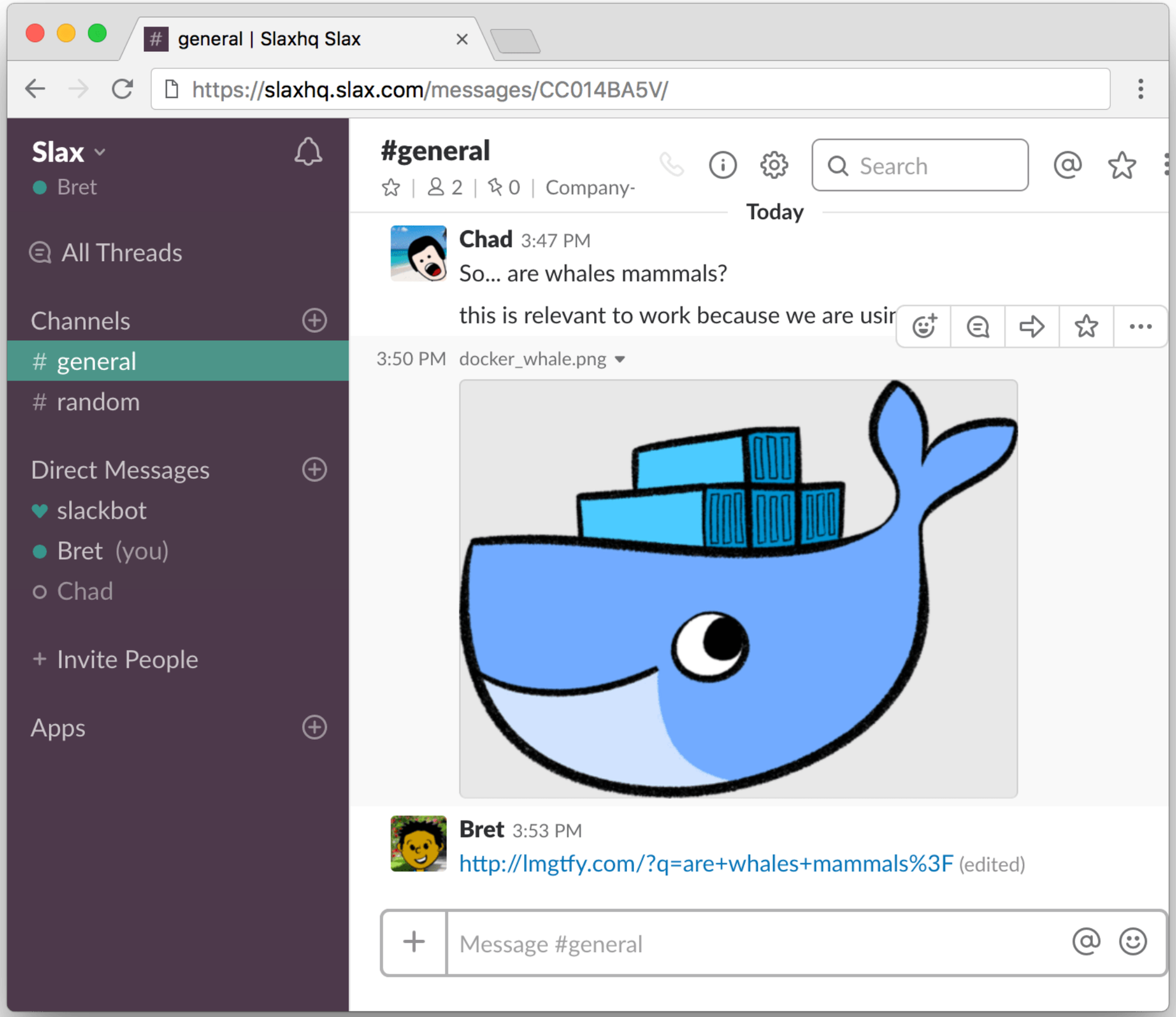
Event Queue

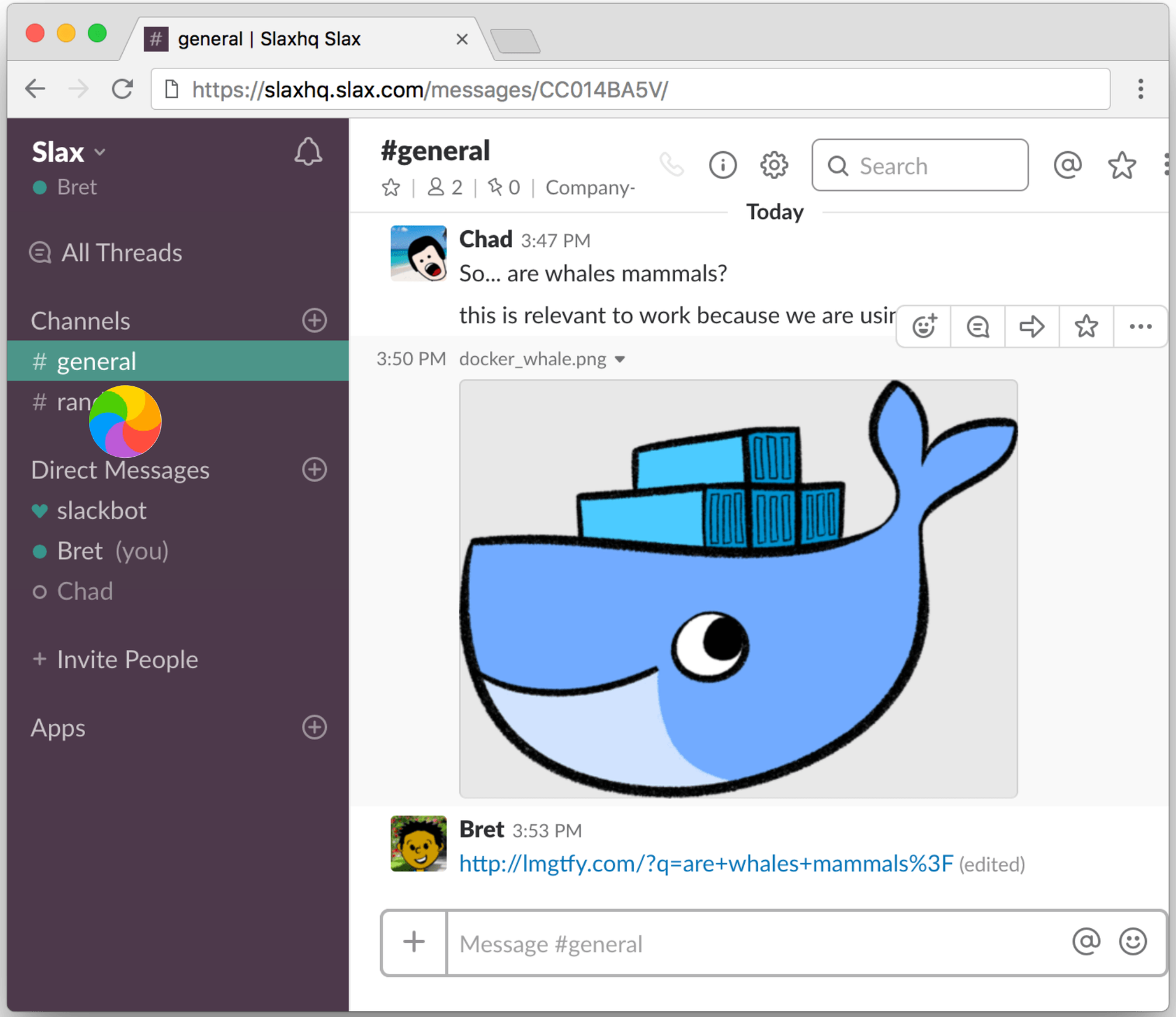
Browser

slax



Long sessions become slow!!!


general | Slaxhq Slax
https://slaxhq.slax.com/messages/CC014BA5V/
Slax
Bret
All Threads
Channels
general
random
Direct Messages
slackbot
Bret (you)
Chad
+ Invite People
Apps
#general
2 | 0 | Company-
Search
Today
Chad 3:47 PM
So... are whales mammals?
this is relevant to work because we are usin
3:50 PM docker_whale.png
Bret 3:53 PM
http://lmgtfy.com/?q=are+whales+mammals%3F (edited)
Message #general


general | Slaxhq Slax
https://slaxhq.slax.com/messages/CC014BA5V/
Slax
Bret
All Threads
Channels
general
Direct Messages
slackbot
Bret (you)
Chad
+ Invite People
Apps
#general
2 | 0 | Company-
Search
Today
Chad 3:47 PM
So... are whales mammals?
this is relevant to work because we are usin
3:50 PM docker_whale.png
Bret 3:53 PM
http://lmgtfy.com/?q=are+whales+mammals%3F (edited)
Message #general

random | Slaxhq Slax

https://slaxhq.slax.com/messages/CBYRHFY91/

Slax

Bret

All Threads

Channels

general

random

Direct Messages

slackbot

Bret (you)

Chad

+ Invite People

Apps

#random

2 | 0 | Non-work

Search

Today

Chad 3:49 PM

LOL

cat_download.jpeg

Message #random

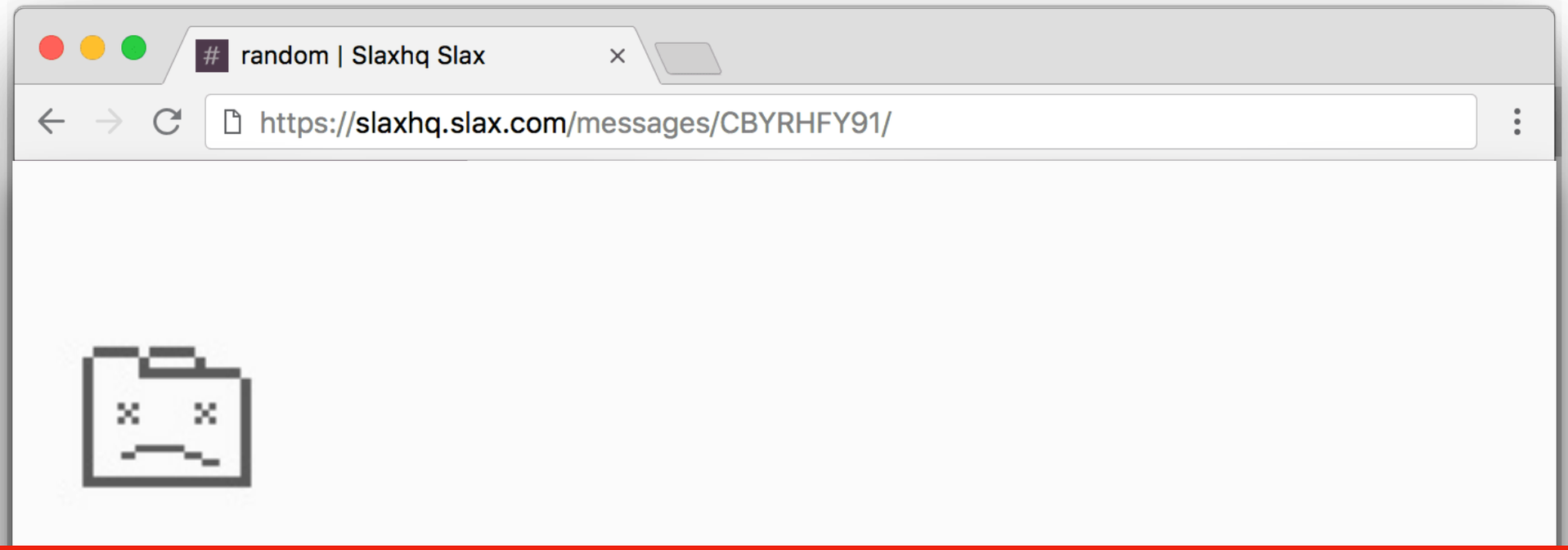
random | Slaxhq Slax

https://slaxhq.slax.com/messages/CBYRHFY91/

Aw, Snap!

Google Chrome ran out of memory while trying to display this webpage.

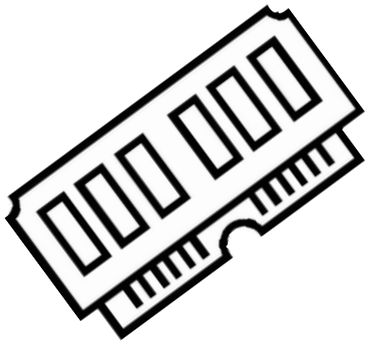
Learn more



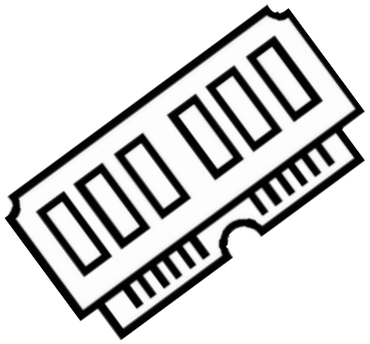
Slax has memory leaks!

Google Chrome ran out of memory while trying to display this webpage.

Learn more



Debugging a Memory Leak in a Web App

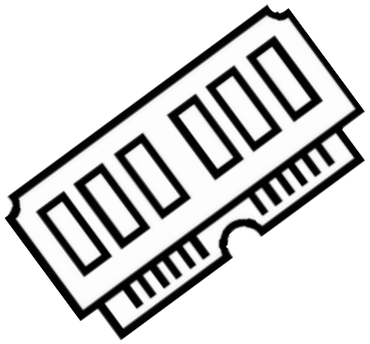


Debugging a Memory Leak in a Web App

Heap Snapshot from airbnb.com

Summary ▼ Class filter Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %



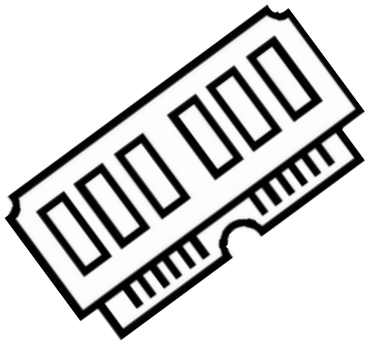
Debugging a Memory Leak in a Web App

Heap Snapshot from airbnb.com

Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %

Internal Chrome objects!



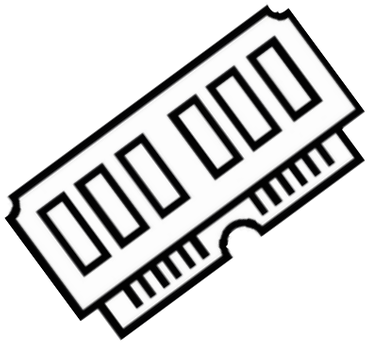
Debugging a Memory Leak in a Web App

Heap Snapshot from airbnb.com

Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %

Every array & "anonymous" object



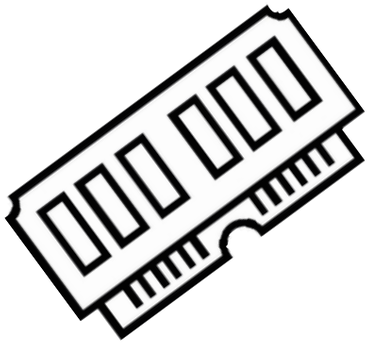
Debugging a Memory Leak in a Web App

Heap Snapshot from airbnb.com

Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %
▶ Xn	5	5 668	1 %	1 042 912	2 %	1 727 696	3 %

Obfuscated (minified) constructor names



Debugging a Memory Leak in a Web App

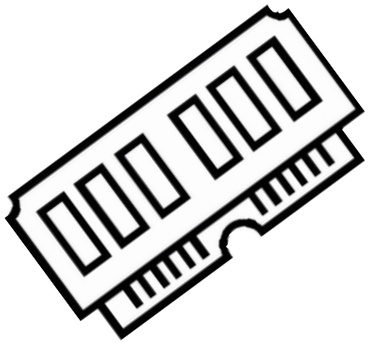
Heap Snapshot from airbnb.com

Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %
▶ Xn	5	5 668	1 %	1 042 912	2 %	1 727 696	3 %

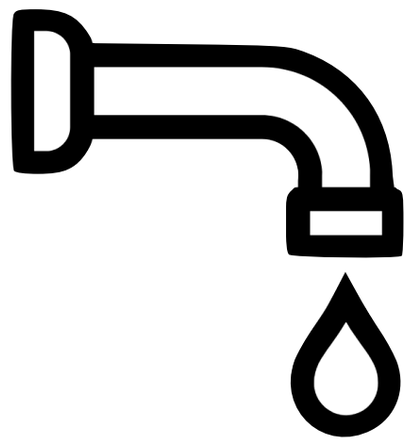
Obfuscated (minified) constructor names

??



Debugging a Memory Leak in a Web App

Challenging even for seasoned developers!



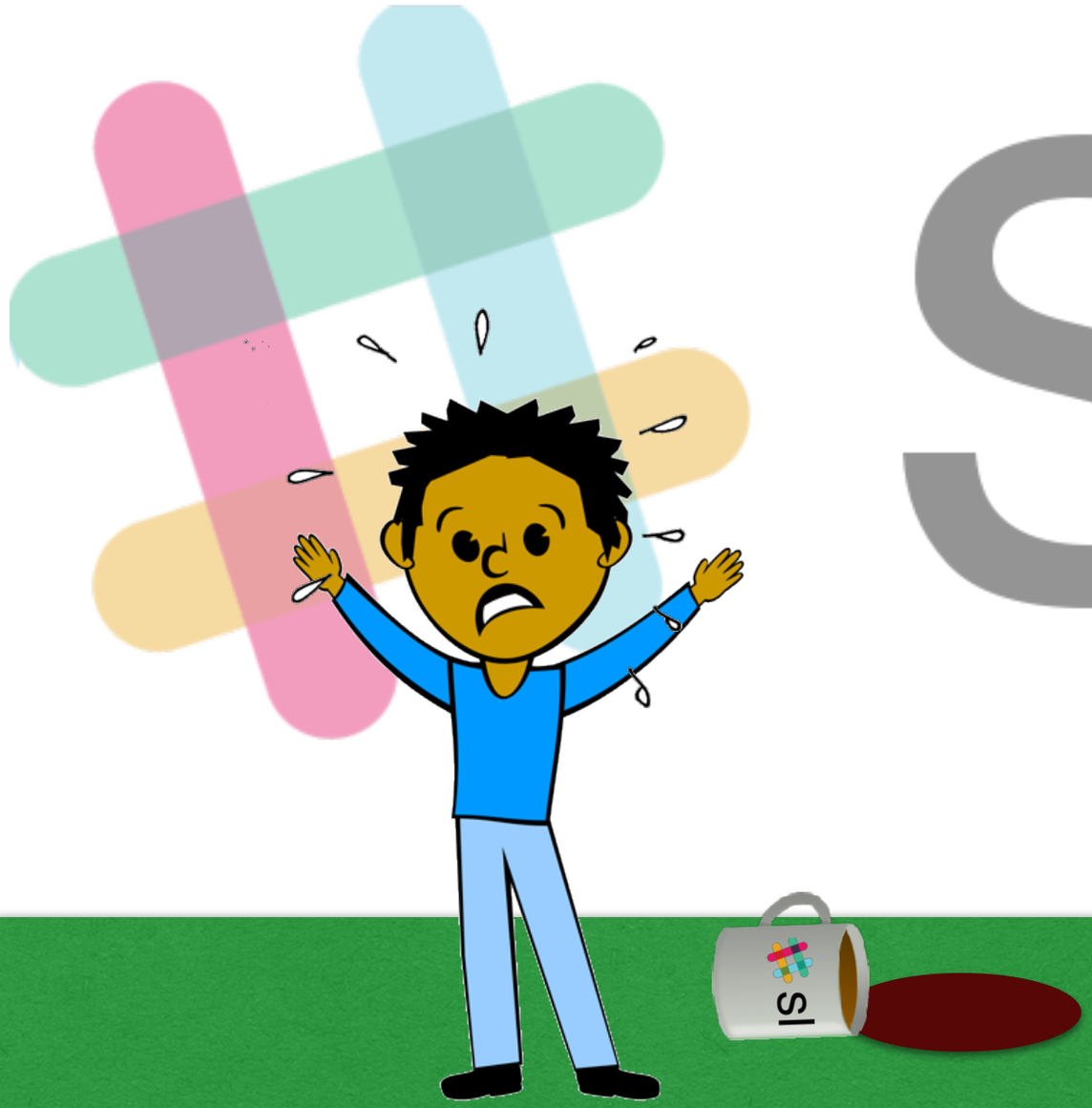
??

Status
Won't Fix (Infeasible)

101 people have starred this issue.

I'm labeling this as won't fix, because this is technically difficult. We're not really sure in how many places we're leaking :-(

~ Google Maps Developer



slax

Slax is a bandwidth hog!
sl

Chrome Developer Tools

Networking Tab

Name	Type	Initiator	Size
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Chrome Developer Tools

Networking Tab

Name	Type	Initiator	Size
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Chrome Developer Tools

Networking Tab

Chrome Developer Tools

Networking Tab

Name	Type	Initiator	Size
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Chrome Developer Tools

Networking Tab

Asynchronous way to eval JavaScript

Name			
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Chrome Developer Tools

Networking Tab

Asynchronous way to eval JavaScript

Name			
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

???.js
or ???.html

insert
<script src="data:text/javascript…">

Chrome Developer Tools

Networking Tab

Asynchronous way to eval JavaScript

Name			
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

???.js
or ???.html

insert
<script src="data:text/javascript…">

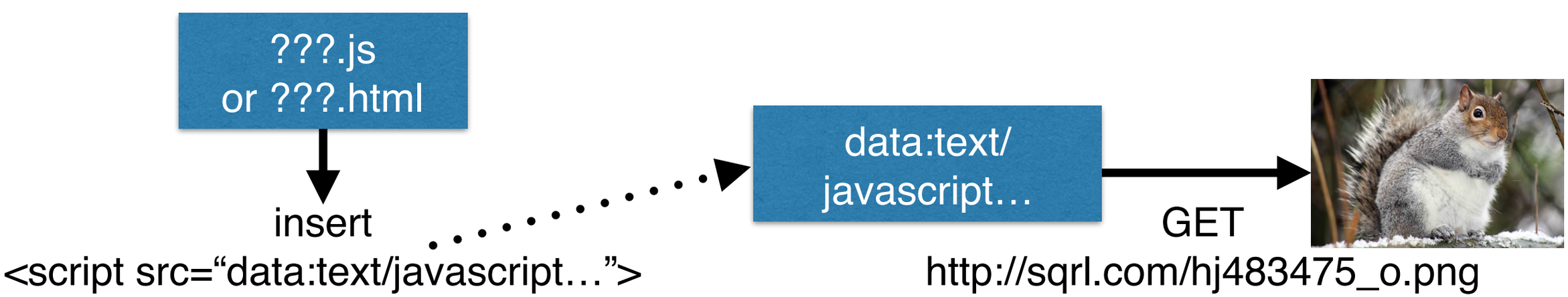
data:text/
javascript…

Chrome Developer Tools

Networking Tab

Asynchronous way to eval JavaScript

Name			
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

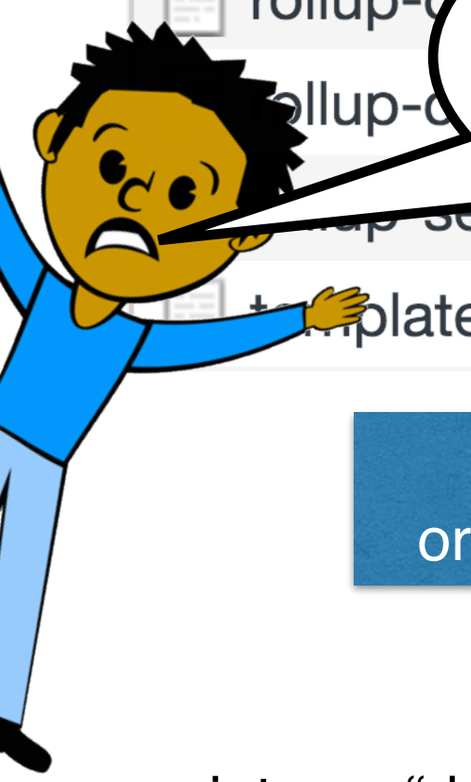


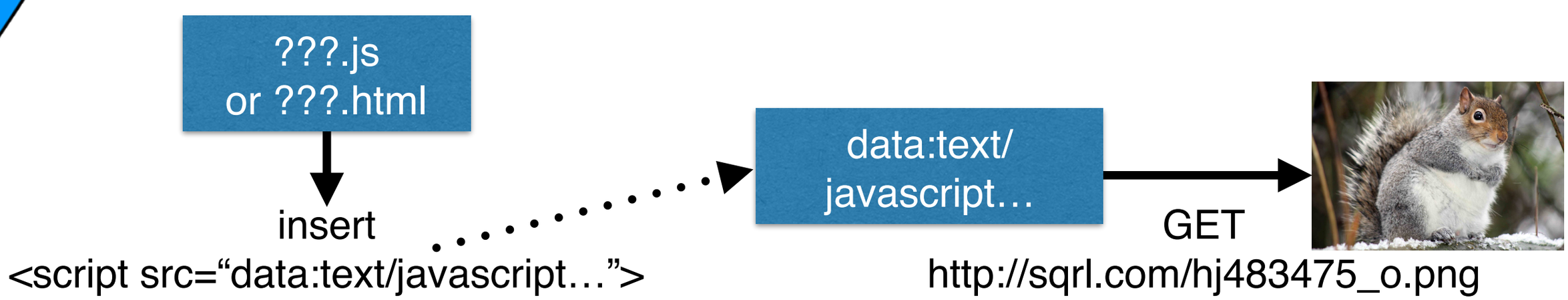
Chrome Developer Tools

Networking Tab

Asynchronous way to eval JavaScript

Name			
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.41		C02FBQJPC	1.1 MB
rollup-c		QJPC	640 KB
llup-c		QJPC	348 KB
llup-secon		02FBQJPC	336 KB
plates.php?cb=91eb_…	script	C02FBQJPC	202 KB

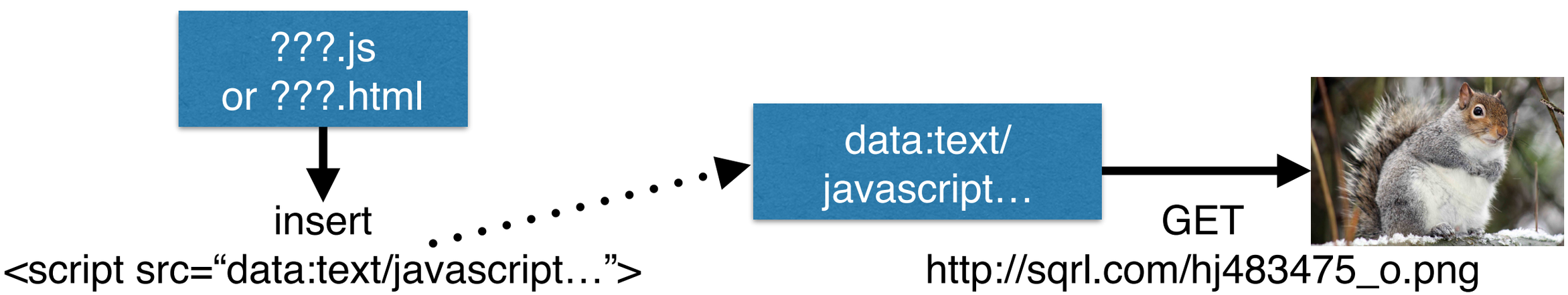




Chrome Developer Tools

Async Call Stacks

Normal call stack:



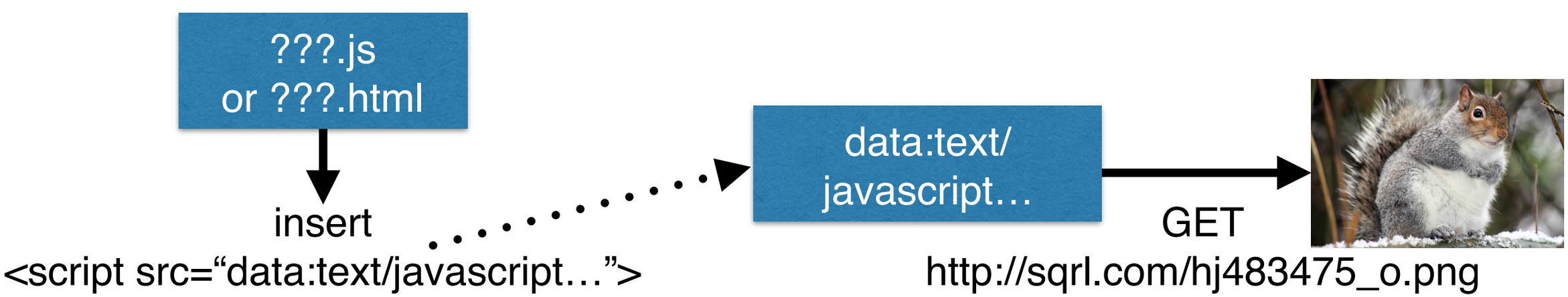
Chrome Developer Tools

Async Call Stacks

Normal call stack:

Async call stack:

Call Stack	
(anonymous function)	anon.html:13
setTimeout (async)	
(anonymous function)	anon.html:12
m.event.dispatch	jquery-1.11.3.min.js:4
m.event.add.r.handle	jquery-1.11.3.min.js:4



Chrome Developer Tools

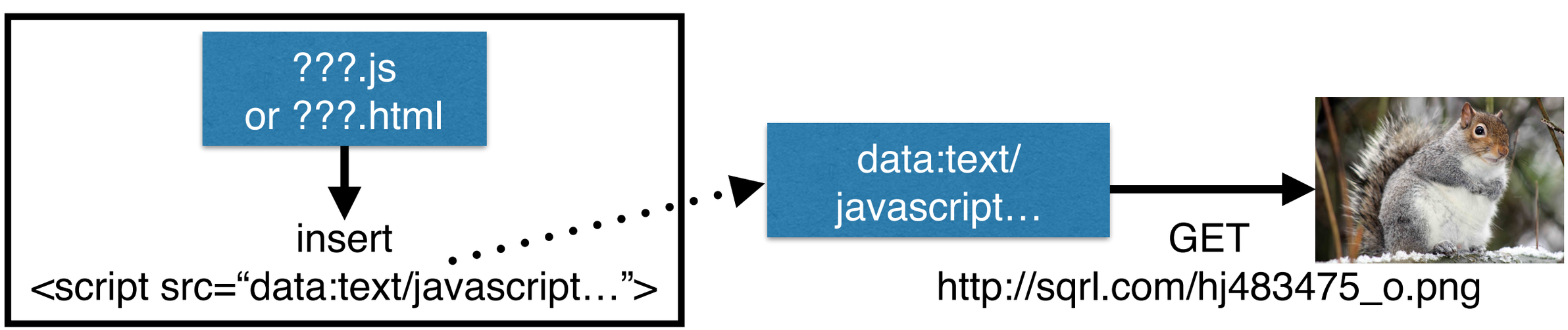
Async Call Stacks

Normal call stack:

Async call stack:

Call Stack	
(anonymous function)	anon.html:13
setTimeout (async)	
(anonymous function)	anon.html:12
m.event.dispatch	jquery-1.11.3.min.js:4
m.event.add.r.handle	jquery-1.11.3.min.js:4

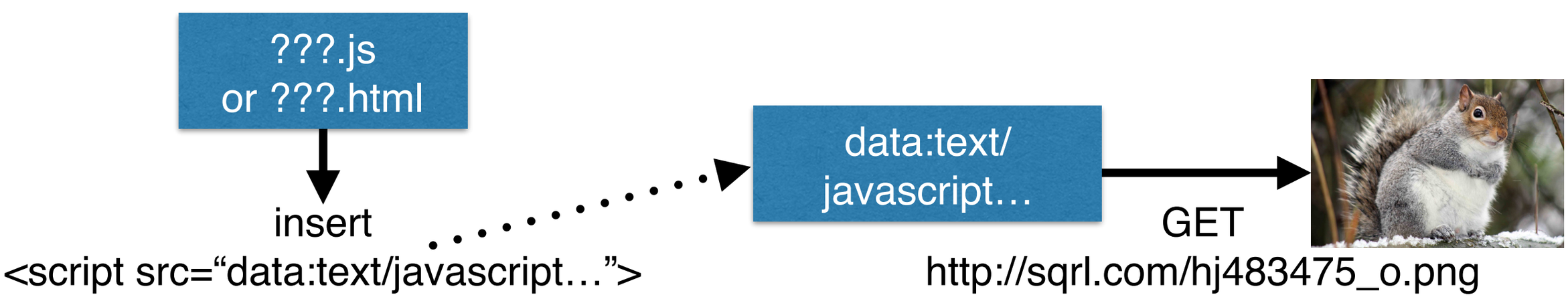
Async call stack?:



Chrome Developer Tools

Async Call Stacks in Networking Tab

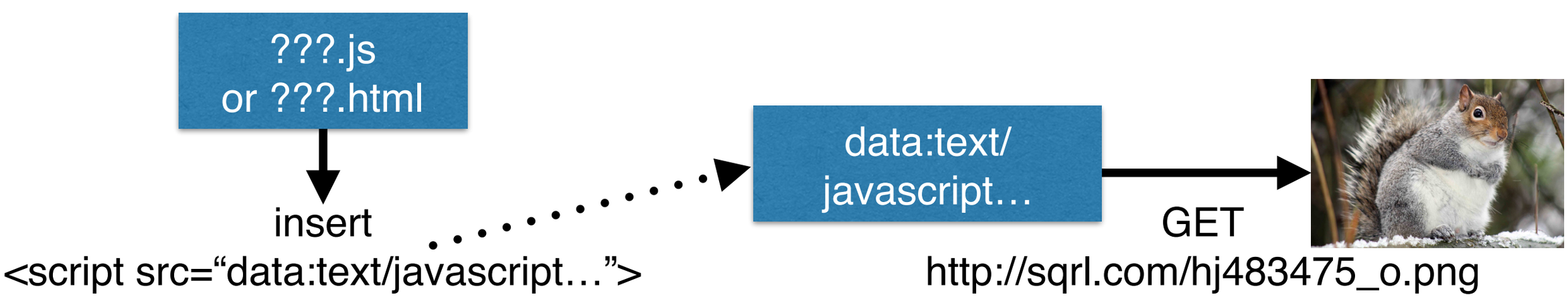
Name	Type	Initiator	Size
hj483475_o.png	png	data://text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB



Chrome Developer Tools

Async Call Stacks in Networking Tab

Name	Type	Initiator	Size
hj483475_o.png	png	data:/text/javascrip…	3.2 MB
application.4182f9e37cd…	script	C02FBQJPC	1.1 MB
rollup-core_required_libs.…	script	C02FBQJPC	640 KB
rollup-client.407bf2c7a4c…	script	C02FBQJPC	348 KB
rollup-secondary_a_requi…	script	C02FBQJPC	336 KB
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB



Chrome Developer Tools

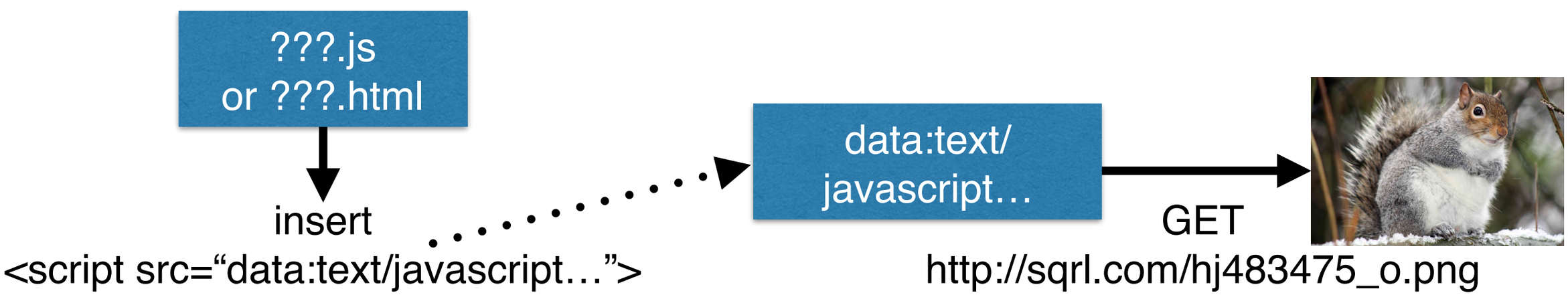
Async Call Stacks in Networking Tab

Name	Type	Initiator	Size
hj48			
appli			
rollu			
rollu			
rollu			
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Async Call Stack

Image (async)

(anonymous) @ data:text/javascript; base64,dmFyI



Chrome Developer Tools

Async Call Stacks in Networking Tab

Name	Type	Initiator	Size
hj48			
rollu			
templates.php?cb=91eb_…	script	C02FBQJPC	202 KB

Async Call Stack

(anonymous) @ data:text/javascript; base64,dmFyI

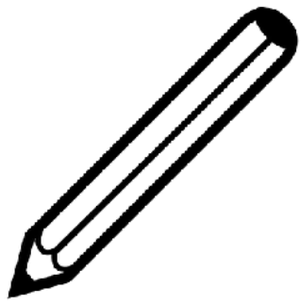
Async call stacks do not support DOM asynchrony!

slax

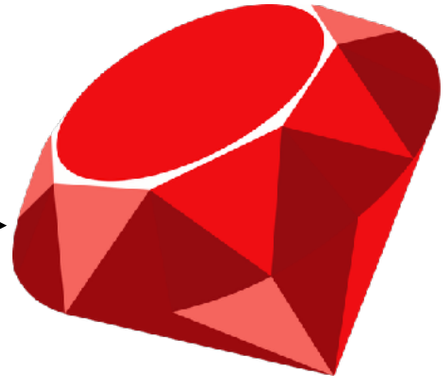
We have too many customers & cannot scale!!!

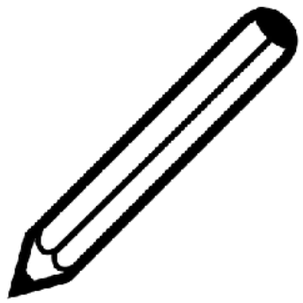
We have too many customers & cannot scale!!!

We have too many customers & cannot scale!!!

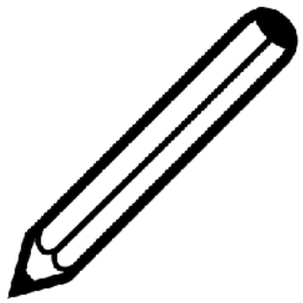


JSON messages



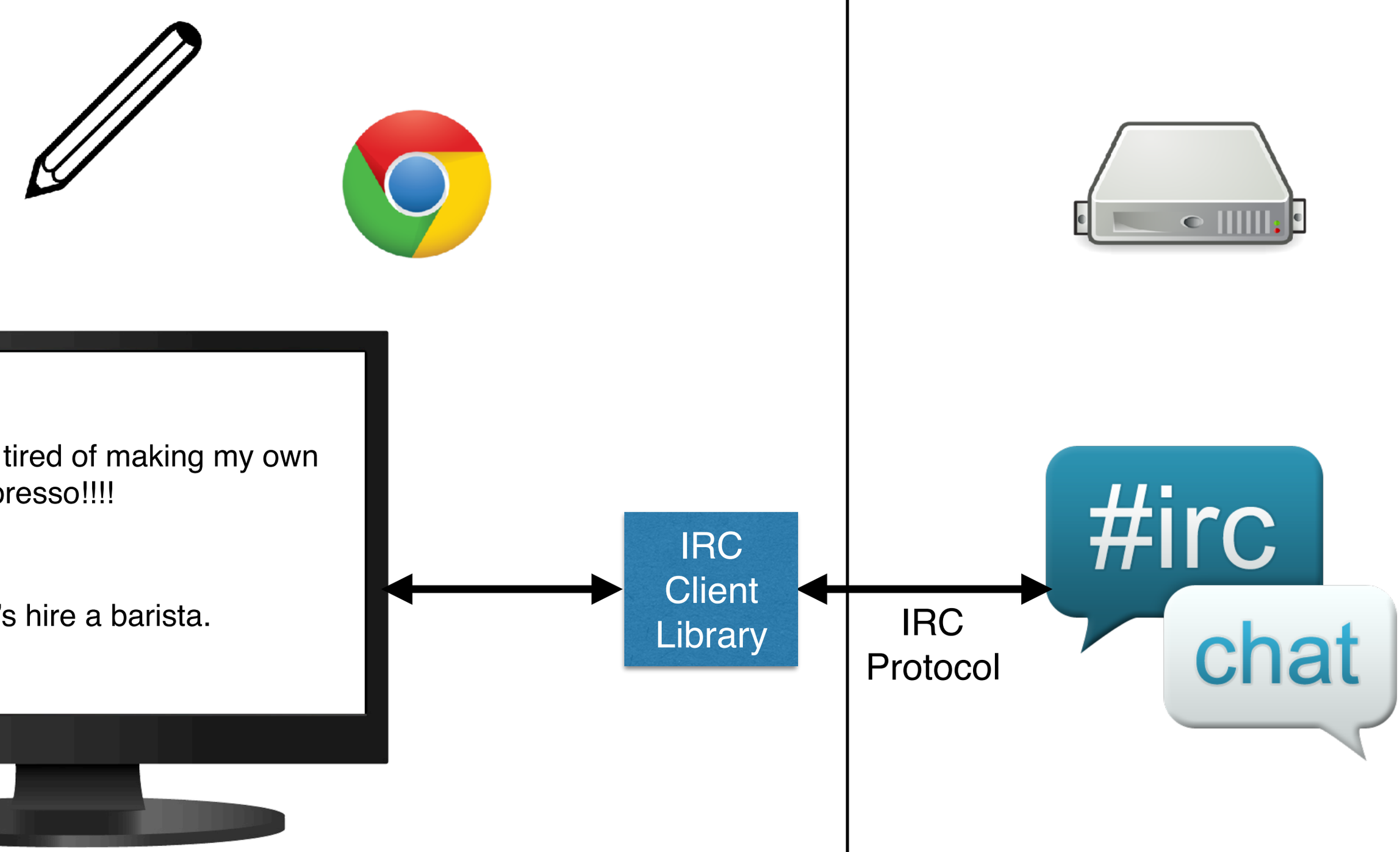


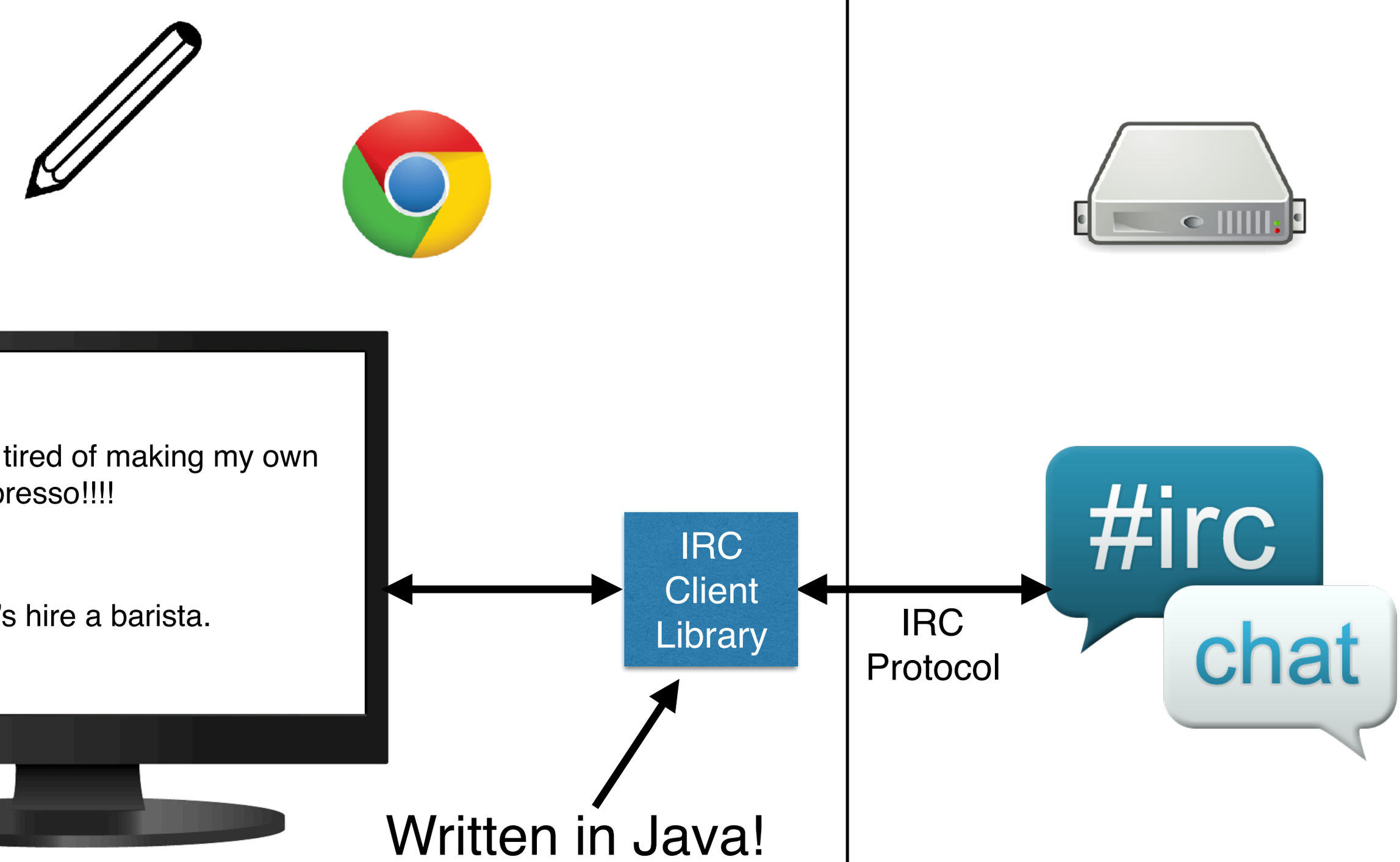
JSON messages

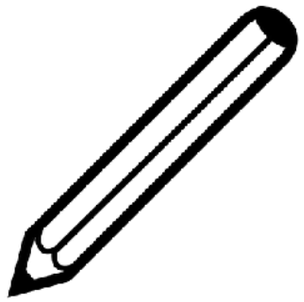


~~JSON messages~~

IRC Protocol


tired of making my own
presso!!!!
's hire a barista.
IRC
Client
Library
IRC
Protocol
#irc
chat


tired of making my own
presso!!!!
's hire a barista.
IRC
Client
Library
IRC
Protocol
#irc
chat
Written in Java!



tired of making m
presso!!!!

's hire a barista.

IRC Specifications

By Patrick Cloke
tags: Instantbird IRC programming specifications

So there's the original specification (RFC 1459) in May 1993; this was expanded and replaced by four di
2812, 2813) in April 2000. Seems

four different specifications

DCC/CTCP

Well, kind of...there's also the DCC/CTCP specifications, which is a separate protocol embedded/hidden within the IRC
s them as normal messages).
roleplaying, SED for
t more complicated — it starts
fully includes the DCC
There's also a CTCP/2
specification from October 1998, which was meant to reformulate a lot of the previous three versions. And *finally*, there's the DCC2 specification (two parts: connection negotiation and file transfers) from April 2004.

protocol embedded/hidden within the IRC protocol

But wait! I lied...that's not really the end of DCC/CTCP, there's also a bunch of extensions to it: Turbo DCC, XDCC (eXtended DCC) in 1993, DCC Whitebo
Voice, etc. Wikipedia has a good sum

parts of it just *don't* have any documentation

Something else to note about the wh
all for SED (at least that I've found, I'

So, we're about halfway through now. There's a bunch of extensions to the IRC protocol specifications that add new commands to the actual protocol.

There's a bunch of extensions [like authentication]

v servers seem to use, a variety of
ISH methods, although BLOWFISH
isn't documented); and SASL itself is covered by at least four RFCs in this situation. There also seems to be a method called "Auth" which I haven't been able to pin down, as well as Ident (which is a more general protocol authentication method I haven't looked into yet).

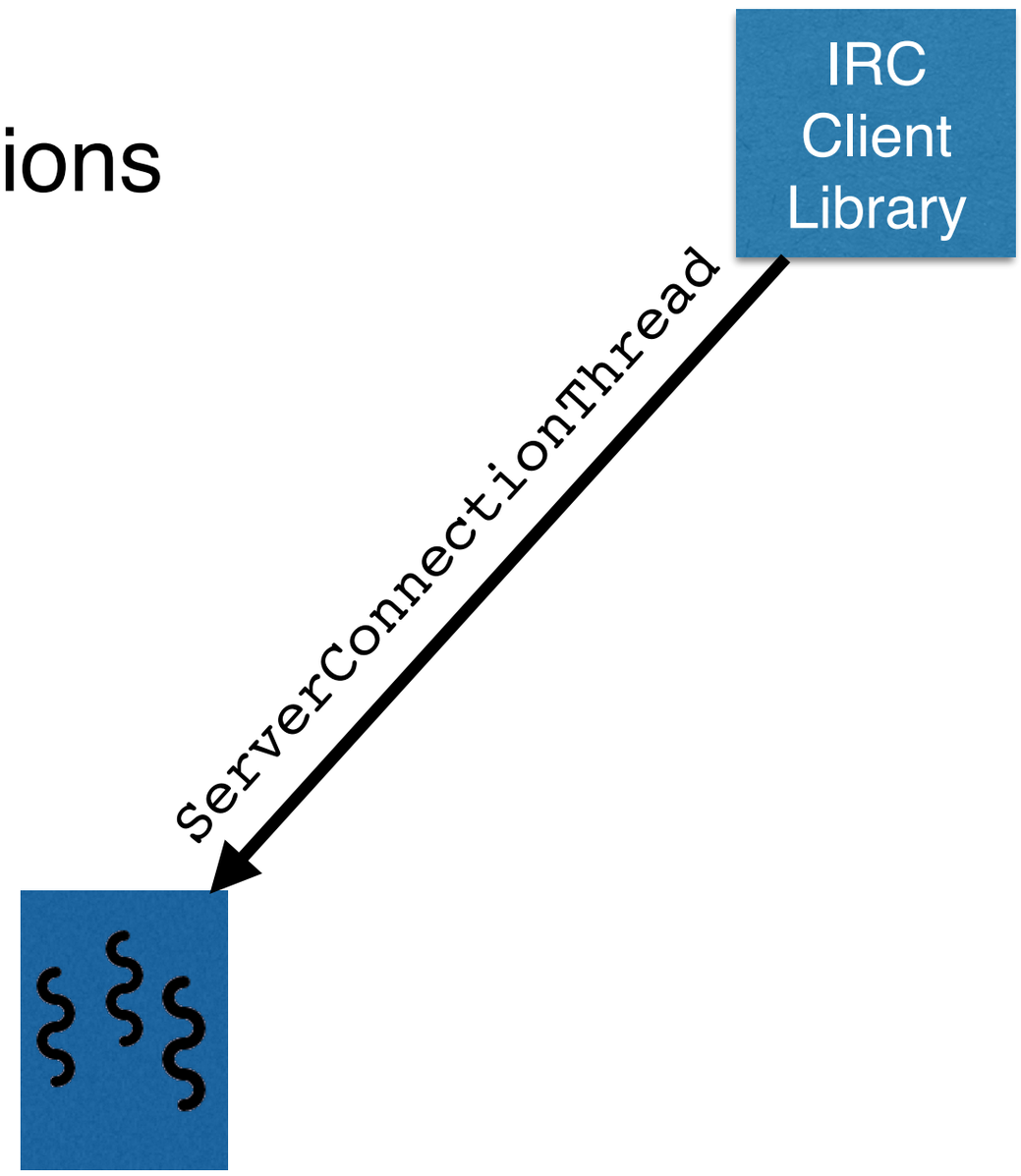
Compile Java to JavaScript?

Browser Restrictions

IRC
Client
Library

Compile Java to JavaScript?

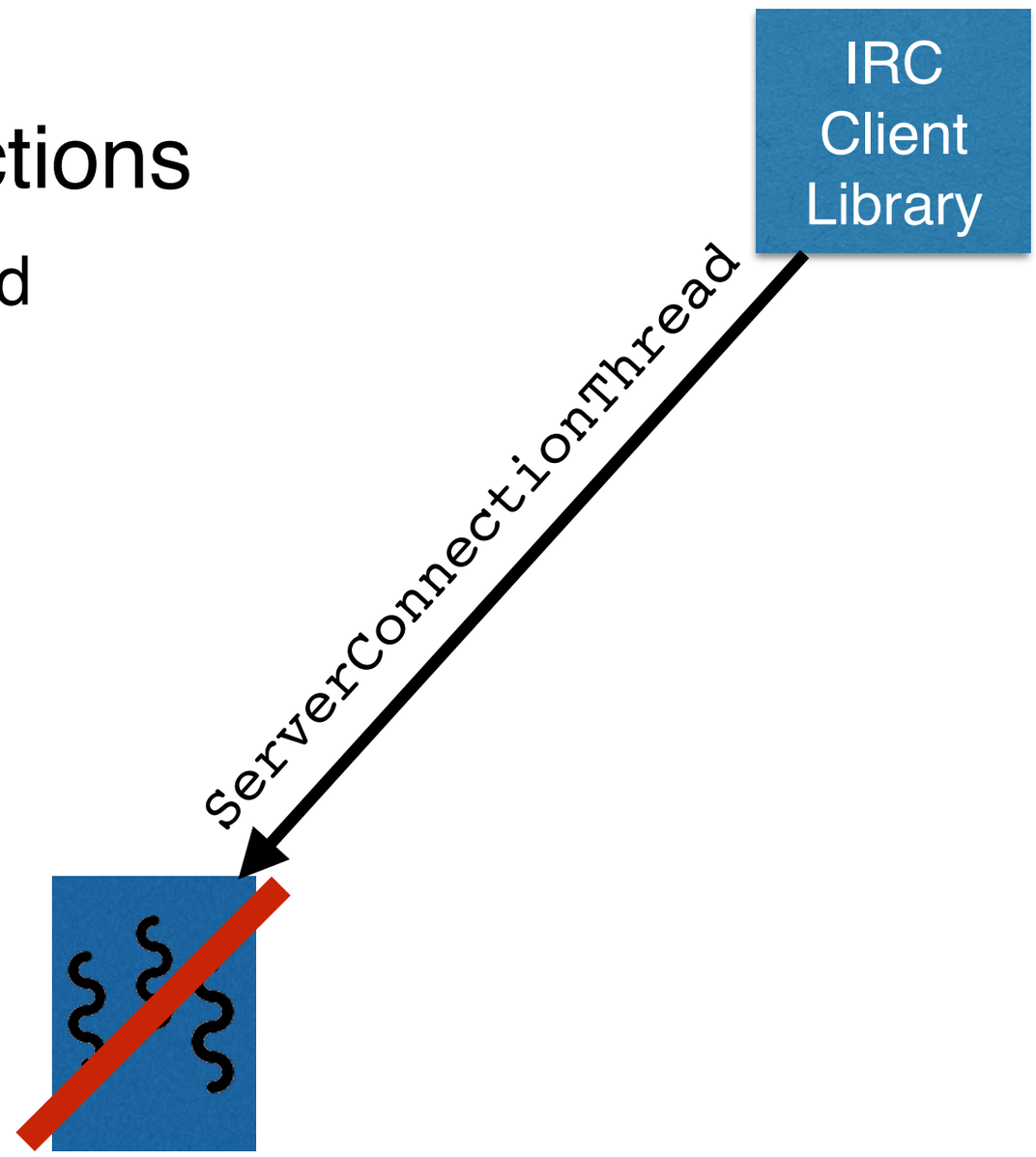
Browser Restrictions



Compile Java to JavaScript?

Browser Restrictions

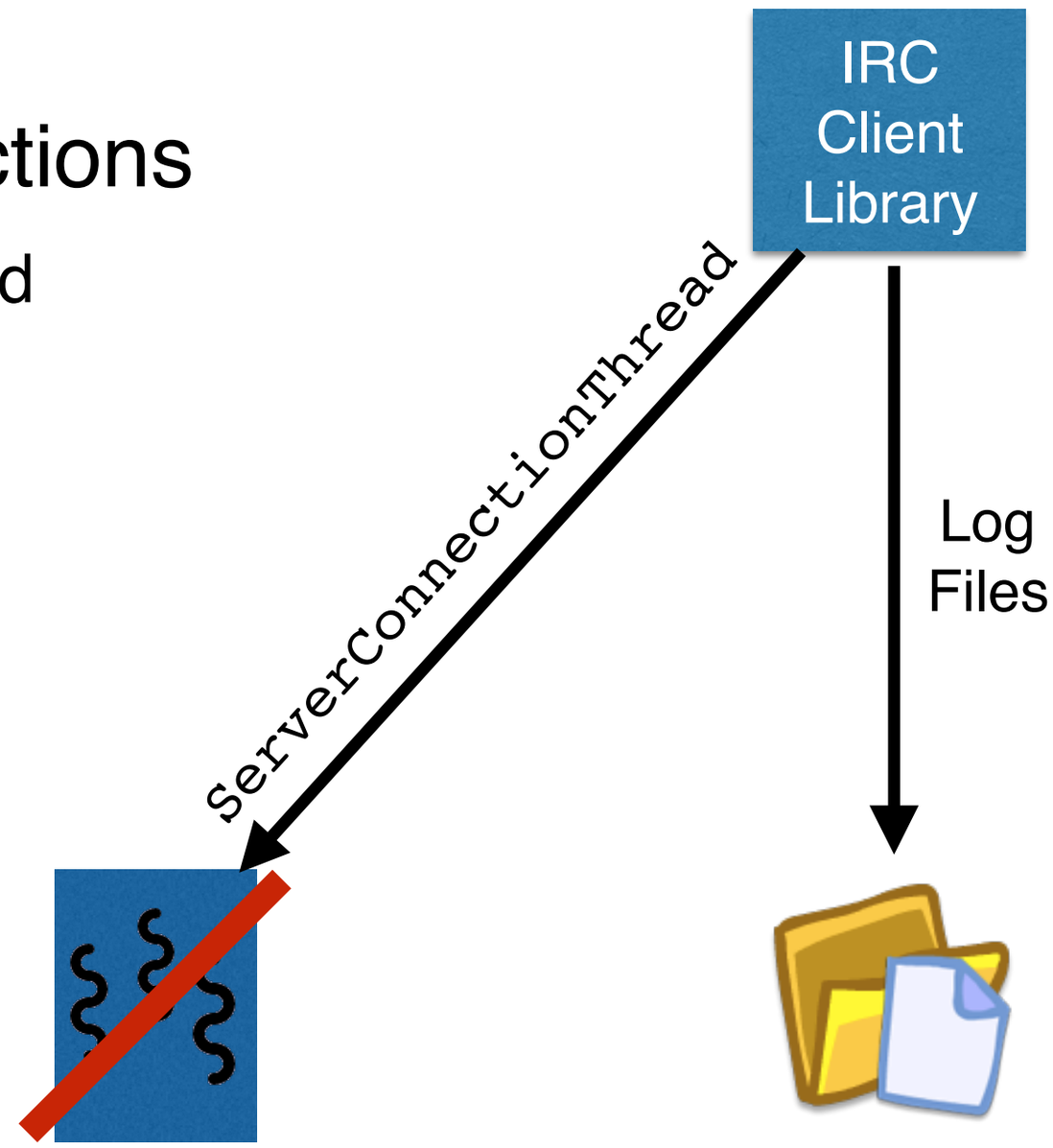
- Single threaded



Compile Java to JavaScript?

Browser Restrictions

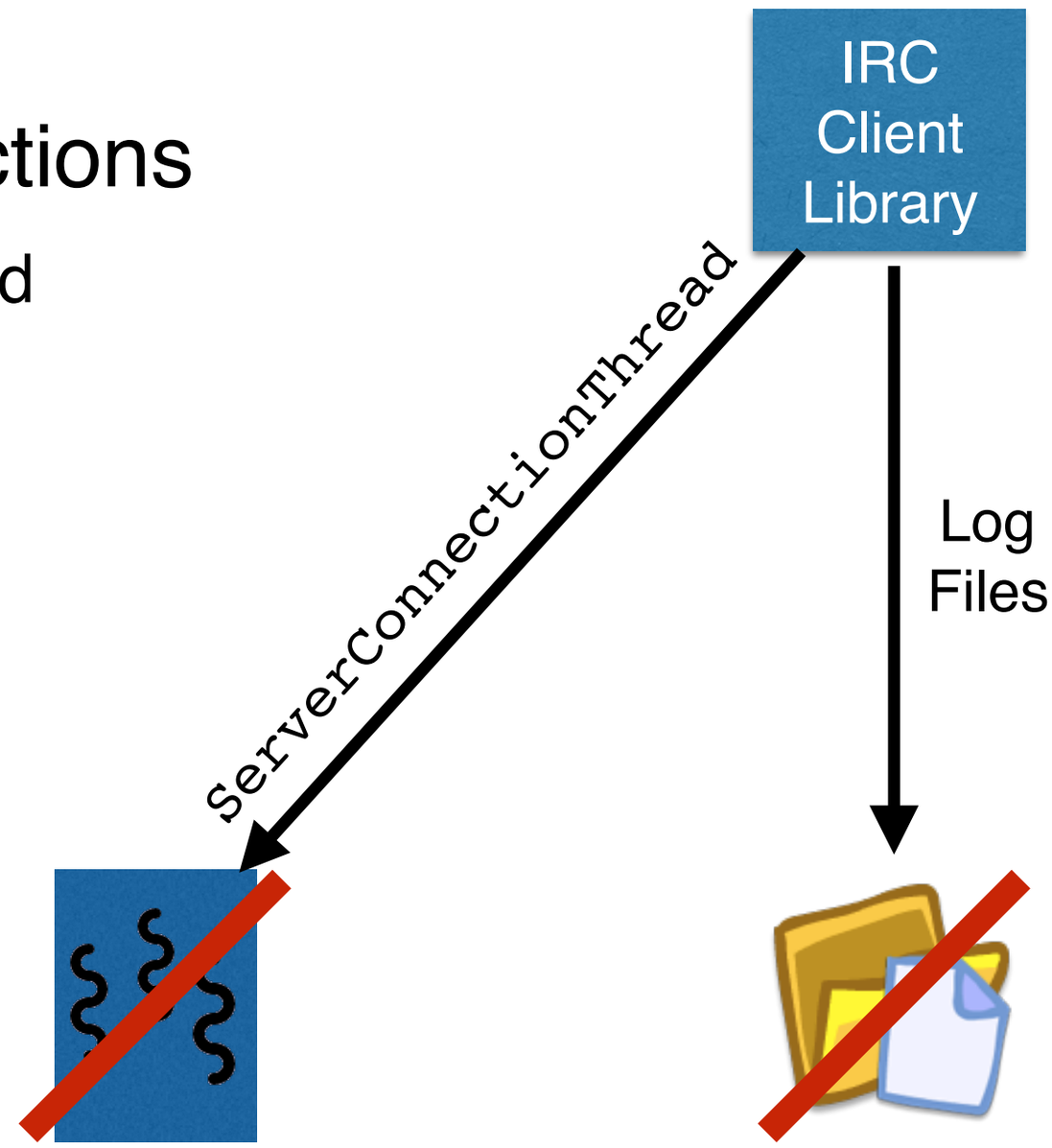
- Single threaded



Compile Java to JavaScript?

Browser Restrictions

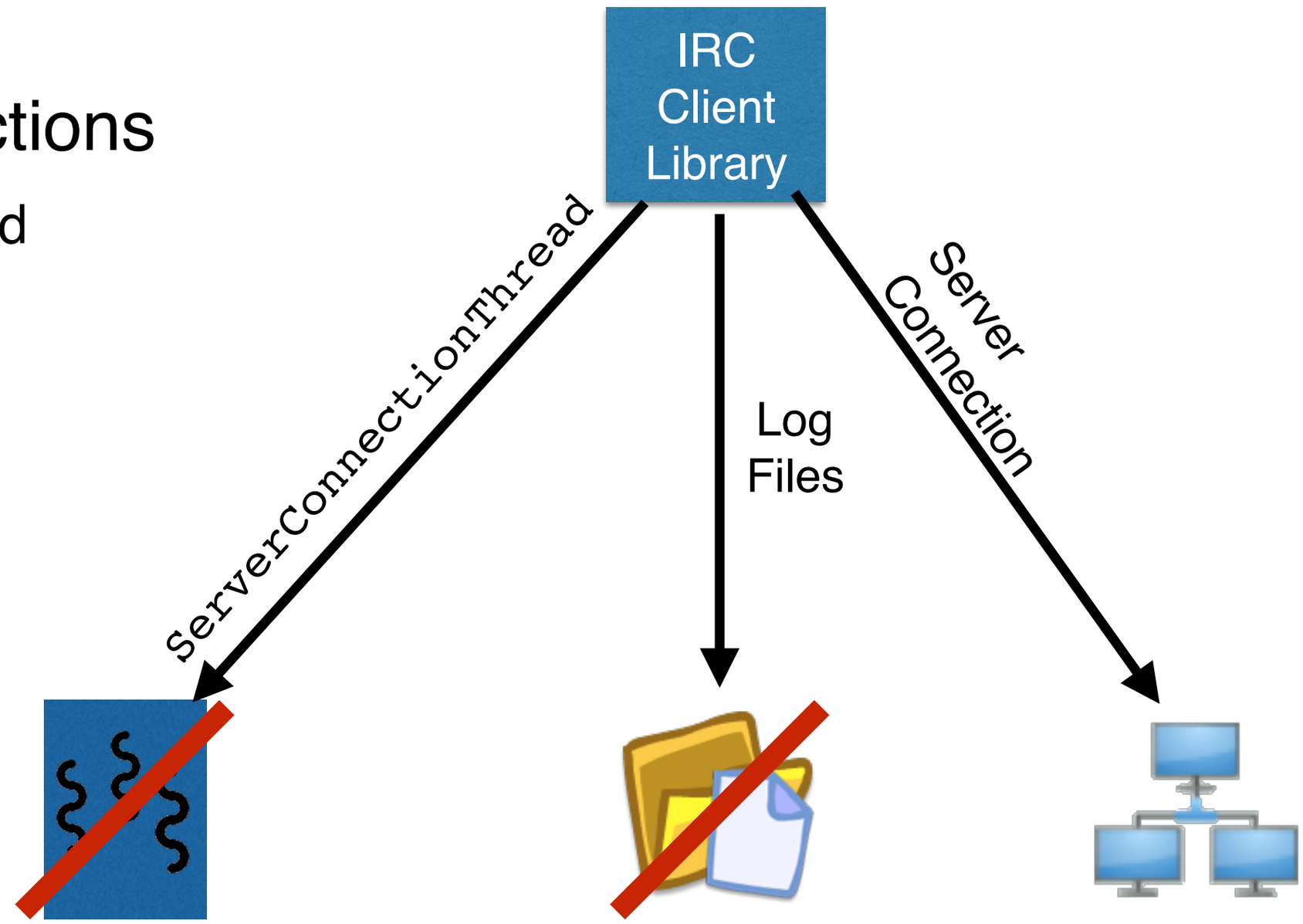
- Single threaded
- No file system



Compile Java to JavaScript?

Browser Restrictions

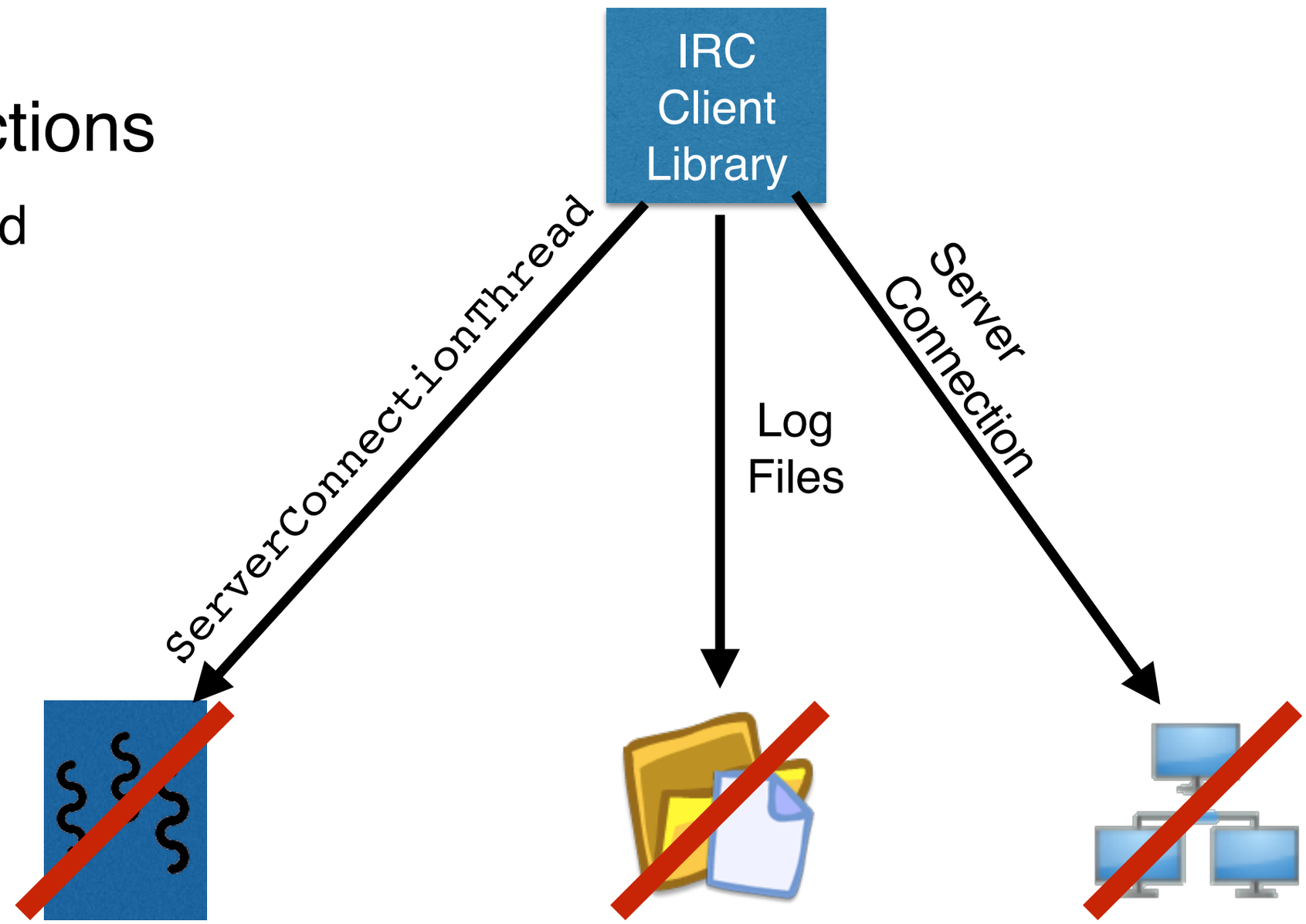
- Single threaded
- No file system



Compile Java to JavaScript?

Browser Restrictions

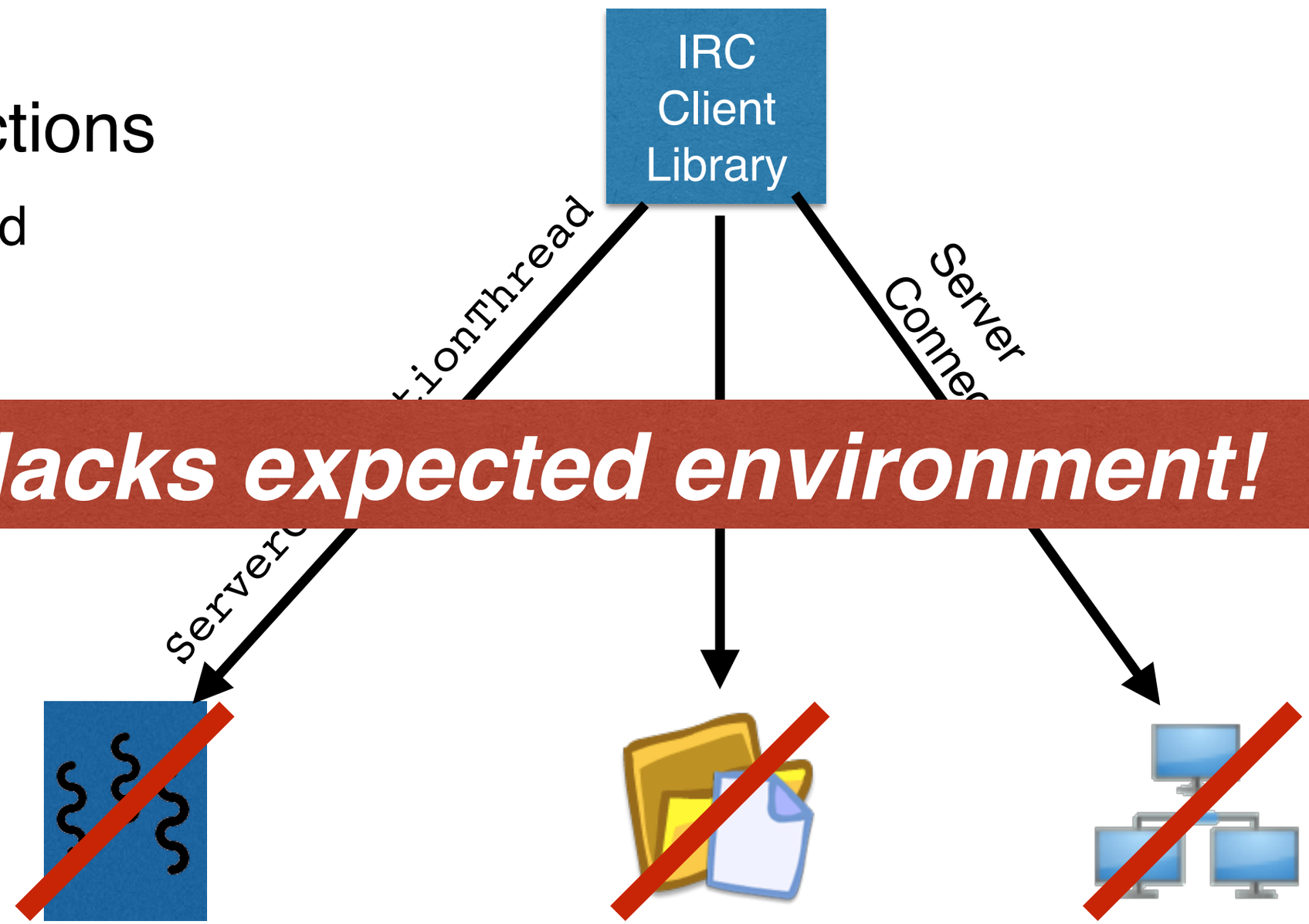
- Single threaded
- No file system
- No sockets



Compile Java to JavaScript?

Browser Restrictions

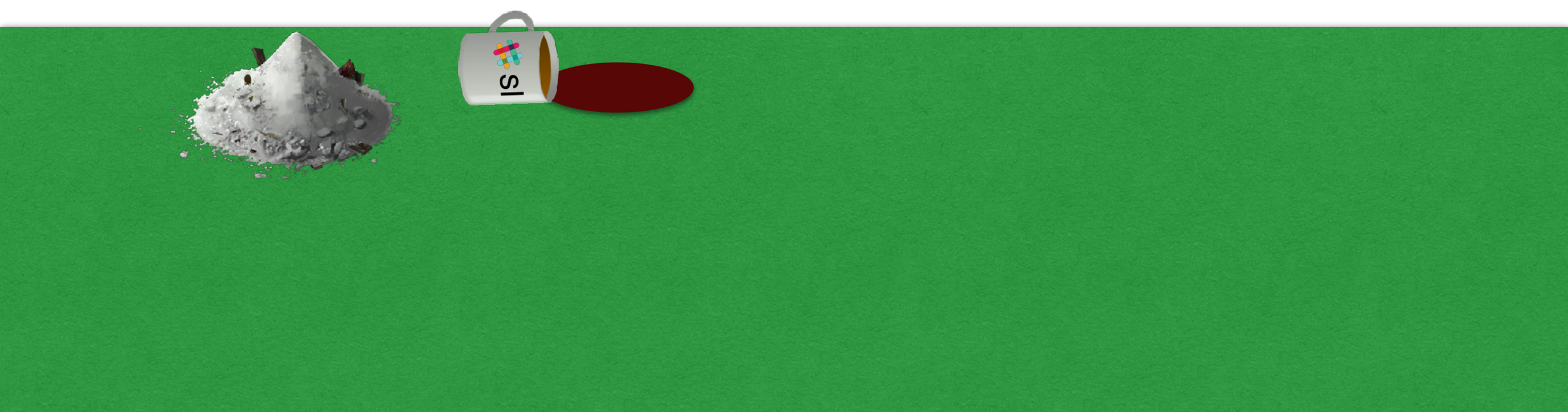
- Single threaded
- No file system
- No sockets

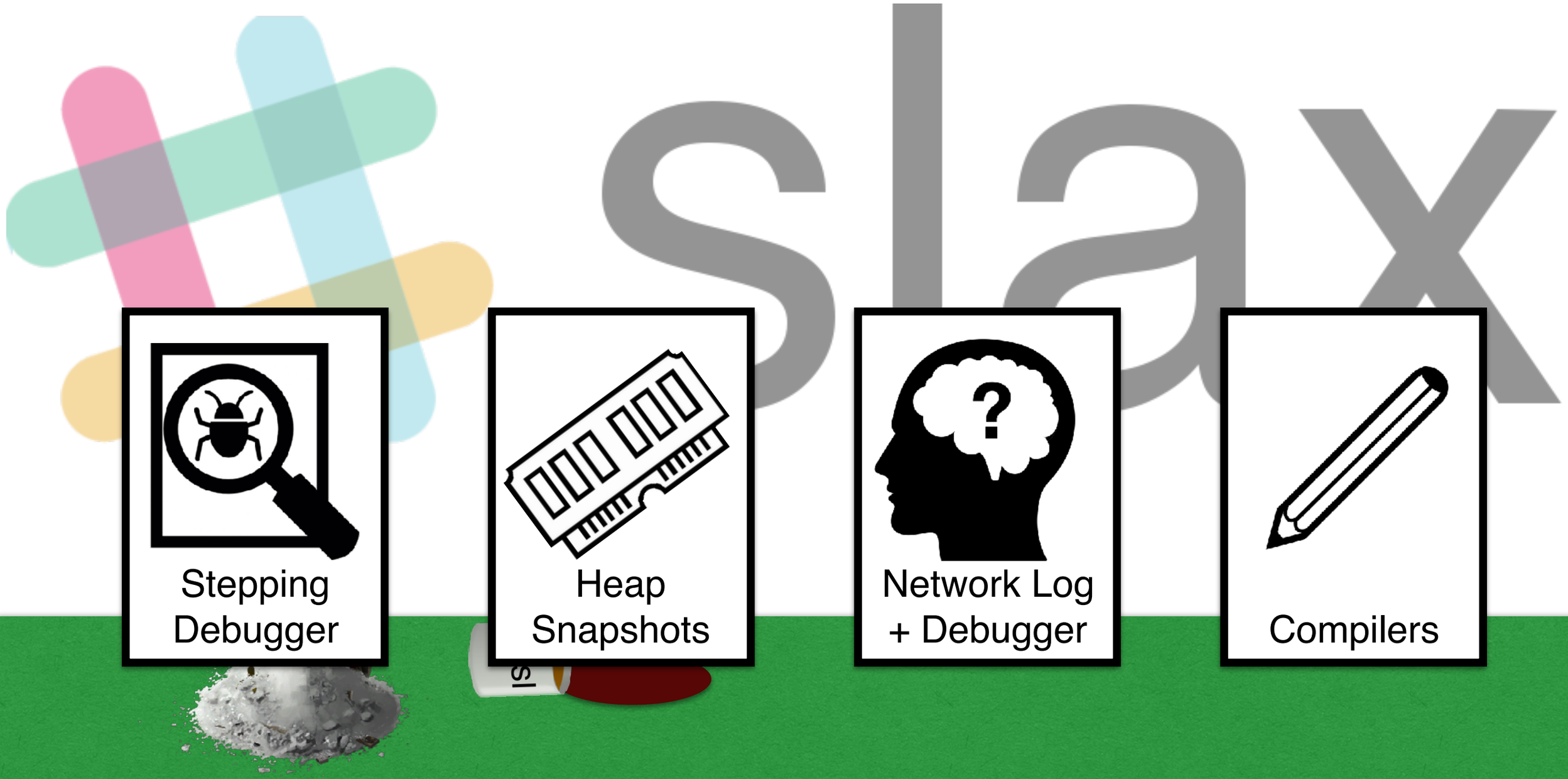


Browser lacks expected environment!

...
sl

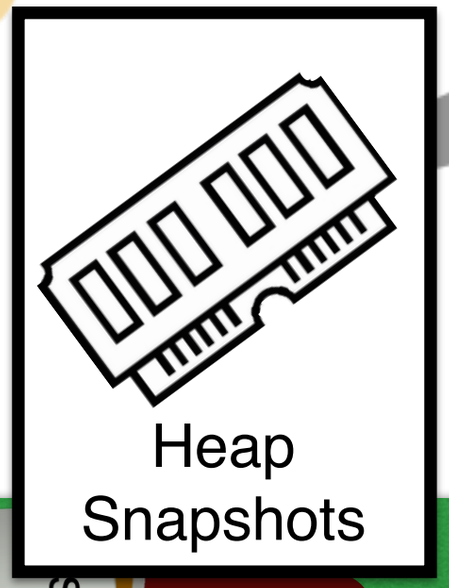
slax



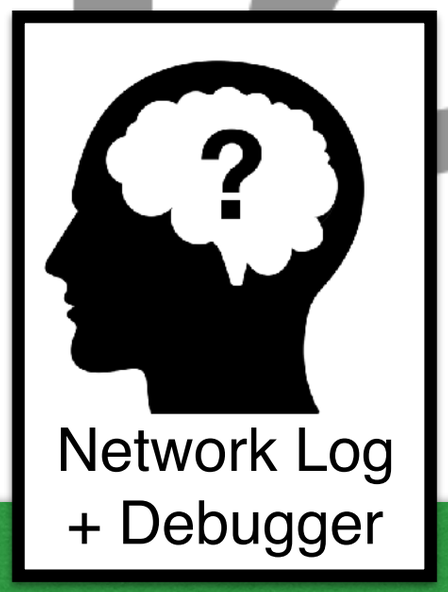

slax
Stepping Debugger
Heap Snapshots
Network Log + Debugger
Compilers

Conventional development tools are ineffective!

Stepping Debugger



Heap Snapshots

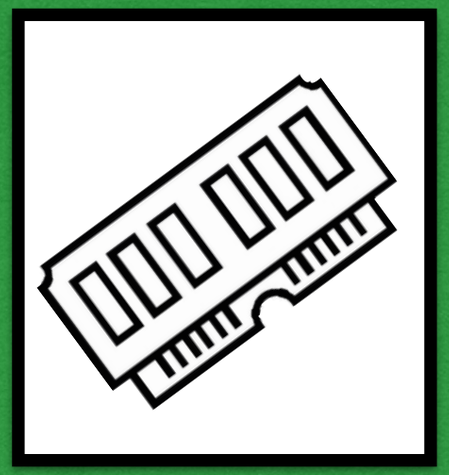


Network Log + Debugger

Compilers

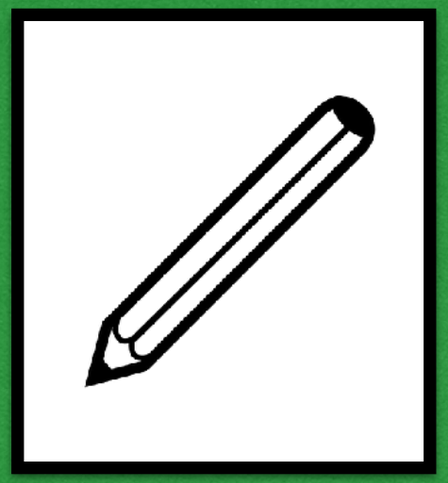
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)

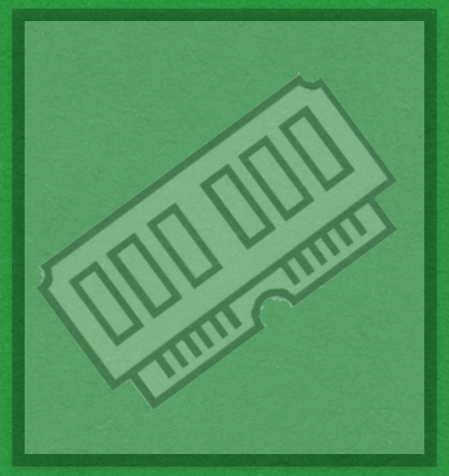


POSIX Support (Doppio)

Unix Support (Browsix)

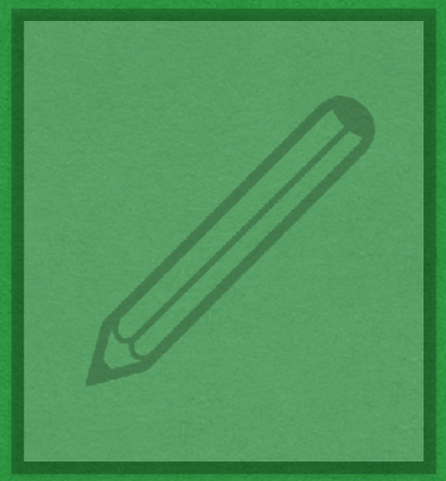
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

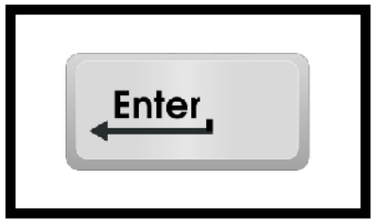
Causal Program Understanding (BCause)

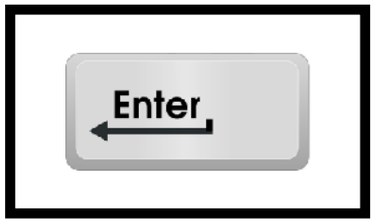


POSIX Support (Doppio)

Unix Support (Browsix)

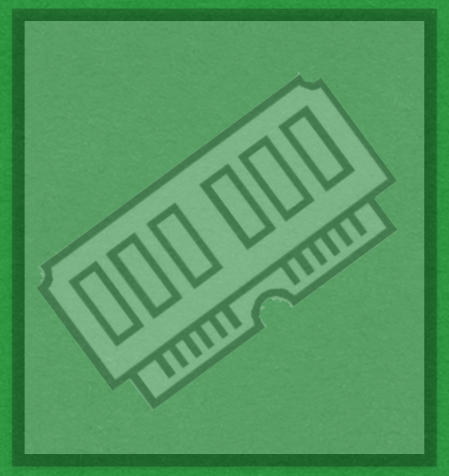
The first time-traveling debugger for web apps





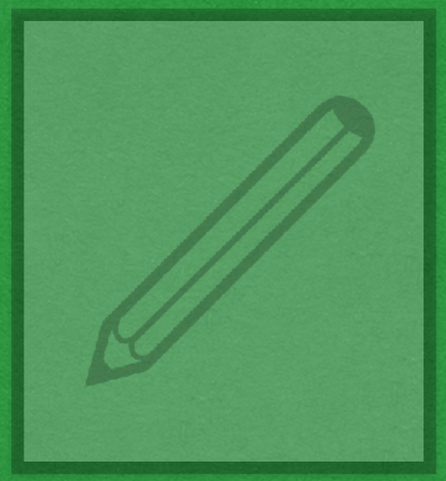
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)

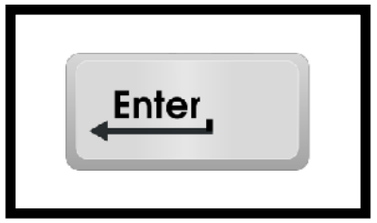


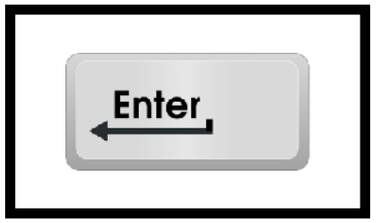
POSIX Support (Doppio)

Unix Support (Browsix)

The first time-traveling debugger for web apps

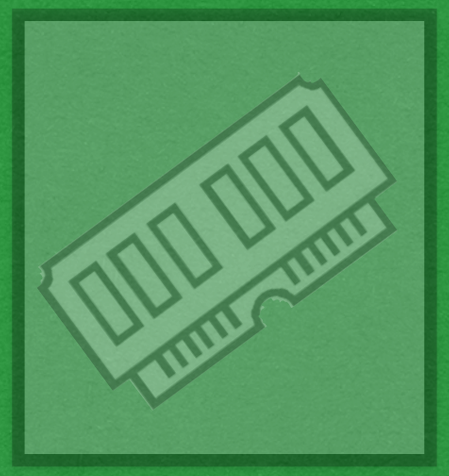
Reproduces browser task and GUI nondeterminism.





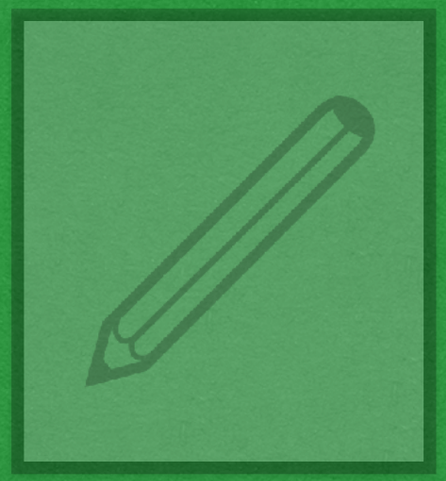
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



POSIX Support (Doppio)

Unix Support (Browsix)

The first time-traveling debugger for web apps

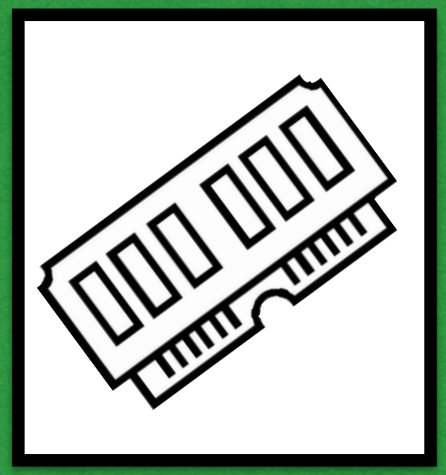
Microsoft

Foundation of new JavaScript time-traveling debugger

github.com/Microsoft/ChakraCore

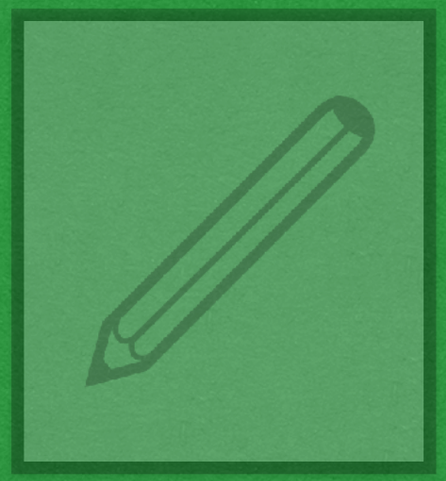
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



POSIX Support (Doppio)

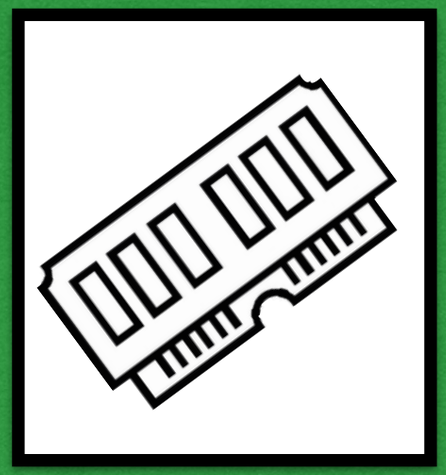
Unix Support (Browsix)

Automatically locates and debugs memory leaks.

Leak Root	Code Responsible
resize' event listeners on document	app.js:32:4, app.js:10:4

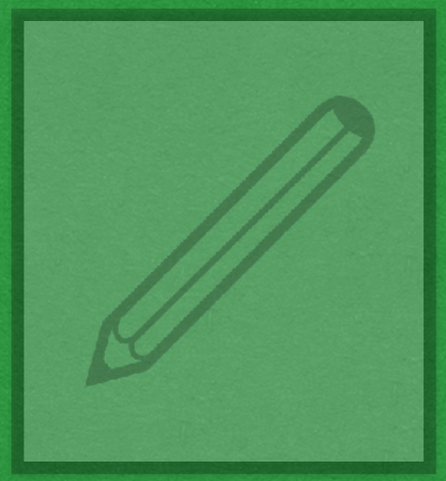
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



POSIX Support (Doppio)

Unix Support (Browsix)

Automatically locates and debugs memory leaks.

ANGULARJS by Google

Firefox debugger.html

jQuery

Google Analytics

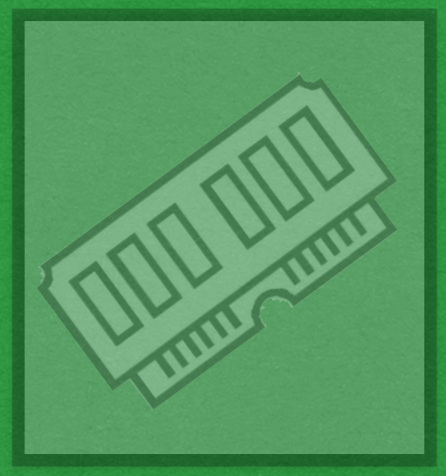
airbnb

Google Maps

Found 50+ new memory leaks in production web applications.

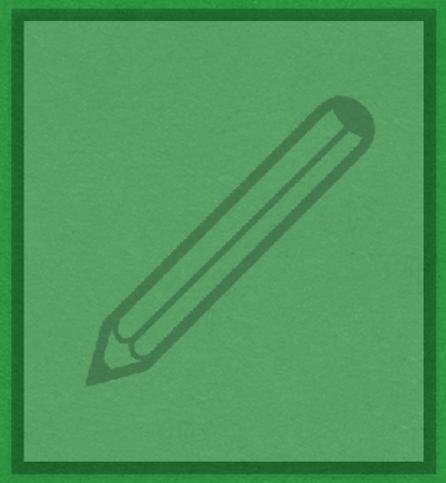
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



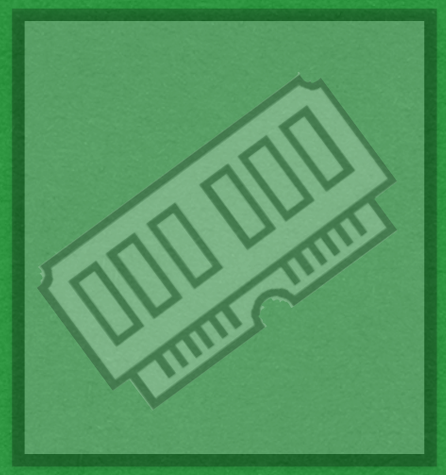
POSIX Support (Doppio)

Unix Support (Browsix)

Builds causal graph of asynchronous program behavior

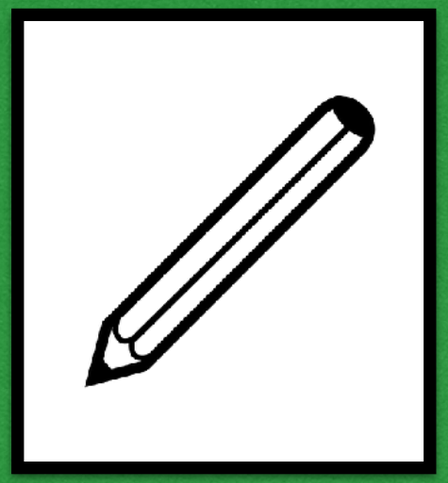
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

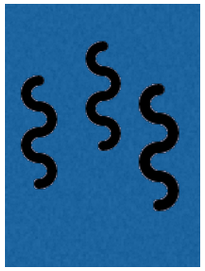
Causal Program Understanding (BCause)



POSIX Support (Doppio)

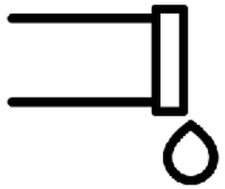
Unix Support (Browsix)

Run existing code in the browser.

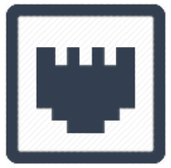


Threads

Shared Filesystem



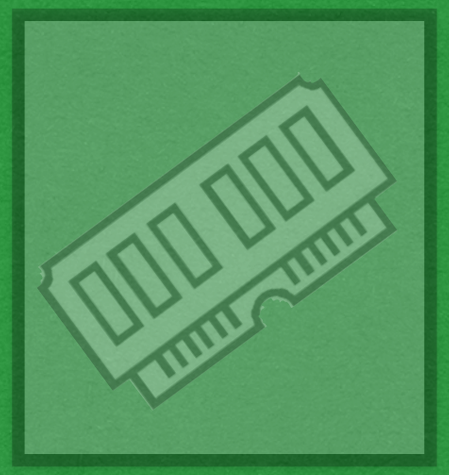
Pipes



Sockets

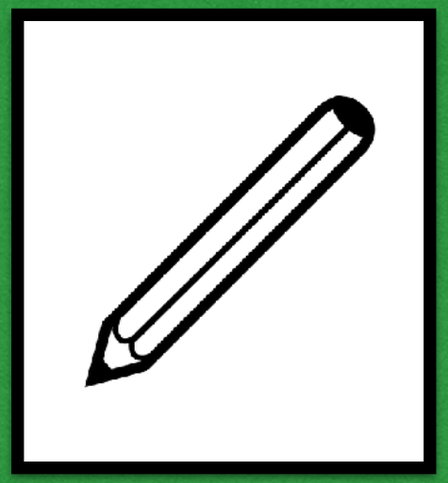
Righting Web Development

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



POSIX Support (Doppio)

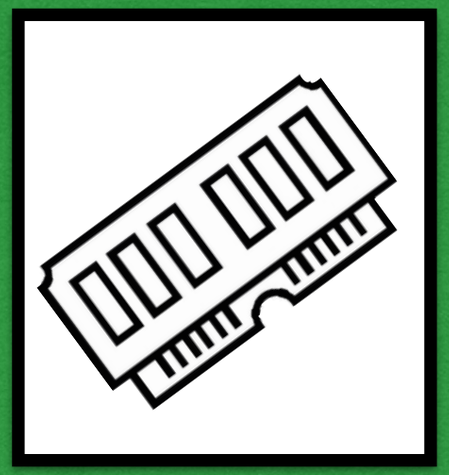
Unix Support (Browsix)

Run existing code in the browser.

INTERNET ARCHIVE

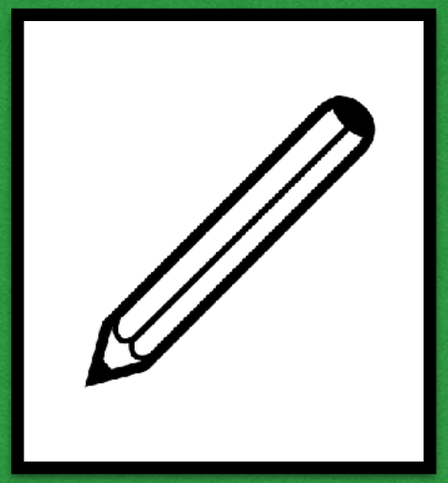
Righting Web Development

Time-Traveling Debugger (McFly)



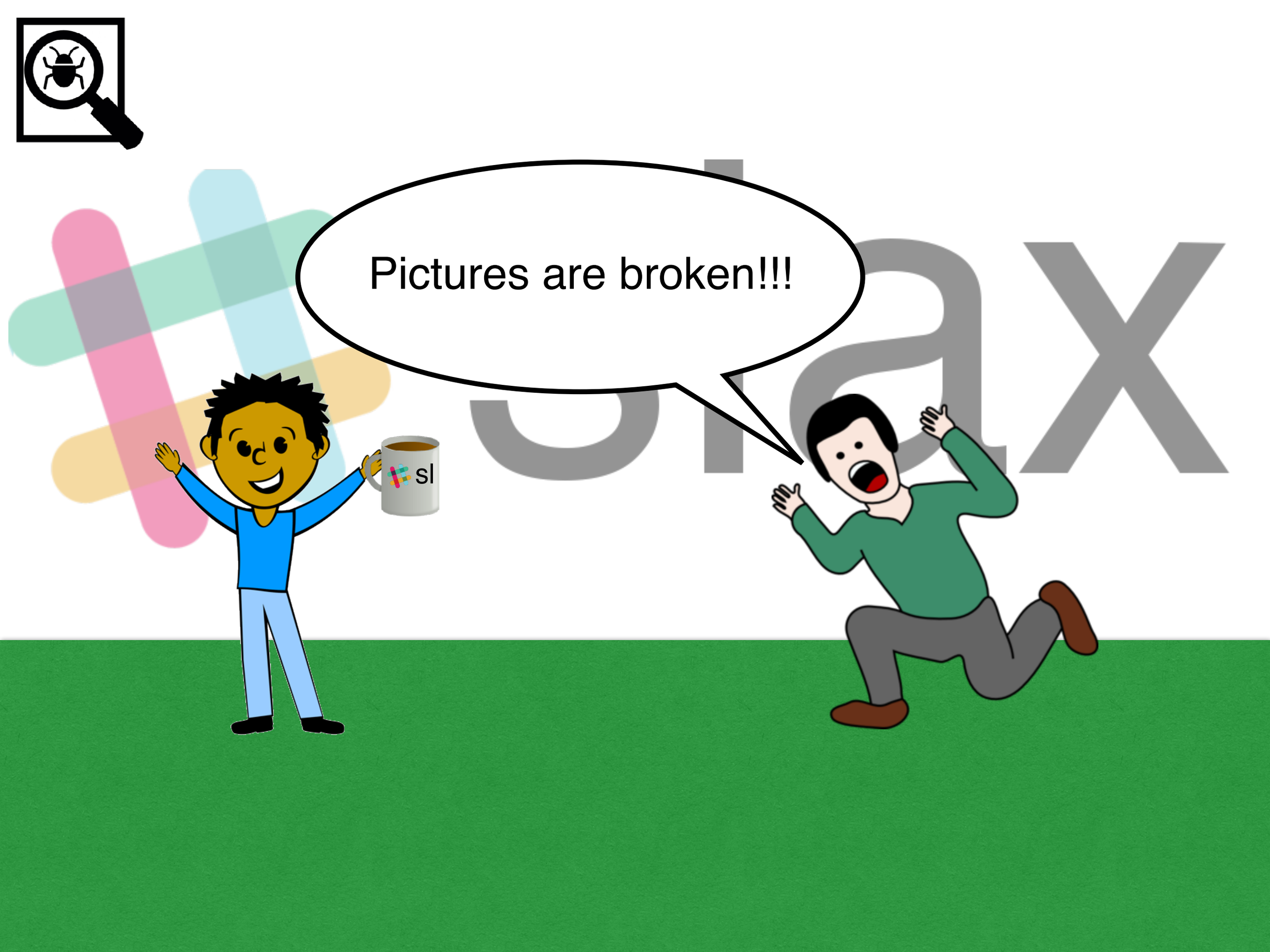
Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



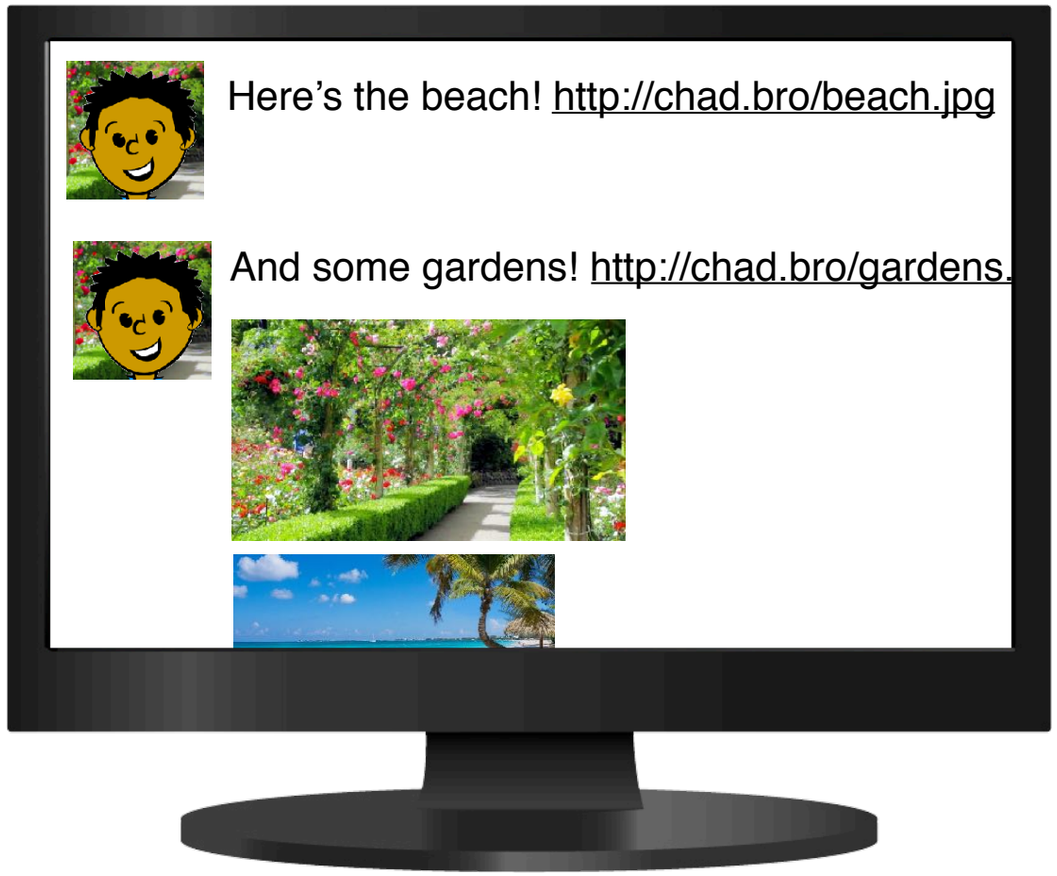
POSIX Support (Doppio)

Unix Support (Browsix)

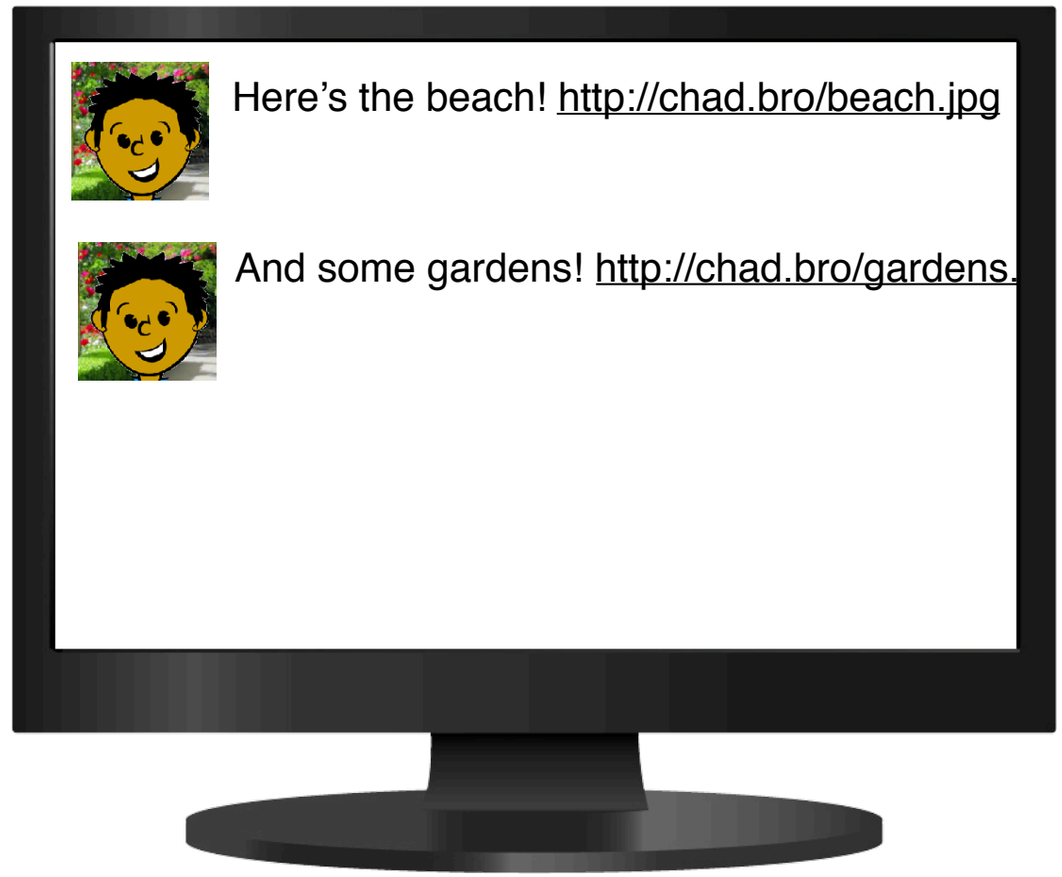

Pictures are broken!!!
sl

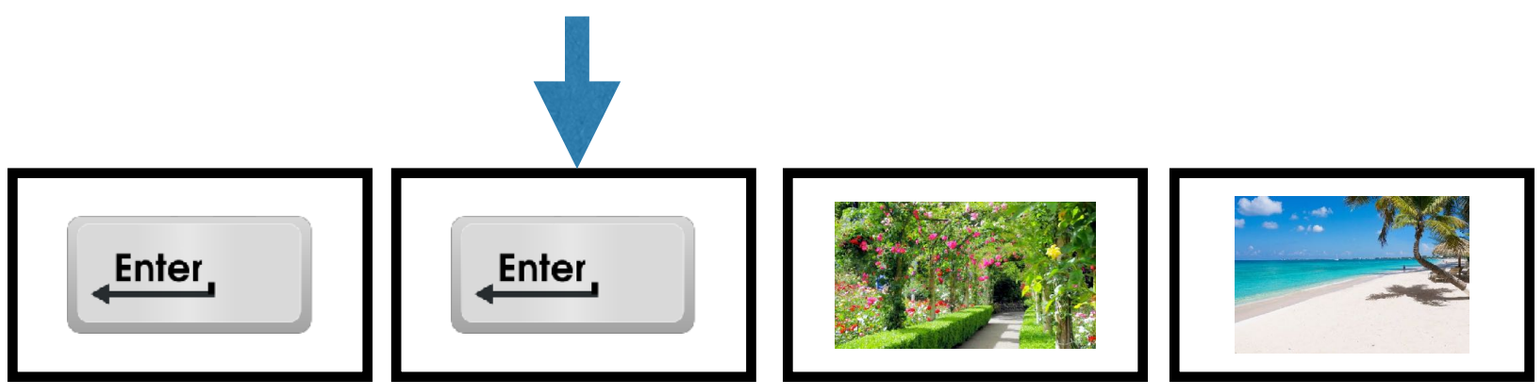
Desired Debugger Experience

Desired Debugger Experience

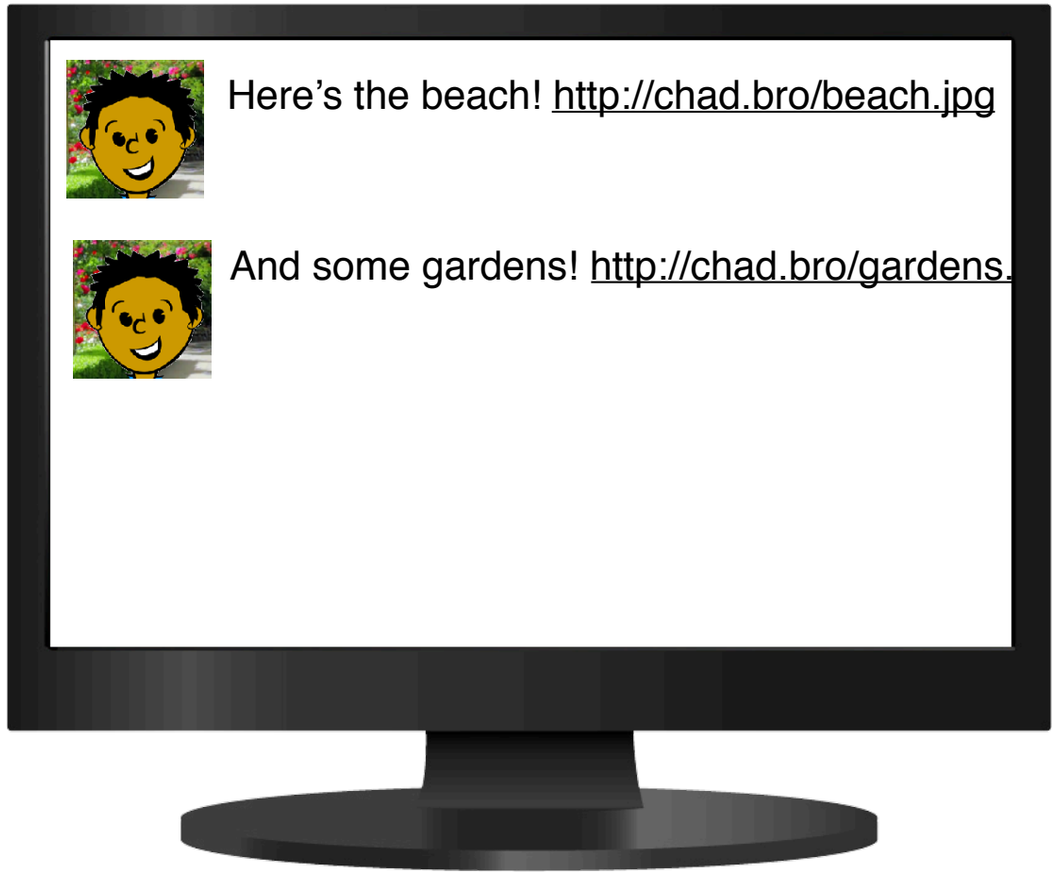


Desired Debugger Experience

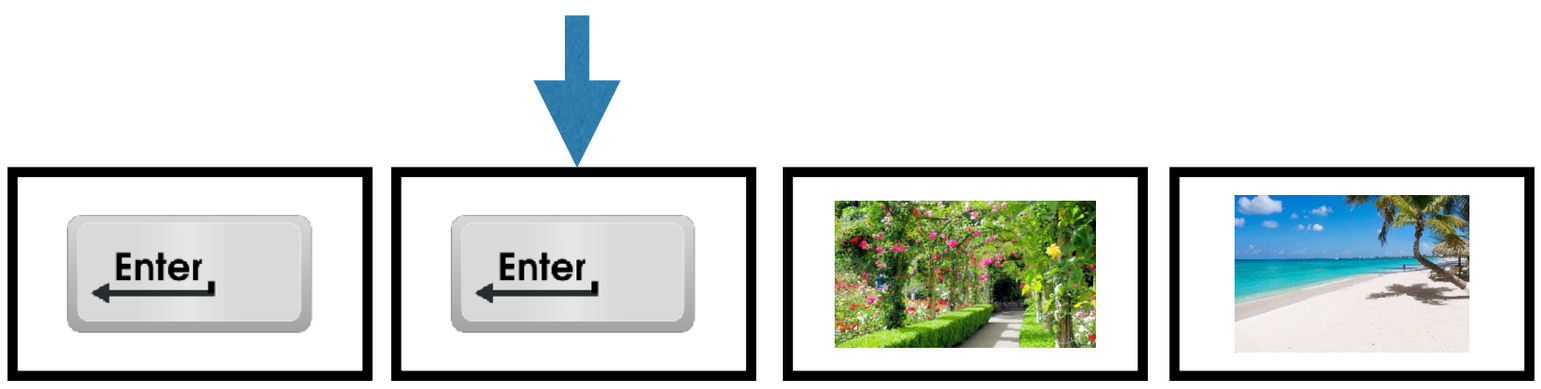




Desired Debugger Experience



Time-Traveling Debugger



Time-Traveling Debuggers

None exist for web applications!

Only exist for conventional programming languages (C/C++/C#)

Time-Traveling Debuggers

None exist for web applications!

Only exist for conventional programming languages (C/C++/C#)

Typical approach: Record + Replay

Conventional Time-Traveling Debuggers

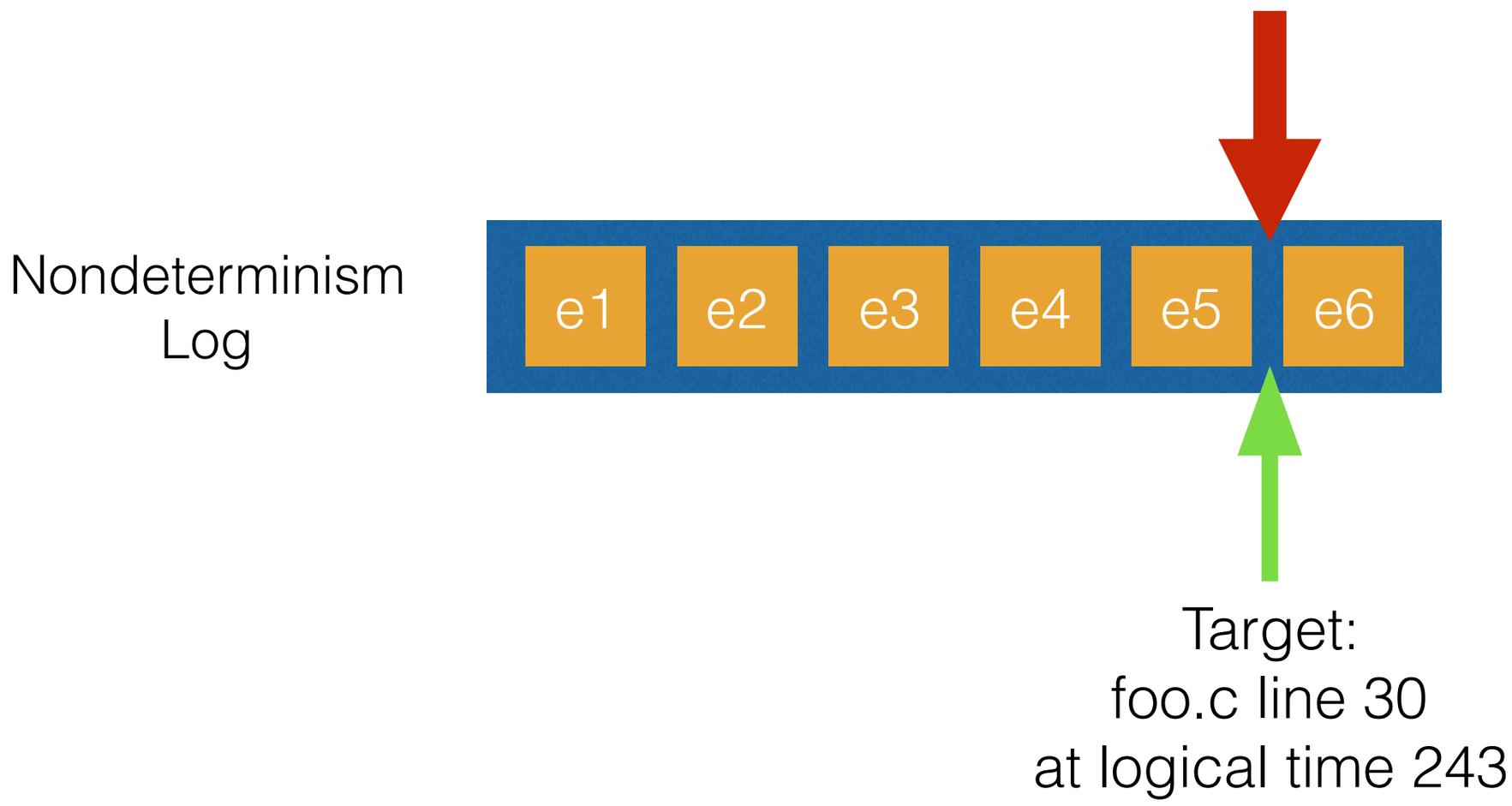
Nondeterminism Log

Conventional Time-Traveling Debuggers

Nondeterminism Log

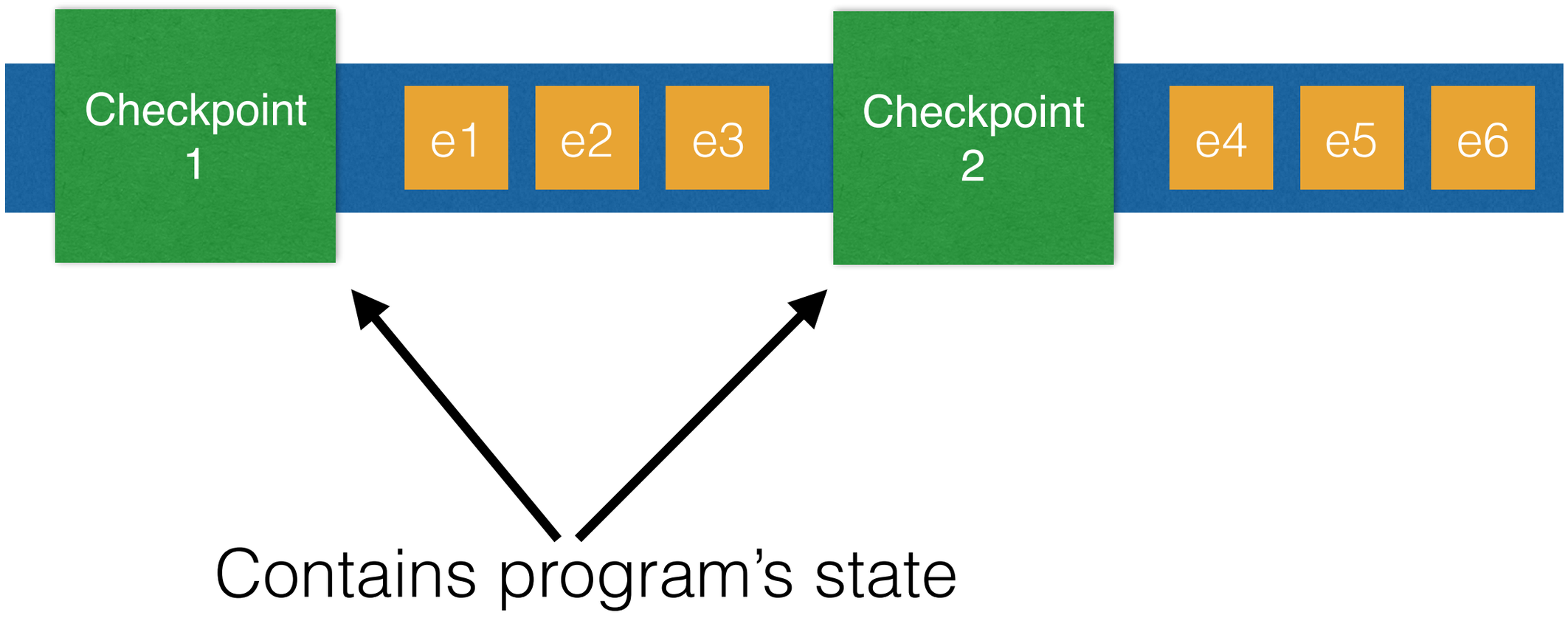
Conventional Time-Traveling Debuggers

Must replay from beginning!



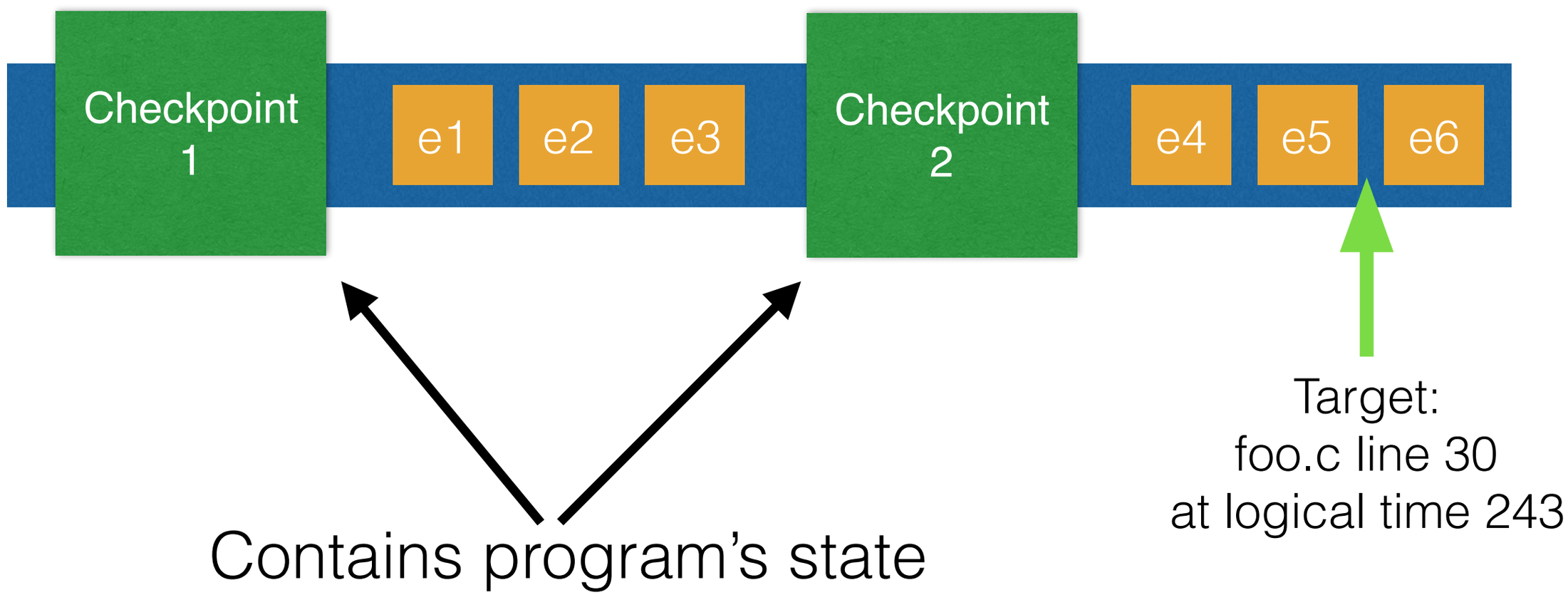
Conventional Time-Traveling Debuggers

Optimization: Checkpoints



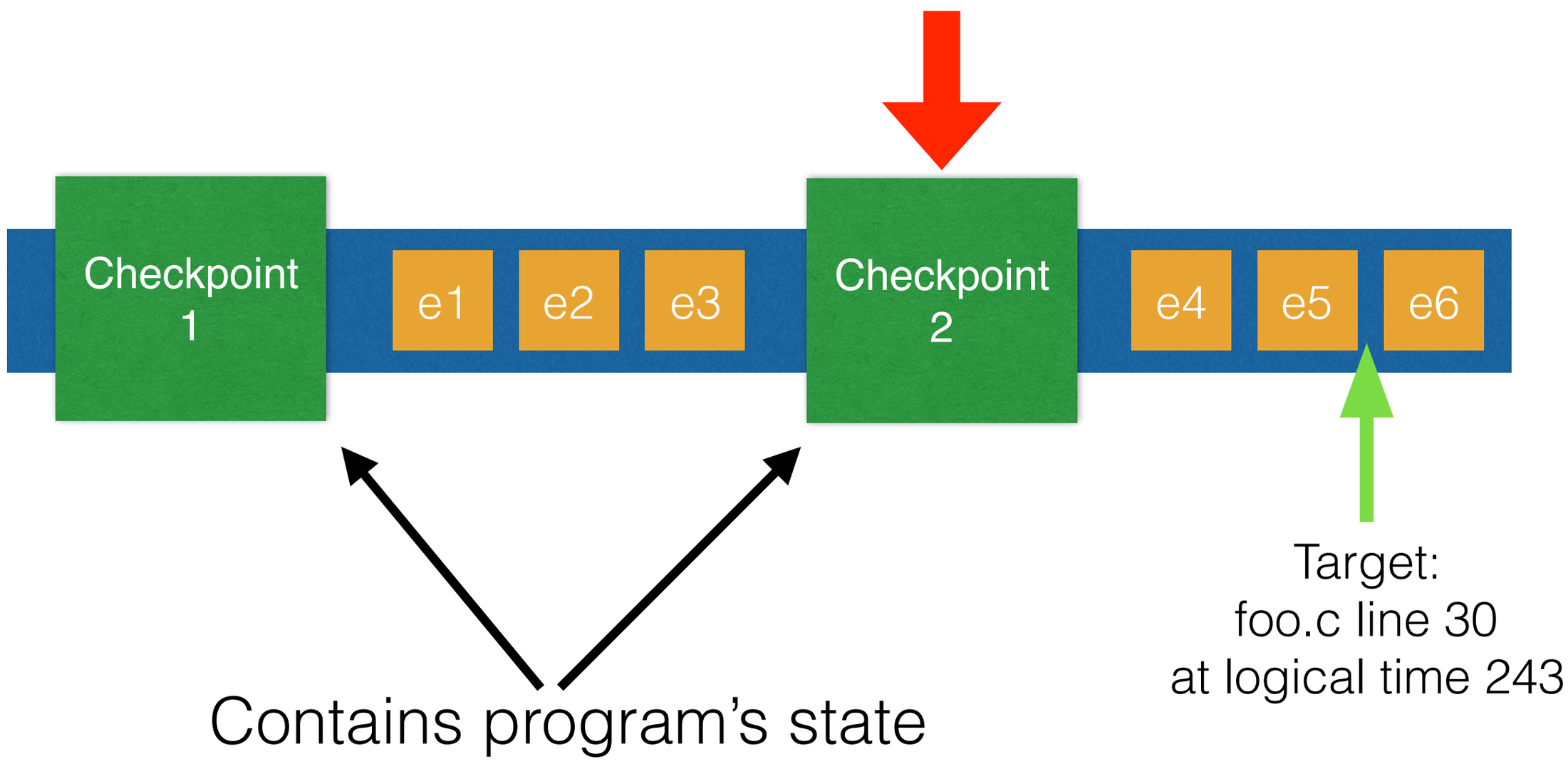
Conventional Time-Traveling Debuggers

Optimization: Checkpoints



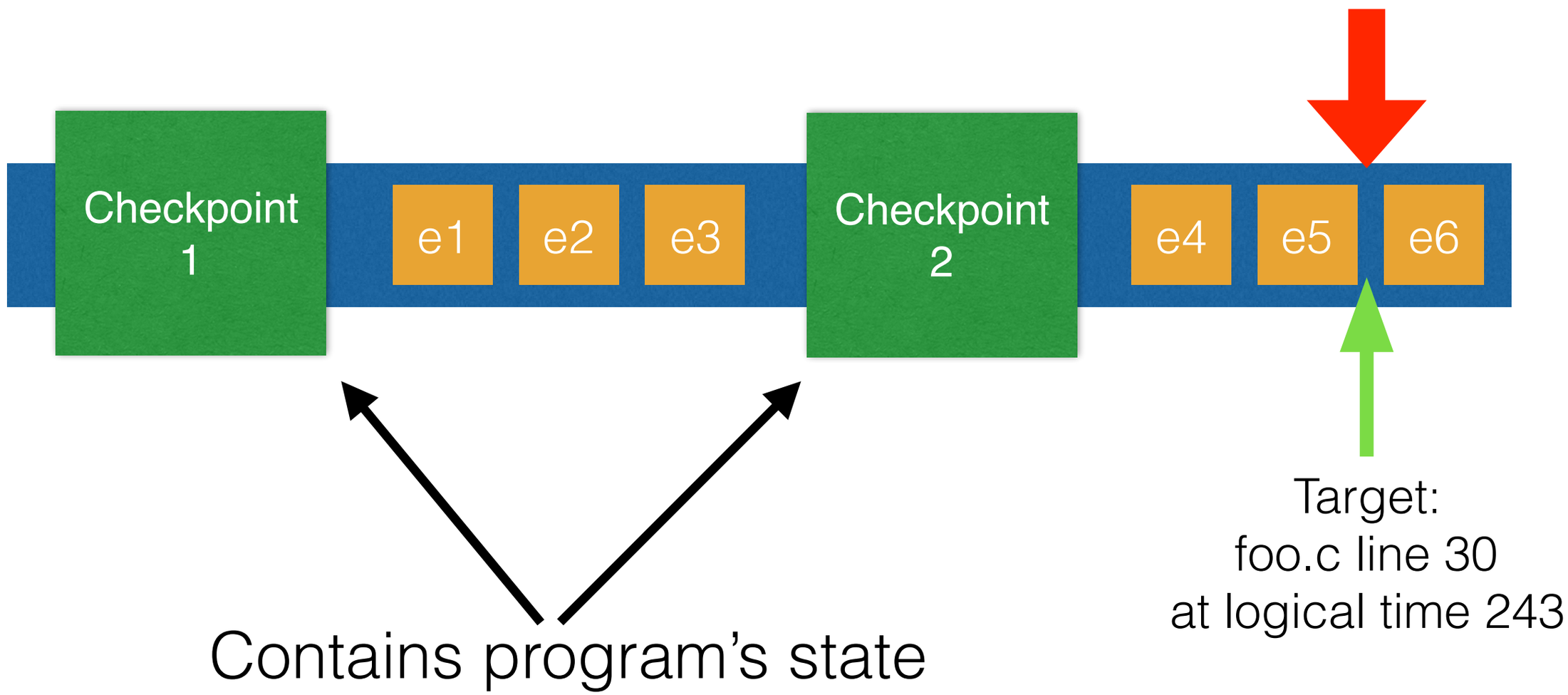
Conventional Time-Traveling Debuggers

Optimization: Checkpoints



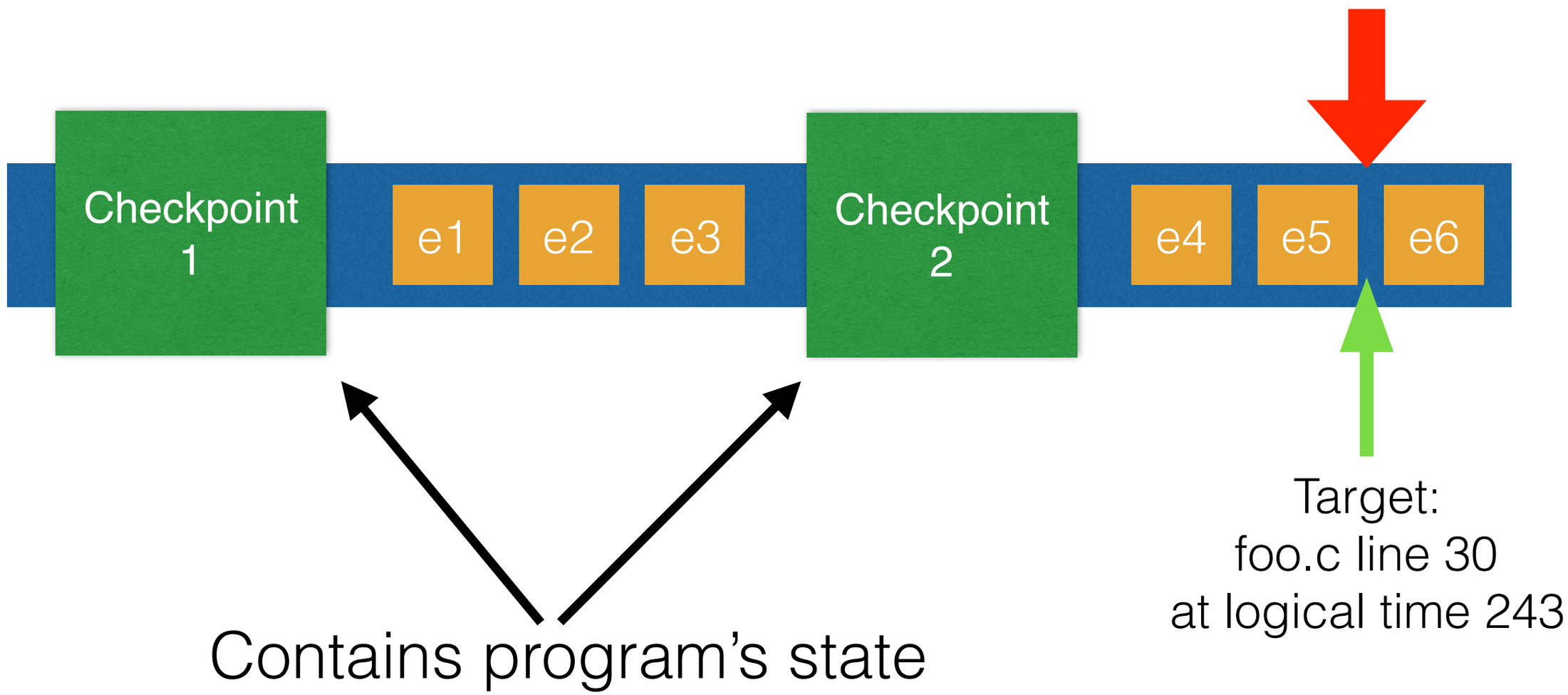
Conventional Time-Traveling Debuggers

Optimization: Checkpoints



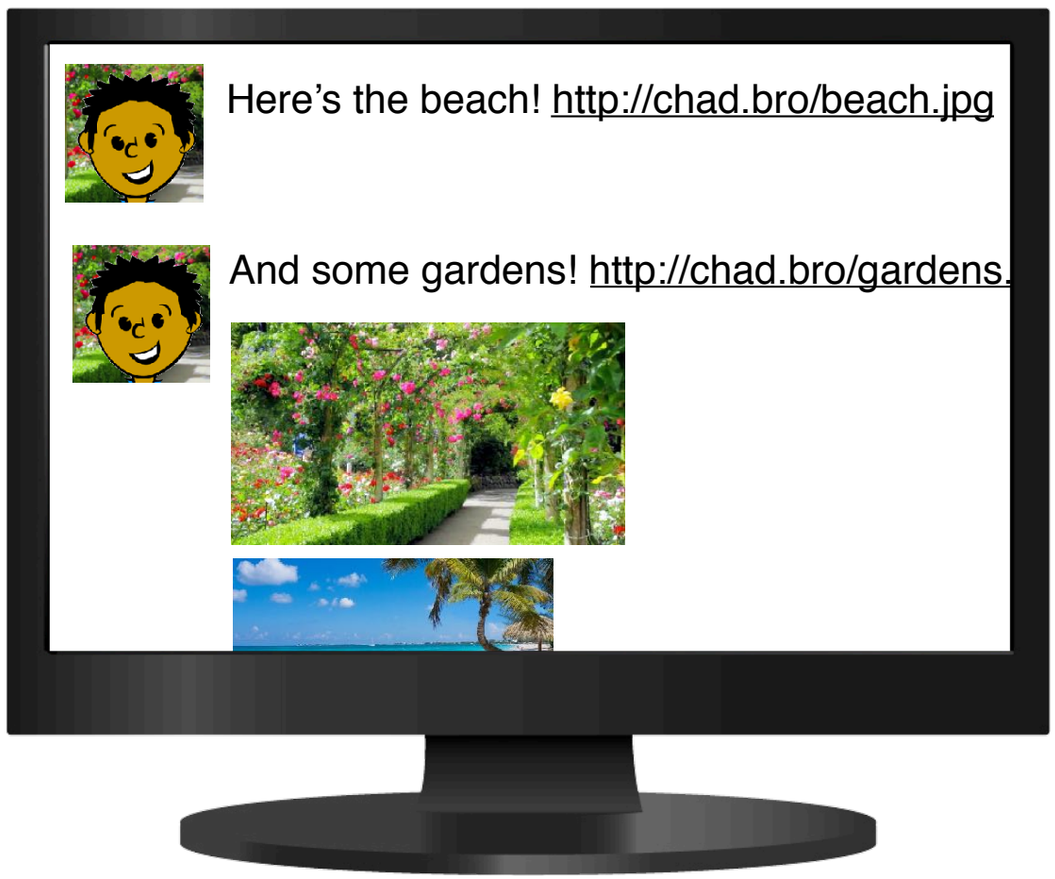
Conventional Time-Traveling Debuggers

Does not support visual state!



Conventional Time-Traveling Debuggers

Does not support visual state!

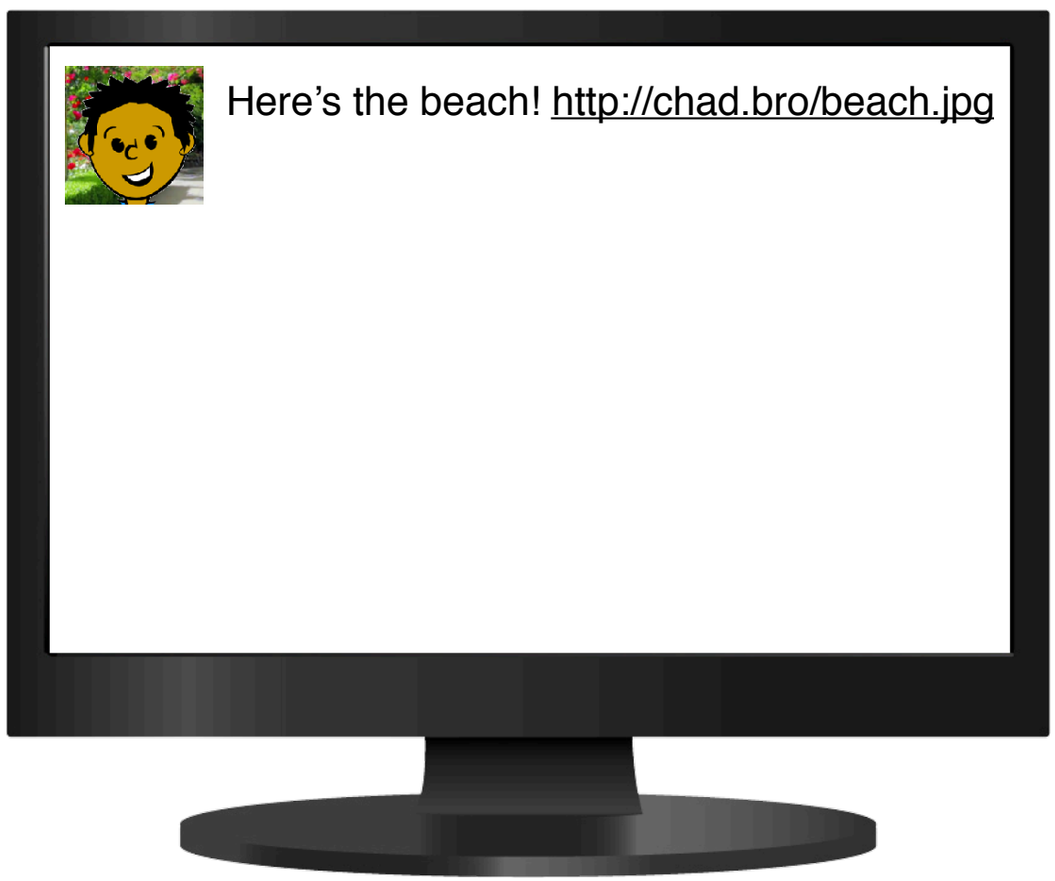


Desired experience while traveling back in time

Actual experience with conventional TTD design

Conventional Time-Traveling Debuggers

Does not support visual state!

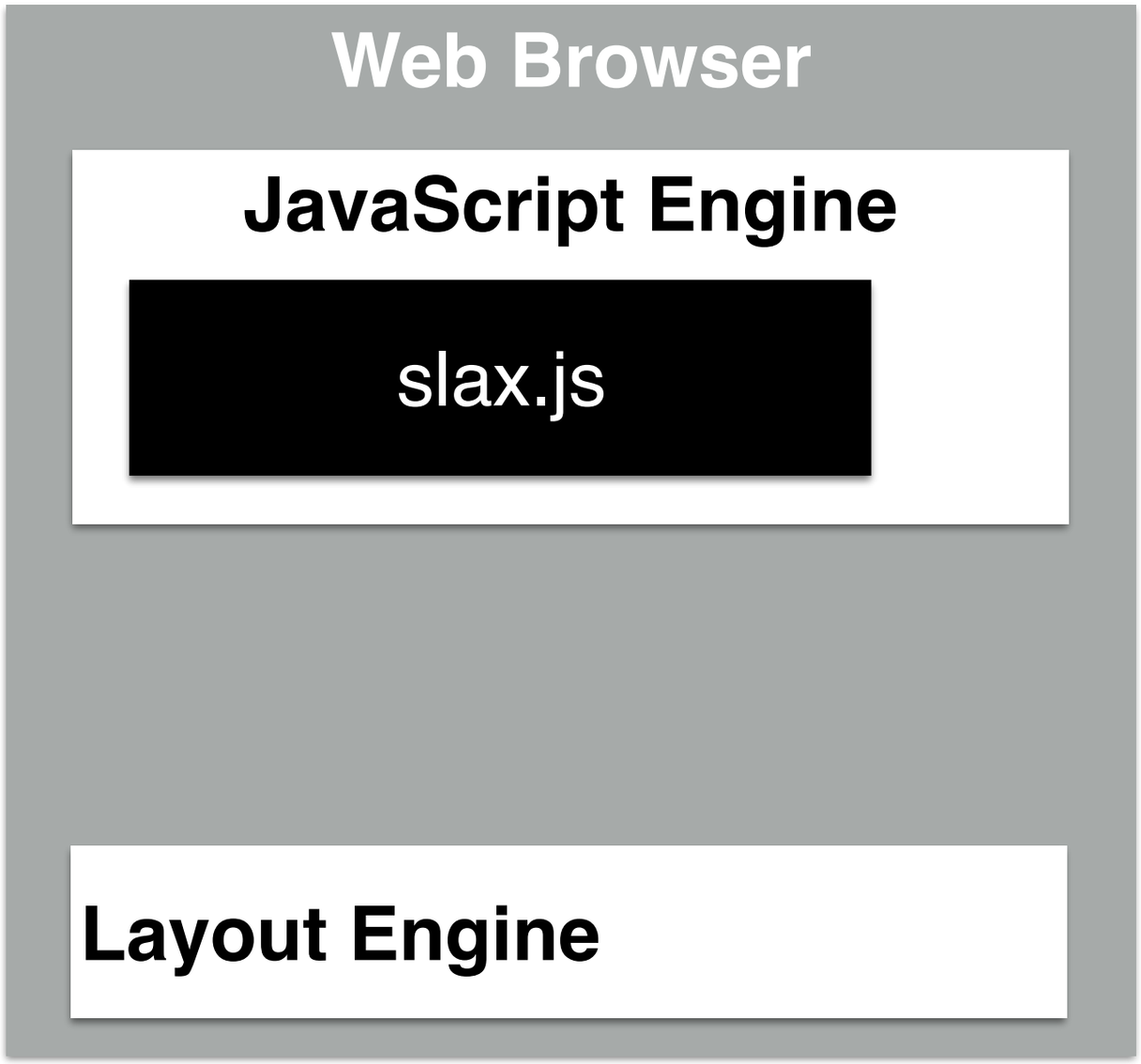


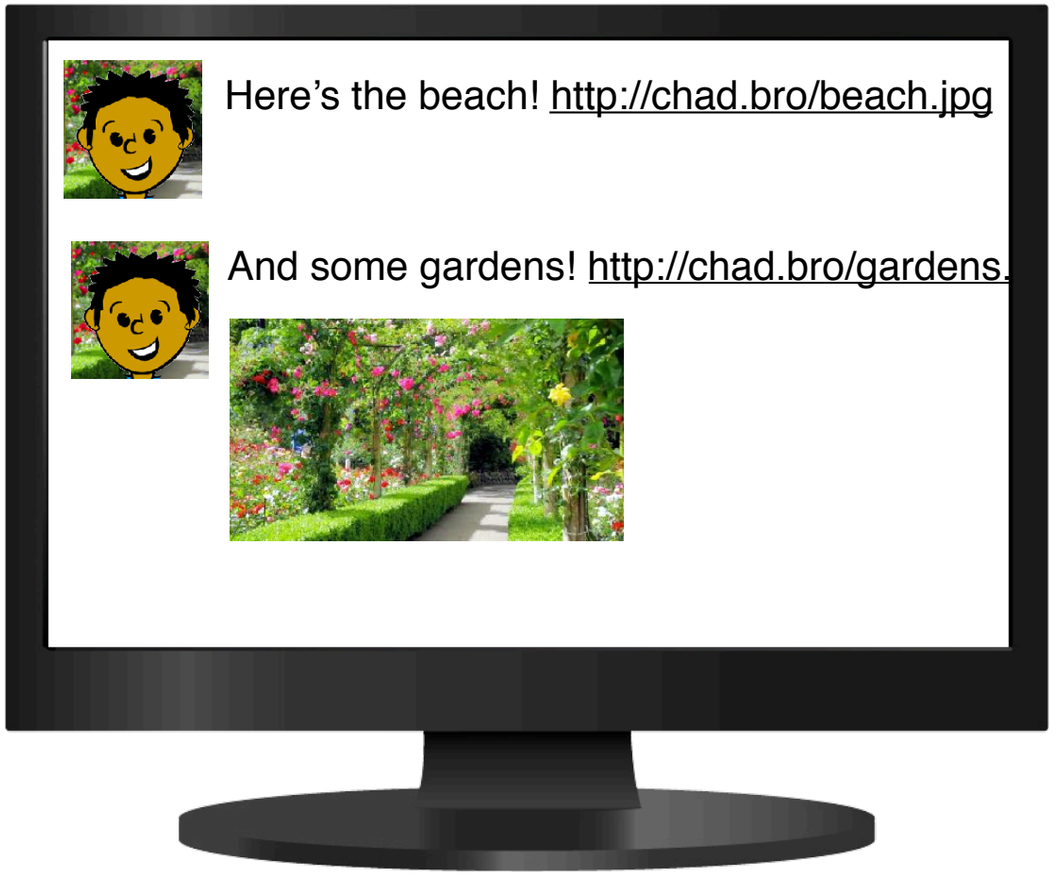
Desired experience
while traveling back in time

Actual experience with
conventional TTD design

Time-Travel Visual State?

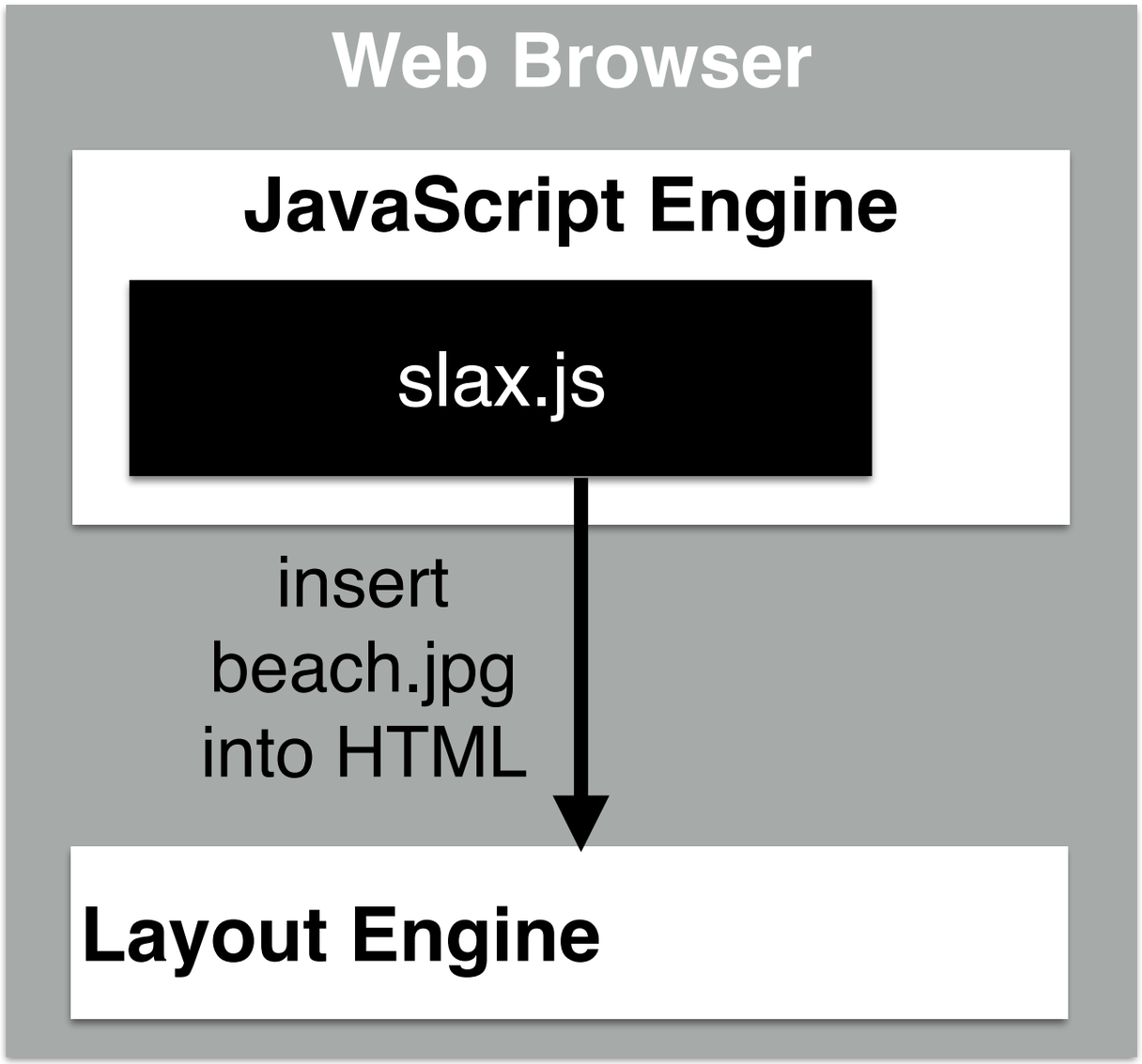
Challenge: All I/O managed by layout engine!

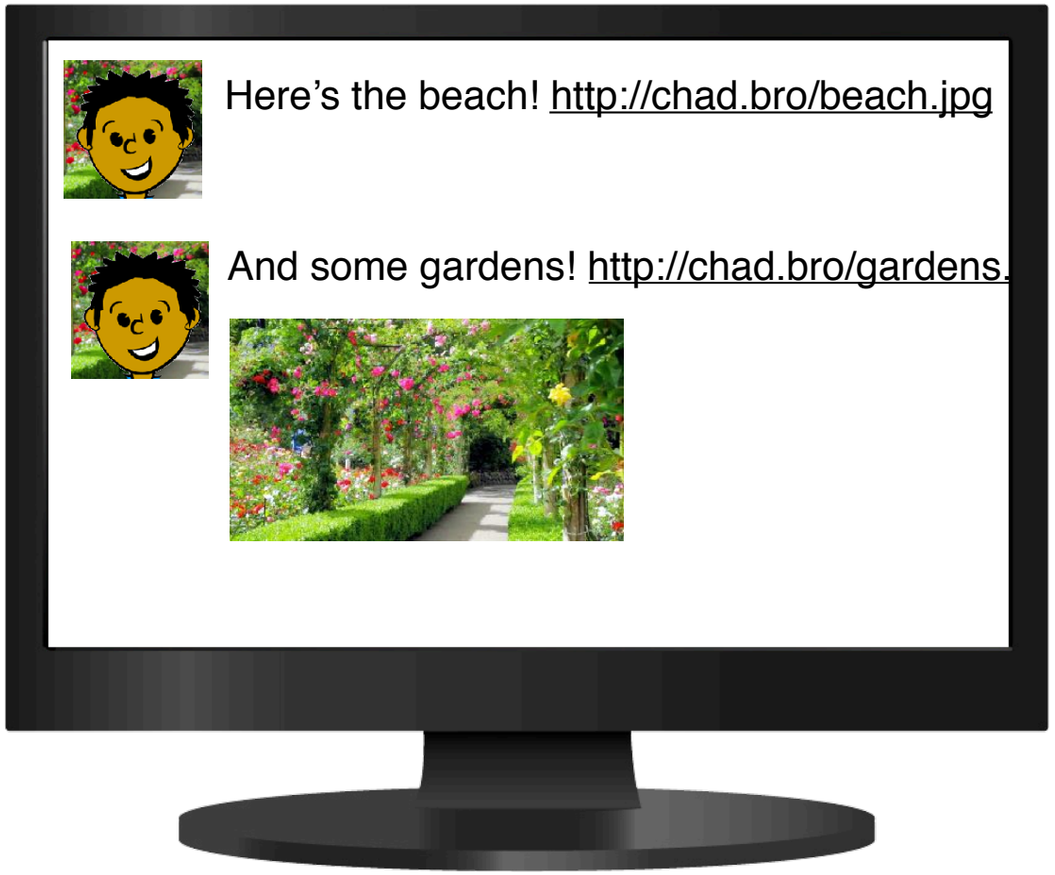




Time-Travel Visual State?

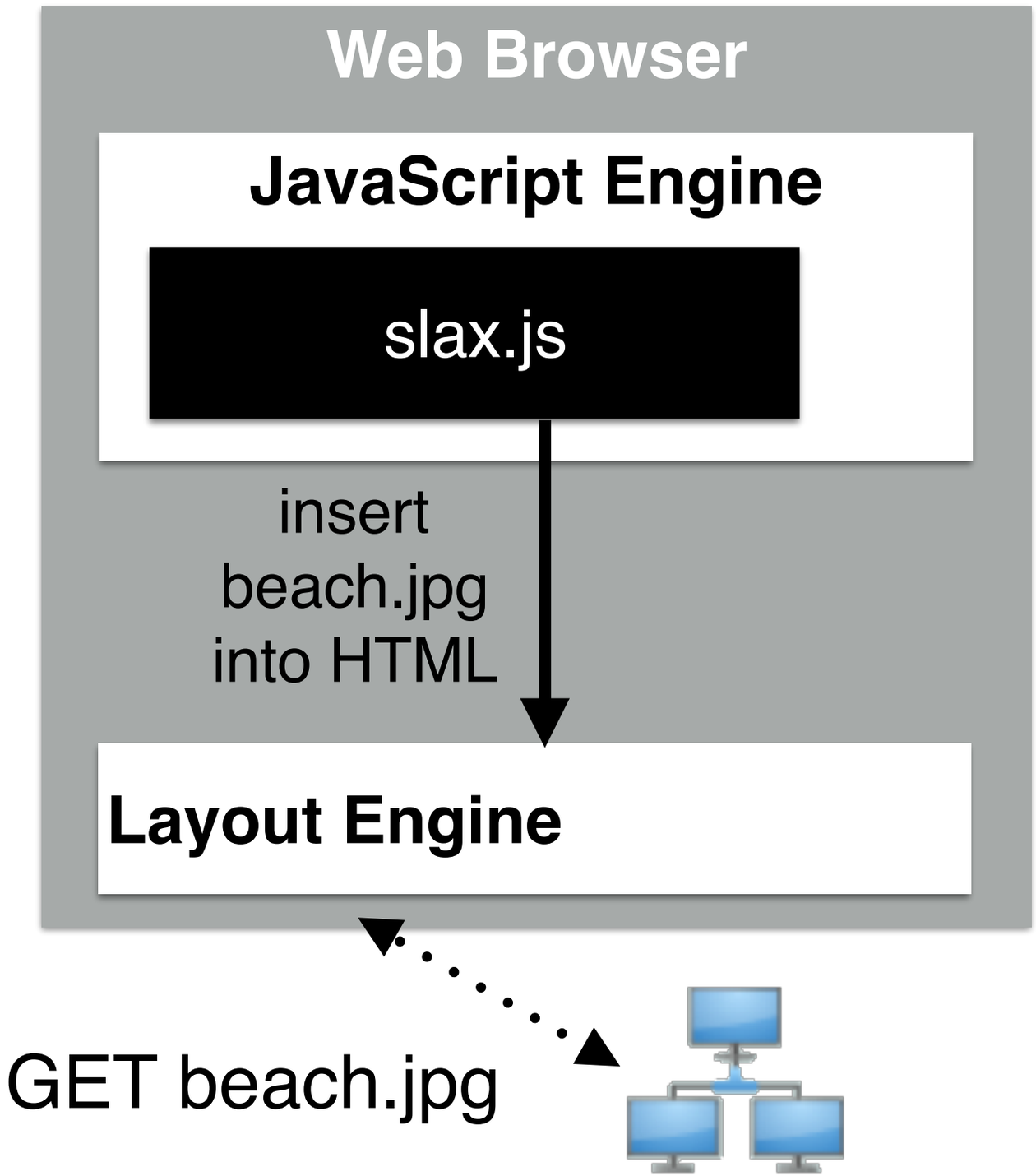
Challenge: All I/O managed by layout engine!





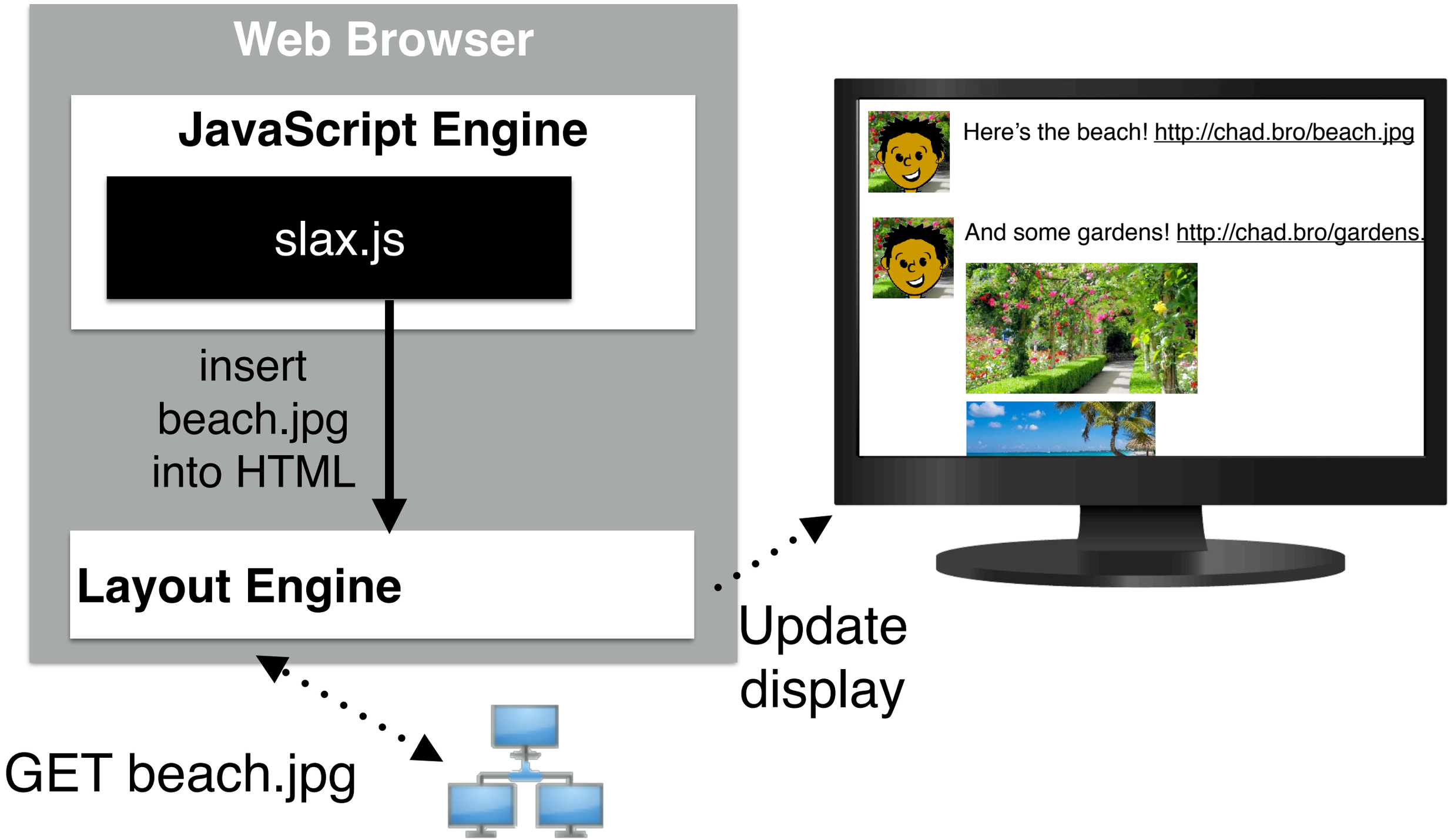
Time-Travel Visual State?

Challenge: All I/O managed by layout engine!



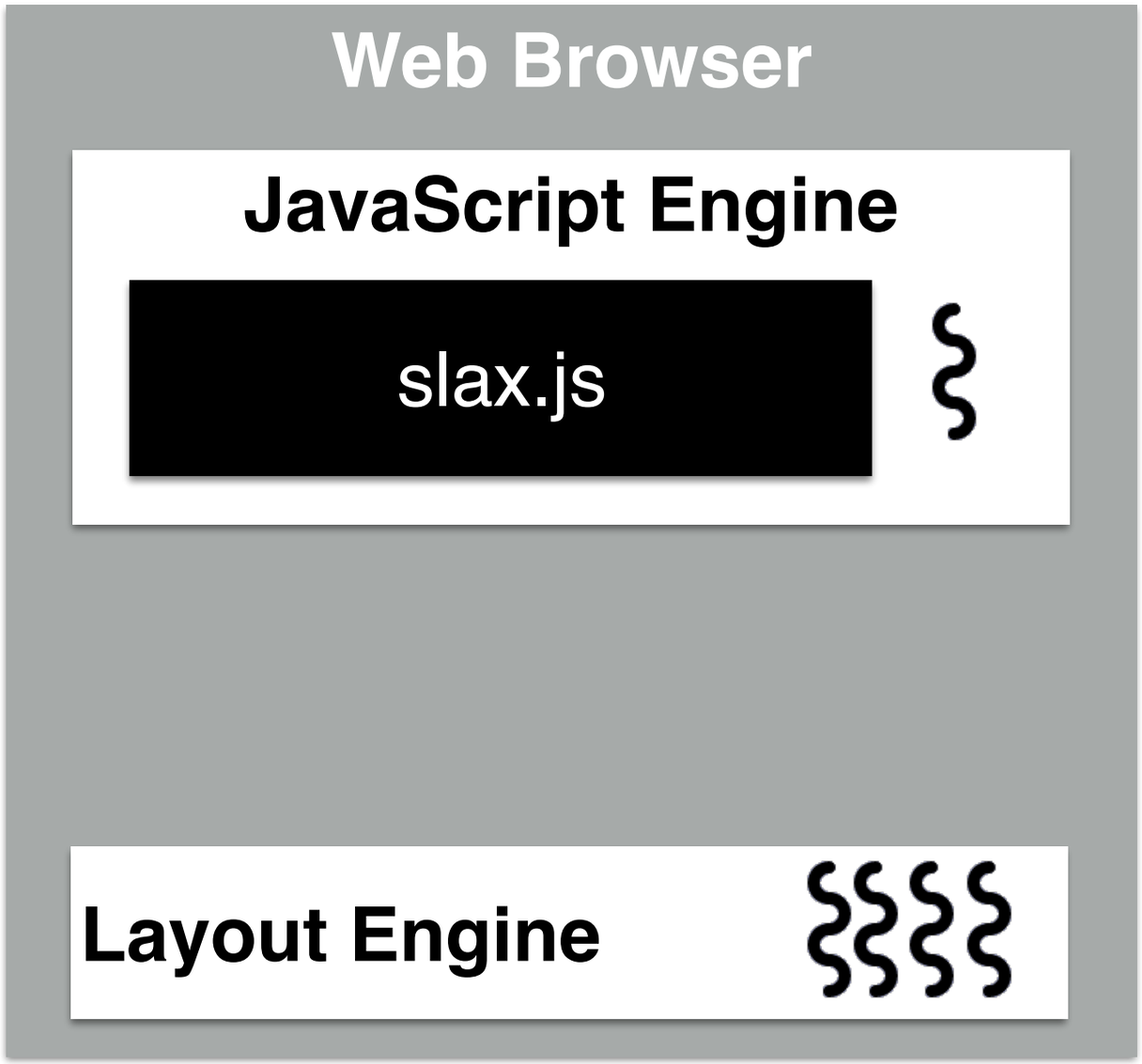
Time-Travel Visual State?

Challenge: All I/O managed by layout engine!



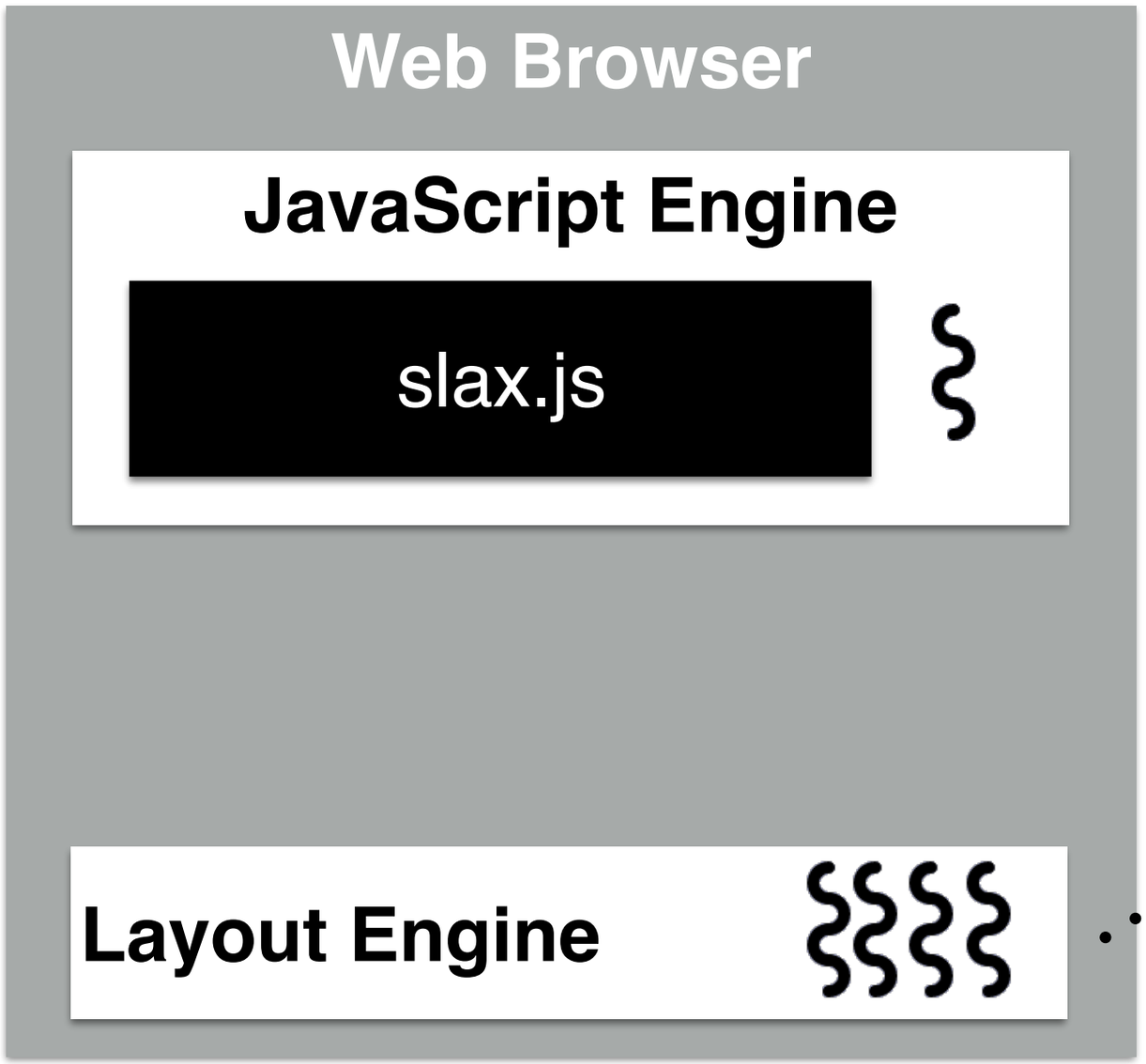
Time-Travel Visual State?

Challenge: Concurrency!



Time-Travel Visual State?

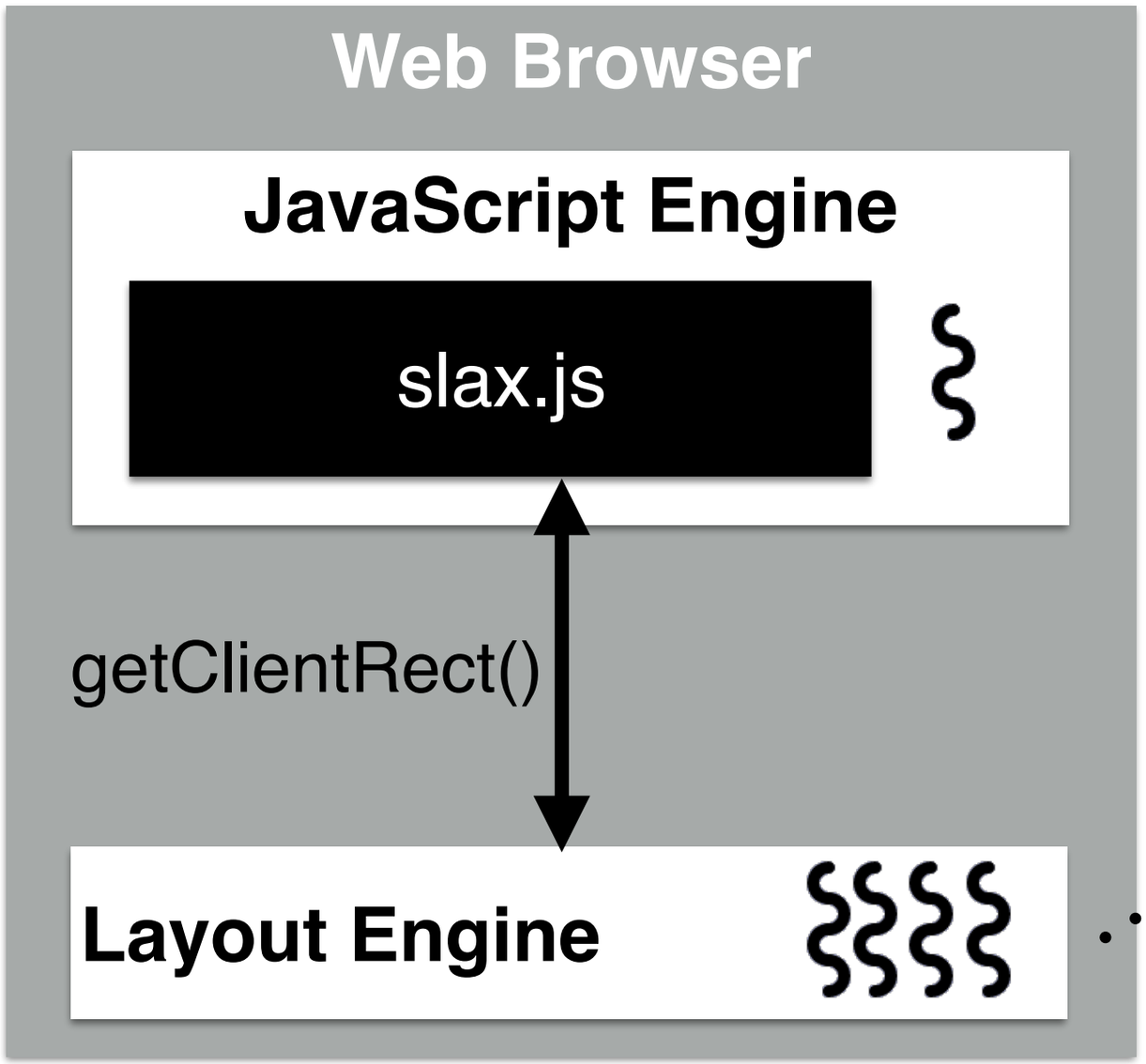
Challenge: Concurrency!



Update animation

Time-Travel Visual State?

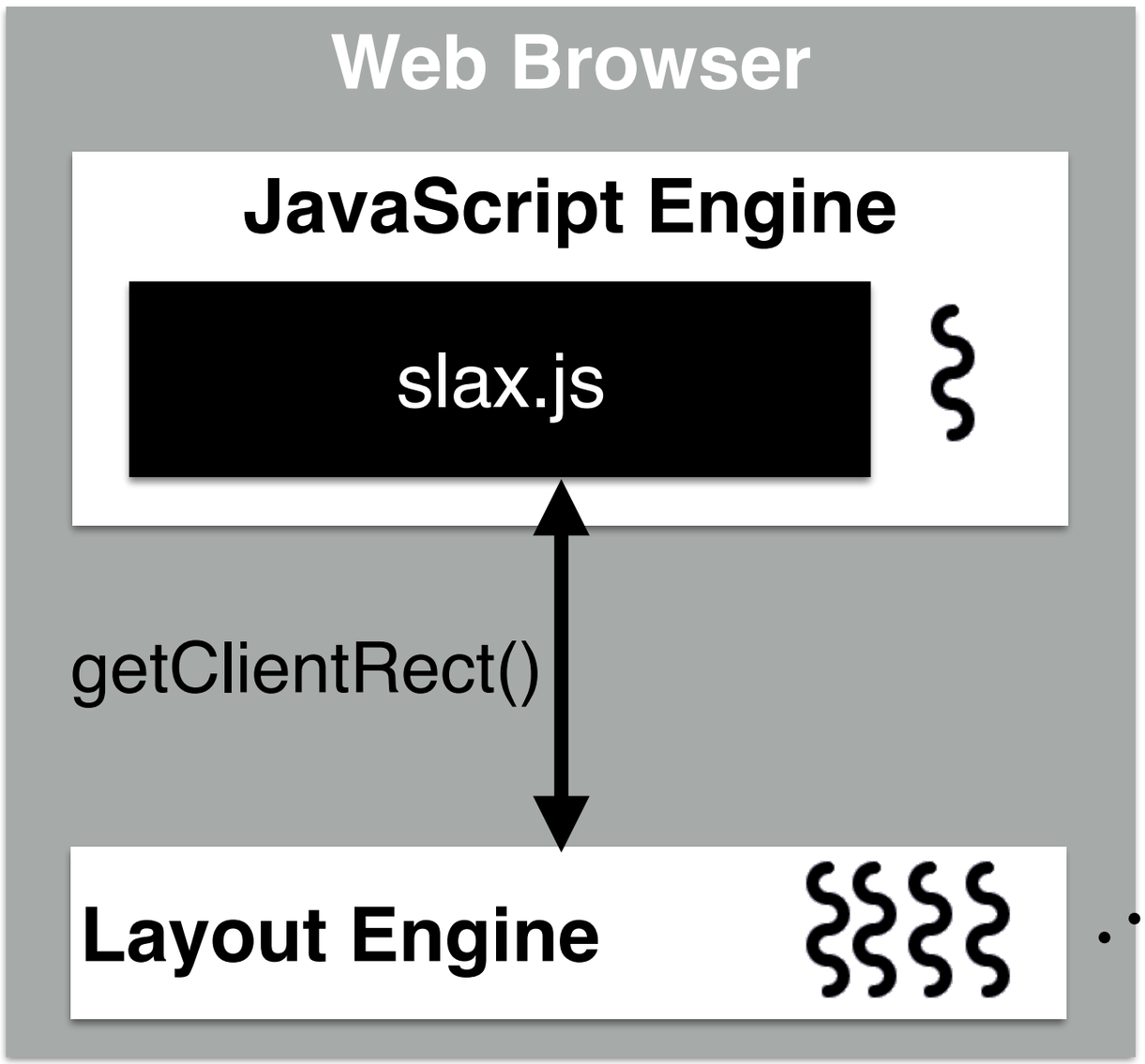
Challenge: Concurrency!



Update animation

Time-Travel Visual State?

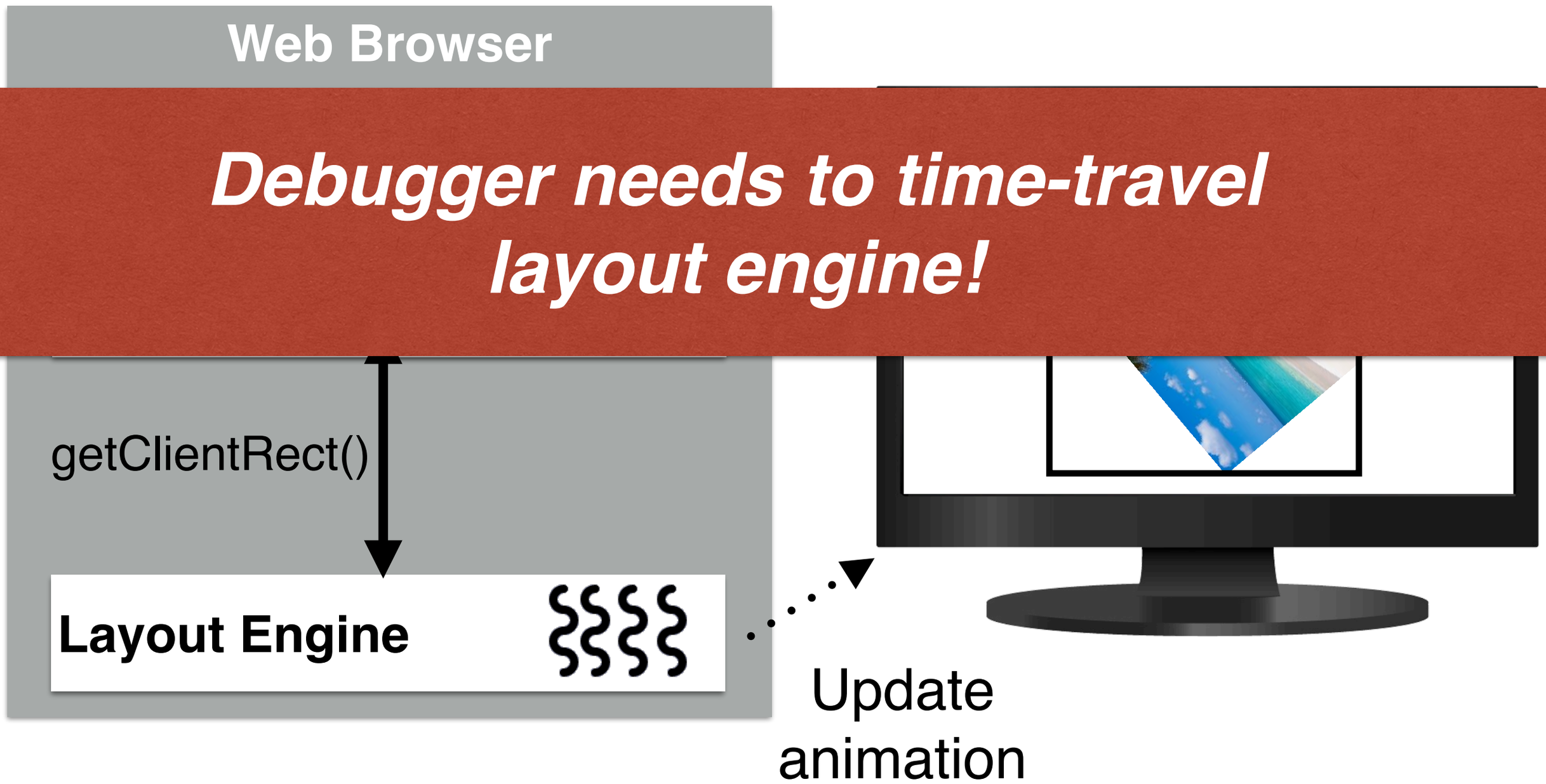
Challenge: Concurrency!



Update animation

Time-Travel Visual State?

Challenge: Concurrency!



Time-Travel Visual State?

Challenge: Layout engine complexity

Layout Engine

Time-Travel Visual State?

Challenge: Layout engine complexity

Layout Engine

- All visual state stored in C++ objects

Time-Travel Visual State?

Challenge: Layout engine complexity

Layout Engine

- All visual state stored in C++ objects
- Multithreaded (sometimes multiprocess)

Time-Travel Visual State?

Challenge: Layout engine complexity

Layout Engine

- All visual state stored in C++ objects
- Multithreaded (sometimes multiprocess)
- Complexity and size of an operating system

Time-Travel Visual State?

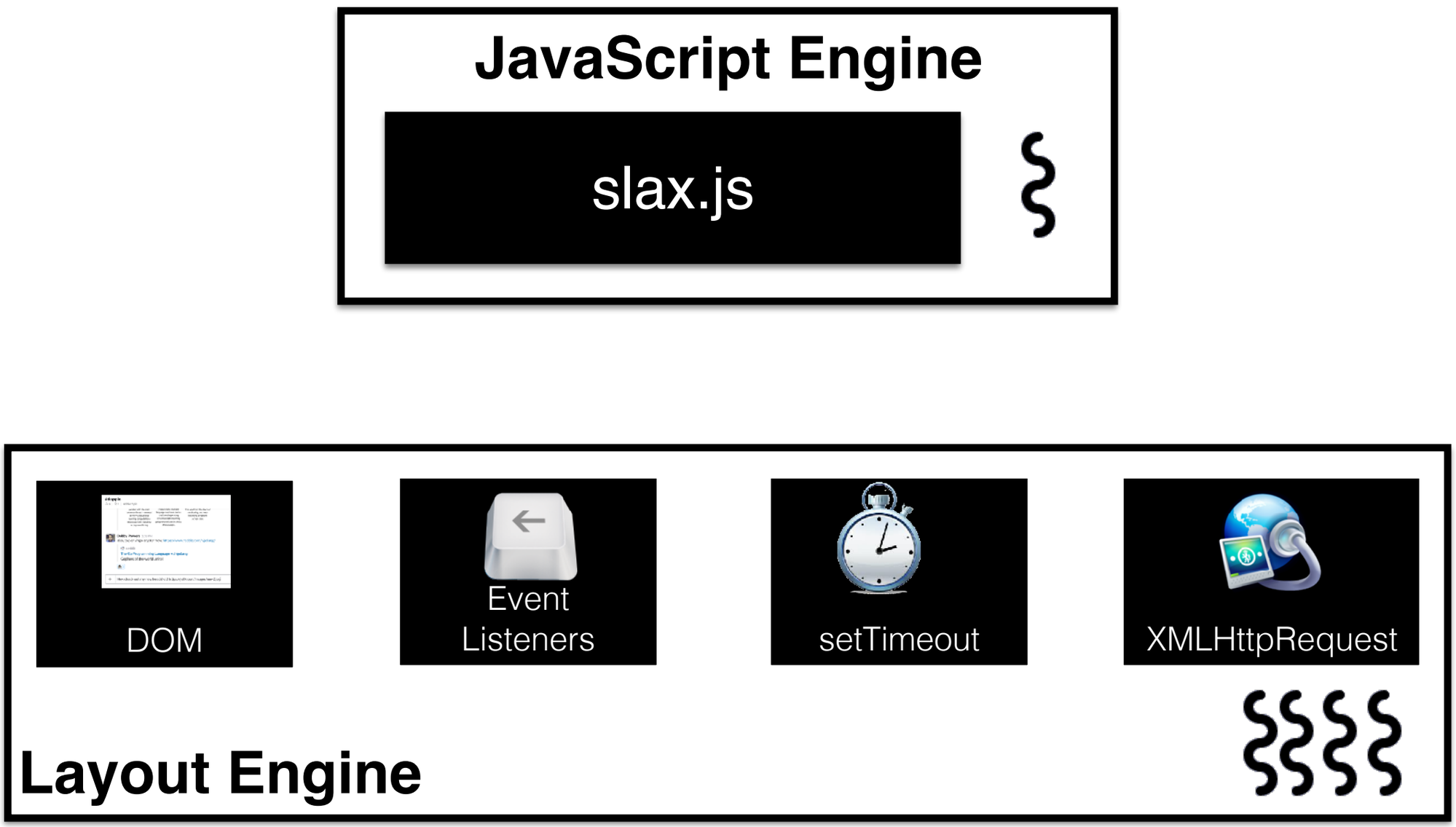
Challenge: Layout engine complexity

Significant modifications are infeasible and not portable

- All visual state stored in C++ objects
- Multithreaded (sometimes multiprocess)
- Complexity and size of an operating system

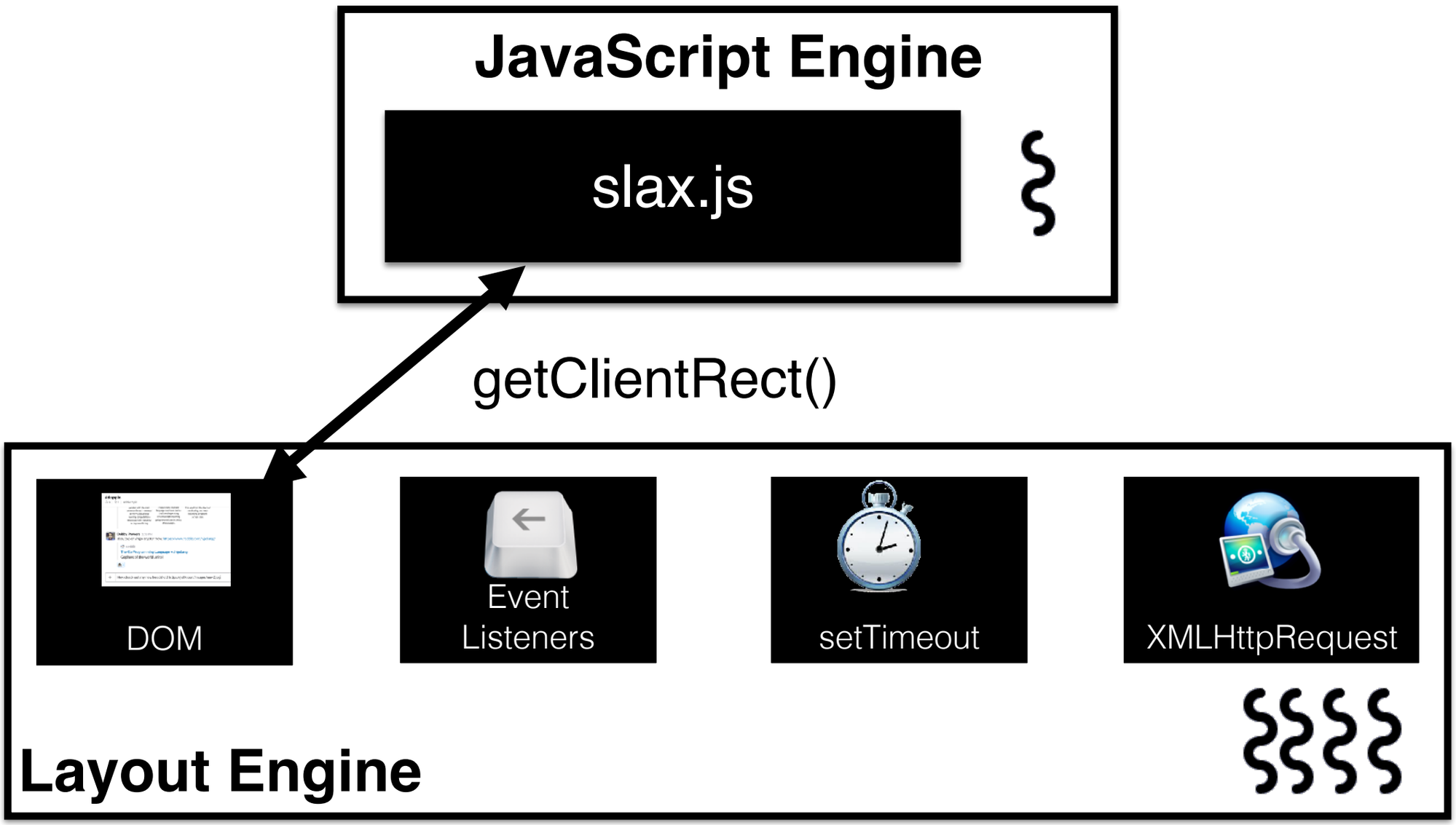
Time-Travel Visual State

Use standardized JavaScript interfaces?



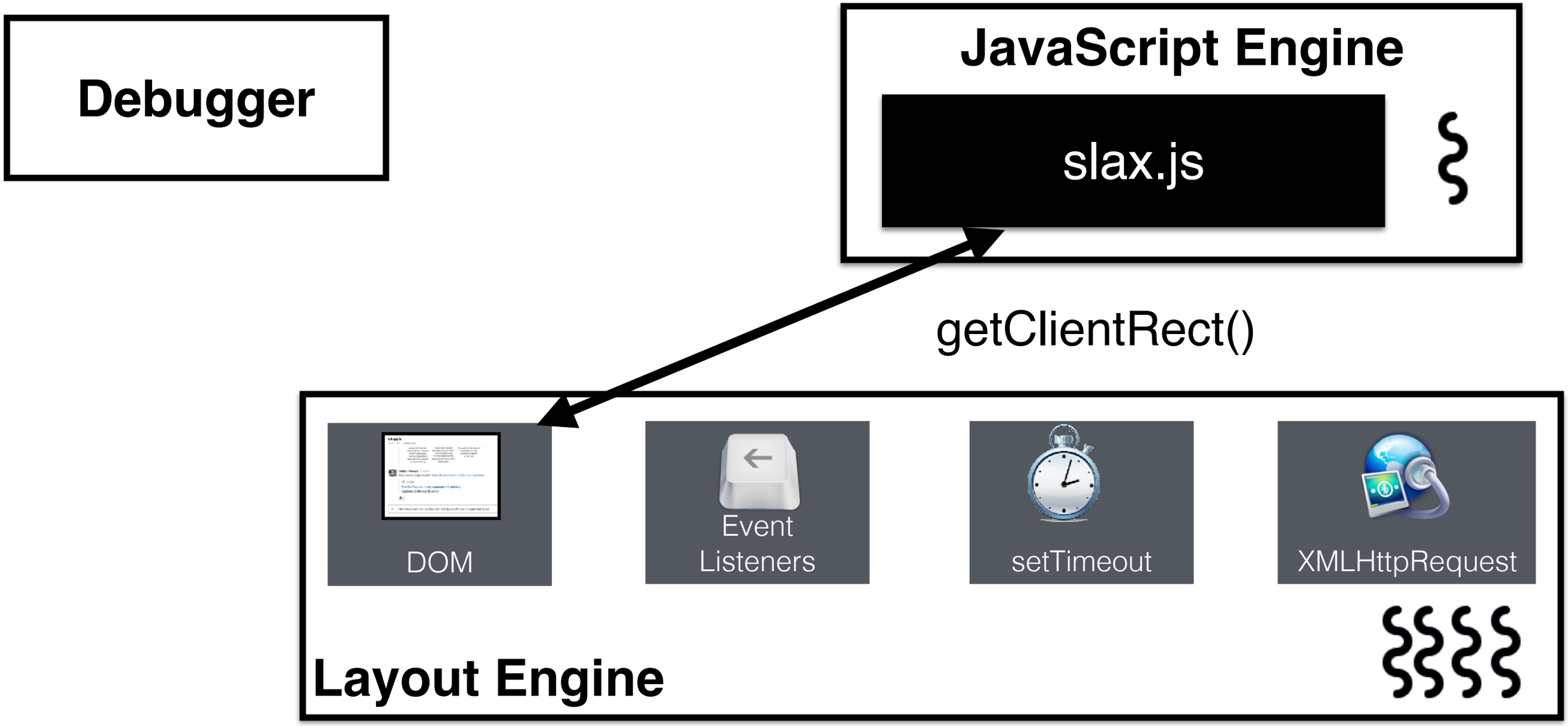
Time-Travel Visual State

Use standardized JavaScript interfaces?



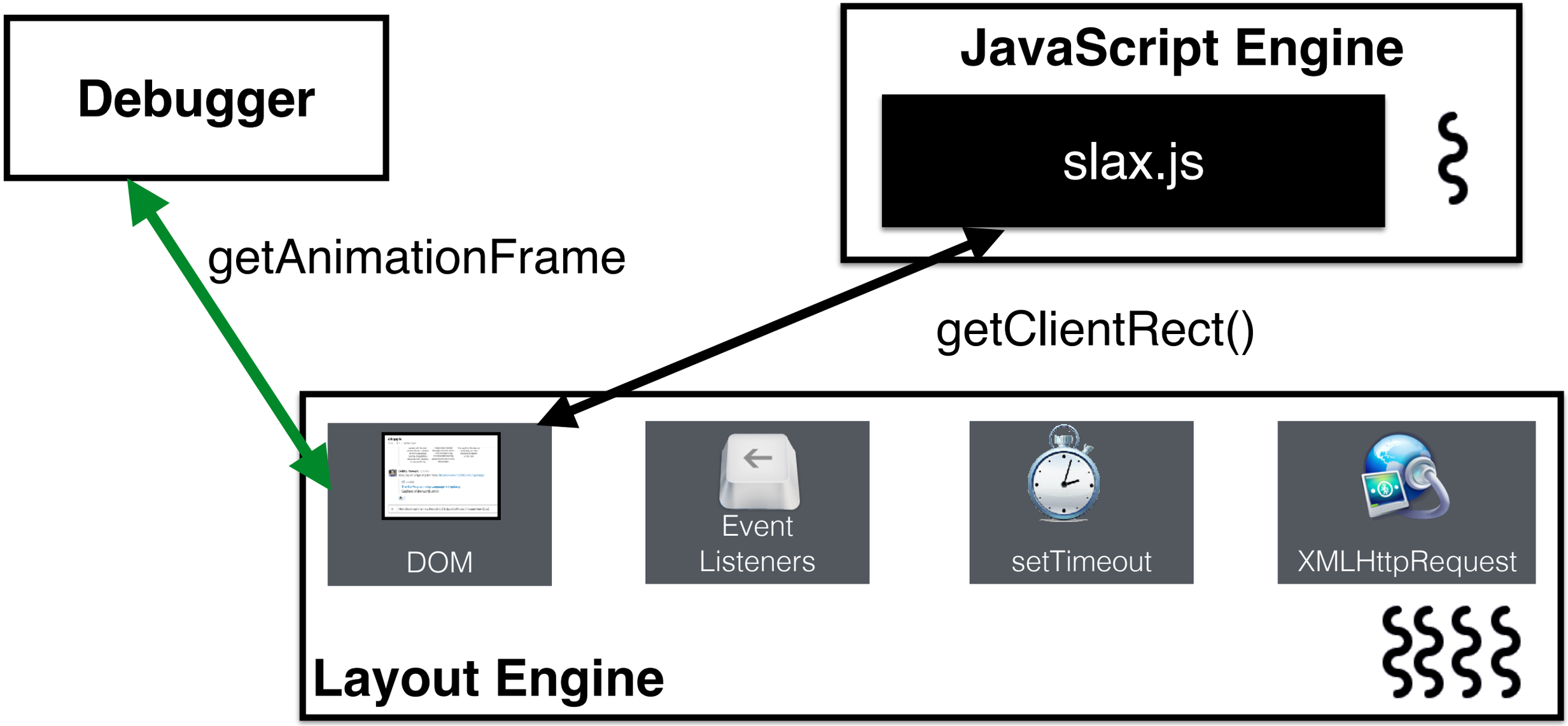
Time-Travel Visual State

Extend standard interfaces to expose hidden state



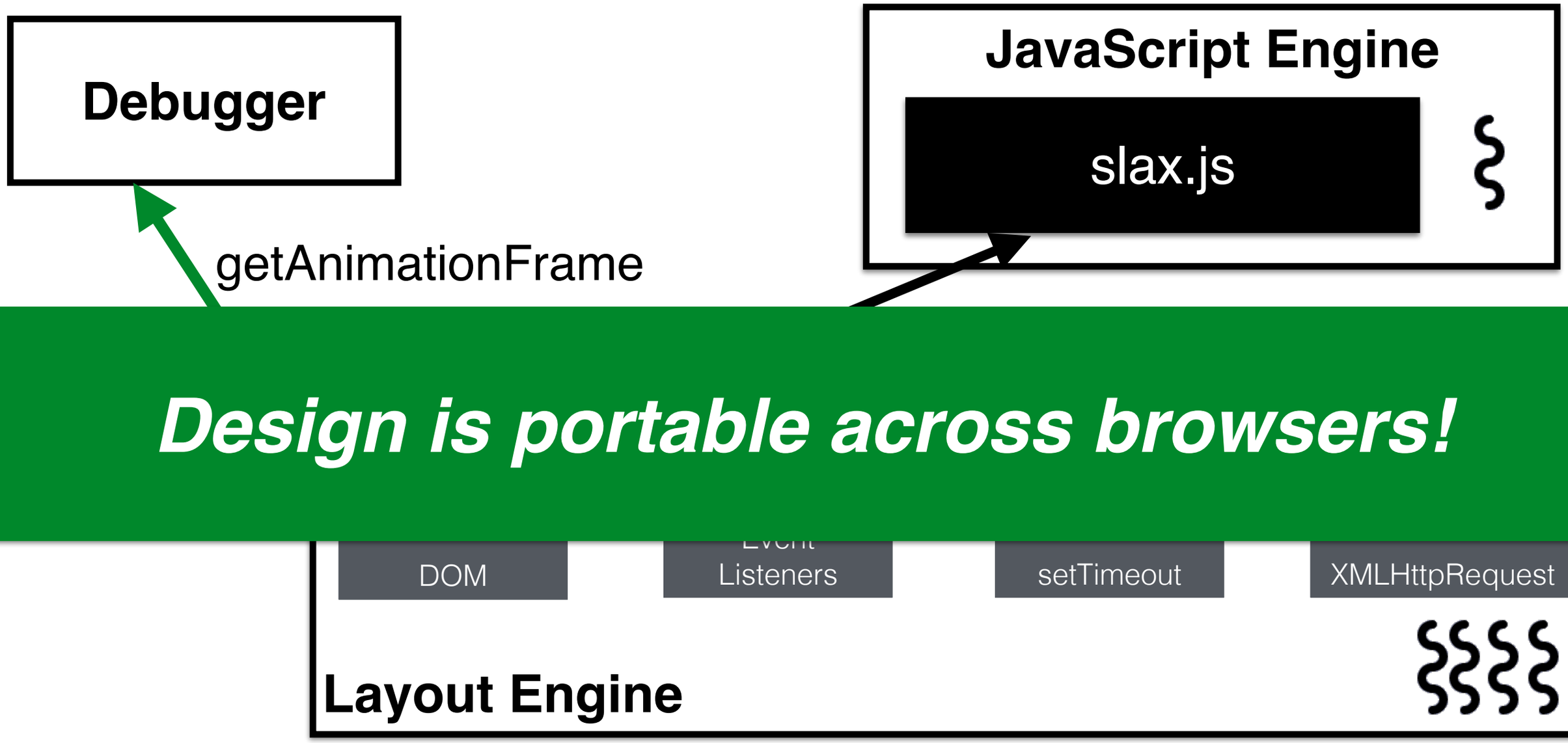
Time-Travel Visual State

Extend standard interfaces to expose hidden state



Time-Travel Visual State

Extend standard interfaces to expose hidden state



Design is portable across browsers!

McFly

The first time-traveling debugger
for web applications

Microsoft

McFly

The first time-traveling debugger
for web applications

Records, replays, and checkpoints
JavaScript *and* layout engine state

McFly

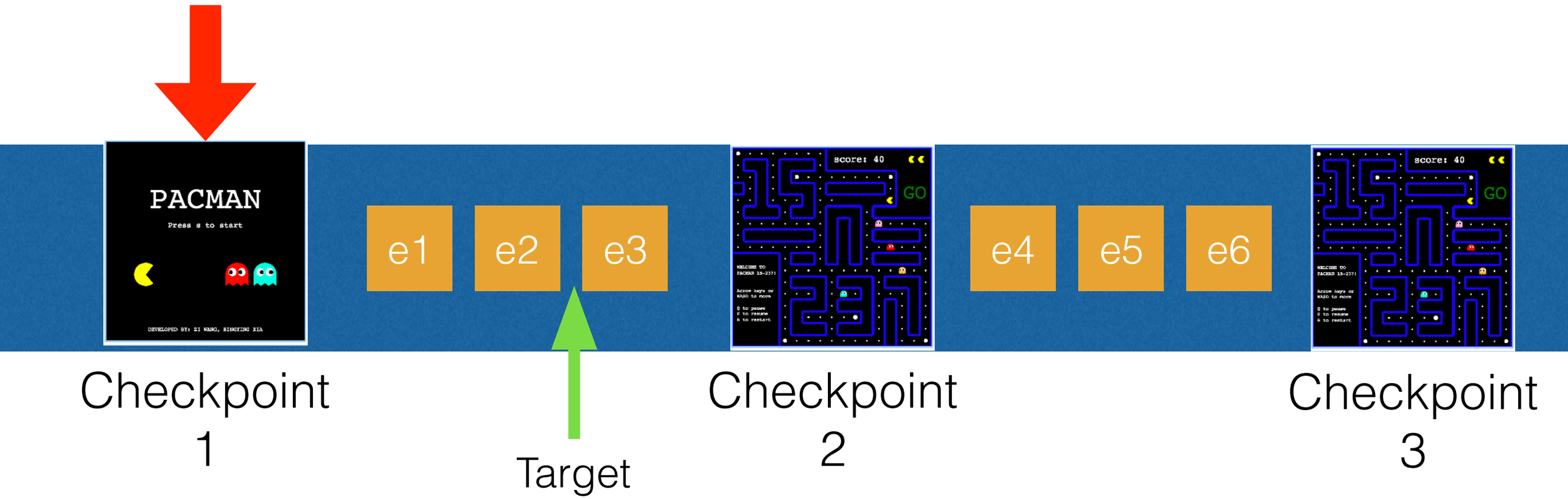
The first time-traveling debugger for web applications

Microsoft

Records, replays, and checkpoints JavaScript *and* layout engine state

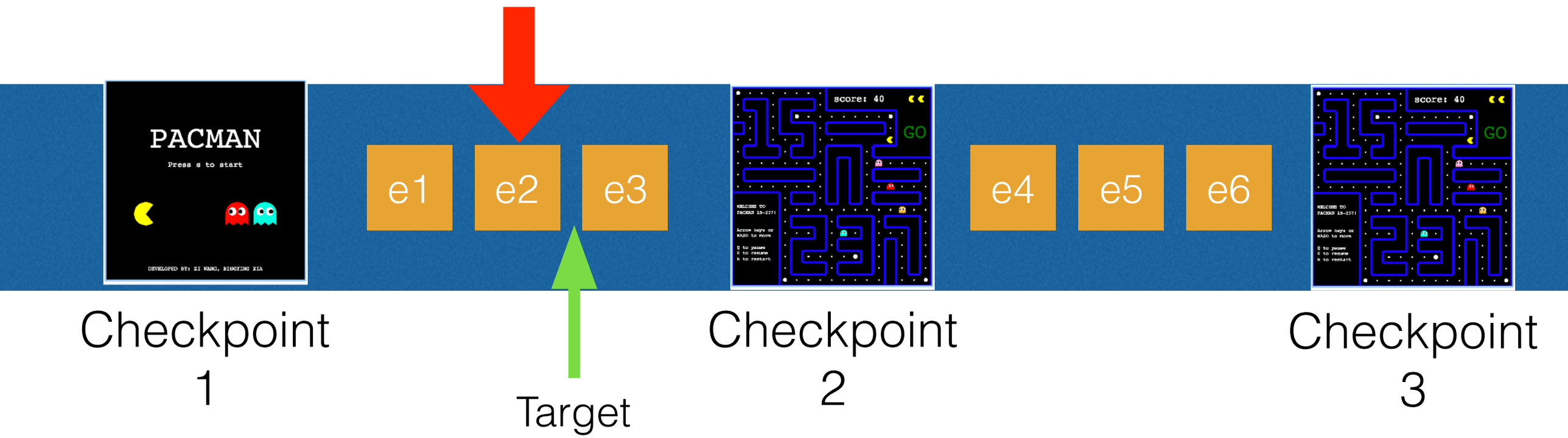
McFly

Step Backward Optimization



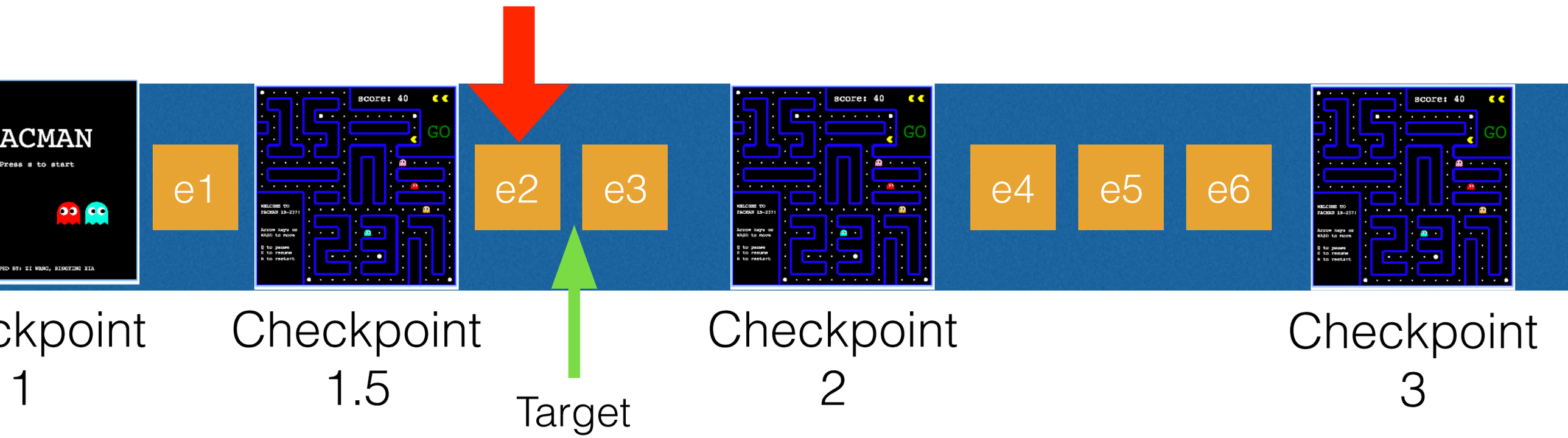
McFly

Step Backward Optimization



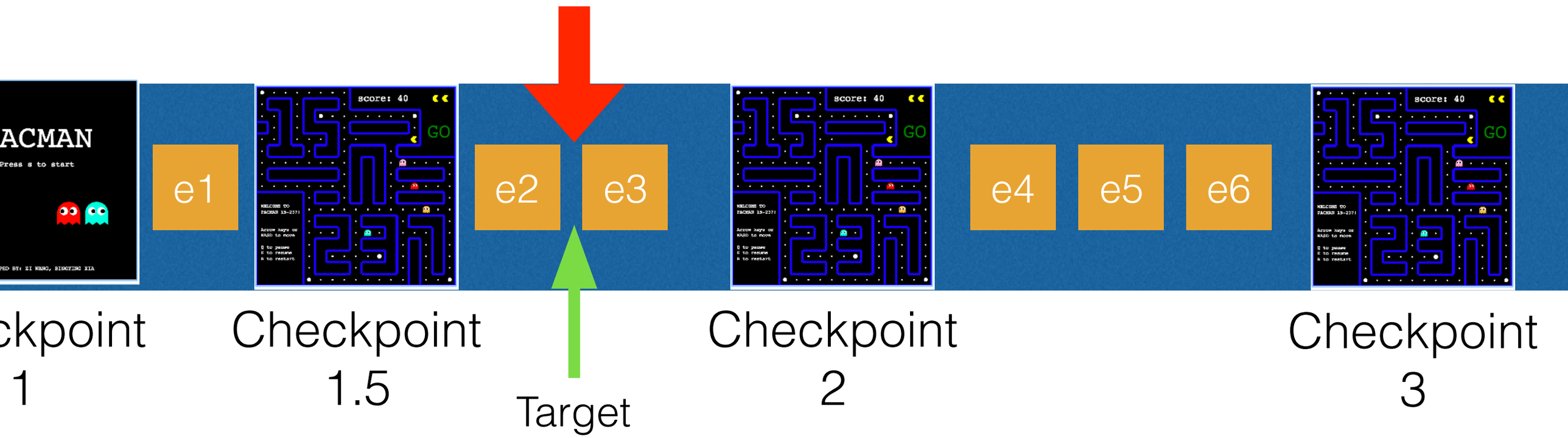
McFly

Step Backward Optimization



McFly

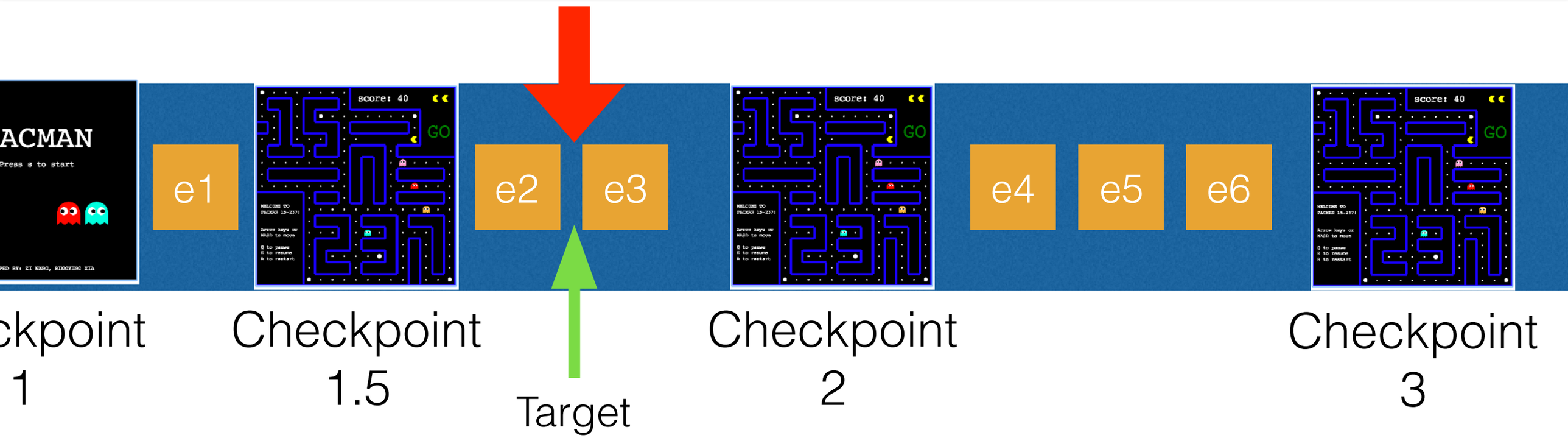
Step Backward Optimization



McFly

Step Backward Optimization

One-time setup cost!



McFly

Step Backward Optimization

One-time setup cost!

ckpoint 1

Che

Target

eckpoint 2

Checkpoint 3

More details in Chapter 3 of dissertation

Evaluation

Benchmarks

Deterministic

Google

Octane

Delta-Blue
Earley-Boyer
RayTrace
Splay

Nondeterministic

Stroop Color Game

CRUD

jQuery

Pac Man

Octane RayTrace w/ GUI

Evaluation

Step Backward Performance

Evaluation

Step Backward Performance

- **Common case**: Takes average of 0.36s to resume from checkpoint (dominates common case of stepping backward)

Evaluation

Step Backward Performance

- **Common case**: Takes average of 0.36s to resume from checkpoint (dominates common case of stepping backward)
- **Startup**: Takes average of 3.8s to take first step backward (w/ checkpoints every 2 seconds)

Evaluation

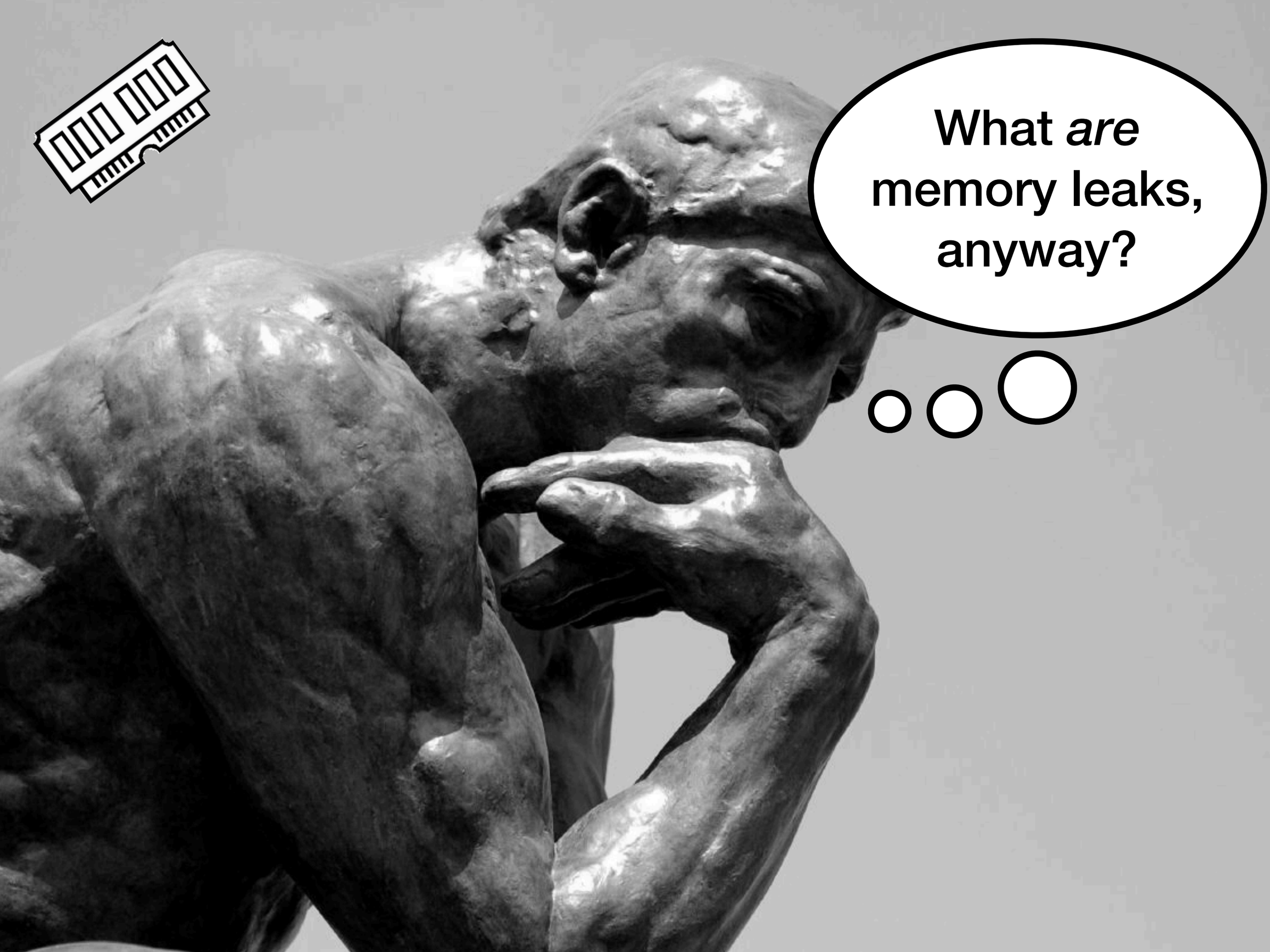
Step Backward Performance

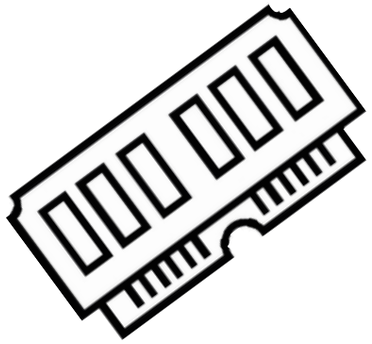
- **Common case**: Takes average of 0.36s to resume from checkpoint (dominates common case of stepping backward)
- **Startup**: Takes average of 3.8s to take first step backward (w/ checkpoints every 2 seconds)
- **Runtime overhead:** 4% overhead on average (w/ checkpoints every 2 seconds)

slax
sl

You fixed image messages already?? What's your secret?
sl

Long sessions become slow!!!


What *are* memory leaks, anyway?



Manual Memory Management

(in C/C++)

Manual Memory Management

(in C/C++)

`malloc()` →

Manual Memory Management

(in C/C++)

`malloc()` →

→ **`free()`**

Manual Memory Management

(in C/C++)

`malloc()` →

→ **`free()`**

Manual Memory Management

(in C/C++)

`malloc()` →

→ **`free()`**

(worthless ~~cash~~ cache)

Manual Memory Management

(in C/C++)

`malloc()` →

→ **`free()`**

→ **`free()`**

(worthless ~~cash~~ cache)

Manual Memory Management

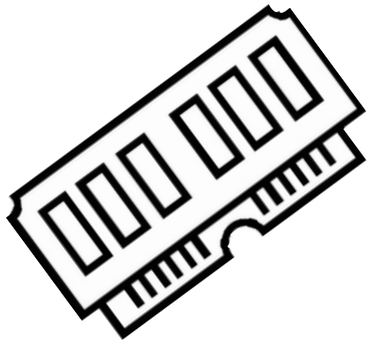
(in C/C++)

`malloc()` →

→ **`free()`**

→ **`free()`**

(worthless ~~cash~~ cache)



Manual Memory Management

(in C/C++)

`malloc()` →

→ **`free()`**

→ **`free()`**

(worthless ~~cash~~ cache)

Manual Memory Management

(in C/C++)

`malloc()` →

→ `free()`

→ `free()`

(worthless ~~cash~~ cache)

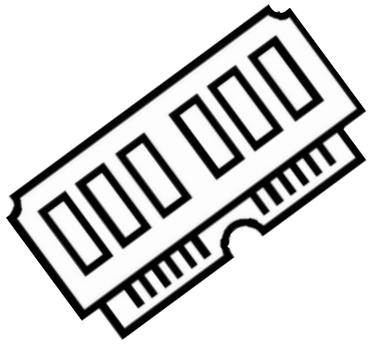
Manual Memory Management

(in C/C++)

(Or: Illness [illegible] che)

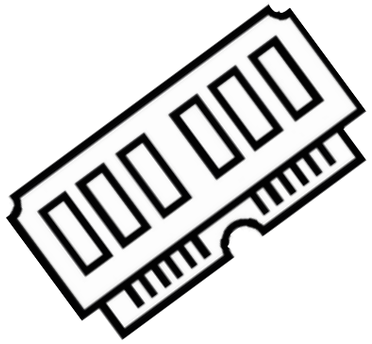
Manual Memory Management

Manual Memory Management



Automatic Memory Management

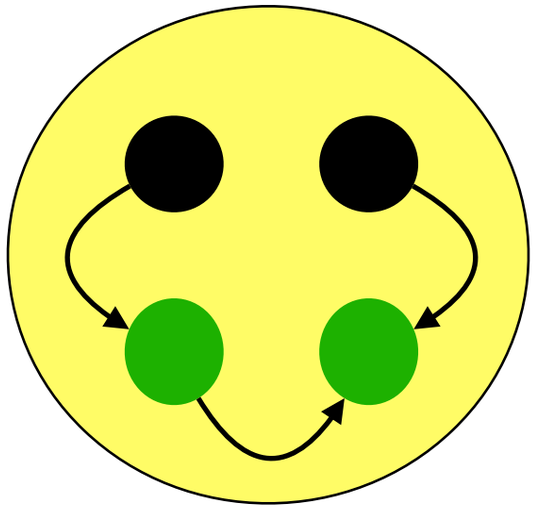
(Garbage Collection)



Automatic Memory Management

(Garbage Collection)

Reachable

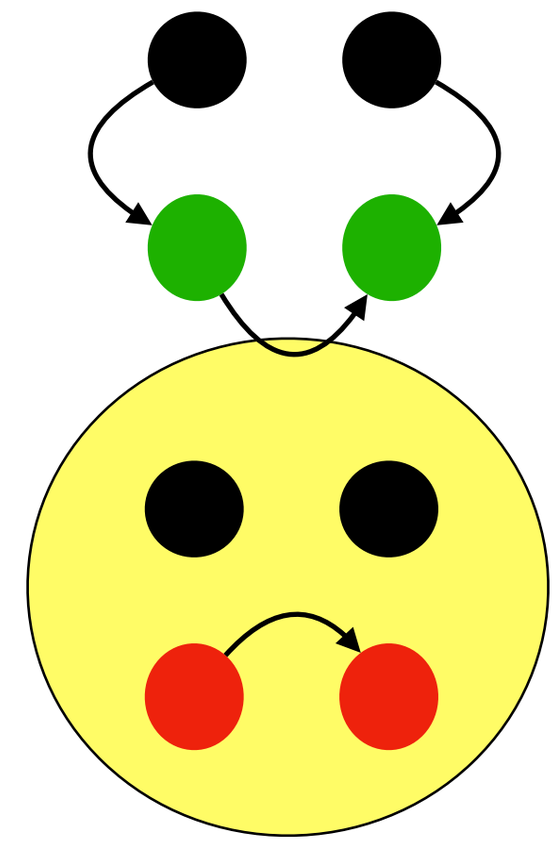


Automatic Memory Management

(Garbage Collection)

Reachable

Unreachable

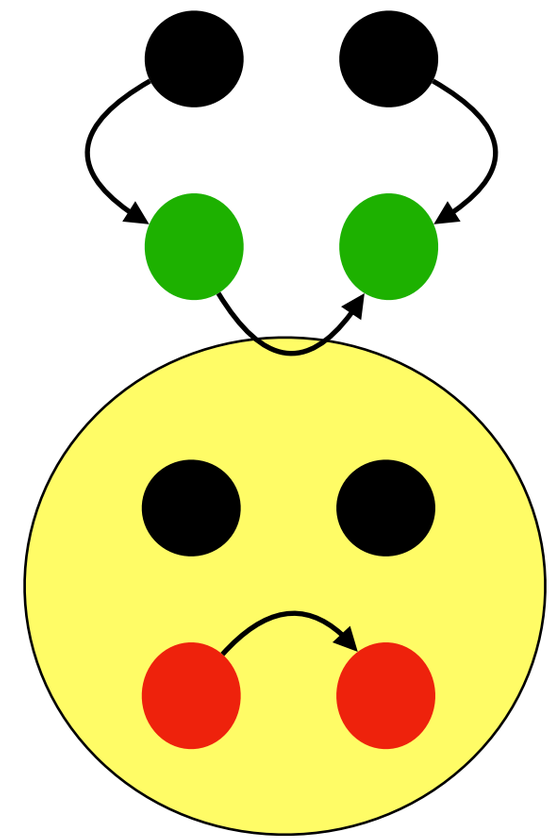


Automatic Memory Management

(Garbage Collection)

Reachable

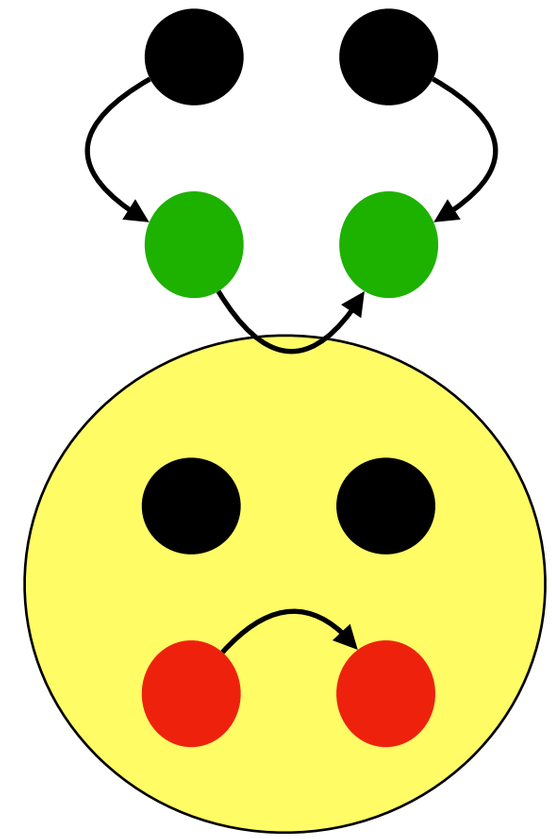
Unreachable



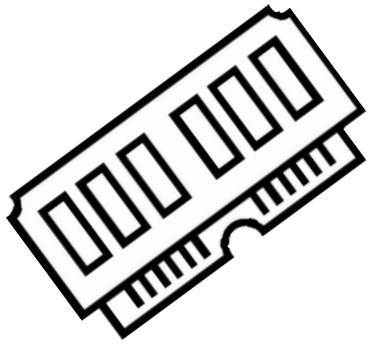
Automatic Memory Management

(Garbage Collection)

Reachable



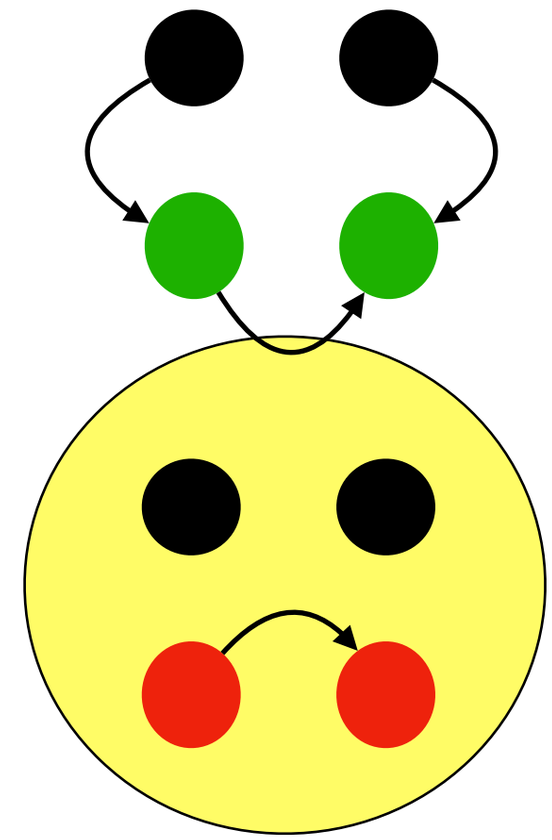
Unreachable



Automatic Memory Management

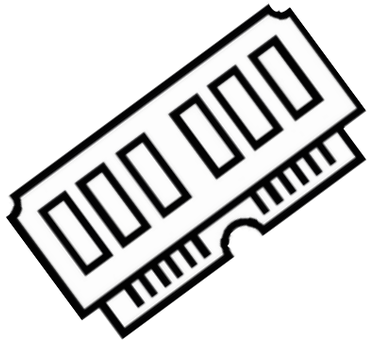
(Garbage Collection)

Reachable

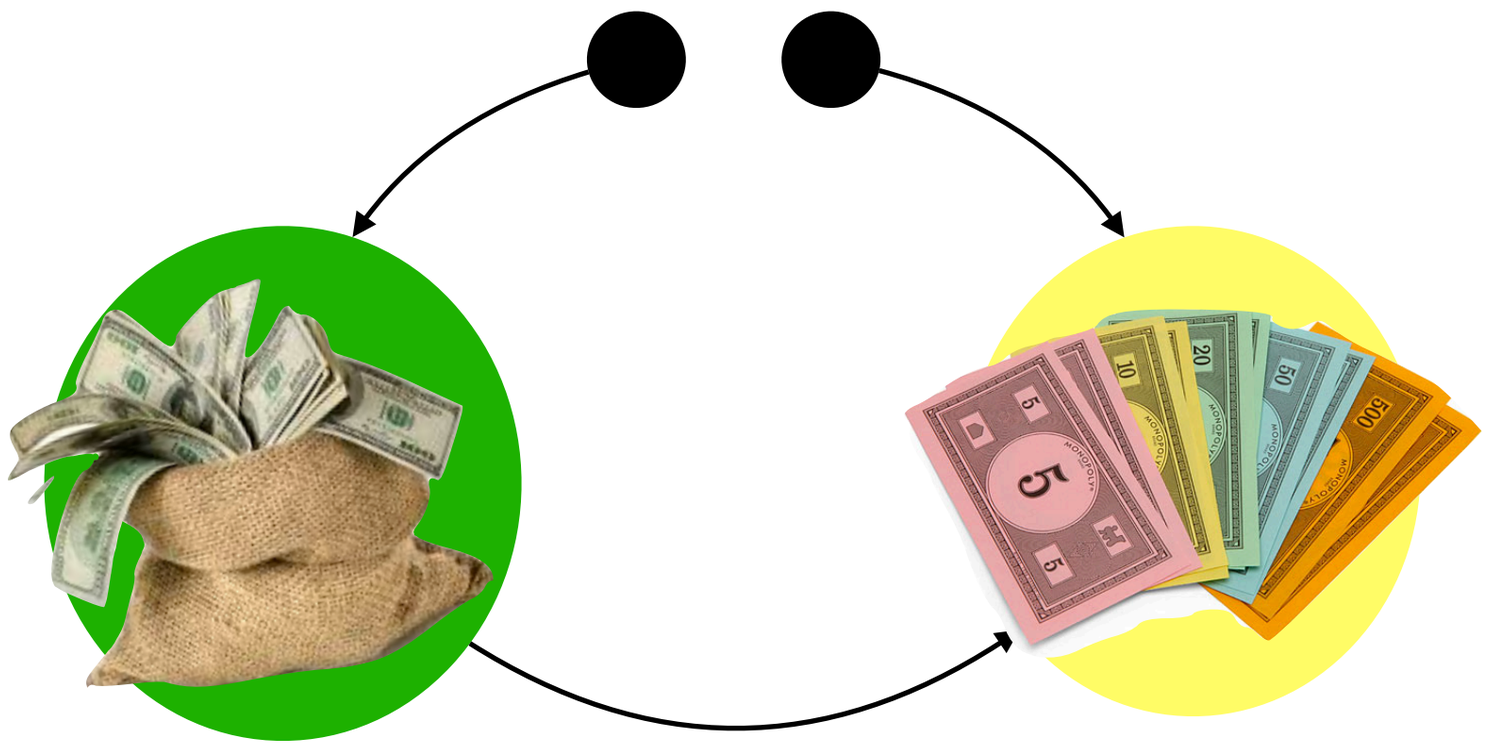


Unreachable

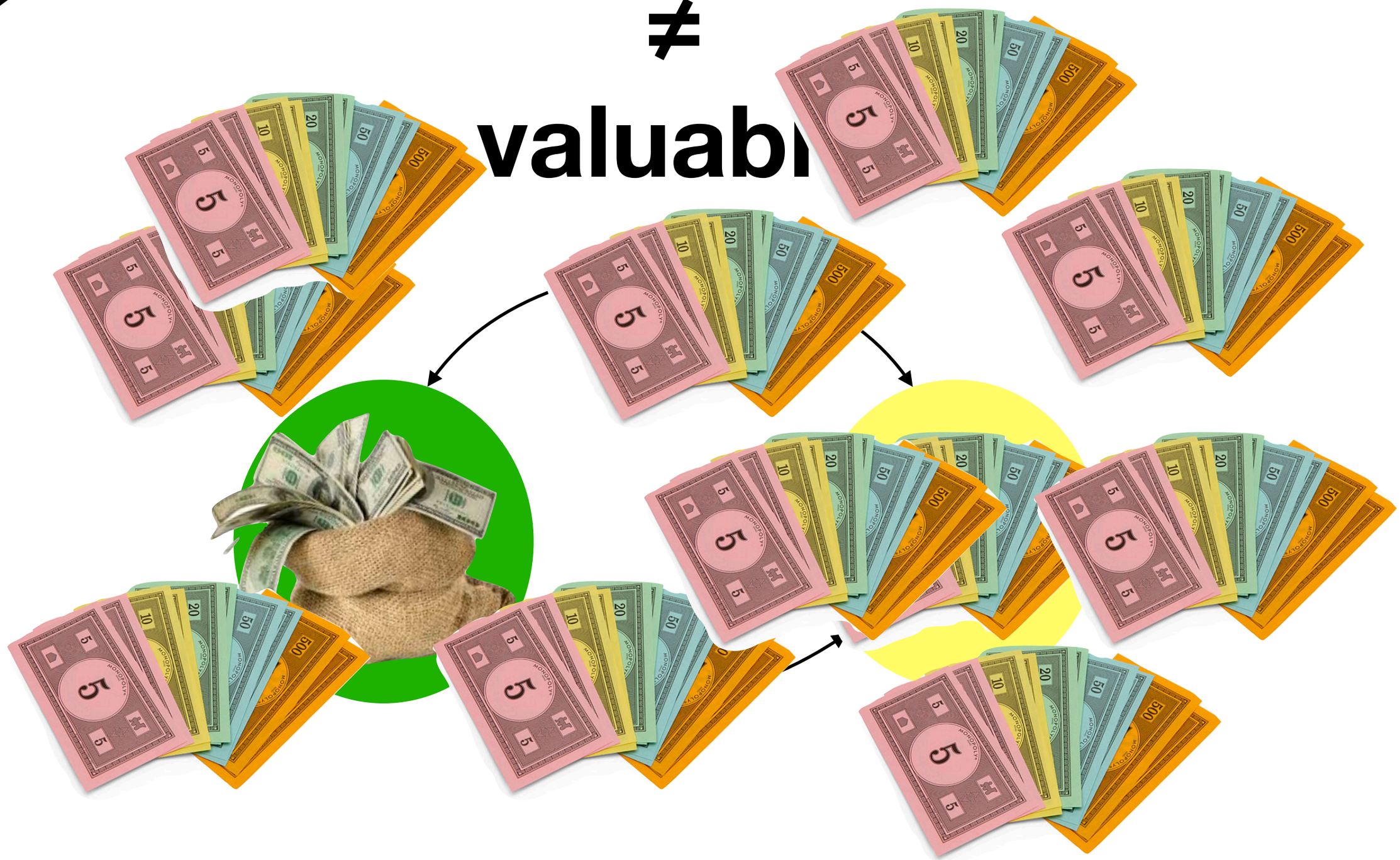
...?



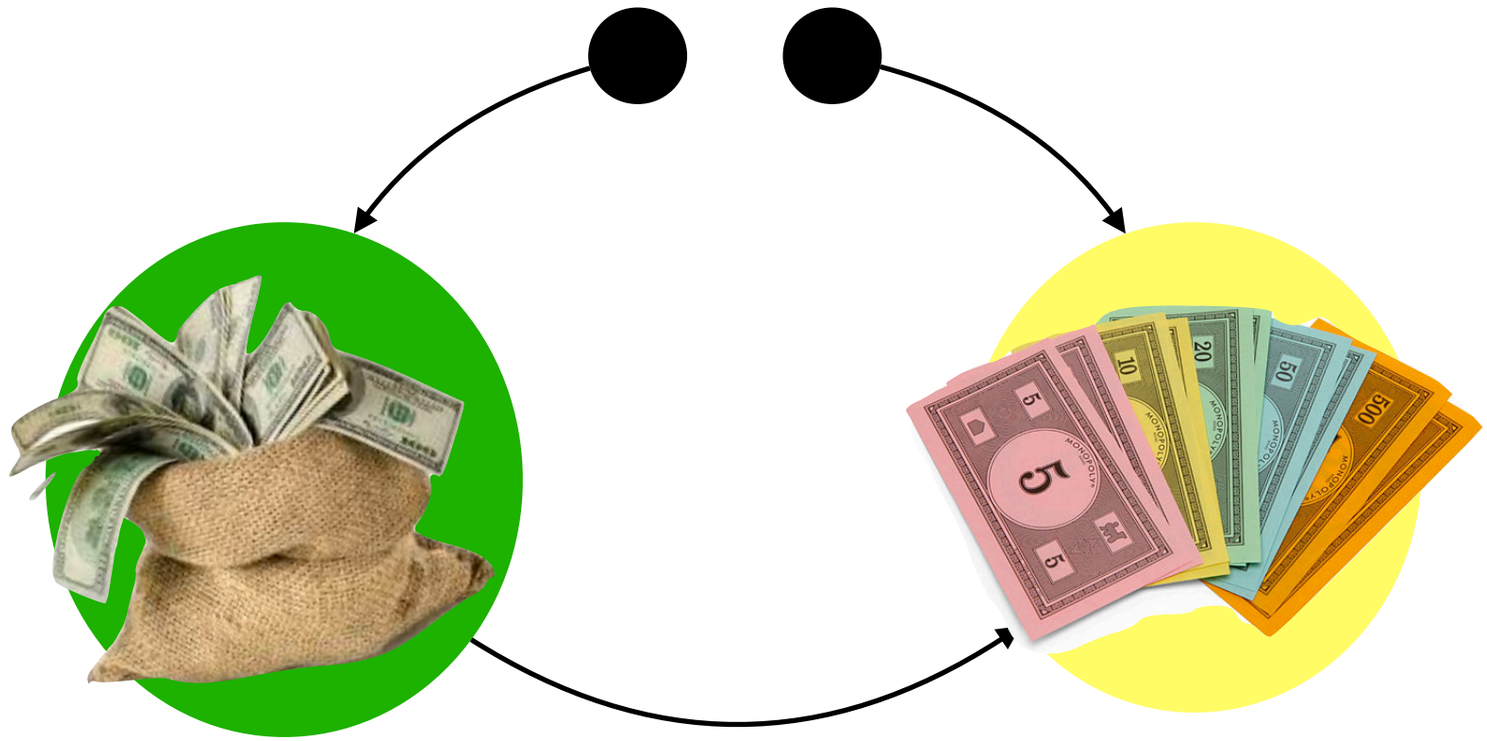
Reachable
≠
valuable



Reachable
≠
valuabl



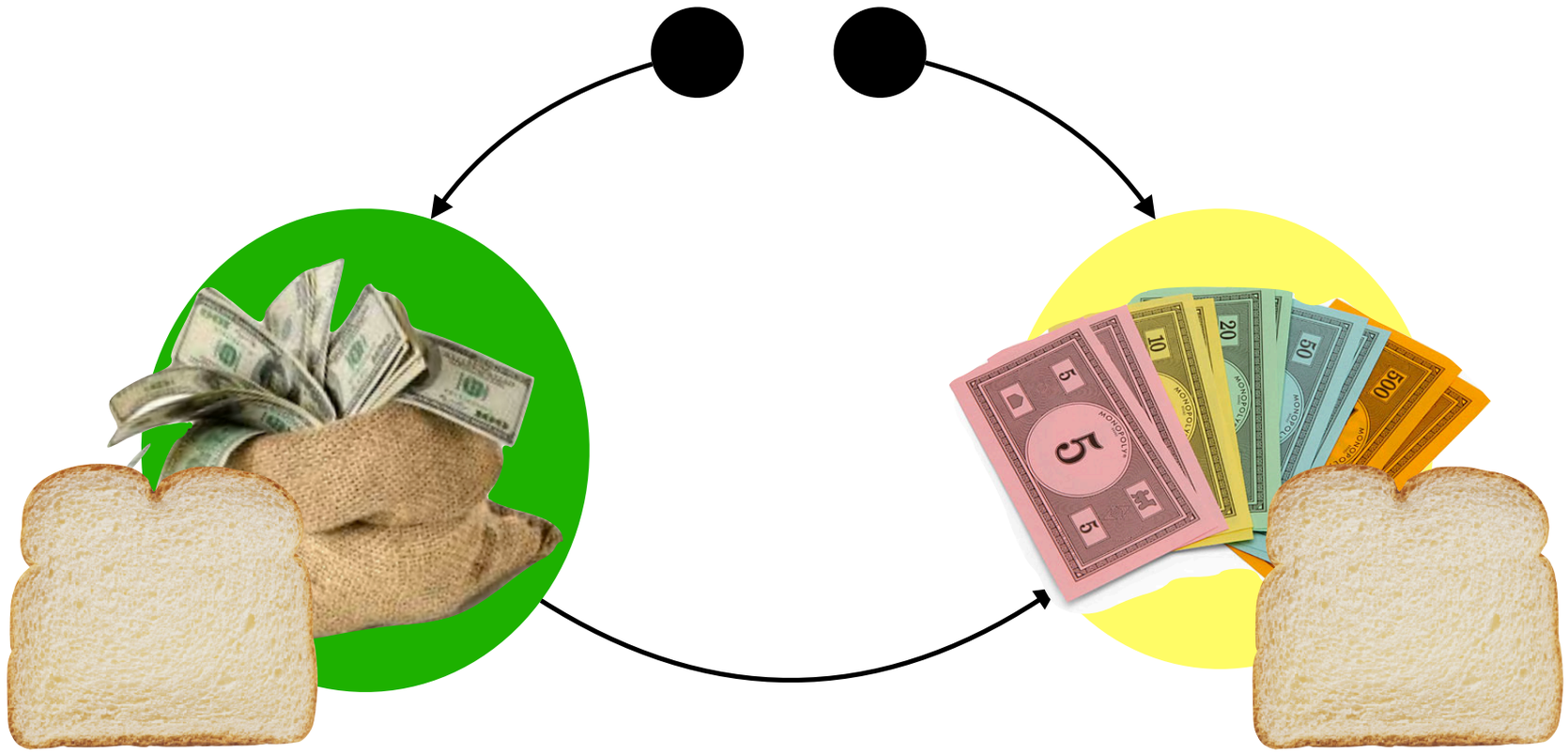
Reachable ≠ valuable



staleness tracking (SWAT, Hound)

[Hauswirth & Chilimbi, ASPLOS 04], [Novark, Berger & Zorn, PLDI 09]

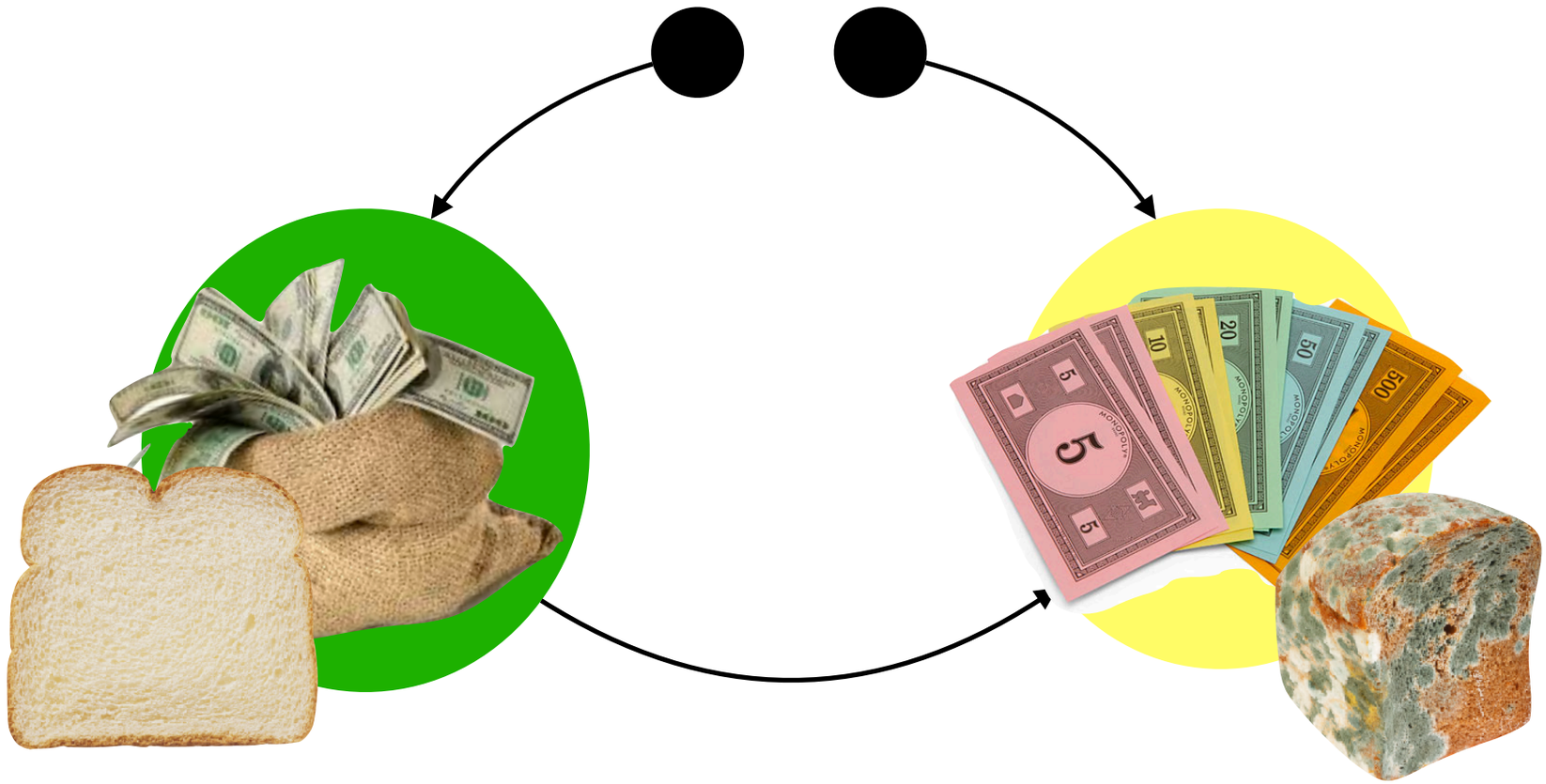
Reachable ≠ valuable



staleness tracking (SWAT, Hound)

[Hauswirth & Chilimbi, ASPLOS 04], [Novark, Berger & Zorn, PLDI 09]

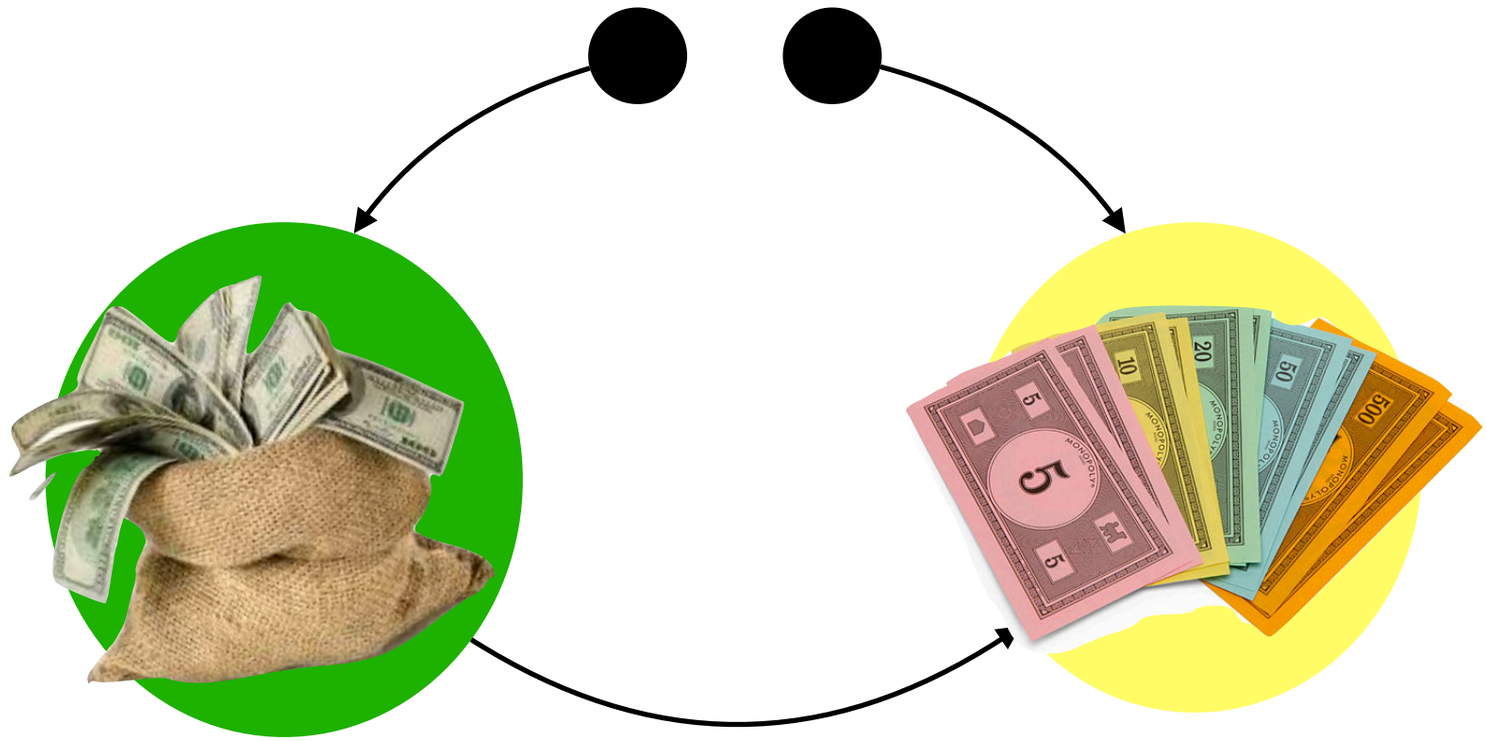
Reachable ≠ valuable



staleness tracking (SWAT, Hound)

[Hauswirth & Chilimbi, ASPLOS 04], [Novark, Berger & Zorn, PLDI 09]

Reachable ≠ valuable



growth analysis (LeakBot, Cork…)

[Mitchell & Sevitsky, ECOOP 03], [Jump & McKinley, POPL 07]

Reachable ≠ valuable

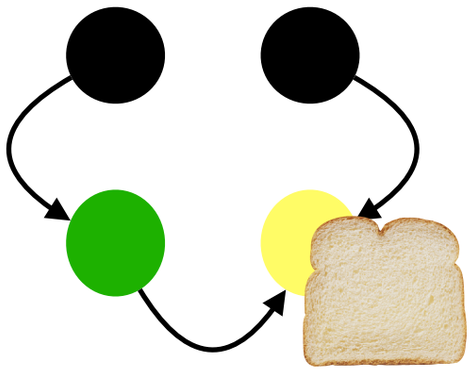
growth analysis (LeakBot, Cork…)

[Mitchell & Sevitsky, ECOOP 03], [Jump & McKinley, POPL 07]

Limitations of Prior Approaches

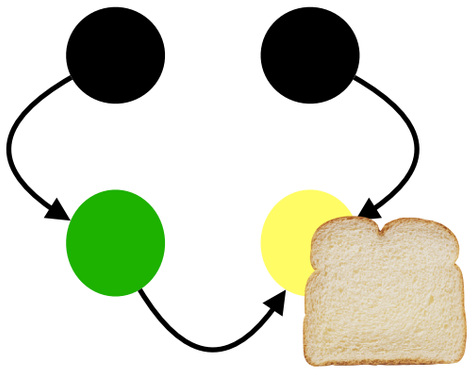
Limitations of Prior Approaches

leaks can be
reachable and
"fresh"



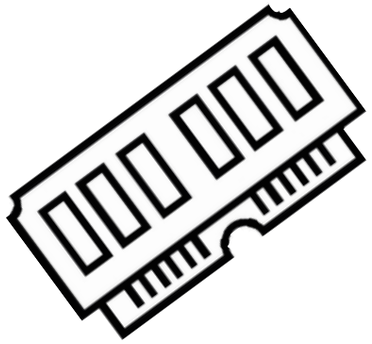
Limitations of Prior Approaches

leaks can be
reachable and
"fresh"



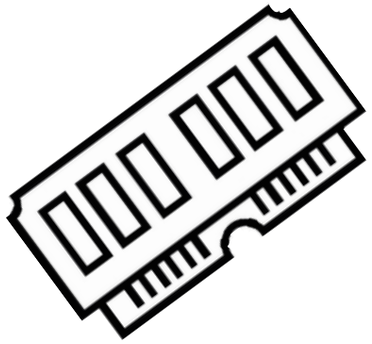
growth does not ⇒ leak!

(e.g. ~~cashes~~ caches)



Semantics-based Definition

isLeaky(objsource):



Semantics-based Definition

isLeaky(objsource):

deleted ⇒ no impact on behavior

Semantics-based Definition

isLeaky(objsource):

deleted ⇒ no impact on behavior

retains unbounded # of objects

Semantics-based Definition

isLeaky(objsource):

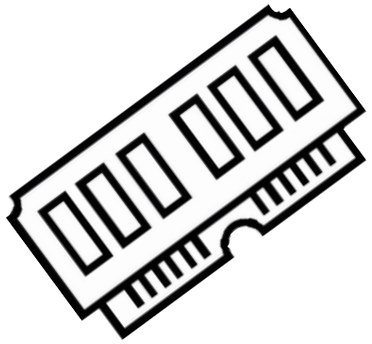
deleted ⇒ no impact on behavior

retains unbounded # of objects

just one problem…

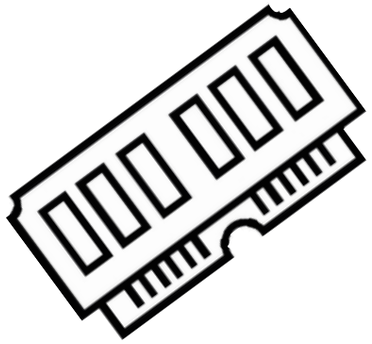
The Oracle at Delphi

The Oracle at Delphi



“EVERYTHING IS LEAKING”

- Our oracle



“EVERYTHING IS LEAKING”

- Our oracle

ANGULARJS by Google

Google Tag Manager

99.2% of Chrome crashes on low-end Androids:

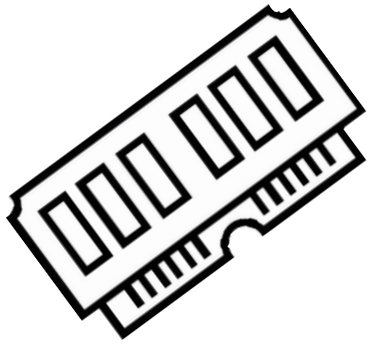
Out of memory!

[Hara, State of Blink’s Speed 17]

Google Analytics

jQuery

Google Maps



Debugging a Memory Leak in a Web App

(Real) Heap Snapshot from Airbnb.com

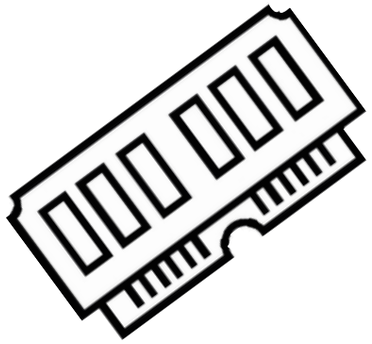
Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %
▶ Xn	5	5 668	1 %	1 042 912	2 %	1 727 696	3 %

Internal Chrome objects!

Every array & "anonymous" object

Obfuscated (minified) constructor names



Debugging a Memory Leak in a Web App

(Real) Heap Snapshot from Airbnb.com

Summary ▼ | Class filter | Objects allocated between Snapshot 1 and Snapshot 2 ▼

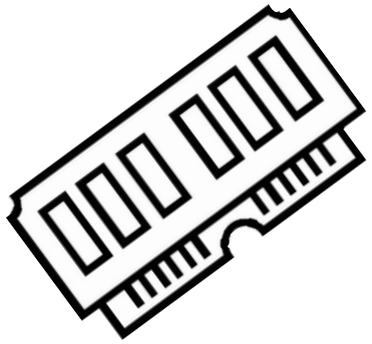
Constructor	Distance	Objects Count		Shallow Size		Retained Size	
▶ Array	3	1 162	0 %	37 184	0 %	3 063 512	5 %
▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %
▶ Xn	5	5 668	1 %	1 042 912	2 %	1 727 696	3 %

Internal Chrome objects!

Every array & "anonymous" object

Obfuscated (minified) constructor names

??



Debugging a Memory Leak in a Web App

(Real) Heap Snapshot from Airbnb.com

This situation is looking bleak…

▶ (system)	–	41 662	5 %	1 930 584	3 %	2 862 360	5 %
▶ (array)	–	7 342	1 %	1 878 624	3 %	2 545 528	4 %
▶ Object	–	16 246	2 %	901 904	1 %	2 163 712	4 %
▶ Xn	5	5 668	1 %	1 042 912	2 %	1 727 696	3 %

Internal Chrome objects!

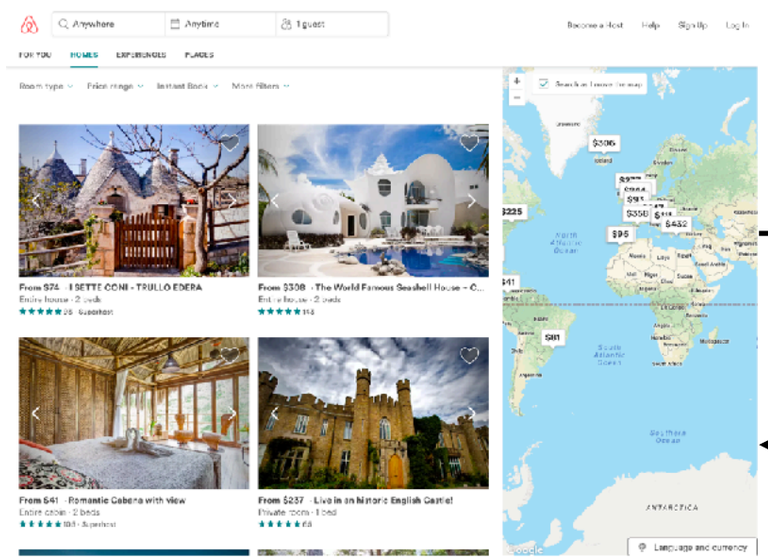
Every array & "anonymous" object

Obfuscated (minified) constructor names

??

Insight: Web Apps Return to Same Visual State

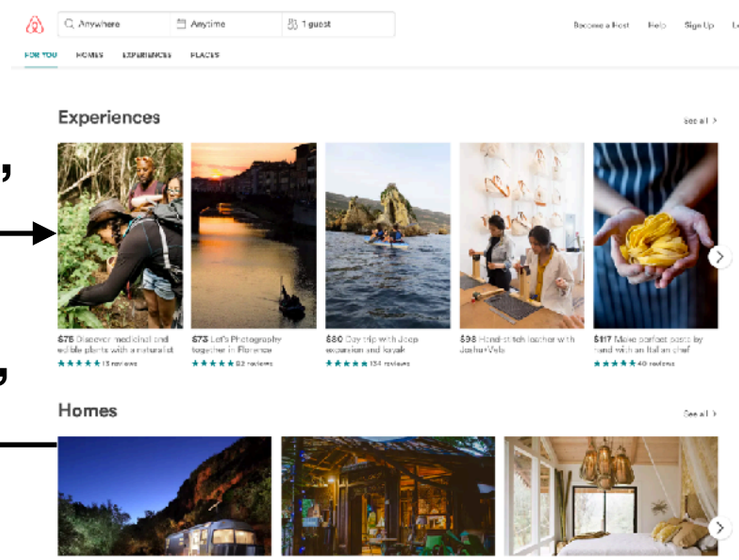
Modern “single page” web app



“Homes” Screen

Click on “for you”

Click on “homes”



“For You” Screen

Insight: Web Apps Return to Same Visual State

Modern “single page” web app

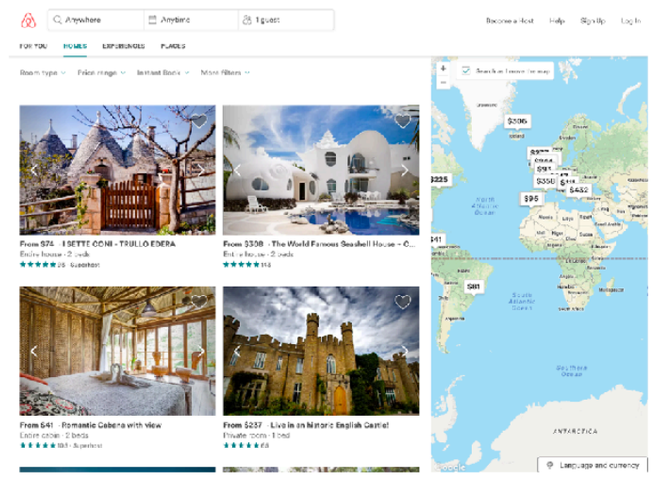
“Homes” Screen

“For You” Screen

Visual states (core output of web app)

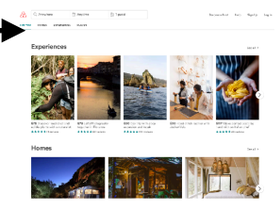
Insight: Web Apps Return to Same Visual State

Modern “single page” web app



“Homes” Screen

Click on “for you”

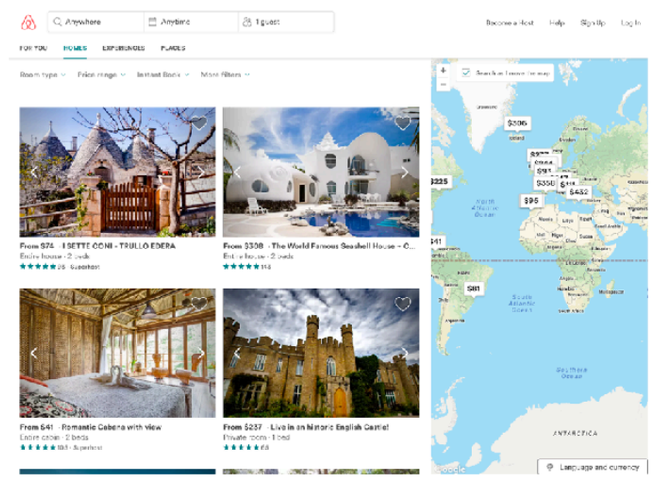


Click on “homes”

“For You” Screen

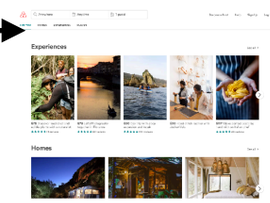
Insight: Web Apps Return to Same Visual State

Modern “single page” web app



“Homes” Screen

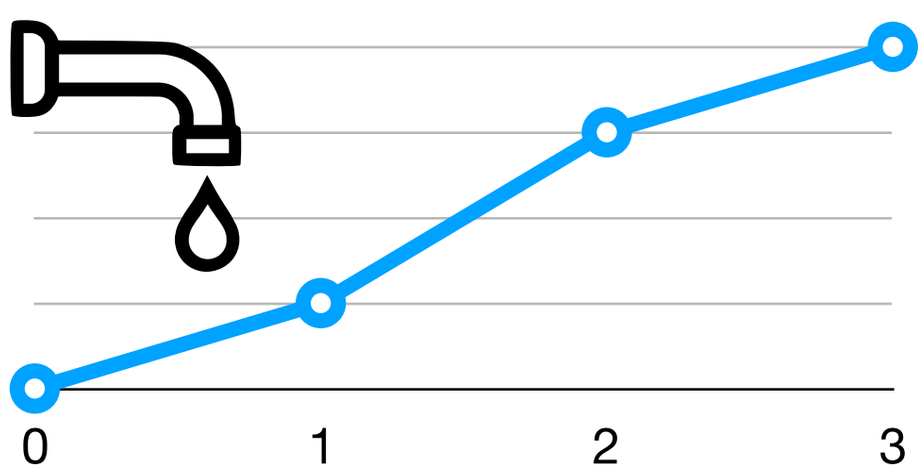
Click on “for you”



Click on “homes”

“For You” Screen

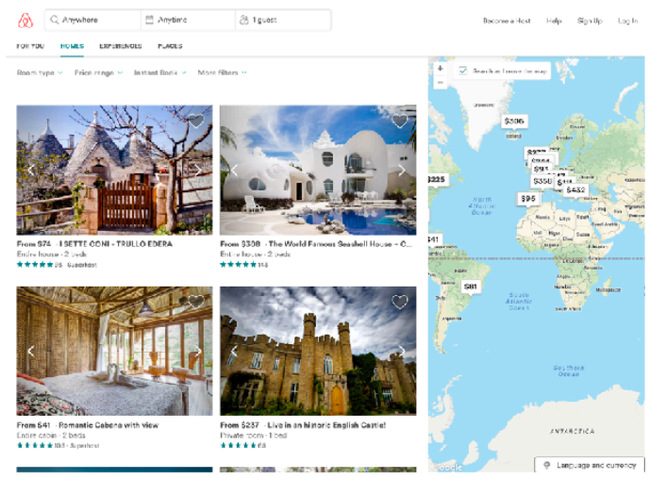
Live Heap Size over Visits to “Homes”



Insight: Web Apps Return to Same Visual State

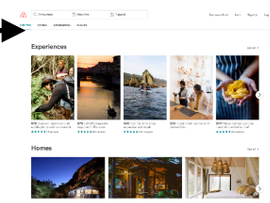
Modern “single page” web app

Growth between visits to same screen is strong indicator of leak



“Homes” Screen

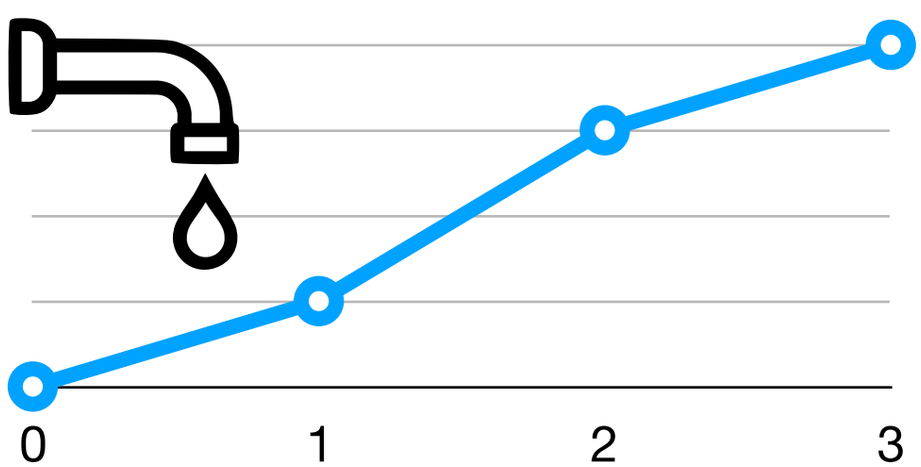
Click on “for you”



Click on “homes”

“For You” Screen

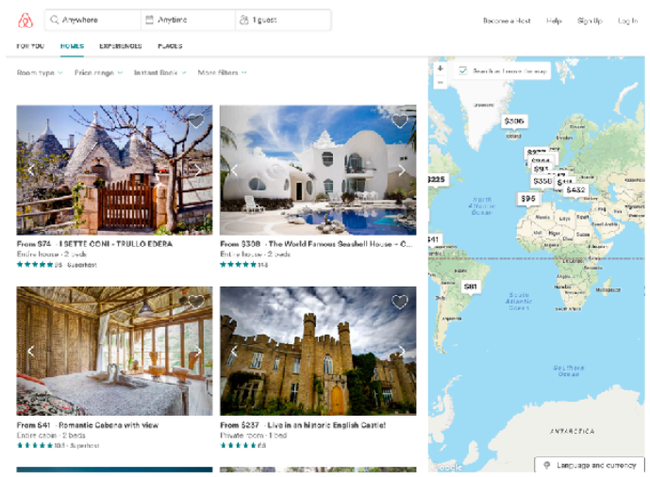
Live Heap Size over Visits to “Homes”



Insight: Web Apps Return to Same Visual State

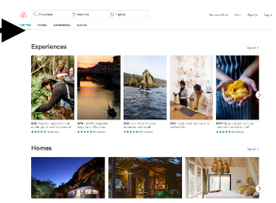
Modern “single page” web app

Growth between visits to same screen is strong indicator of leak



“Homes” Screen

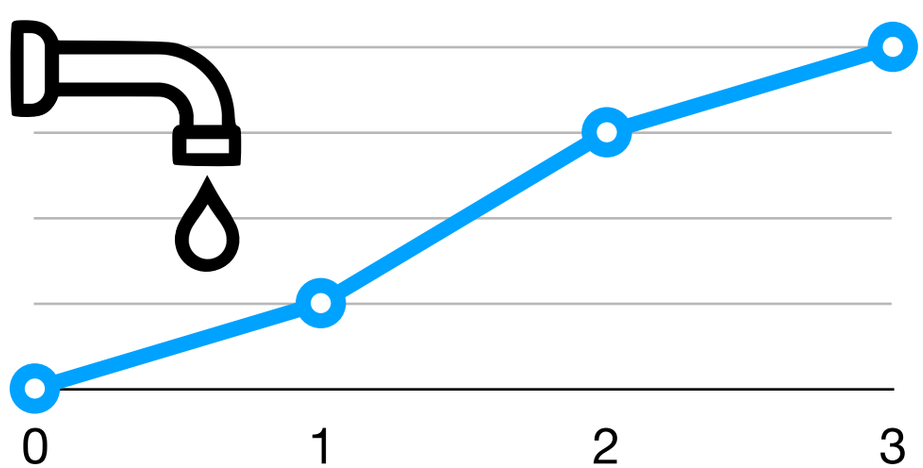
Click on “for you”



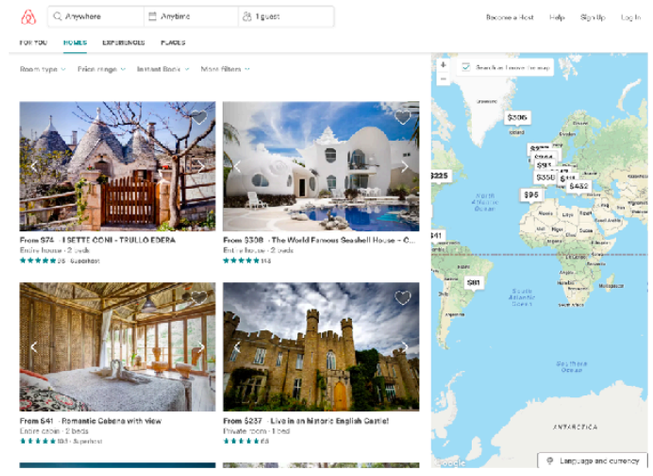
Click on “homes”

“For You” Screen

Live Heap Size over Visits to “Homes”

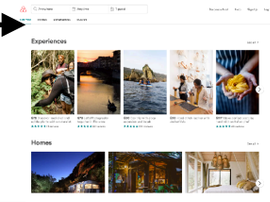


BLeak: Automatic Leak Debugger for Web Applications



“Homes” Screen

Click on “for you”

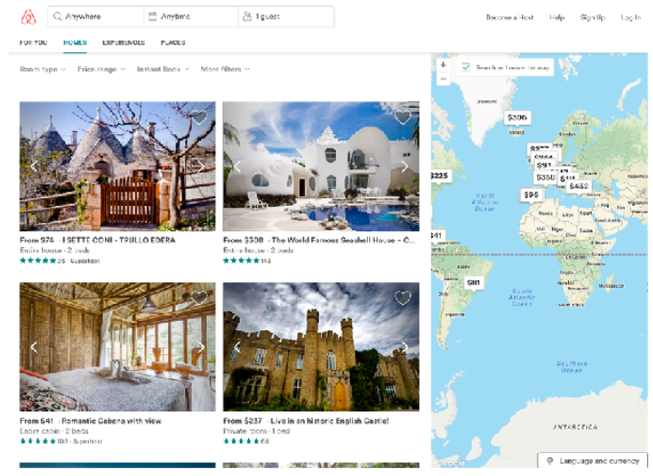


Click on “homes”

“For You” Screen

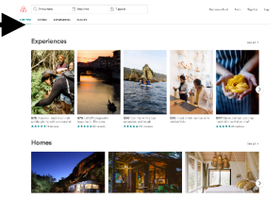
PLDI 2018

BLeak: Automatic Leak Debugger for Web Applications



“Homes” Screen

Click on “for you”



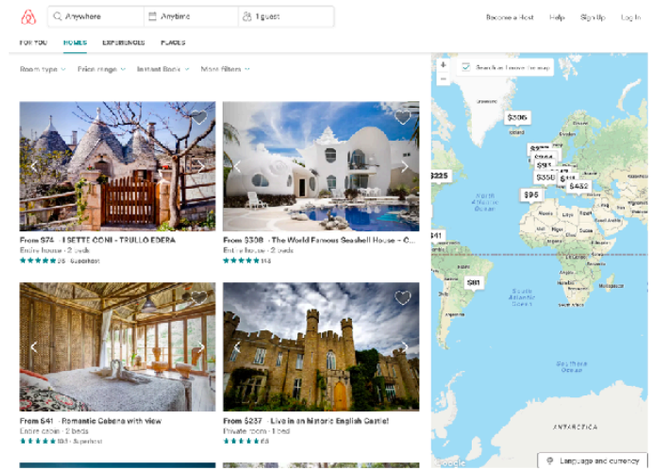
“For You” Screen

Click on “homes”

Leverages “oracle” to find leaks

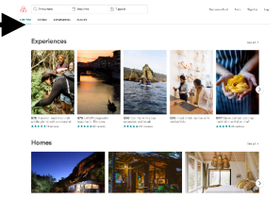
PLDI 2018

BLeak: Automatic Leak Debugger for Web Applications



“Homes” Screen

Click on “for you”



Click on “homes”

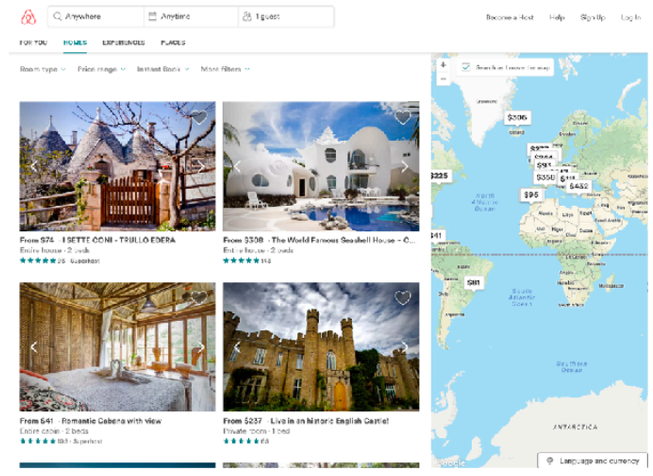
“For You” Screen

Leverages “oracle” to find leaks

High precision (> 90%)

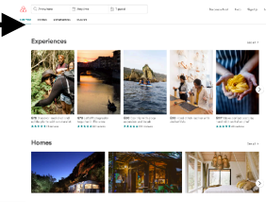
PLDI 2018

BLeak: Automatic Leak Debugger for Web Applications



"Homes" Screen

Click on "for you"



Click on "homes"

"For You" Screen

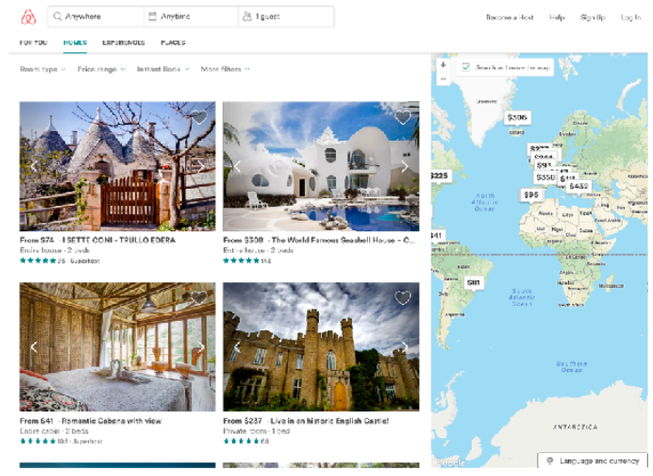
Leverages "oracle" to find leaks

High precision (> 90%)

High impact (found big leaks in production apps)

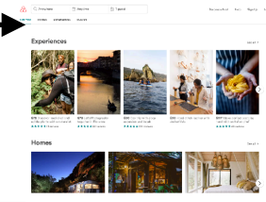
PLDI 2018

BLeak: Automatic Leak Debugger for Web Applications



"Homes" Screen

Click on "for you"



Click on "homes"

"For You" Screen

Leverages "oracle" to find leaks

High precision (> 90%)

High impact (found big leaks in production apps)

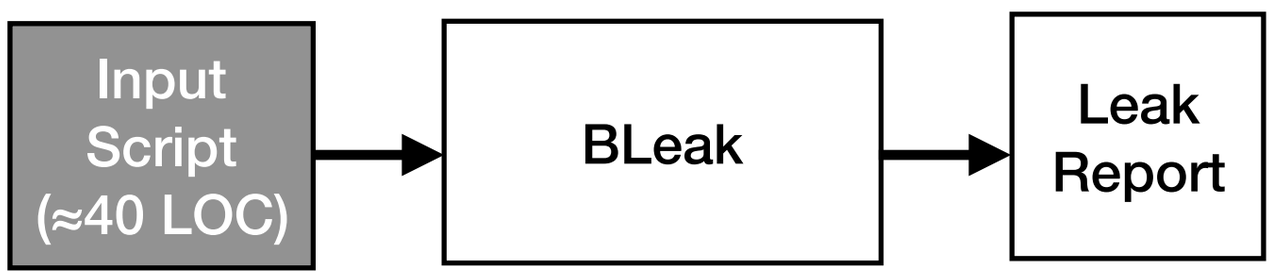
Reports code directly responsible for leaks!

PLDI 2018

BLeak: Automatic Leak Debugger for Web Applications

Input
Script
(≈40 LOC)

BLeak: Automatic Leak Debugger for Web Applications



BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

```
exports.loop = [{
  check: function() {
    const link4 = document.getElementsByTagName('a')[4];
    return link4.getAttribute('aria-selected') === 'true';
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
}, {
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

17 LOC

```
exports.loop = [{
  check: function() {
    const link4 = document.getElementsByTagName('a')[4];
    return link4.getAttribute('aria-selected') === 'true';
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
}, {
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() === "R
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

Visual States

```
exports.loop = [{
  check: function() {
    const link4 = document.getElementsByTagName('a')[4];
    return link4.getAttribute('aria-selected') === 'true';
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
},{
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() ==  "R
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

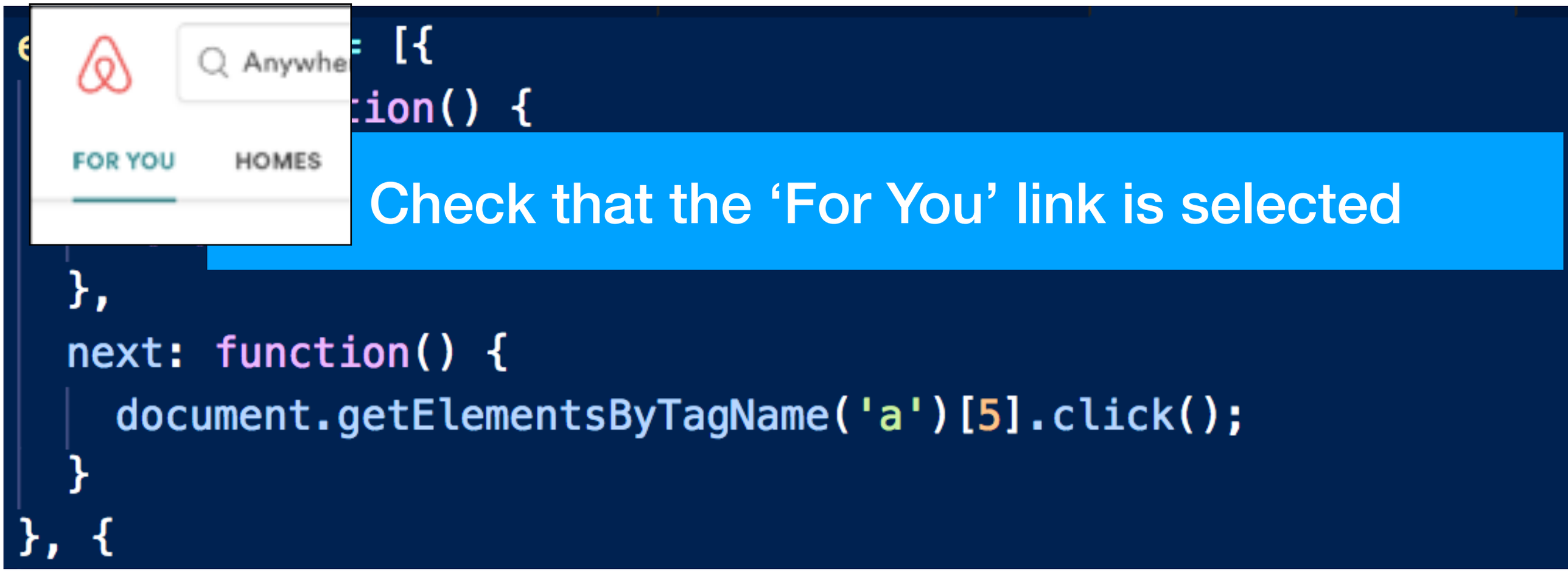
BLeak: Automatic Leak Debugger for Web Applications

Airbnb “For Me” Visual State:

```
exports.loop = [{
  check: function() {
    const link4 = document.getElementsByTagName('a')[4];
    return link4.getAttribute('aria-selected') === 'true';
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
}, {
```

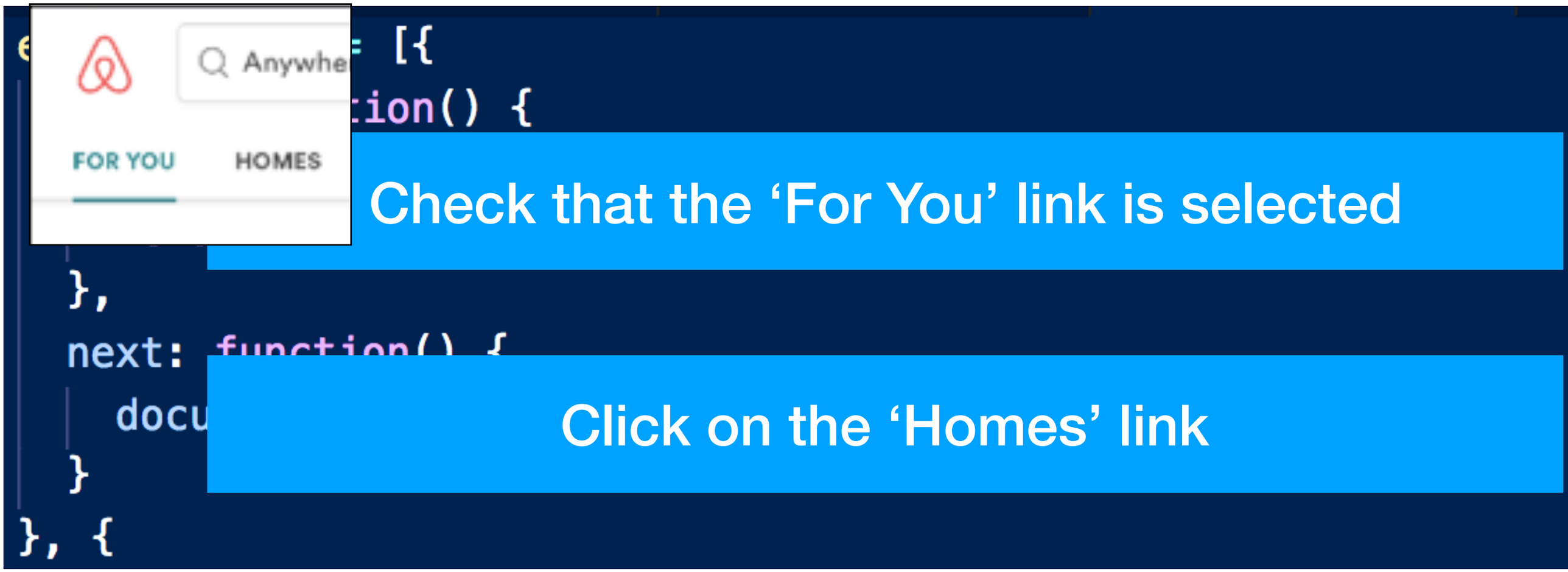
BLeak: Automatic Leak Debugger for Web Applications

Airbnb “For Me” Visual State:



BLeak: Automatic Leak Debugger for Web Applications

Airbnb “For Me” Visual State:



BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

```
exports.loop = [{
  check: function() {
    const link4 = document.getElementsByTagName('a')[4];
    return link4.getAttribute('aria-selected') === 'true';
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
}, {
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

Wait for application to display ‘For You’ screen

```
exports.loop = [{
  },
  next: function() {
    document.getElementsByTagName('a')[5].click();
  }
}, {
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

Wait for application to display ‘For You’ screen

Transition to ‘Homes’ screen

```
exports.loop = [{
  },
  next: function() {
}, {
  check: function() {
    const buttons = document.getElementsByTagName('button');
    const link5 = document.getElementsByTagName('a')[5];
    return link5.getAttribute('aria-selected') === 'true' &&
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

```
exports.loop = [{
  },
  next: function() {
}, {
  check: function() {
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
  next: function() {
    document.getElementsByTagName('a')[4].click();
  }
}];
```

Wait for application to display ‘For You’ screen

↓

Transition to ‘Homes’ screen

↓

Wait for application to display ‘Homes’ screen

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

```
exports.loop = [{
  },
  next: function() {
}, {
  check: function() {
    buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
  },
}];
```

Wait for application to display ‘For You’ screen

Transition to ‘Homes’ screen

Wait for application to display ‘Homes’ screen

Transition to ‘For You’ screen

BLeak: Automatic Leak Debugger for Web Applications

Input script for airbnb:

```
exports.loop = [{
  }, {
    check: function() {
      buttons.length > 11 && buttons[11].innerText.trim() === "Room type";
    },
}];
```

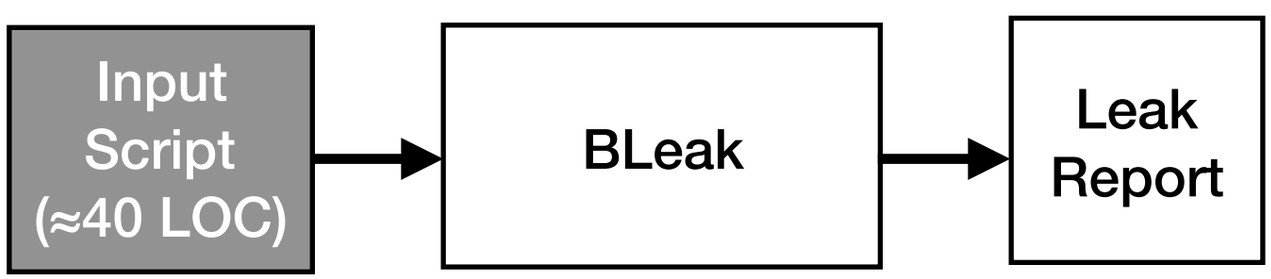
Wait for application to display ‘For You’ screen

Transition to ‘Homes’ screen

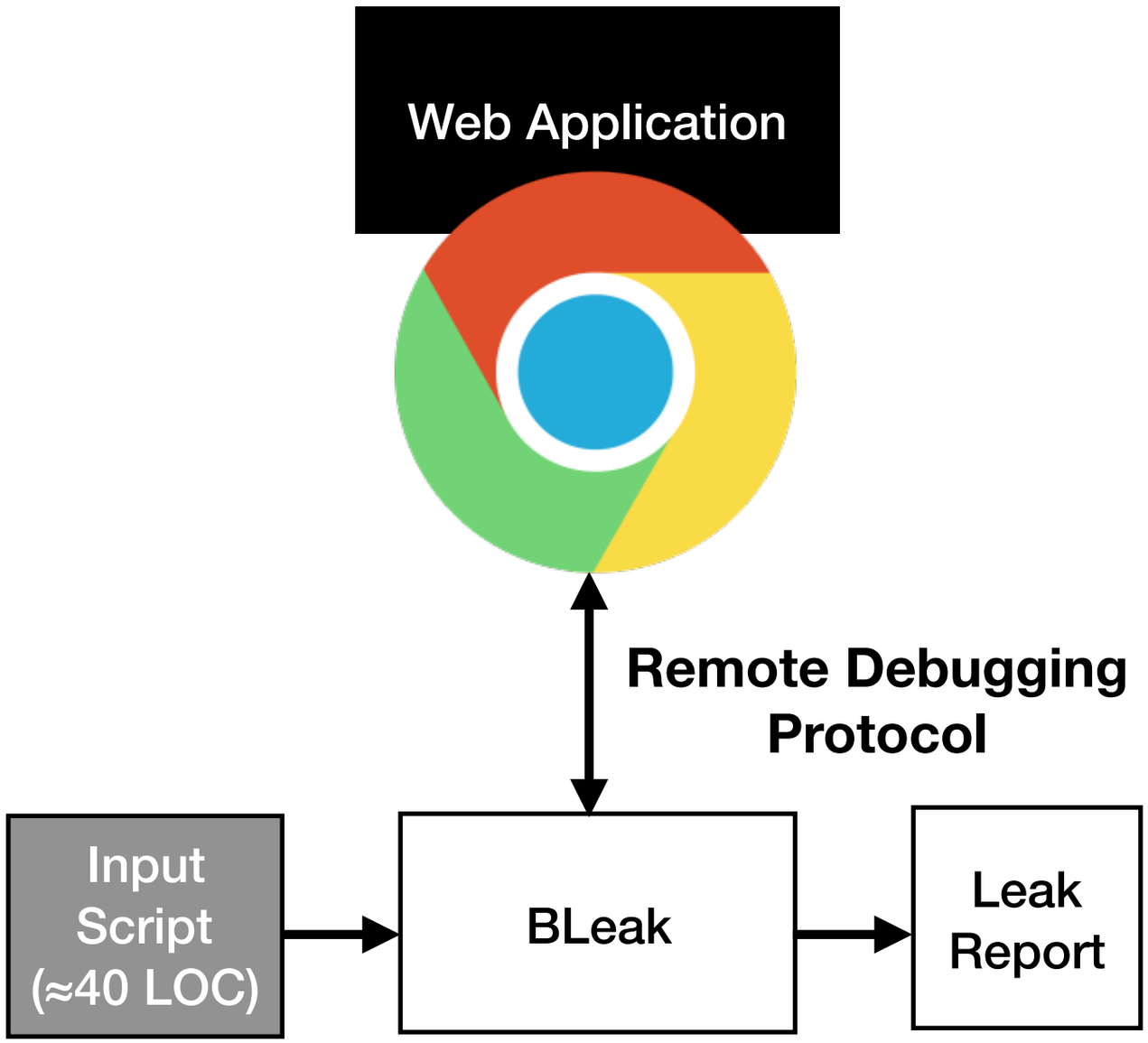
Wait for application to display ‘Homes’ screen

Transition to ‘For You’ screen

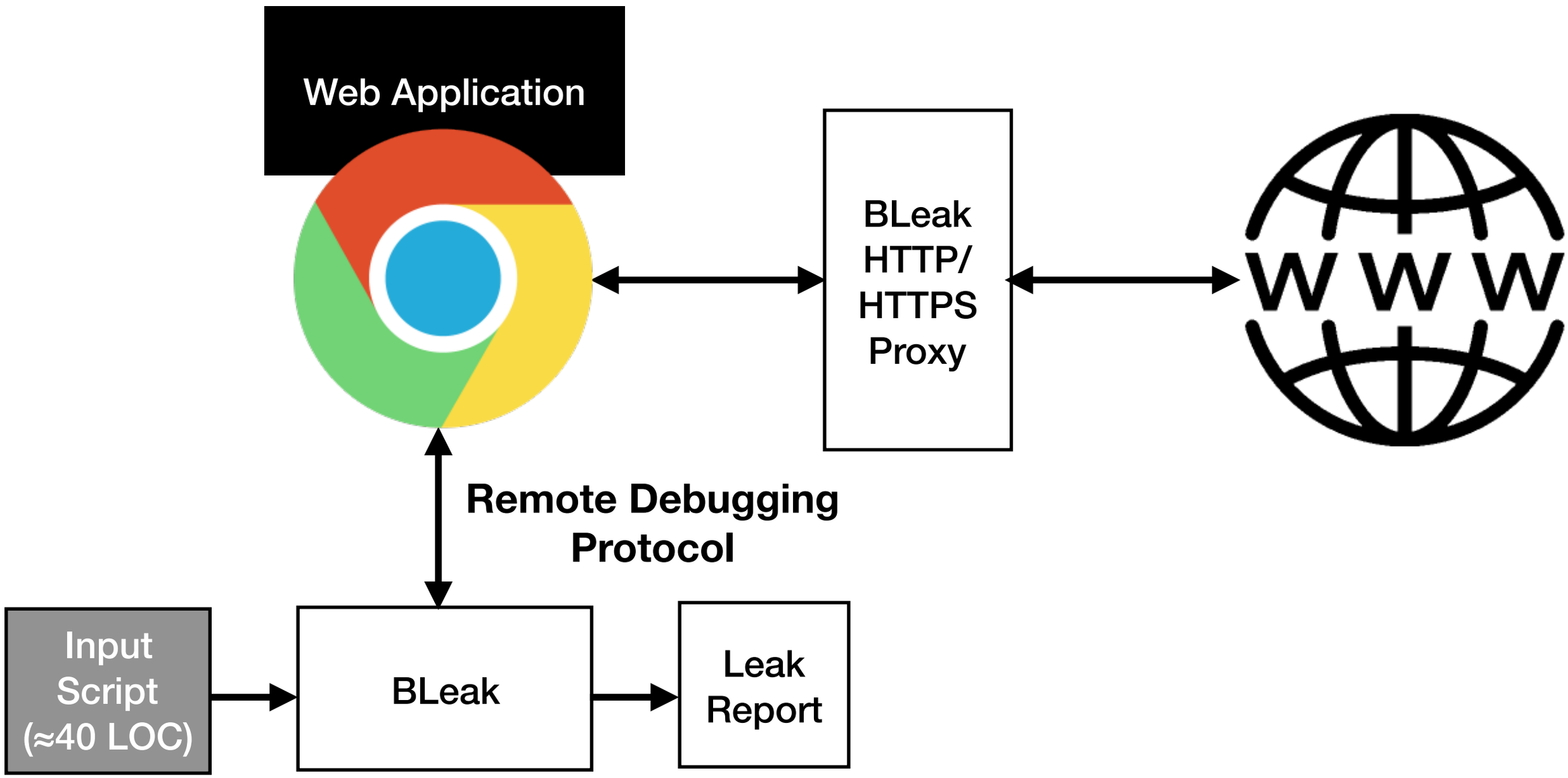
BLeak: Automatic Leak Debugger for Web Applications



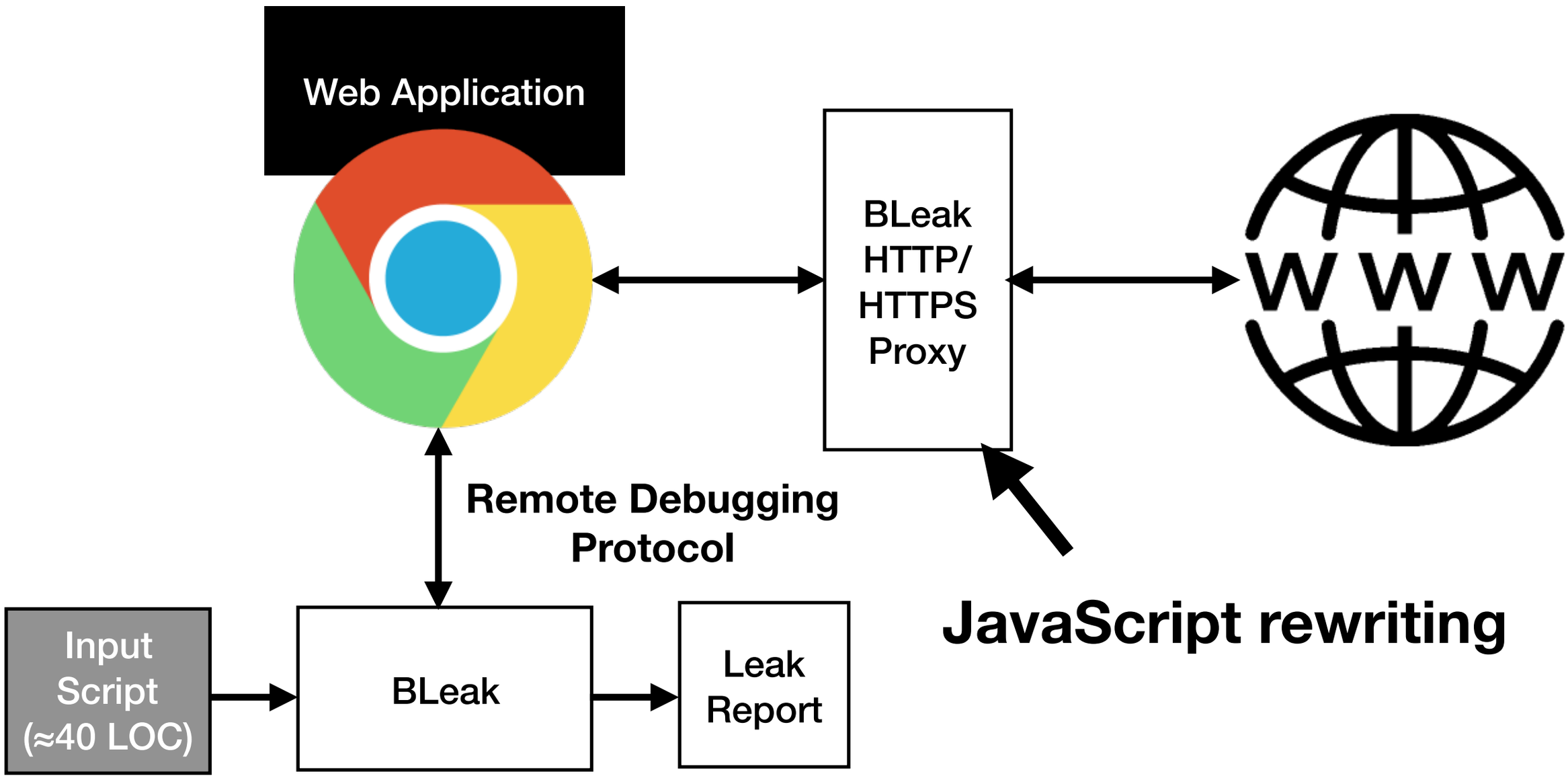
BLeak: Automatic Leak Debugger for Web Applications



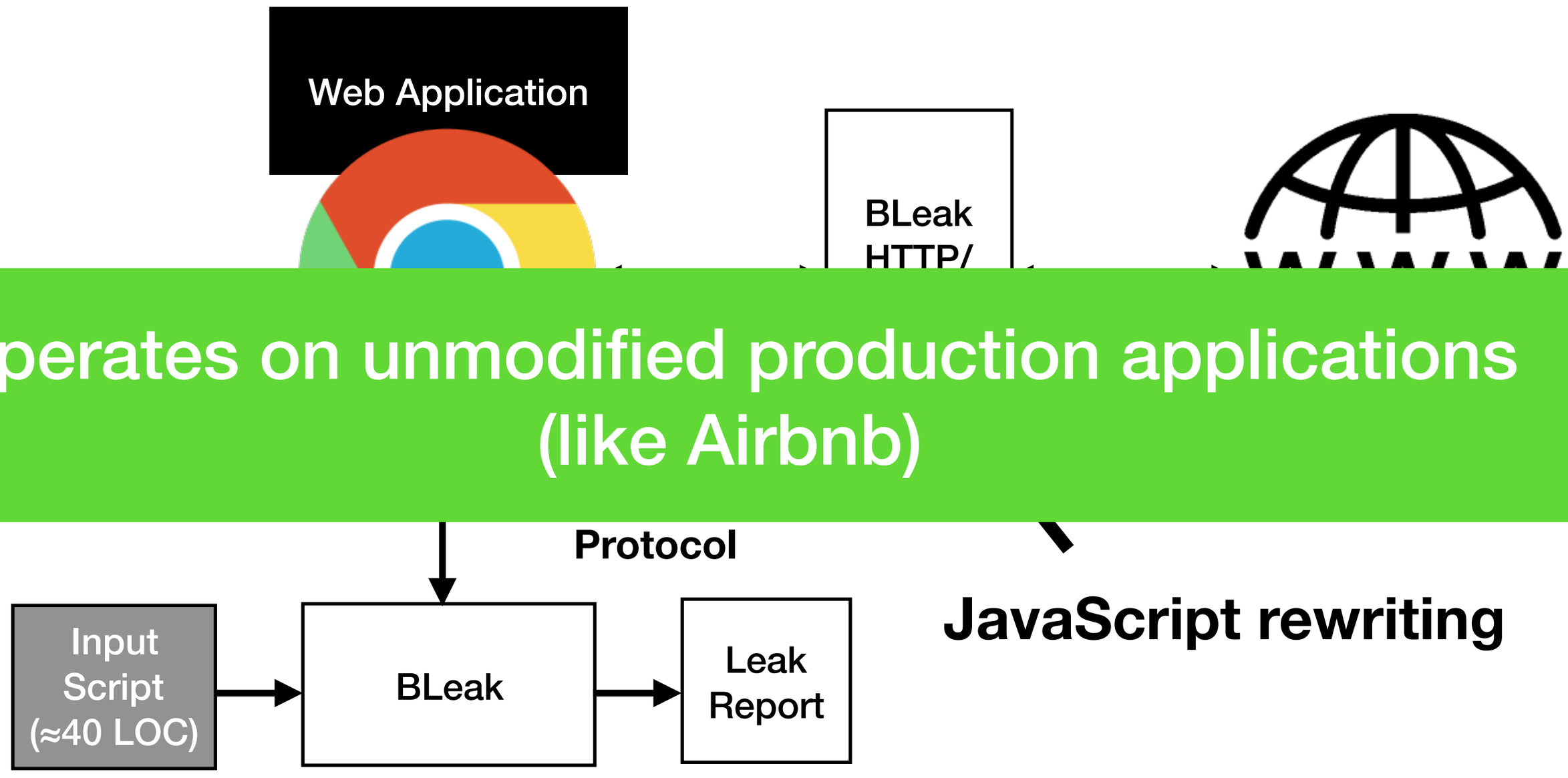
BLeak: Automatic Leak Debugger for Web Applications



BLeak: Automatic Leak Debugger for Web Applications



BLeak: Automatic Leak Debugger for Web Applications



Operates on unmodified production applications (like Airbnb)

BLeak: Automatic Leak Debugger for Web Applications

Found+reported 50+ unknown memory leaks in:

ANGULARJS by Google

jQuery

airbnb

Google Analytics

criteo

Google Tag Manager

mailpile

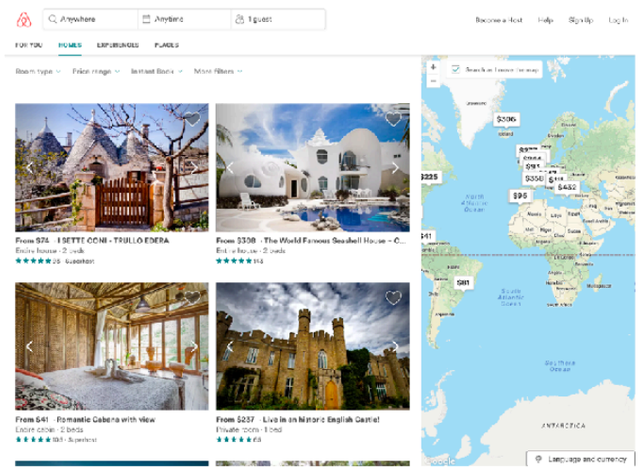
PIWIK

LOOMIO make decisions together

Firefox debugger.html

Google Maps

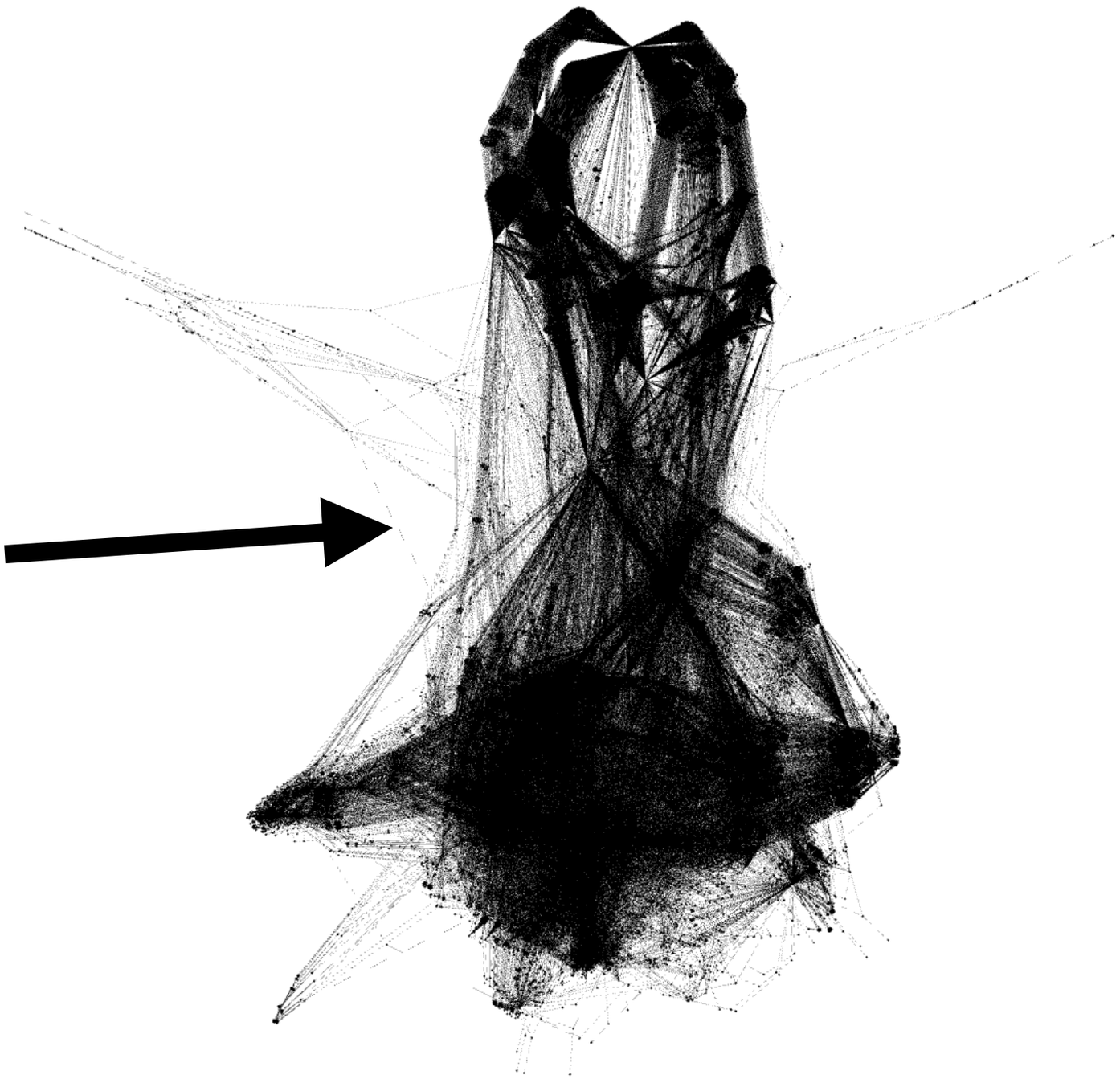
BLeak: Identifying Memory Leaks



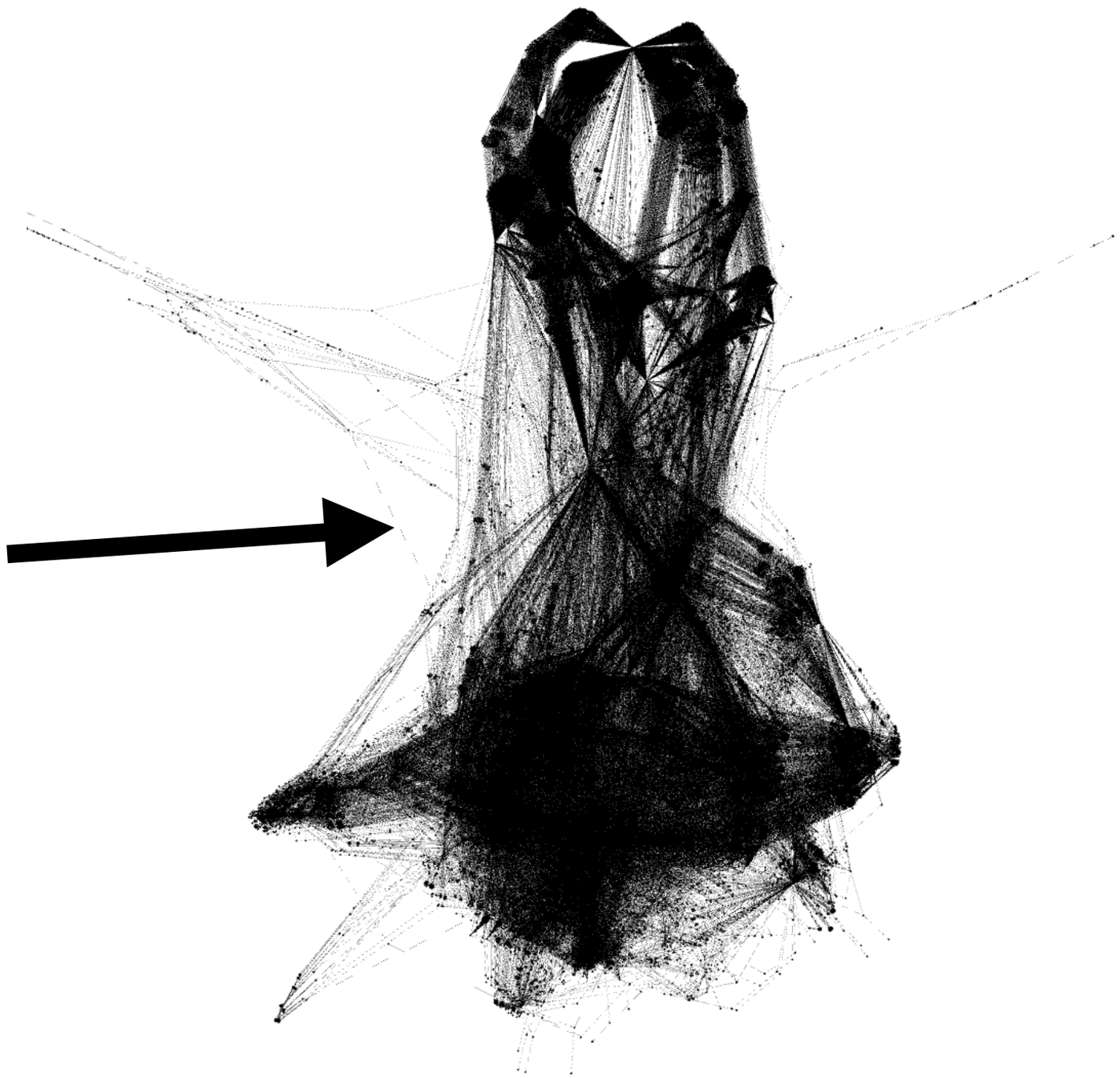
“Homes” Screen

BLeak: Identifying Memory Leaks

about:blank
heap
graph



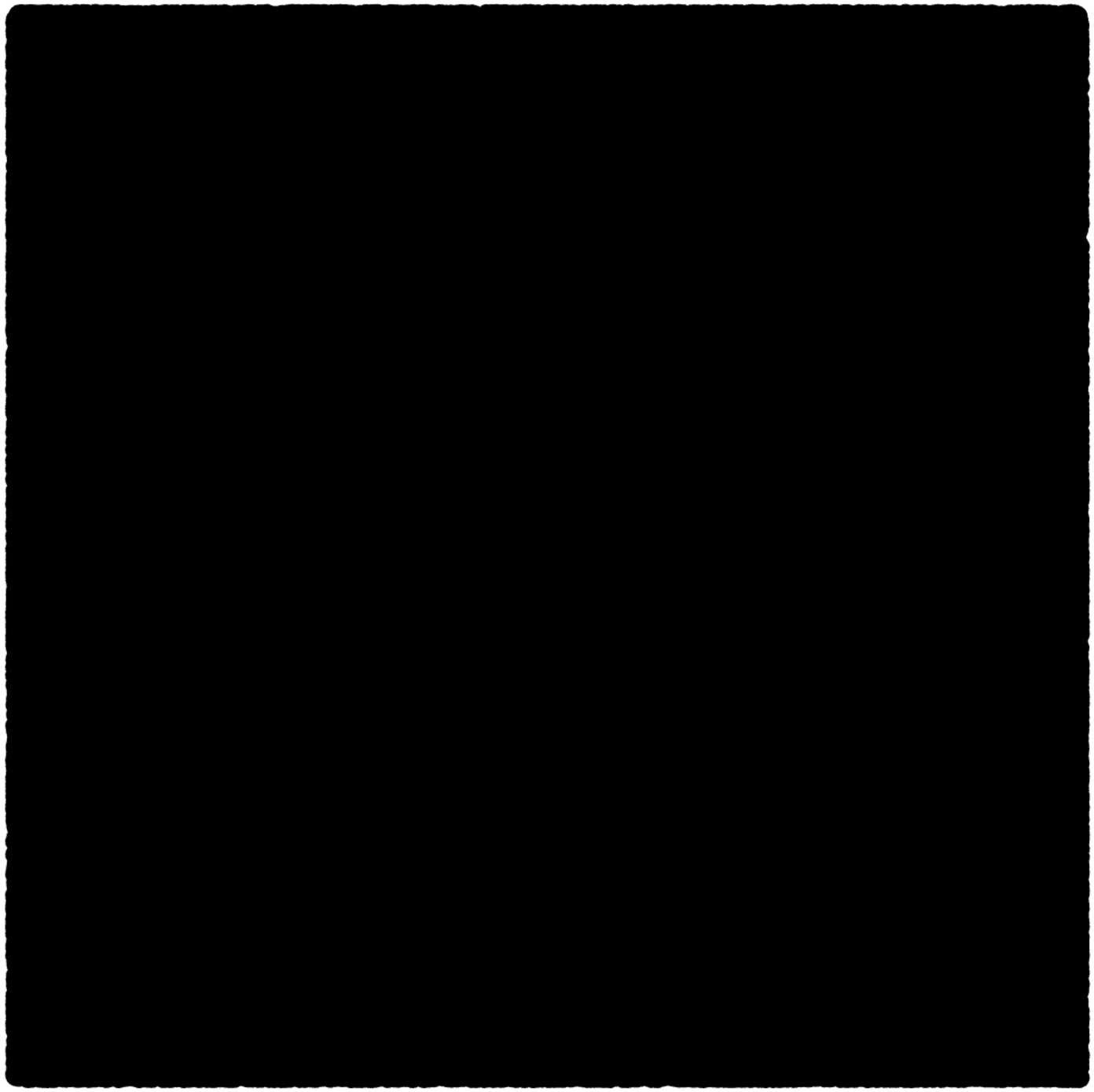
BLeak: Identifying Memory Leaks



about:blank
heap
graph

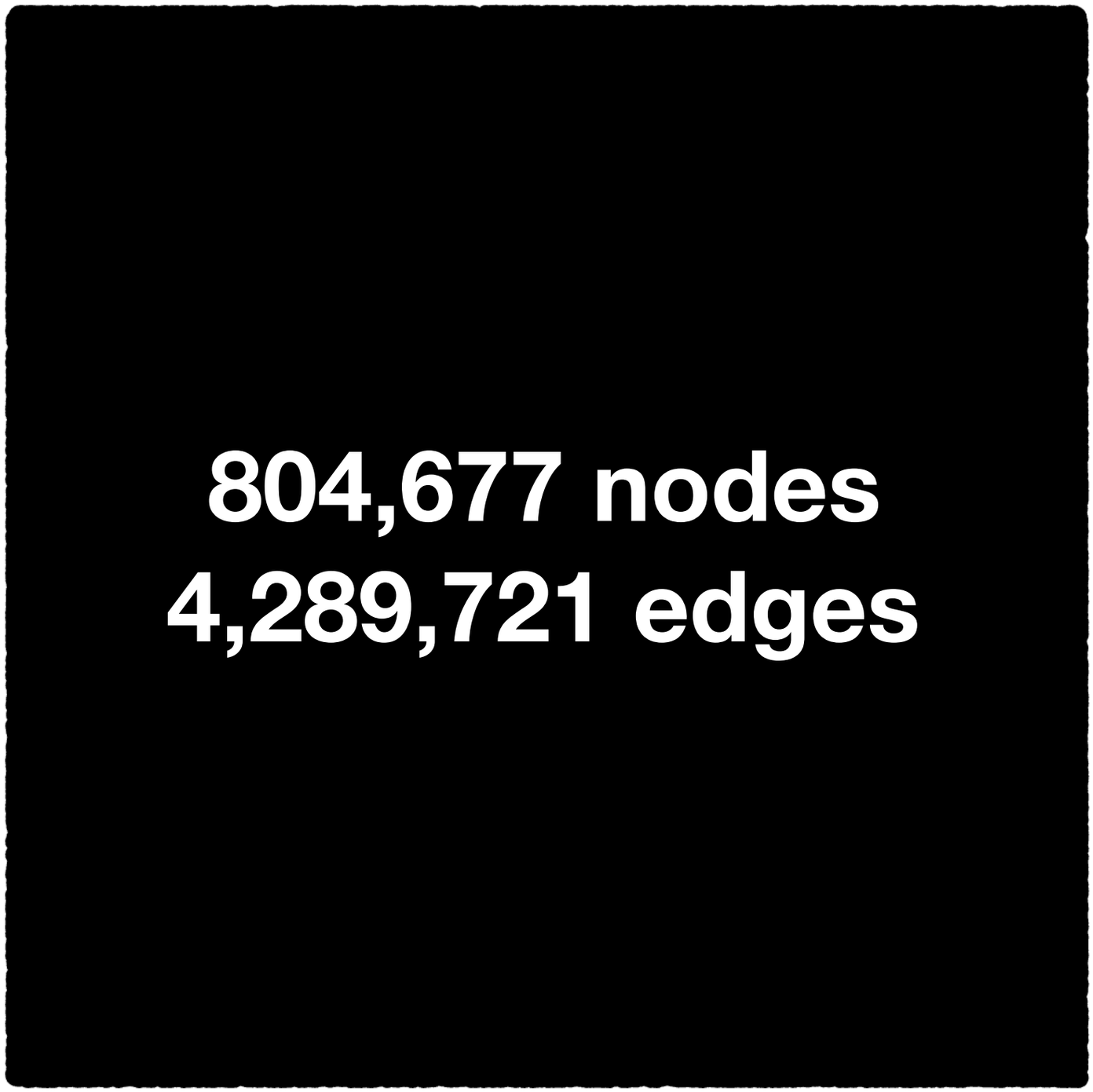
27,699 nodes
117,083 edges

BLeak: Identifying Memory Leaks



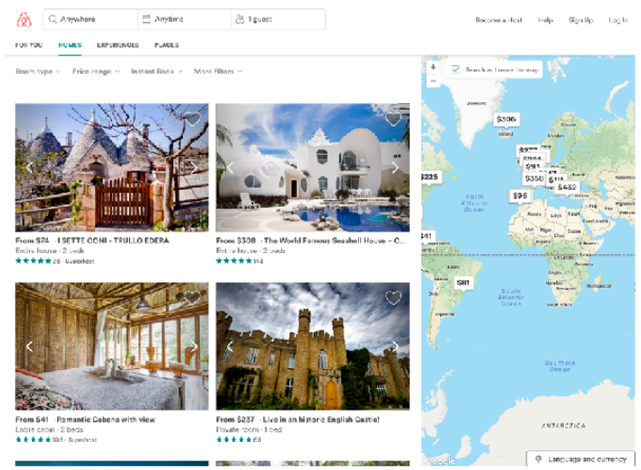
Real Airbnb heap graph (rendered by Gephi)

BLeak: Identifying Memory Leaks



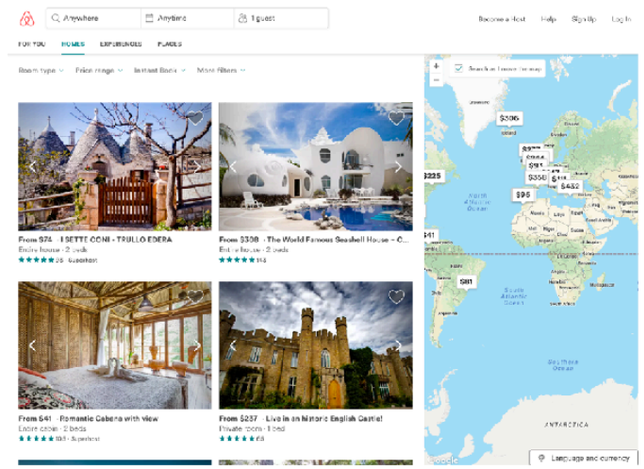
Real Airbnb heap graph (rendered by Gephi)

BLeak: Identifying Memory Leaks

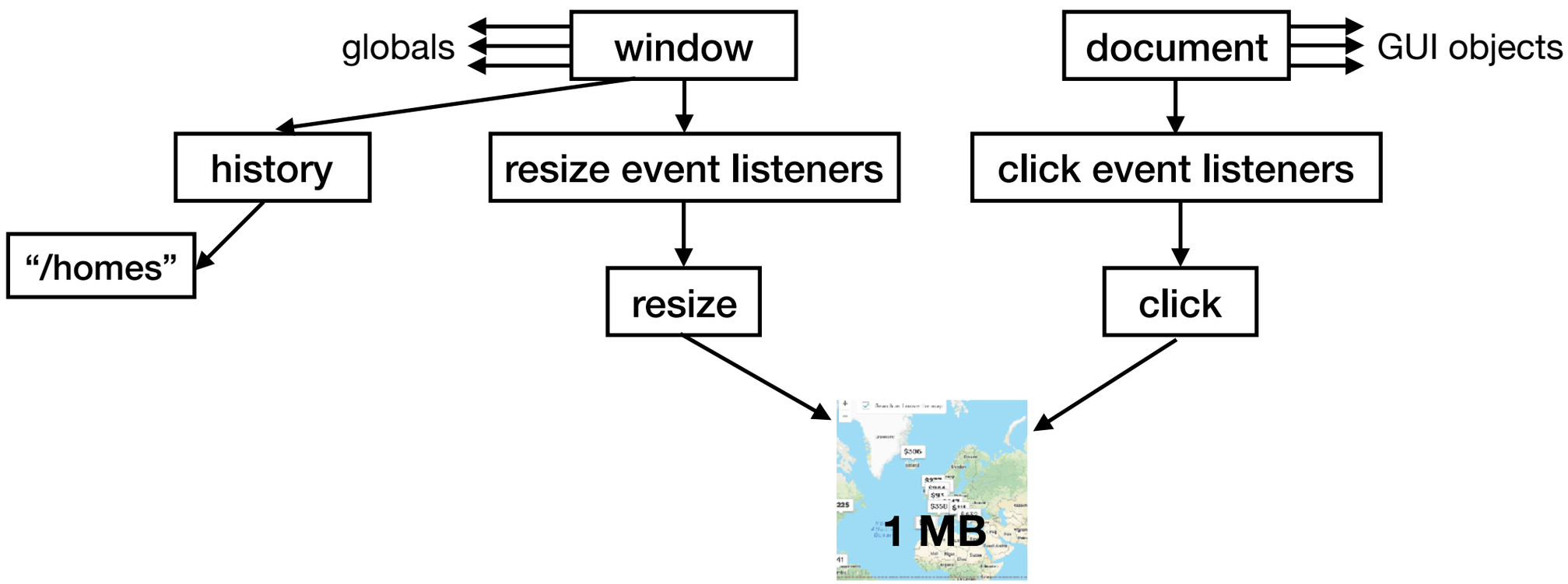


“Homes” Screen

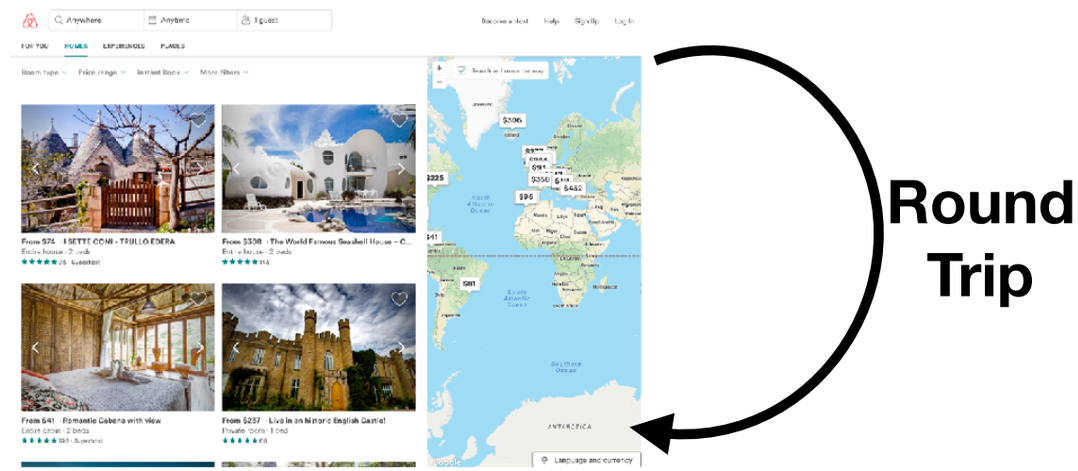
BLeak: Identifying Memory Leaks



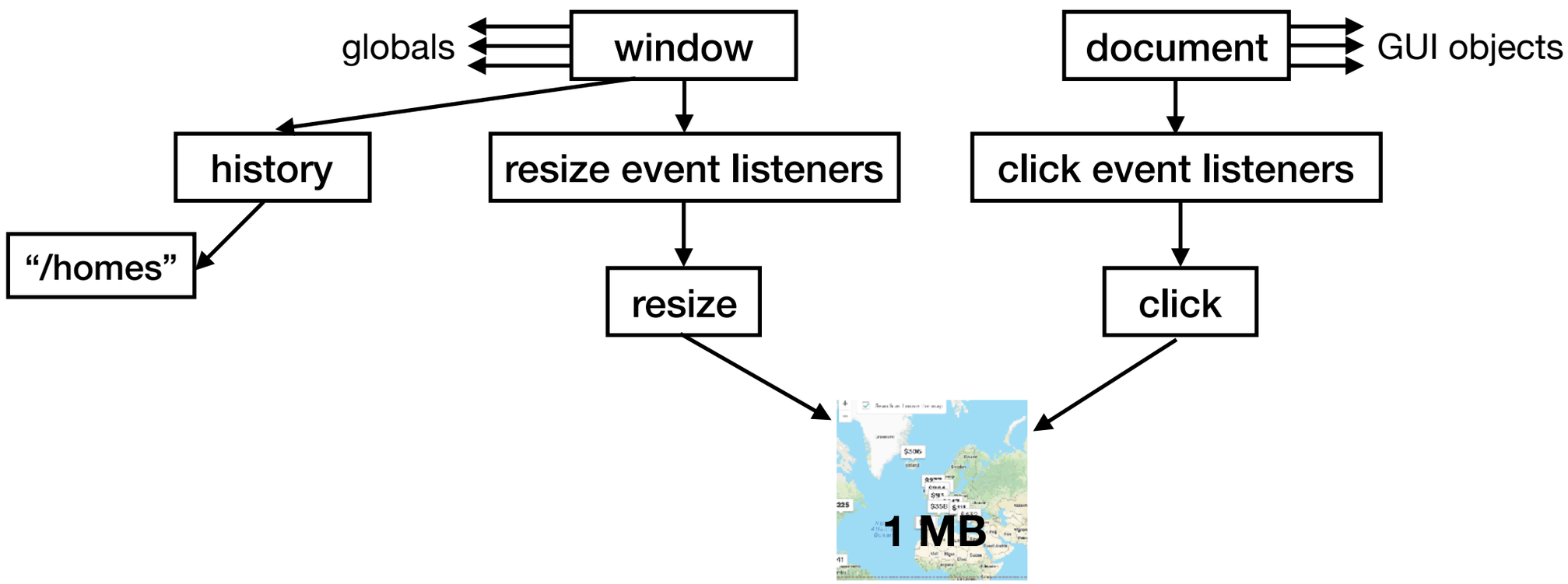
“Homes” Screen



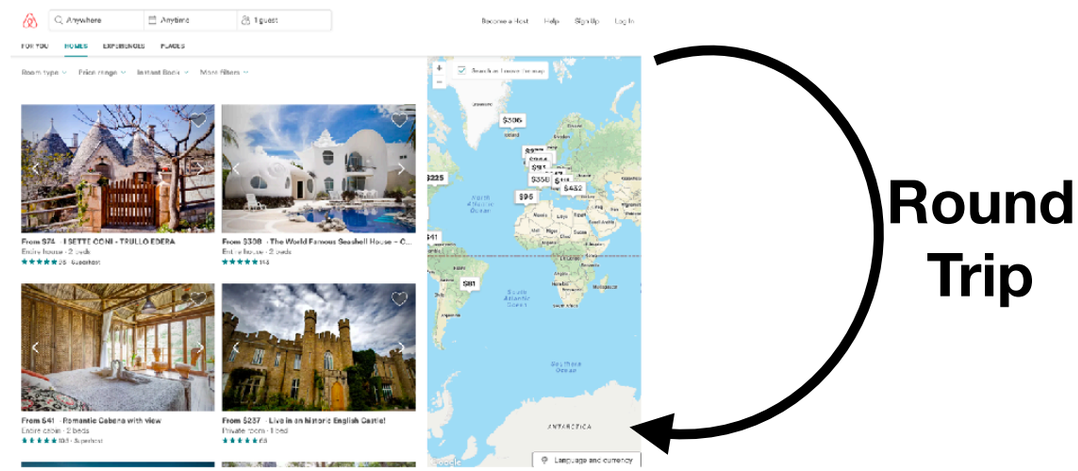
BLeak: Identifying Memory Leaks



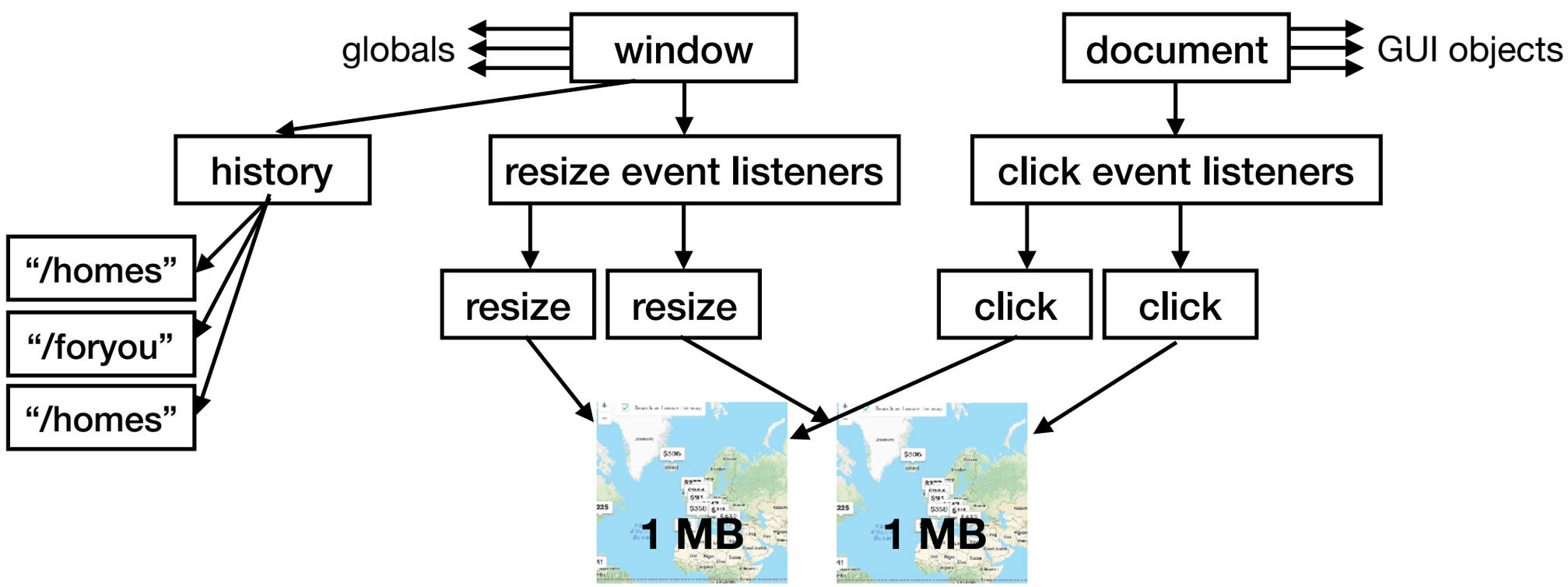
"Homes" Screen



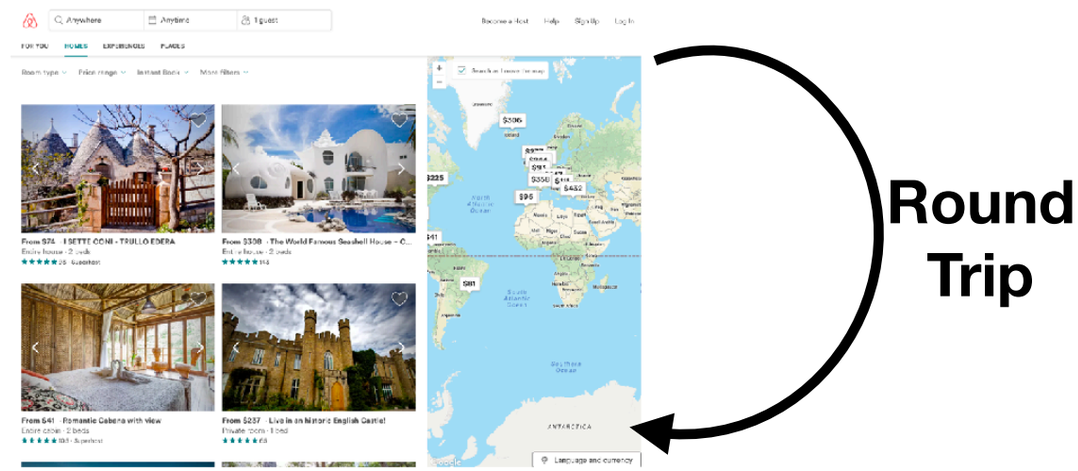
BLeak: Identifying Memory Leaks



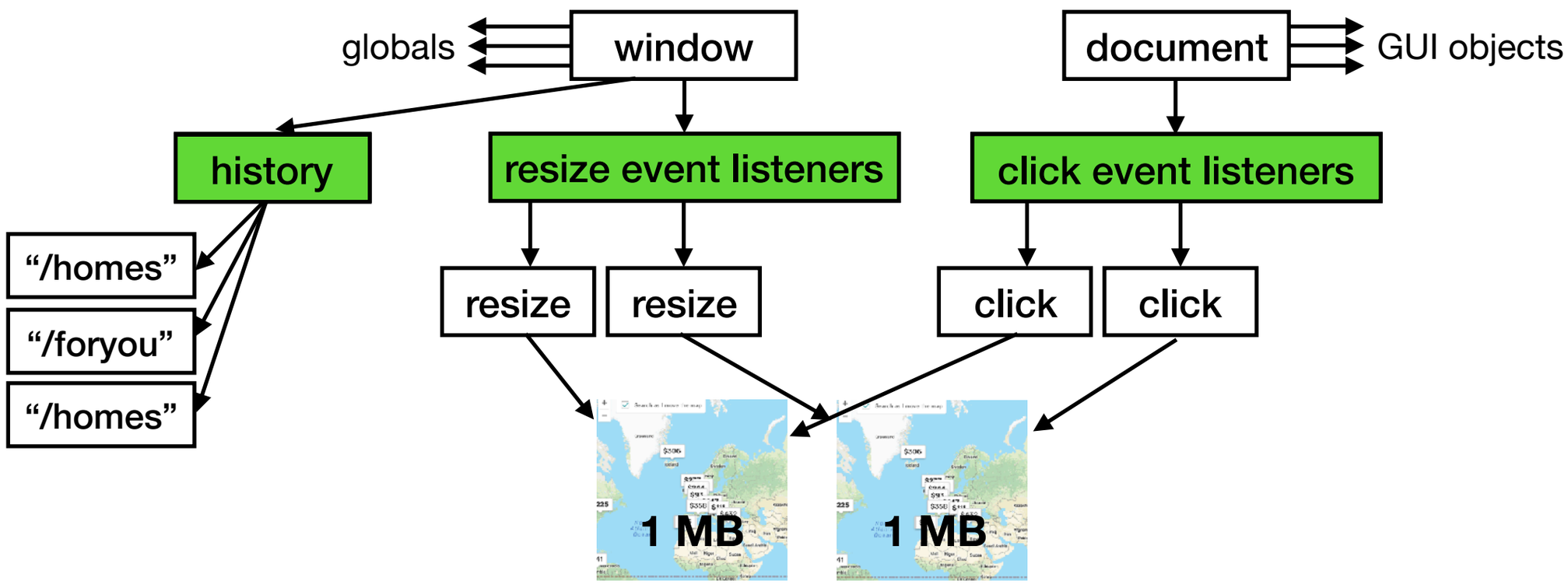
"Homes" Screen



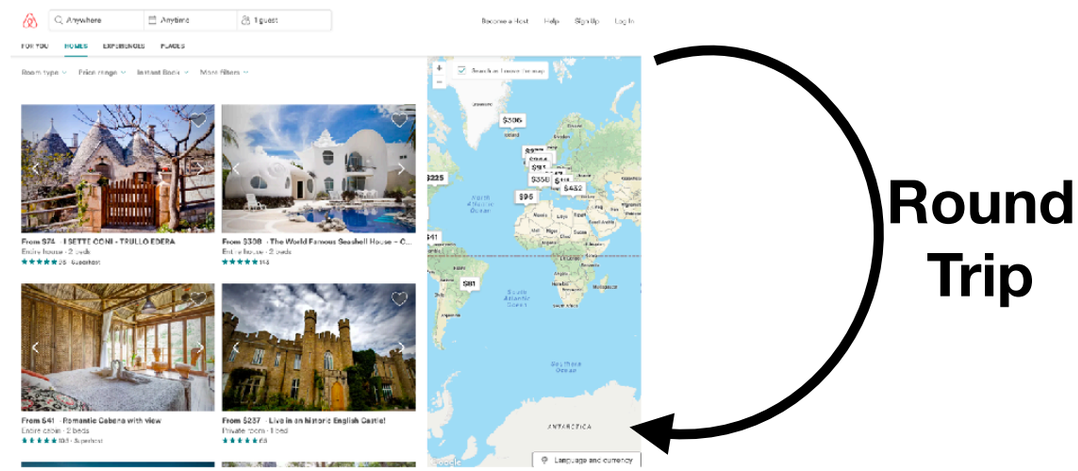
BLeak: Identifying Memory Leaks



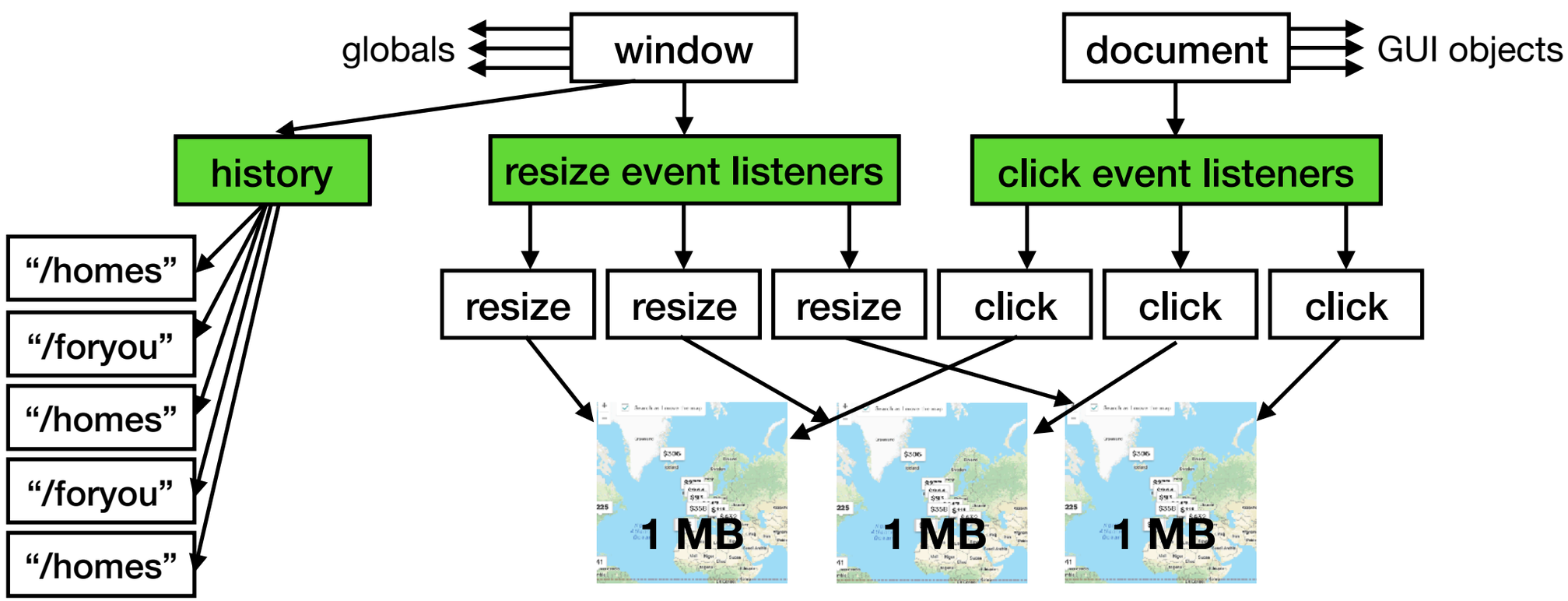
"Homes" Screen



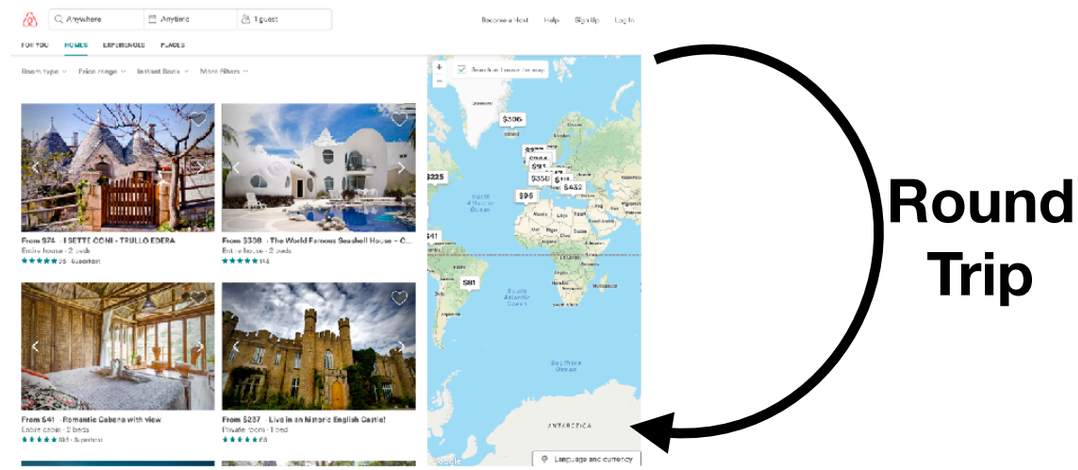
BLeak: Identifying Memory Leaks



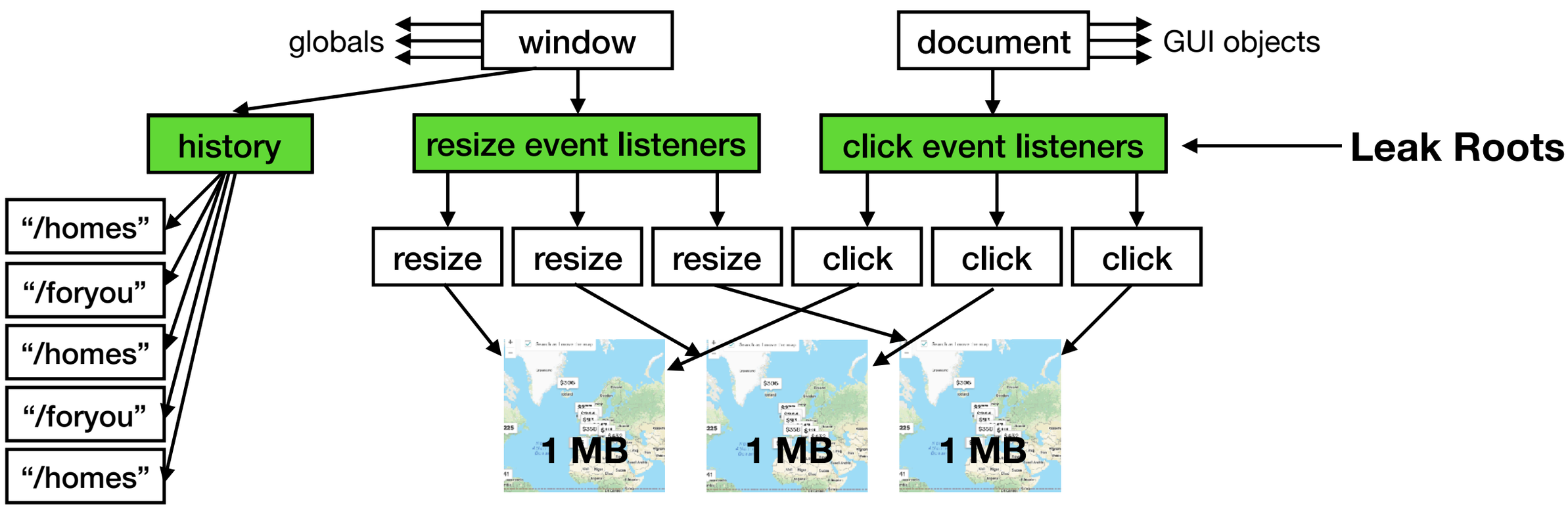
"Homes" Screen



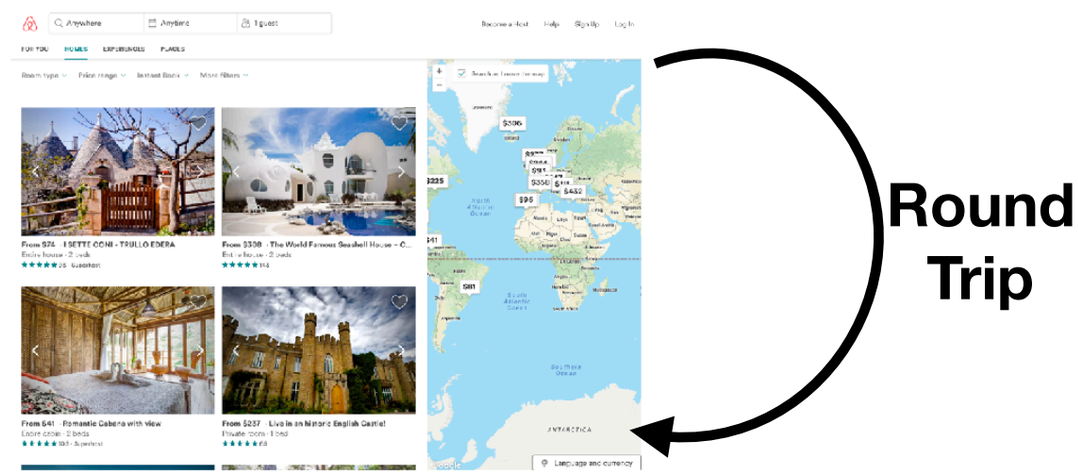
BLeak: Identifying Memory Leaks



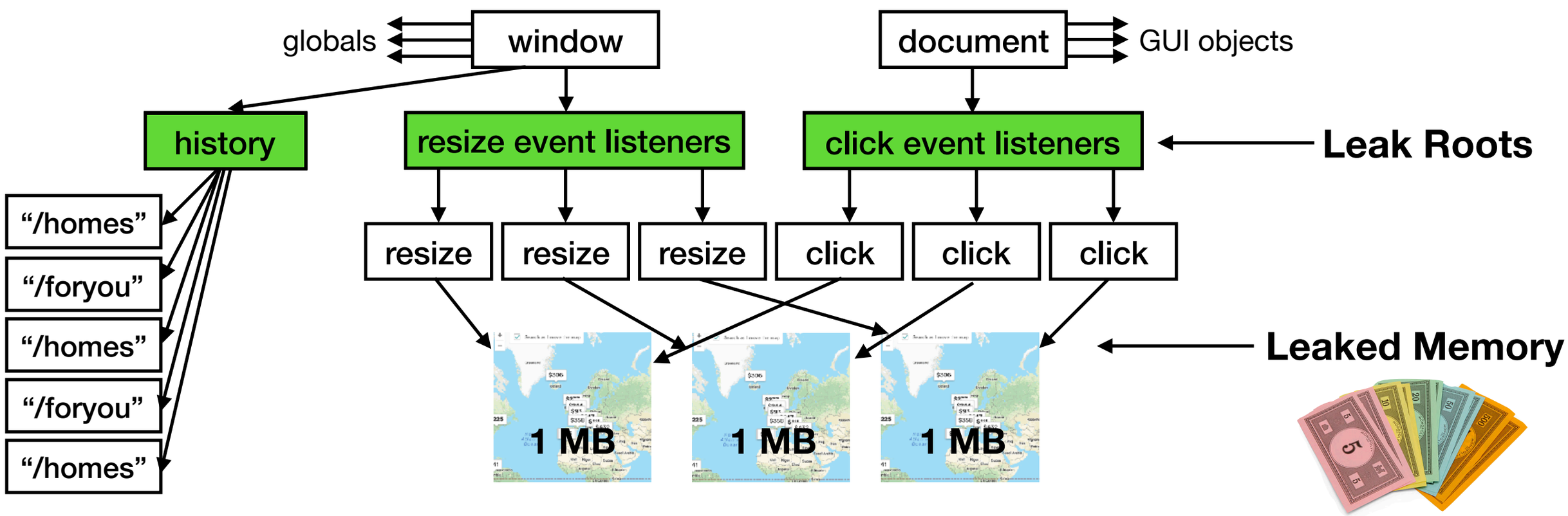
"Homes" Screen



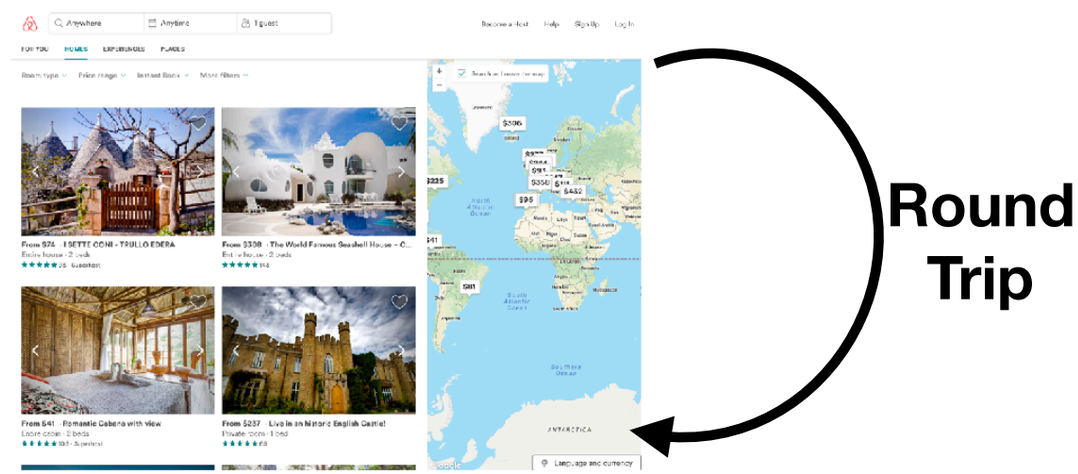
BLeak: Identifying Memory Leaks



"Homes" Screen

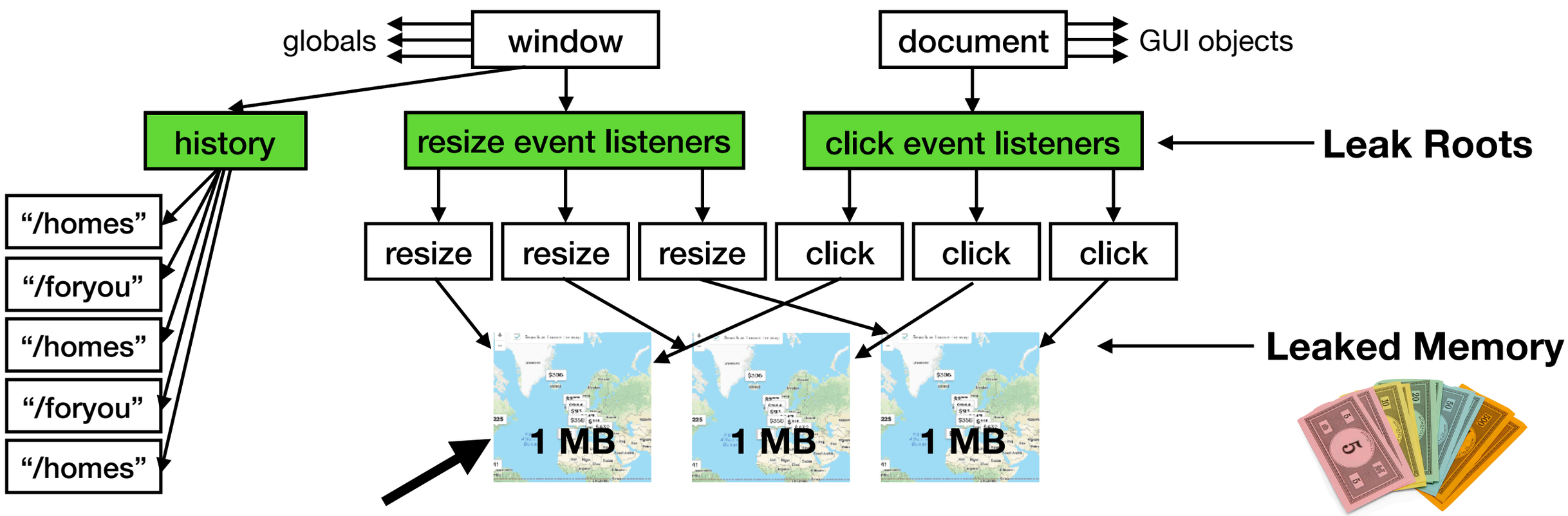


BLeak: Identifying Memory Leaks



Round Trip

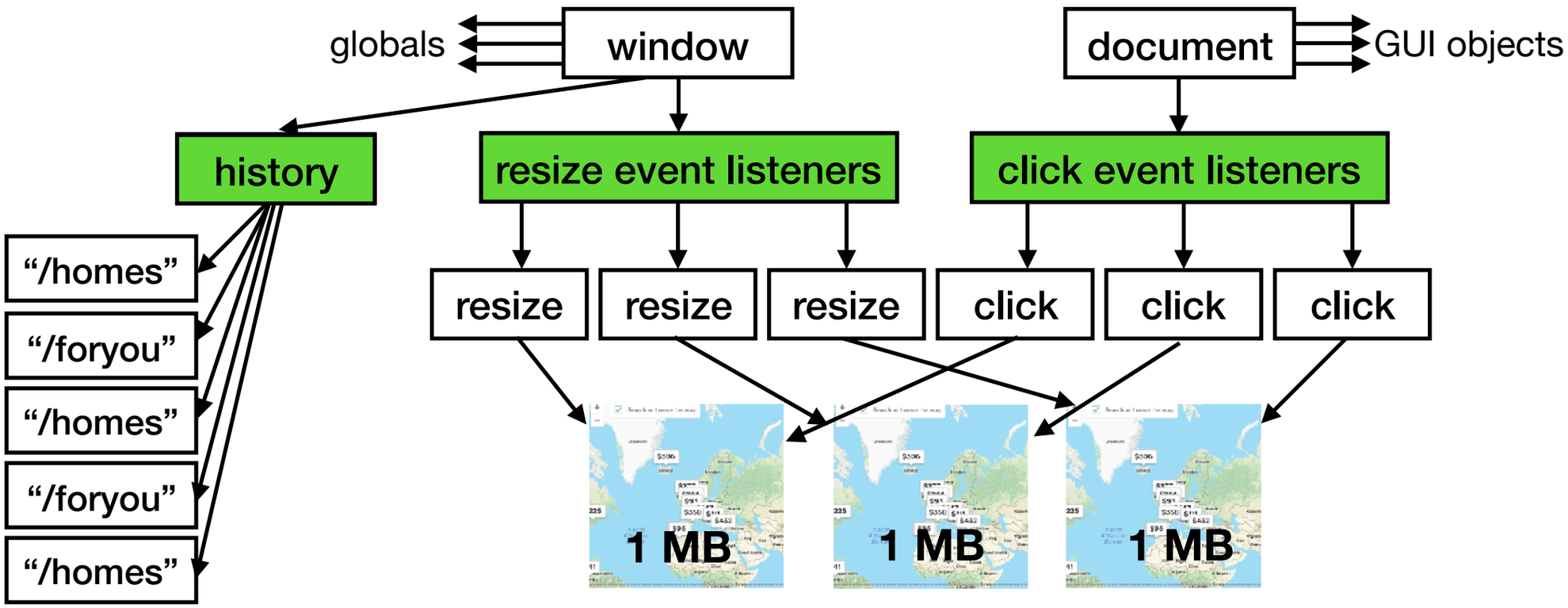
"Homes" Screen

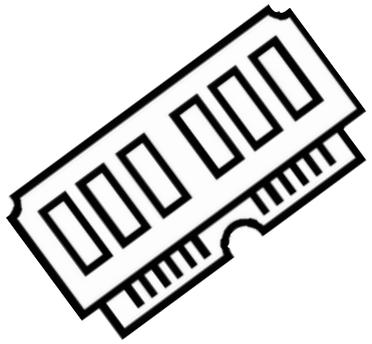


Is actually a large subgraph of small objects

Ranking Leak Roots

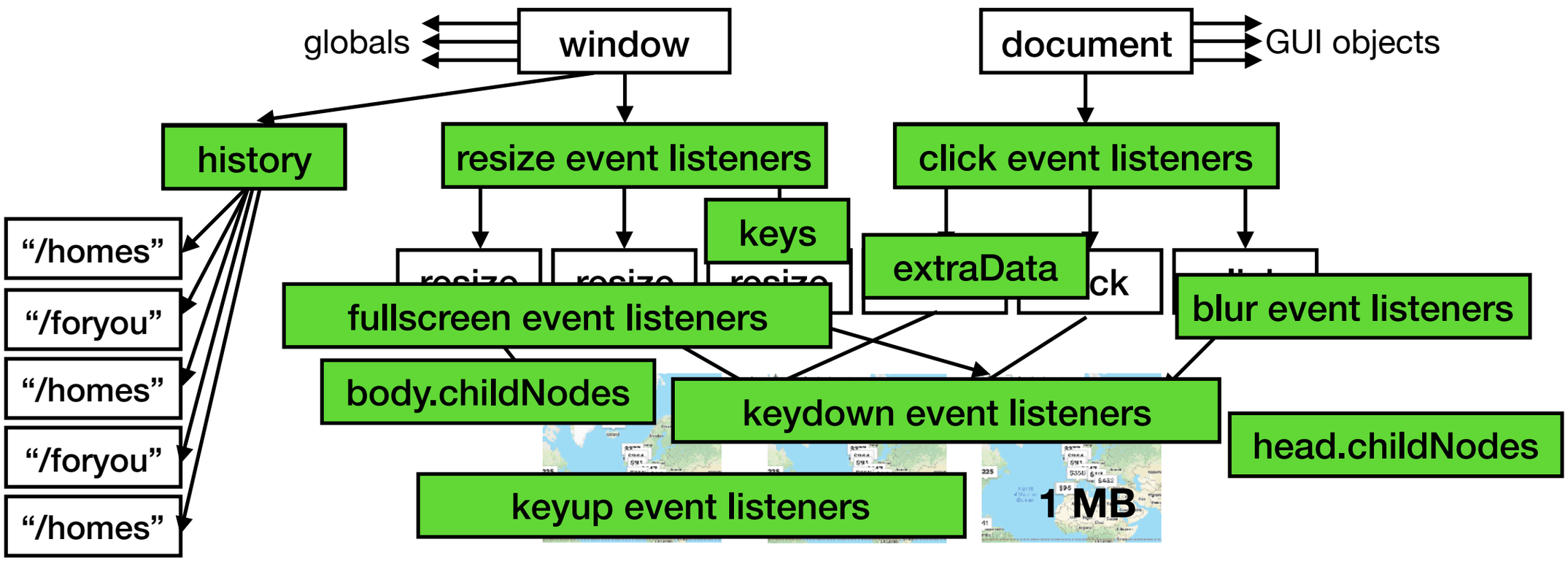
What to focus on?

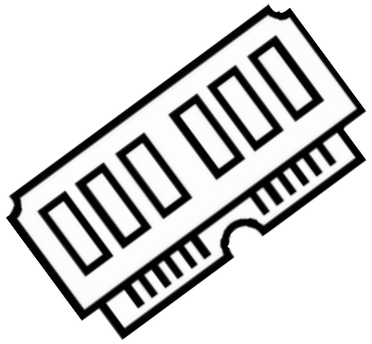




Ranking Leak Roots

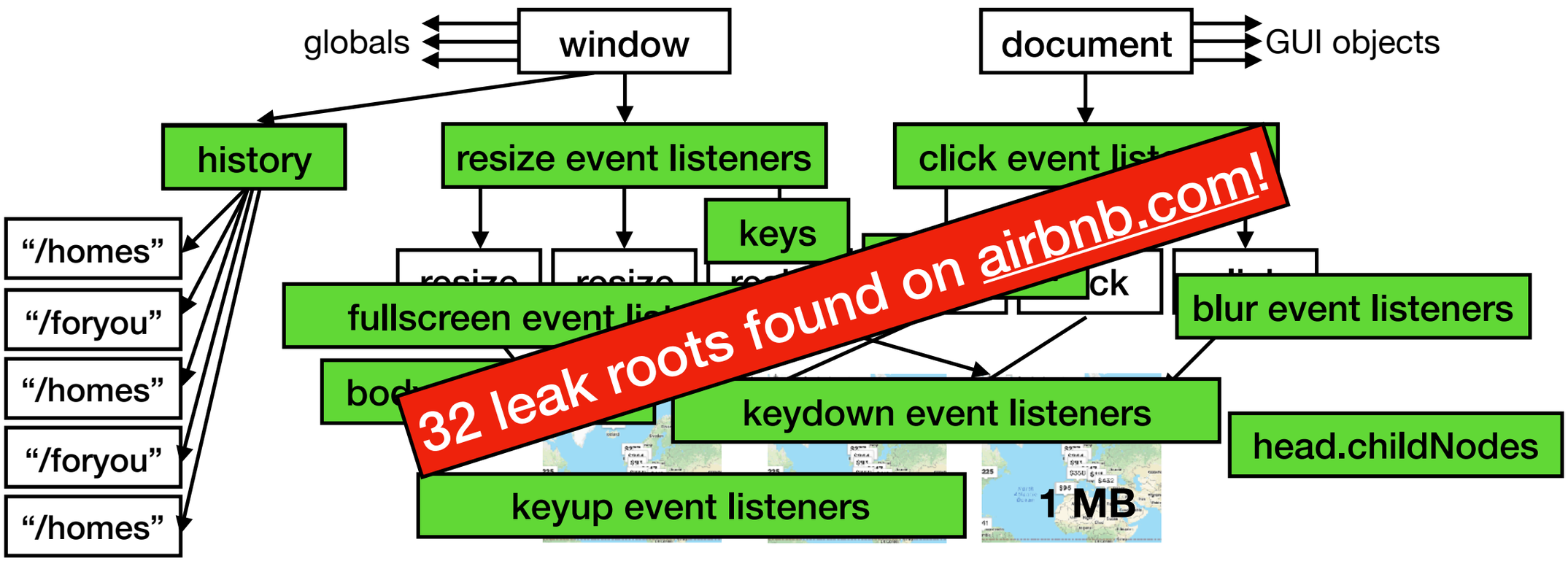
What to focus on?





Ranking Leak Roots

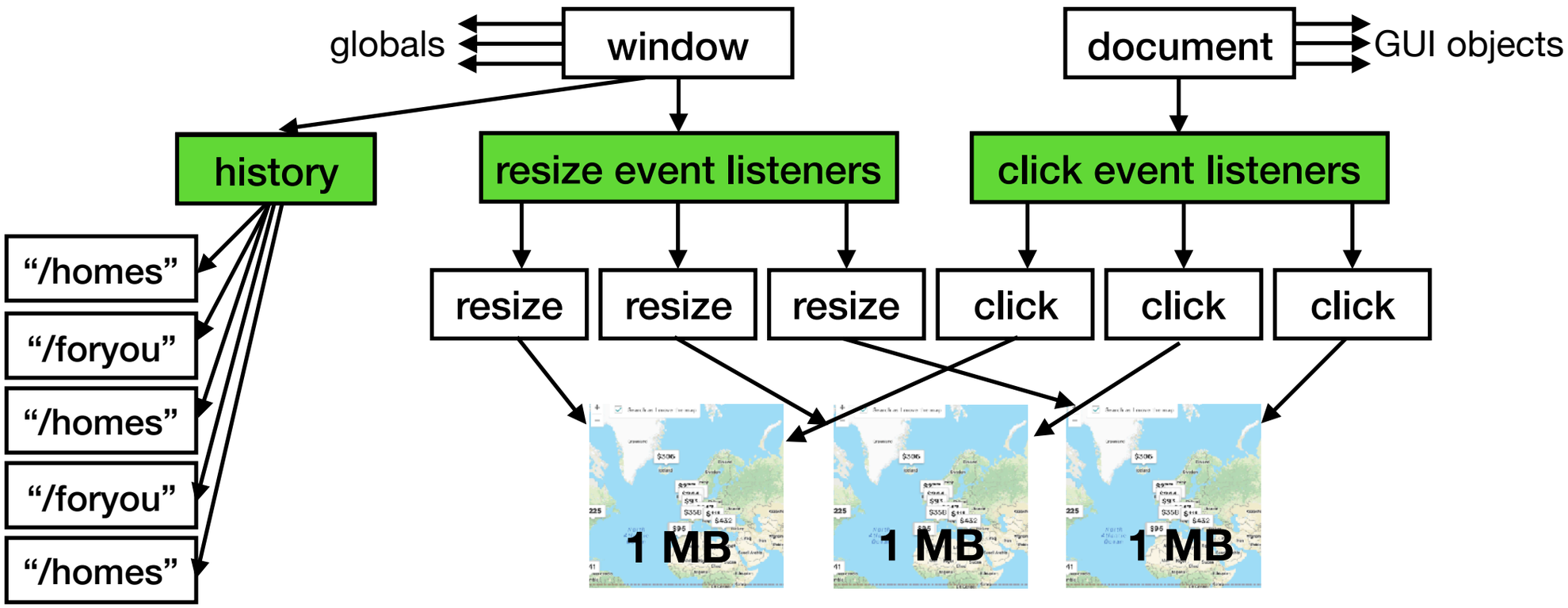
What to focus on?



Ranking Leak Roots

Retained Size (Standard Approach)

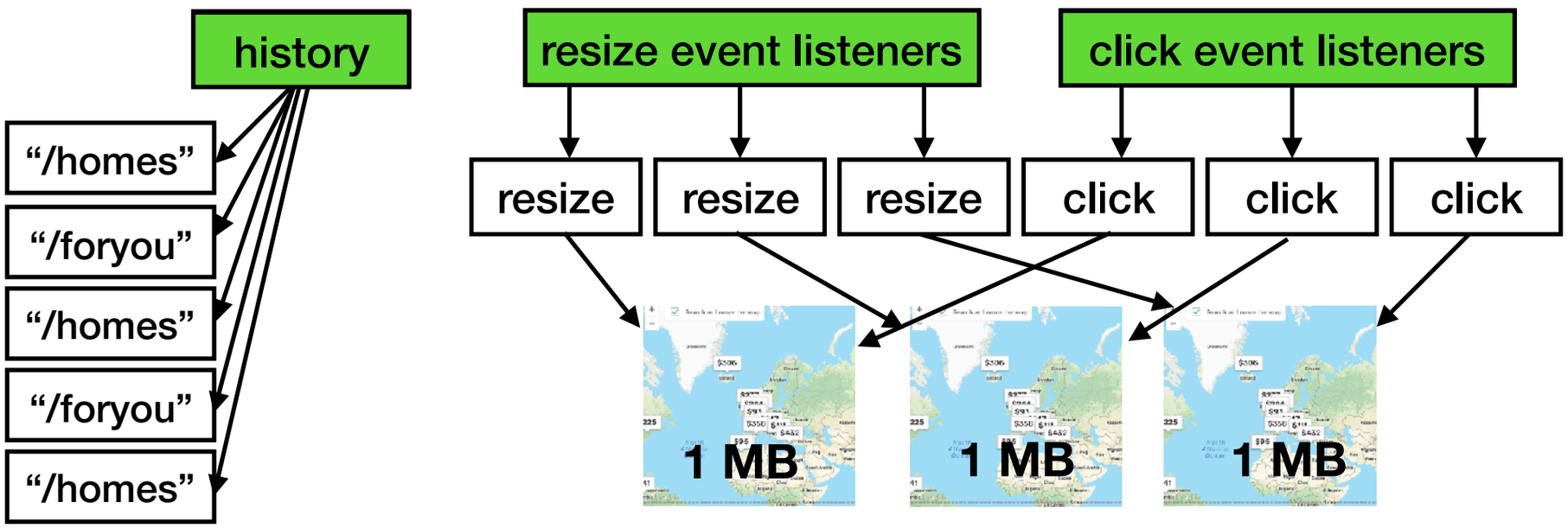
"The quantity of memory the object preserves from garbage collection"



Ranking Leak Roots

Retained Size (Standard Approach)

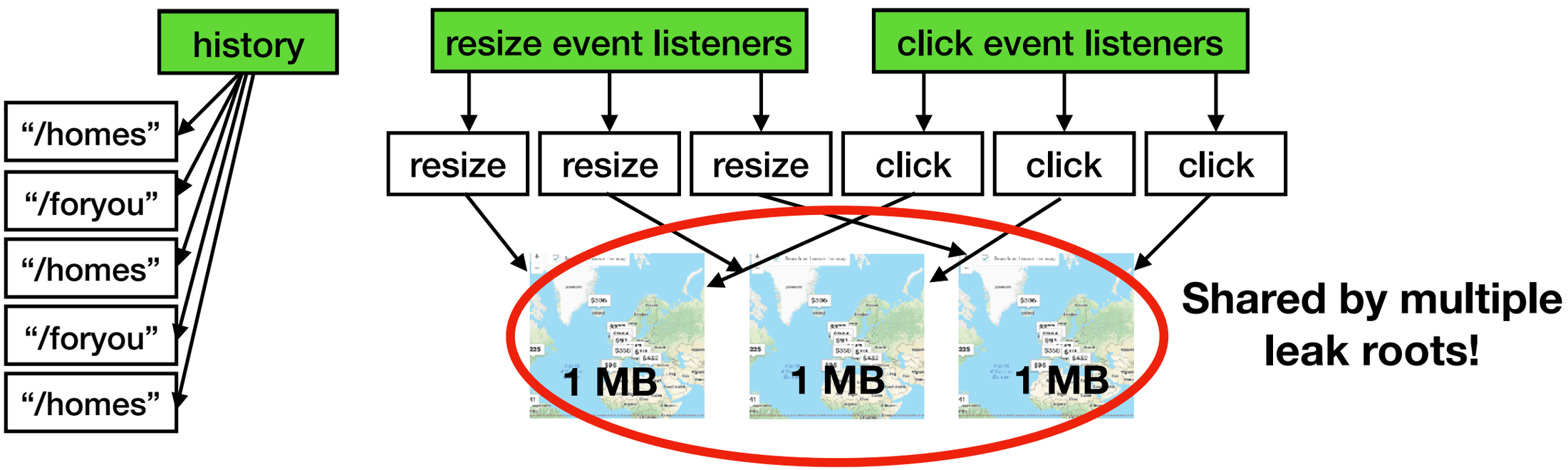
"The quantity of memory the object preserves from garbage collection"



Ranking Leak Roots

Retained Size (Standard Approach)

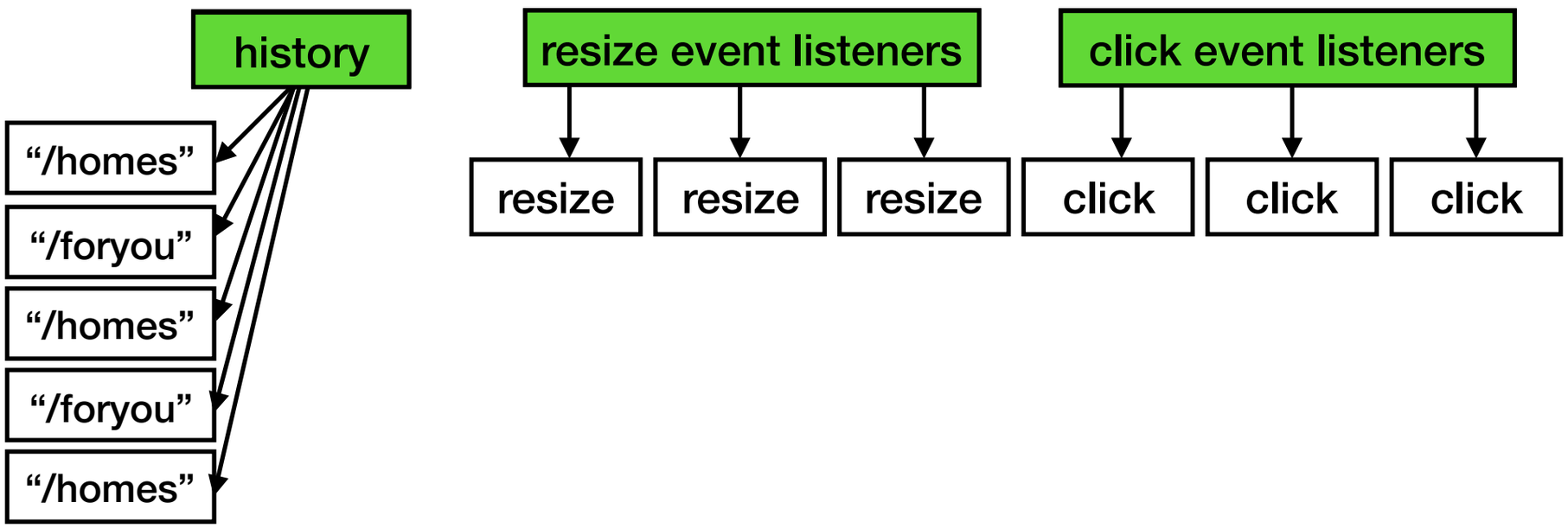
"The quantity of memory the object preserves from garbage collection"

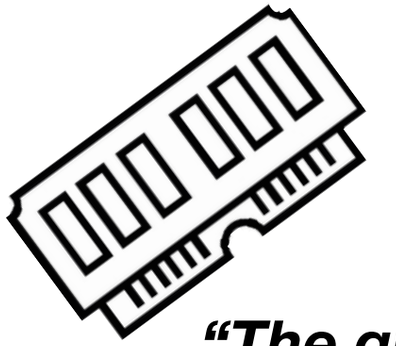


Ranking Leak Roots

Retained Size (Standard Approach)

"The quantity of memory the object preserves from garbage collection"

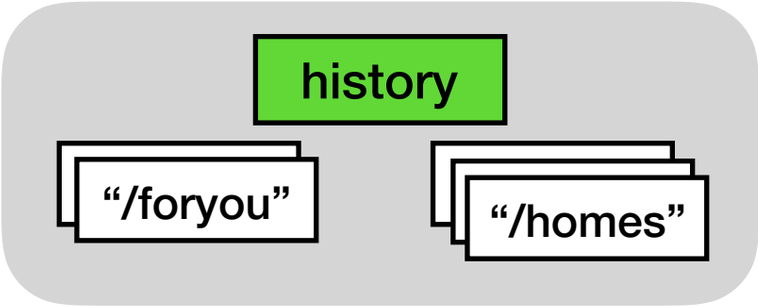




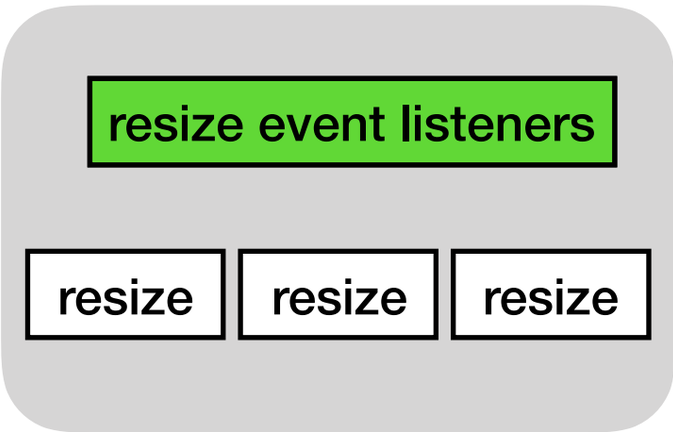
Ranking Leak Roots

Retained Size (Standard Approach)

"The quantity of memory the object preserves from garbage collection"



Retained Size: 800 bytes



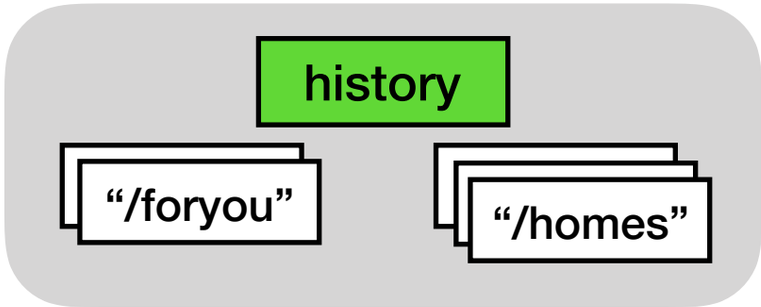
Retained Size: 400 bytes

Retained Size: 400 bytes

Ranking Leak Roots

Retained Size (Standard Approach)

"The quantity of memory the object preserves from garbage collection"



Retained Size: 800 bytes

Retained size misrepresents impact of leaks!

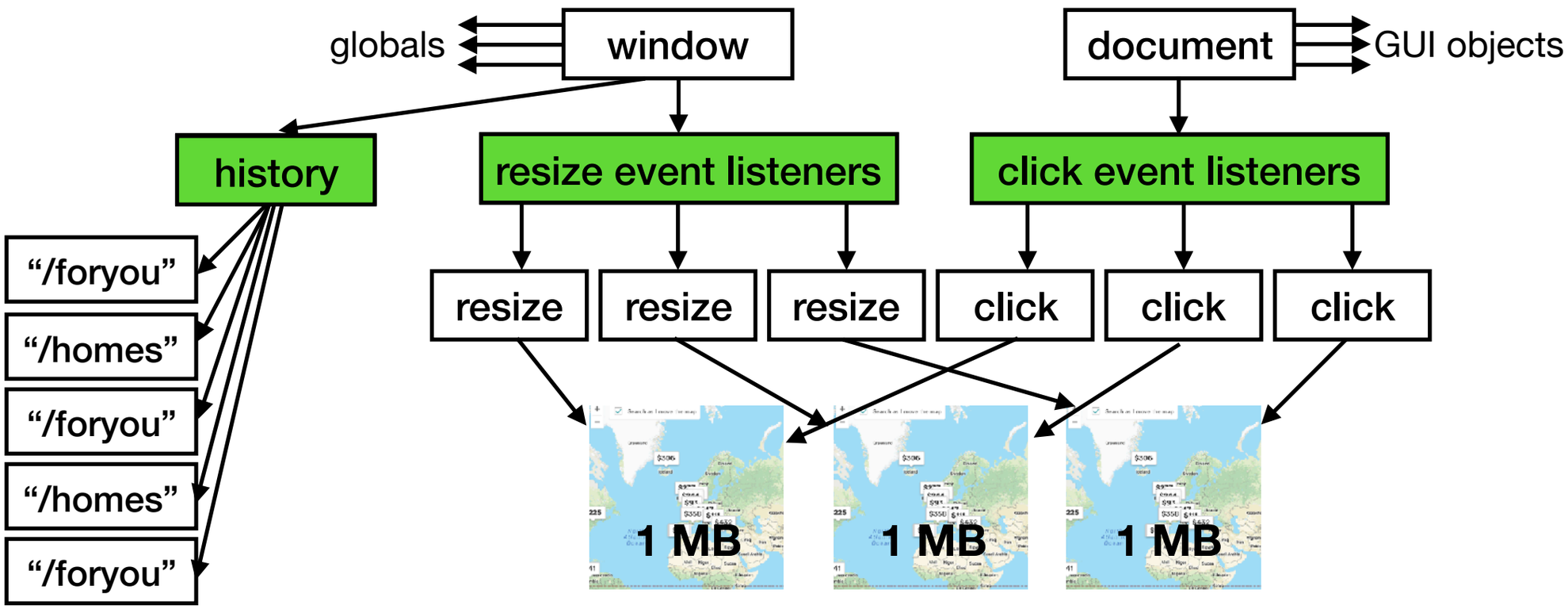
Retained Size: 400 bytes

Retained Size: 400 bytes

BLeak: Ranking Leak Roots

Proposal: *LeakShare*

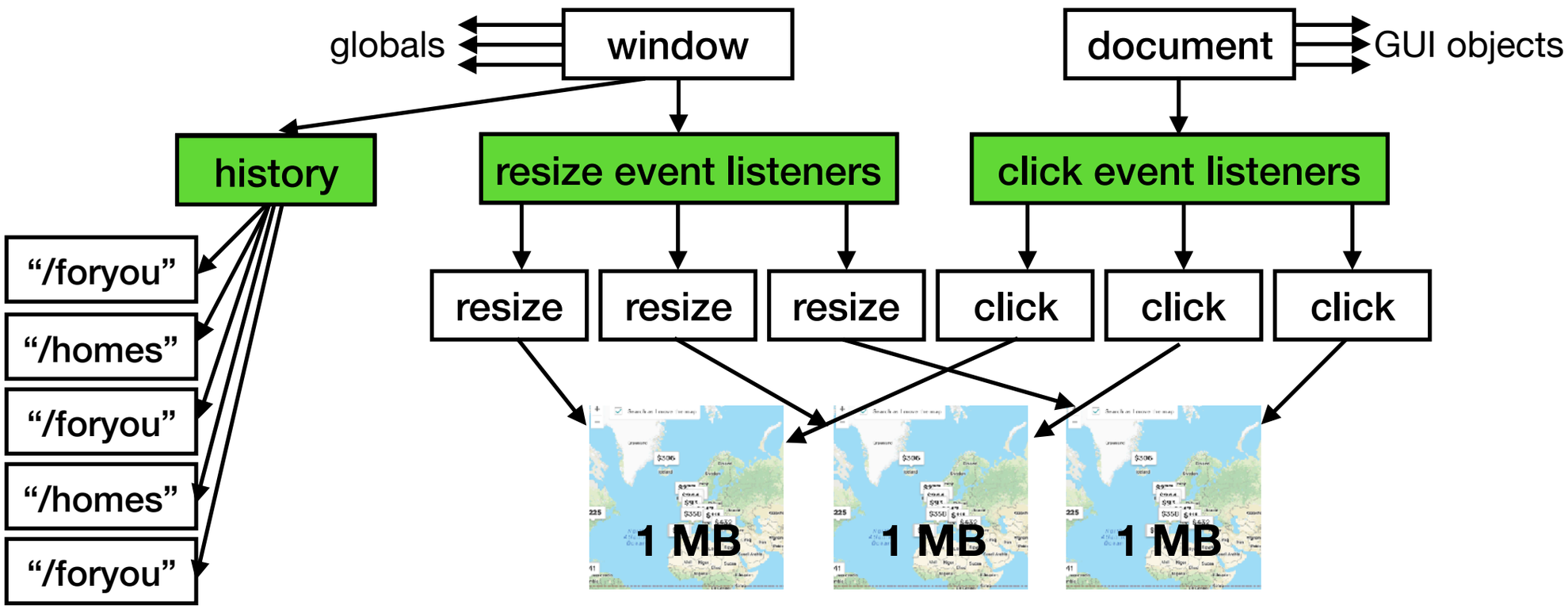
Split objects shared between leak roots



BLeak: Ranking Leak Roots

Proposal: *LeakShare*

Split objects shared between leak roots

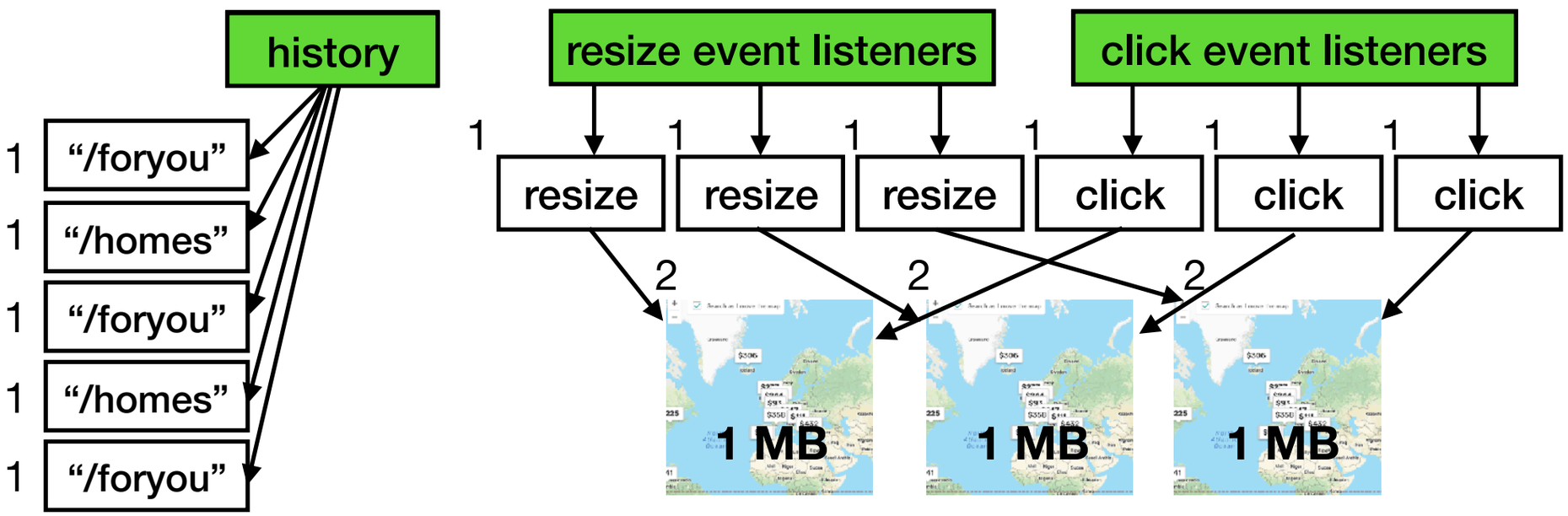


Step 1: Ignore objects reachable from non-leaks

BLeak: Ranking Leak Roots

Proposal: *LeakShare*

Split objects shared between leak roots



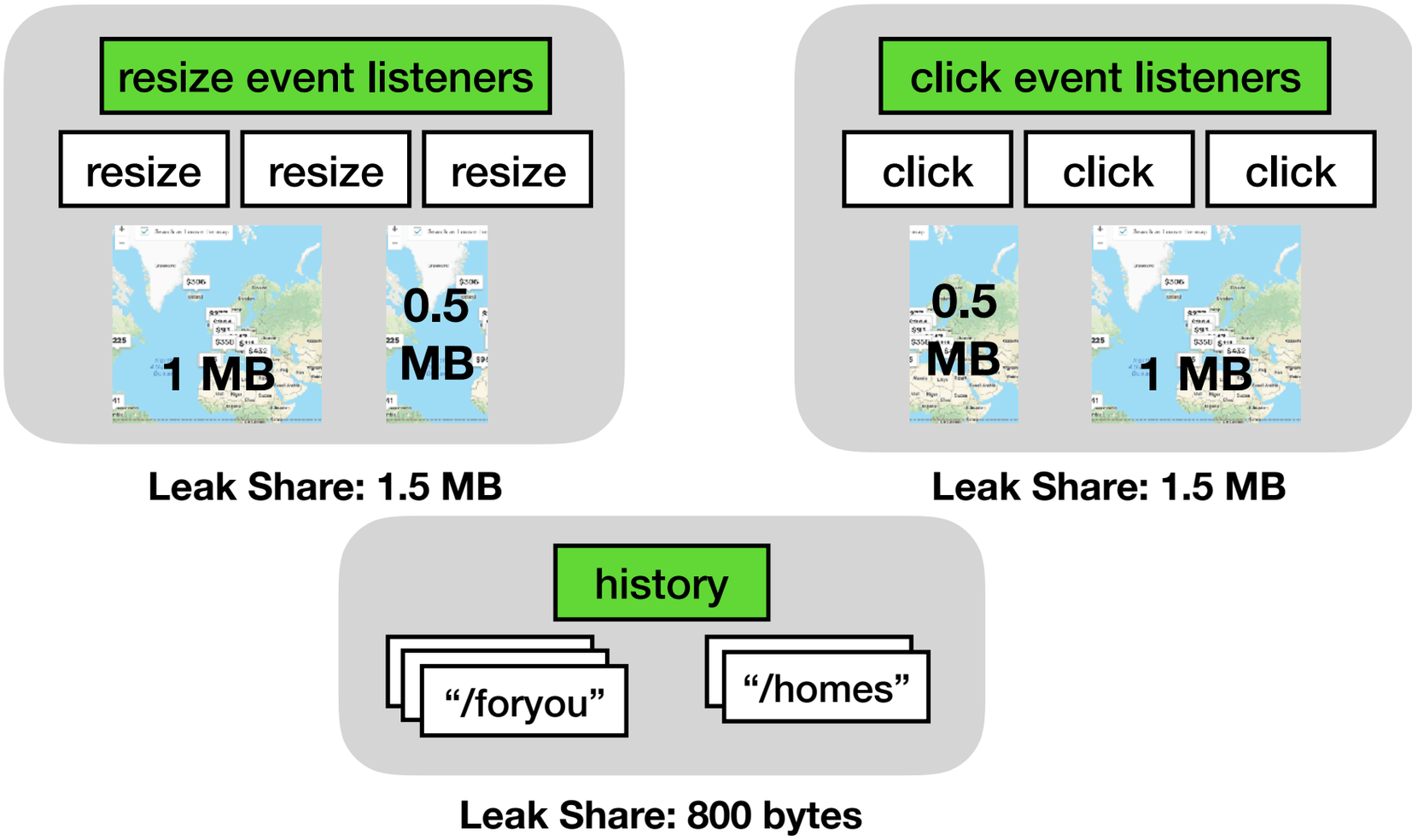
Step 1: Ignore objects reachable from non-leaks

Step 2: For each object, count number of leak roots that retain it

BLeak: Ranking Leak Roots

Proposal: *LeakShare*

Split objects shared between leak roots



Step 1: Ignore objects reachable from non-leaks

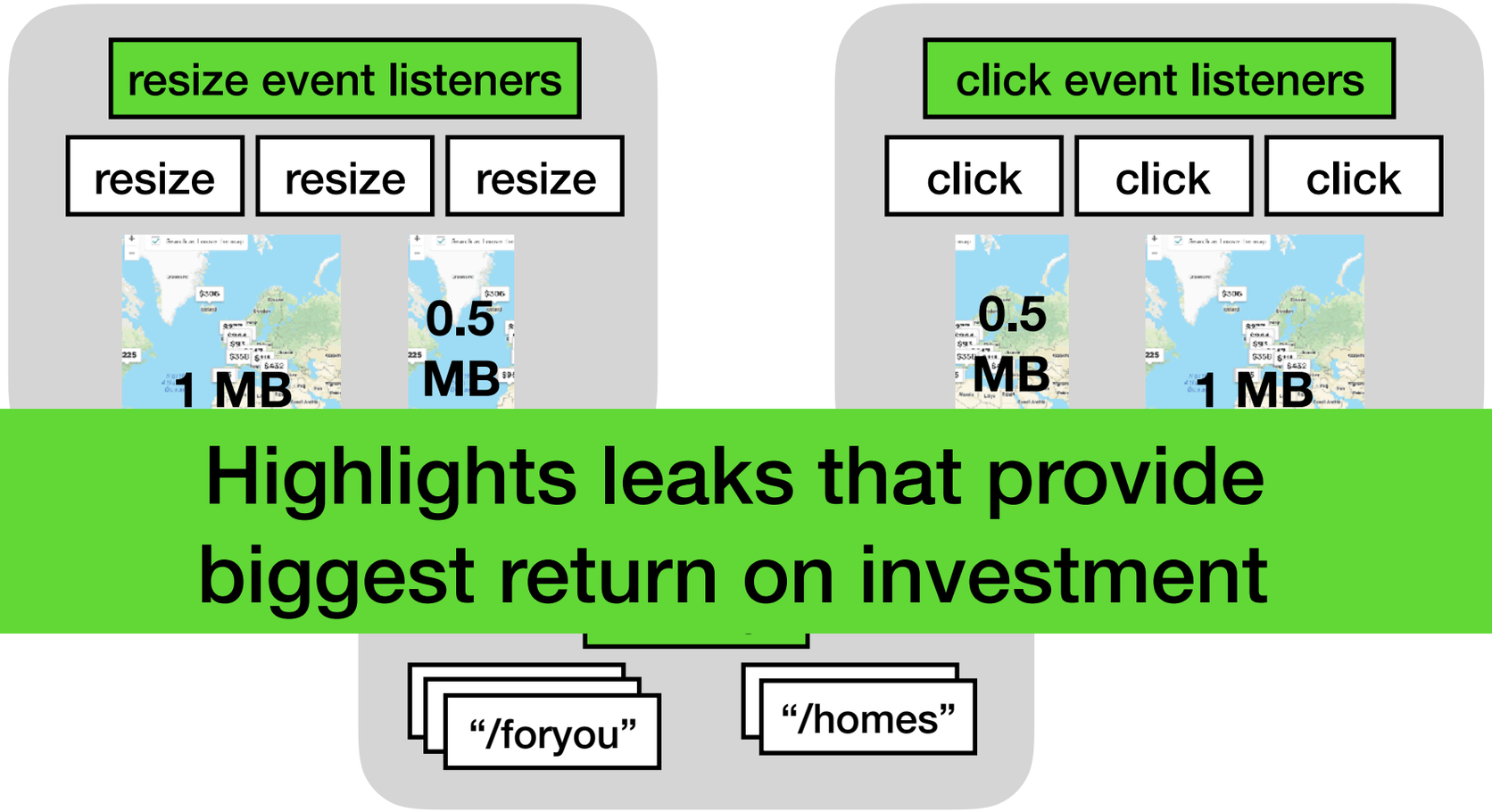
Step 2: For each object, count number of leak roots that retain it

Step 3: Split each object evenly between leak roots that retain it

BLeak: Ranking Leak Roots

Proposal: *LeakShare*

Split objects shared between leak roots



Highlights leaks that provide biggest return on investment

Leak Share: 800 bytes

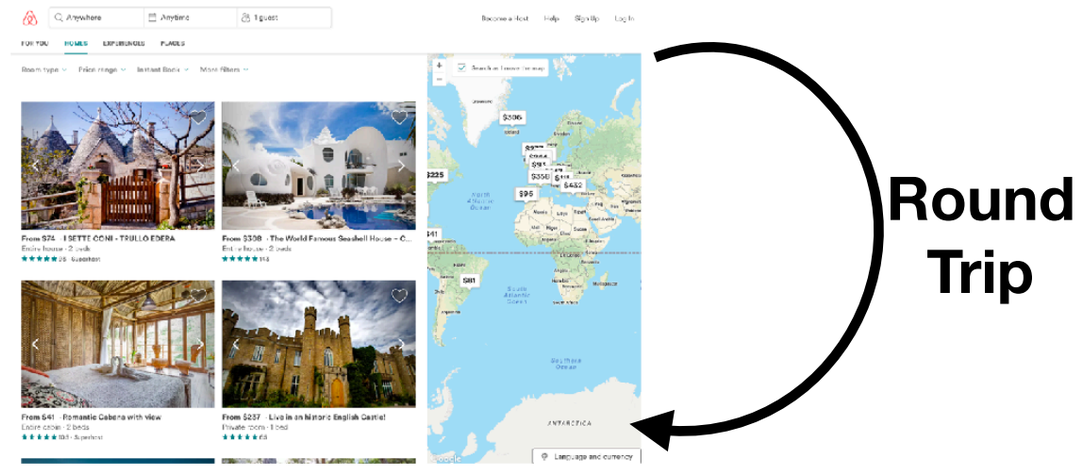
Step 1: Ignore objects reachable from non-leaks

Step 2: For each object, count number of leak roots that retain it

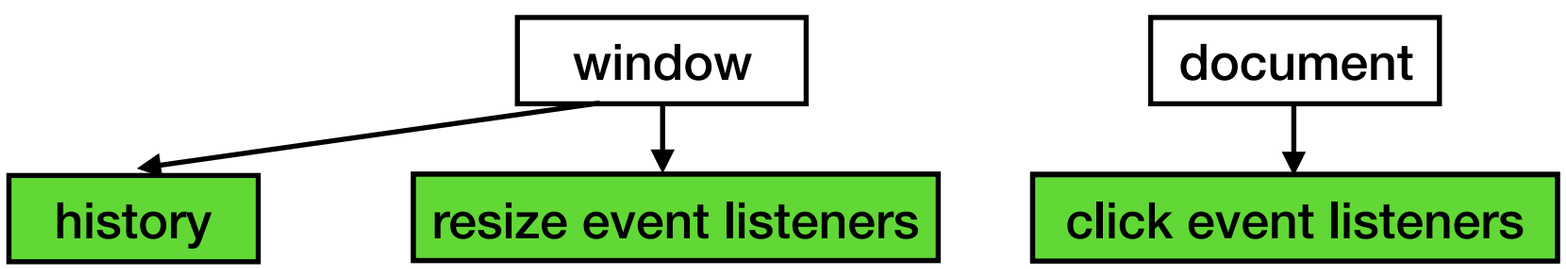
Step 3: Split each object evenly between leak roots that retain it

BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow

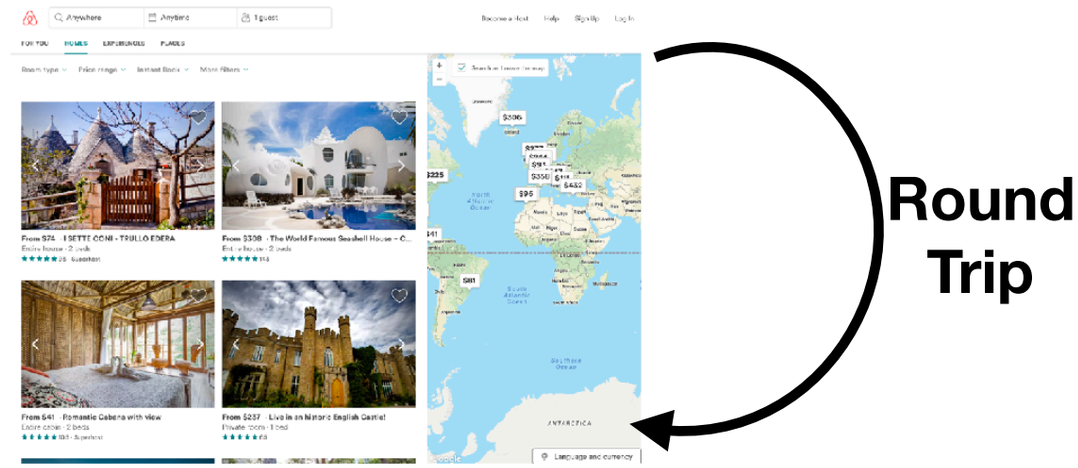


“Homes” Screen

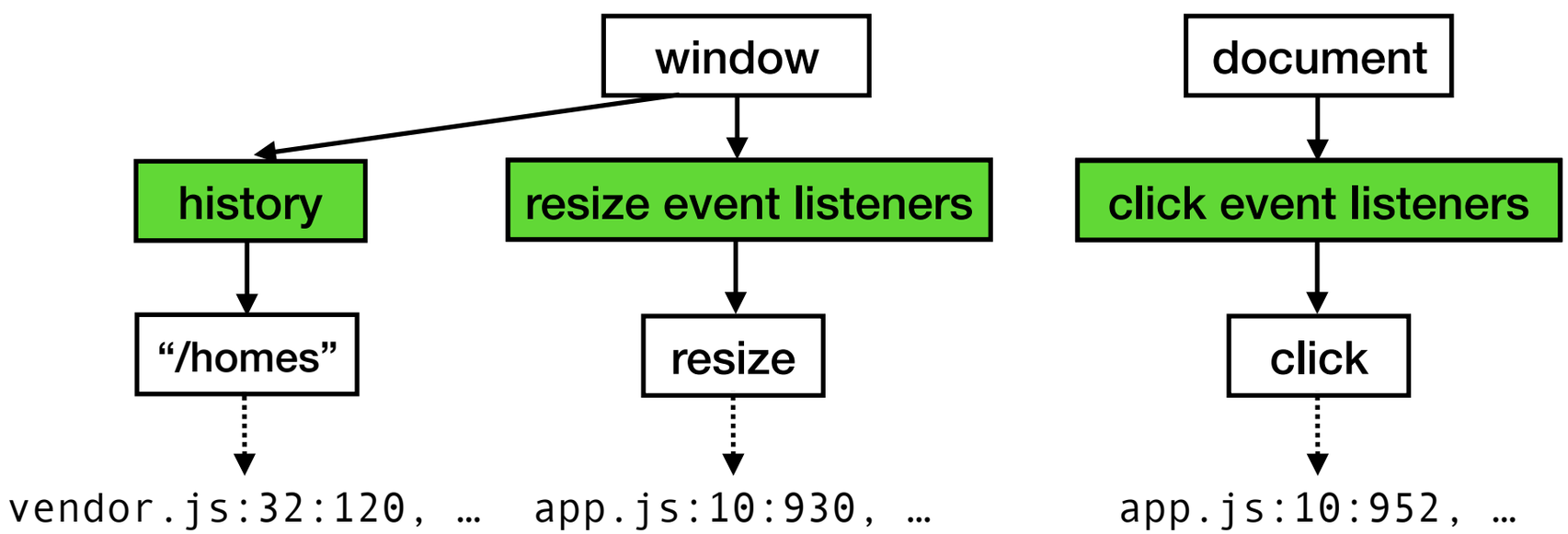


BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow

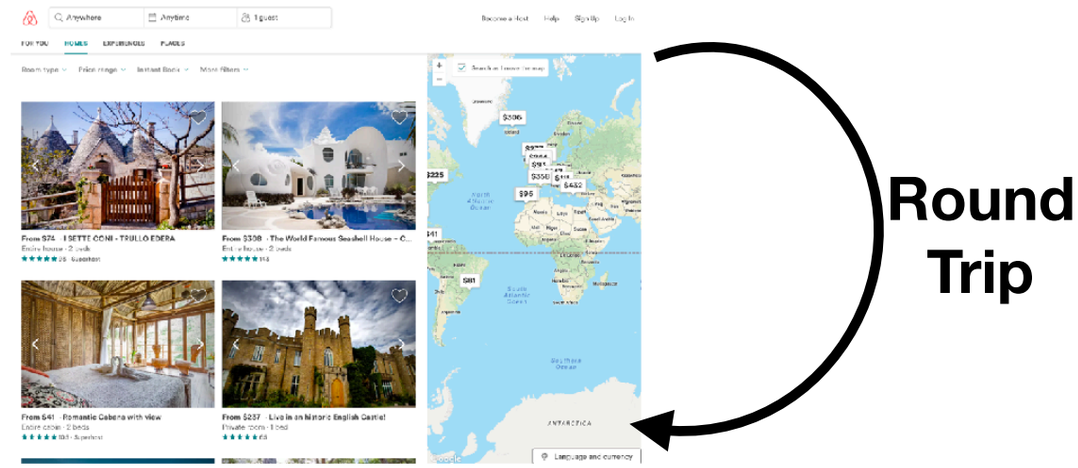


“Homes” Screen

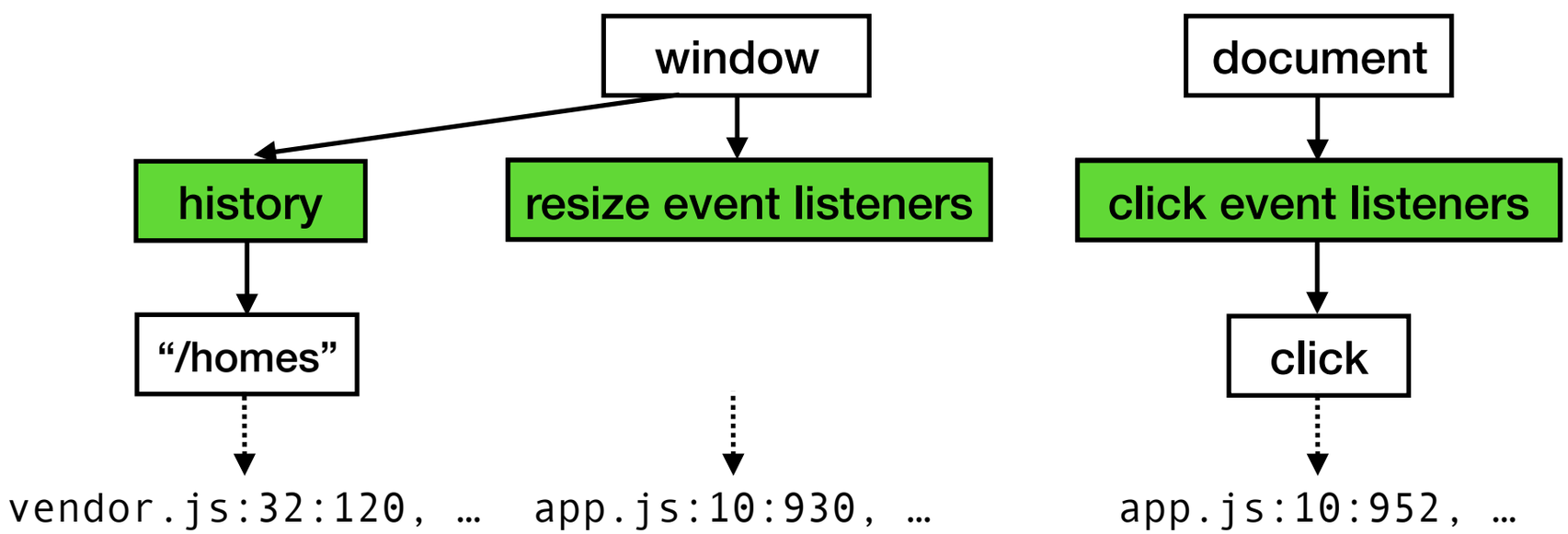


BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow

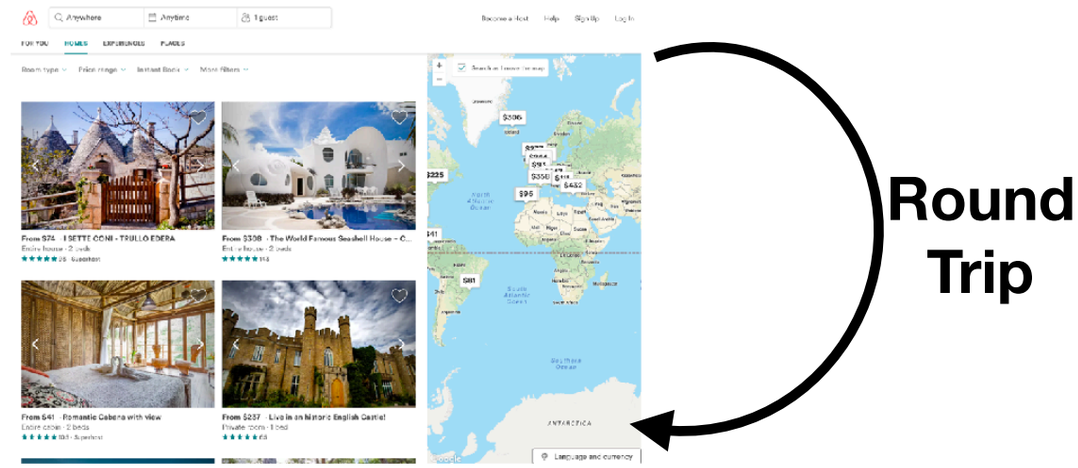


“Homes” Screen

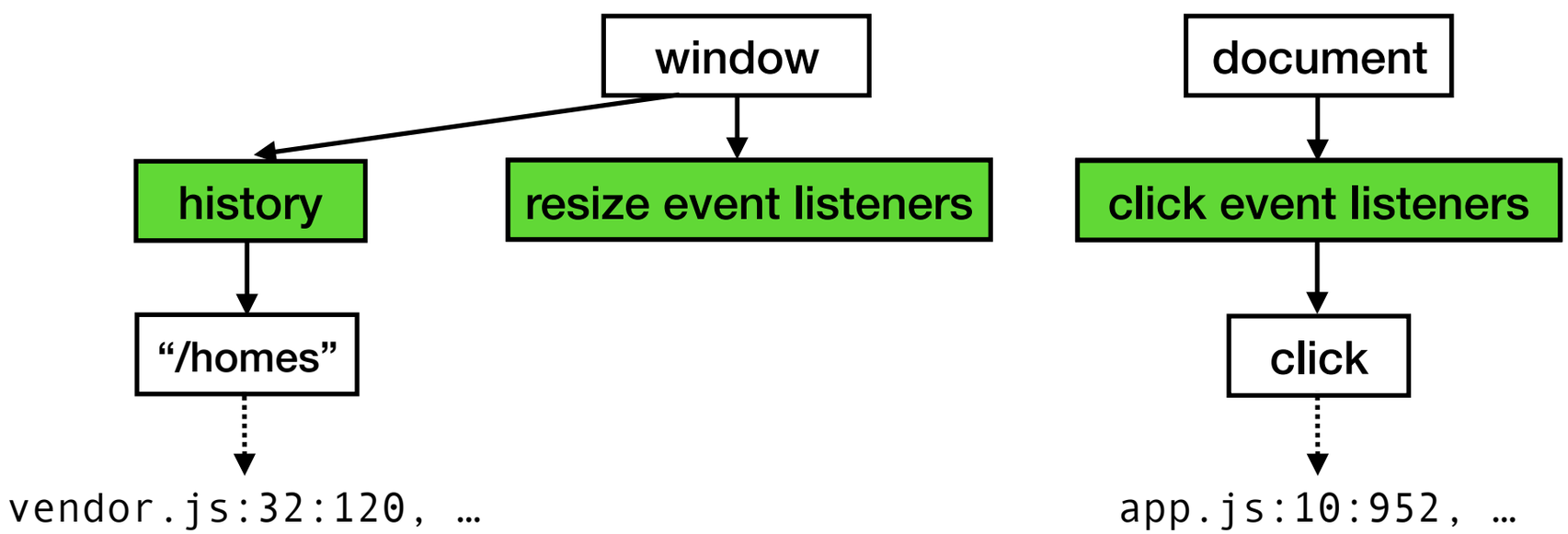


BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow

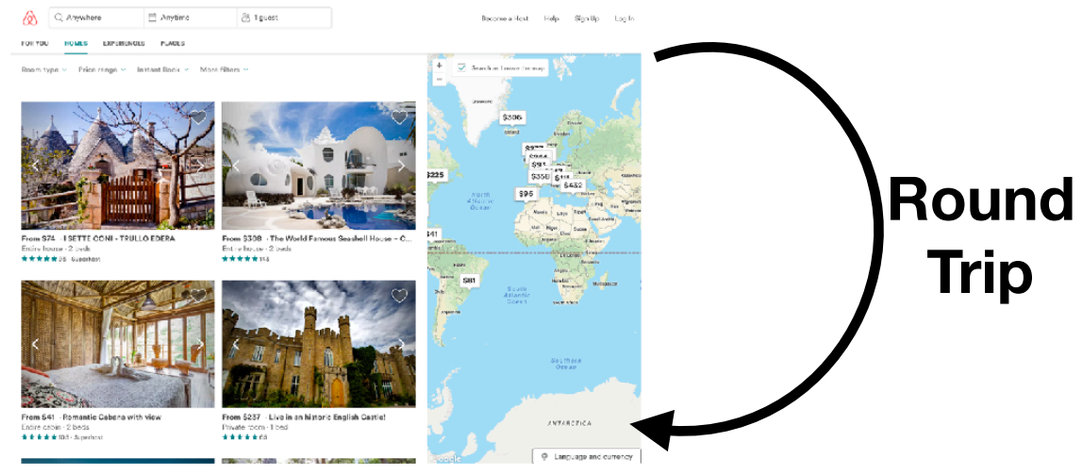


“Homes” Screen

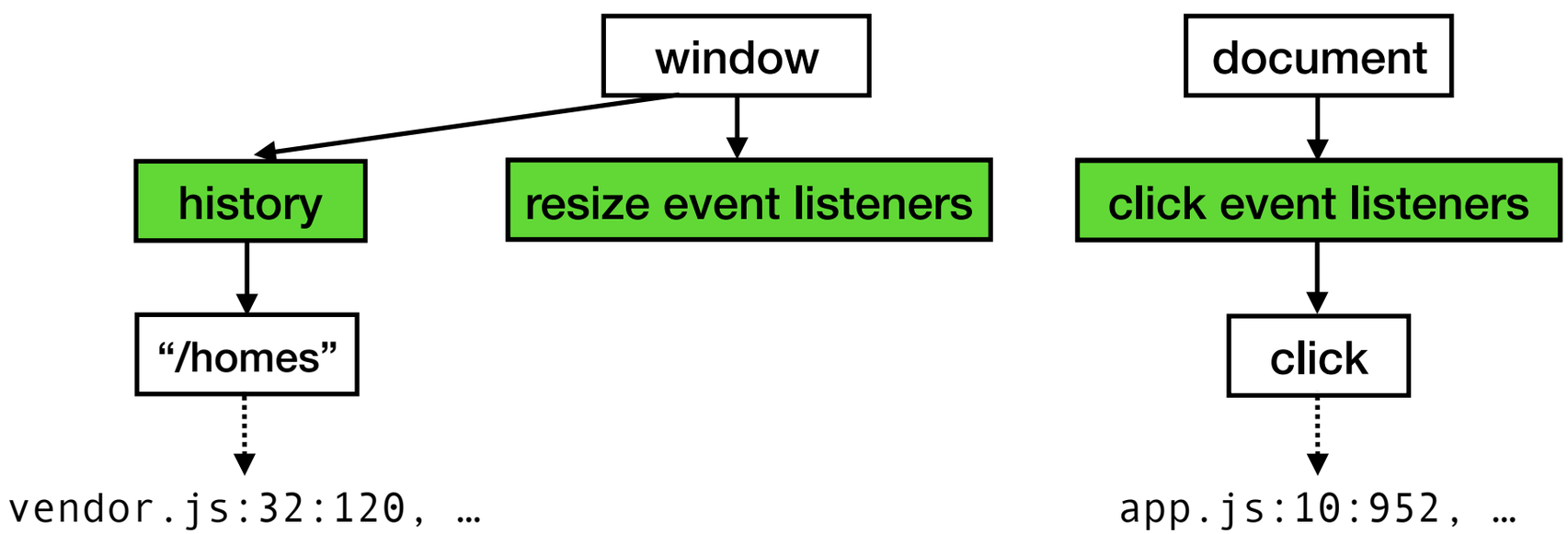


BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow



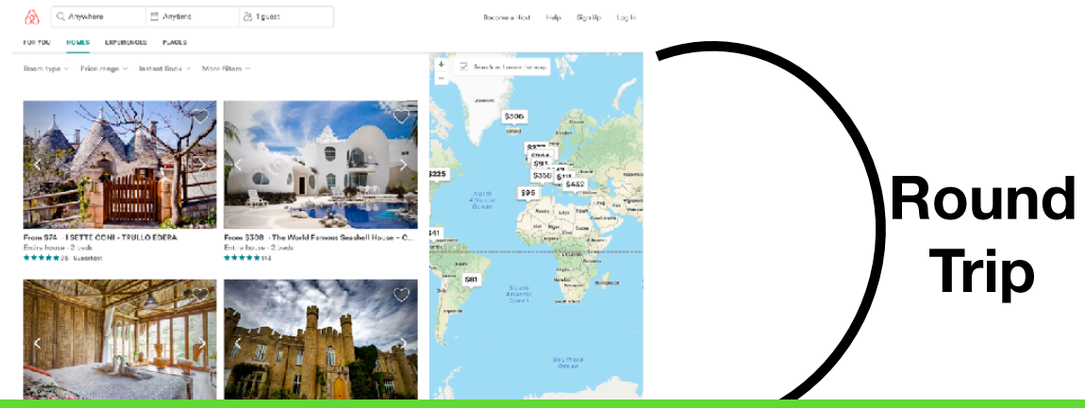
“Homes” Screen



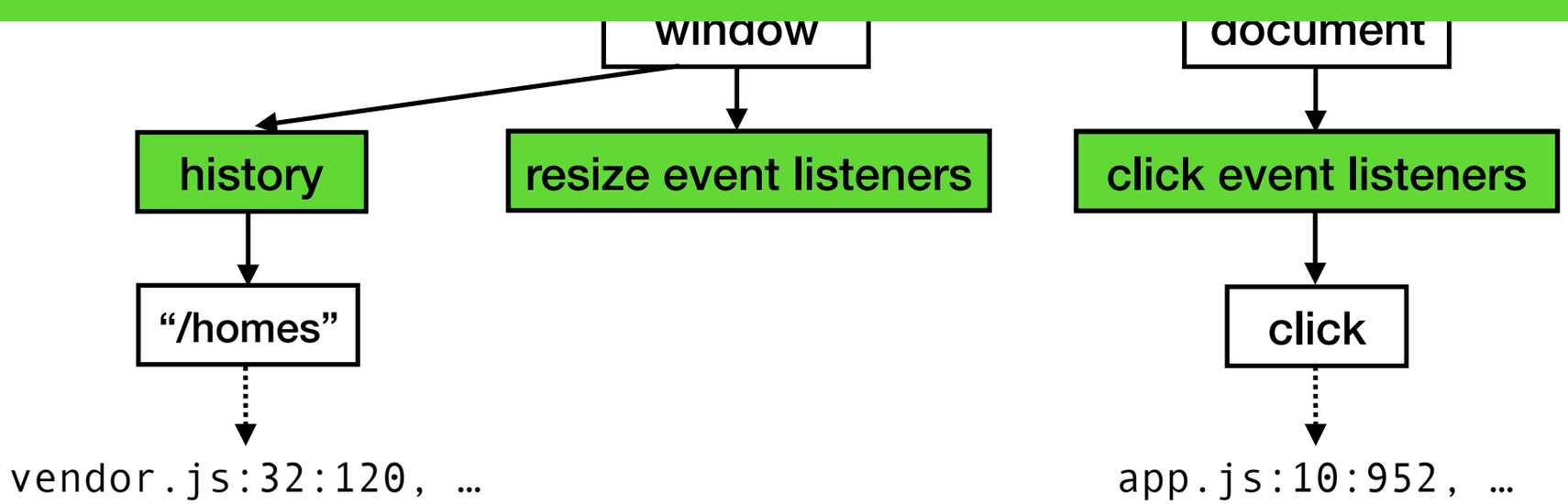
Collected via JavaScript reflection + program transformations

BLeak: Diagnosing Memory Leaks

Collect stack traces when leak roots grow



Points directly to code responsible for leaks



Collected via JavaScript reflection + program transformations

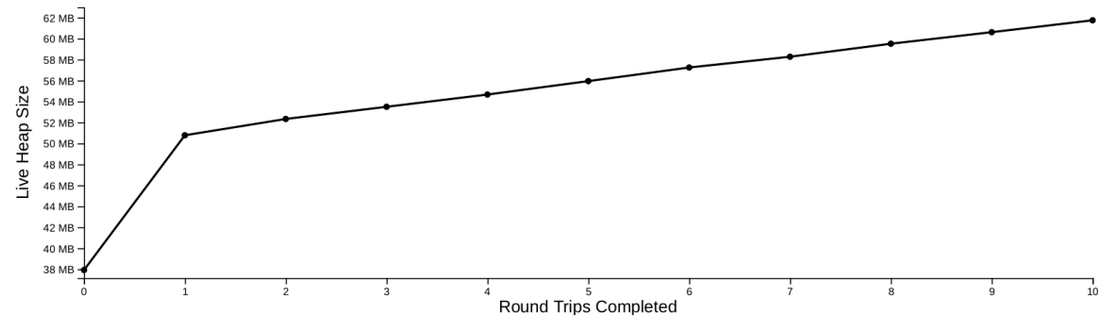
BLeak Output: airbnb.com

Report with actionable information!

Live Heap Size

Average Growth: 1.16MB / round trip, 95% CI [1.07, 1.25]

(The above stats ignore the impact of first 5 heap snapshots, which are typically noisy due to application startup + JavaScript engine warmup)



Leak Roots and Stack Traces

Rank By: LeakShare

- Score 389216 document.childNodes[3].childNodes[3].childNodes
- Score 214611 window.$$listeners.blur
- Score 212459 window.$$listeners.resize
- Score 211235 List of 'click' listeners on document
- Score 209811 window.$$listeners.scroll
- Score 209219 List of 'keydown' listeners on document
- Score 209211 List of 'keypress' listeners on document
- Score 209155 document.__e3_.keydown
- Score 209051 List of 'keyup' listeners on document
- Score 208803 window.__e3_.resize
- Score 208771 document.__e3_.keyup
- Score 208771 document.__e3_.click
- Score 208771 window.__e3_.blur
- Score 208771 document.__e3_.keypress
- Score 204339 List of 'MSFullscreenChange' listeners on document
- Score 204339 List of 'fullscreenchange' listeners on document
- Score 204339 List of 'webkitfullscreenchange' listeners on document
- Score 204339 List of 'mozfullscreenchange' listeners on document
- Score 204323 document.__e3_.fullscreenchange

Source Code

- ▼ https://a0.muscache.com
  - ▼ airbnb/static
    - ► packages
    - HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js
    - webcot-ForYouContainer_async-async-bb0ac06dfcf5e3524101.js
- ► https://www.airbnb.com
- ► https://maps.googleapis.com
- ► https://www.googleadservices.com
- ► https://www.google-analytics.com
- ► https://sslwidget.criteo.com
- ► https://www.googletagmanager.com
- ► https://static.criteo.net

https://a0.muscache.com/airbnb/static/HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js (Pretty Printed)

View Original

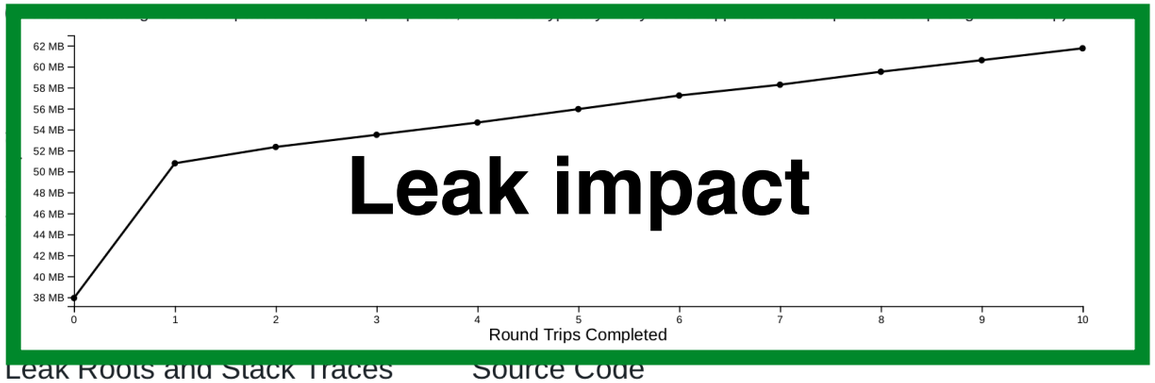
```
window.__MEMFIX__ = function() {
  return true;
}
;
!function() {
  var e = webpackJsonp([690], {
    "/jFZ": function(e, t) {
      function n(e) {
        var t = 0
          , n = 0
          , i = 0
          , r = ""
          , a = void 0
          , s = void 0;
        for (t = 0; t < e.length; ++t) {
          var l = babelHelpers.slicedToArray(e[t], 2);
          a = l[0],
          s = l[1],
          r += o(n, i, a, s),
          n = a,
          i = s
        }
        return r += o(n, i, e[0][0], e[0][1])
      }
      function o(e, t, n, o) {
        var r = Math.round(1e5 * n)
          , a = Math.round(1e5 * e)
          , s = Math.round(1e5 * o)
          , l = Math.round(1e5 * t)
          , u = s - l;
        return i(r - a) + i(u)
      }
      function i(e) {
        var t = e << 1;
        return e < 0 && (t = ~t),
        r(t)
      }
      function r(e) {
        for (var t = ""; e >= 32; )
          t += String.fromCharCode(63 + (32 | 31 & e)),
```

BLeak Output: airbnb.com

Report with actionable information!

Live Heap Size

Average Growth: 1.16MB / round trip, 95% CI [1.07, 1.25]



Leak Roots and Stack Traces

Rank By: LeakShare

- Score 389216 document.childNodes[3].childNodes[3].childNodes
- Score 214611 window.$$listeners.blur
- Score 212459 window.$$listeners.resize
- Score 211235 List of 'click' listeners on document
- Score 209811 window.$$listeners.scroll
- Score 209219 List of 'keydown' listeners on document
- Score 209211 List of 'keypress' listeners on document
- Score 209155 document.__e3_.keydown
- Score 209051 List of 'keyup' listeners on document
- Score 208803 window.__e3_.resize
- Score 208771 document.__e3_.keyup
- Score 208771 document.__e3_.click
- Score 208771 window.__e3_.blur
- Score 208771 document.__e3_.keypress
- Score 204339 List of 'MSFullscreenChange' listeners on document
- Score 204339 List of 'fullscreenchange' listeners on document
- Score 204339 List of 'webkitfullscreenchange' listeners on document
- Score 204339 List of 'mozfullscreenchange' listeners on document
- Score 204323 document.__e3_.fullscreenchange

Source Code

- ▼ https://a0.muscache.com
  - ▼ airbnb/static
    - ► packages
    - HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js
    - webcot-ForYouContainer_async-async-bb0ac06dfcf5e3524101.js
- ► https://www.airbnb.com
- ► https://maps.googleapis.com
- ► https://www.googleadservices.com
- ► https://www.google-analytics.com
- ► https://sslwidget.criteo.com
- ► https://www.googletagmanager.com
- ► https://static.criteo.net

https://a0.muscache.com/airbnb/static/HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js (Pretty Printed)

View Original

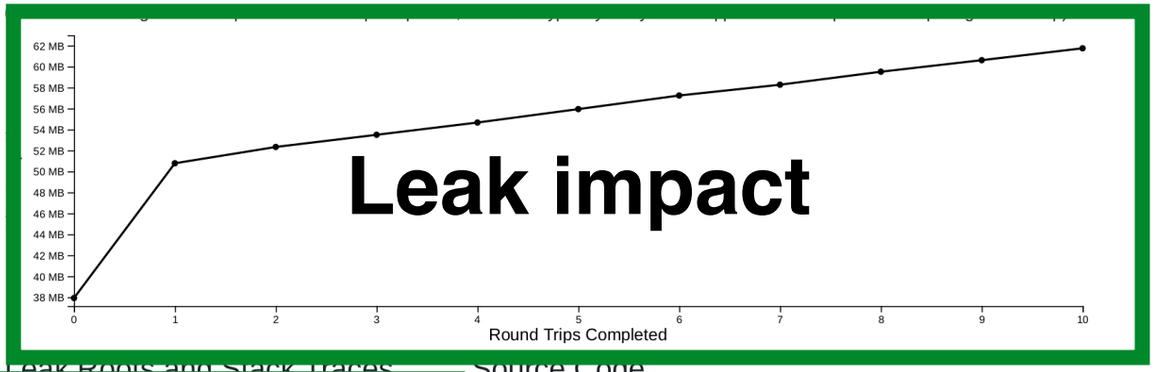
```
window.__MEMFIX__ = function() {
  return true;
}
;
!function() {
  var e = webpackJsonp([690], {
    "/jFZ": function(e, t) {
      function n(e) {
        var t = 0
          , n = 0
          , i = 0
          , r = ""
          , a = void 0
          , s = void 0;
        for (t = 0; t < e.length; ++t) {
          var l = babelHelpers.slicedToArray(e[t], 2);
          a = l[0],
          s = l[1],
          r += o(n, i, a, s),
          n = a,
          i = s
        }
        return r += o(n, i, e[0][0], e[0][1])
      }
      function o(e, t, n, o) {
        var r = Math.round(1e5 * n)
          , a = Math.round(1e5 * e)
          , s = Math.round(1e5 * o)
          , l = Math.round(1e5 * t)
          , u = s - l;
        return i(r - a) + i(u)
      }
      function i(e) {
        var t = e << 1;
        return e < 0 && (t = ~t),
        r(t)
      }
      function r(e) {
        for (var t = ""; e >= 32; )
          t += String.fromCharCode(63 + (32 | 31 & e)),
```

BLeak Output: airbnb.com

Report with actionable information!

Live Heap Size

Average Growth: 1.16MB / round trip, 95% CI [1.07, 1.25]



Leak Roots and Stack Traces

Rank By: LeakShare

Score 389216 document.childNodes[3].childNodes[3].childNodes

Score 214611 window.$$listeners.blur

Score 212459 window.$$listeners.resize

Score 211235 List of 'click' listeners on document

Score 209811 window.$$listeners.scroll

Score 209219 List of 'keydown' listeners on document

Score 209211 List of 'keypress' listeners on document

Score 209155 document.__e3_.keydown

Score 208951 list of keyup listeners on document

Score 208803 window.__e3_.resize

Score 208771 document.__e3_.keyup

Score 208771 document.__e3_.click

Score 208771 window.__e3_.blur

Score 204339 document.__e3_.keypress

Score 204339 List of 'MSFullscreenChange' listeners on document

Score 204339 List of 'fullscreenchange' listeners on document

Score 204339 List of 'webkitfullscreenchange' listeners on document

Score 204339 List of 'mozfullscreenchange' listeners on document

Score 204323 document.__e3_.fullscreenchange

Leaks ranked by return on investment

Source Code

- ▼ https://a0.muscache.com
  - ▼ airbnb/static
    - ► packages
    - HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js
    - webcot-ForYouContainer_async-async-bb0ac06dfcf5e3524101.js
- ► https://www.airbnb.com
- ► https://maps.googleapis.com
- ► https://www.googleadservices.com
- ► https://www.google-analytics.com
- ► https://sslwidget.criteo.com
- ► https://www.googletagmanager.com
- ► https://static.criteo.net

https://a0.muscache.com/airbnb/static/HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js (Pretty Printed)

View Original

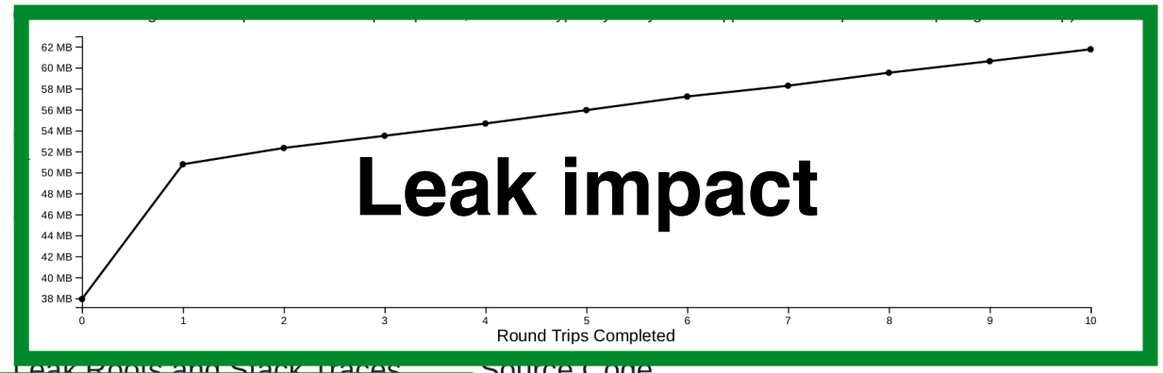
```
window.__MEMFIX__ = function() {
  return true;
}
;
!function() {
  var e = webpackJsonp([690], {
    "/jFZ": function(e, t) {
      function n(e) {
        var t = 0
          , n = 0
          , i = 0
          , r = ""
          , a = void 0
          , s = void 0;
        for (t = 0; t < e.length; ++t) {
          var l = babelHelpers.slicedToArray(e[t], 2);
          a = l[0],
          s = l[1],
          r += o(n, i, a, s),
          n = a,
          i = s
        }
        return r += o(n, i, e[0][0], e[0][1])
      }
      function o(e, t, n, o) {
        var r = Math.round(1e5 * n)
          , a = Math.round(1e5 * e)
          , s = Math.round(1e5 * o)
          , l = Math.round(1e5 * t)
          , u = s - l;
        return i(r - a) + i(u)
      }
      function i(e) {
        var t = e << 1;
        return e < 0 && (t = ~t),
        r(t)
      }
      function r(e) {
        for (var t = ""; e >= 32; )
          t += String.fromCharCode(63 + (32 | 31 & e)),
```

BLeak Output: airbnb.com

Report with actionable information!

Live Heap Size

Average Growth: 1.16MB / round trip, 95% CI [1.07, 1.25]



Leak impact

Leak Roots and Stack Traces

Rank By: LeakShare

Score 389216 document.childNodes[3].childNodes[3].childNodes

Score 214611 window.$$listeners.blur

Score 212459 window.$$listeners.resize

Score 211235 List of 'click' listeners on document

Score 209811 window.$$listeners.scroll

Score 209219 List of 'keydown' listeners on document

Score 209211 List of 'keypress' listeners on document

Score 209155 document.__e3_.keydown

Score 208951 list of keyup listeners on document

Score 208803 window.__e3_.resize

Score 208771 document.__e3_.keyup

Score 208771 document.__e3_.click

Score 208771 window.__e3_.blur

Score 208771 document.__e3_.keypress

Score 204339 List of 'MSFullscreenChange' listeners on document

Score 204339 List of 'fullscreenchange' listeners on document

Score 204339 List of 'webkitfullscreenchange' listeners on document

Score 204339 List of 'mozfullscreenchange' listeners on document

Score 204323 document.__e3_.fullscreenchange

Leaks ranked by return on investment

Source Code

- ▼ https://a0.muscache.com
  - ▼ airbnb/static
    - ► packages
    - HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js
    - webcot-ForYouContainer_async-async-bb0ac06dfcf5e3524101.js
- ► https://www.airbnb.com
- ► https://maps.googleapis.com
- ► https://www.googleadservices.com
- ► https://www.google-analytics.com
- ► https://sslwidget.criteo.com
- ► https://www.googletagmanager.com
- ► https://static.criteo.net

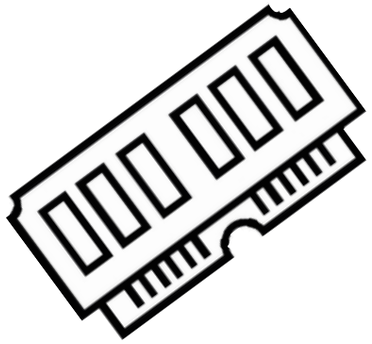
https://a0.muscache.com/airbnb/static/HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js (Pretty Printed)

View Original

```
window.__MEMFIX__ = function() {
  return true;
}
;
!function() {
  var e = webpackJsonp([690], {
    "/jFZ": function(e, t) {
      function n(e) {
        var
          , [illegible] = 0
          , [illegible] = 0
          , r = ""
          , a = void 0
          , s = void 0;
        for (t = 0; t < e.length; ++t) {
          var [illegible]
            [illegible][0]
            [illegible][1]
            r += [illegible](n, i, a, s),
            n = a,
            i = s
        }
        return r += o(n, i, [illegible][0], [illegible][1])
      }
      function o(e, t, n, o) {
        var r = [illegible]
          , a = Math.round(1e5 * e)
          , s = Math.round(1e5 * o)
          , l = Math.round(1e5 * t)
          , u = s - [illegible];
        return i([illegible], u
      }
      function i(e) {
        var t = e << 1;
        return e < 0 && (t = ~t),
        r(t)
      }
      function r(e) {
        for (var t = ""; e >= 32; )
          t += String.fromCharCode(63 + (32 | 31 & e)),
```

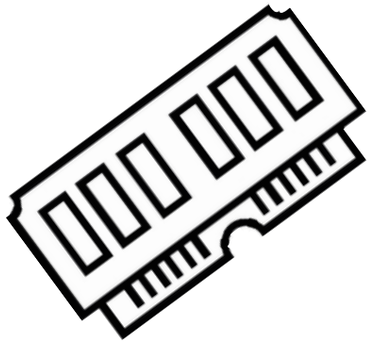
Highlights source code responsible for leaks

BLeak Results for airbnb.com



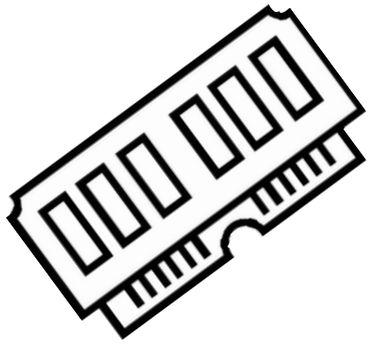
BLeak Results for airbnb.com

- 32 leak roots reported
  - 2 false positives (94% precision)



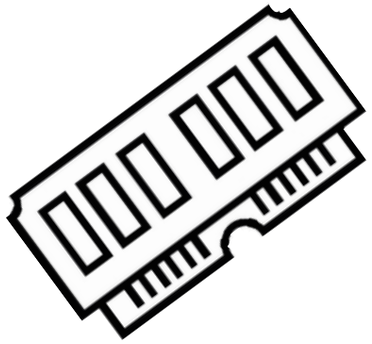
BLeak Results for airbnb.com

- 32 leak roots reported
  - 2 false positives (94% precision)
- Fixing leaks eliminates 1.04MB of live heap growth per round trip
  - 81% reduction!



BLeak Results for airbnb.com

- 32 leak roots reported
  - 2 false positives (94% precision)
- Fixing leaks eliminates 1.04MB of live heap growth per round trip
  - 81% reduction!
- Developed fix for Google Maps memory leak!



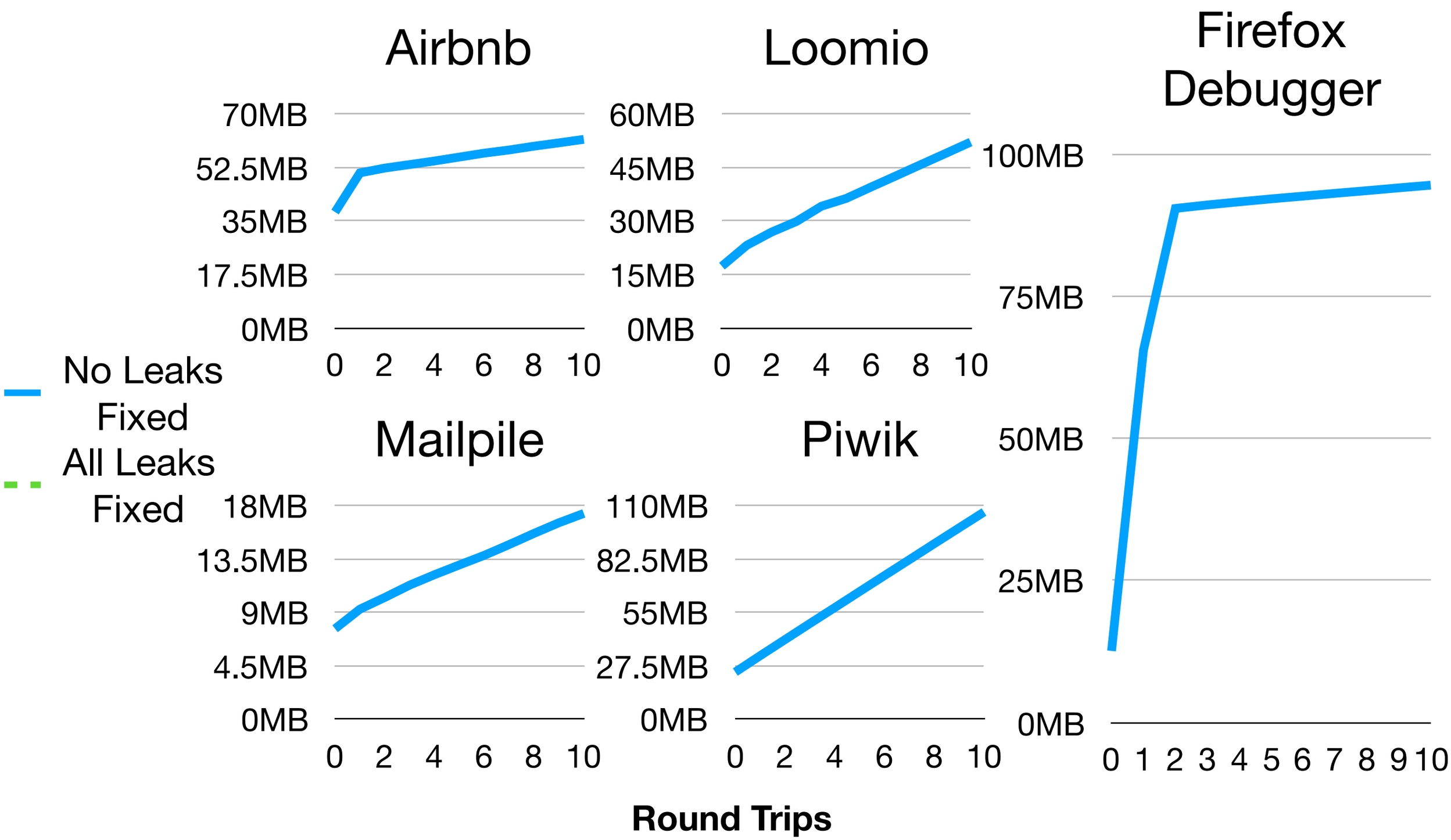
Evaluation Overview

Live Heap Size Growth Before and After Fixes

Round Trips

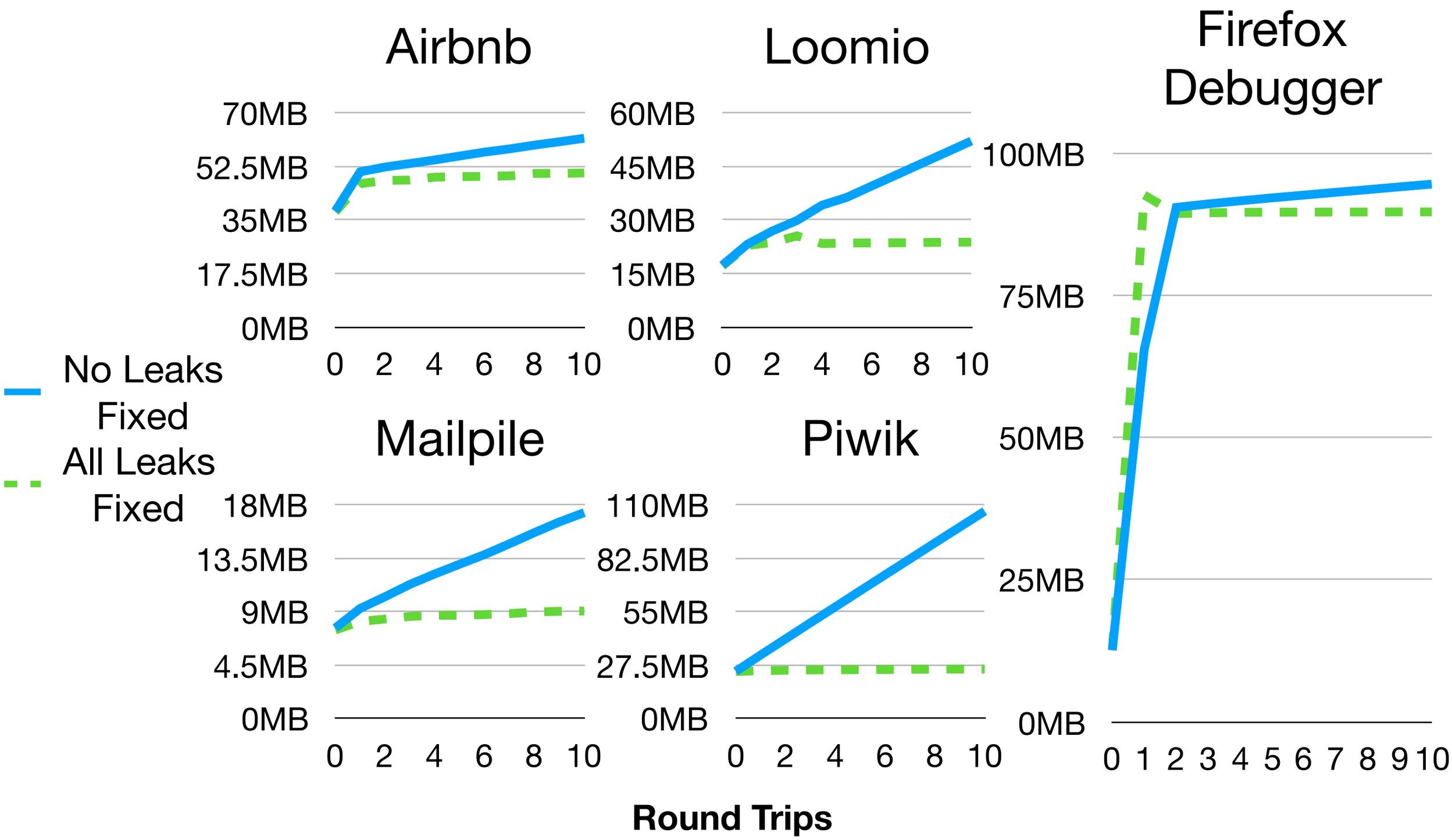
Evaluation Overview

Live Heap Size Growth Before and After Fixes



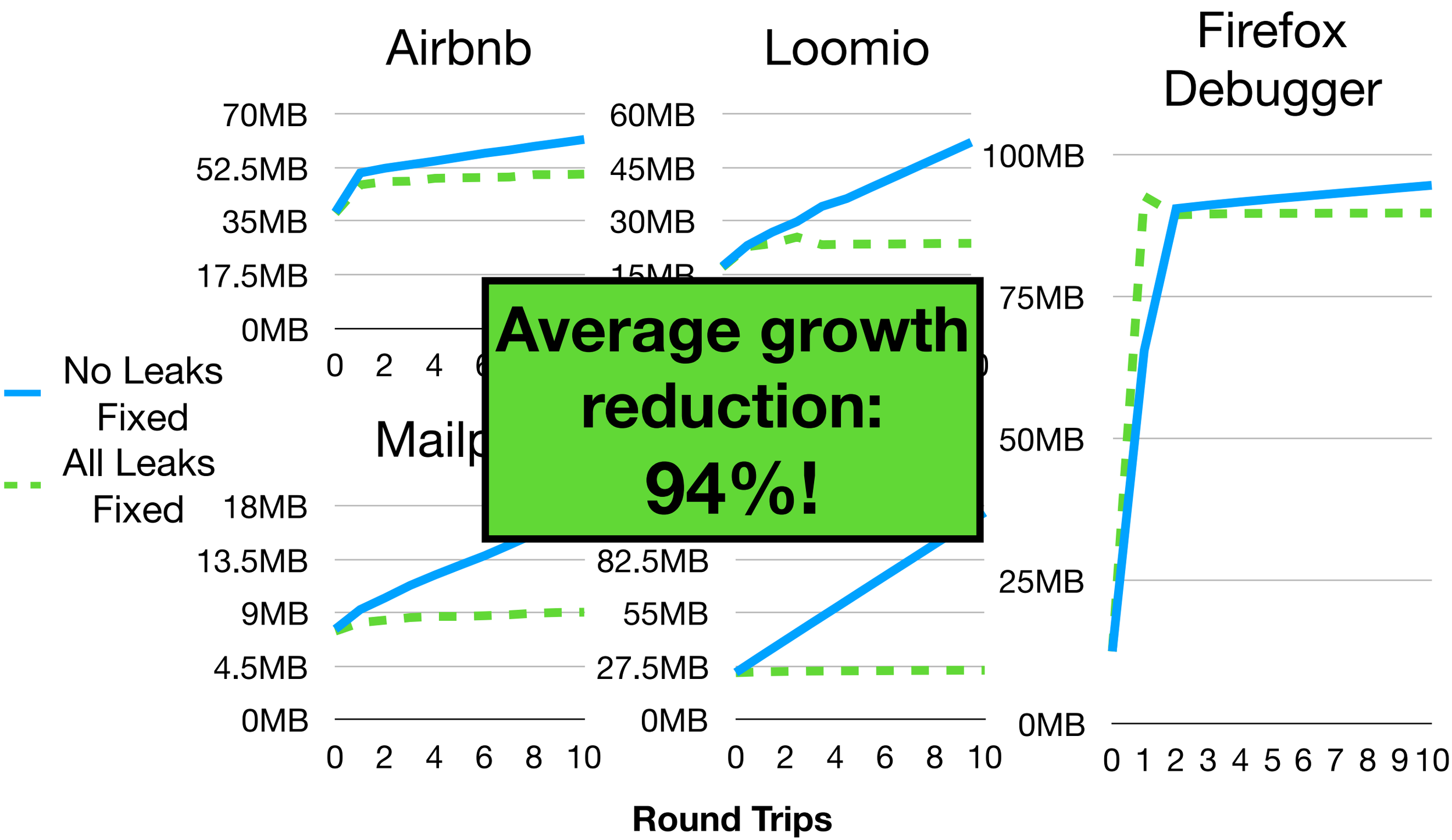
Evaluation Overview

Live Heap Size Growth Before and After Fixes

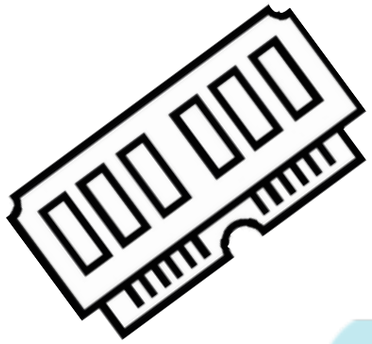


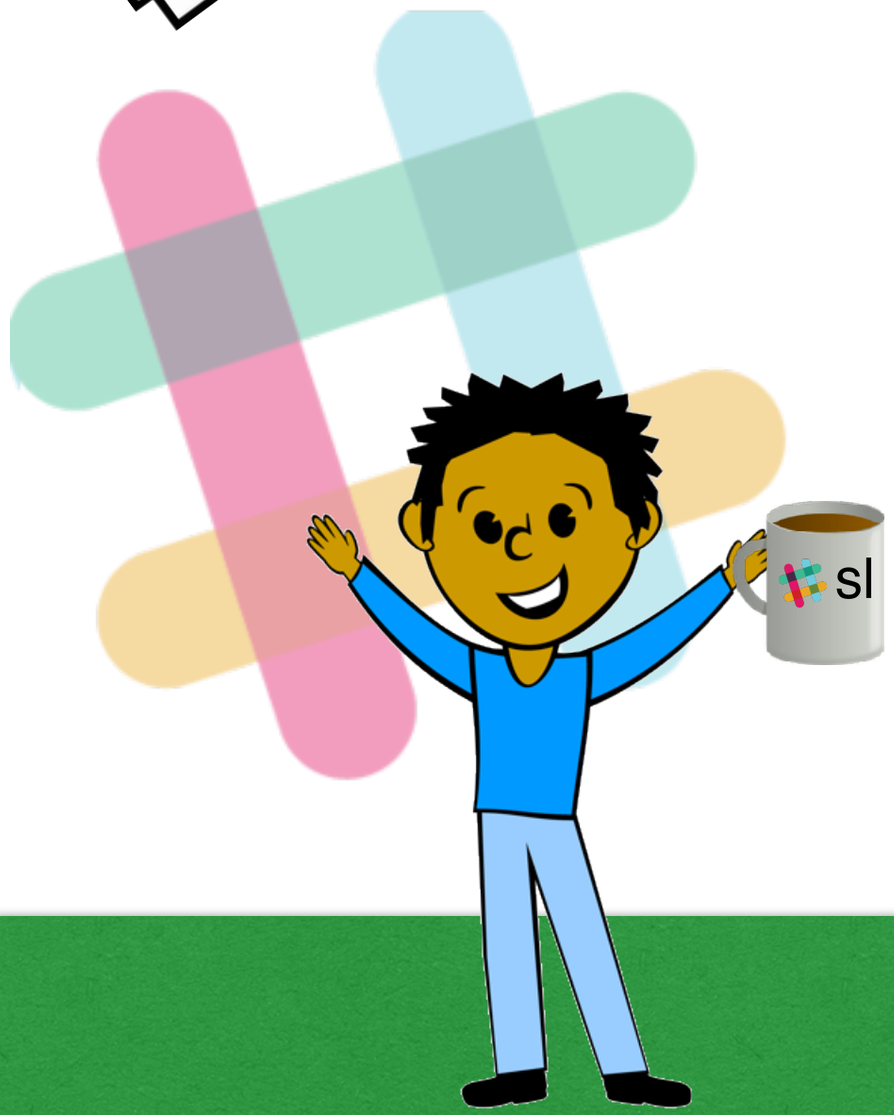
Evaluation Overview

Live Heap Size Growth Before and After Fixes



Average growth reduction: 94%!

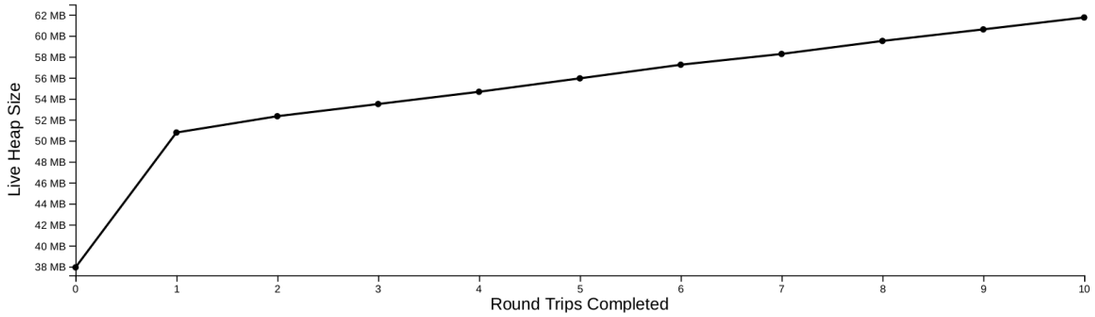




Live Heap Size

Average Growth: 1.16MB / round trip, 95% CI [1.07, 1.25]

(The above stats ignore the impact of first 5 heap snapshots, which are typically noisy due to application startup + JavaScript engine warmup)



Leak Roots and Stack Traces

Rank By: LeakShare

- Score 389216 document.childNodes[3].childNodes[3].childNodes
- Score 214611 window.$$listeners.blur
- Score 212459 window.$$listeners.resize
- Score 211235 List of 'click' listeners on document
- Score 209811 window.$$listeners.scroll
- Score 209219 List of 'keydown' listeners on document
- Score 209211 List of 'keypress' listeners on document
- Score 209155 document.__e3_.keydown
- Score 209051 List of 'keyup' listeners on document
- Score 208803 window.__e3_.resize
- Score 208771 document.__e3_.keyup
- Score 208771 document.__e3_.click
- Score 208771 window.__e3_.blur
- Score 208771 document.__e3_.keypress
- Score 204339 List of 'MSFullscreenChange' listeners on document
- Score 204339 List of 'fullscreenchange' listeners on document
- Score 204339 List of 'webkitfullscreenchange' listeners on document
- Score 204339 List of 'mozfullscreenchange' listeners on document
- Score 204323 document.__e3_.fullscreenchange

Source Code

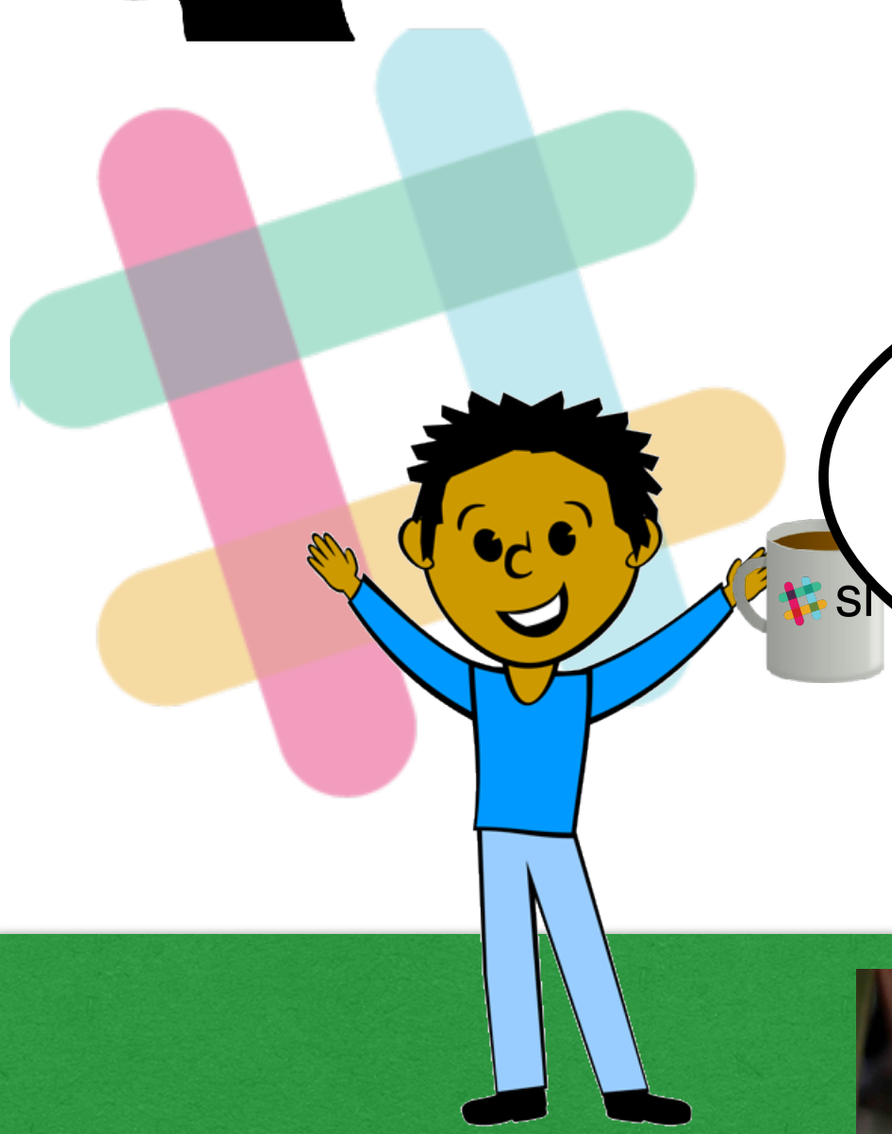
- ▼ https://a0.muscache.com
  - ▼ airbnb/static
    - ► packages
    - HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js
    - webcot-ForYouContainer_async-async-bb0ac06dfcf5e3524101.js
- ► https://www.airbnb.com
- ► https://maps.googleapis.com
- ► https://www.googleadservices.com
- ► https://www.google-analytics.com
- ► https://sslwidget.criteo.com
- ► https://www.googletagmanager.com
- ► https://static.criteo.net

https://a0.muscache.com/airbnb/static/HomeSearch_HomesSearchResultsMap-async-c0d3ef05e58224a53be7.js (Pretty Printed)

View Original

```
window.__MEMFIX__ = function() {
  return true;
}
;
!function() {
  var e = webpackJsonp([690], {
    "/jFZ": function(e, t) {
      function n(e) {
        var t = 0
          , n = 0
          , i = 0
          , r = ""
          , a = void 0
          , s = void 0;
        for (t = 0; t < e.length; ++t) {
          var l = babelHelpers.slicedToArray(e[t], 2);
          a = l[0],
          s = l[1],
          r += o(n, i, a, s),
          n = a,
          i = s
        }
        return r += o(n, i, e[0][0], e[0][1])
      }
      function o(e, t, n, o) {
        var r = Math.round(1e5 * n)
          , a = Math.round(1e5 * e)
          , s = Math.round(1e5 * o)
          , l = Math.round(1e5 * t)
          , u = s - l;
        return i(r - a) + i(u)
      }
      function i(e) {
        var t = e << 1;
        return e < 0 && (t = ~t),
        r(t)
      }
      function r(e) {
        for (var t = ""; e >= 32; )
          t += String.fromCharCode(63 + (32 | 31 & e)),
```

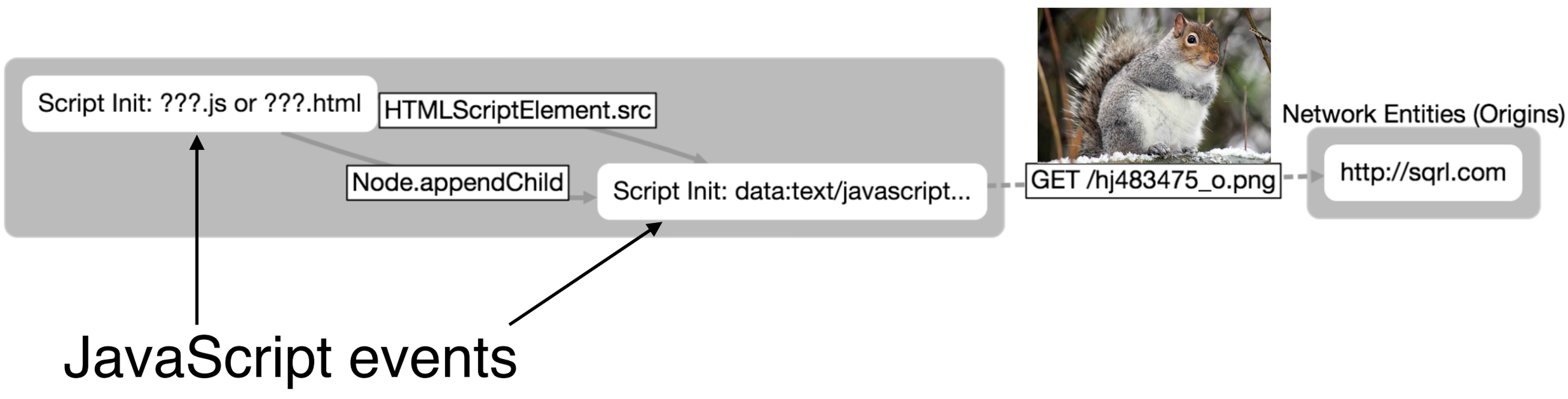
Slax is a bandwidth hog!!!



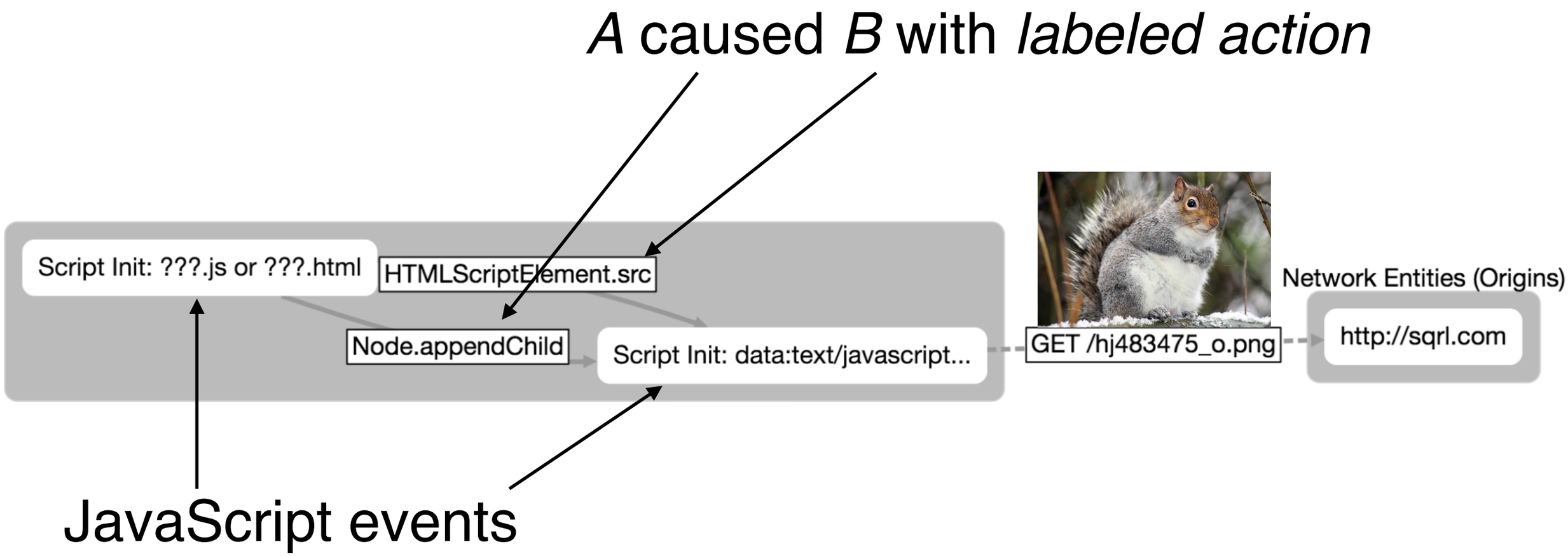
Slax is a bandwidth hog!!!

Causal Graphs

Causal Graphs



Causal Graphs



Causal Graphs

A caused *B* with *labeled action*

Would identify mystery code!

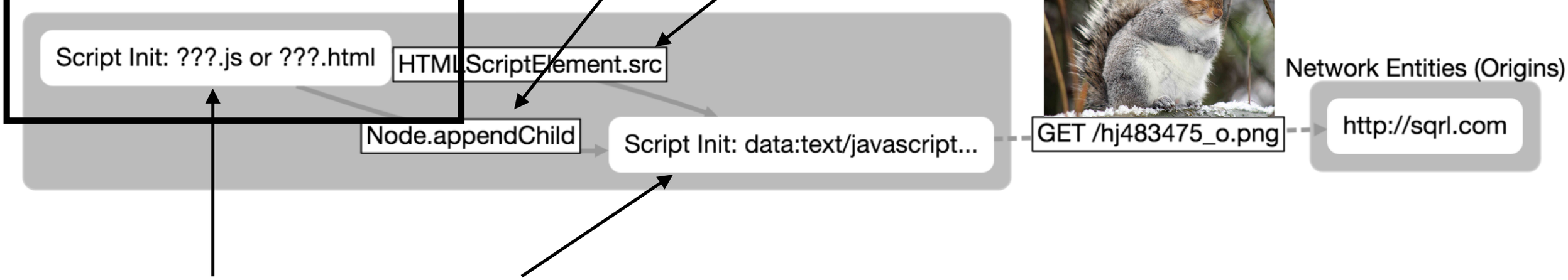
JavaScript events

Causal Graphs

No existing tools can create this graph!

A caused *B* with *labeled action*

Would identify mystery code!



JavaScript events

Challenge: Determining Cause of Events

Challenge: Determining Cause of Events

Slack event log, captured while loading Slack:

Start Time	Self Time	Total Time	Activity
4283.2 ms	0.0 ms	0.0 ms	Event
4283.3 ms	0.0 ms	0.0 ms	Event
4283.4 ms	0.0 ms	0.0 ms	Event
4283.4 ms	0 ms	0 ms	unloadEventStart
4283.4 ms	0.0 ms	0.0 ms	Event
4283.4 ms	0 ms	0 ms	unloadEventEnd
4284.3 ms	0 ms	0 ms	domLoading
4284.3 ms	0.0 ms	0.0 ms	Event
4350.9 ms	0 ms	0 ms	requestStart
4351.3 ms	0 ms	0 ms	requestStart
4354.3 ms	0 ms	0 ms	requestStart
4357.0 ms	0 ms	0 ms	requestStart
4357.6 ms	0 ms	0 ms	requestStart
4357.8 ms	0 ms	0 ms	requestStart
4361.4 ms	0 ms	0 ms	requestStart
4368.9 ms	0 ms	0 ms	requestStart

Challenge: Determining Cause of Events

Slack event log, captured while loading Slack:

Not clear *WHY* each event is happening or *HOW* events are related!

4283.4 ms	0.0 ms	0.0 ms	Event
4283.4 ms	0 ms	0 ms	unloadEventStart
4283.4 ms	0.0 ms	0.0 ms	Event
4283.4 ms	0 ms	0 ms	unloadEventEnd
4284.3 ms	0 ms	0 ms	domLoading
4284.3 ms	0.0 ms	0.0 ms	Event
4350.9 ms	0 ms	0 ms	requestStart
4351.3 ms	0 ms	0 ms	requestStart
4354.3 ms	0 ms	0 ms	requestStart
4357.0 ms	0 ms	0 ms	requestStart
4357.6 ms	0 ms	0 ms	requestStart
4357.8 ms	0 ms	0 ms	requestStart
4361.4 ms	0 ms	0 ms	requestStart
4368.9 ms	0 ms	0 ms	requestStart

Challenge: Determining Cause of Events

Slack event log, captured while loading Slack:

Not clear *WHY* each event is happening or *HOW* events are related!

4283.4 ms	0.0 ms	0.0 ms	Event

Causes are buried in standards documents:

↪ **If the download was successful and the user agent was able to determine the image's width and height**

1. Set the `img` element to the completely available state.
2. Add the image to the list of available images using the key *key*.
3. If the resource is CORS-same-origin: fire a progress event named `load` at the `img` element.

   If the resource is CORS-cross-origin: fire a simple event named `load` at the `img` element.
4. If the resource is CORS-same-origin: fire a progress event named `loadend` at the `img` element.

   If the resource is CORS-cross-origin: fire a simple event named `loadend` at the `img` element.

4368.9 ms	0 ms	0 ms	requestStart

Challenge: Determining Cause of Events

Slack event log, captured while loading Slack:

Not clear *WHY* each event is happening or *HOW* events are related!

4283.4 ms	0.0 ms	0.0 ms	Event

Causes are buried in standards documents:

↪ **If the download was successful and the user agent was able to determine the image's width and height**

1. Set the `img` element to the completely available state.
2. Add the image to the list of available images using the key *key*.
3. If the resource is CORS-same-origin fire a progress event named `load` at the `img` element.

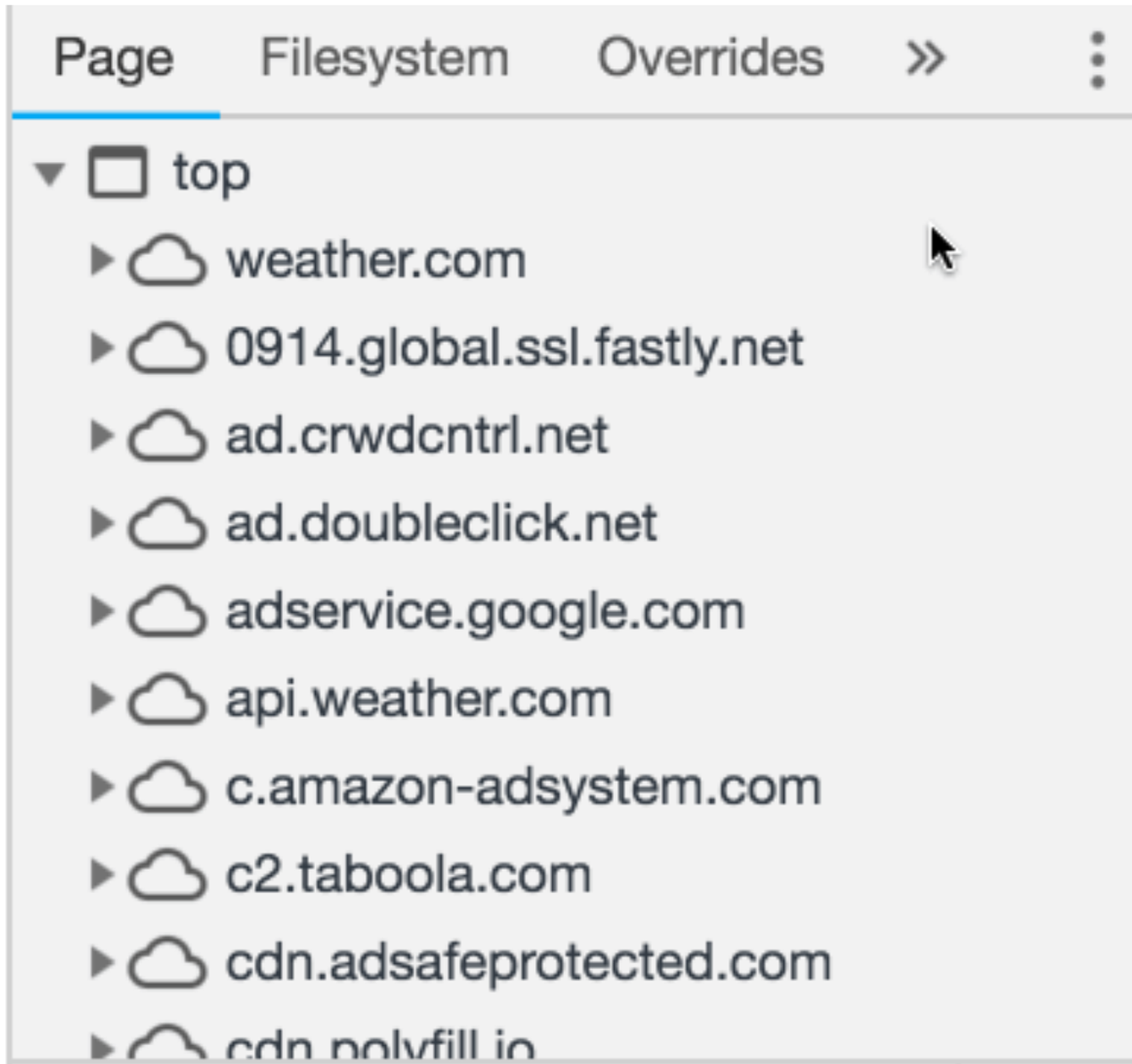
   If the resource is CORS-cross-origin fire a simple event named `load` at the `img` element.
4. If the resource is CORS-same-origin fire a progress event named `loadend` at the `img` element.

   If the resource is CORS-cross-origin fire a simple event named `loadend` at the `img` element.

4368.9 ms	0 ms	0 ms	requestStart

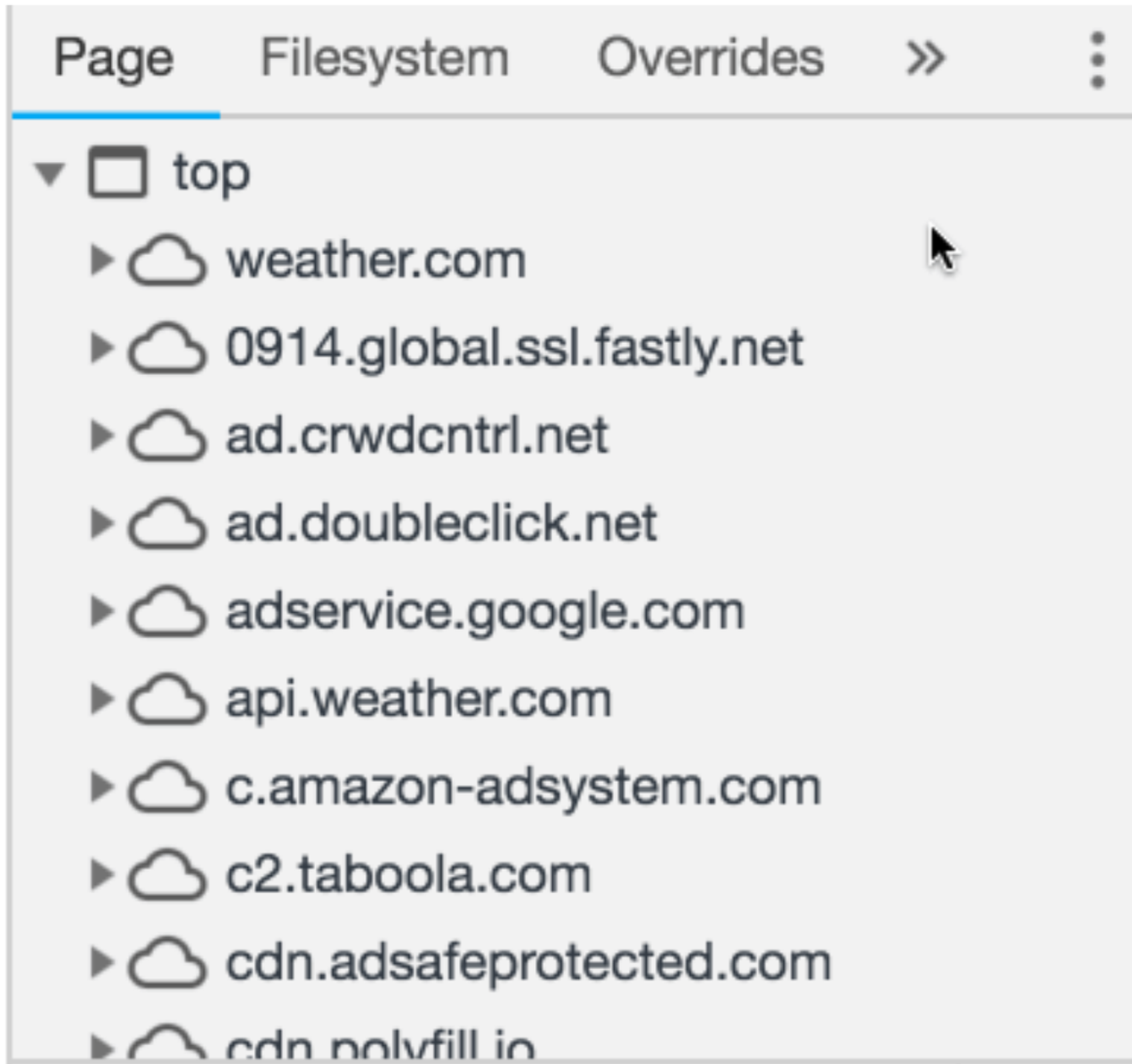
Challenge: Obfuscated Third Party Code and Ads

List of domains weather.com loads content from:



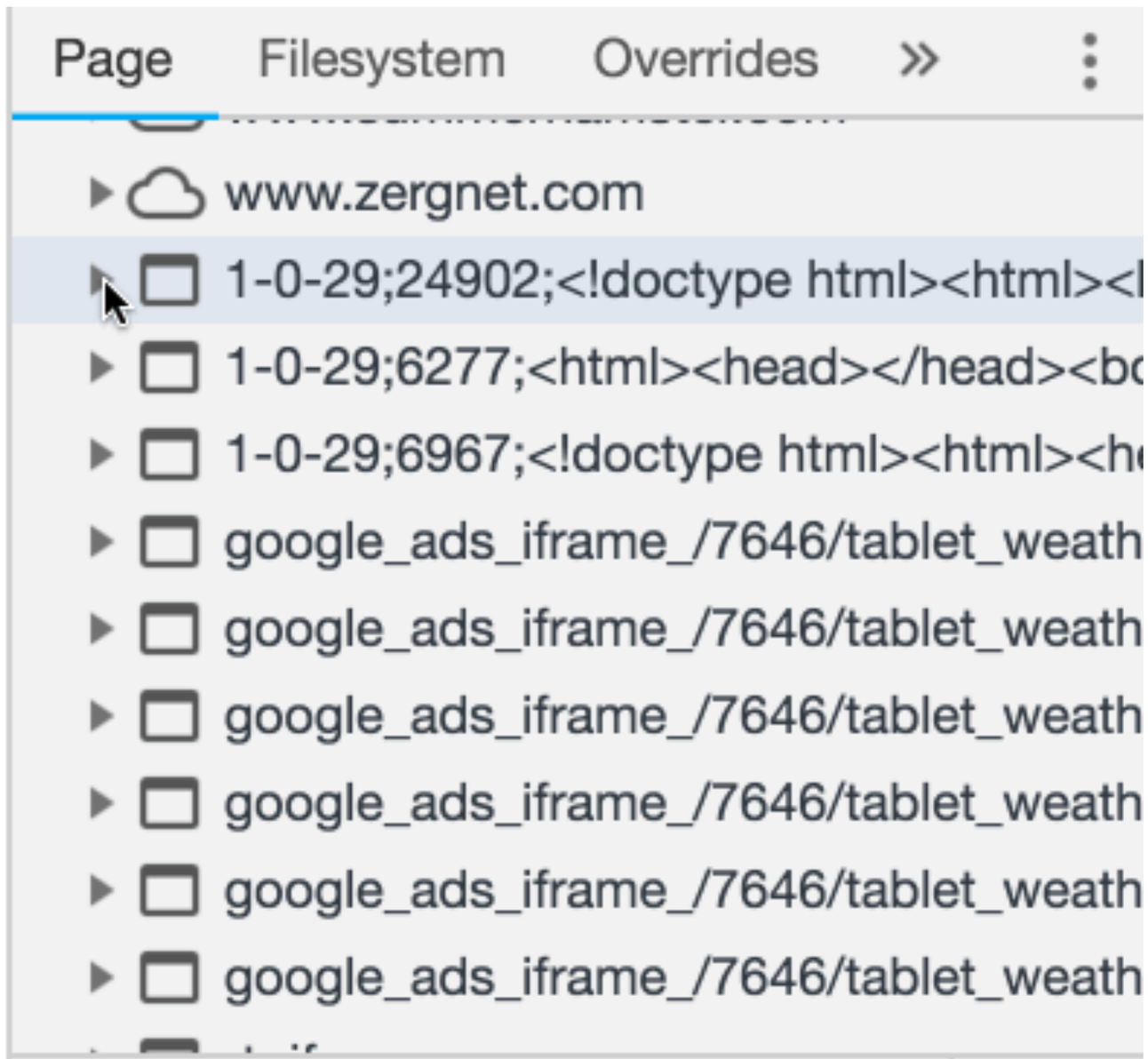
Challenge: Obfuscated Third Party Code and Ads

List of domains weather.com loads content from:



Challenge: Obfuscated Third Party Code and Ads

List of domains weather.com loads content from:



Challenge: Obfuscated Third Party Code and Ads

List o rom:

```
eval((function(s){var
a,c,e,i,j,o="",r,t="ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
$@^`~" ;for(i=0;i<s.length;i++){r=t+s[i][2];a=s[i][1].split
(".");for(j=a.length-1;j>=0;j--){s[i][0]=s[i][0].split(r.charAt(
j)).join(a[j])}o+=s[i][0]}var p=21054,x=function(r){var
c,p,s,l='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_01
23456789';if(r<63)c=l.charAt(r);else{r-=63;p=Math.floor(r/63);s=
r%63;c=l.charAt(p)+l.charAt(s)}return
c};a=o.substr(p).split(':');r=a[1].split('?');a=a[0].split('?');
o=o.substr(0,p);if(!''.replace(/^/,String)){var
z={};for(i=0;i<533;i++){var
y=x(i);z[y]=r[i]||y}t=/\b\w\w?\b/g;y=function(a){return
z[a]||a};o=o.replace(t,y)}else{for(j=a[a.length-1]-1;j>=0;j--){i
f(r[j])o=o.replace(new
RegExp('\b'+(j<63?c.charAt(j):c.charAt((j-63)/63)+c.charAt((j-63
)%63))+'\b','g'),r[j])}}return o.replace(/·/g,"\"")})([["if(w
ï¿½==ï¿½j'ï¿½ï¿½a,cï¿½i=0,e@Z,dï¿½copyï¿½,f=a;ï¿½!cï¿½cï¿½z-a}ï¿
½i·e·-2ï¿½·i]=e[i+2]}ï¿½a;a<ï¿½z-c;a++·e·-2]=d[a-c]}ï¿½z-@-e·+2ï
¿½d.slice(f,f+c)ï¿½k
```

REAL CODE FOUND ON WEATHER.COM

Challenge: Obfuscated Third Party Code and Ads

List o rom:

```
eval((function(s){var
a,c,e,i,j,o="",r,t="ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½
·····$@^`~" ;for(i=0;i<s.length;i++){r=t+s[i][2];a=s[i][1].split
("·");for(j=a.length-1;j>=0;j--){s[i][0]=s[i][0].split(r.charAt(
i)).join(a[j])}o+=s[i][0]}var p=21054,x=function(r){var
```

Tools must support obfuscated third-party code!

```
o=o.substr(0,p);if(!''.replace(/^/,String)){var
z={};for(i=0;i<533;i++){var
y=x(i);z[y]=r[i]||y}t=/\b\w\w?\b/g;y=function(a){return
z[a]||a};o=o.replace(t,y)}else{for(j=a[a.length-1]-1;j>=0;j--){i
f(r[j])o=o.replace(new
RegExp('\b'+(j<63?c.charAt(j):c.charAt((j-63)/63)+c.charAt((j-63
)%63))+'\b','g'),r[j])}}return o.replace(/·/g,"\"")})([["if(w
ï¿½==ï¿½j'ï¿½ï¿½a,cï¿½i=0,e@Z,dï¿½copyï¿½,f=a;ï¿½!cï¿½cï¿½z-a}ï¿
½i·e·-2ï¿½·i]=e[i+2]}ï¿½a;a<ï¿½z-c;a++·e·-2]=d[a-c]}ï¿½z-@-e·+2ï
¿½d.slice(f,f+c)ï¿½k
```

REAL CODE FOUND ON WEATHER.COM

```
¿½1¿½cx1¿½n1¿½cL1¿½v}1¿½a1++1¿½dz1¿½A®a11¿½dE1¿½11¿½1¿½1¿½1¿½1¿½
```

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

<script src="ad.js">

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

<script src="ad.js">

- Creates an HTMLScriptElement JavaScript object

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

<script src="ad.js">

- Creates an HTMLScriptElement JavaScript object
- Initiates an HTTP request to download "ad.js"

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

<script src="ad.js">

- Creates an HTMLScriptElement JavaScript object
- Initiates an HTTP request to download "ad.js"
- Emits a 'load' or 'error' JavaScript event

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

<script src="ad.js">

- Creates an HTMLScriptElement JavaScript object
- Initiates an HTTP request to download "ad.js"
- Emits a 'load' or 'error' JavaScript event
- Executes JavaScript contained in ad.js

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

Link

<script src="ad.js">

IFrame

- Creates an HTMLScriptElement JavaScript objec
- Initiates an HTTP request to dow ”

Media

- Emits ” JavaS

Img

- Executes JavaScript contained in ad.js

Challenge: Tight Coupling with HTML

HTML affects JavaScript execution + program behavior

Link

<script src="ad.js">

IFrame

Need full support for HTML/DOM!

- Initiates an HTTP request to

Media

- Emits ' JavaS

Img

- Executes JavaScript contained in ad.js

WebIDL

Describes browser’s JavaScript interfaces

WebIDL

Describes browser’s JavaScript interfaces

- Standardized!
  - Included in all modern web standards

WebIDL

Describes browser's JavaScript interfaces

- Standardized!
  - Included in all modern web standards
- Accurately describes implementations
  - Used to generate JavaScript interfaces in most browsers

WebIDL

Describes browser's JavaScript interfaces

- Standardized!
  - Included in all modern web standards
- Accurately describes implementations
  - Used to generate JavaScript interfaces in most browsers
- Can be annotated
  - Chrome adds annotations for JavaScript properties that reflect HTML attributes

WebIDL

Relates JavaScript objects to events and HTML

HTMLImageElement / <img> Interface

```
interface HTMLImageElement : HTMLElement {
    [Reflect] attribute DOMString alt;
    [Reflect] attribute DOMString src;
    [Reflect] attribute long width;
    [Reflect] attribute long height;
    [Reflect] attribute DOMString border;
    attribute EventHandler onload;
};
```

WebIDL

Relates JavaScript objects to events and HTML

HTMLImageElement / <img> Interface

```
interface HTMLImageElement : HTMLElement {
    [Reflect] attribute DOMString alt;
    [Reflect] attribute DOMString src;
    [Reflect] attribute long width;
    [Reflect] attribute long height;
    [Reflect] attribute DOMString border;
    attribute EventHandler onload;
};
```

Emits a ‘load’ event

WebIDL

Relates JavaScript objects to events and HTML

HTMLImageElement / <img> Interface

```
interface HTMLImageElement : HTMLElement {
    [Reflect] attribute DOMString alt;
    [Reflect] attribute DOMString src;
    [Reflect] attribute long width;
    [Reflect] attribute long height;
    [Reflect] attribute DOMString border;
    attribute EventHandler onload;
};
```

Can also be modified via HTML

Emits a ‘load’ event

WebIDL

Relates JavaScript objects to events and HTML

HTMLImageElement / <img> Interface

```
interface HTMLImageElement : HTMLElement {
    [Reflect] attribute DOMString alt;
    [Reflect] attribute DOMString src;
    [Reflect] attribute long width;
    [Reflect] attribute long height
    [Reflect] attribute DOMString border;
    attribute EventHandler onload;
};
```

Can also be modified via HTML

CAUSES

Emits a ‘load’ event

WebIDL

Relates JavaScript objects to events and HTML

HTMLImageElement / <img> Interface

```
interface HTMLImageElement : HTMLElement {
    [Reflect] attribute long height;
    [Reflect] attribute DOMString border;
    attribute EventHandler onload;
};
```

Can be used to infer most causal relations!
Can add annotations to specify rest!

via HTML

Emits a ‘load’ event

BCause: Framework for Understanding Asynchronous Control Flow

BCause: Framework for Understanding Asynchronous Control Flow

- Produces a trace of web application behavior

BCause: Framework for Understanding Asynchronous Control Flow

- Produces a trace of web application behavior
- Uses trace to produce a *causal graph* of JavaScript events

BCause: Framework for Understanding Asynchronous Control Flow

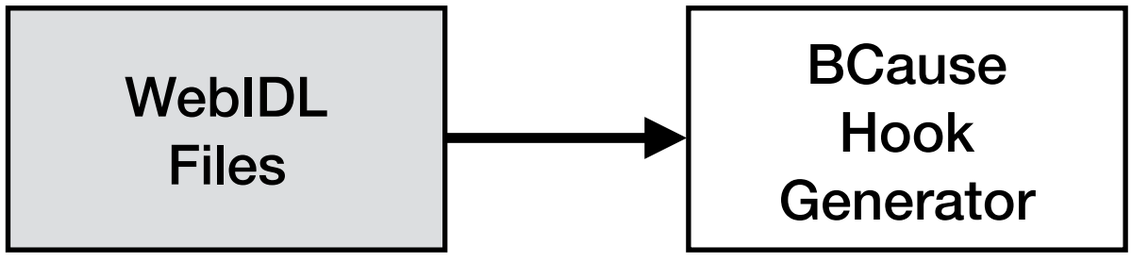
- Produces a trace of web application behavior
- Uses trace to produce a *causal graph* of JavaScript events

- No broken chains - relates all JavaScript events back to initial HTML document!

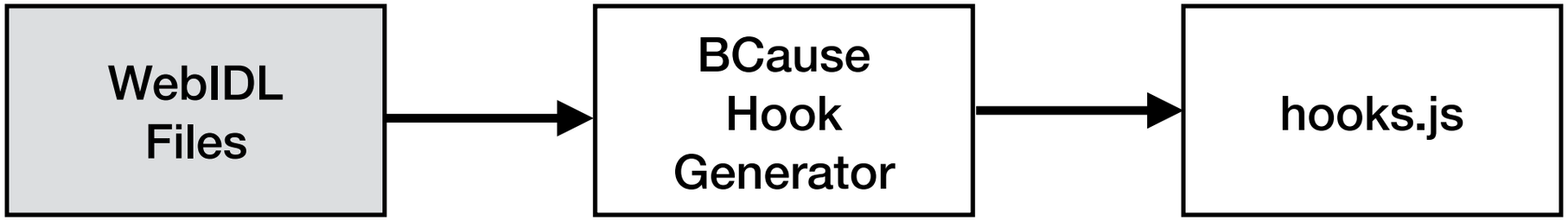
BCause System Diagram

BCause
Hook
Generator

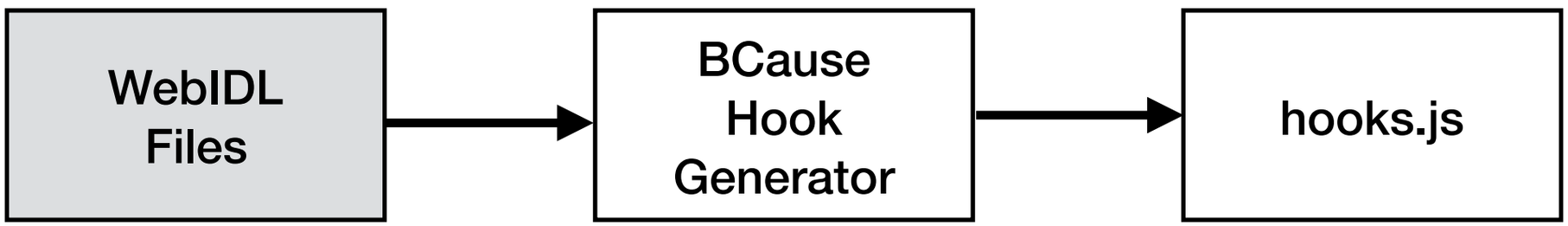
BCause System Diagram



BCause System Diagram

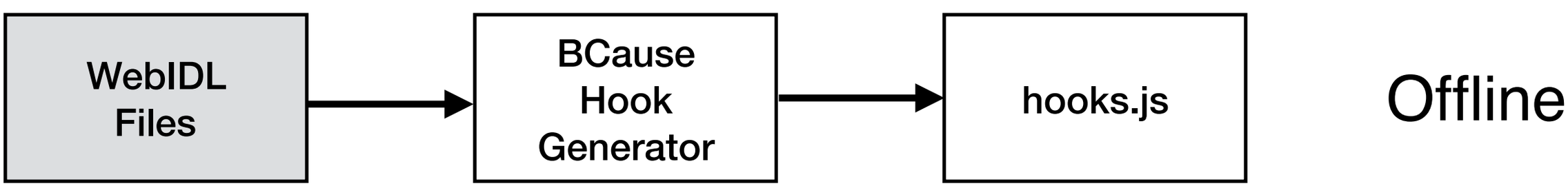


BCause System Diagram

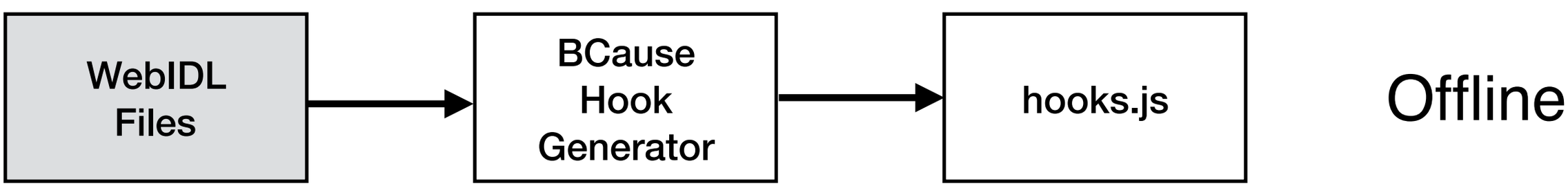


Hooks use JavaScript reflection to intercept and log program actions

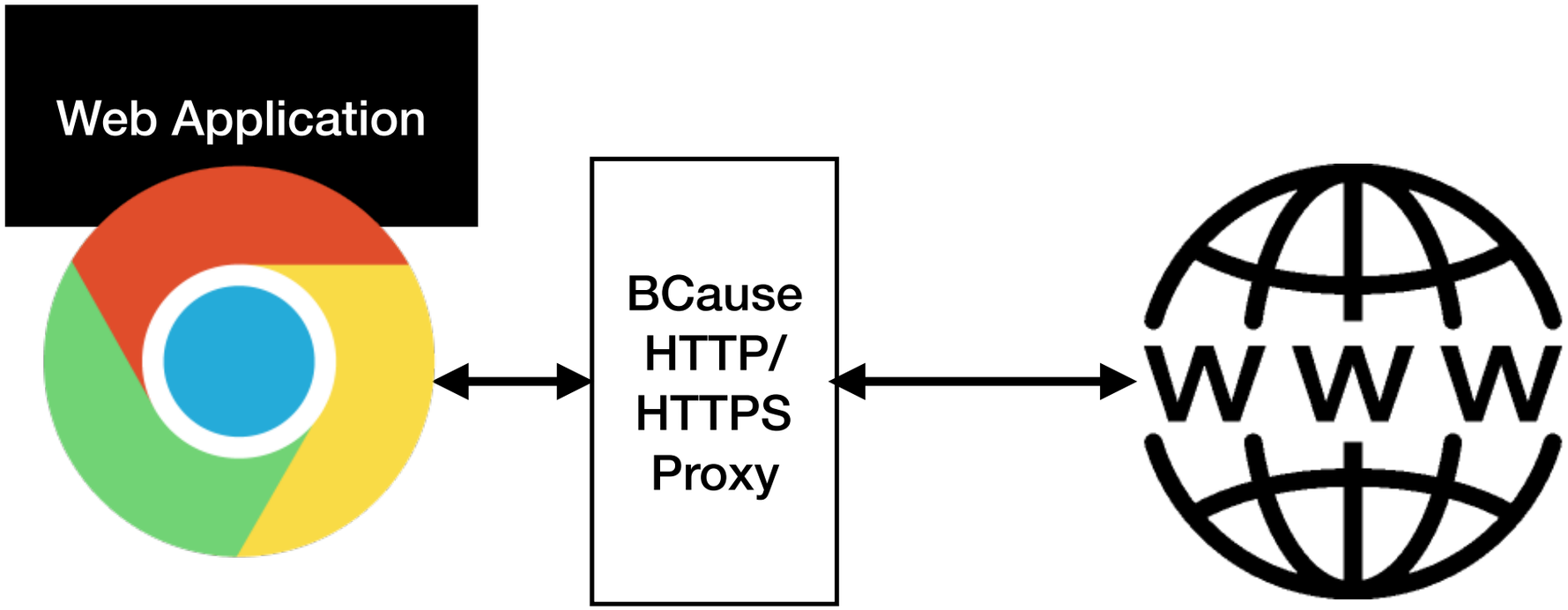
BCause System Diagram

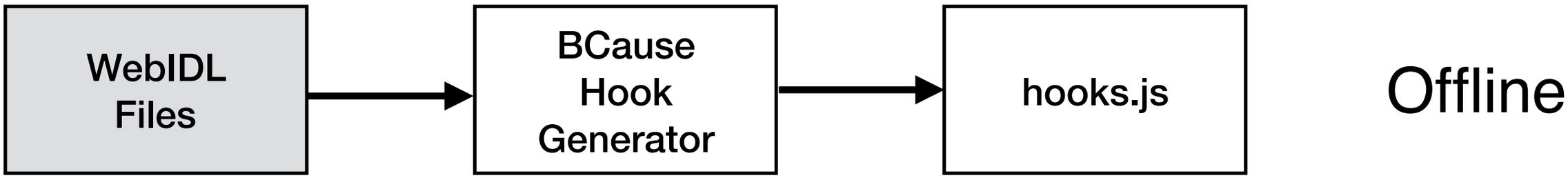


BCause System Diagram



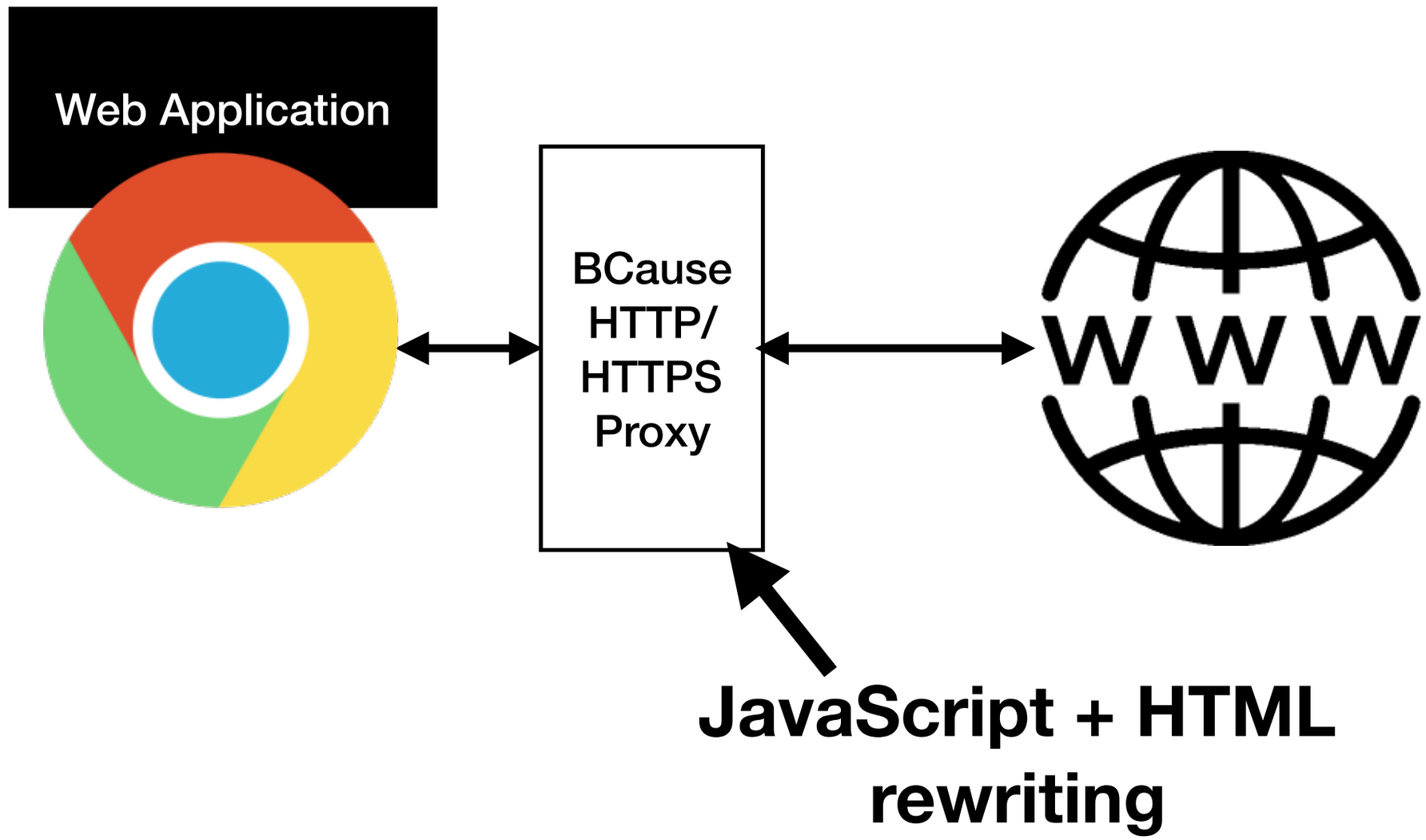
BCause System Diagram

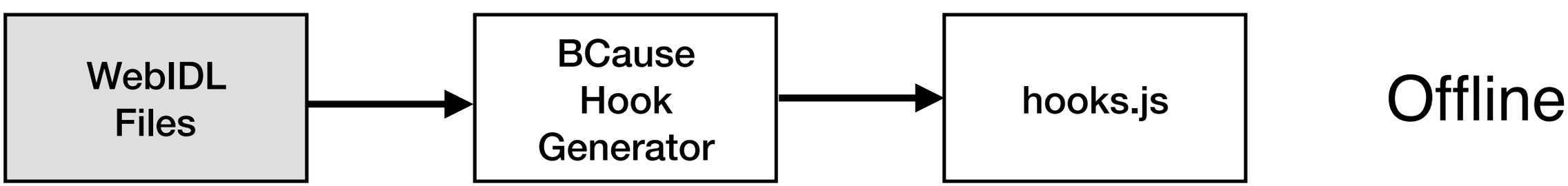




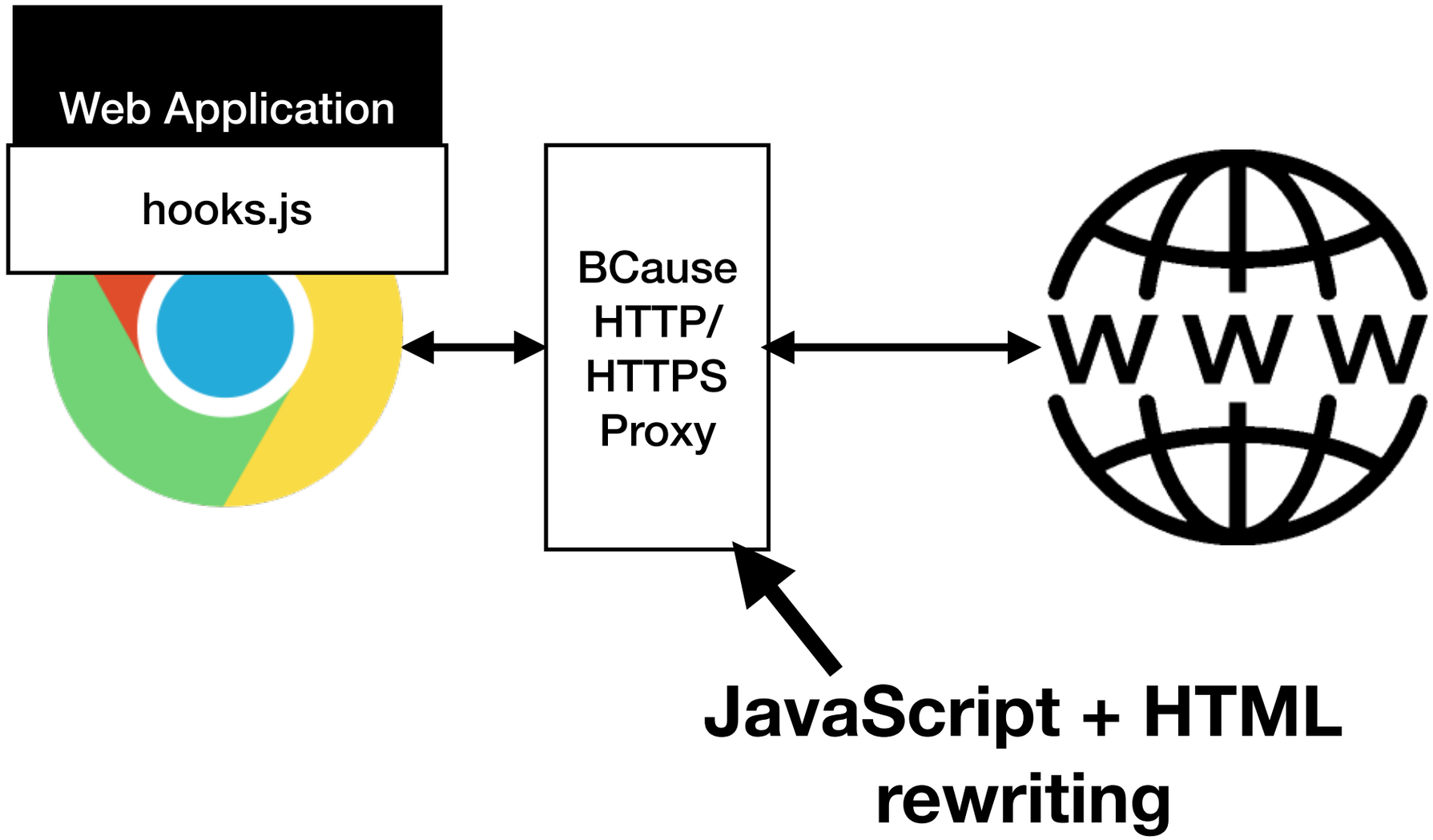
Offline

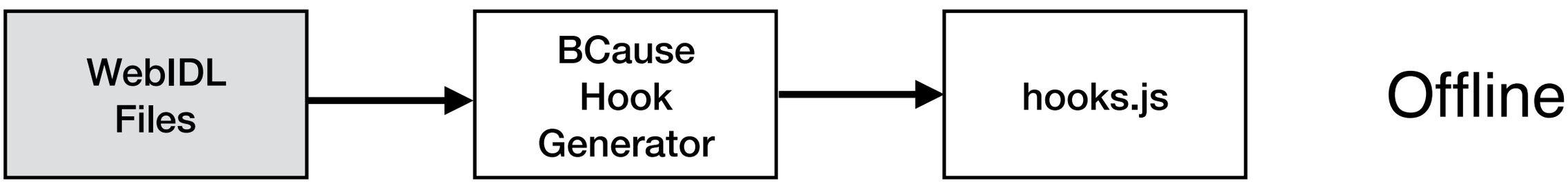
BCause System Diagram





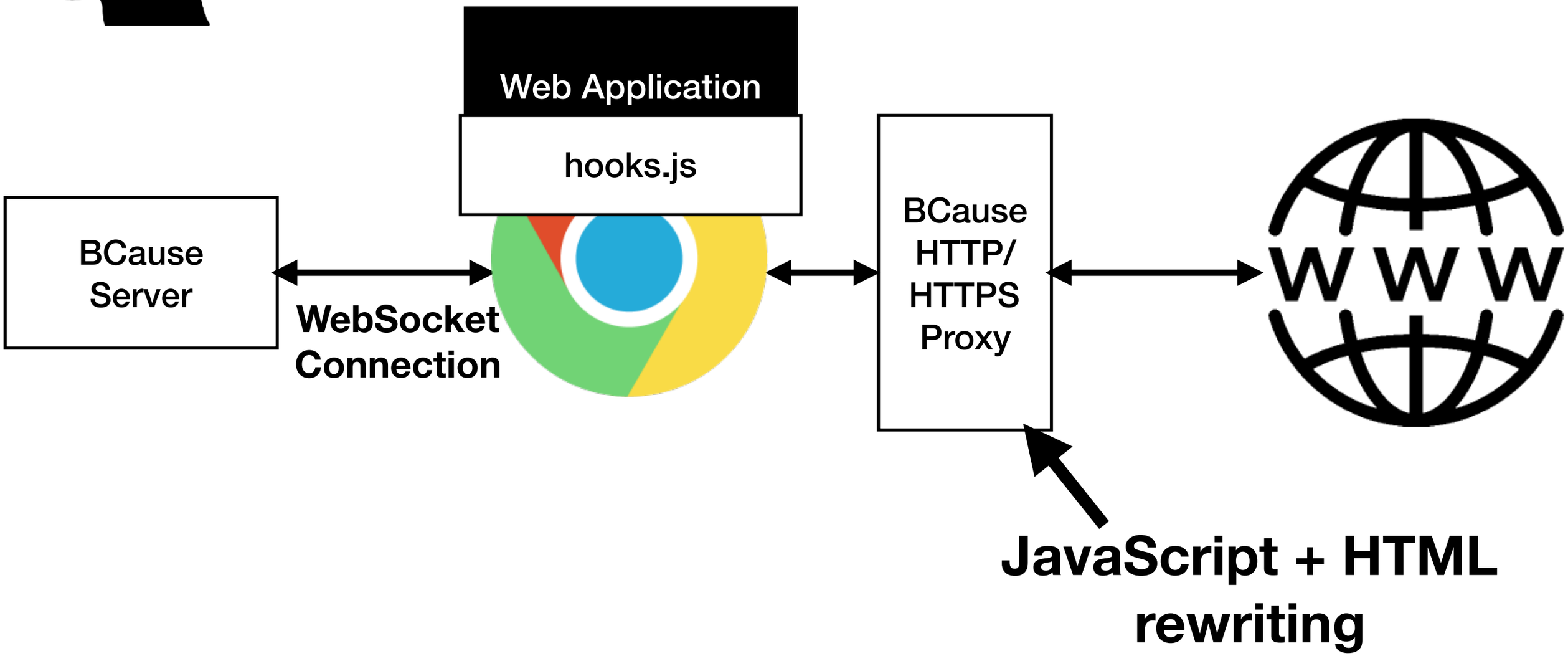
BCause System Diagram

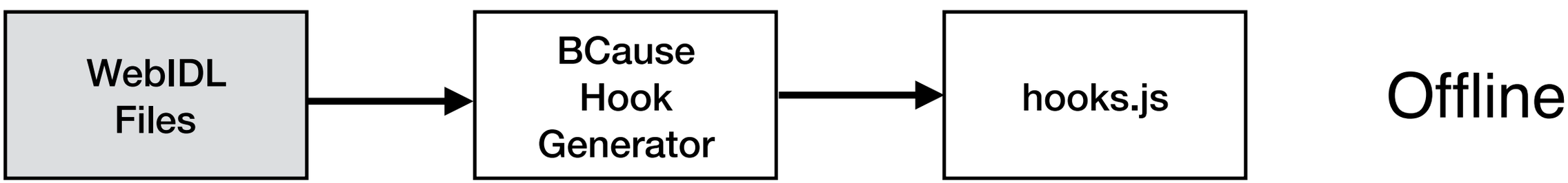




Offline

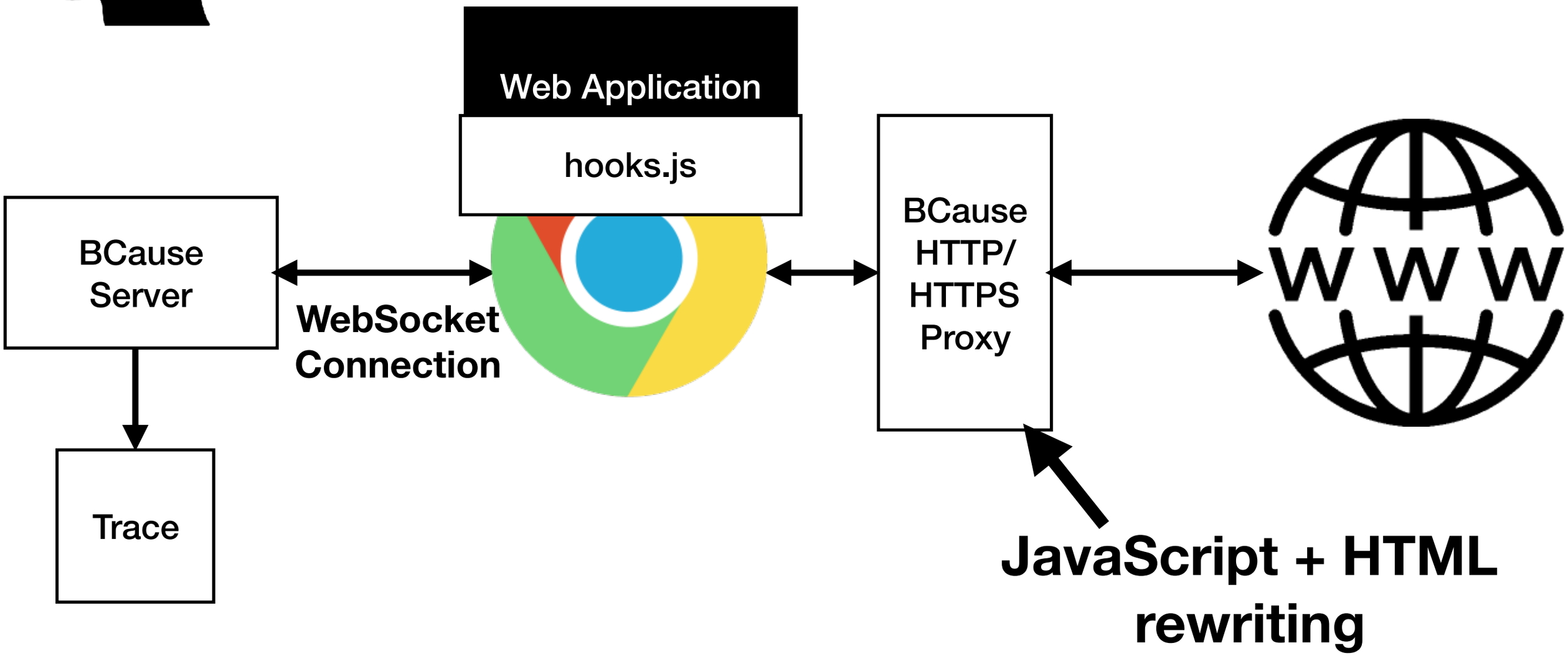
BCause System Diagram

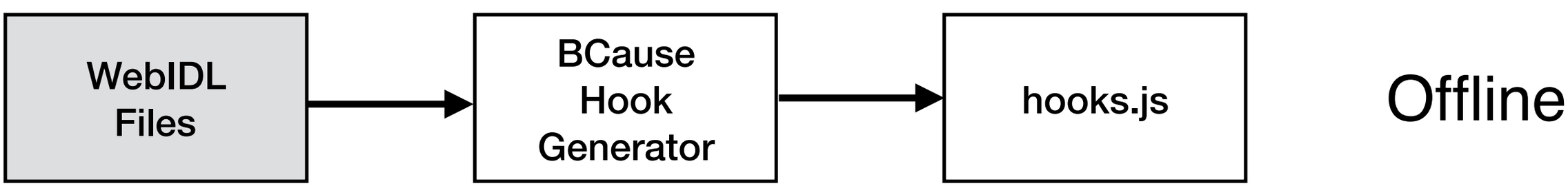




Offline

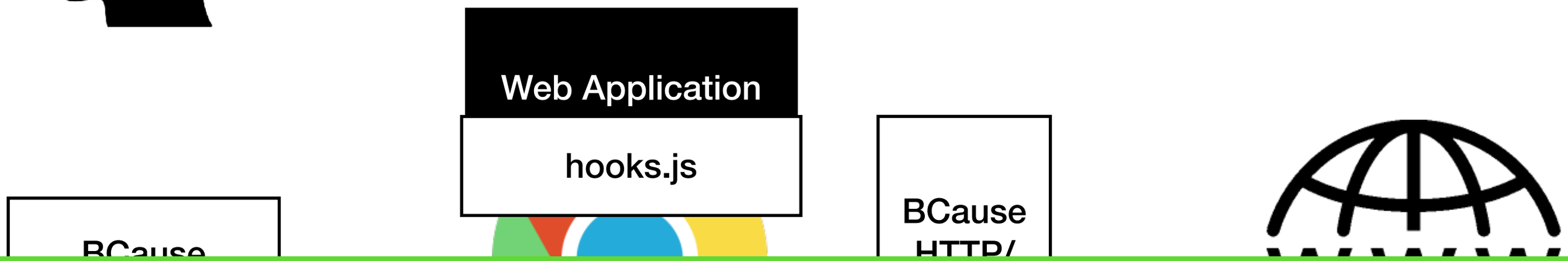
BCause System Diagram





Offline

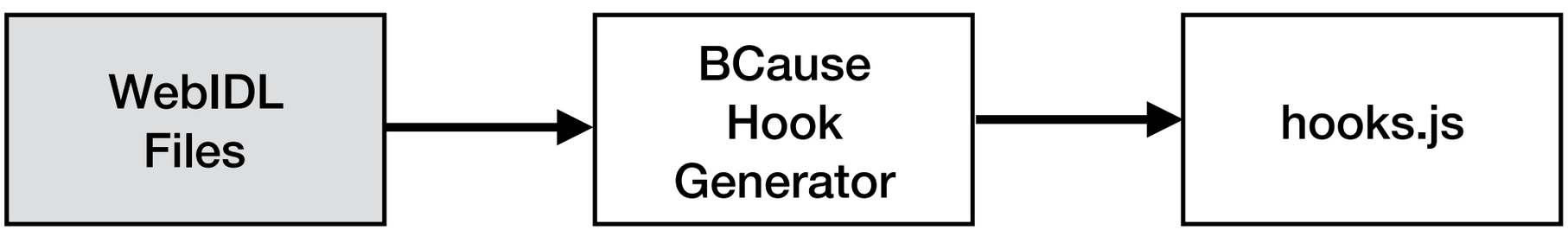
BCause System Diagram



Operates on unmodified production applications (like weather.com)

Trace

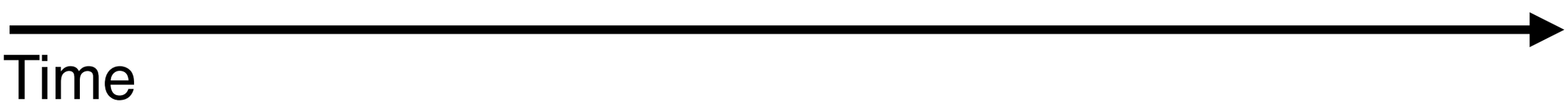
JavaScript + HTML rewriting



Offline

BCause Traces

Contain sequence of events + causal relations



BCause Traces

Contain sequence of events + causal relations

BCause Traces

Contain sequence of events + causal relations

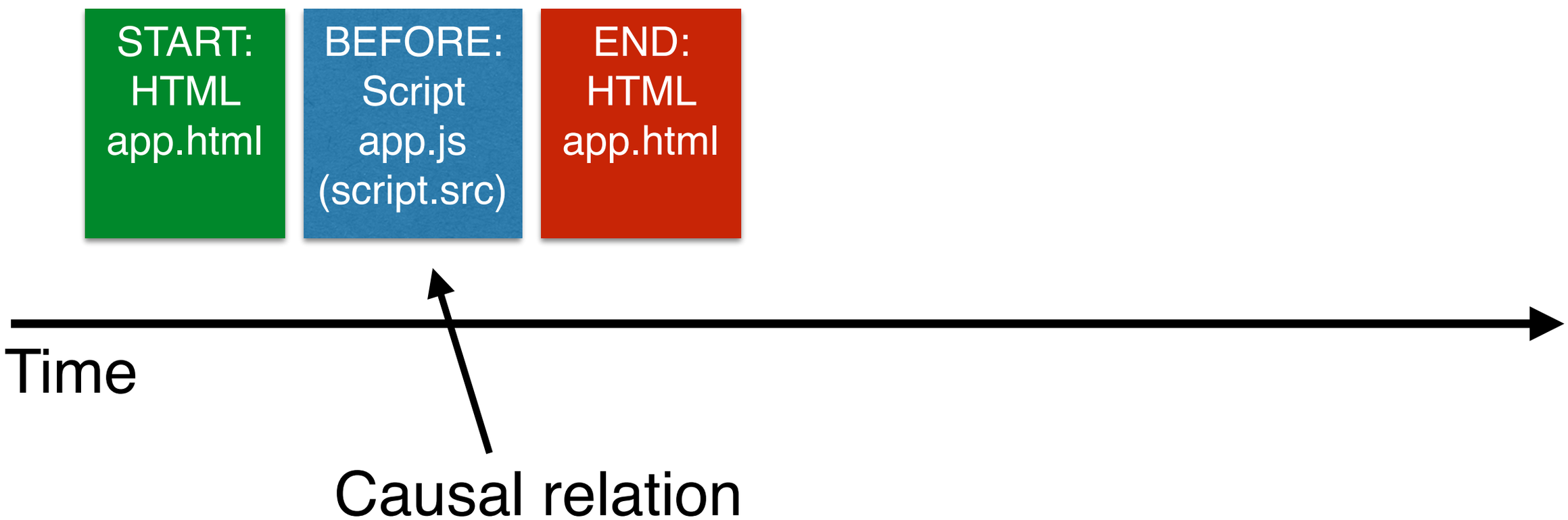
Indicate HTML initializing

BCause Traces

Contain sequence of events + causal relations

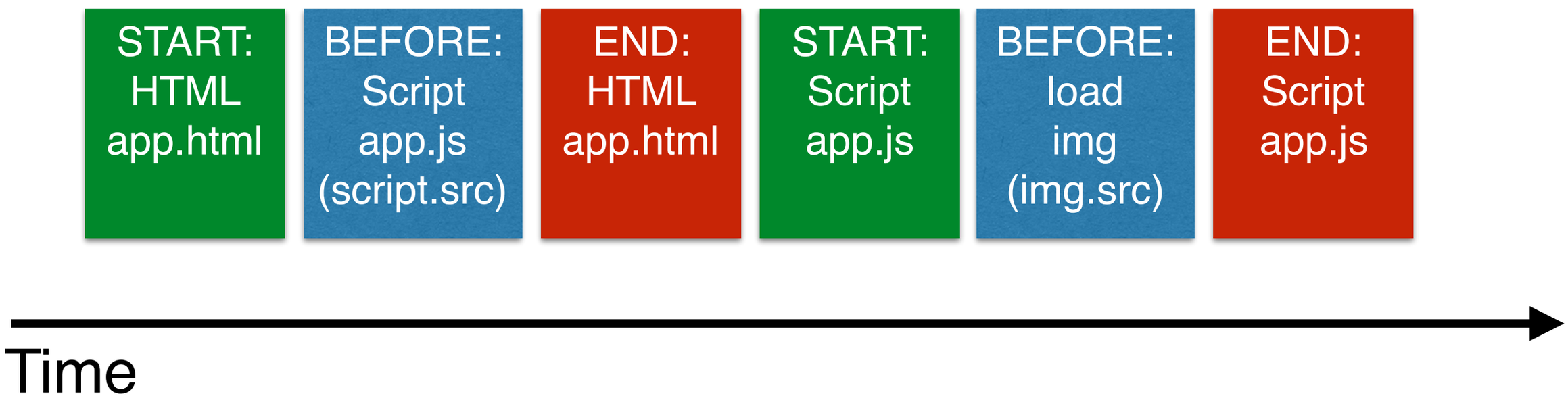
BCause Traces

Contain sequence of events + causal relations



BCause Traces

Contain sequence of events + causal relations



Traces to Causal Graphs

START: HTML app.html	BEFORE: Script app.js (script.src)	END: HTML app.html	START: Script app.js	BEFORE: load img (img.src)	END: Script app.js

Traces to Causal Graphs

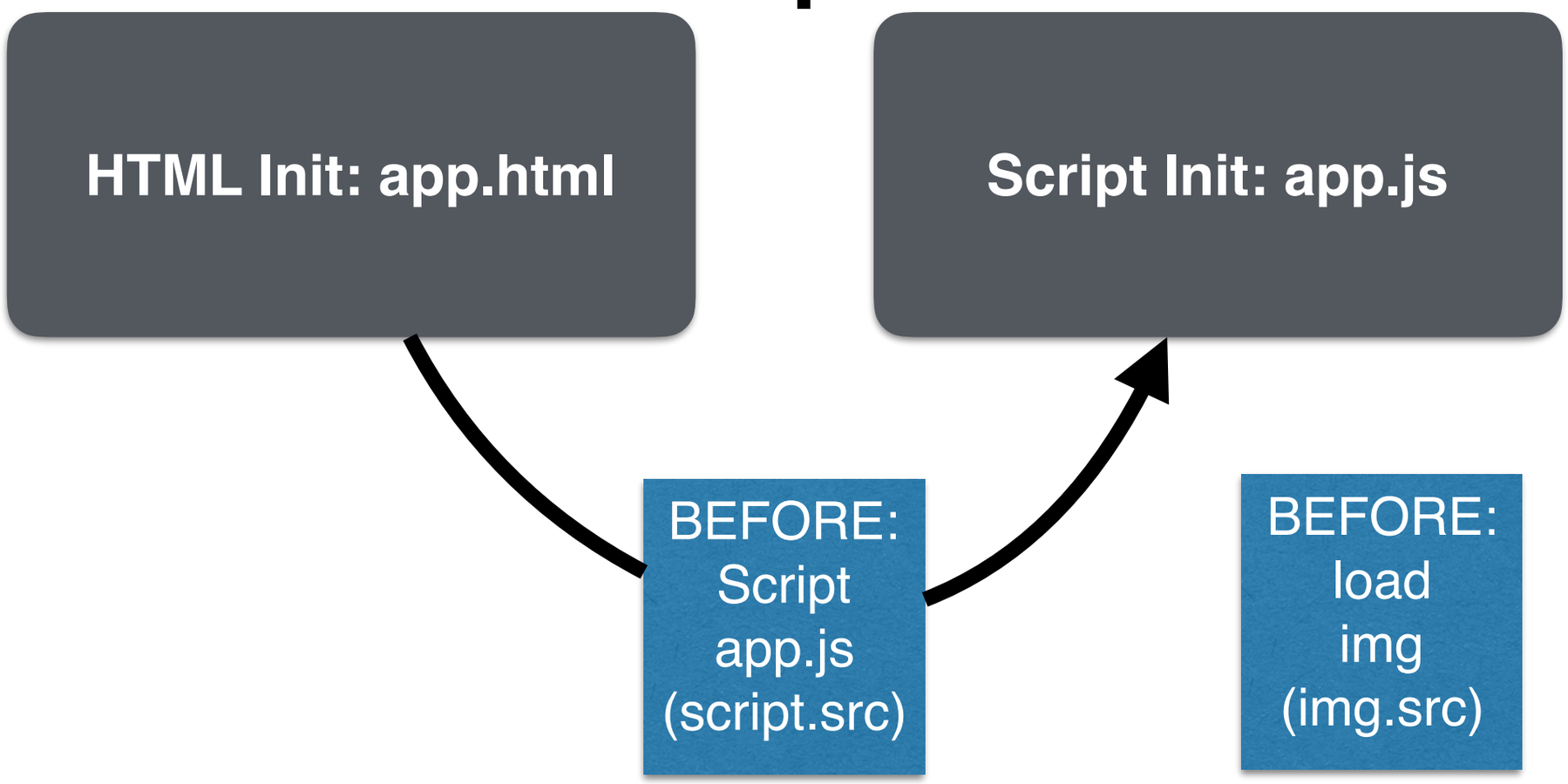
HTML Init: app.html

BEFORE:
Script
app.js
(script.src)

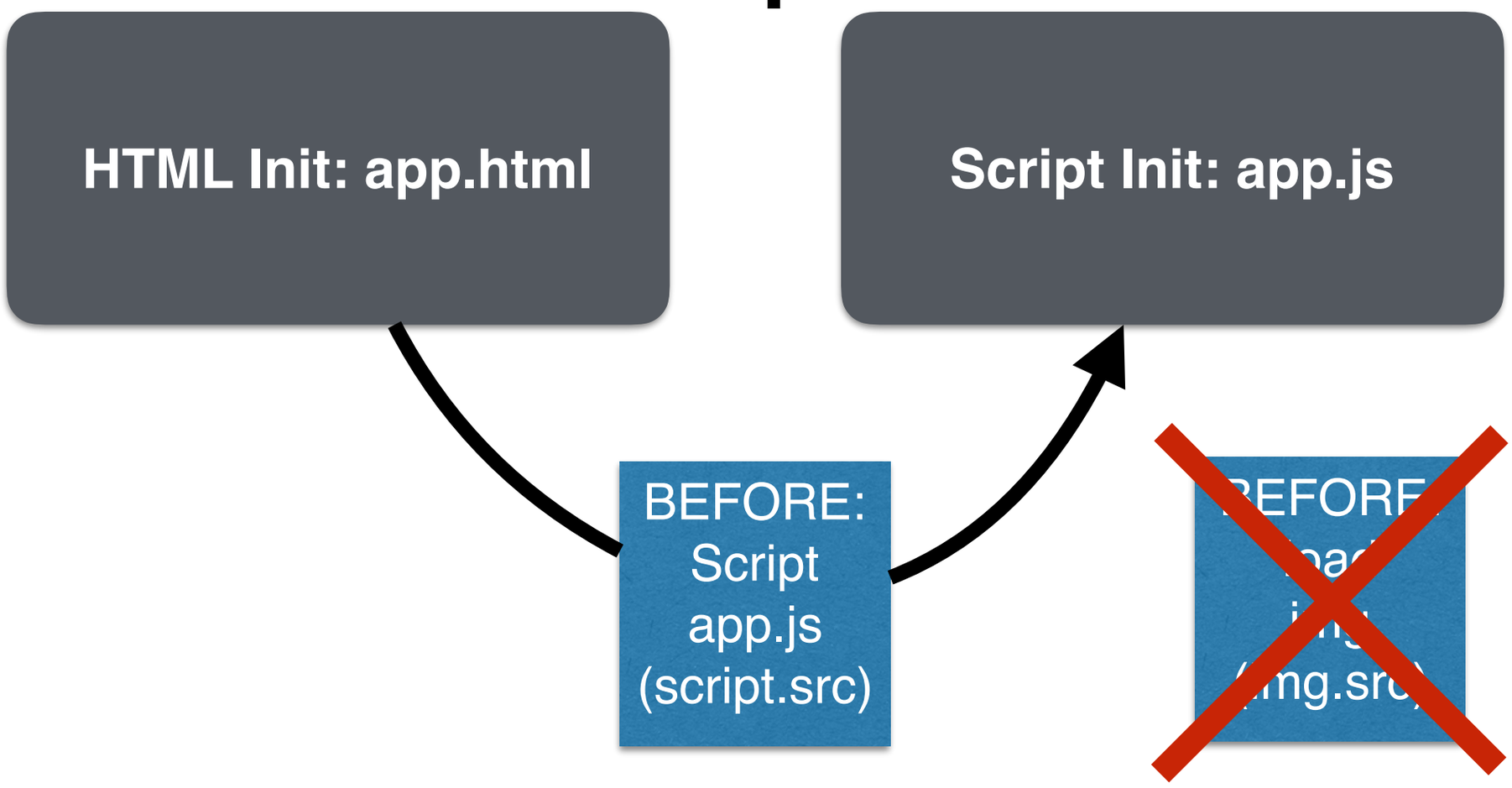
Script Init: app.js

BEFORE:
load
img
(img.src)

Traces to Causal Graphs



Traces to Causal Graphs



Primary Browser Events

Nodes in causal graph

- DOM events
- Asynchronous operations
- HTML/script initialization
- Cross-document messages

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

1. Web application must register *event handler*

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

1. Web application must register *event handler*
2. Event must happen

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

Inferred

1. Web application must register *event handler*
2. Event must happen

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

Inferred

Annotated

1. Web application must register *event handler*
2. Event must happen

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

Inferred

1. Web application must register *event handler*

Annotated

2. Event must happen

```
interface HTMLImageElement : HTMLElement {
    [Reflect, Fires=(this, load)]
      attribute DOMString src;
    attribute EventHandler onload;
};
```

DOM Event Support

Named events that occur on objects

Prerequisites (incoming edges in graph):

Inferred

1. Web application must register *event handler*

Required 66 annotations across 22 interfaces
(42 annotations across 16 interfaces without IndexedDB)

```
interface HTMLImageElement : HTMLElement {
    [Reflect, Fires=(this, load)]
      attribute DOMString src;
    attribute EventHandler onload;
};
```

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

Promise-based

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

```
setTimeout(function(){
 // Runs when timer
 // completes
}, 10);
```

Promise-based

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

```
setTimeout(function(){
 // Runs when timer
 // completes
}, 10);
```

Promise-based

```
var p = fetch("sqrl.jpg");
p.then(function() {
  // Runs when download
  // finishes
});
```

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

```
setTimeout(function(){
 // Runs when timer
 // completes
}, 10);
```

Promise-based

```
var p = fetch("sqrl.jpg");
p.then(function() {
  // Runs when download
  // finishes
});
```

Cause of event (incoming edge in graph):
Invoking the API in the first place!

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

```
setTimeout(function(){
 // Runs when timer
 // completes
}, 10);
```

Promise-based

```
var p = fetch("sqrl.jpg");
p.then(function() {
  // Runs when download
  // finishes
});
```

Inferred

Cause of event (incoming edge in graph):
Invoking the API in the first place!

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

Accept functions as arguments

Promise-based

```
var p = fetch("sqrl.jpg");
p.then(function() {
  // Runs when download
  // finishes
});
```

Inferred

Cause of event (incoming edge in graph):
Invoking the API in the first place!

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

Accept functions as arguments

Promise-based

Return Promise objects

Inferred

Cause of event (incoming edge in graph):
Invoking the API in the first place!

Asynchronous Operation Support

Tasks that occur in parallel with JavaScript

Callback-based

Promise-based

No manual annotations required!

Accept functions as arguments

Return Promise objects

Inferred

Cause of event (incoming edge in graph):
Invoking the API in the first place!

HTML/Script Initialization

Asynchronous initialization of HTML and JavaScript

Complete list of actions (incoming edges in graph):

HTMLScriptElement src
HTMLScriptElement text
Adding HTMLScriptElement to DOM
HTMLIFrameElement src
HTMLIFrameElement srcdoc
Adding HTMLIFrameElement to DOM

HTML/Script Initialization

Asynchronous initialization of HTML and JavaScript

Complete list of actions (incoming edges in graph):

HTMLScriptElement src
HTMLScriptElement text
Adding HTMLScriptElement to DOM
HTMLIFrameElement src
HTMLIFrameElement srcdoc
Adding HTMLIFrameElement to DOM

HTML/Script Initialization

Asynchronous initialization of HTML and JavaScript

Complete list of actions (incoming edges in graph):

HTMLScriptElement src
HTMLScriptElement text
Adding HTMLScriptElement to DOM
HTMLIFrameElement src
HTMLIFrameElement srcdoc
Adding HTMLIFrameElement to DOM

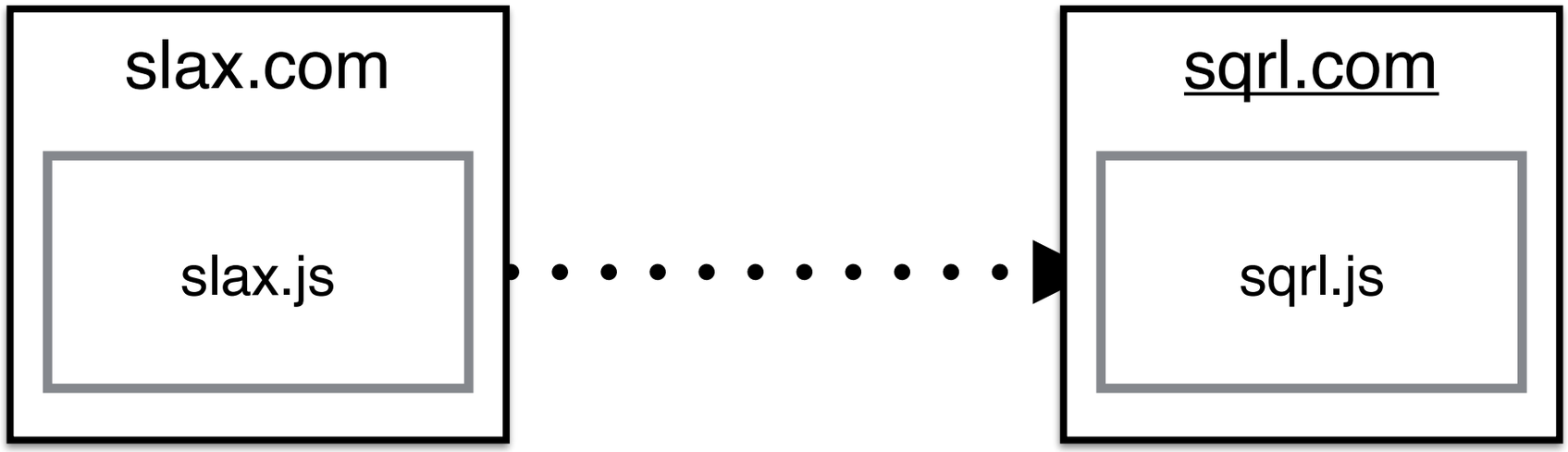
Also: Proxy modifies HTML and JavaScript
to mark start/end of initialization

Cross-document Messages

Using postMessage to communicate across different domains

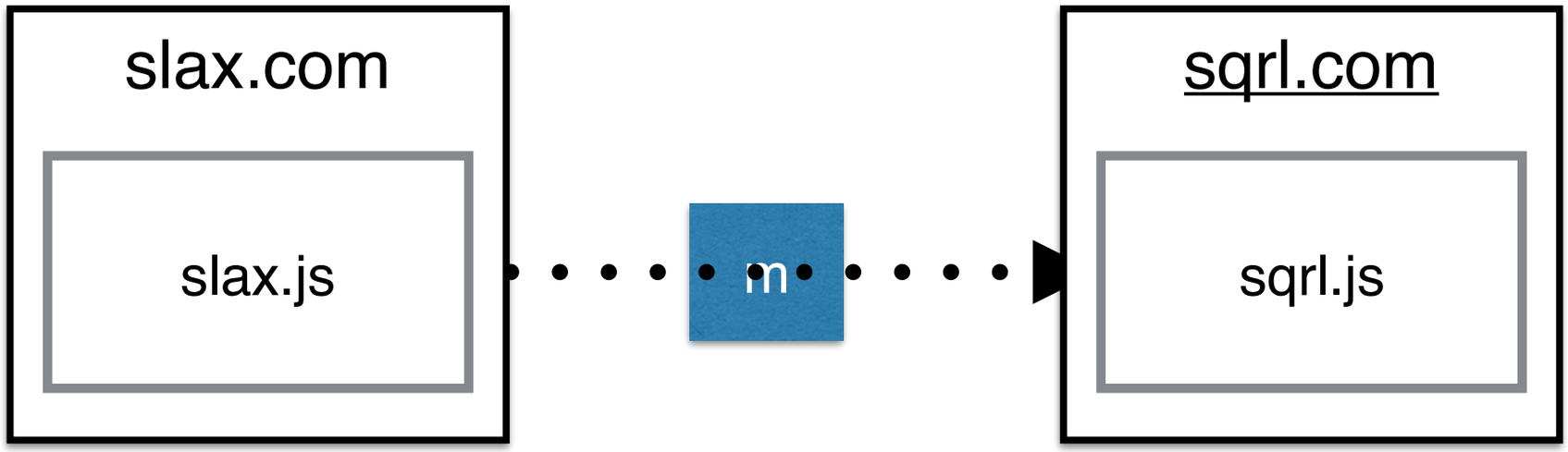
Cross-document Messages

Using postMessage to communicate across different domains



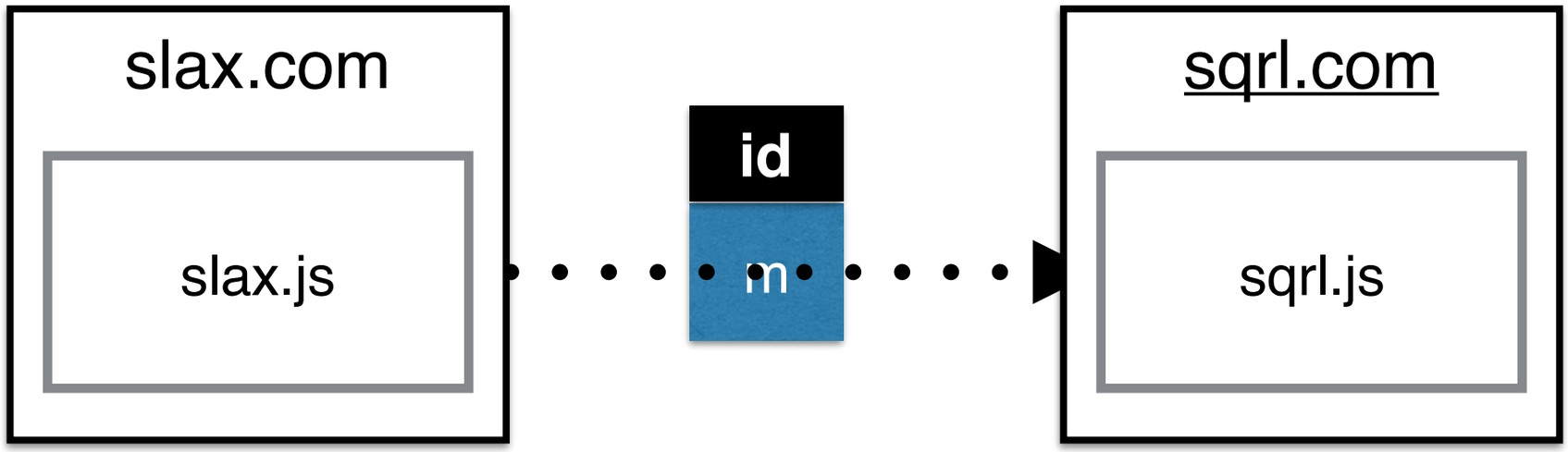
Cross-document Messages

Using postMessage to communicate across different domains



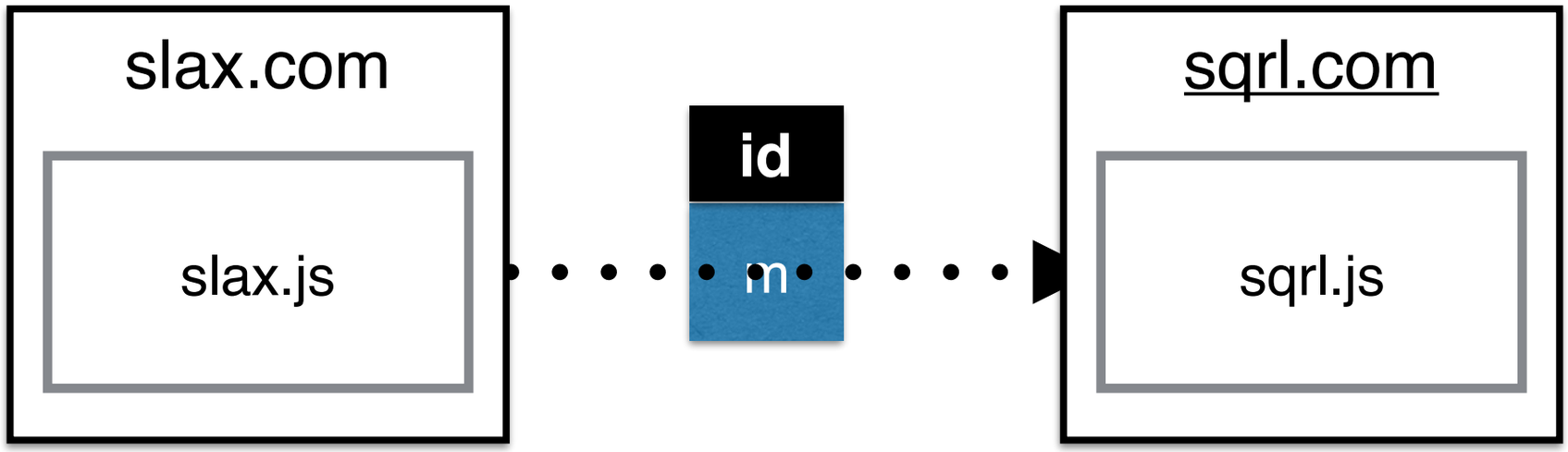
Cross-document Messages

Using postMessage to communicate across different domains



Cross-document Messages

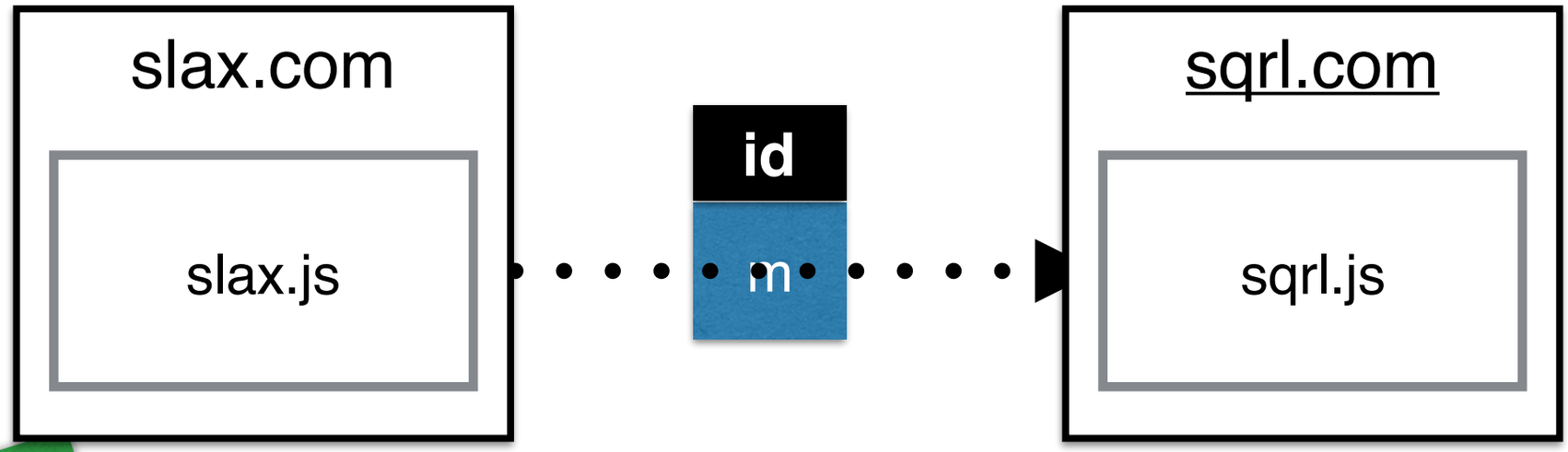
Using postMessage to communicate across different domains




```
interface MessagePort : EventTarget {
    [PostMessage] void postMessage(any
message, optional sequence<Transferable>
transfer);
};
```

Cross-document Messages

Using postMessage to communicate across different domains



Inferred

```
interface MessagePort : EventTarget {
    [PostMessage] void postMessage(any
message, optional sequence<Transferable>
transfer);
};
```

Case Study: AdBlame

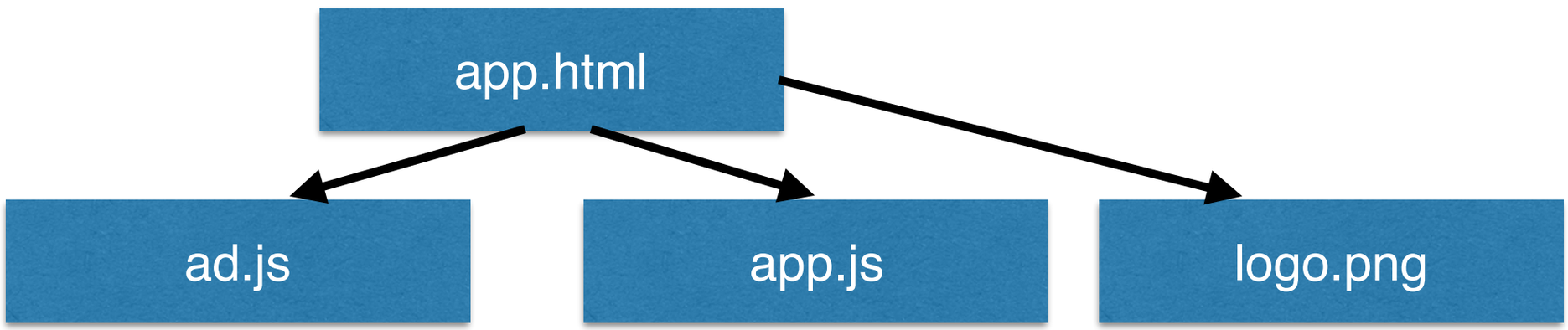
Estimates bandwidth consumption of web applications with ad blocking enabled

Ad Blockers

Filter Lists

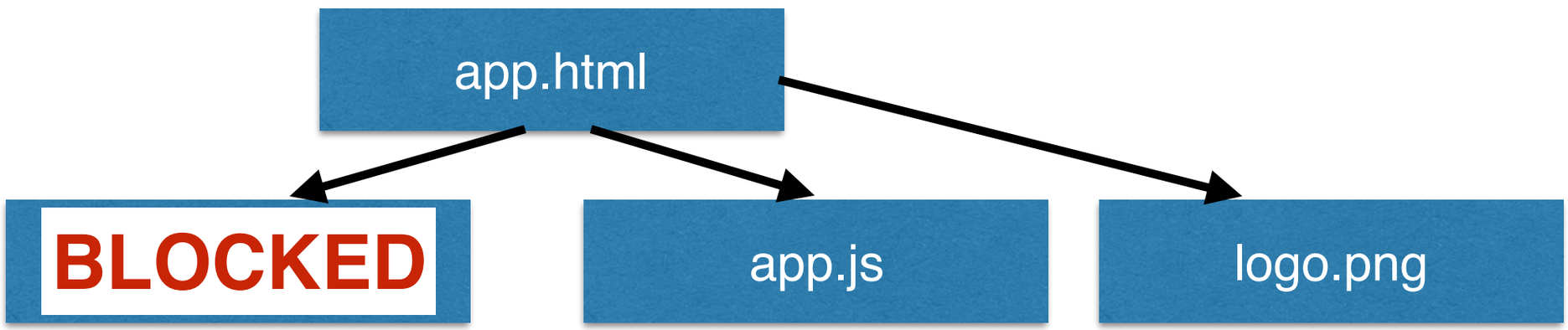
Ad Blockers

Filter Lists



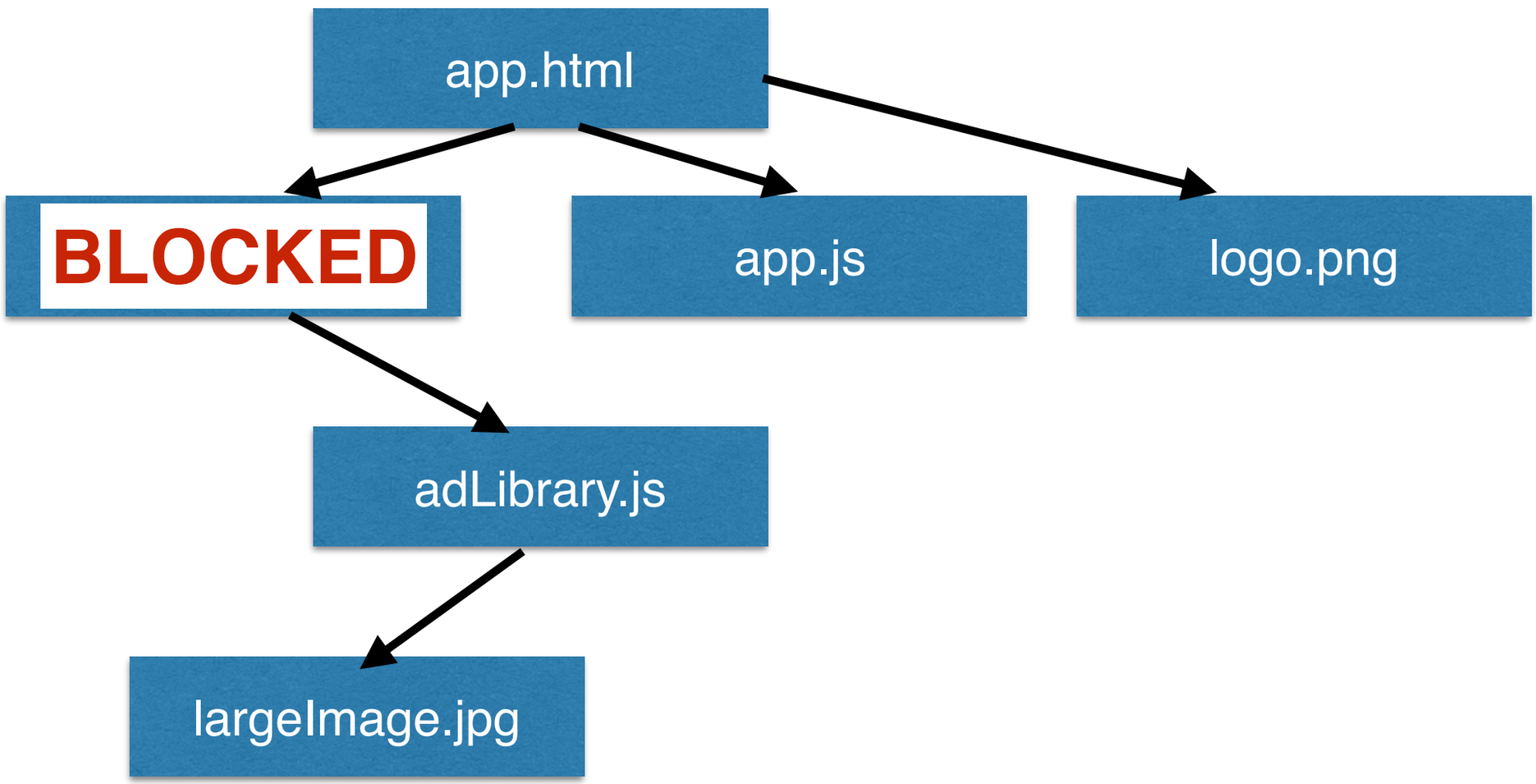
Ad Blockers

Filter Lists



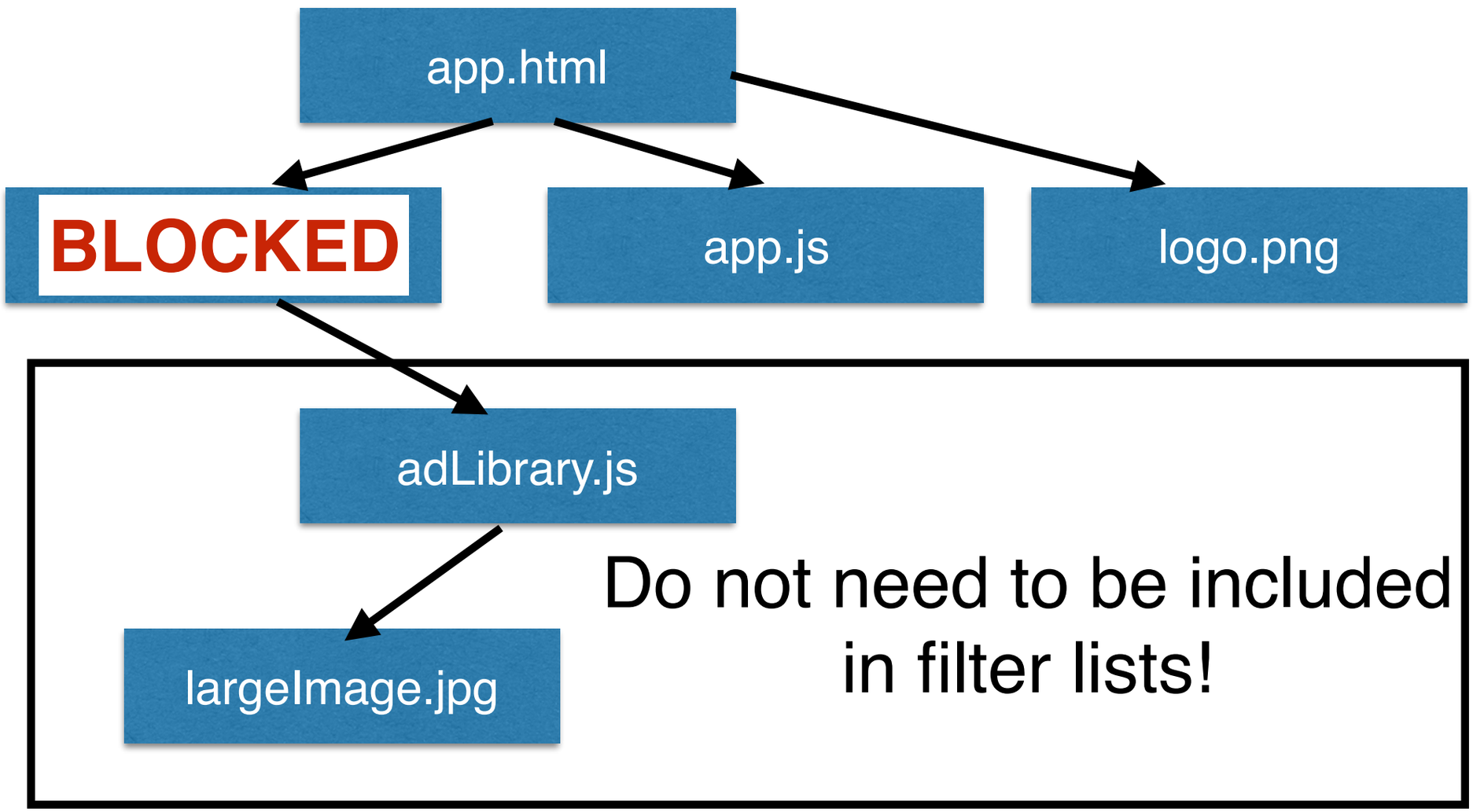
Ad Blockers

Filter Lists



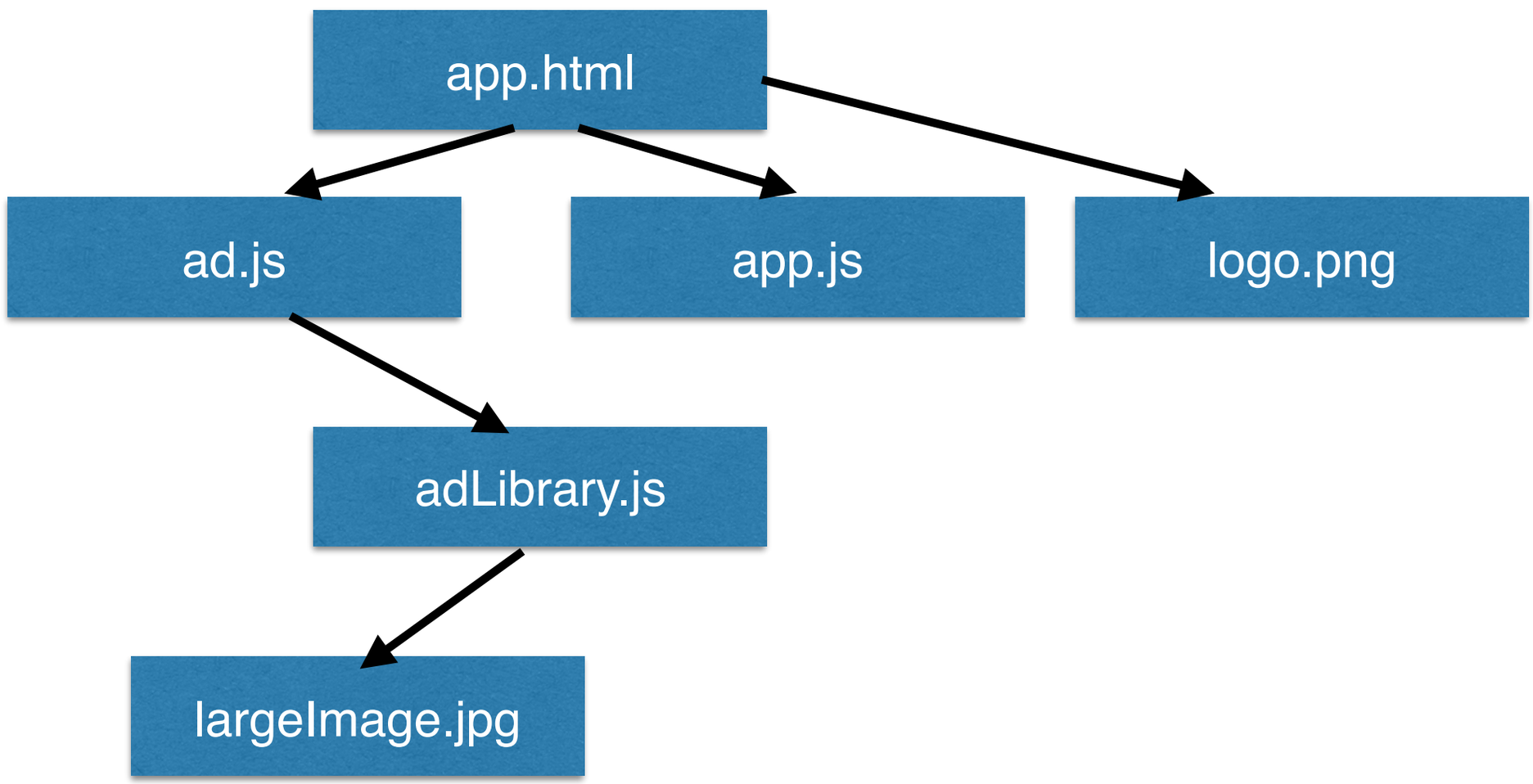
Ad Blockers

Filter Lists



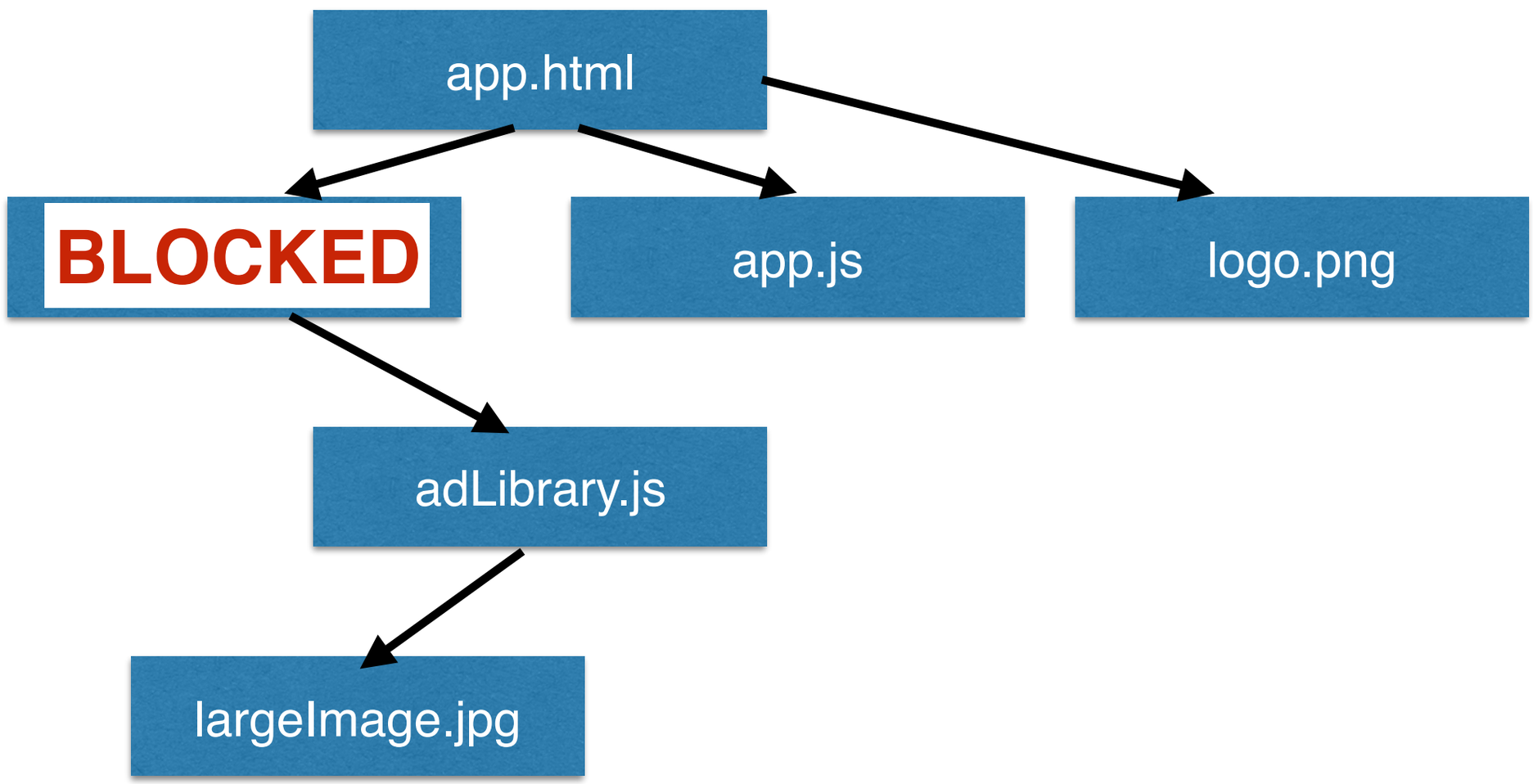
Case Study: AdBlame

Estimates bandwidth consumption of web applications with ad blocking enabled



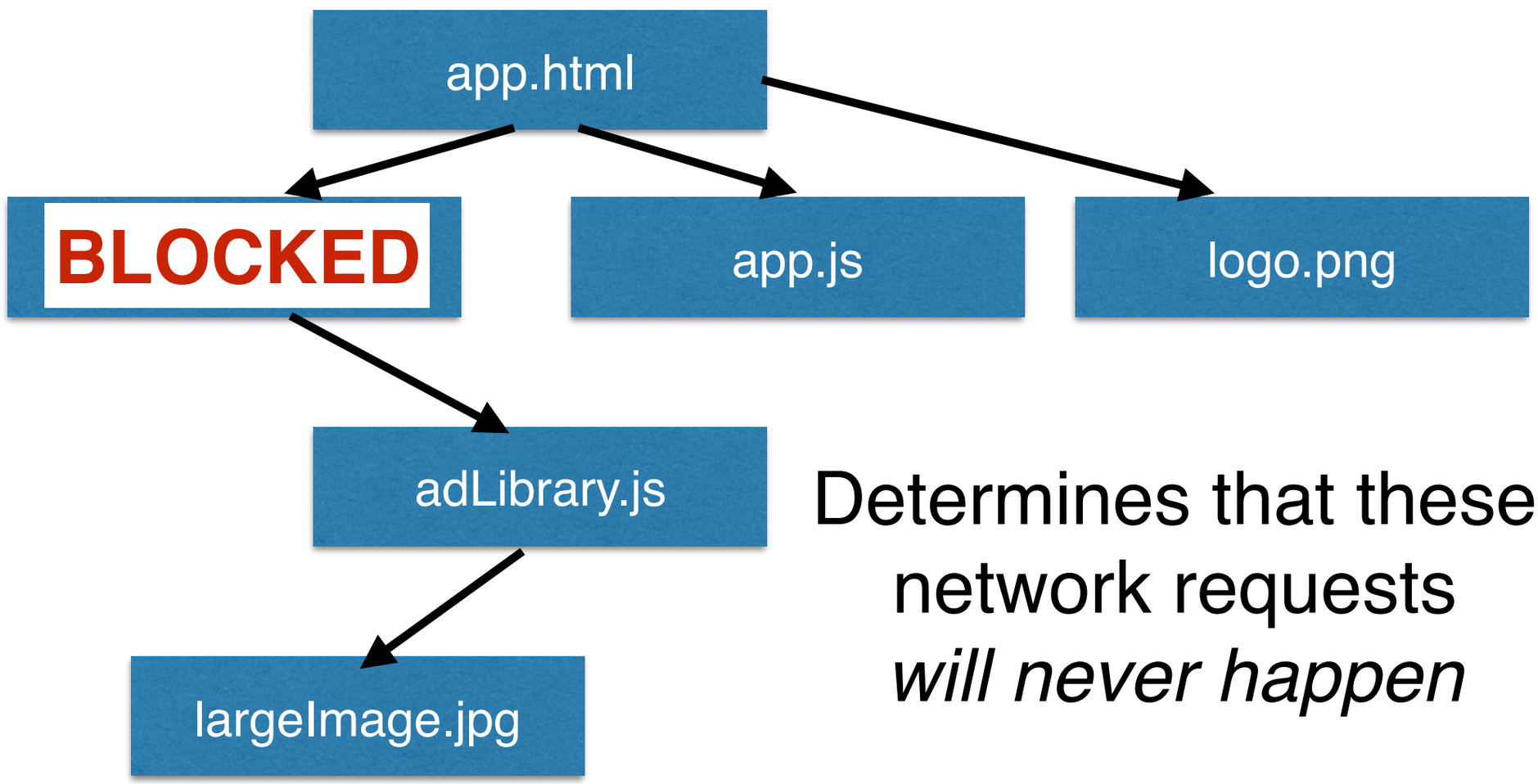
Case Study: AdBlame

Estimates bandwidth consumption of web applications with ad blocking enabled



Case Study: AdBlame

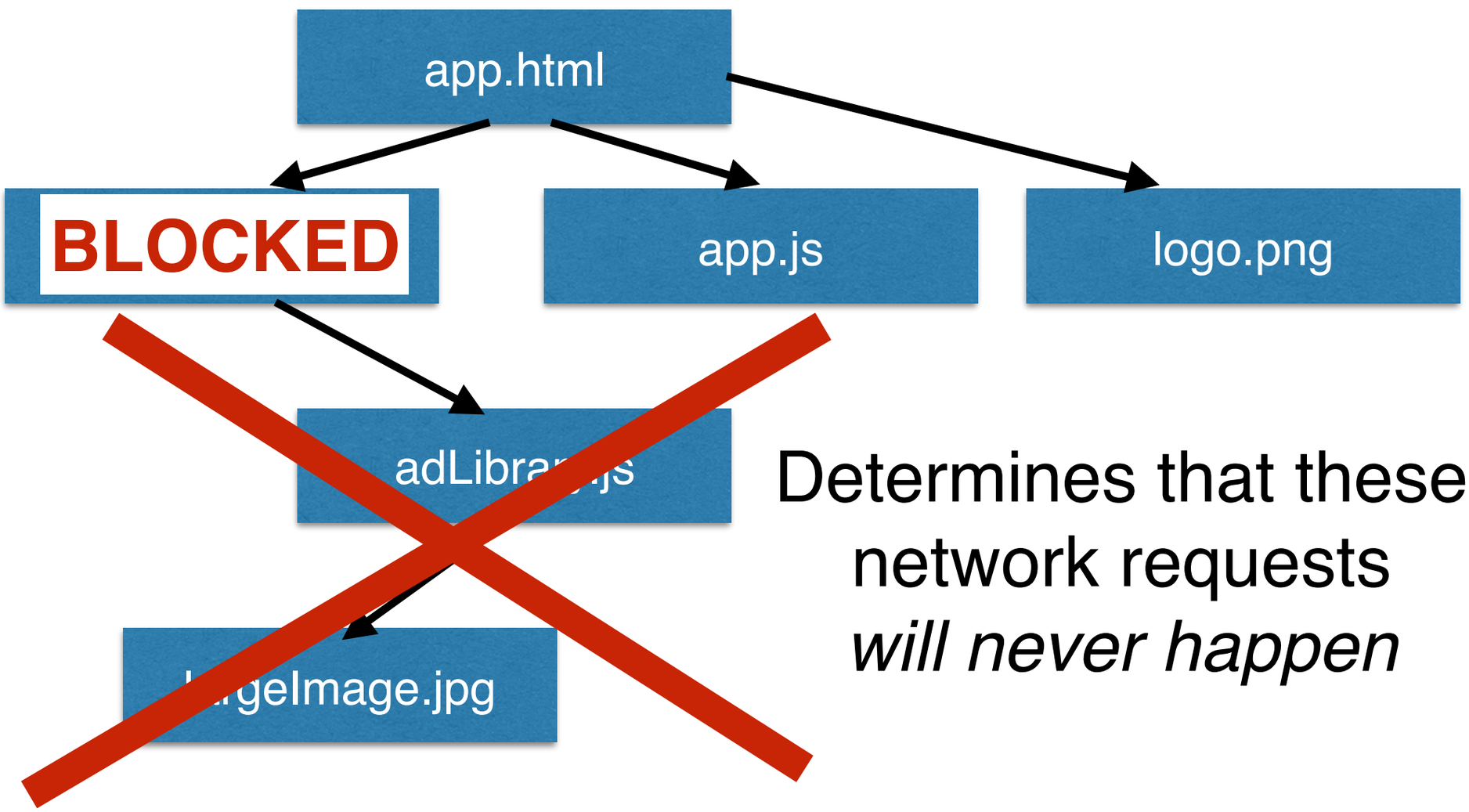
Estimates bandwidth consumption of web applications with ad blocking enabled



Determines that these network requests *will never happen*

Case Study: AdBlame

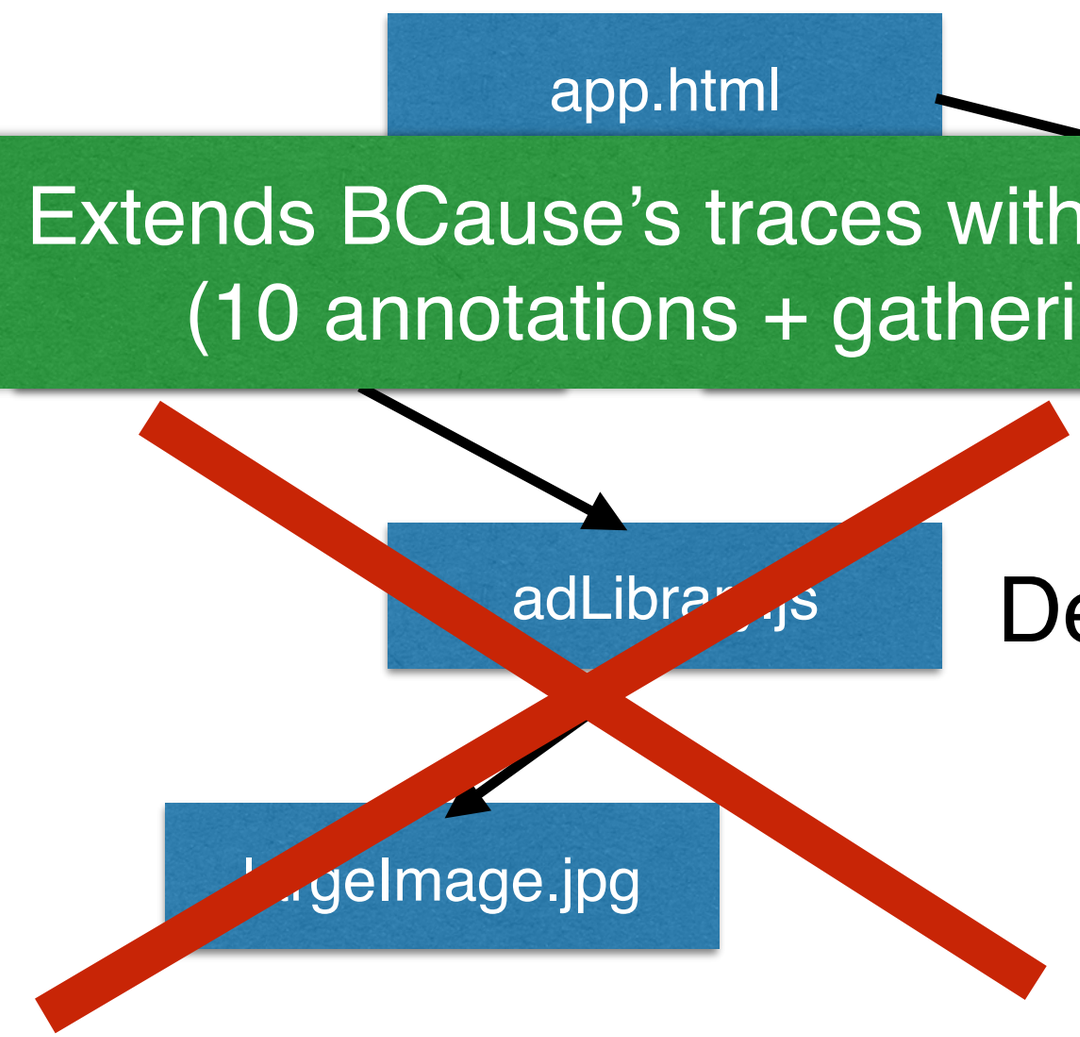
Estimates bandwidth consumption of
web applications with ad blocking enabled



Determines that these
network requests
will never happen

Case Study: AdBlame

Estimates bandwidth consumption of web applications with ad blocking enabled



Extends BCause's traces with network request entries (10 annotations + gathering stats from proxy)

Determines that these network requests *will never happen*

AdBlame Evaluation

Benchmarks: Ad-heavy websites

weather.com cnn.com

AdBlame Evaluation

Benchmarks: Ad-heavy websites

weather.com cnn.com

Baseline: Running network requests through filter list

AdBlame Evaluation

Benchmarks: Ad-heavy websites

weather.com cnn.com

Baseline: Running network requests through filter list

Ground truth: Visiting same website with uBlock Origin

AdBlame Evaluation

Benchmarks: Ad-heavy websites

weather.com cnn.com

Baseline: Running network requests through filter list

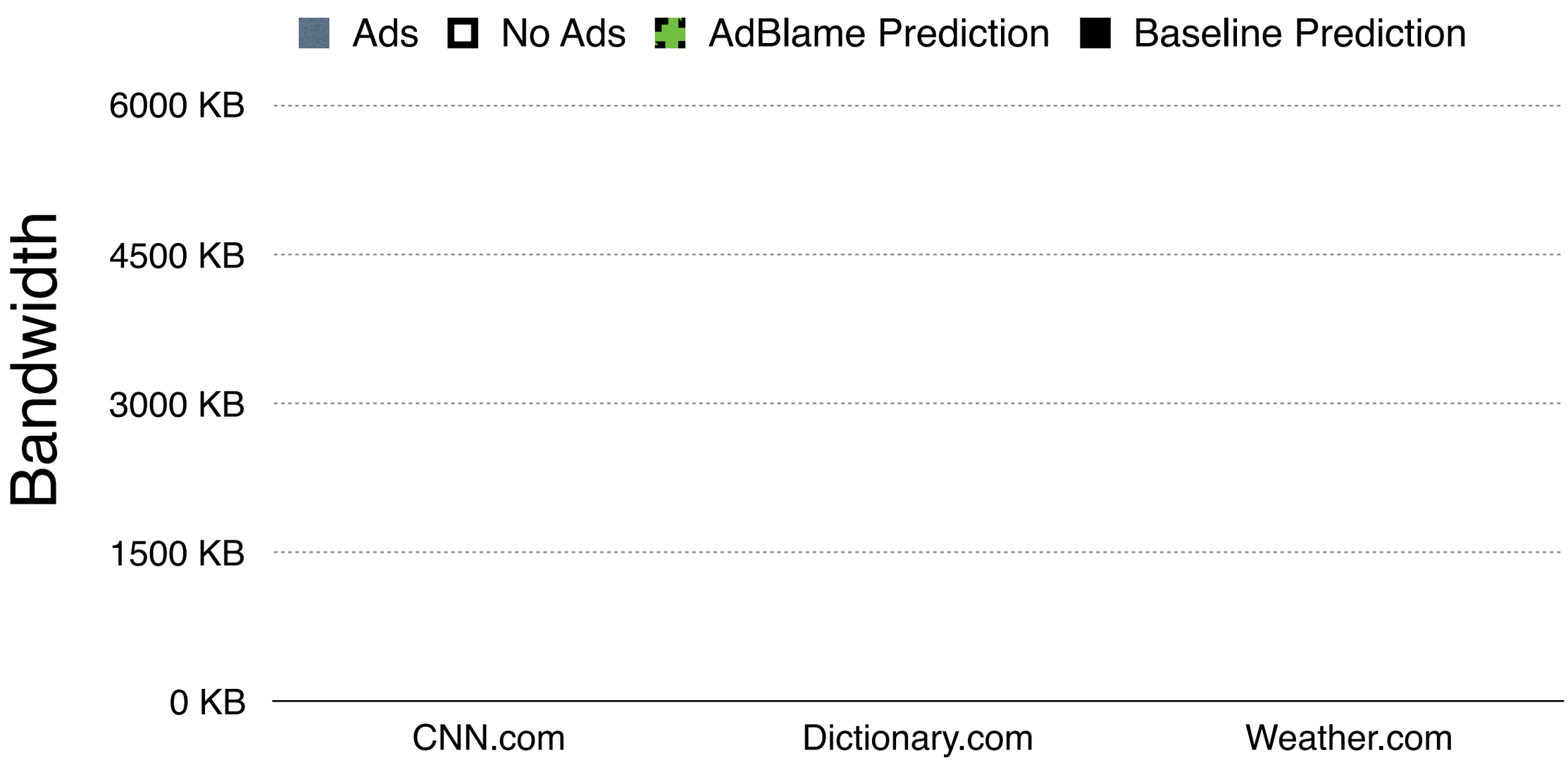
Ground truth: Visiting same website with uBlock Origin

Filter lists: EasyList and EasyPrivacy

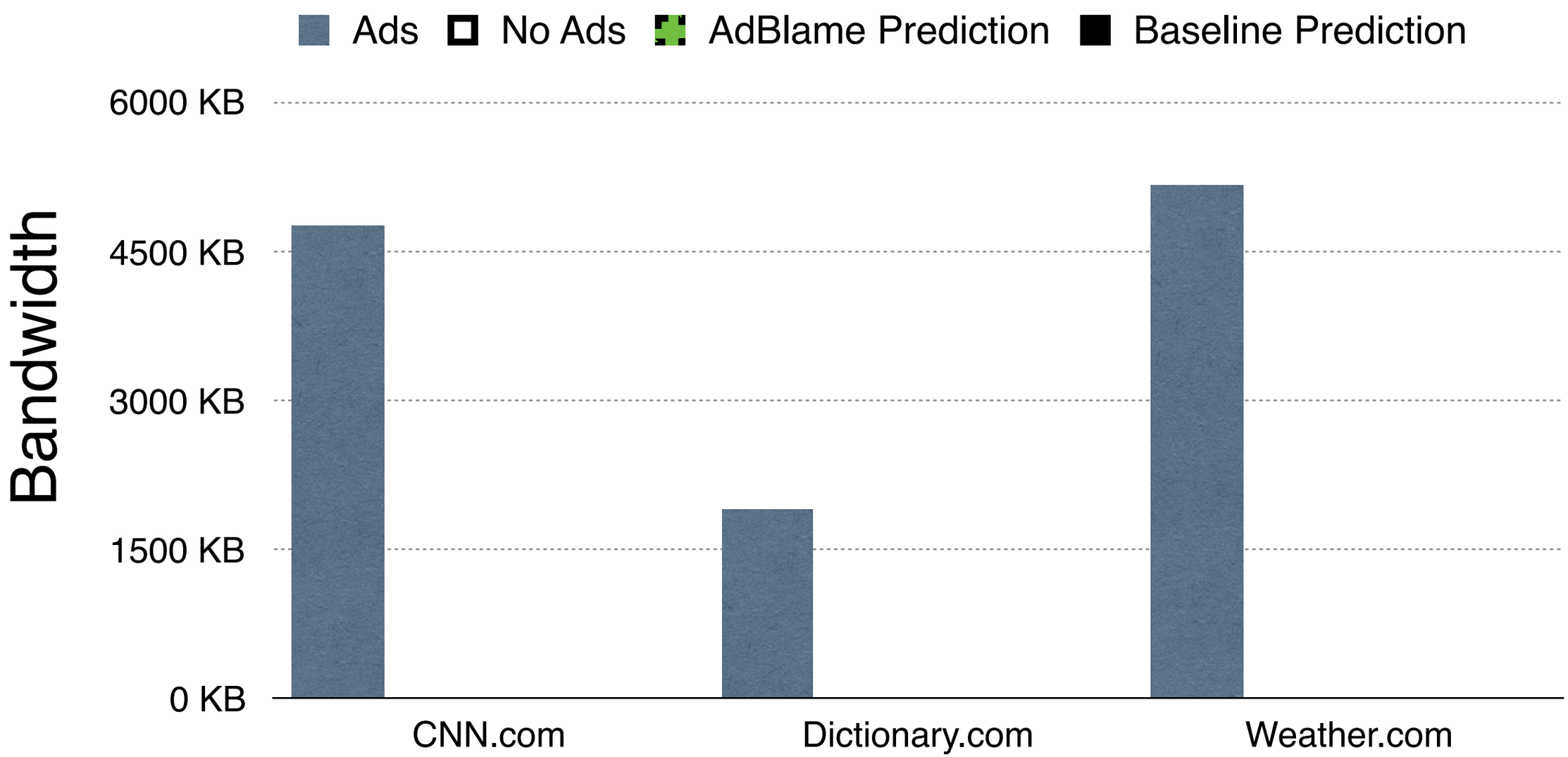
AdBlame Evaluation

Bandwidth

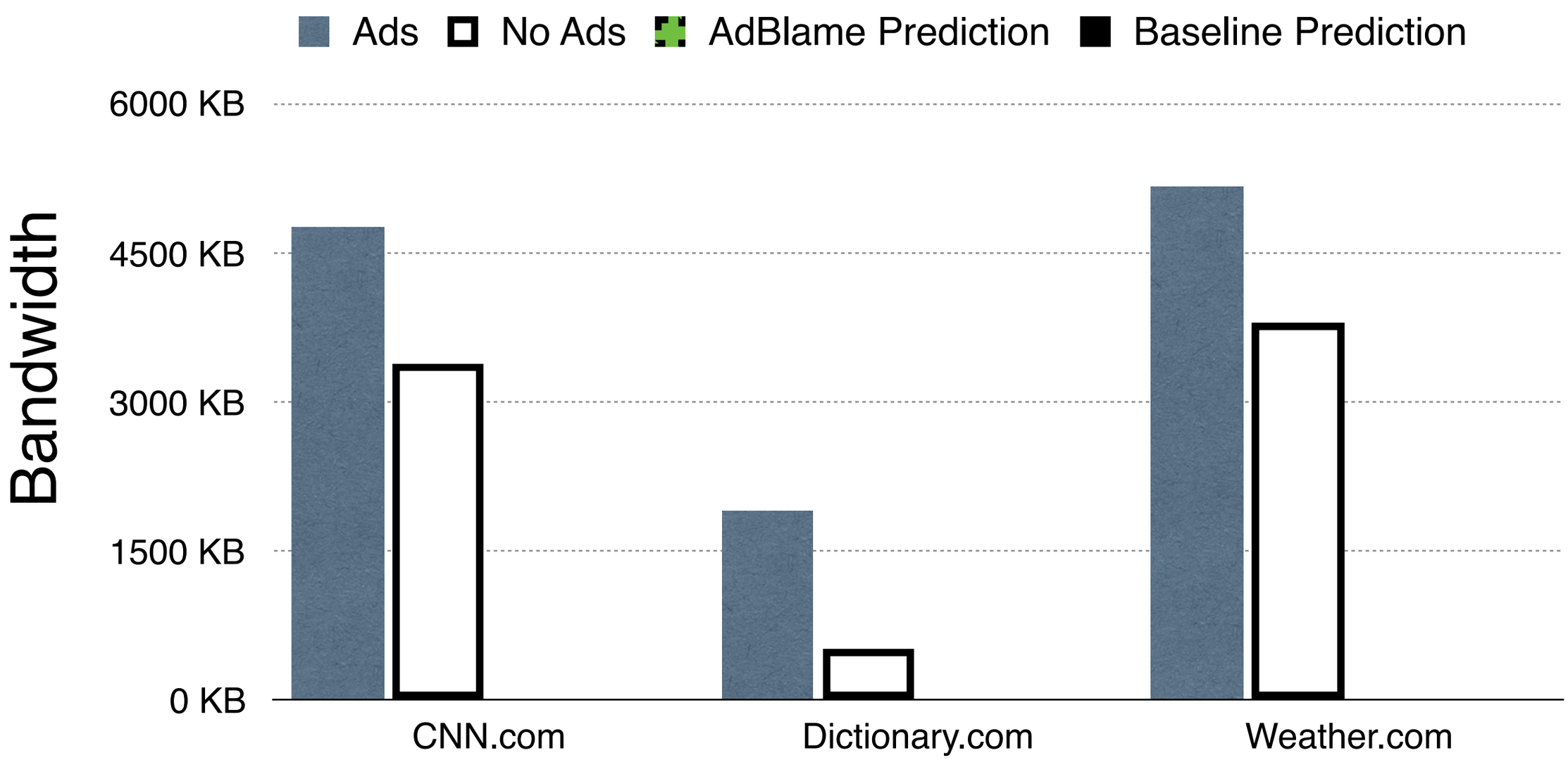
AdBlame Evaluation



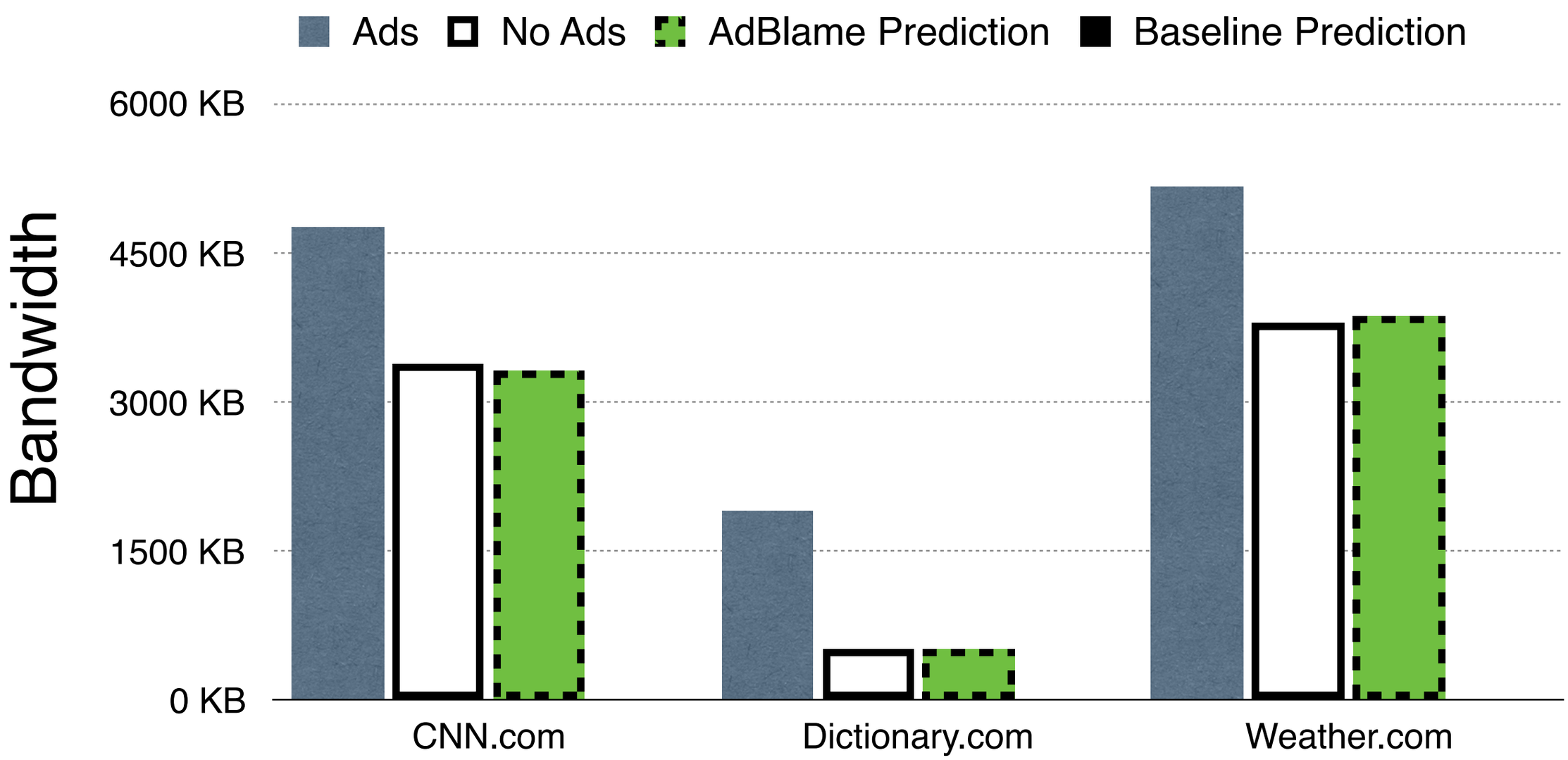
AdBlame Evaluation



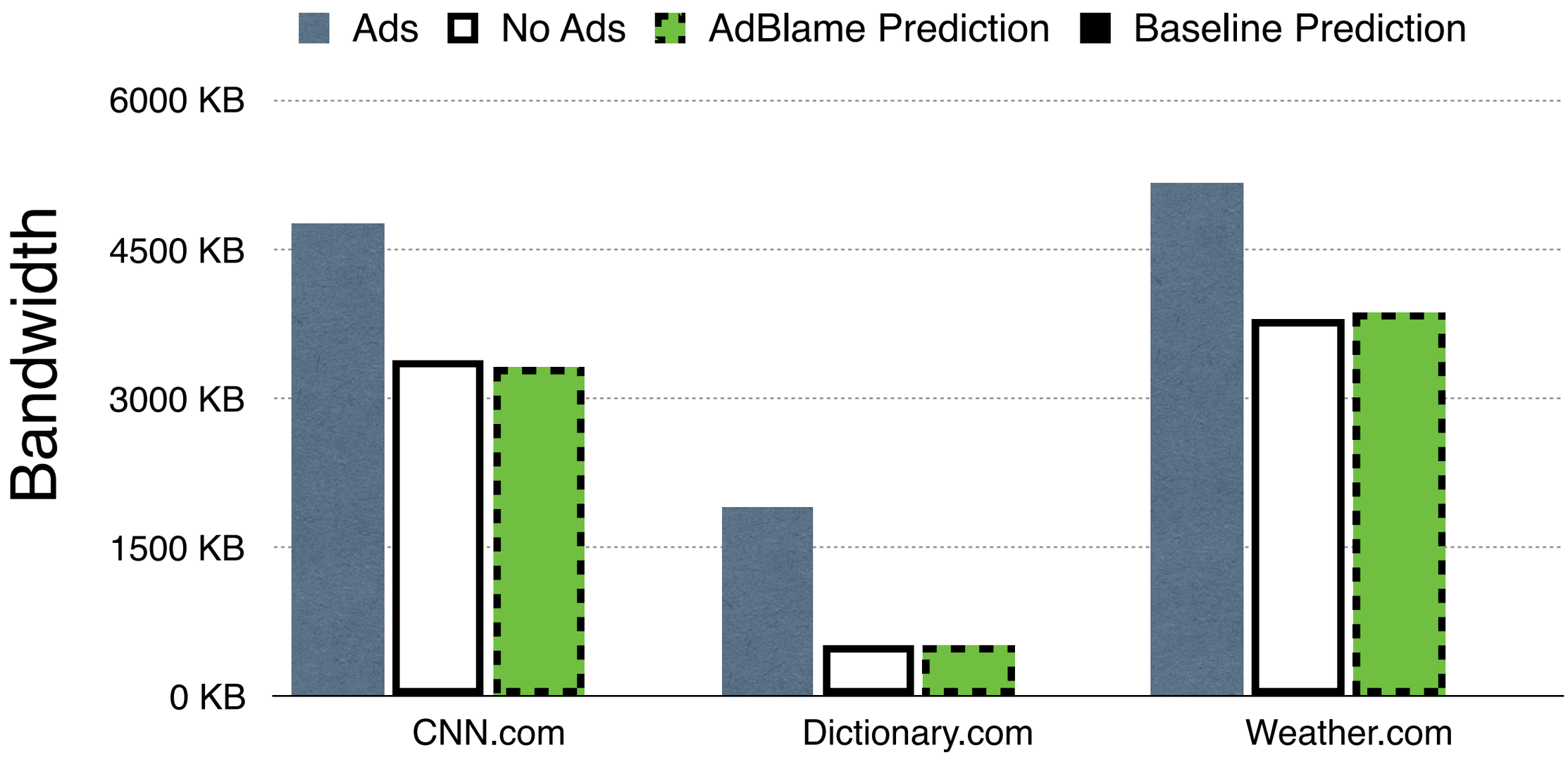
AdBlame Evaluation



AdBlame Evaluation

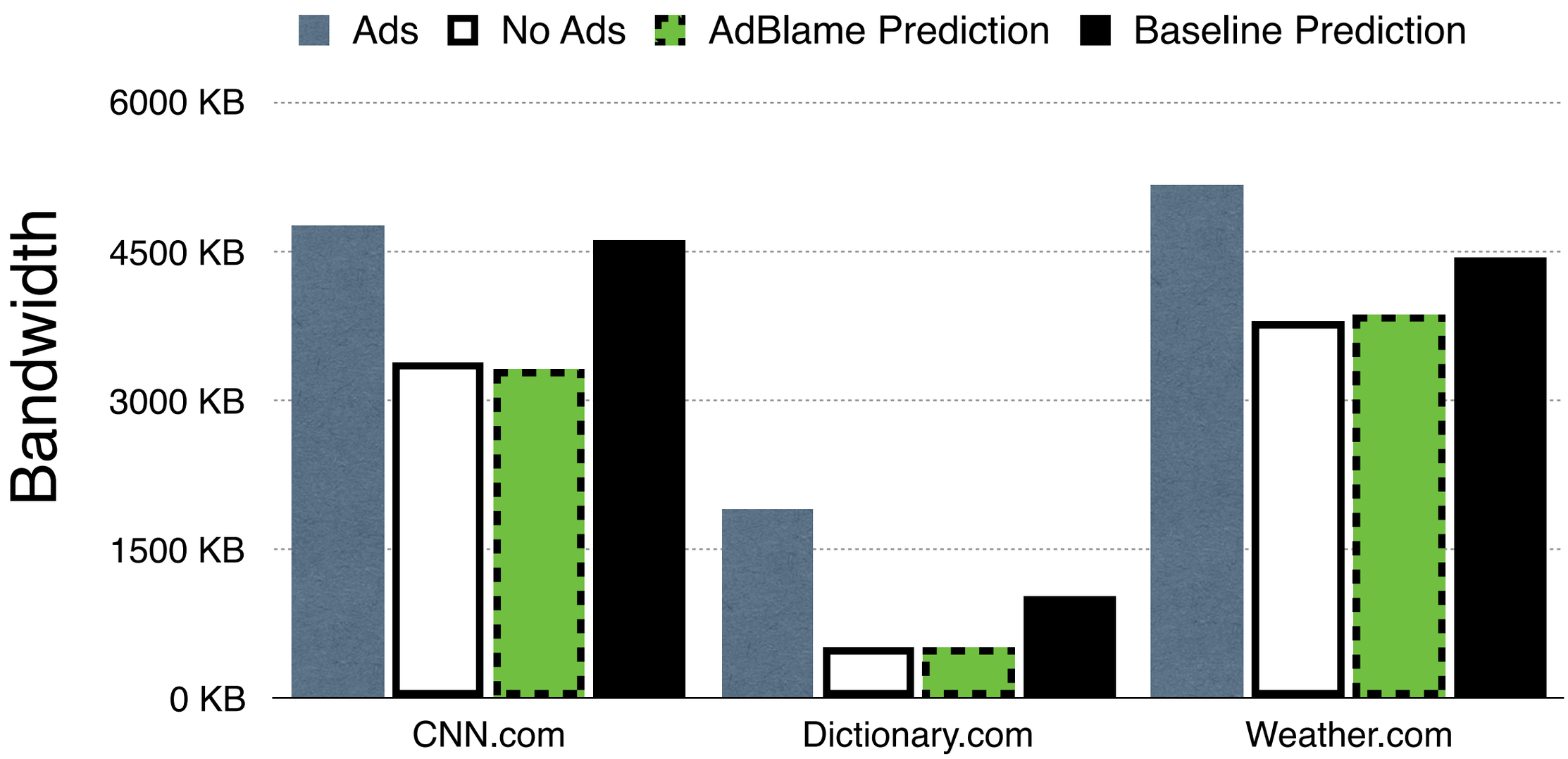


AdBlame Evaluation



AdBlame: ***within 2.2%*** of ground truth

AdBlame Evaluation



AdBlame: ***within 2.2%*** of ground truth

Baseline: ***within 50%*** of ground truth

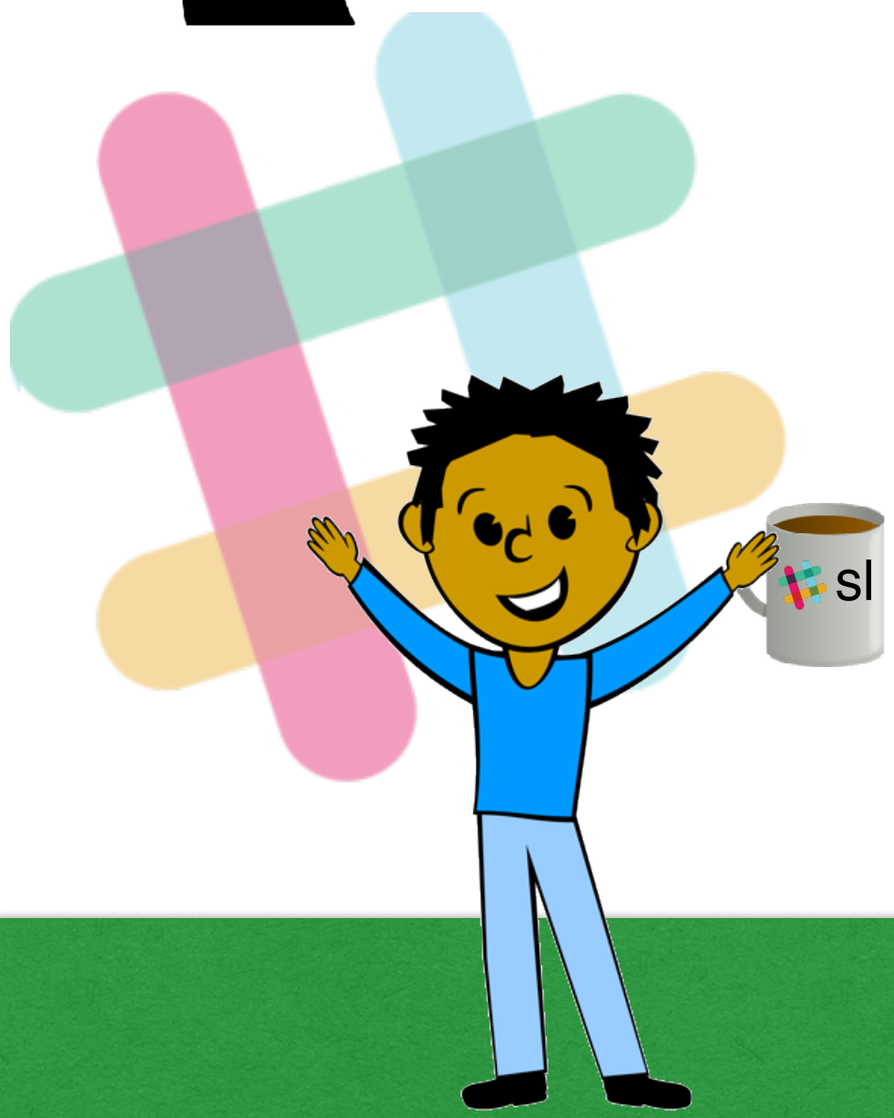
slax
sl

slax.html

slax.html

↓

ad.html



slax

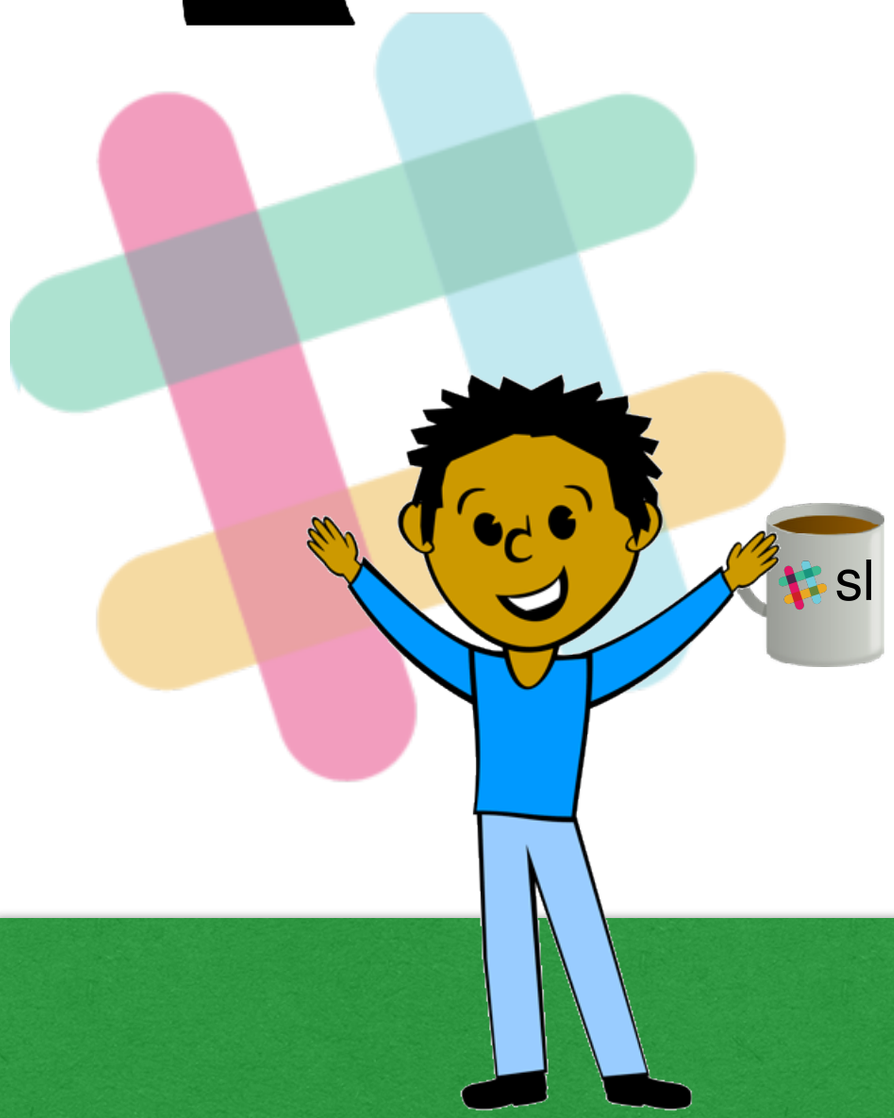
slax.html

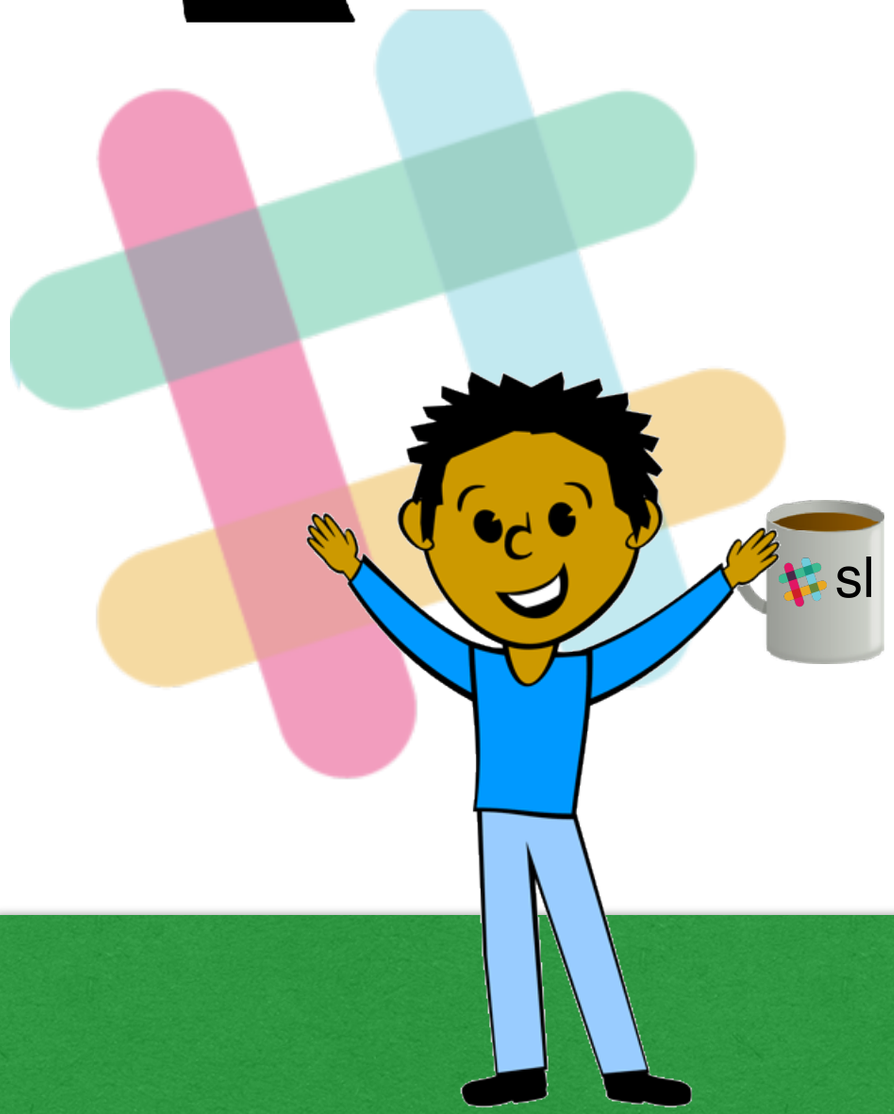
↓

ad.html

↓

ad-324j234j.js





slax.html

↓

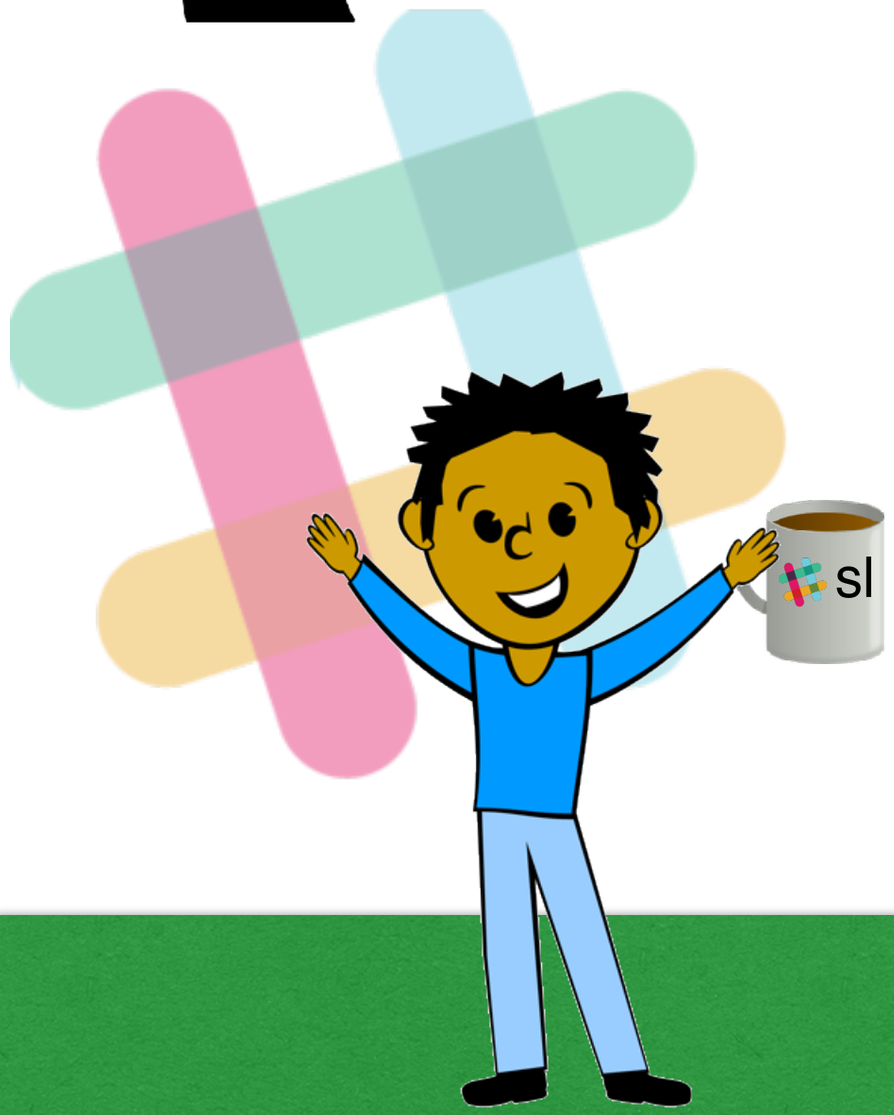
ad.html

↓

ad-324j234j.js

↓

data:text/javascript…



slax

slax.html

↓

ad.html

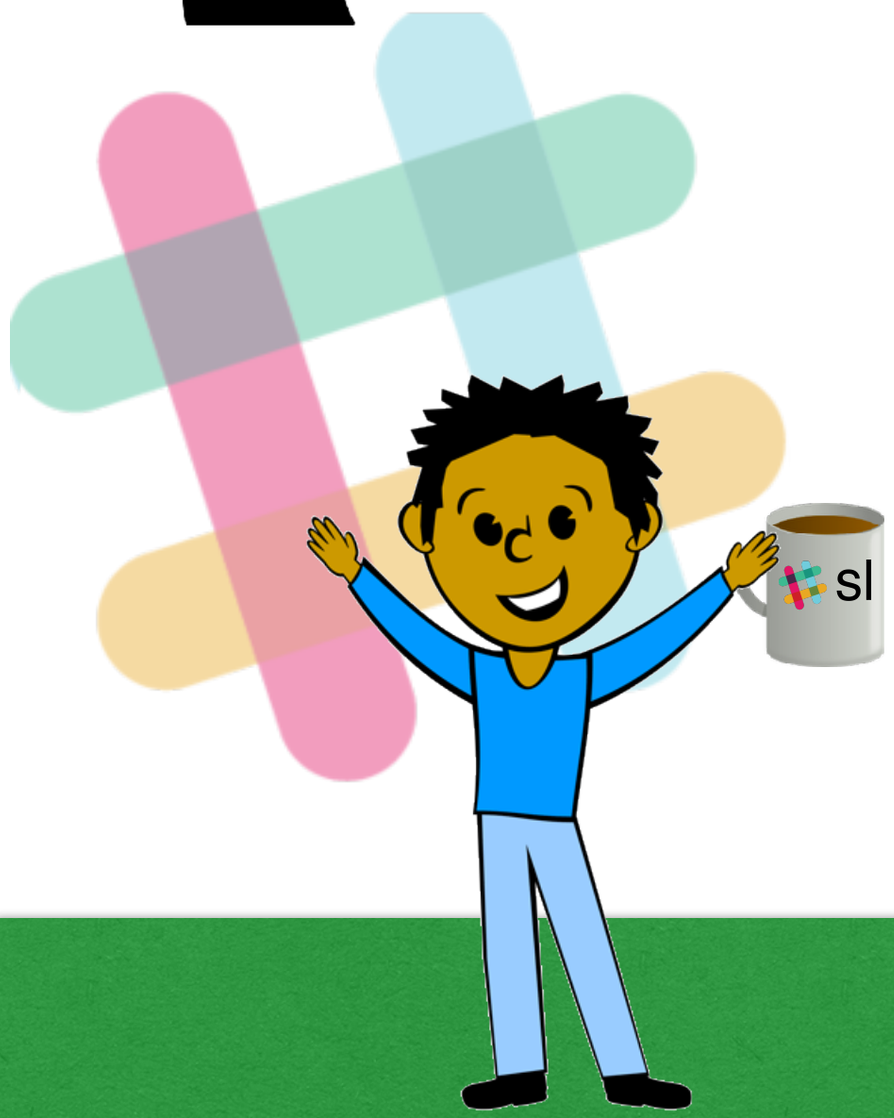
↓

ad-324j234j.js

↓

data:text/javascript…

↓



slax.html

↓

ad.html

↓

ad-324j234j.js

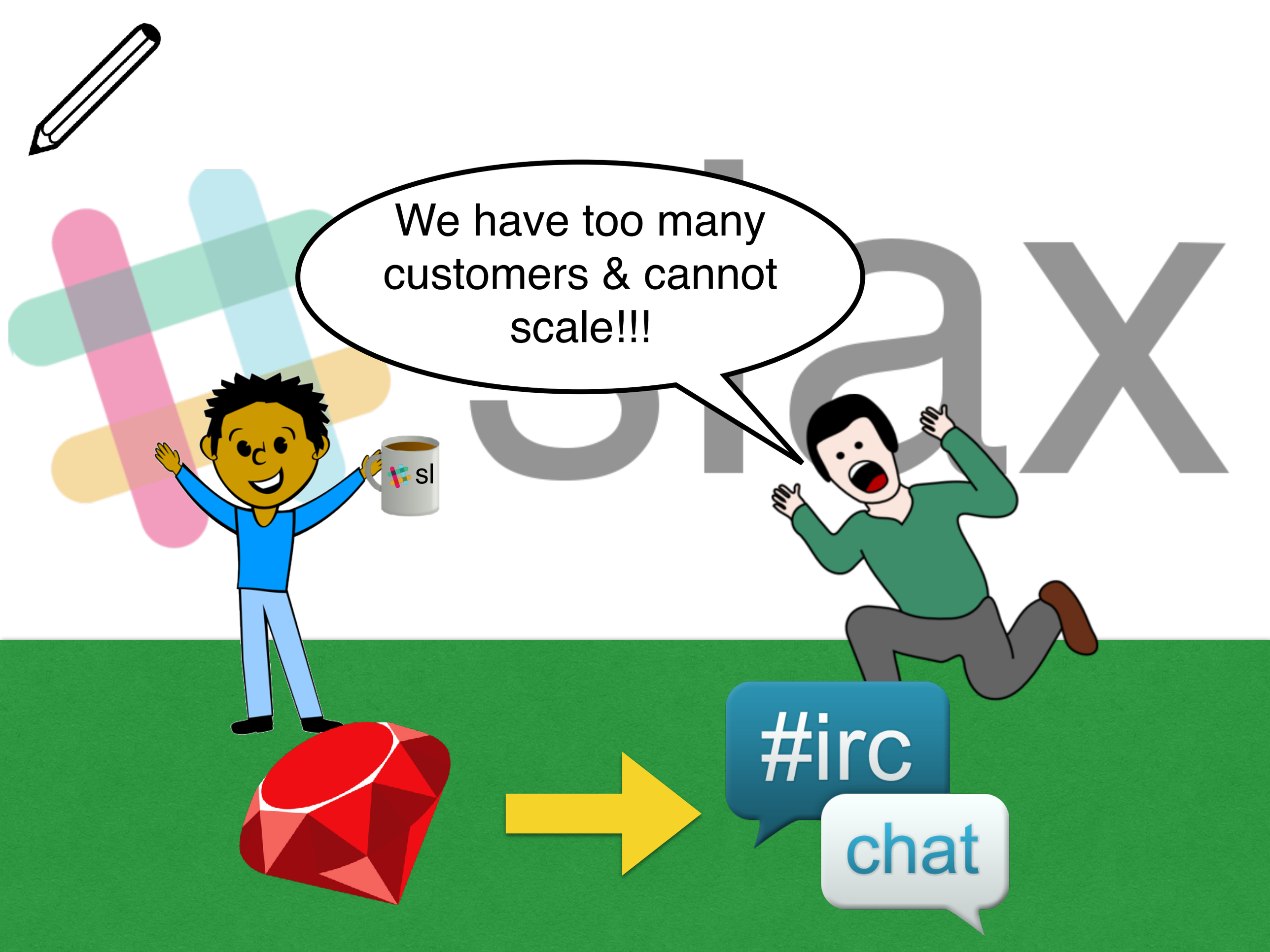
↓

data:text/javascript…

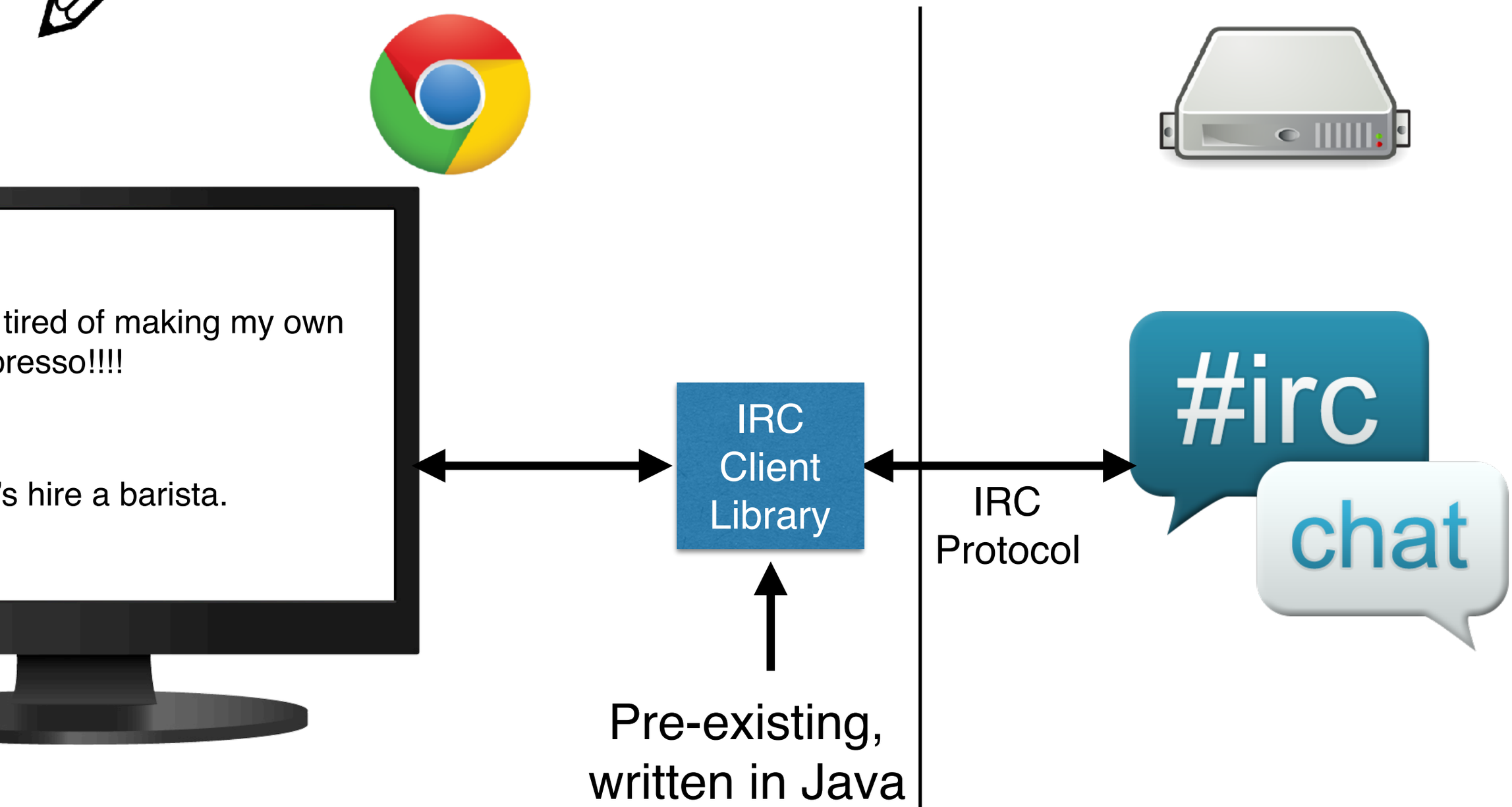
↓

We have too many customers & cannot scale!!!
sl

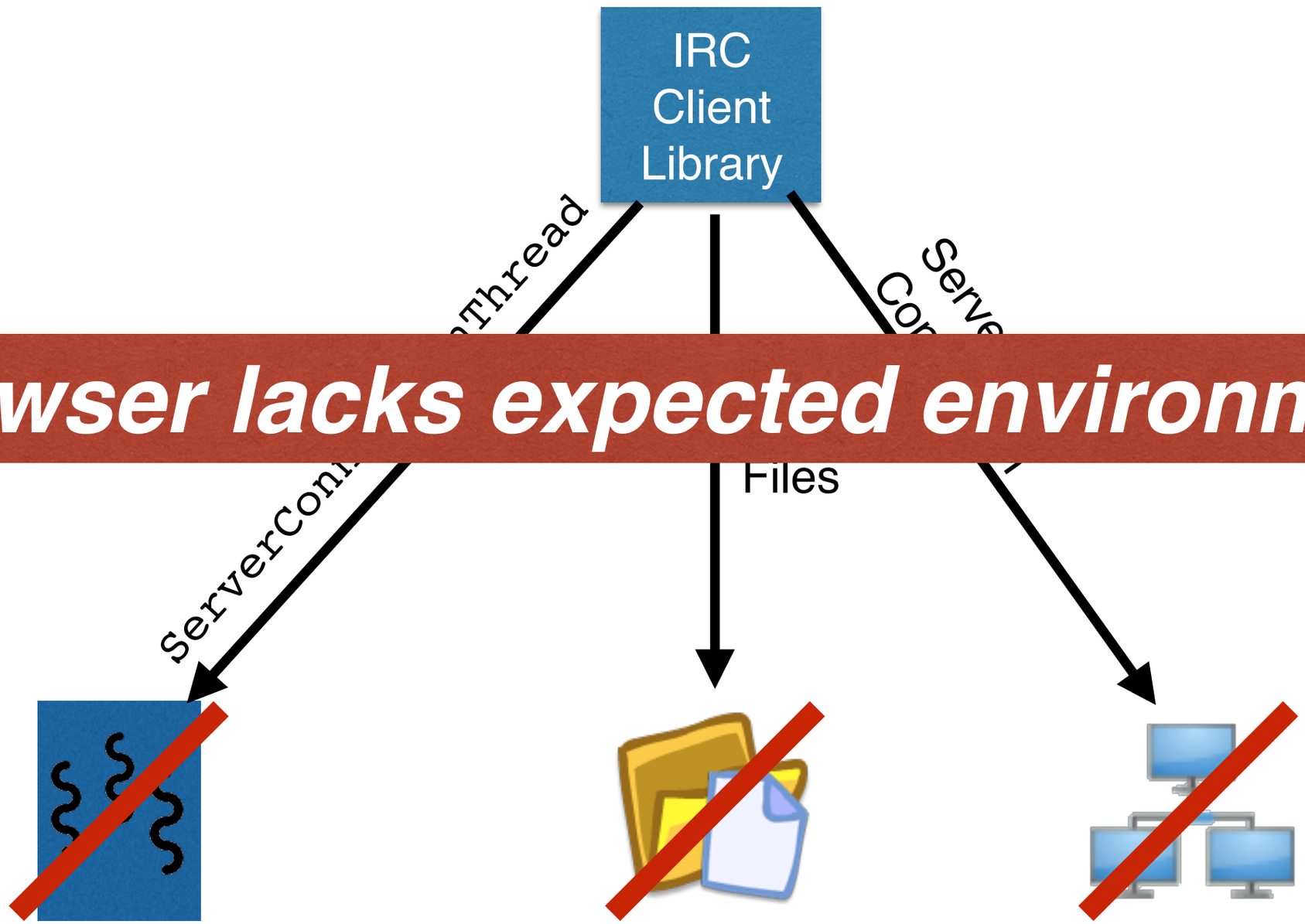
We have too many customers & cannot scale!!!


We have too many customers & cannot scale!!!
sl
#irc
chat

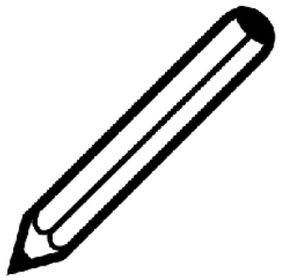
Desired Initial Architecture



Compile Java to JavaScript?



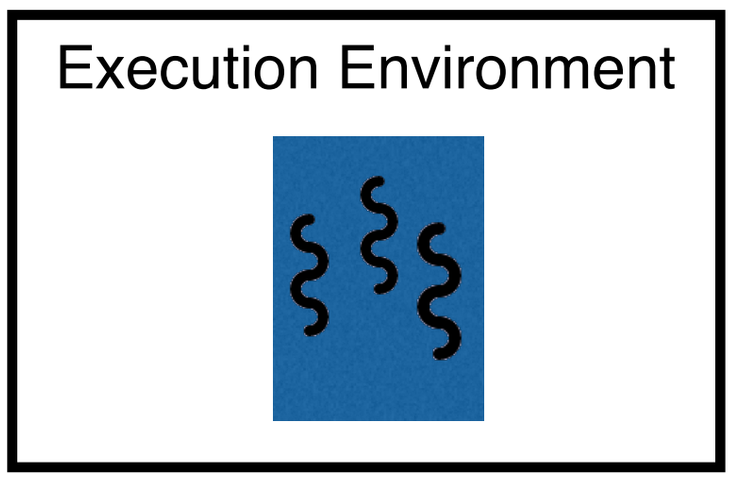
Browser lacks expected environment!



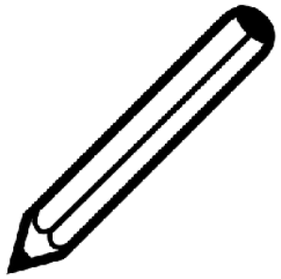
Doppio: Breaking the Browser Language Barrier

PLDI 2014, Distinguished Artifact Award,
SIGPLAN Research Highlight

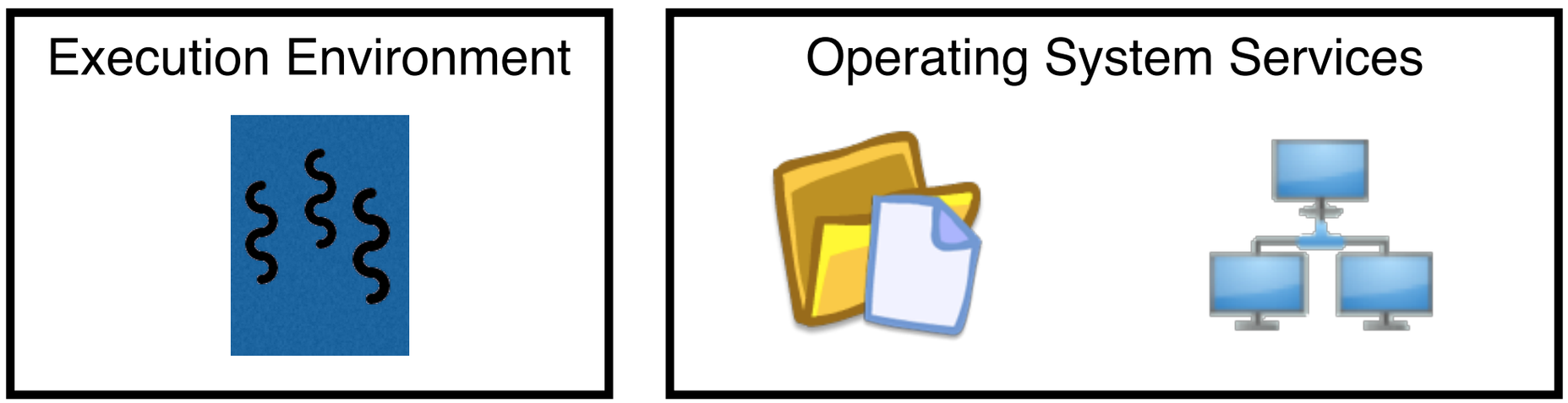
Doppio: Breaking the Browser Language Barrier



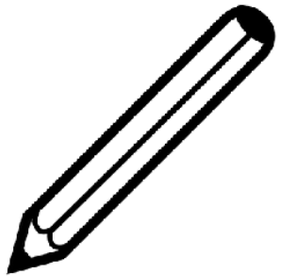
PLDI 2014, Distinguished Artifact Award,
SIGPLAN Research Highlight



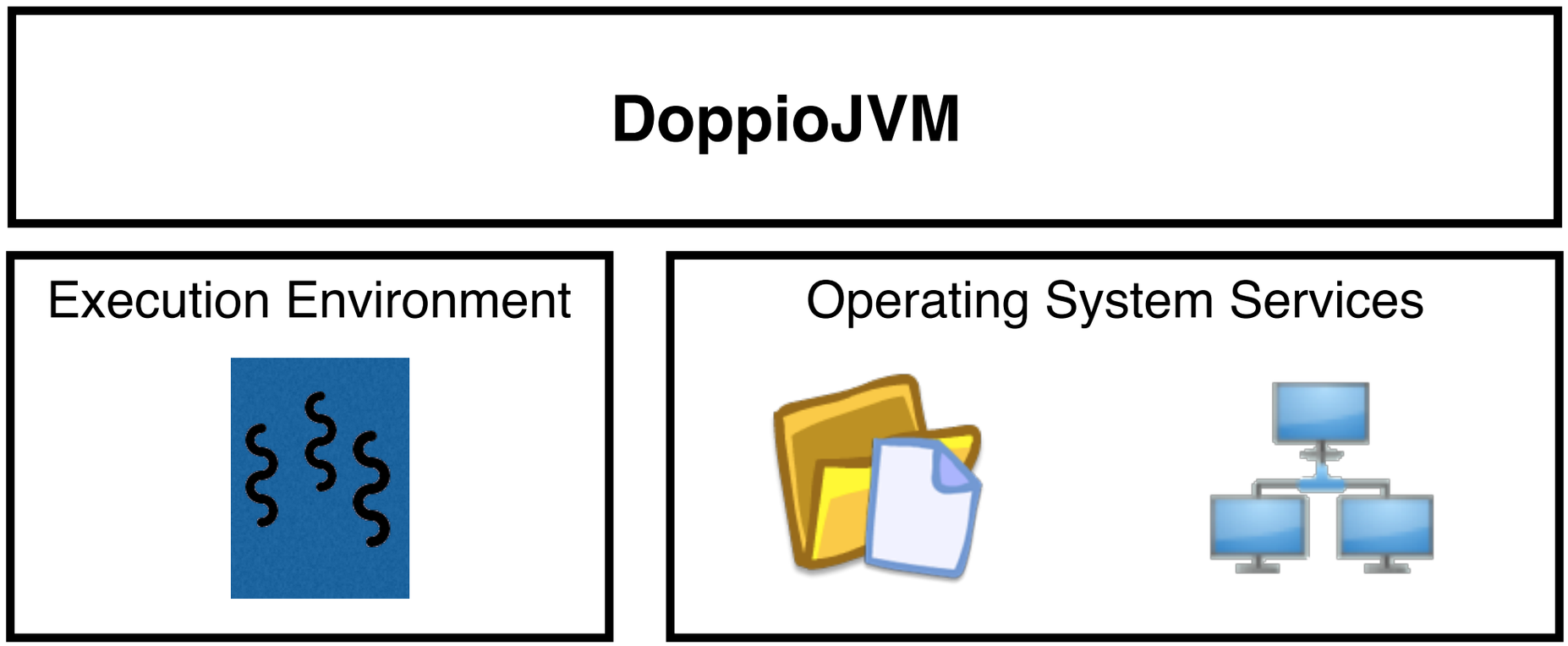
Doppio: Breaking the Browser Language Barrier



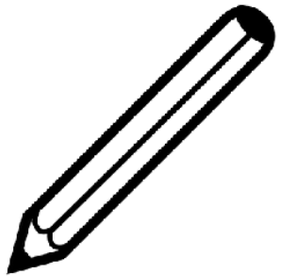
PLDI 2014, Distinguished Artifact Award,
SIGPLAN Research Highlight



Doppio: Breaking the Browser Language Barrier



PLDI 2014, Distinguished Artifact Award,
SIGPLAN Research Highlight

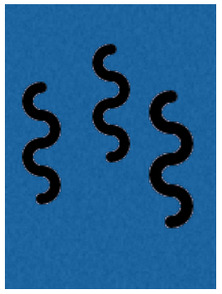


Doppio: Breaking the Browser Language Barrier

DoppioJVM

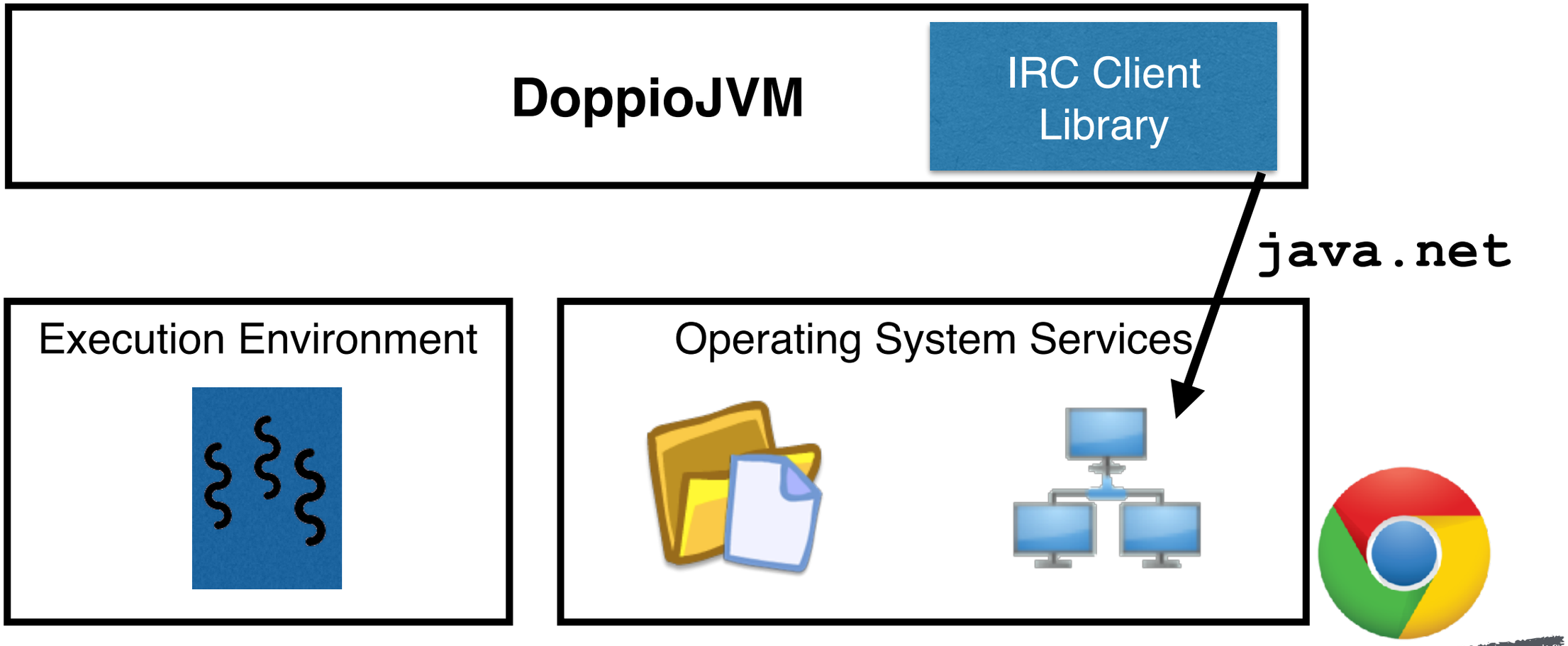
IRC Client Library

Execution Environment

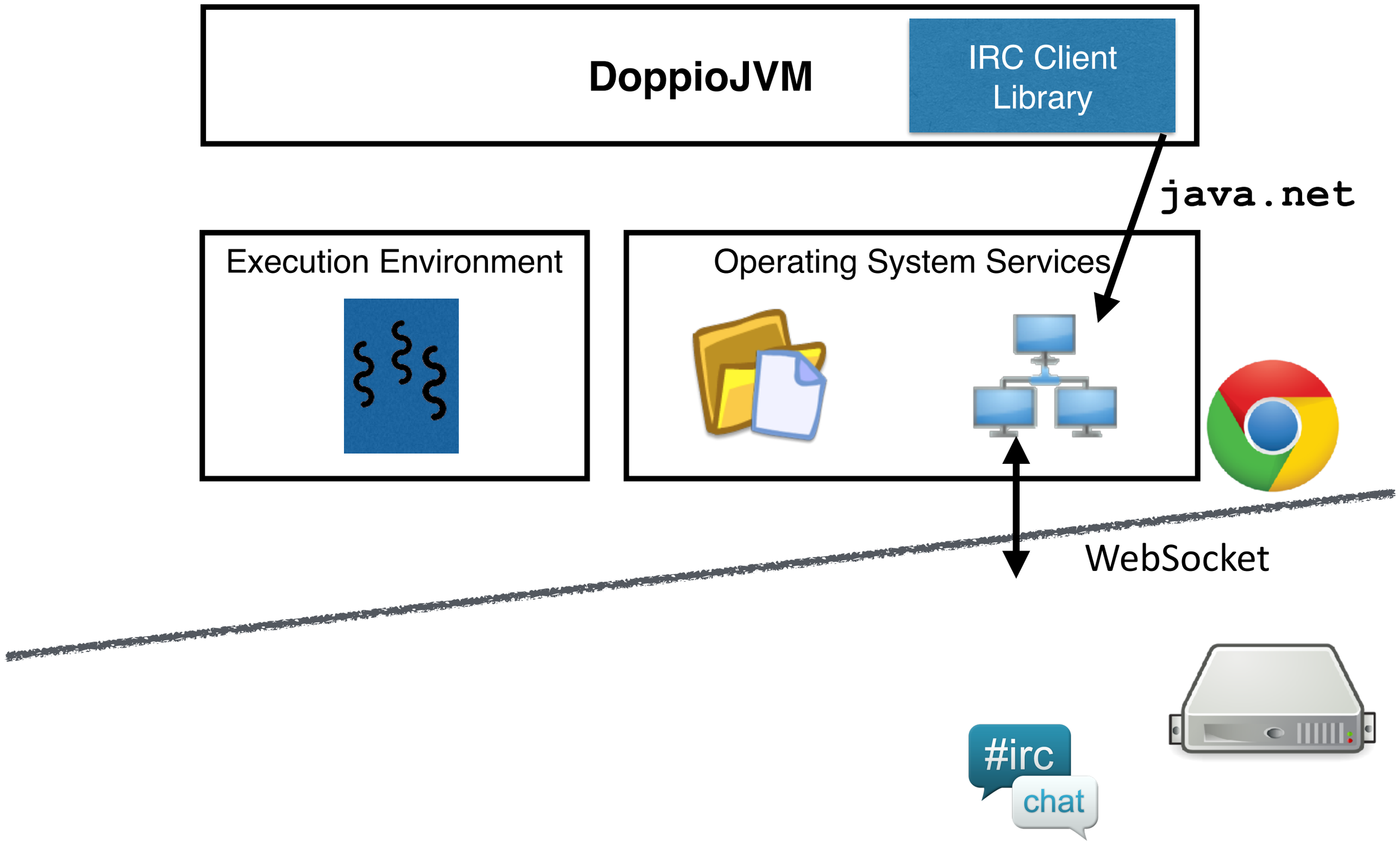


Operating System Services

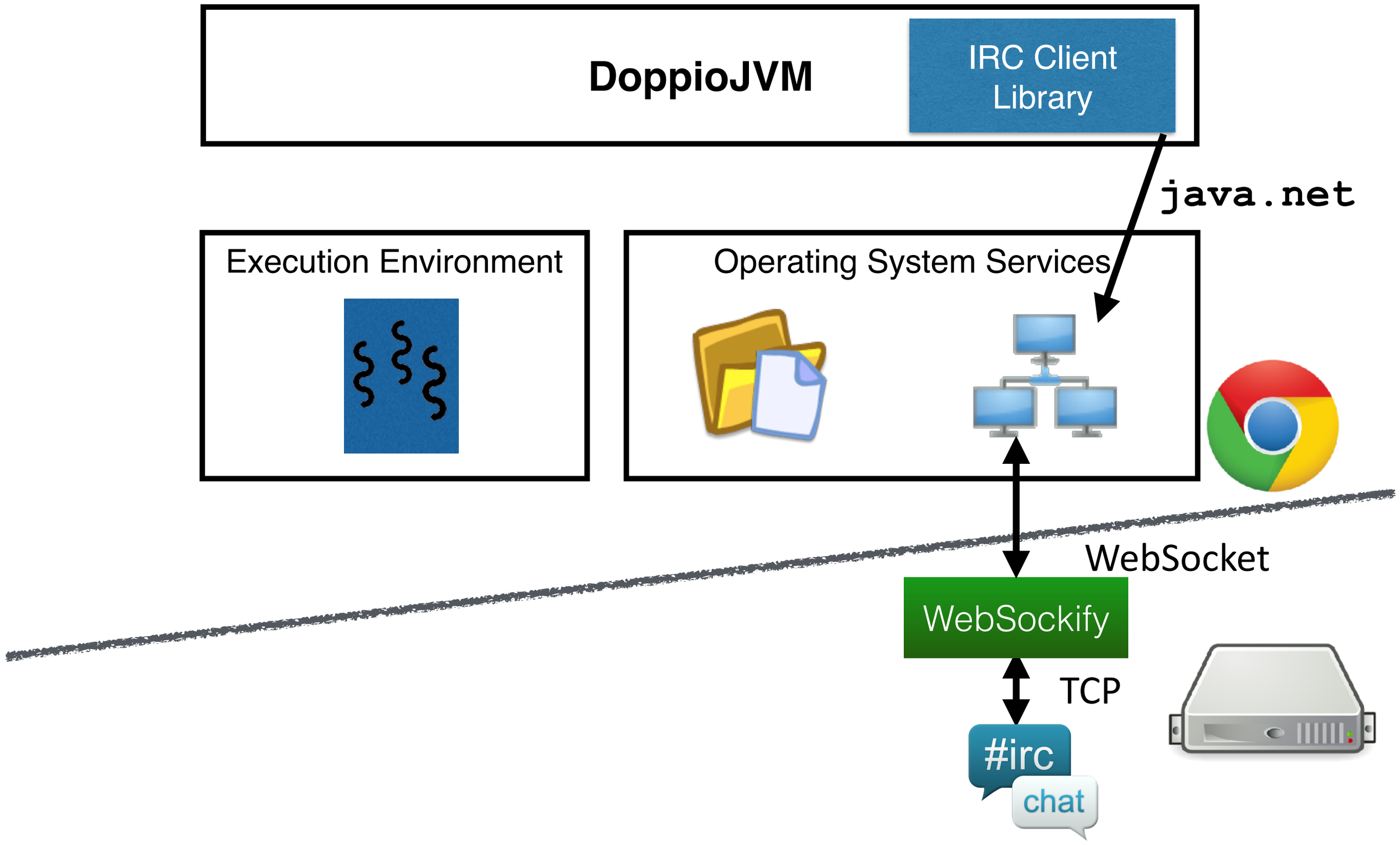
Doppio: Breaking the Browser Language Barrier



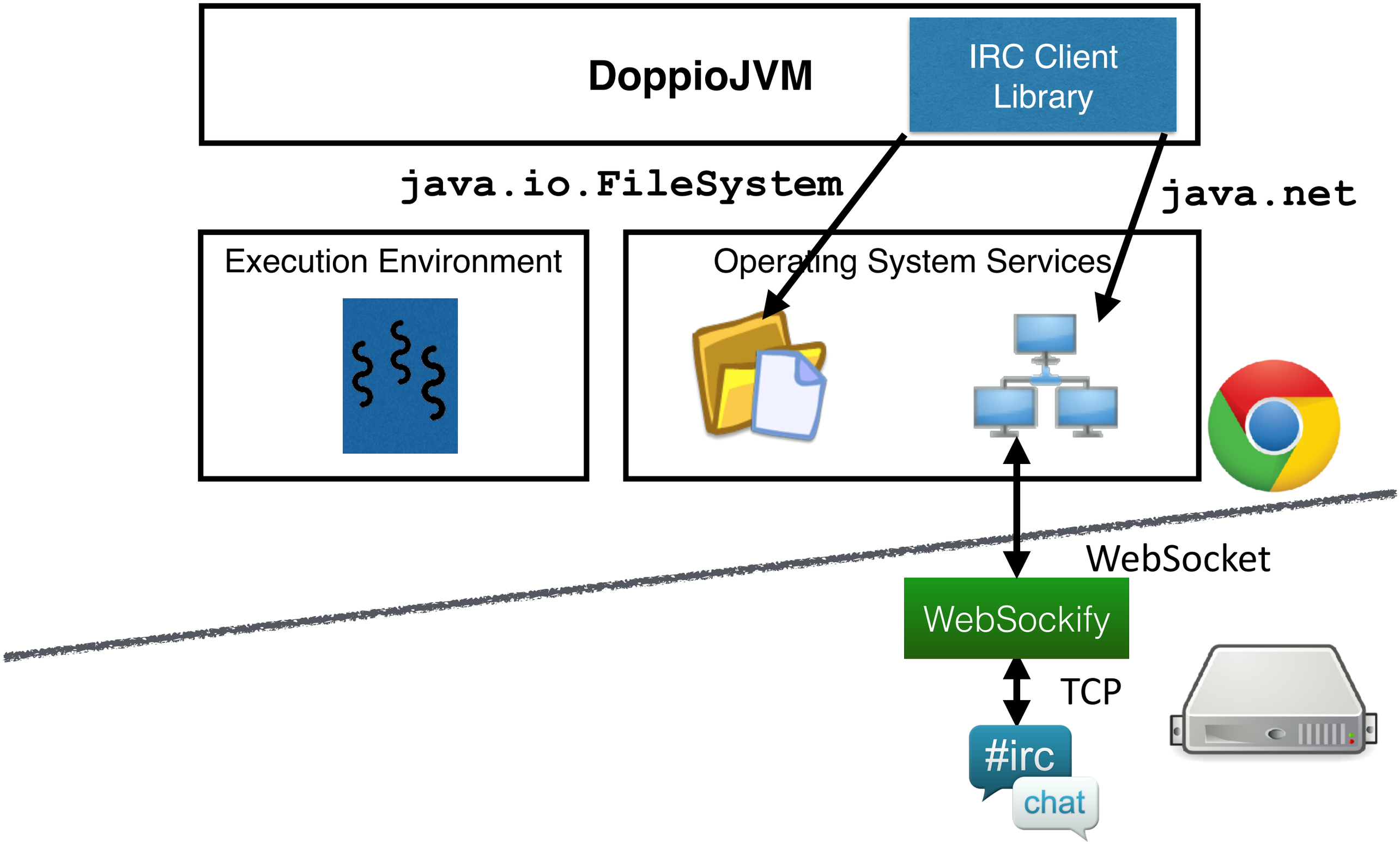
Doppio: Breaking the Browser Language Barrier



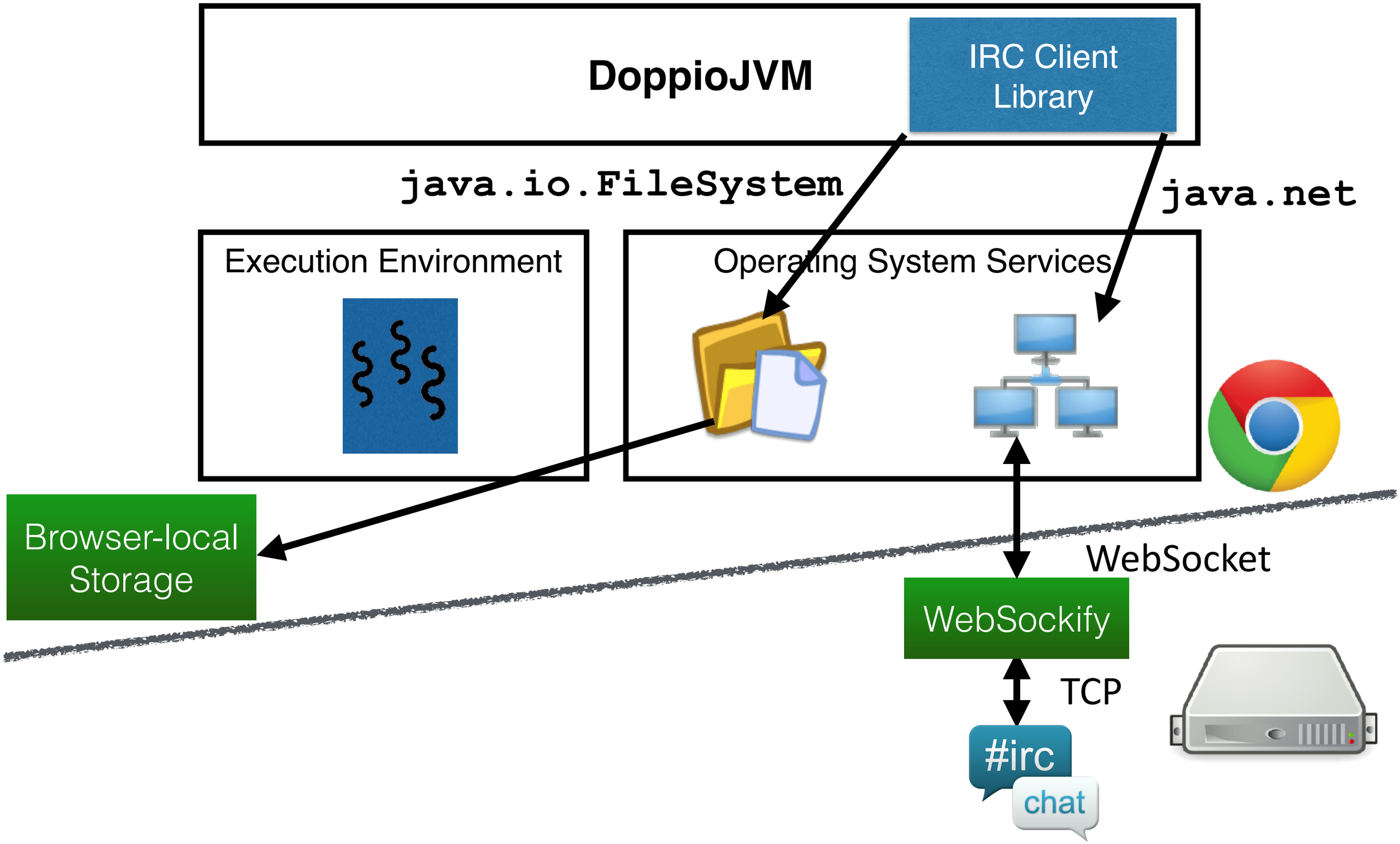
Doppio: Breaking the Browser Language Barrier



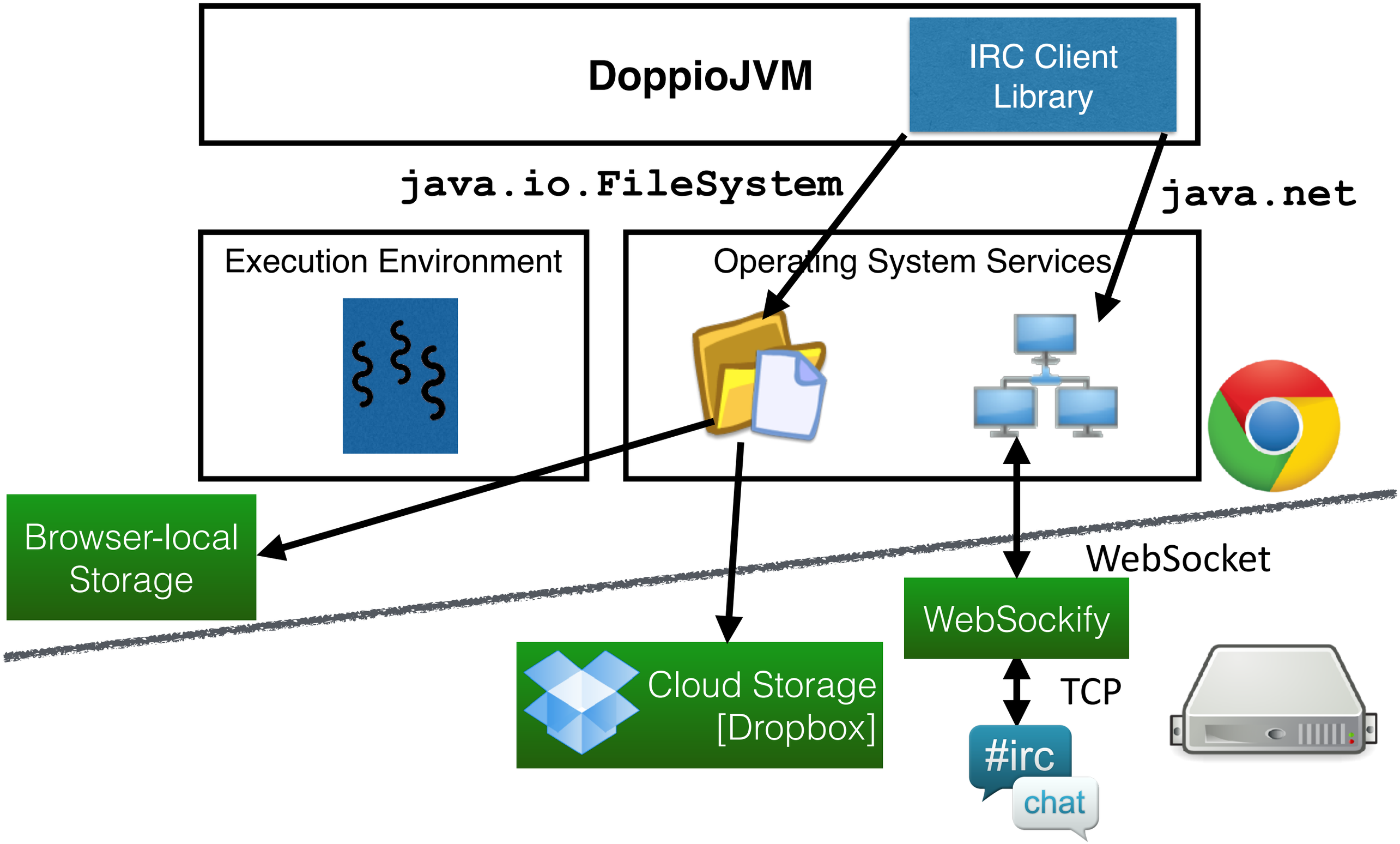
Doppio: Breaking the Browser Language Barrier



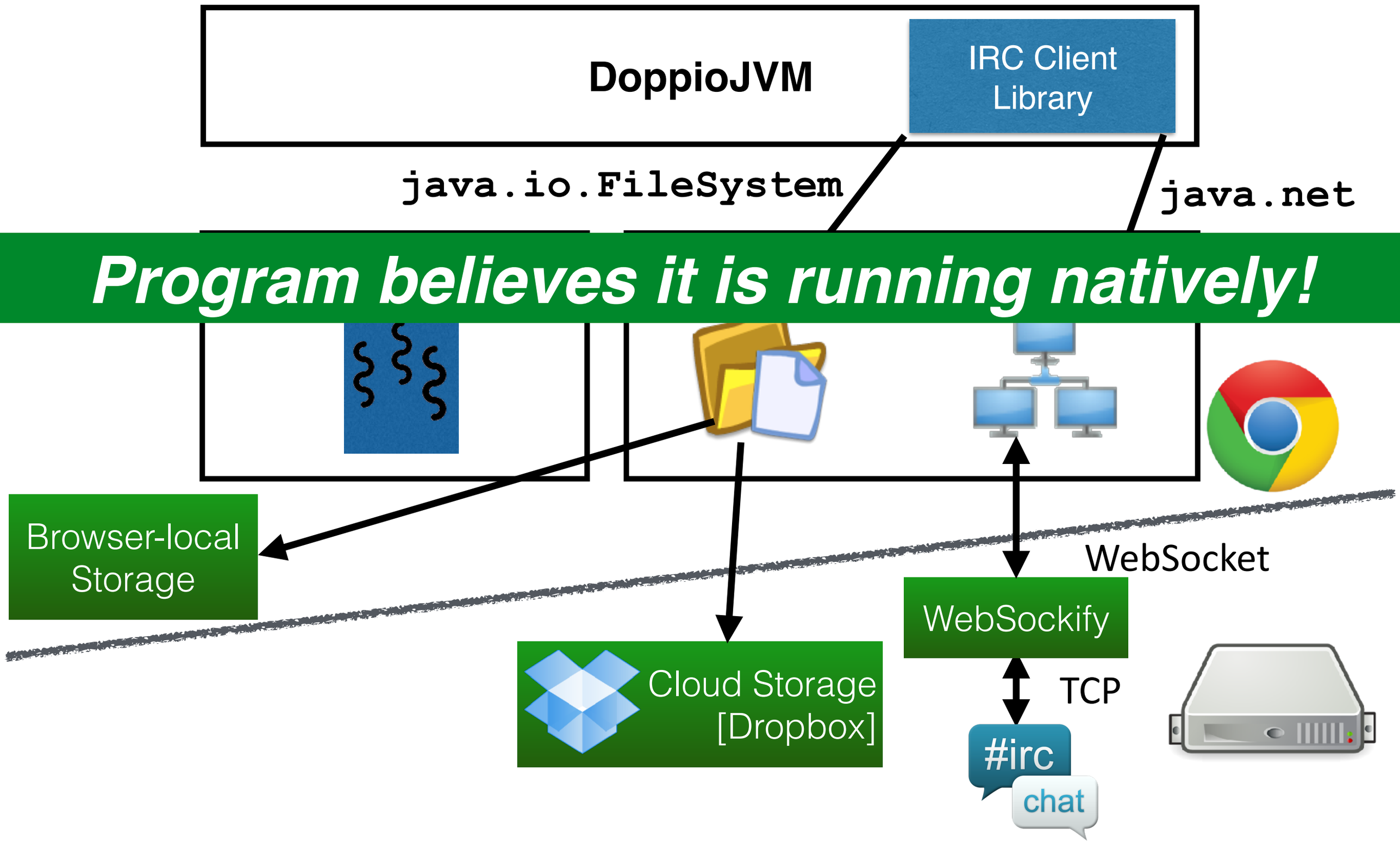
Doppio: Breaking the Browser Language Barrier



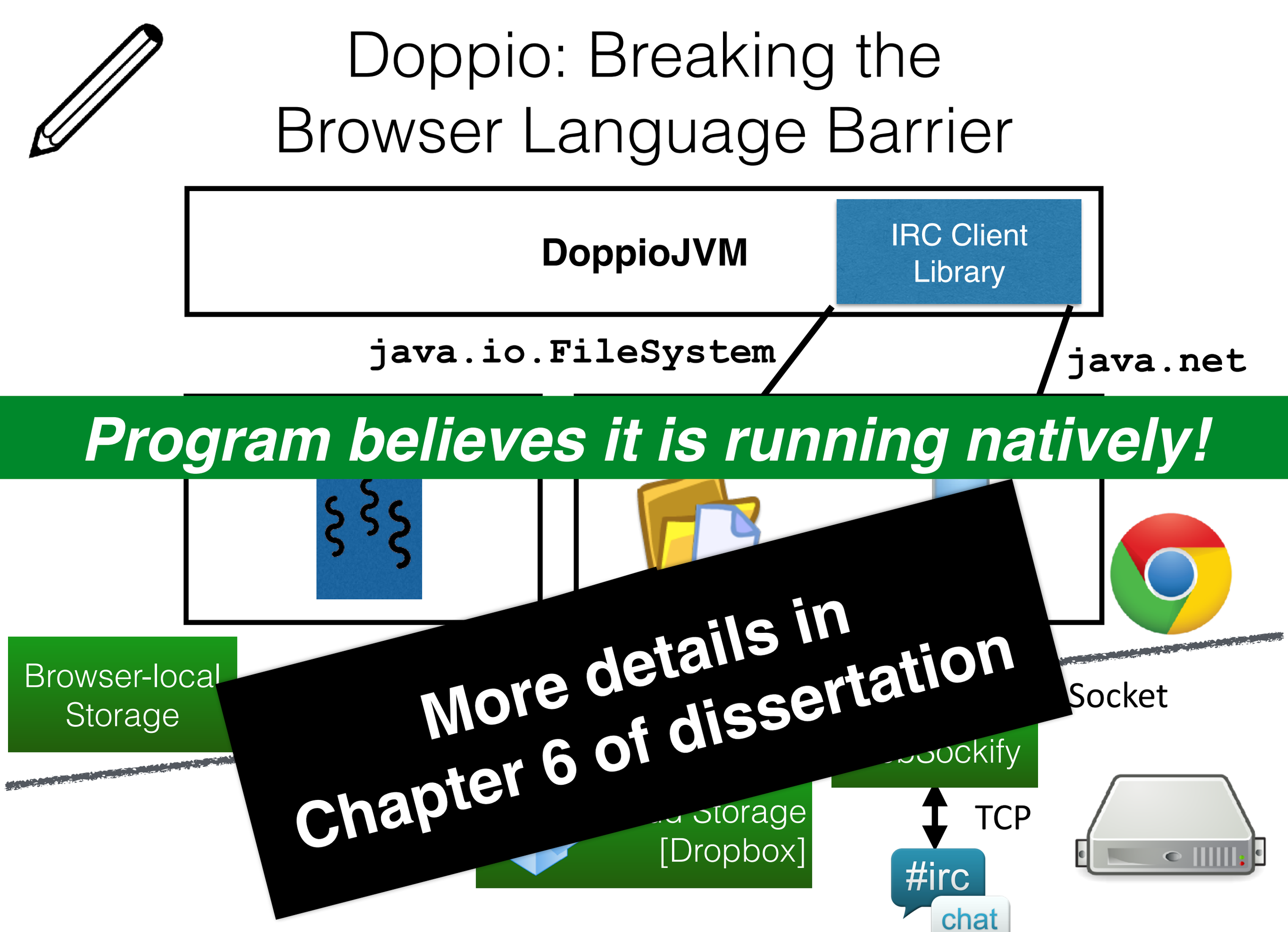
Doppio: Breaking the Browser Language Barrier



Doppio: Breaking the Browser Language Barrier

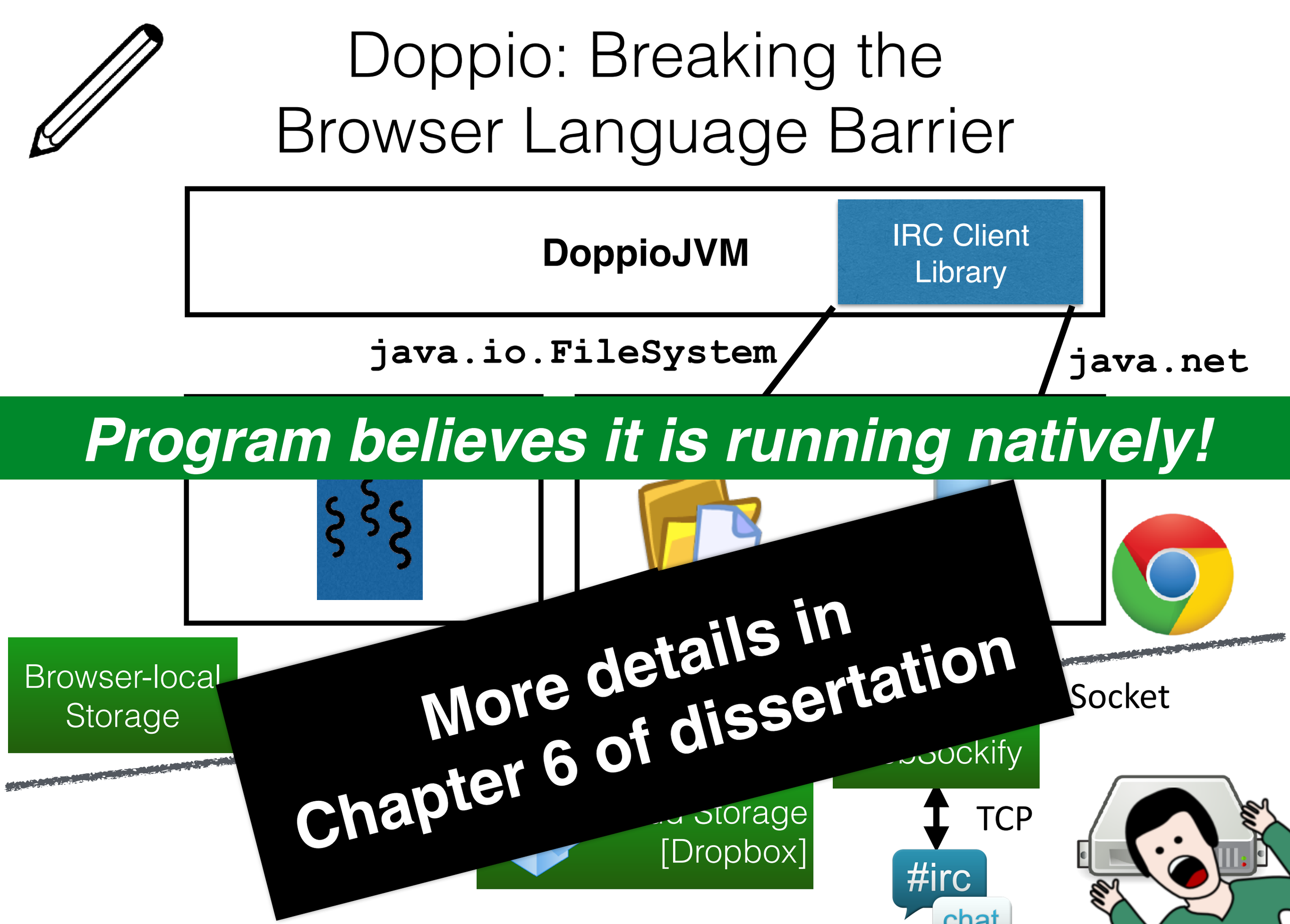


Doppio: Breaking the Browser Language Barrier



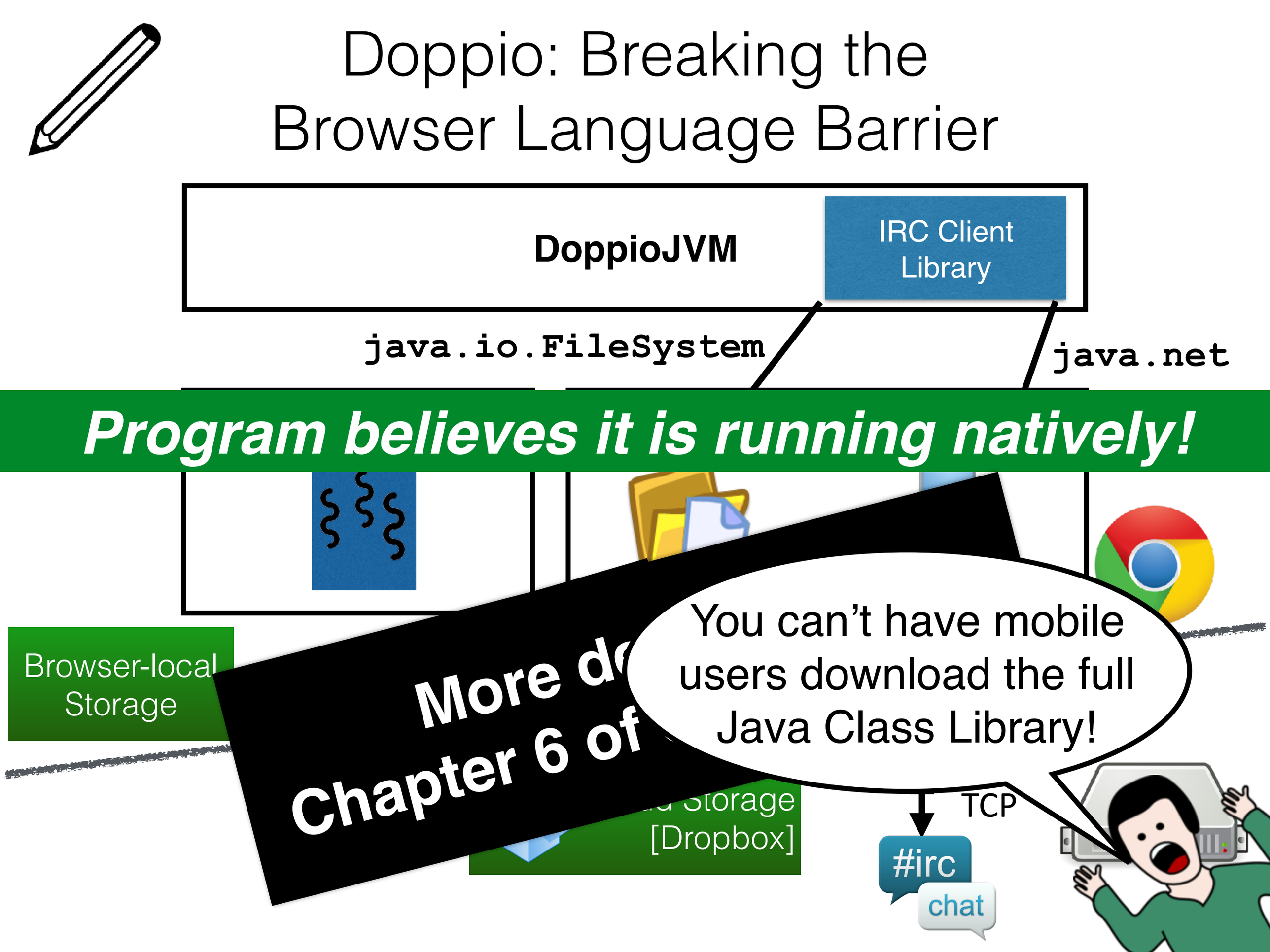
More details in Chapter 6 of dissertation

Doppio: Breaking the Browser Language Barrier

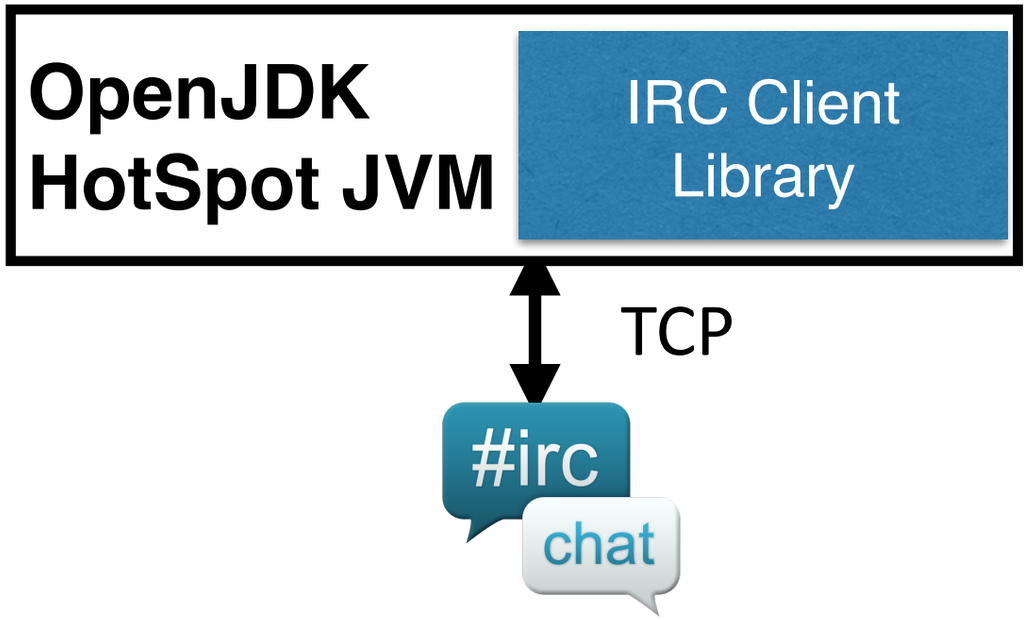


More details in Chapter 6 of dissertation

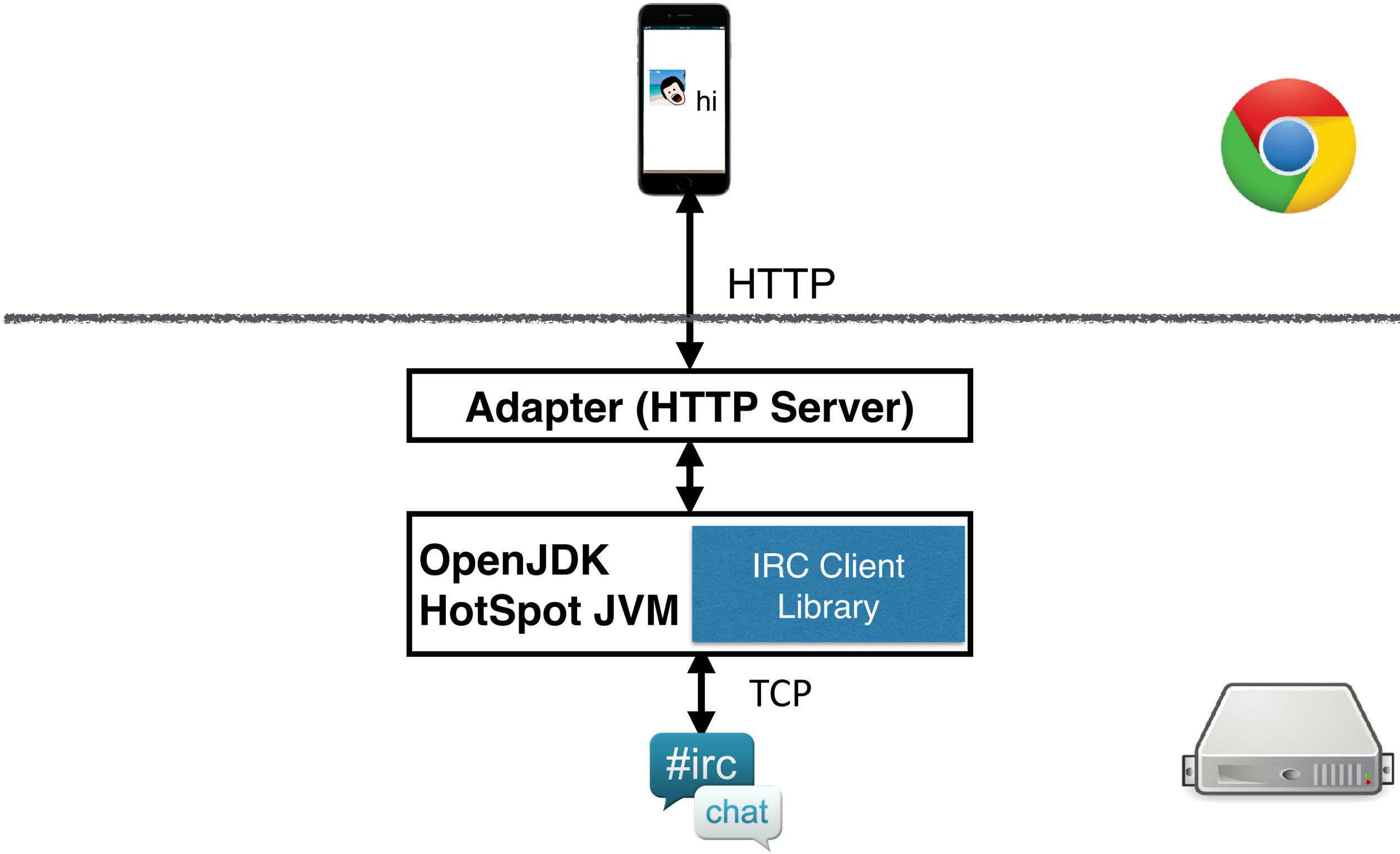
Doppio: Breaking the Browser Language Barrier



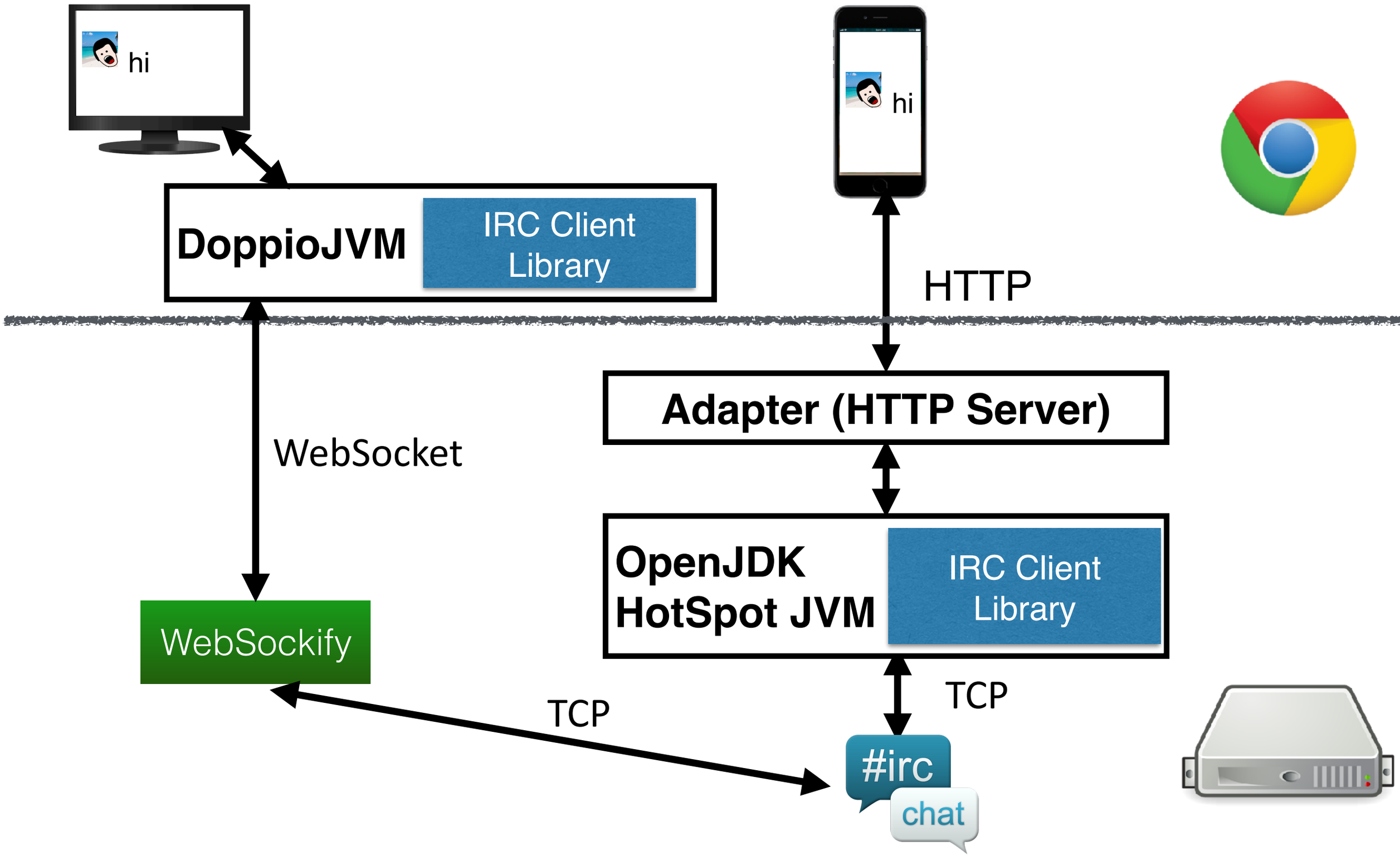
Offload IRC client library to server?



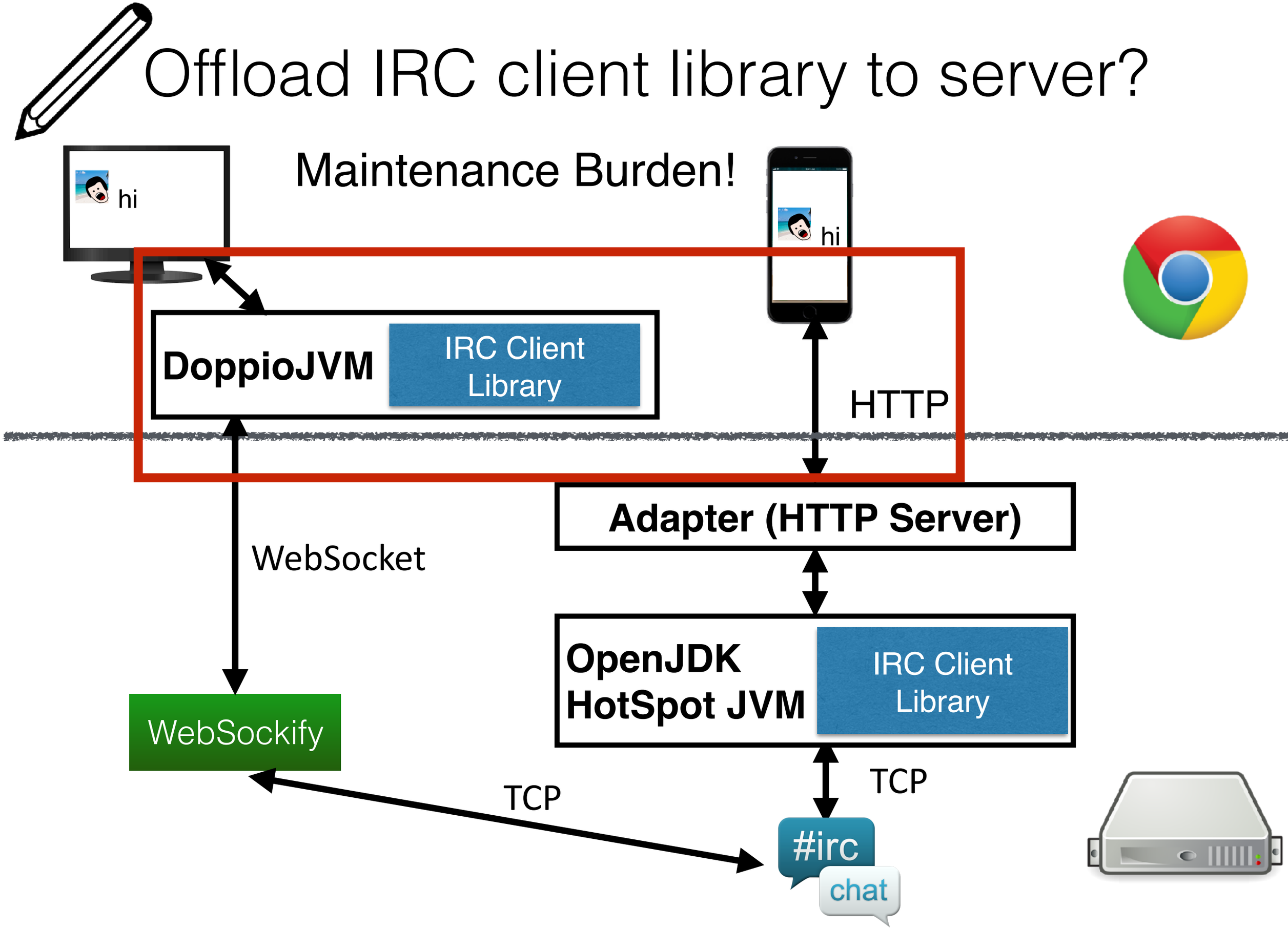
Offload IRC client library to server?



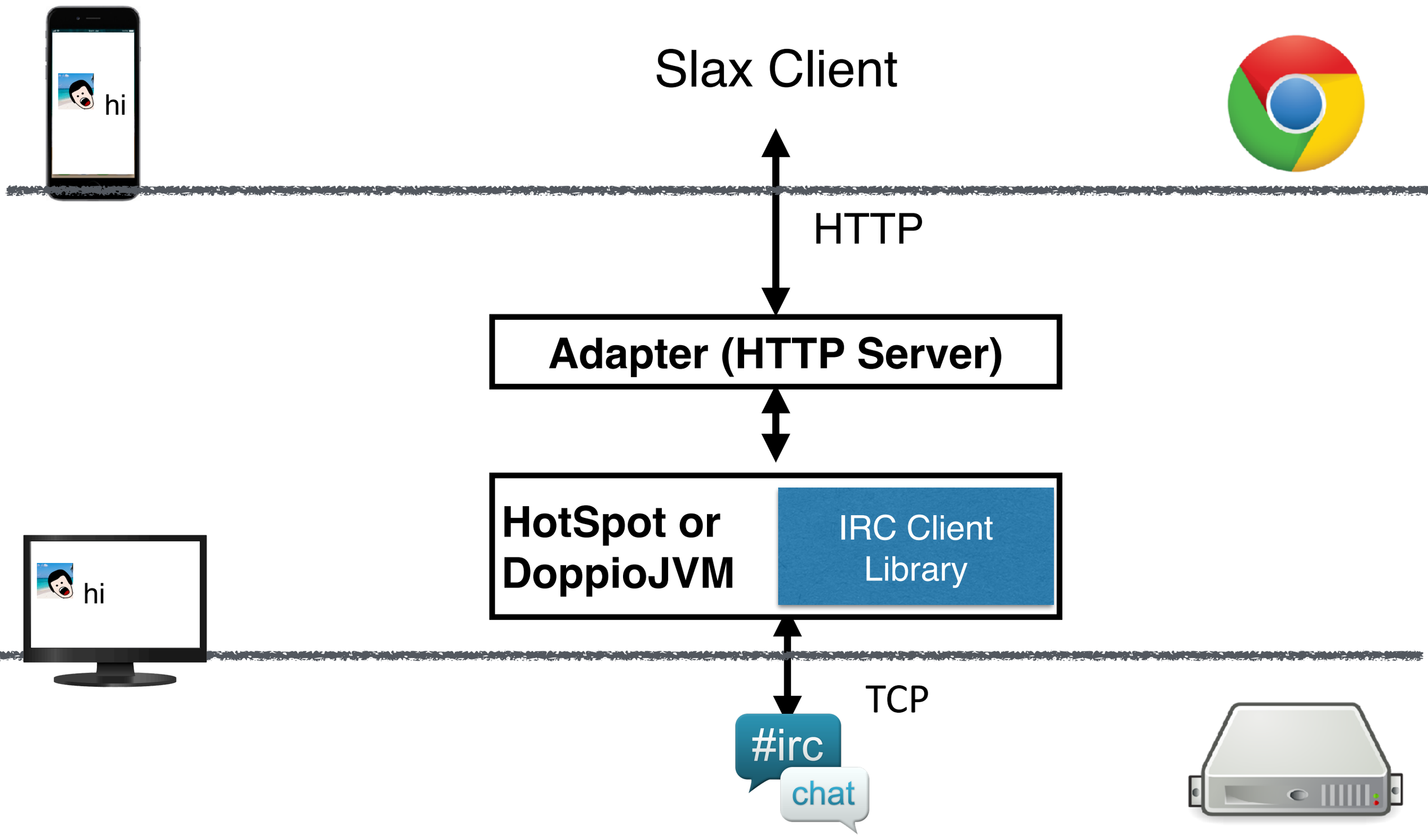
Offload IRC client library to server?



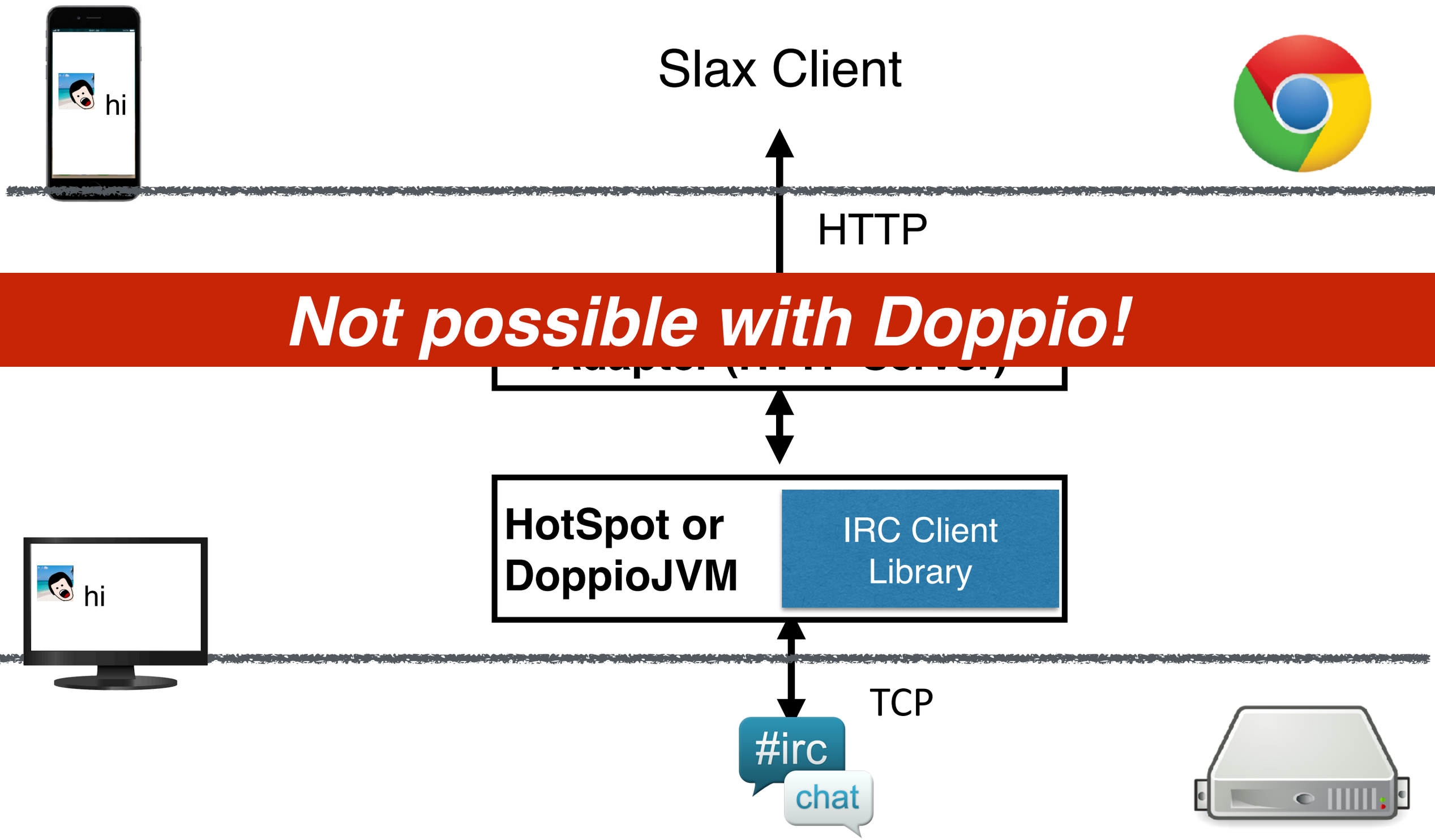
Offload IRC client library to server?



Run HTTP server adapter client-side?



Run HTTP server adapter client-side?



Not possible with Doppio!

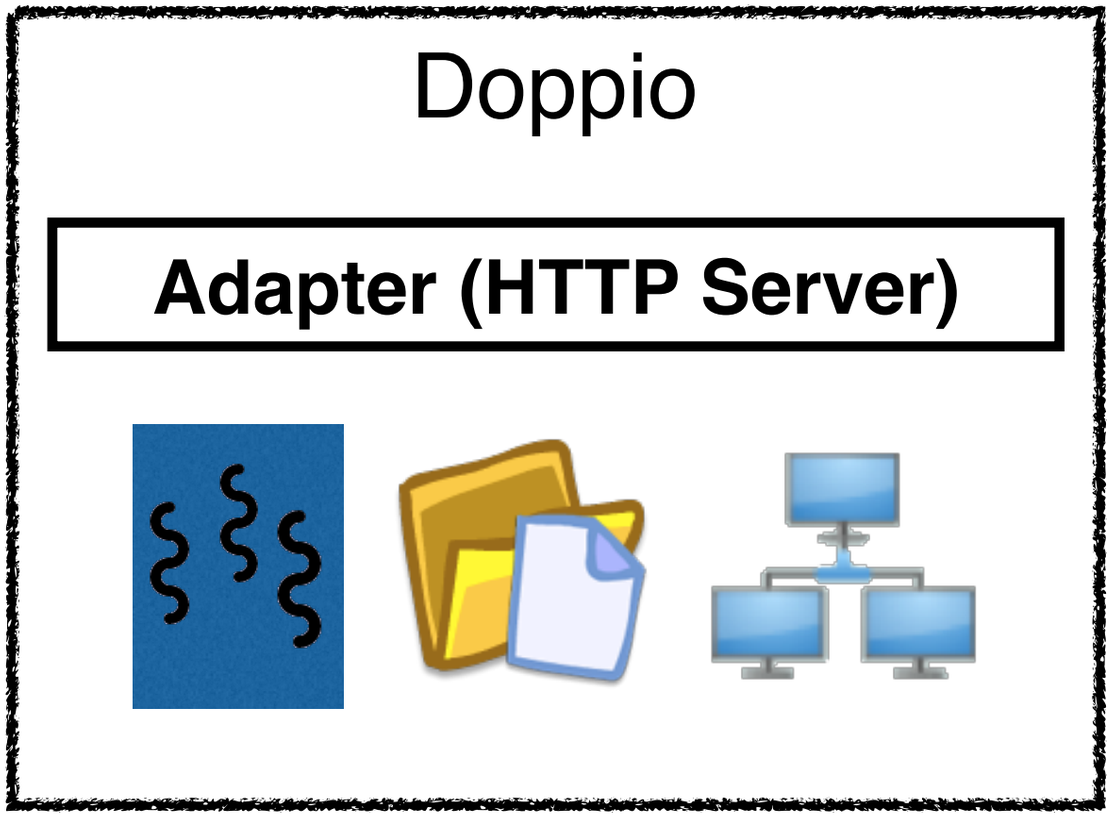
Doppio Provides Single Program Operating System Services

Adapter (HTTP Server)

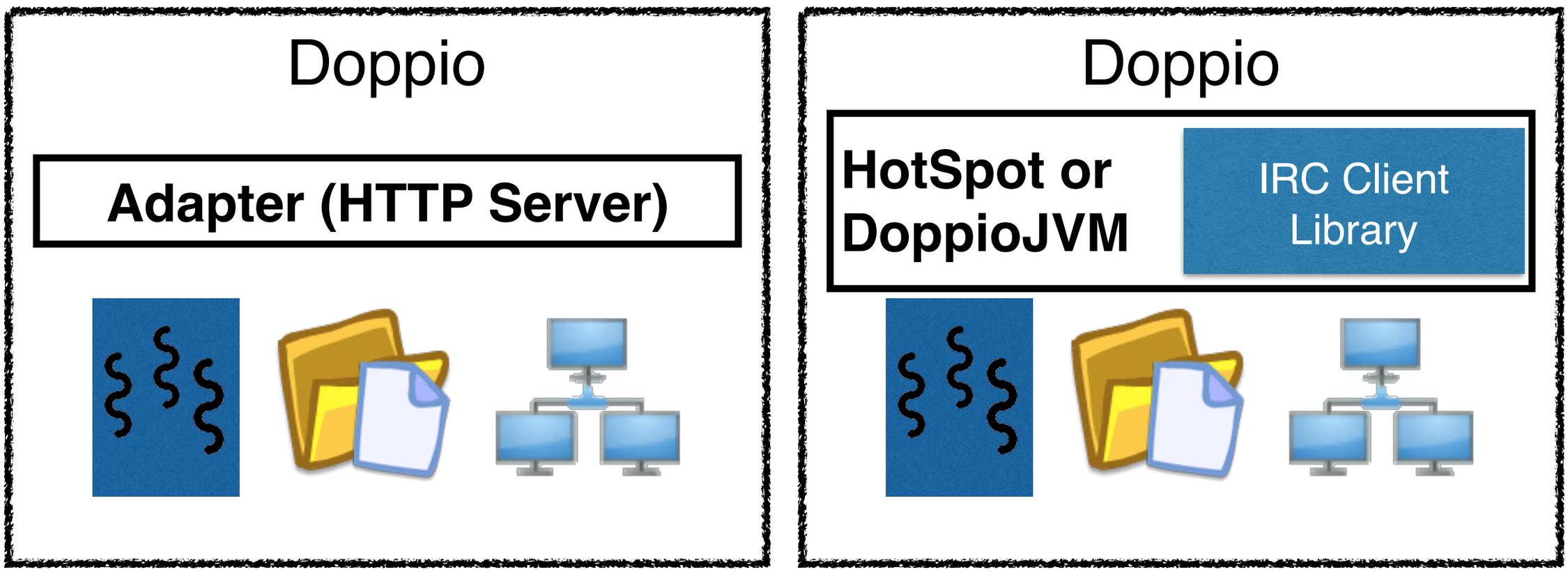
HotSpot or DoppioJVM

IRC Client Library

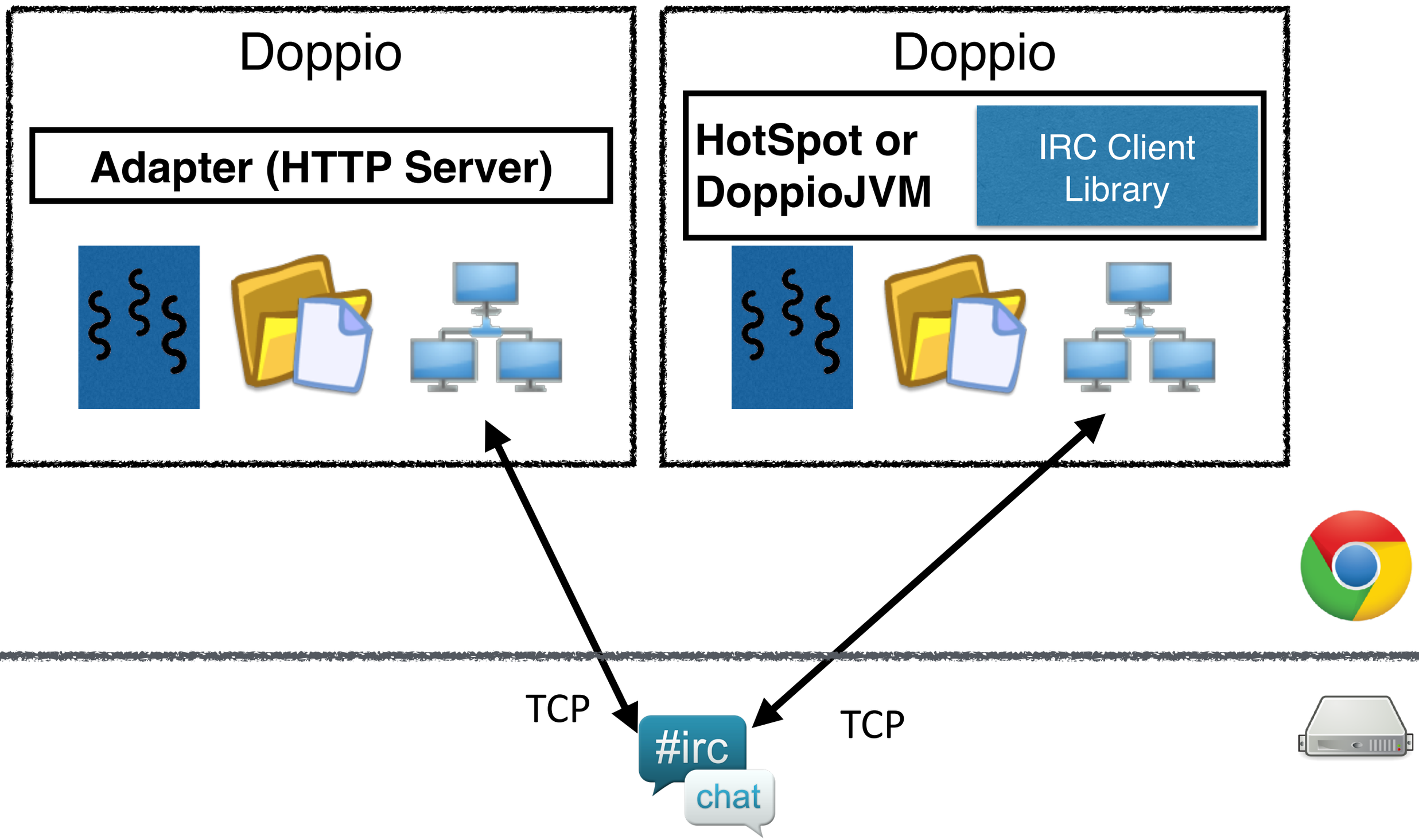
Doppio Provides Single Program Operating System Services



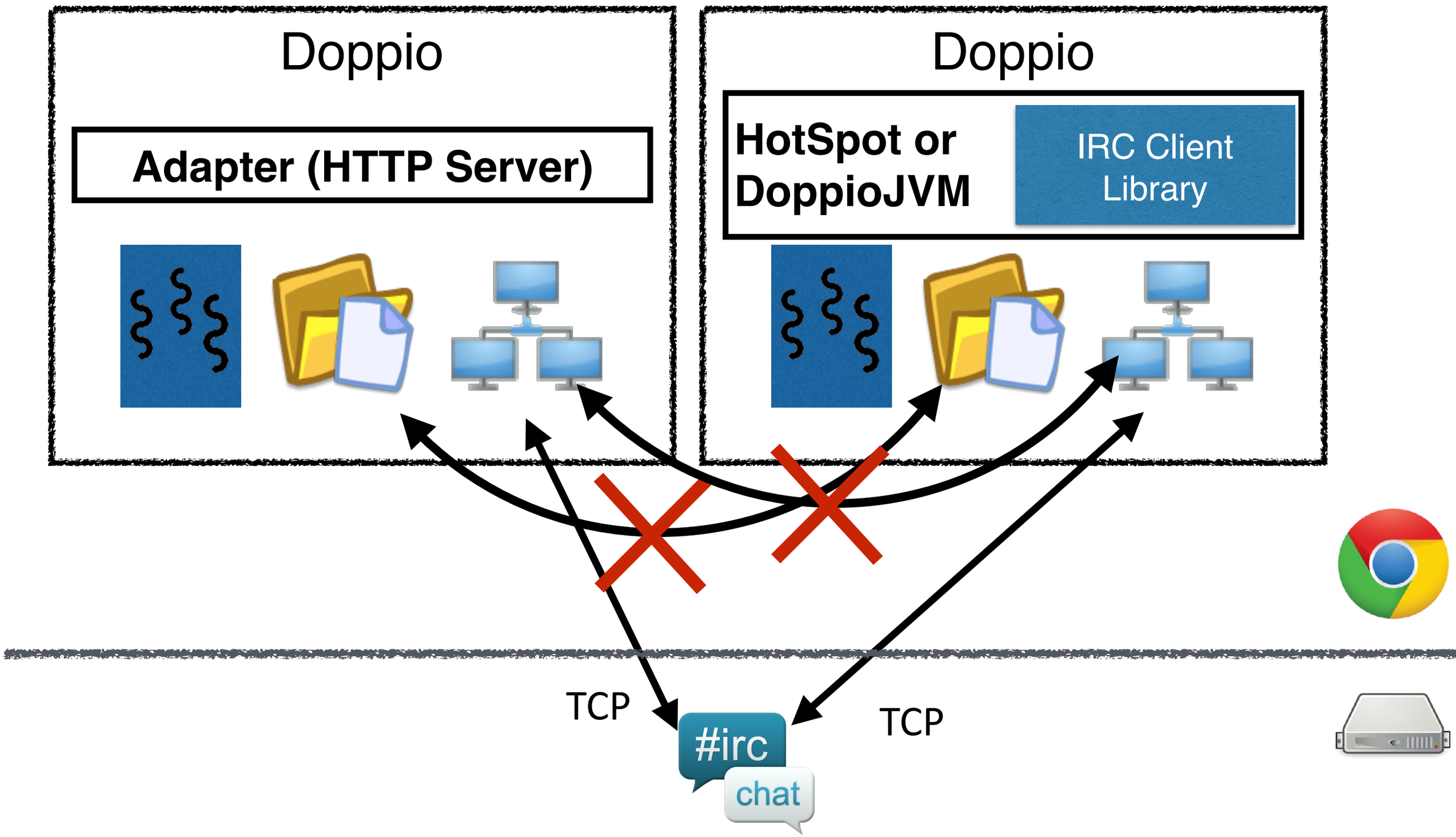
Doppio Provides Single Program Operating System Services



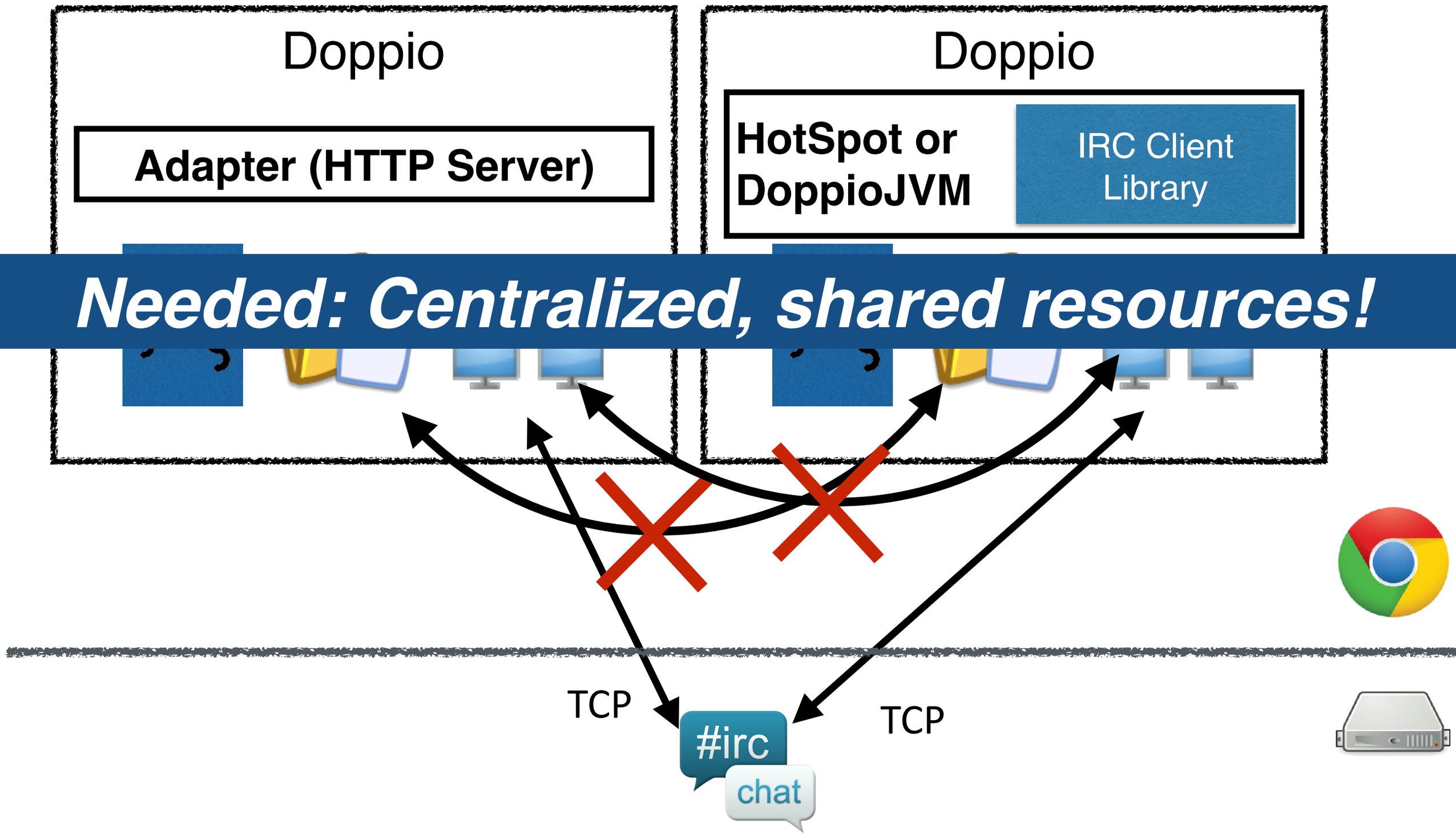
Doppio Provides Single Program Operating System Services



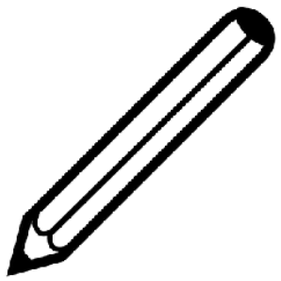
Doppio Provides Single Program Operating System Services



Doppio Provides Single Program Operating System Services



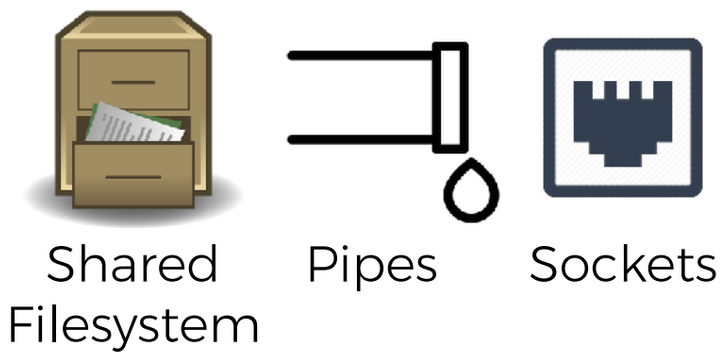
Needed: Centralized, shared resources!



Browsix: Bridging the Gap Between Unix and the Browser

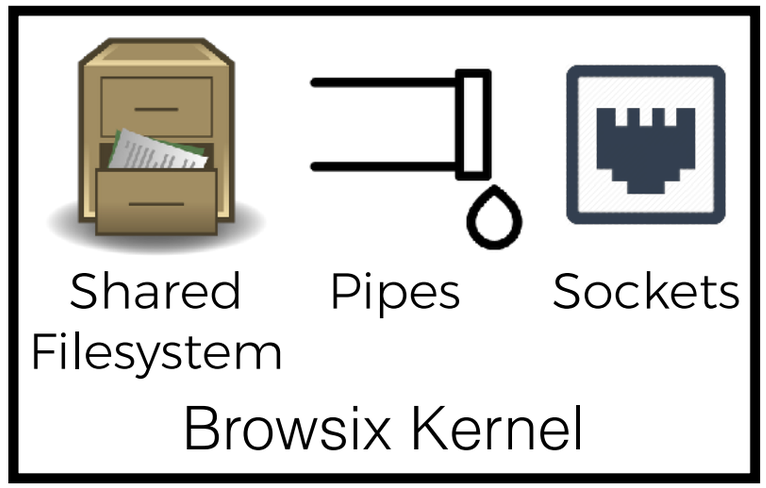
ASPLOS
2017

Browsix: Bridging the Gap Between Unix and the Browser



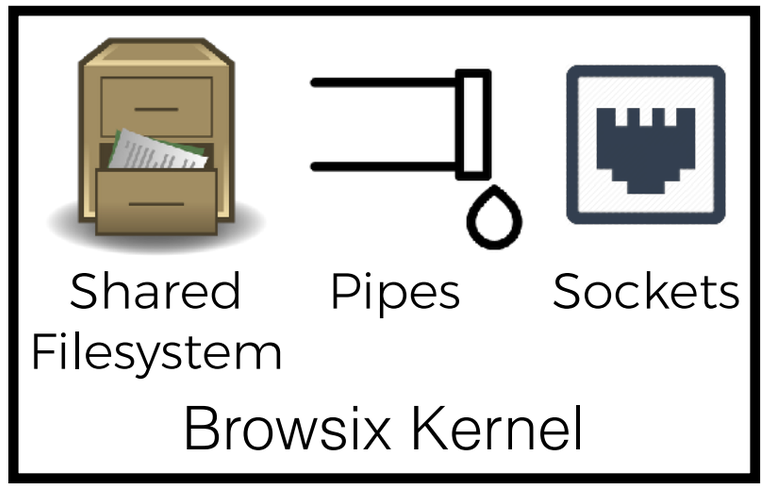
ASPLOS
2017

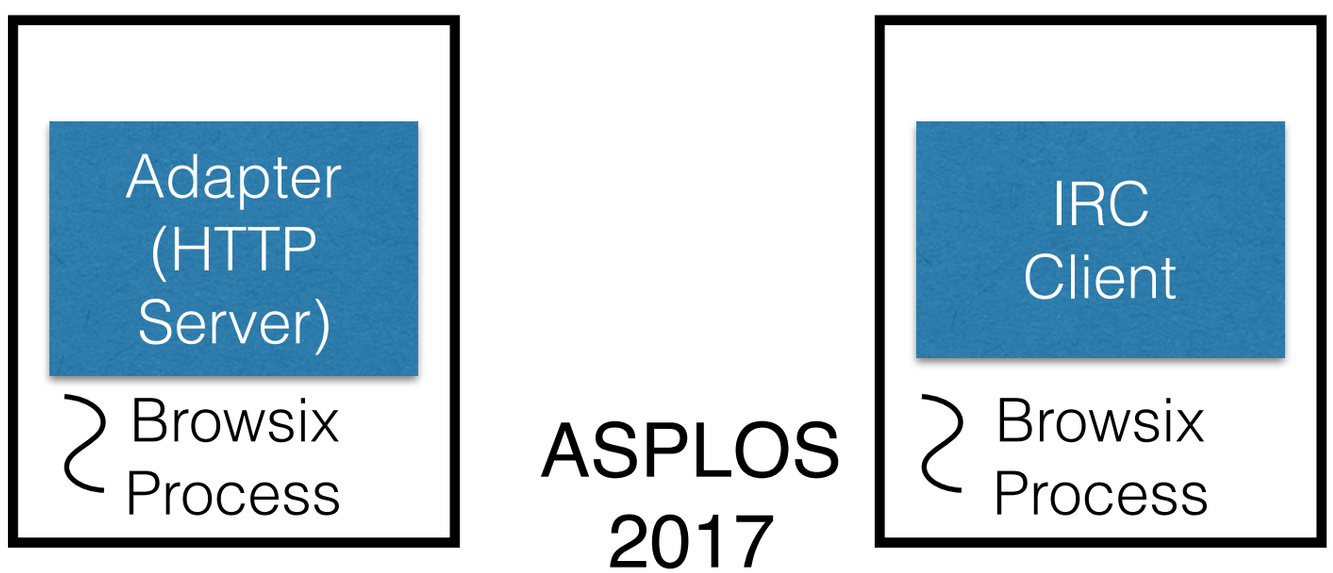
Browsix: Bridging the Gap Between Unix and the Browser



ASPLOS
2017

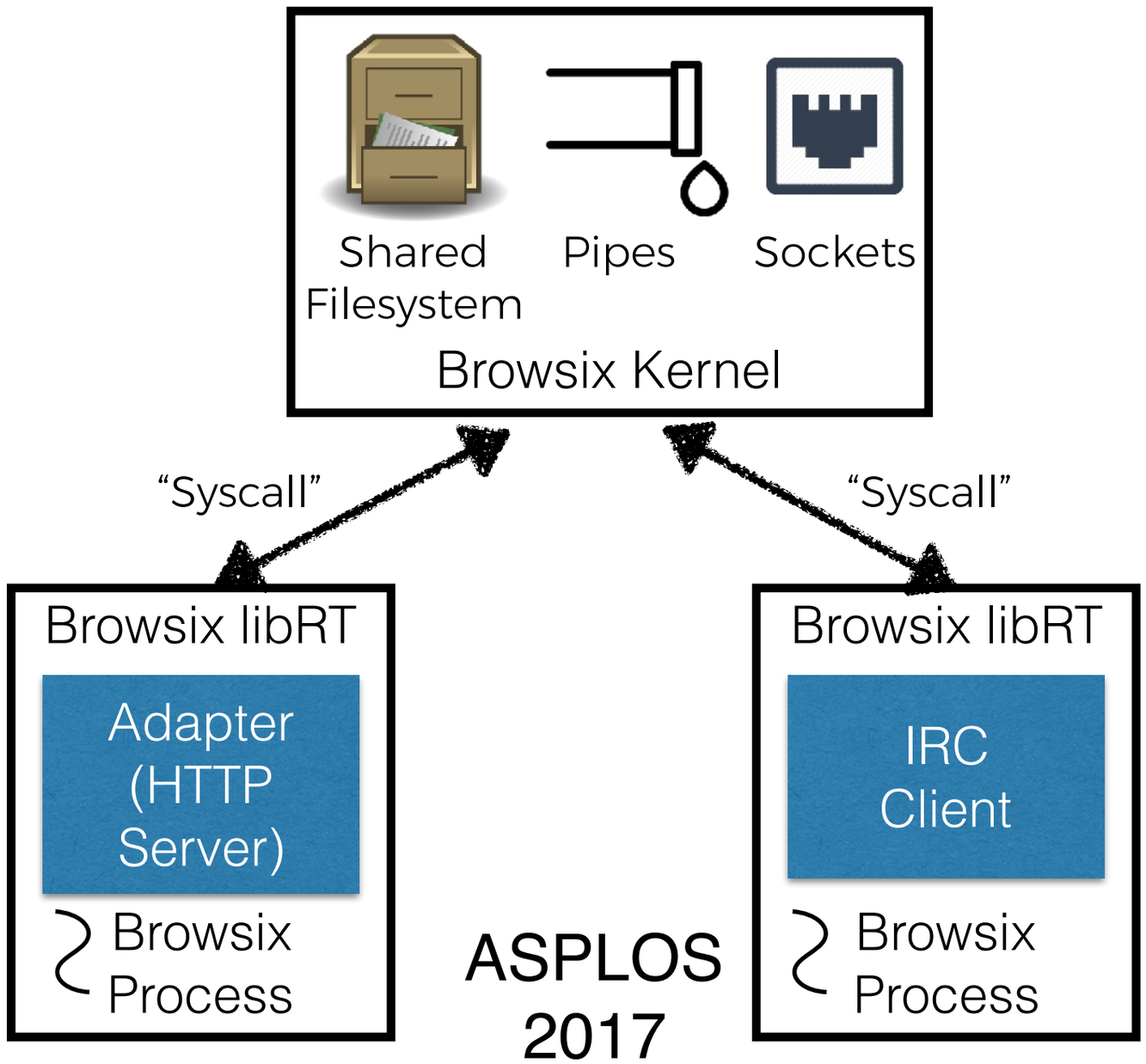
Browsix: Bridging the Gap Between Unix and the Browser



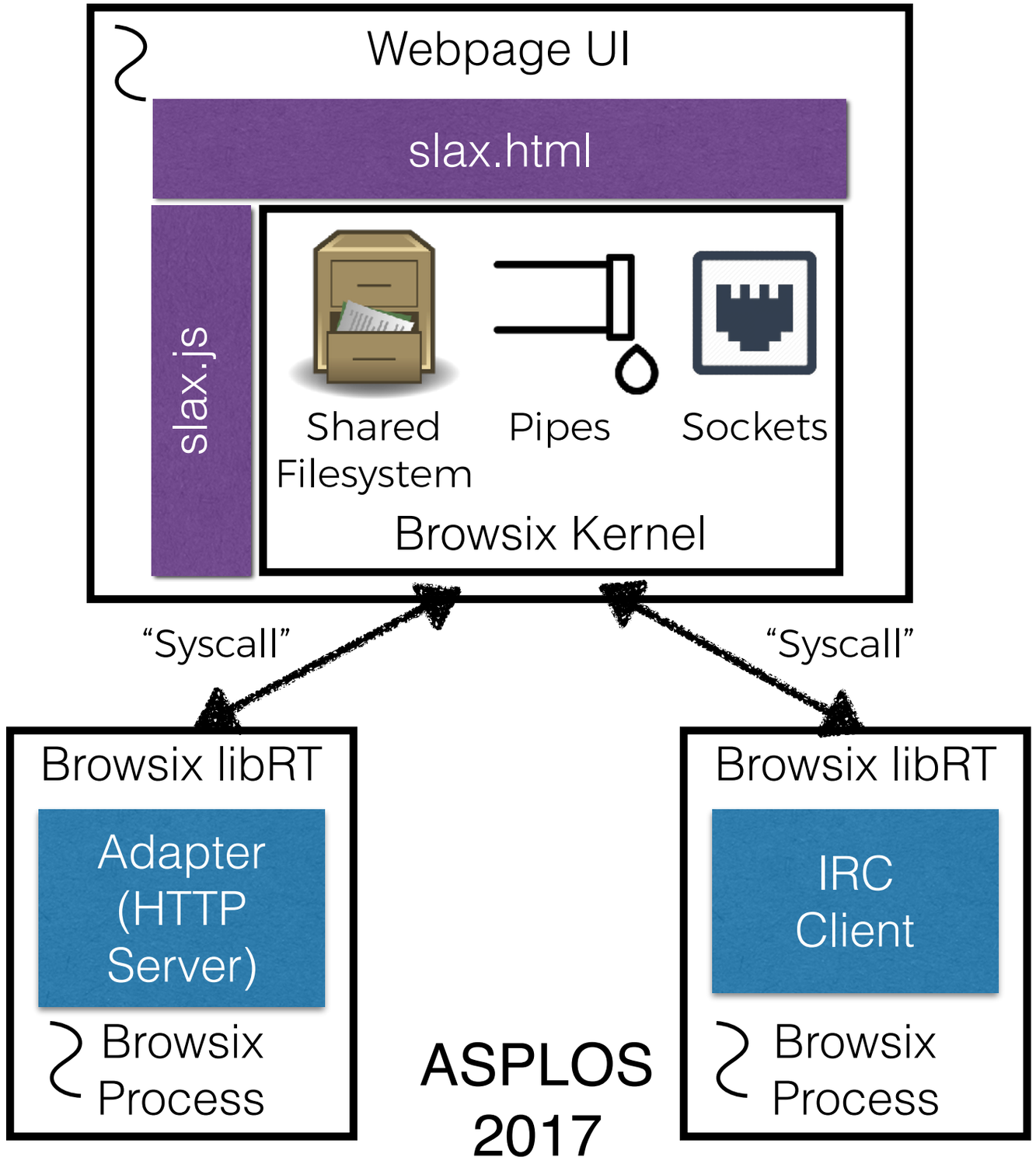


ASPLOS 2017

Browsix: Bridging the Gap Between Unix and the Browser

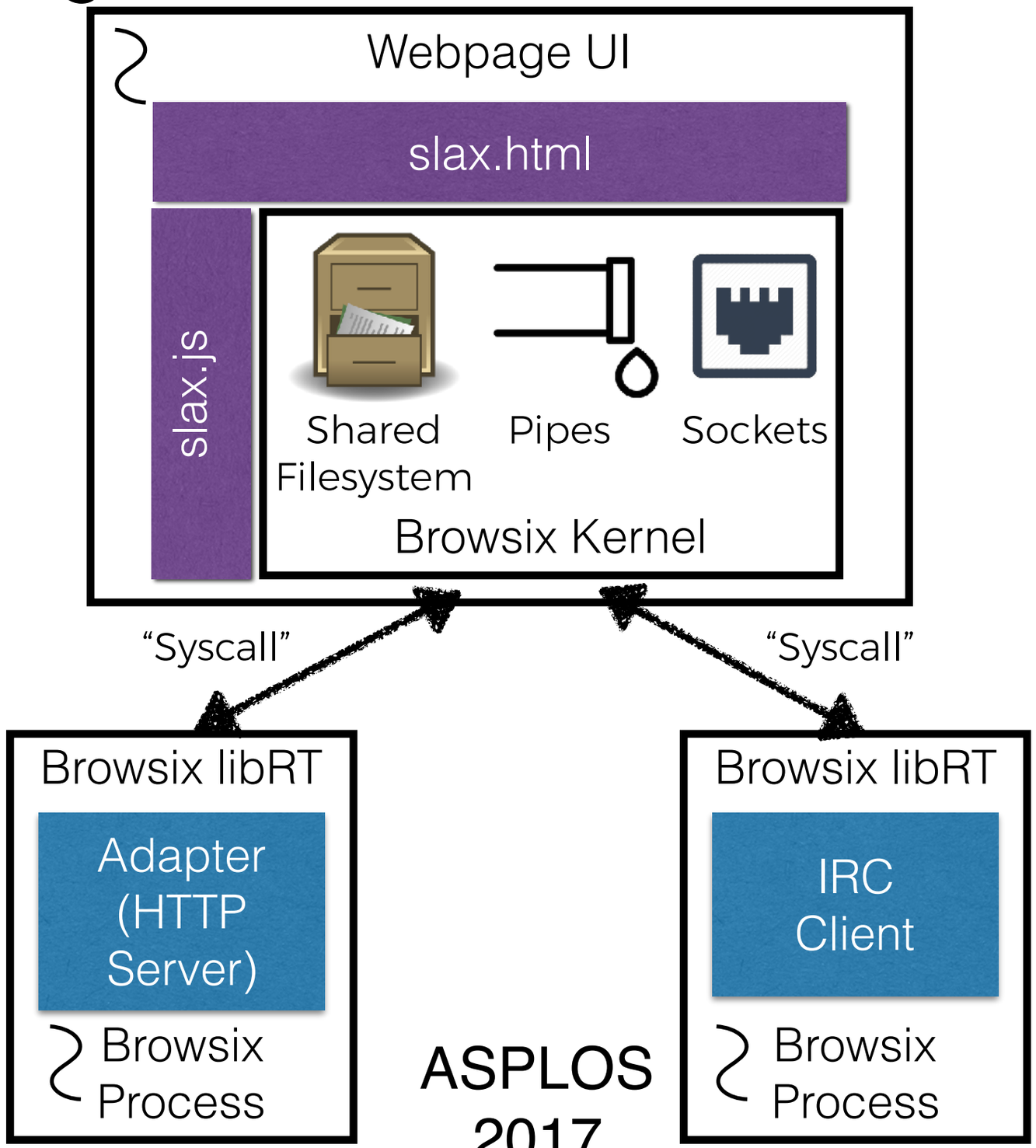


Browsix: Bridging the Gap Between Unix and the Browser



Browsix: Bridging the Gap Between Unix and the Browser

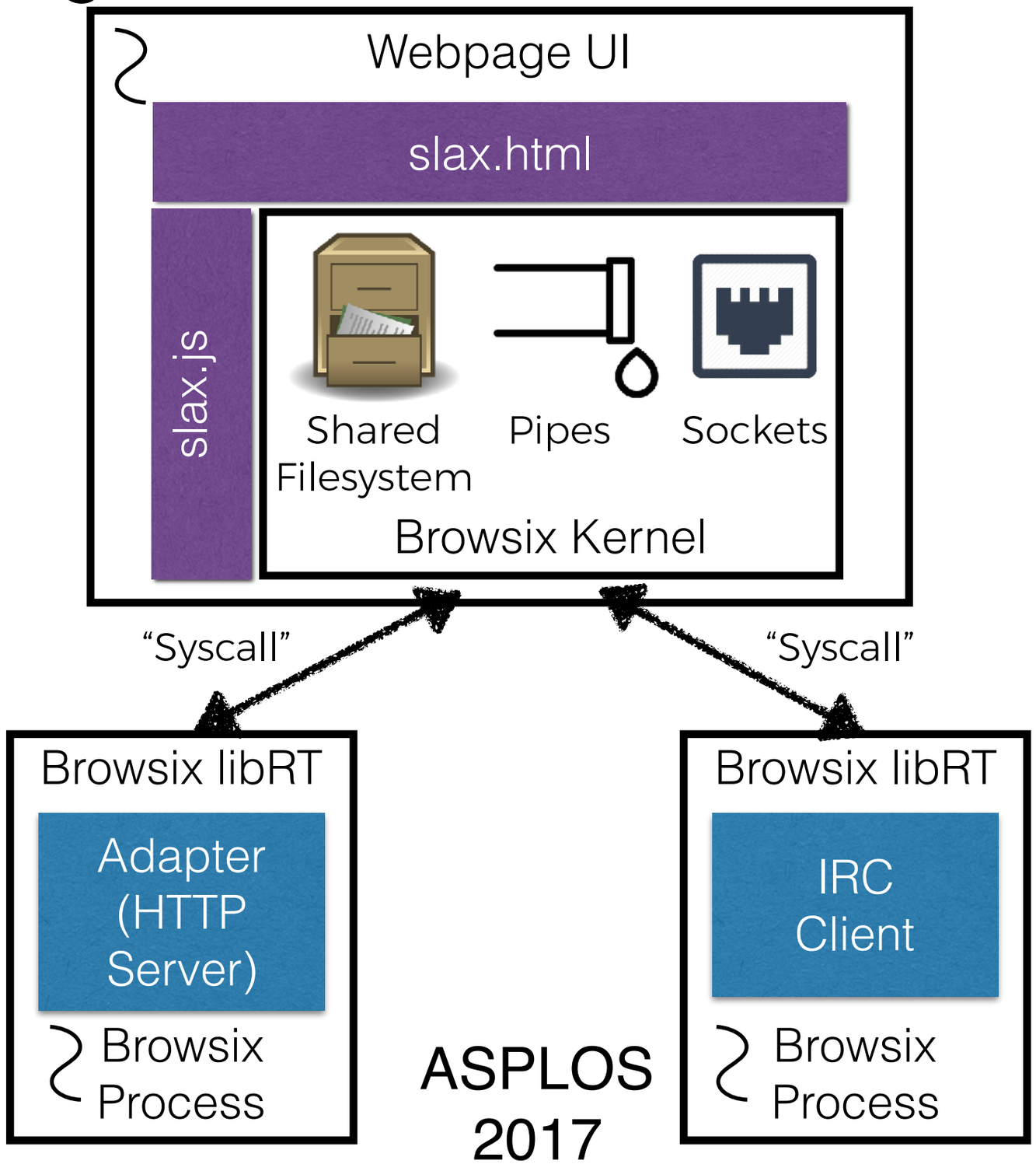
browsix.org



ASPLOS 2017

Browsix: Bridging the Gap Between Unix and the Browser

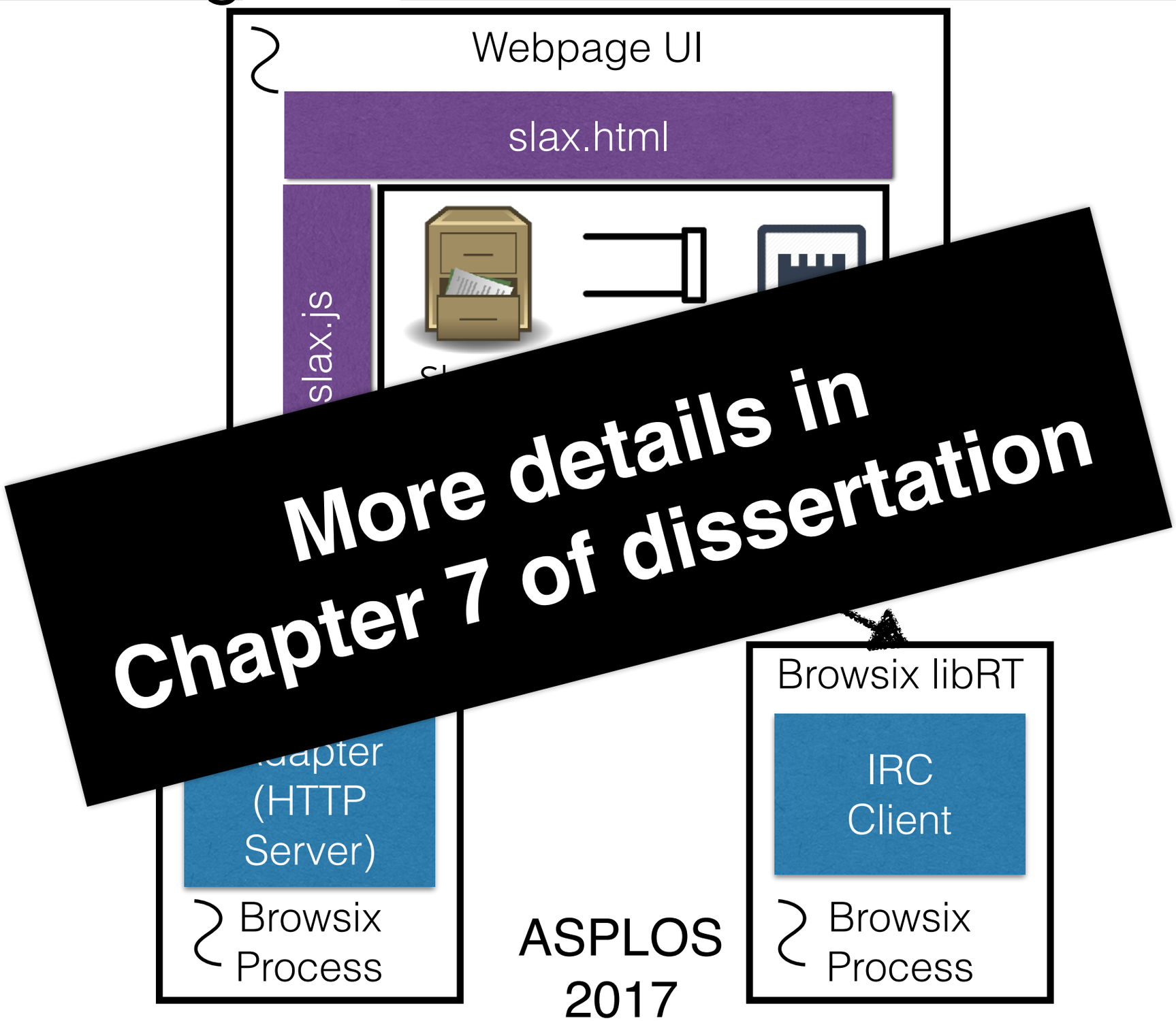
browsix.org



ASPLOS 2017

Browsix: Bridging the Gap Between Unix and the Browser

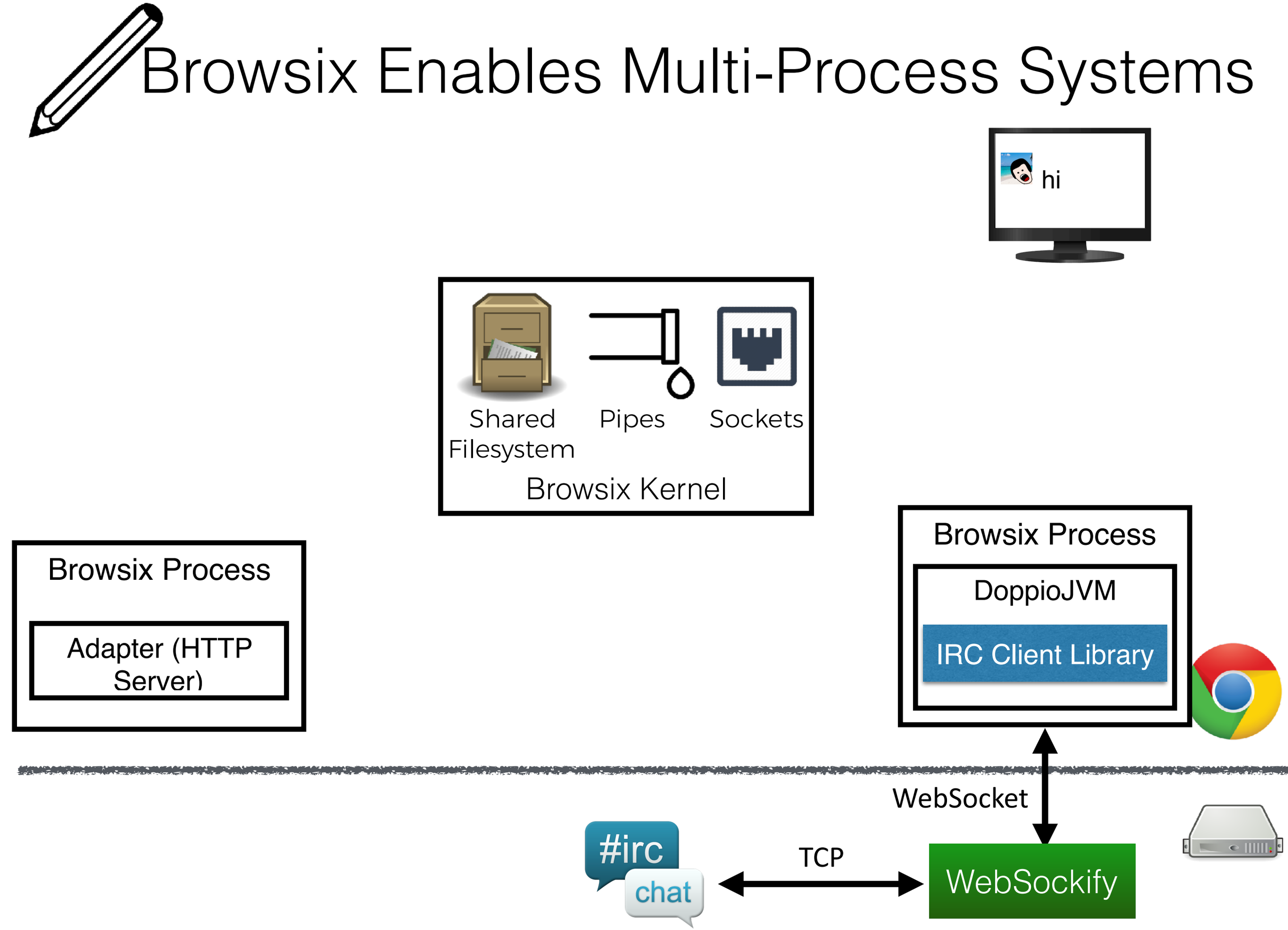
browsix.org



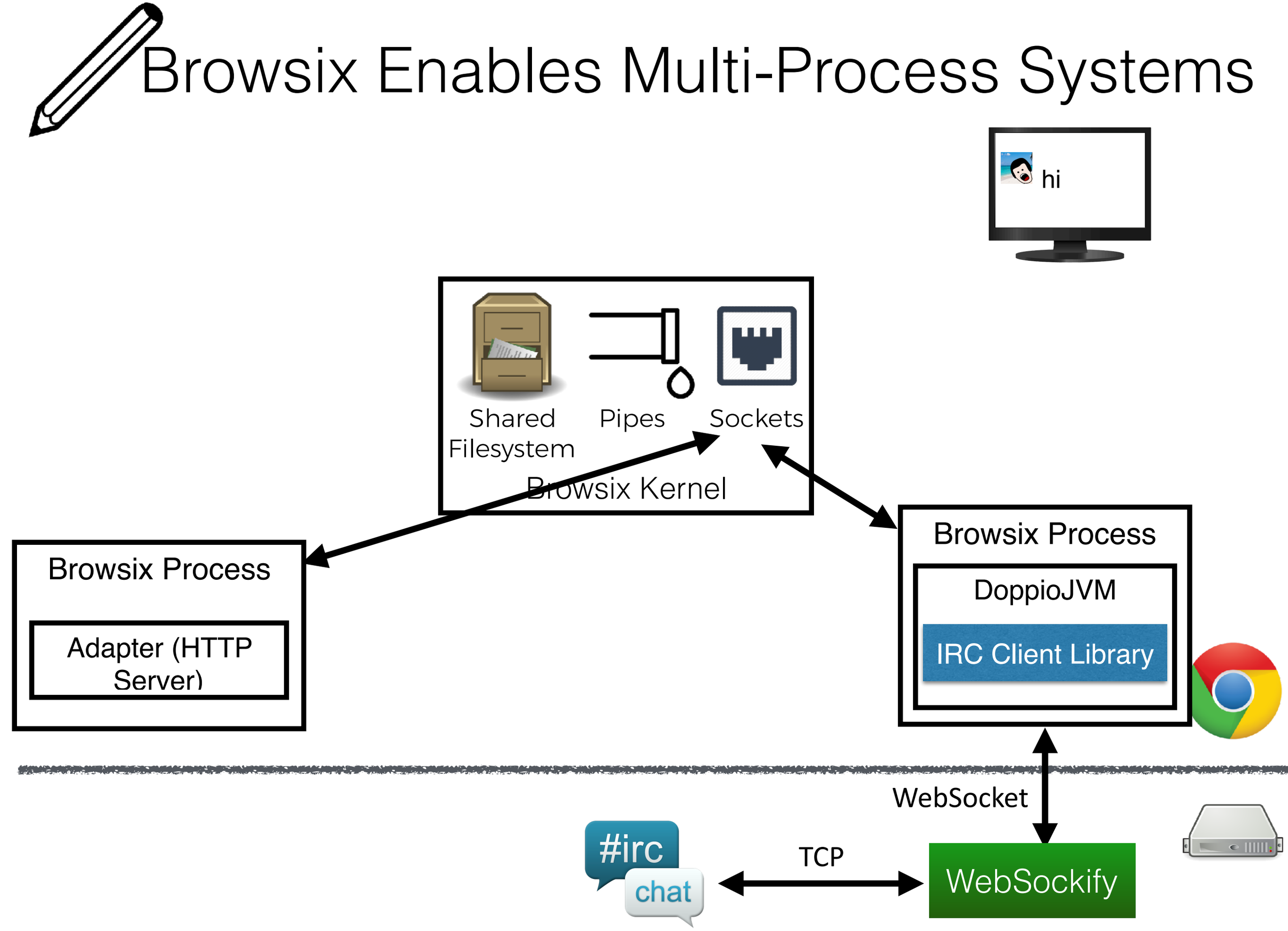
More details in Chapter 7 of dissertation

ASPLOS 2017

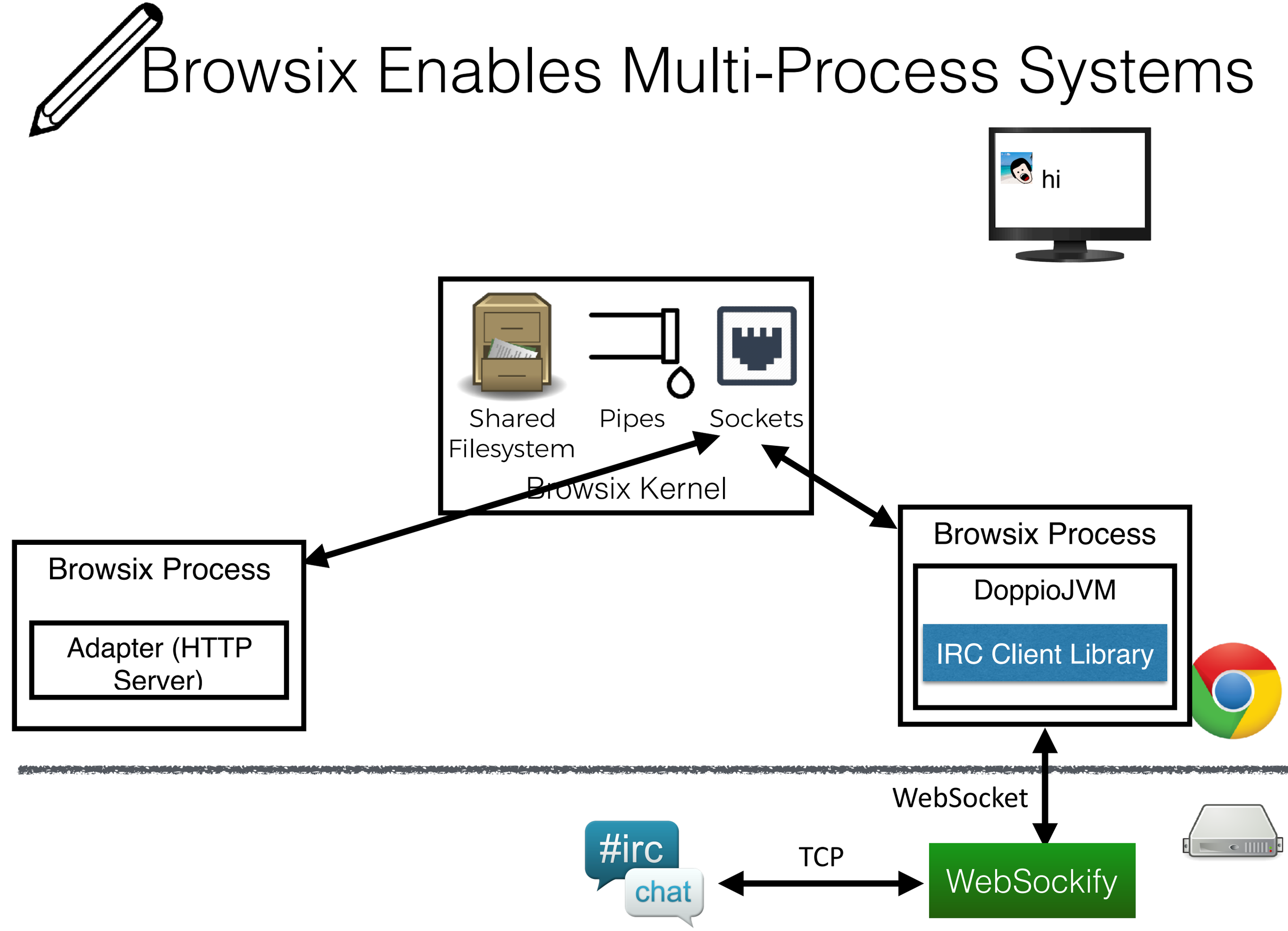
Browsix Enables Multi-Process Systems



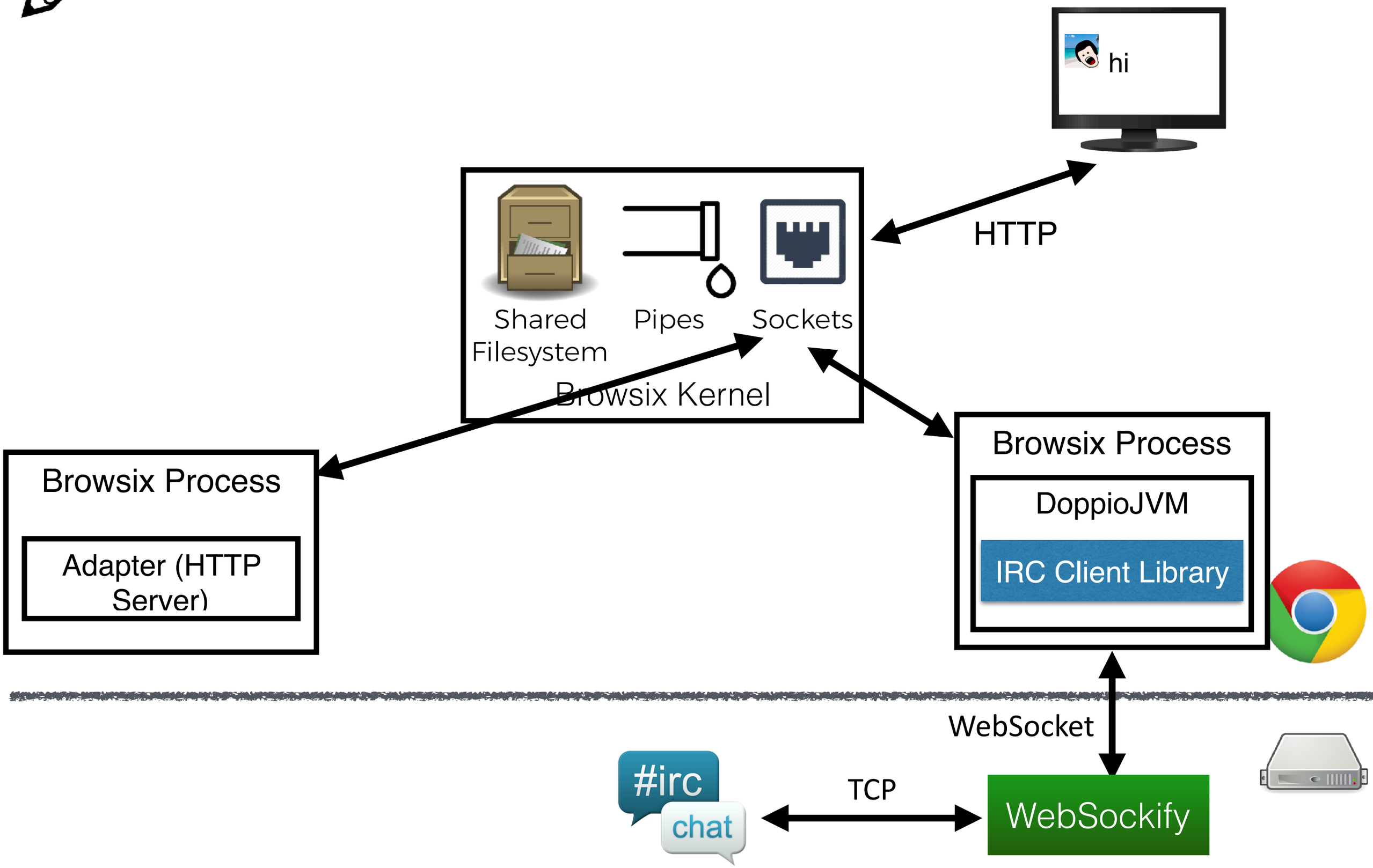
Browsix Enables Multi-Process Systems



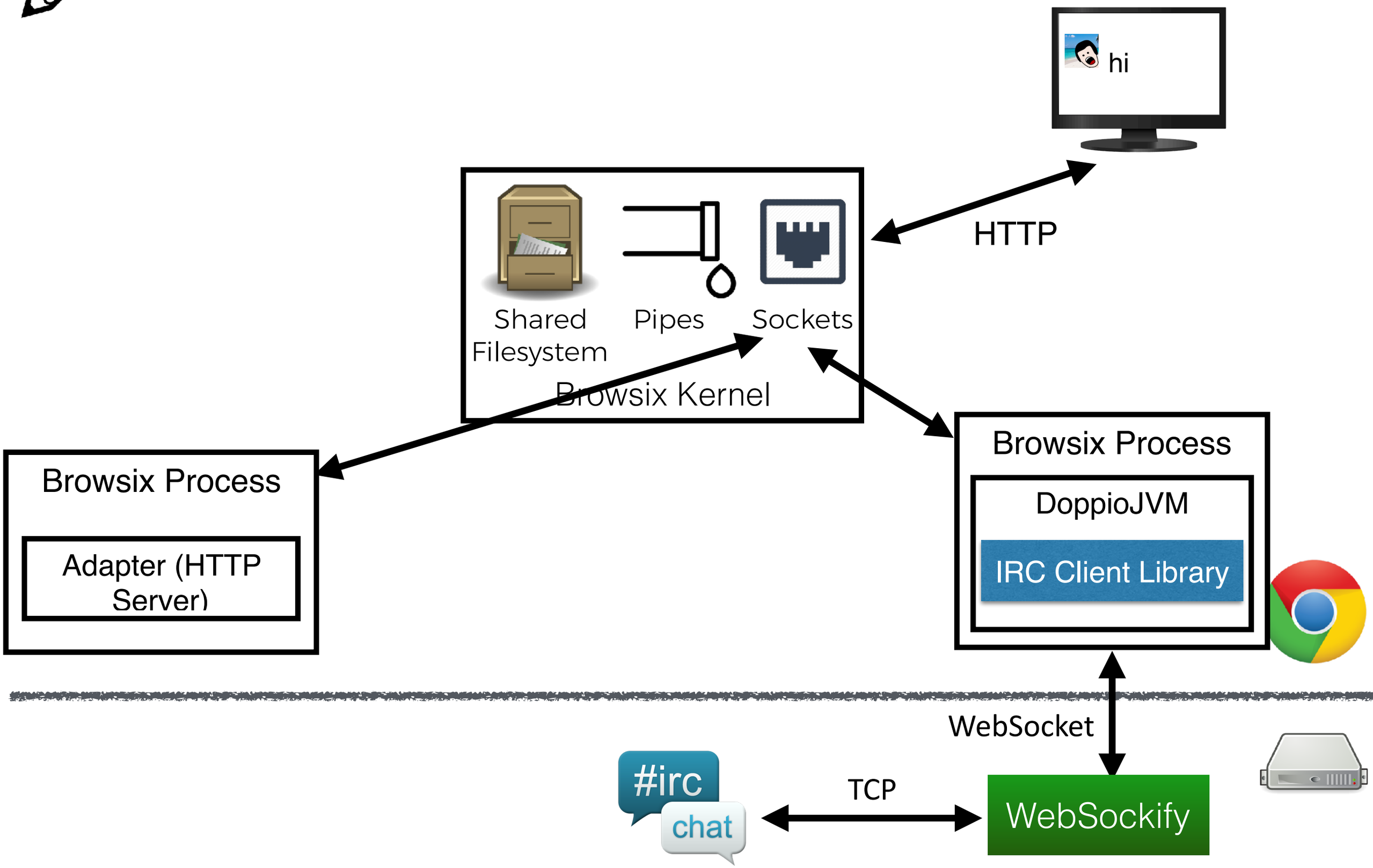
Browsix Enables Multi-Process Systems



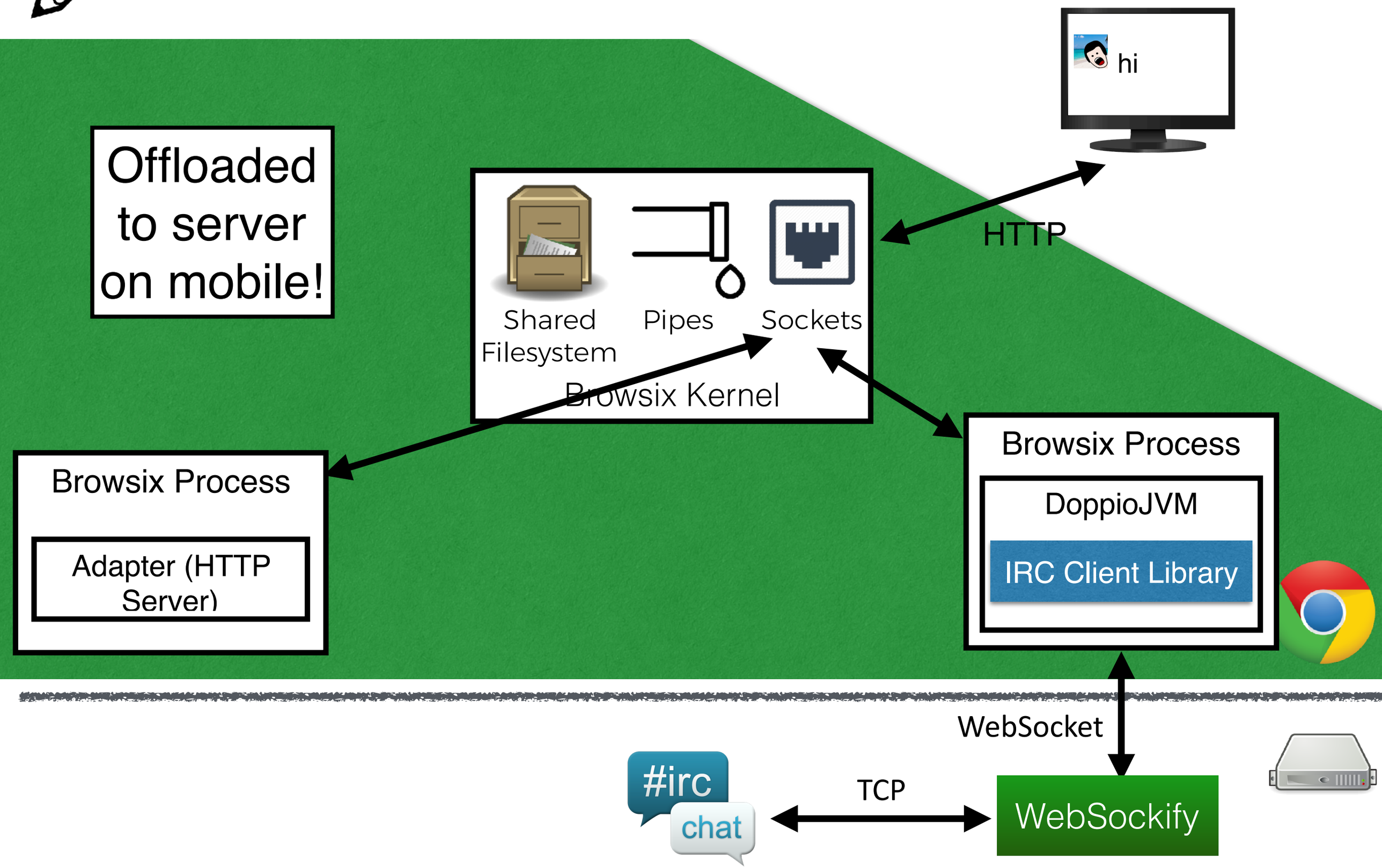
Browsix Enables Multi-Process Systems



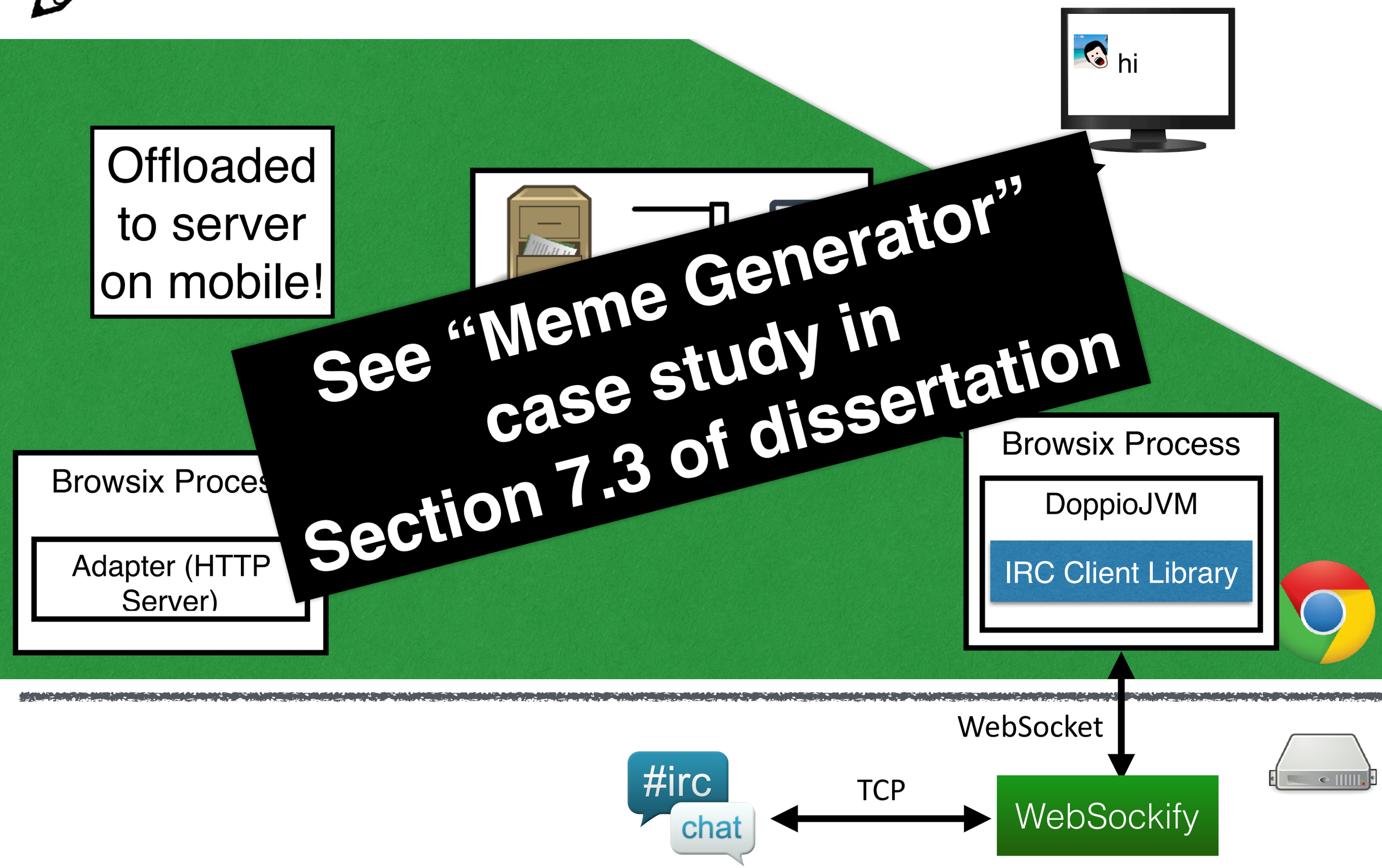
Browsix Enables Multi-Process Systems



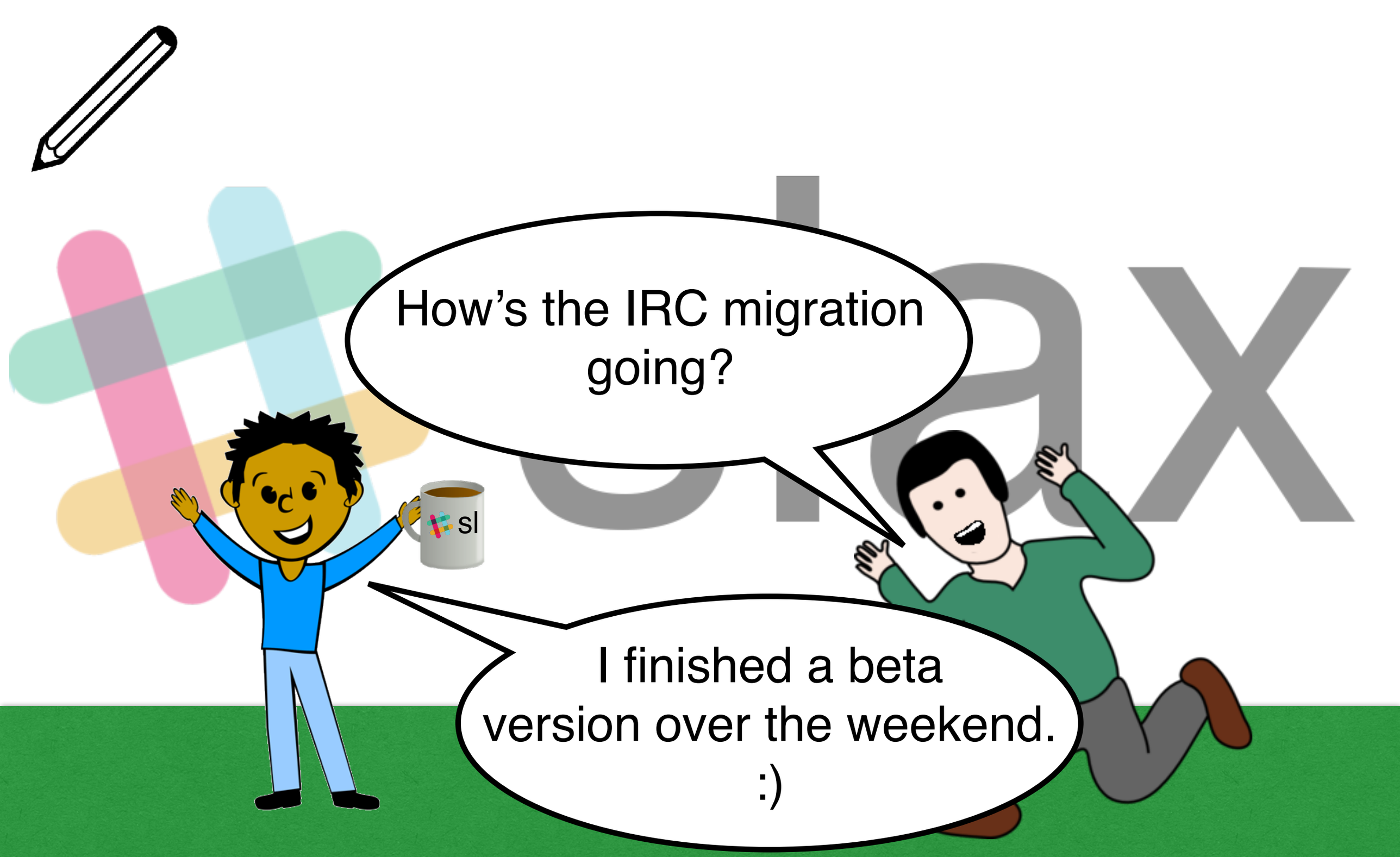
Browsix Enables Multi-Process Systems



Browsix Enables Multi-Process Systems



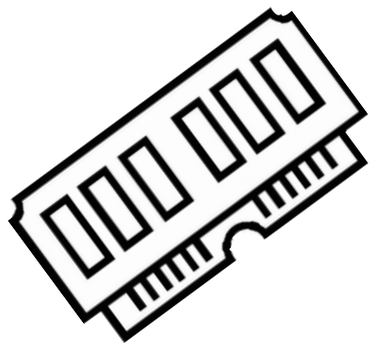
slax
sl



MOVE FAST AND BREAK LESS OFTEN

Conclusion

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

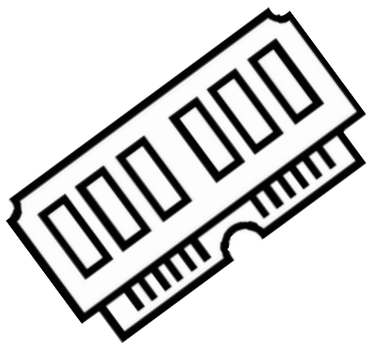
Causal Program Understanding (BCause)

POSIX Support (Doppio)

Unix Support (Browsix)

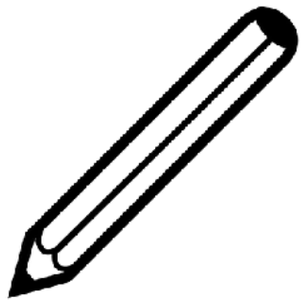
Conclusion

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

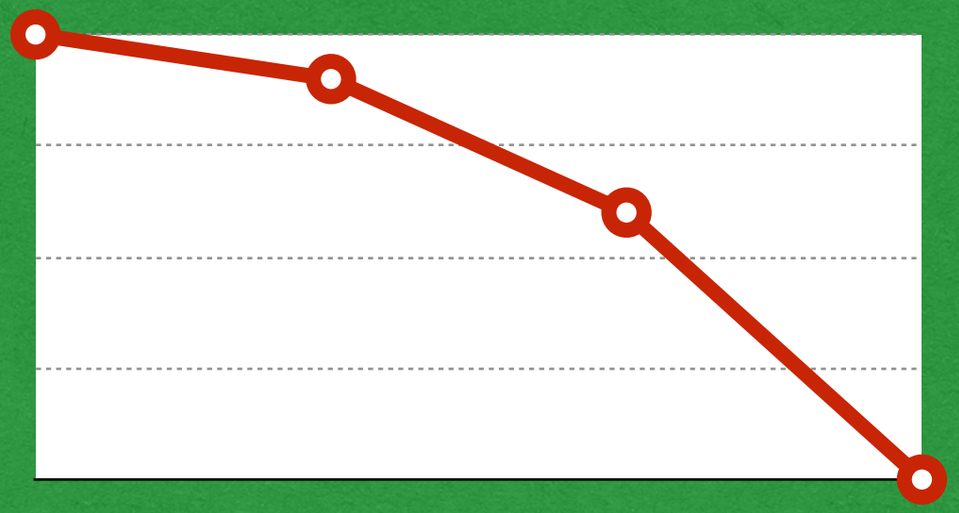
Causal Program Understanding (BCause)



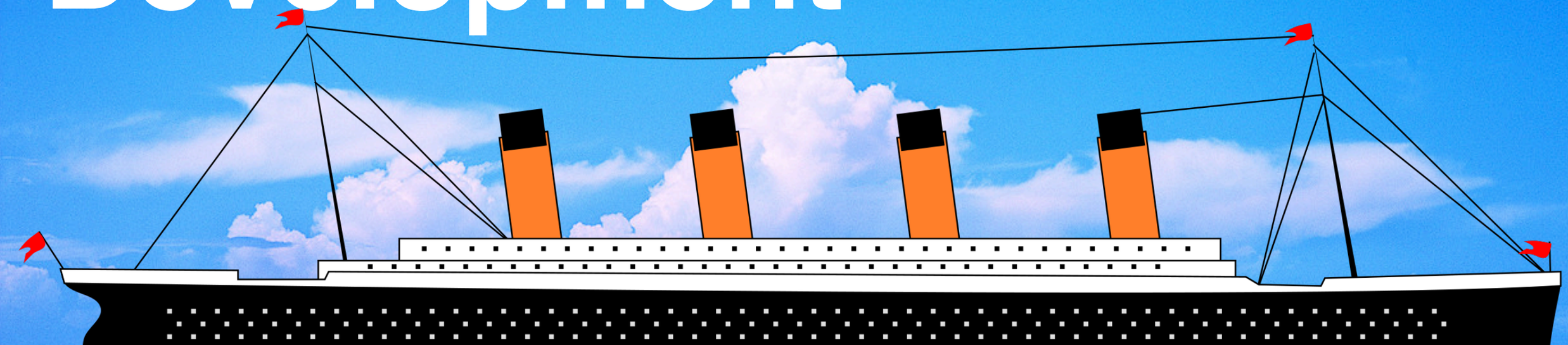
POSIX Support (Doppio)

Unix Support (Browsix)

Slax's Bottom Line



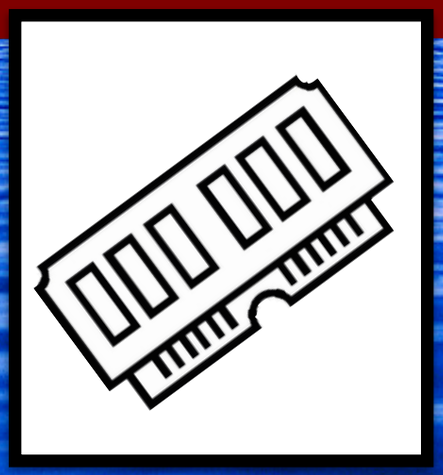
Righting Web Development



Dissertation Defense

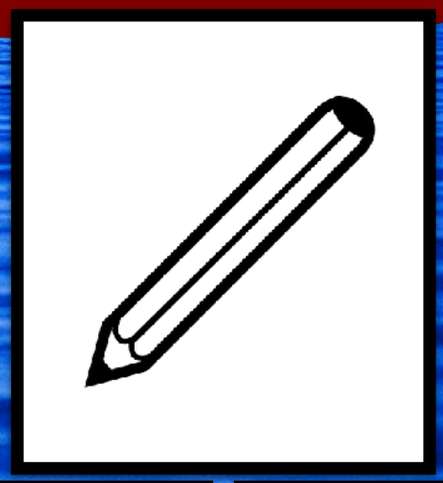
John Vilk

Time-Traveling Debugger (McFly)



Automatic Memory Leak Debugger (BLeak)

Causal Program Understanding (BCause)



POSIX Support (Doppio)

Unix Support (Browsix)