

Sinatra: Stateful Instantaneous Updates for Commercial Browsers through Multi-Version eXecution

Ugnius Rumsevicius
Siddhanth Venkateshwaran
Ellen Kidane
Luís Pina

University of Illinois Chicago



UIC



CCF-2227183



ENGINEERING

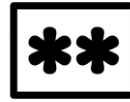


“Google is aware that an exploit for CVE-2023-2136 exists in the wild,” the company warned.

The official CVE report adds that exploiting the flaw (...) could pave a way for the hacker to (...) run untrusted malicious code on a computer

<https://www.pcmag.com/news/google-detects-second-zero-day-chrome-exploit-days-after-patching-another>

Browsers keep private data



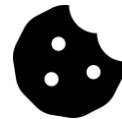
Passwords



Credit Cards



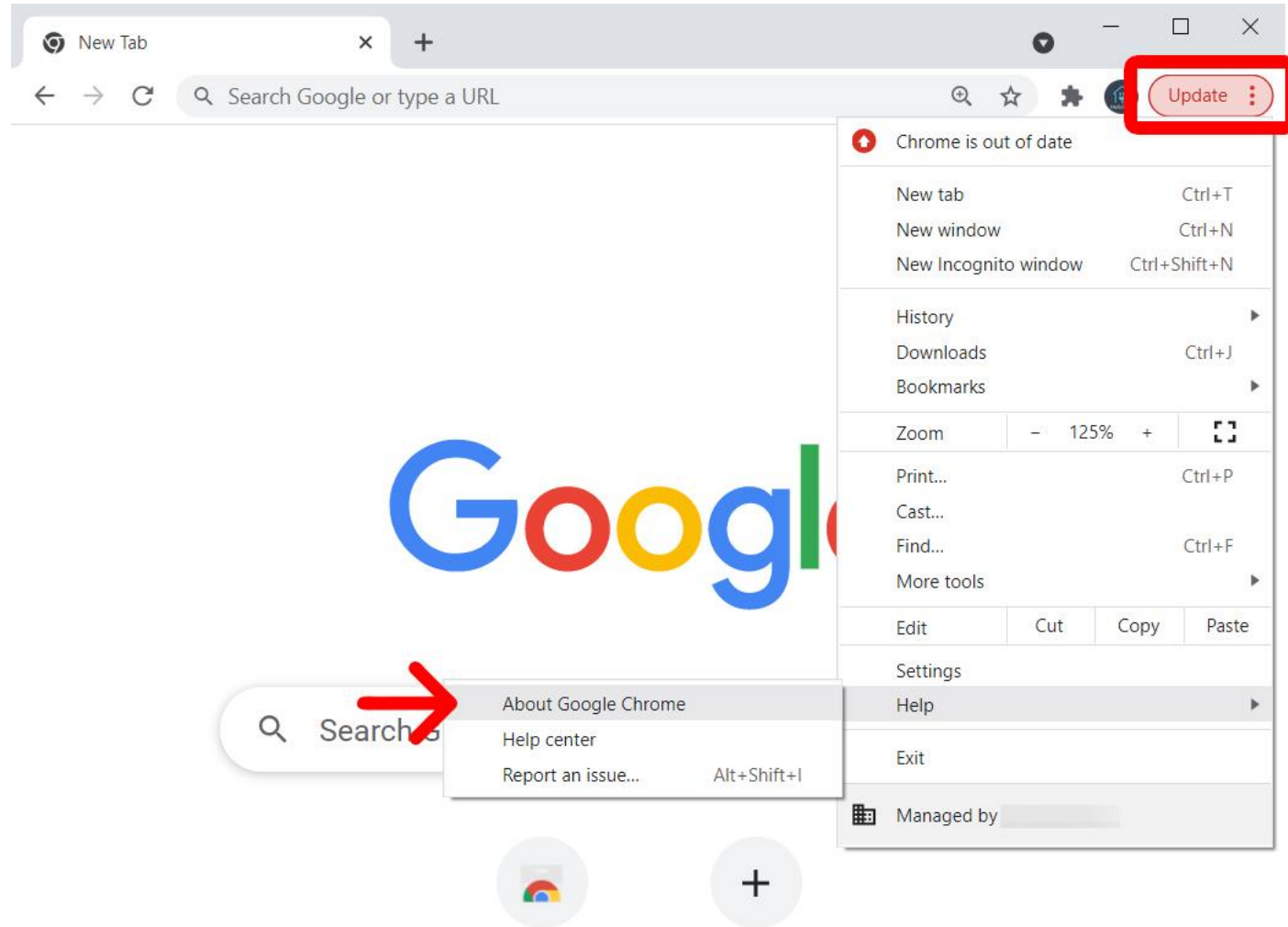
Home address



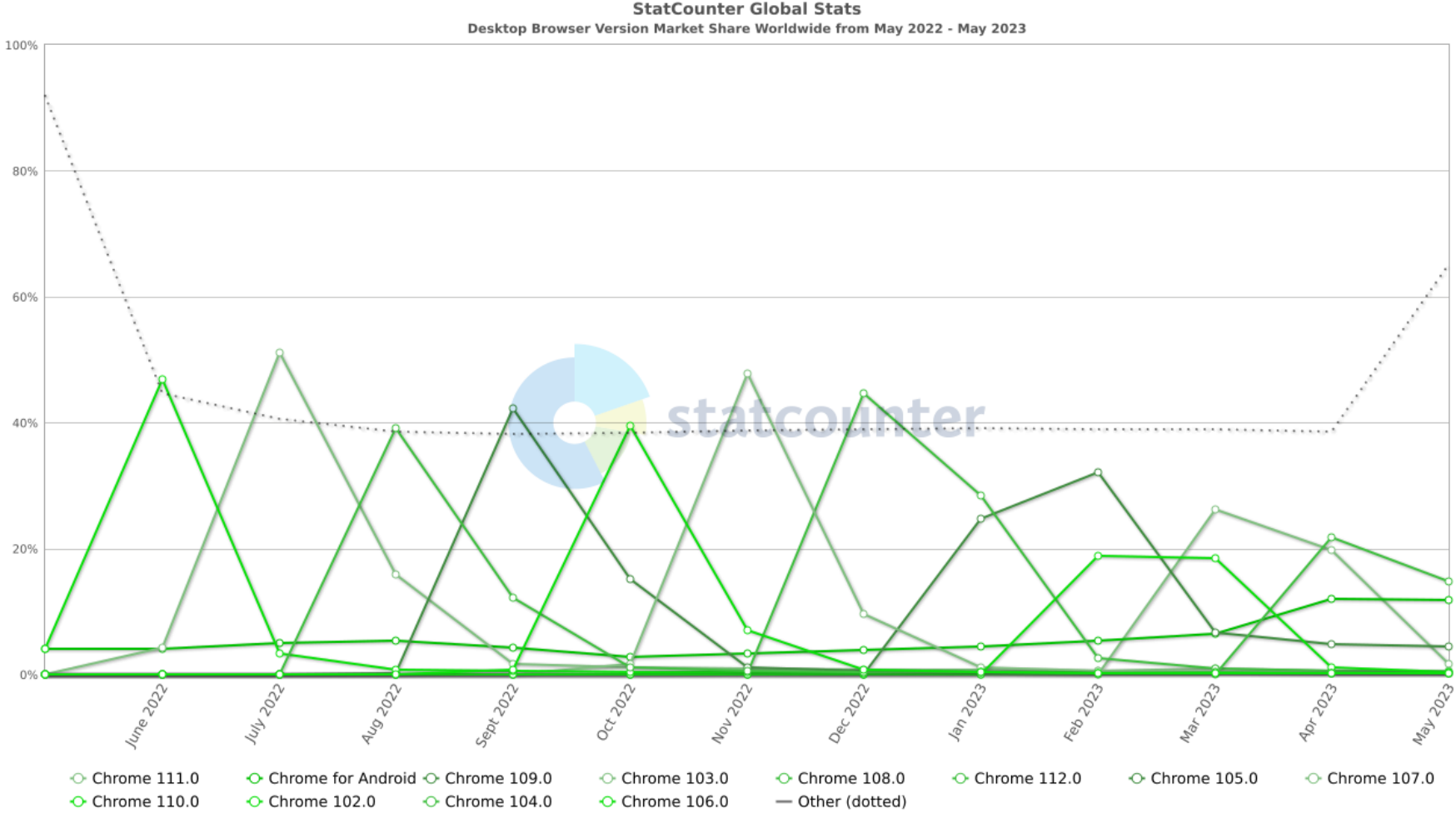
Cookies



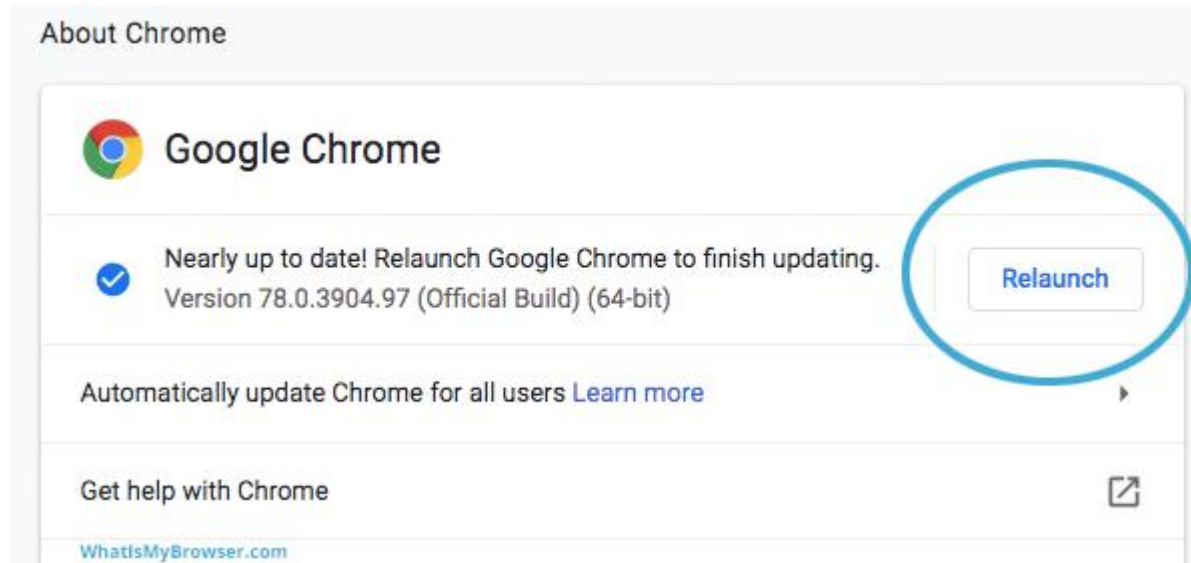
Best defense: Frequent updates



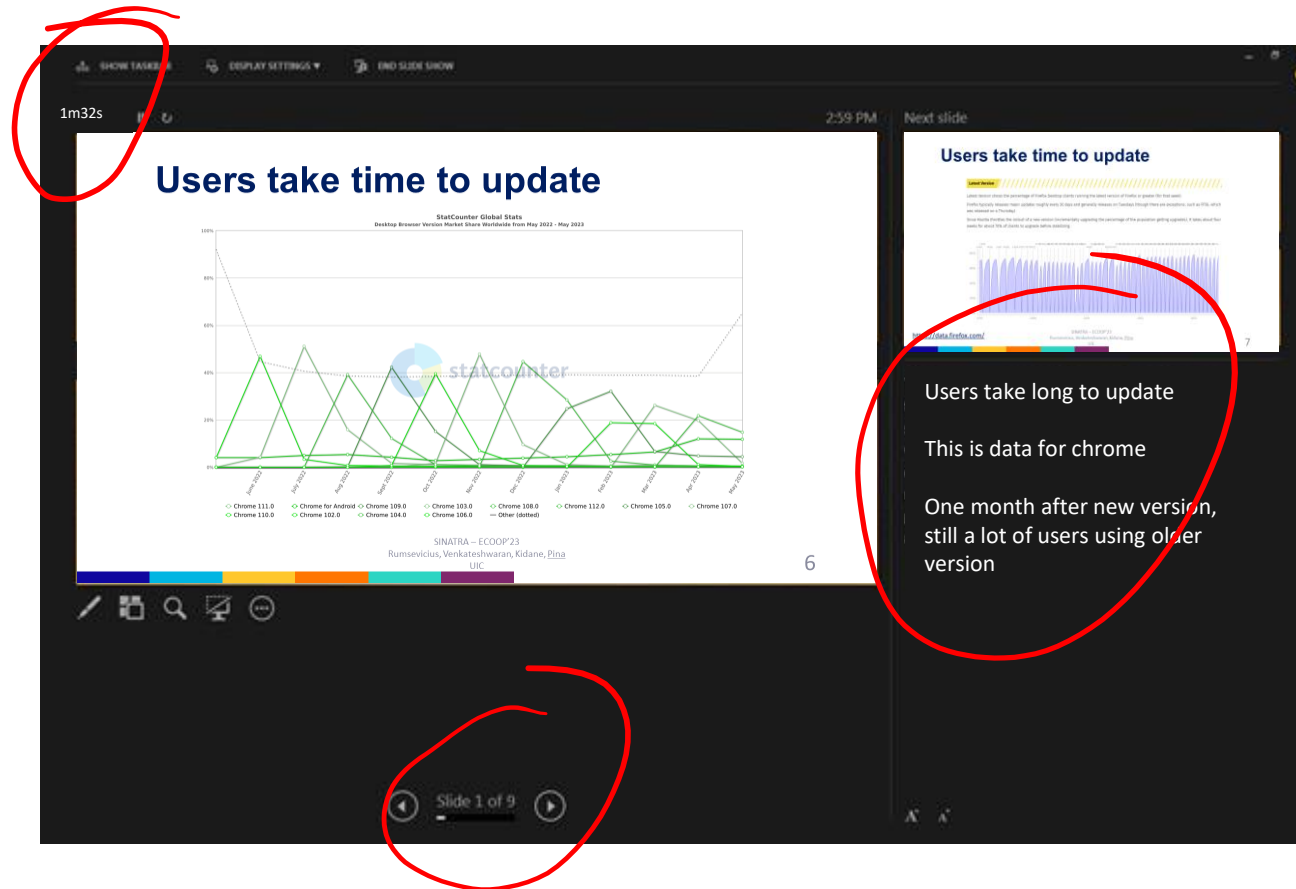
Users take time to update



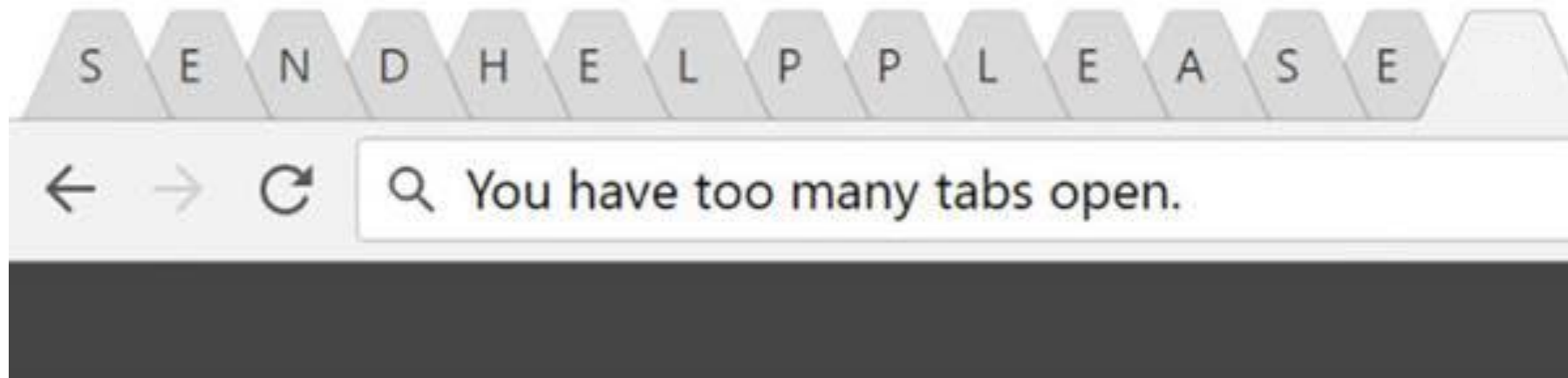
Browser updates take time



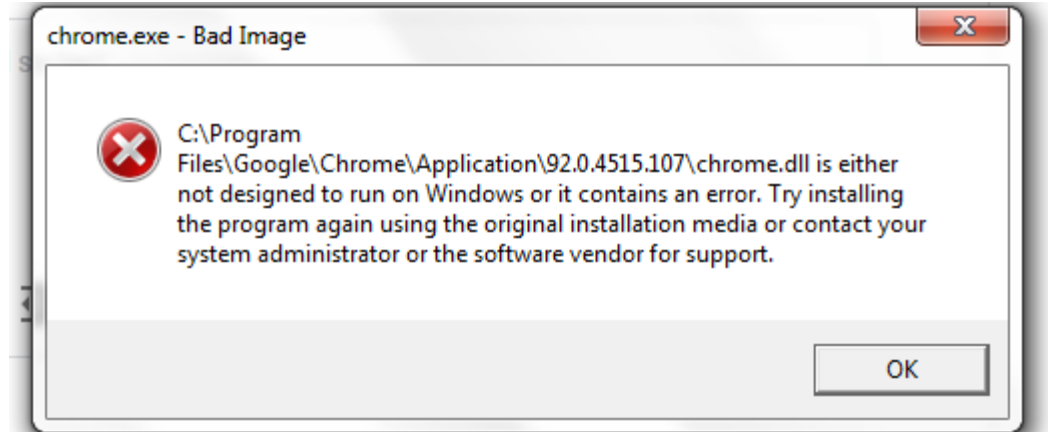
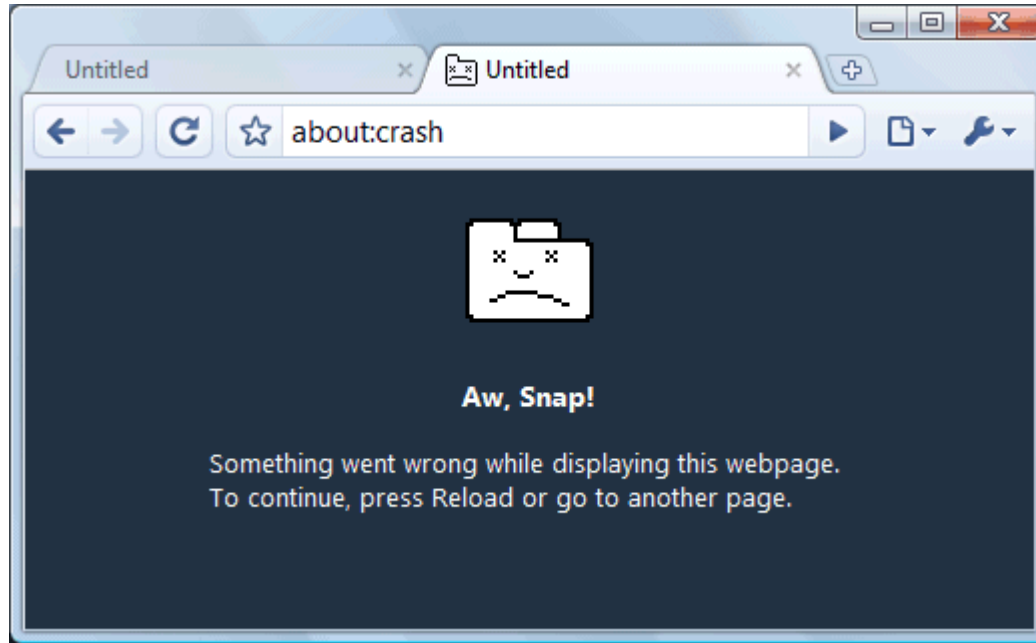
Browser updates lose state



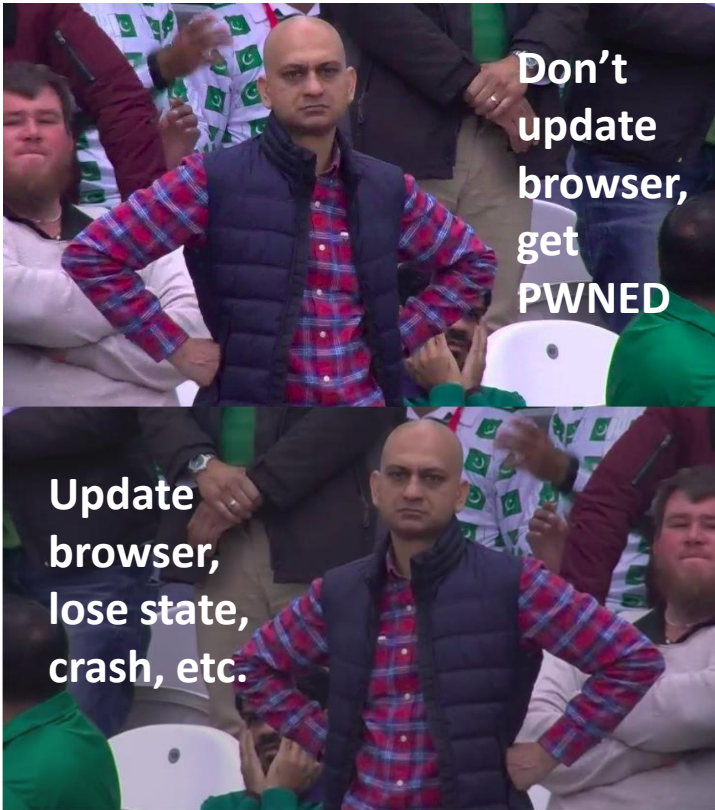
Browser updates lose state



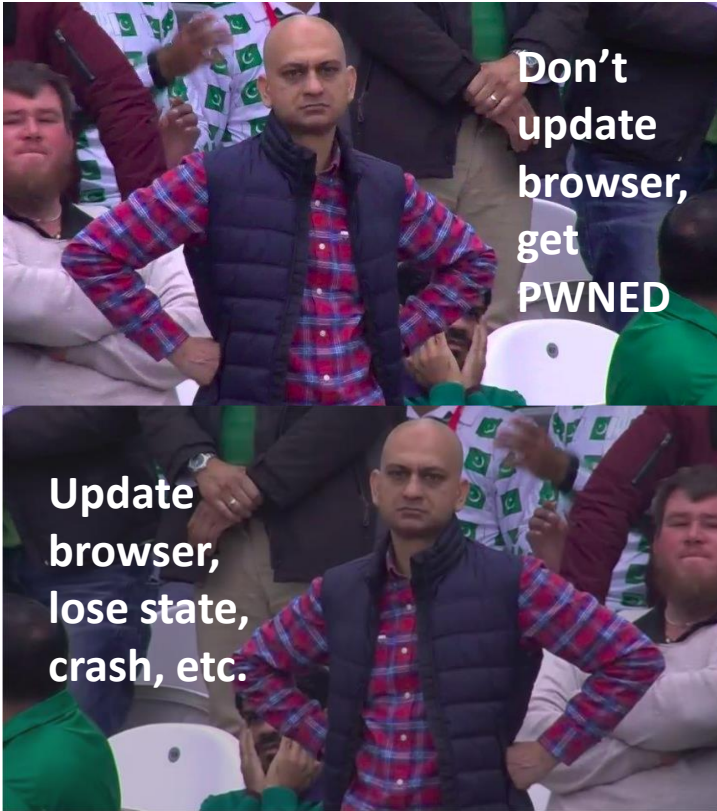
Browser updates may fail



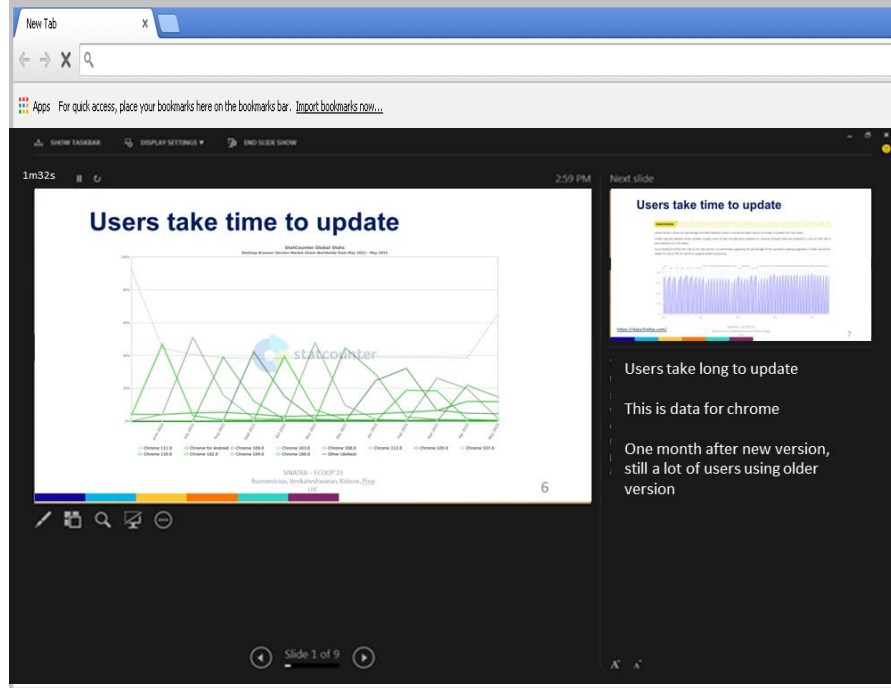
No good option



No good option



SINATRA



First step in automatic updates

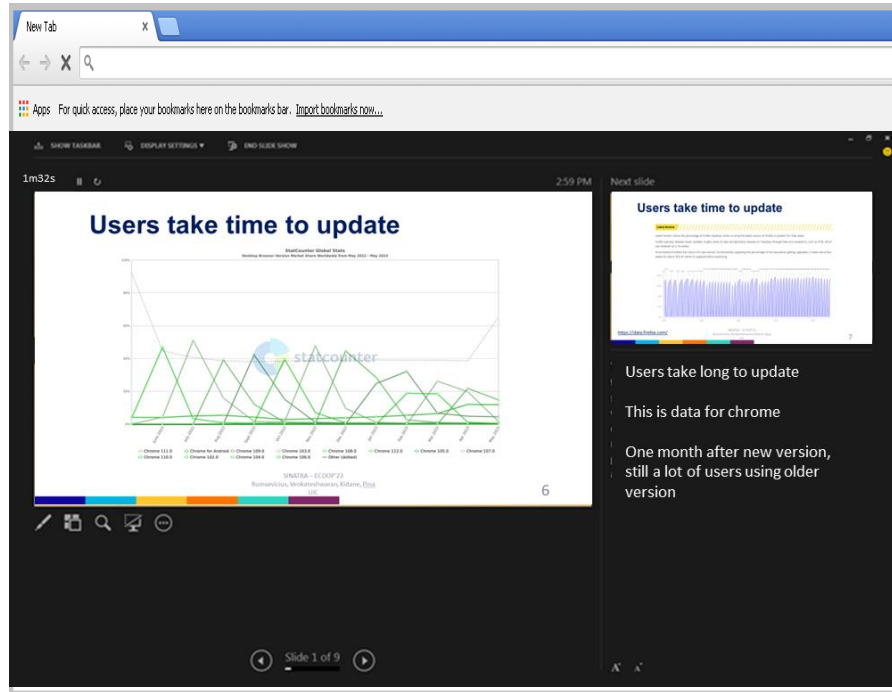
Browser updates as soon as possible without user noticing

Only 10ms pause to perform updates

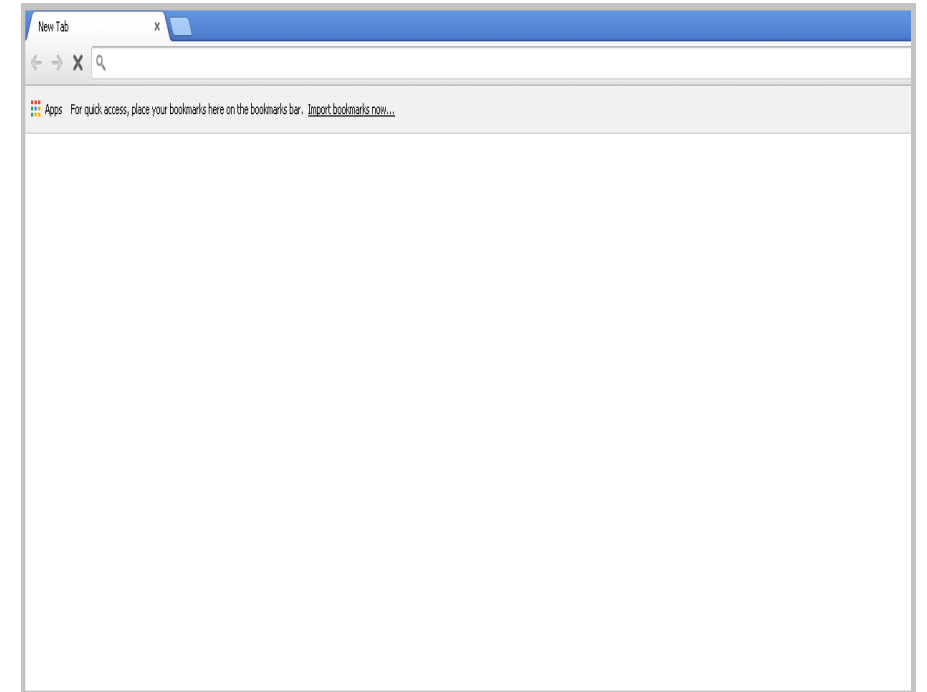
Browser agnostic



SINATRA

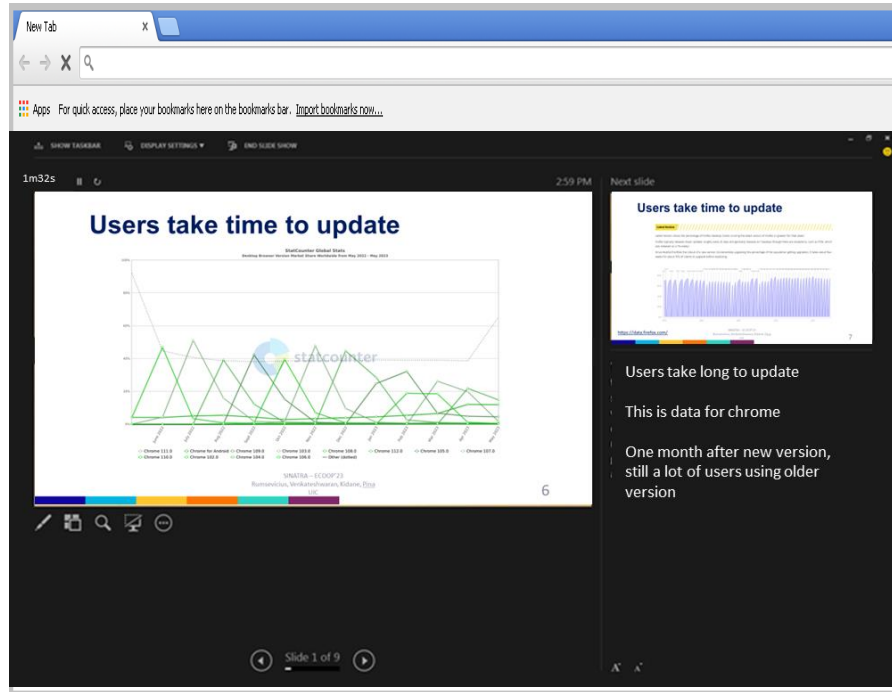


Old browser version

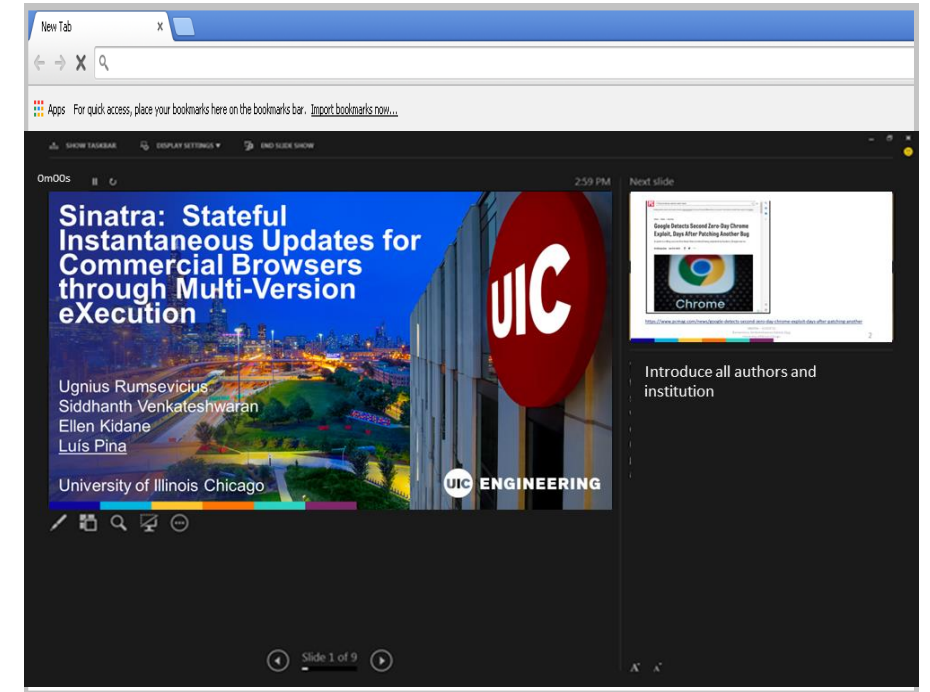


1. Launch new browser version

SINATRA

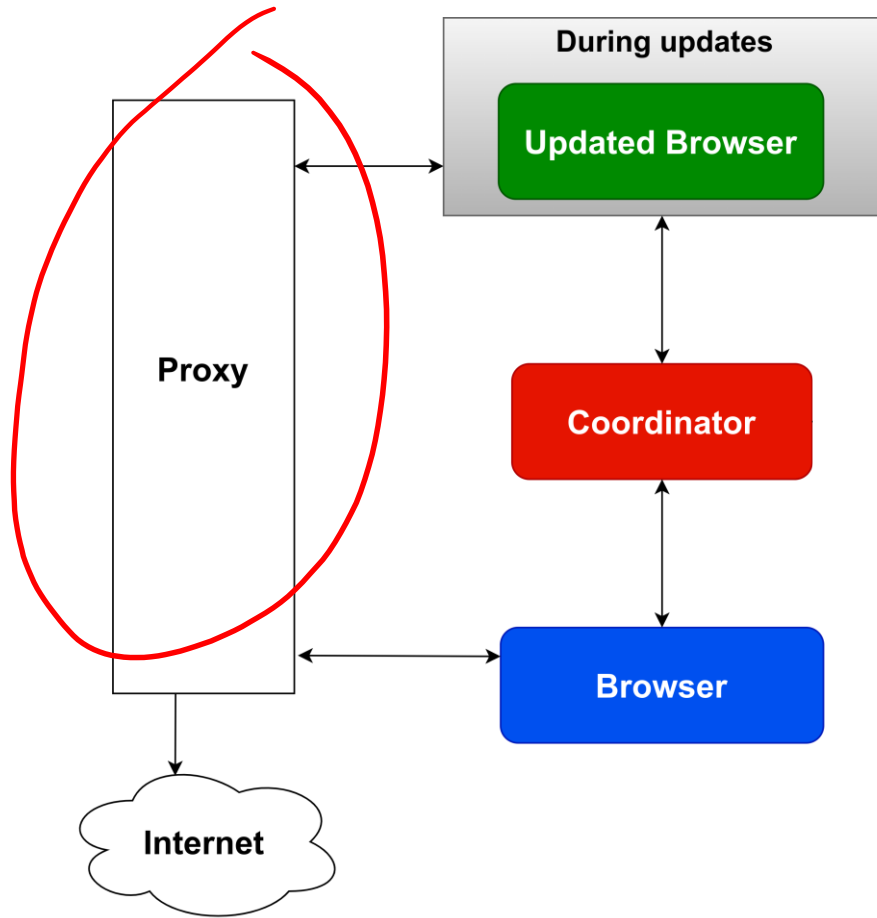


Old browser version

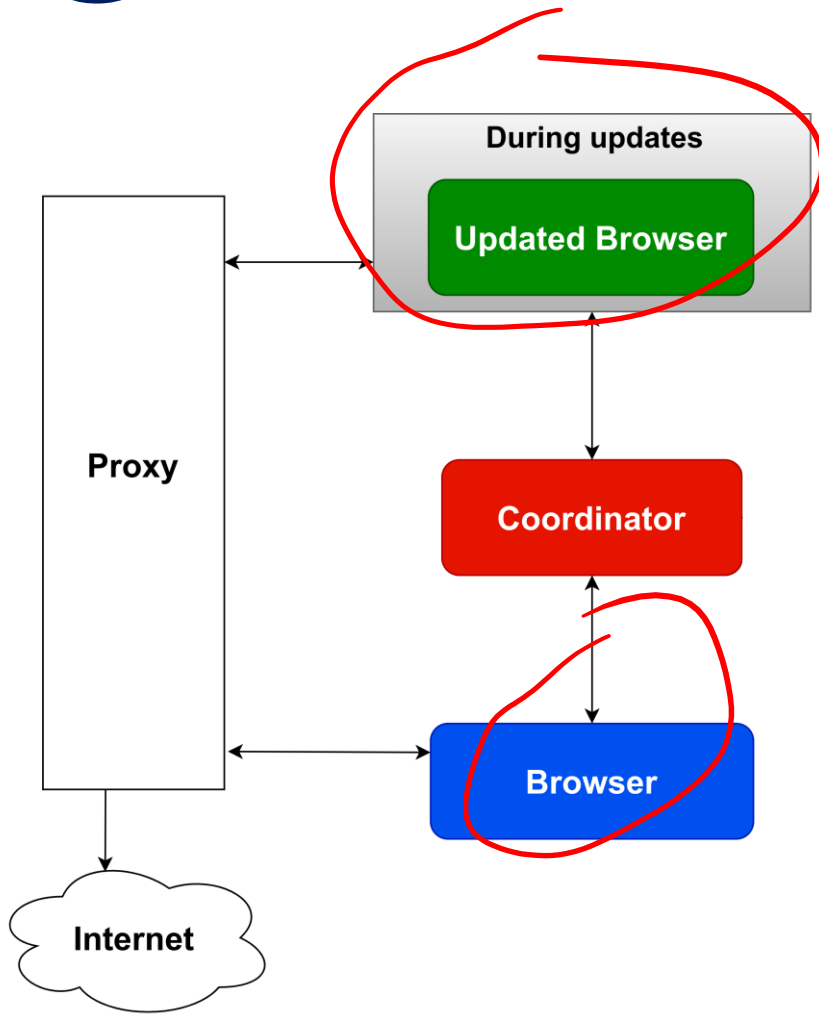


1. Launch new browser version
2. Open same page, get same contents

SINATRA architecture



SINATRA architecture

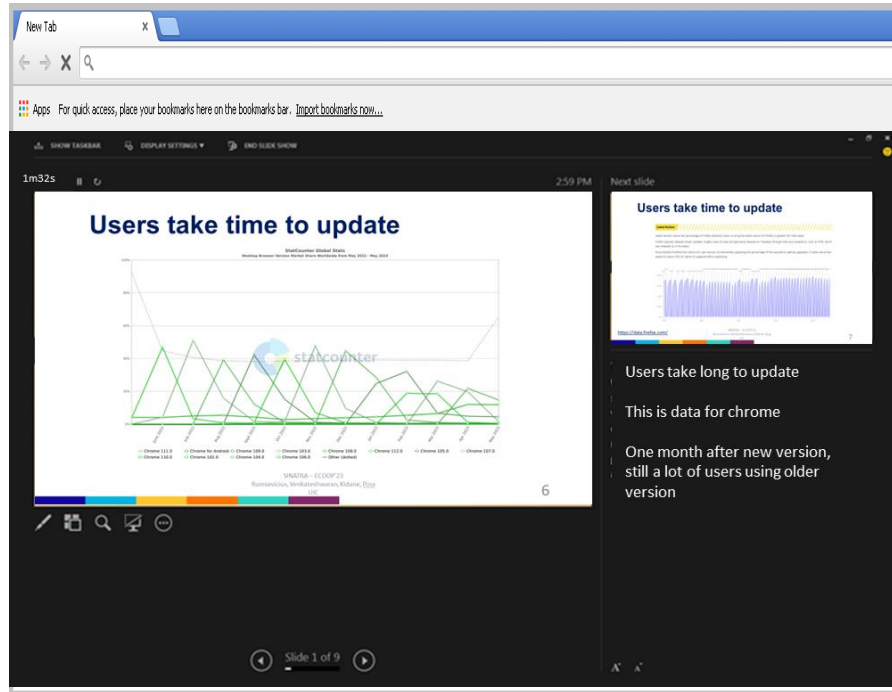


```
Flows
GET https://www.google.com/
  → 200 text/html 64.52k 487ms
GET https://www.google.com/logos/doodles/2018/doodle-snow-games-day-12-6870619765473288-s.png
  → 200 image/png 2.63k 184ms
GET https://www.google.com/logos/2018/snowgames_skijump/cta.png
  → 200 image/png 13.4k 229ms
>> GET https://www.gstatic.com/external_hosted/createjs/createjs-2015.11.26.min.js
  → 200 text/javascript 46.51k 475ms
GET https://ssl.gstatic.com/gb/images/i2_2ec824b0.png
  → 200 image/png 23.64k 253ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb
  → 200 application/octet-stream 67.92k 356ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
  → 200 application/octet-stream 67.92k 412ms
GET https://www.google.com/logos/2018/snowgames_skijump/skijump18.js
  → 200 text/javascript 258.18k 909ms
POST https://www.google.com/gen_204?sr=webaft&atyp=csi&ei=vCGLW6uMkK8gTYs6y1Am&rt=wsrt.2615,oft.1379,prt.1379
  → 204 text/html [no content] 379ms
GET https://www.gstatic.com/og/_js/kwoag.og2.en_US.u1hn@N1161.0/rt-tj/m-def/exm-in,foot/d-1/ed-1/rs-AA2YrUvDKaJhL
  → 200 text/javascript 46.4k 265ms
GET https://www.google.com/xjs/_js/kxjs.s.en.zjivxe8FVgY.0/m=ex,sb,cdo,s,cr,elag,hsm,jso,r,d,csi/amwCL0eME5yP8
  → 200 text/javascript 144.26k 368ms
GET https://www.google.com/xjs/_js/kxjs.s.en.zjivxe8FVgY.0/m=aa,abd,asyn,c,dvl,foot,fp,e,ipv6,lu,m,mu,sf,sonic,s
  → 200 text/javascript 30.54k 195ms
GET https://www.google.com/logos/2018/snowgames_skijump/main-sprite.png
  → 200 image/png 13.4k 229ms
0 [34/36]
• replay_client [Flow] [*:9999]
```

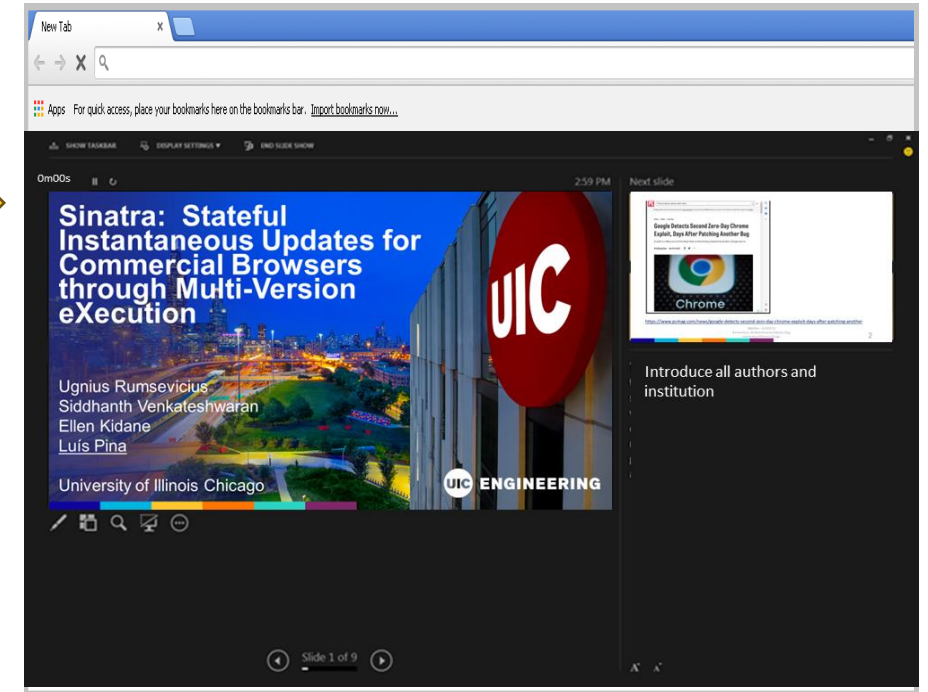
mitmproxy supports HTTPS and sophisticated rules

<https://mitmproxy.org/>

SINATRA

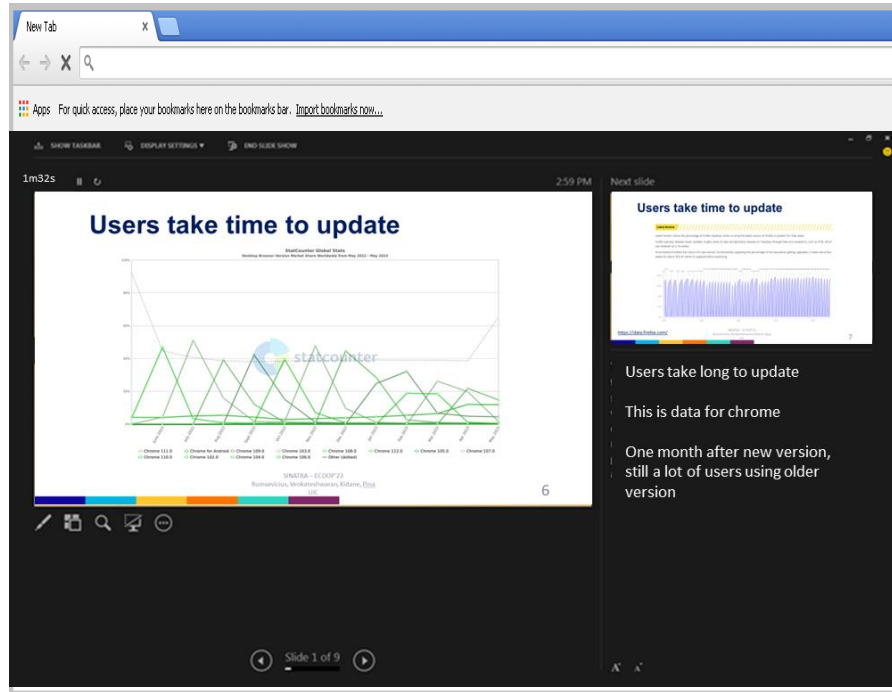


Old browser version

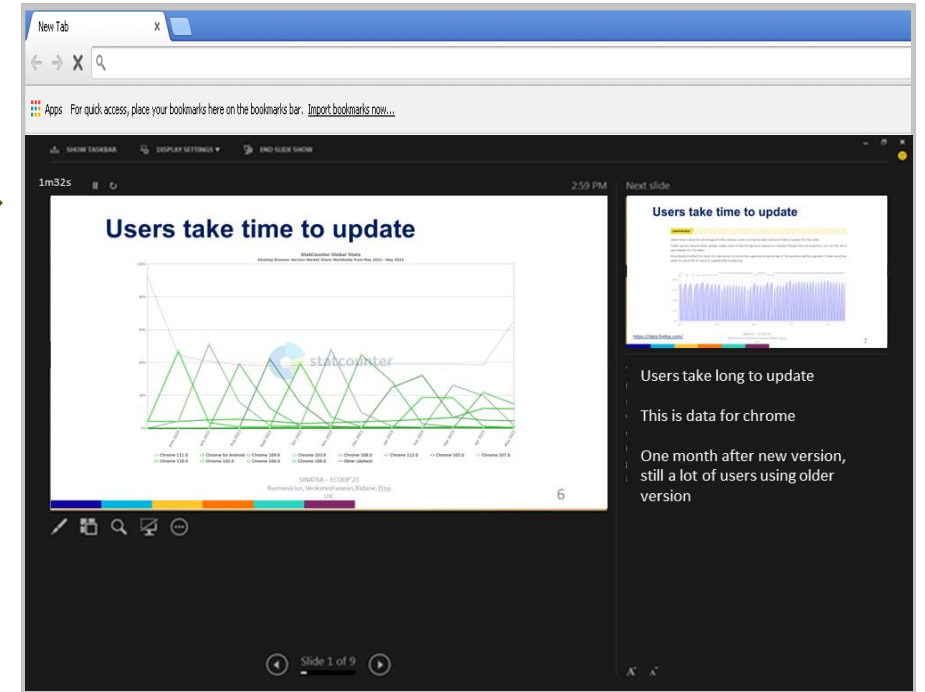


1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser

SINATRA

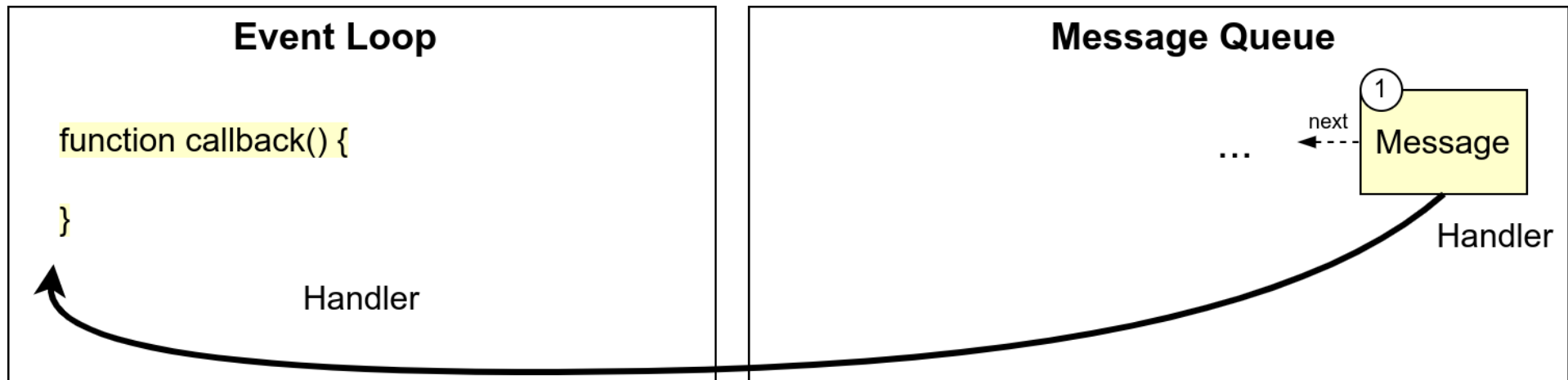


Old browser version

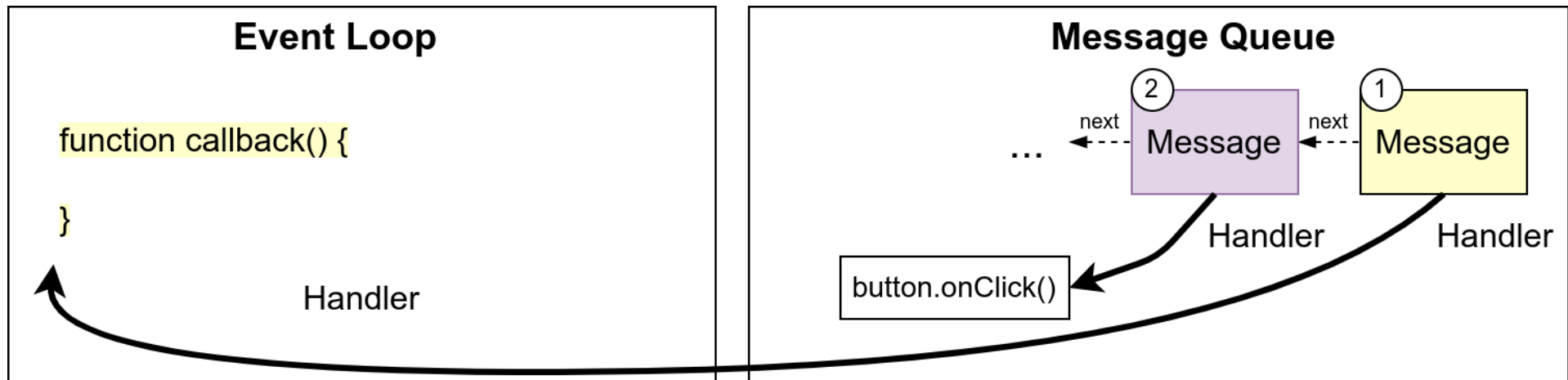


1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser

Javascript Events



Javascript Events



Intercepting Javascript Events

```
1 <html>
2   <head>
3 +   <script src="mvx/sinatra.js" type="text/javascript"></script>
4 +   <script src="mvx/sinatra_init.js" type="text/javascript" defer></script>
5   ...
6   </head>
7   <body>
8     ...
9   </body>
10 </html>
```

Intercepting Javascript Events

```
1 const originalAddEventListener = HTMLElement.prototype.addEventListener;  
2 HTMLElement.prototype.addEventListener = function(evType, evListener, u) {  
3  
4  
5  
6  
7  
8 }
```

Intercepting Javascript Events

```
1 const originalAddEventListener = HTMLElement.prototype.addEventListener;  
2 HTMLElement.prototype.addEventListener = function(evType, evListener, u) {  
3   let closure = function (ev) {  
4  
5  
6   }  
7   originalAddEventListener.call(this, evType, closure, u);  
8 }
```


Intercepting Javascript Events

```
1 const originalAddEventListener = HTMLElement.prototype.addEventListener;  
2 HTMLElement.prototype.addEventListener = function(evType, evListener, u) {  
3   let closure = function (ev) {  
4  
5     evListener.call(this, ev, u);  
6   }  
7   originalAddEventListener.call(this, evType, closure, u);  
8 }
```

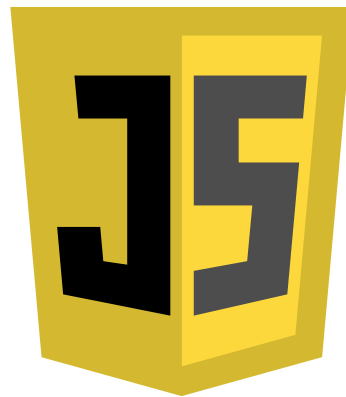
Intercepting Javascript Events

```
1 const originalAddEventListener = HTMLElement.prototype.addEventListener;
2 HTMLElement.prototype.addEventListener = function(evType, evListener, u) {
3   let closure = function (ev) {
4     sendToCoordinator(evType, ev);
5     evListener.call(this, ev, u);
6   }
7   originalAddEventListener.call(this, evType, closure, u);
8 }
```

Intercepting Javascript Events

Fully implemented in Javascript

```
1  
2  
3  
4     sendToCoordinator(evType, ev);  
5     evListener.call(this, ev, u);  
6 }  
7 originalAddEventListener.call(this, evType, closure, u);  
8 }
```



Intercepting Javascript Events

Fully implemented in Javascript

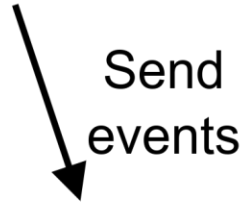
Browser agnostic



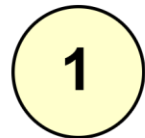
SINATRA phases



Version 0

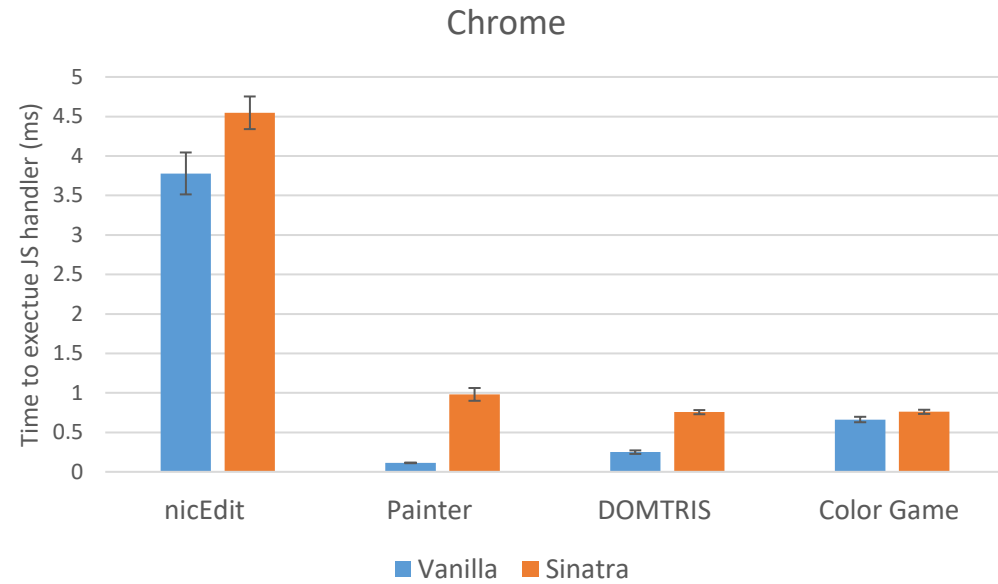
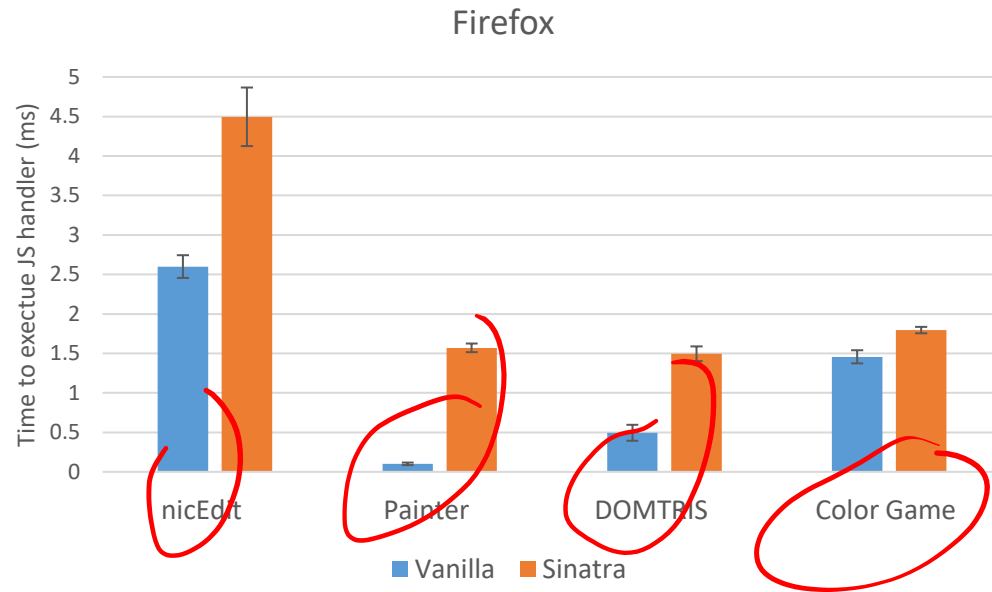


Coordinator



Record

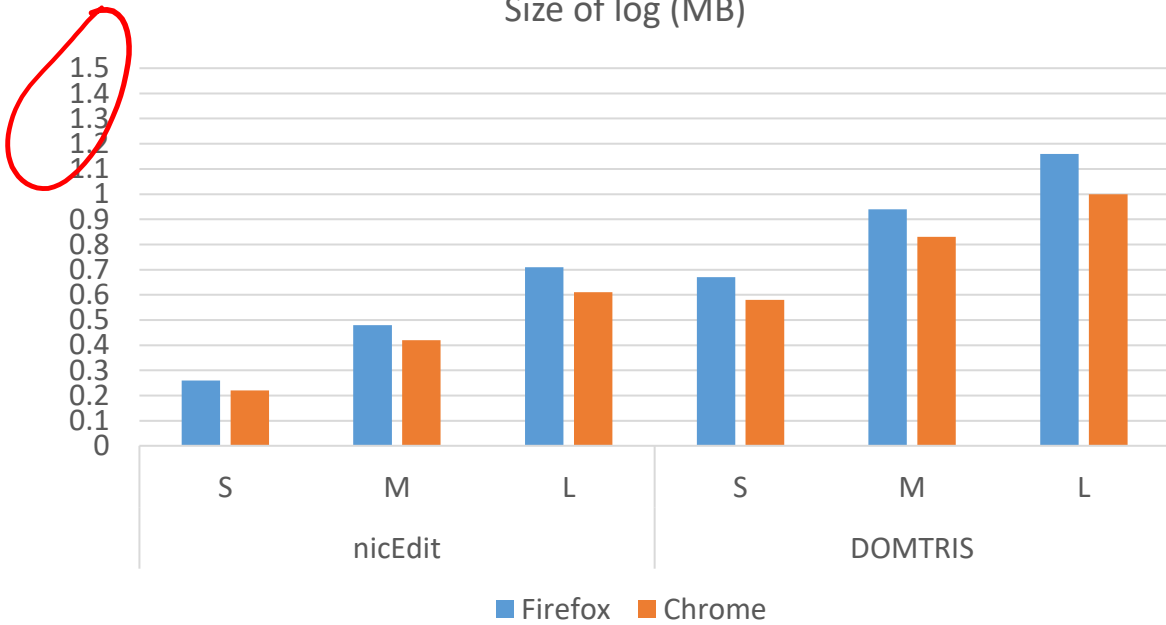
Intercepting Javascript Events



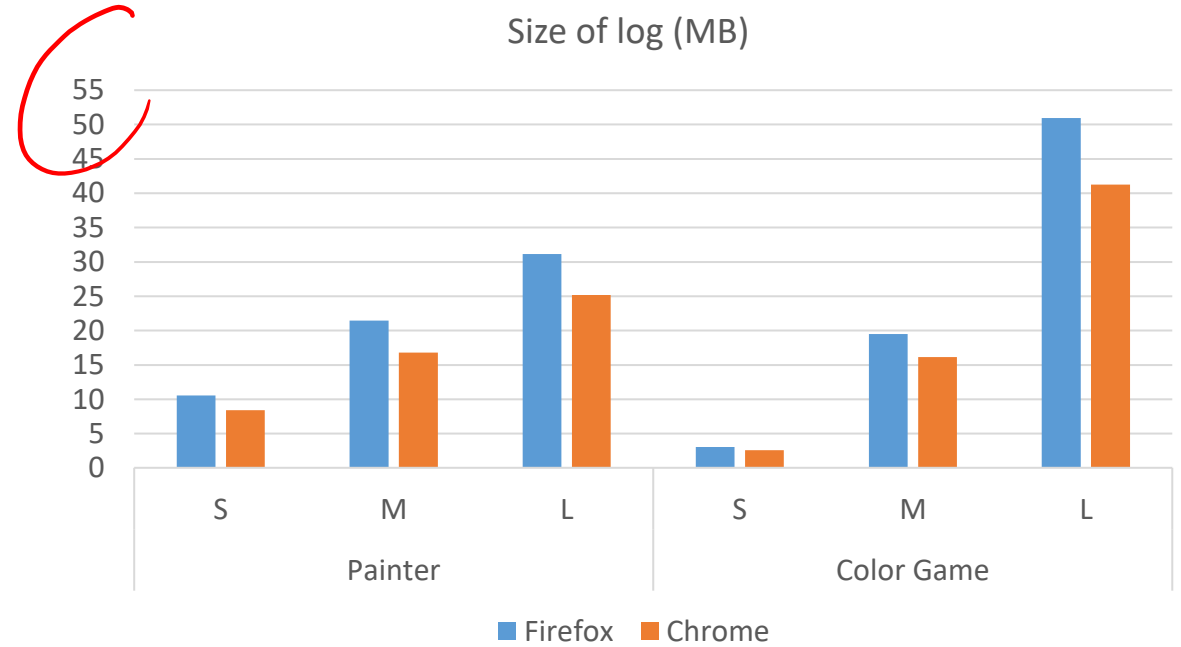
Low overhead (max +1.896ms per handler)

Intercepting Javascript Events

Size of log (MB)

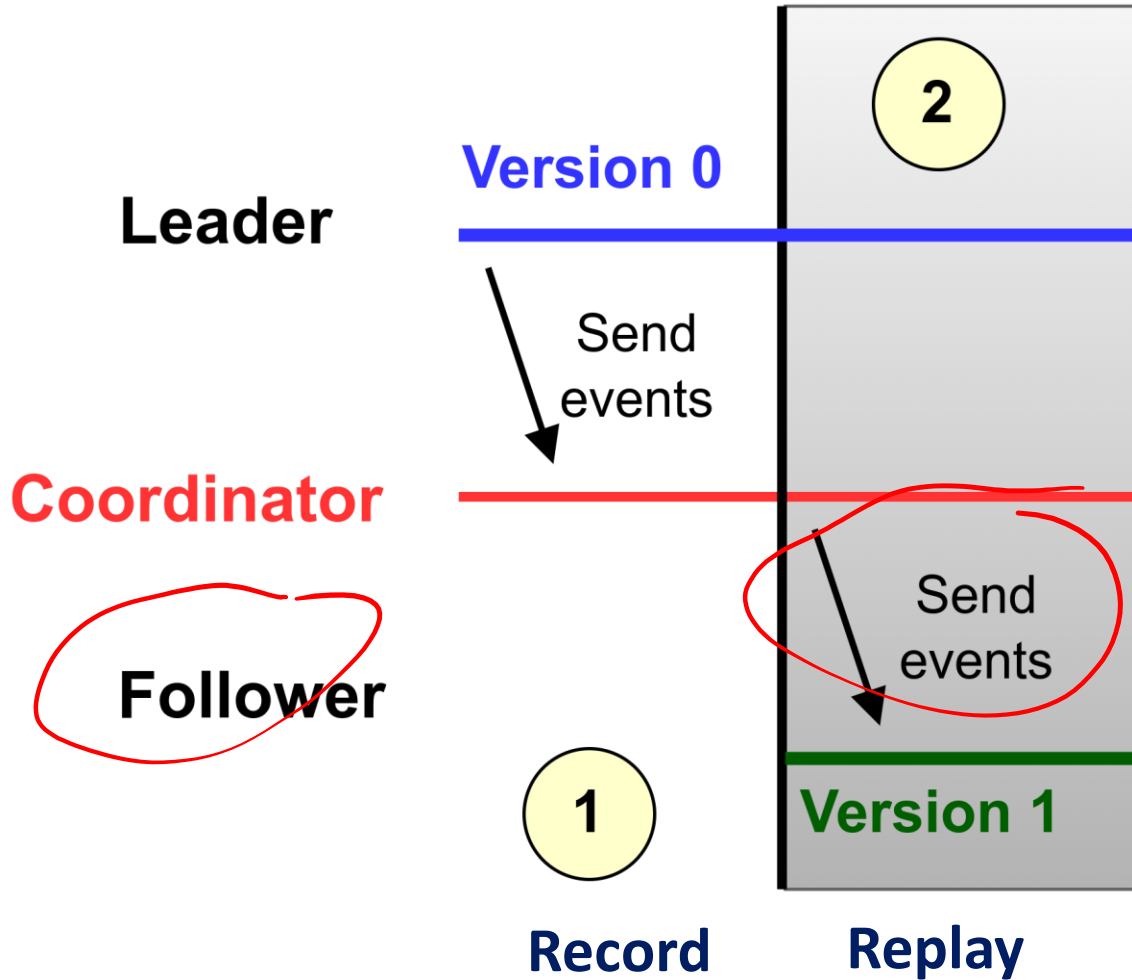


Size of log (MB)

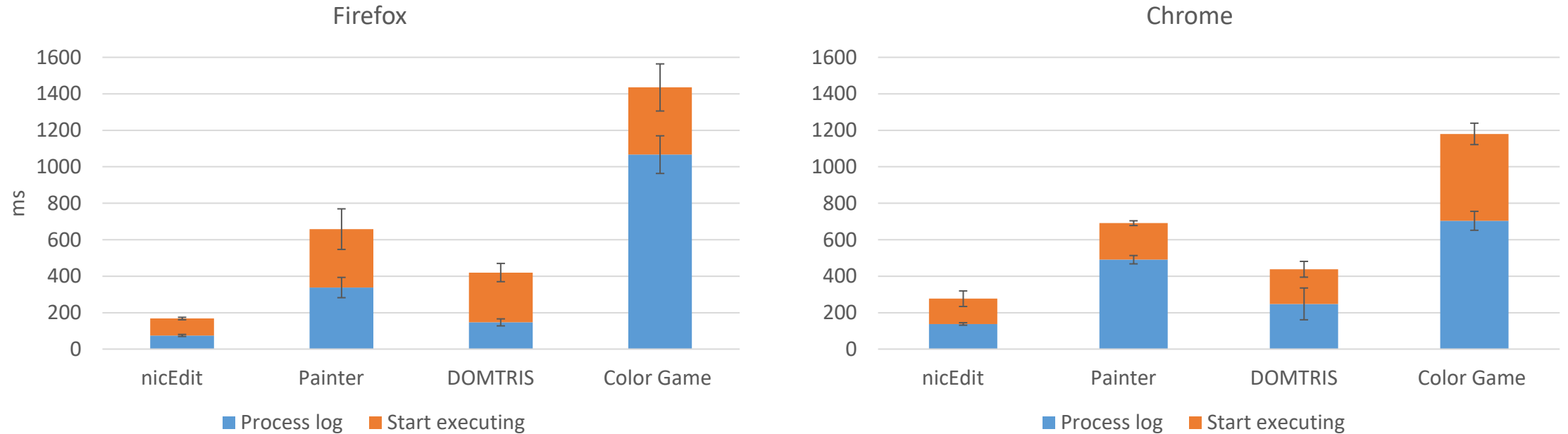


Not a lot of storage needed (max 50MB for long interaction)

SINATRA phases

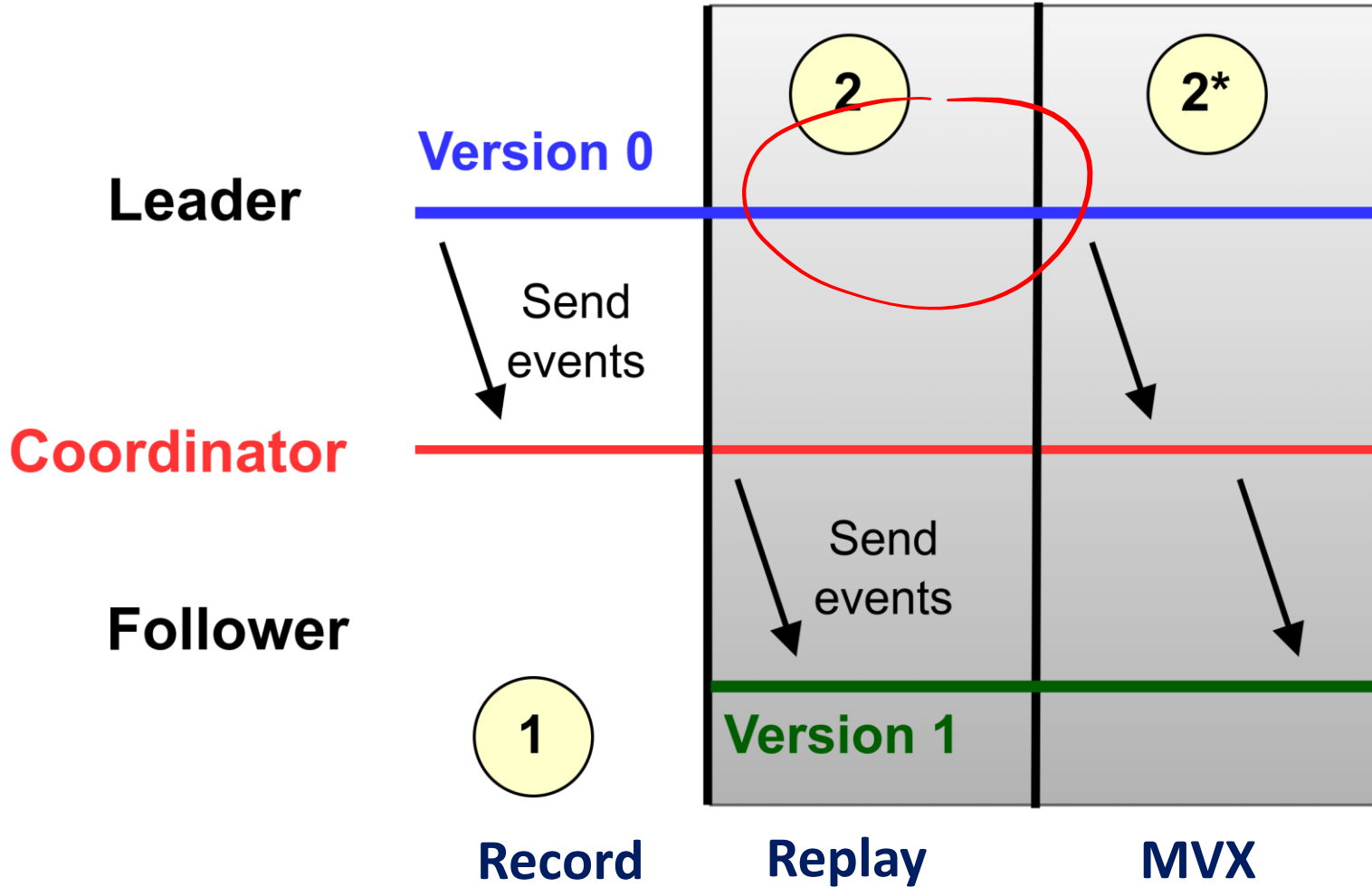


Replaying Javascript Events

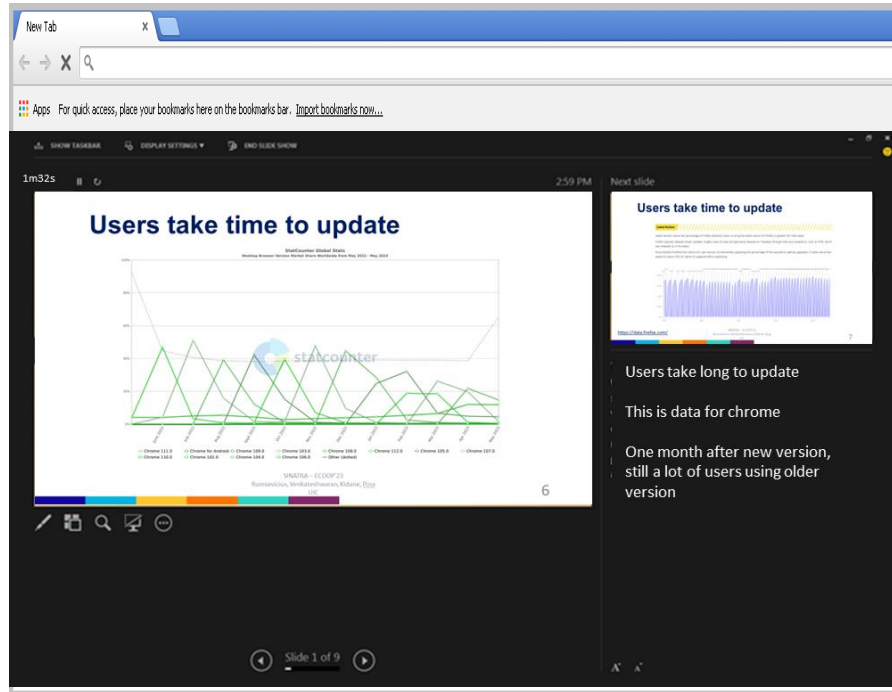


New browser version “catches up” in less than 2sec

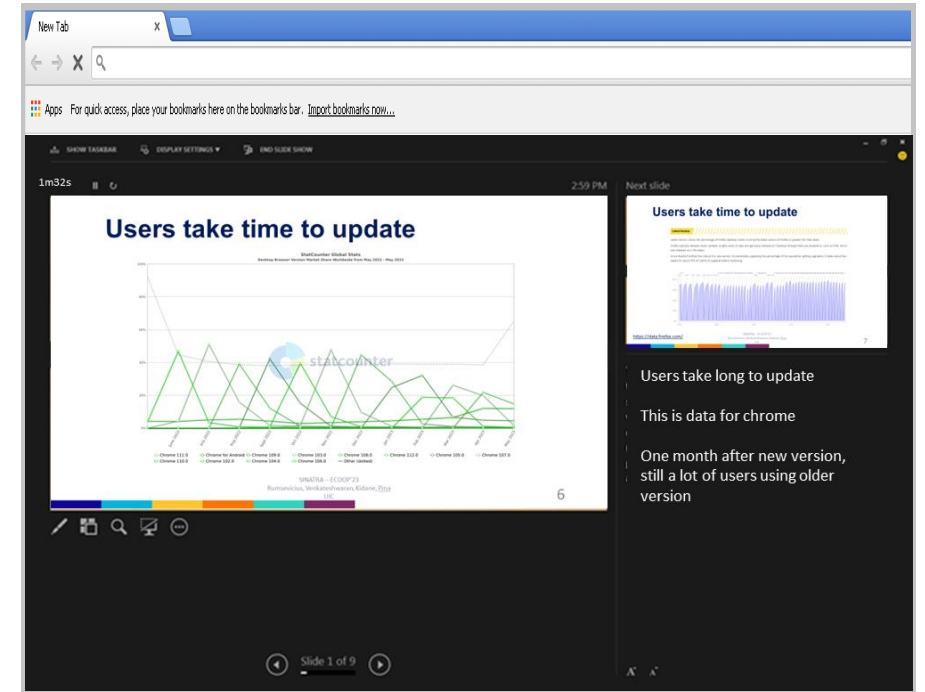
SINATRA phases



SINATRA

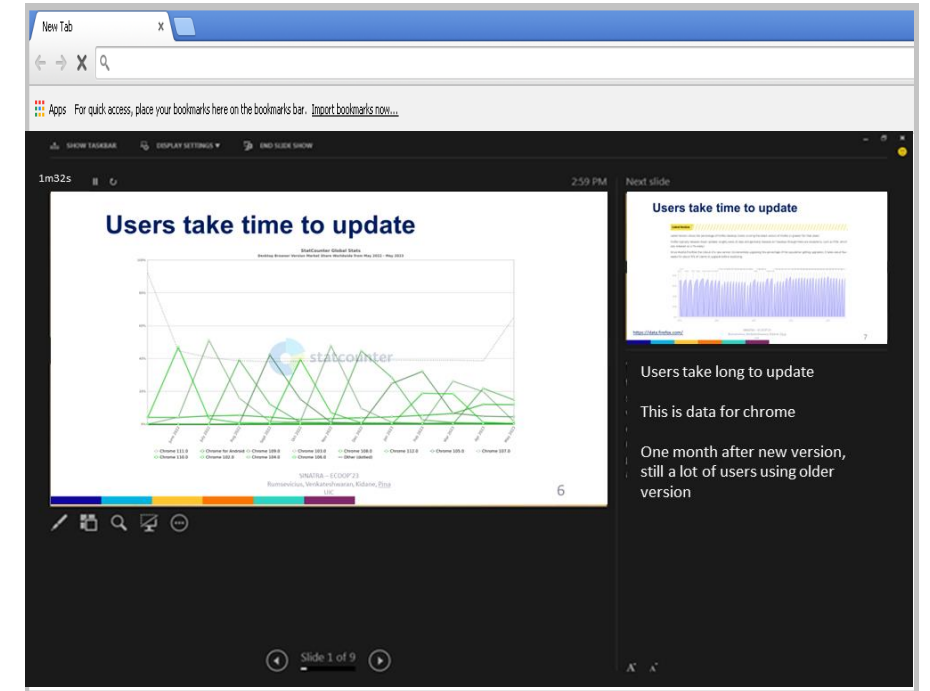
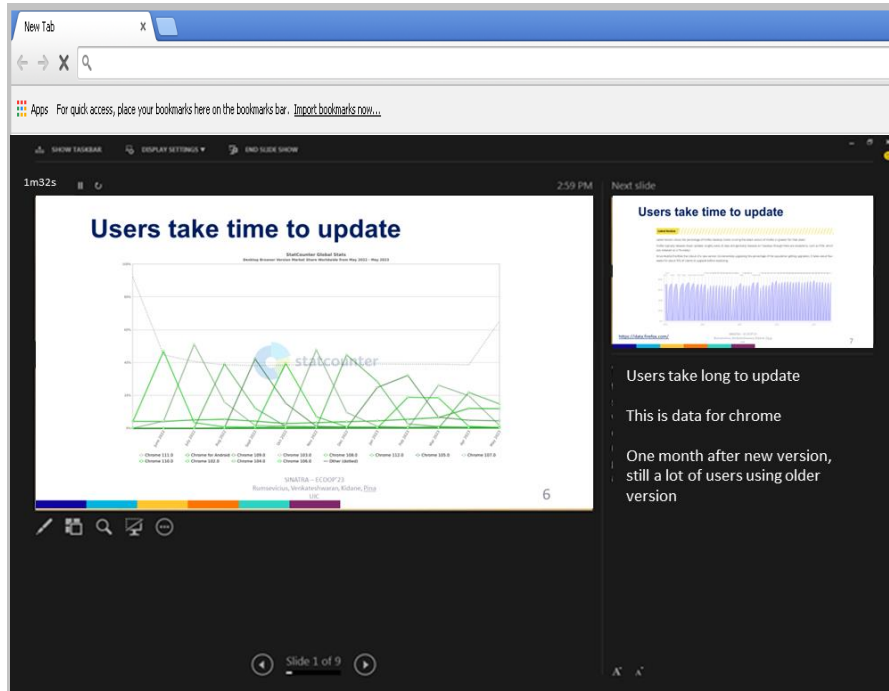


Old browser version



1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser
4. Swap roles

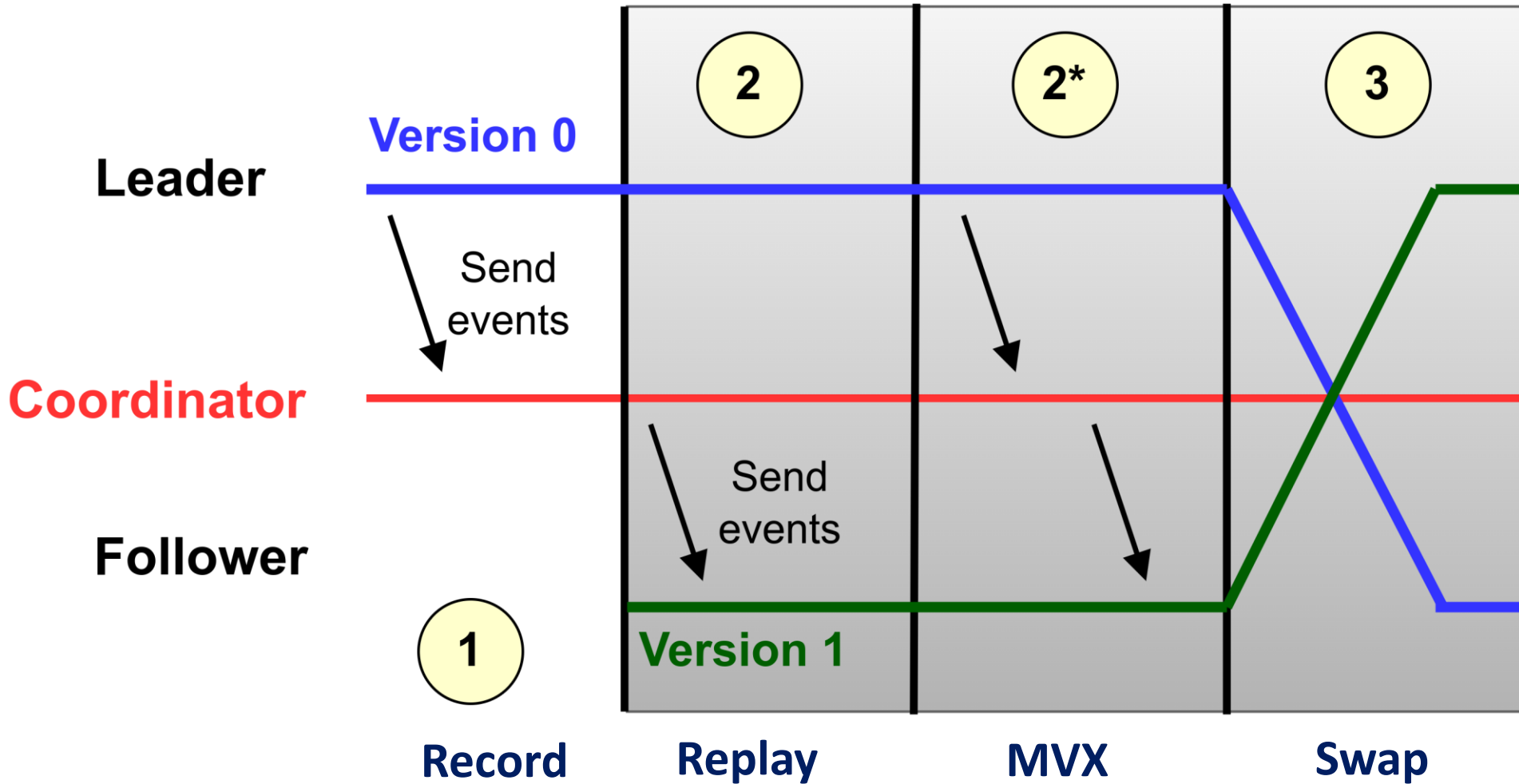
SINATRA



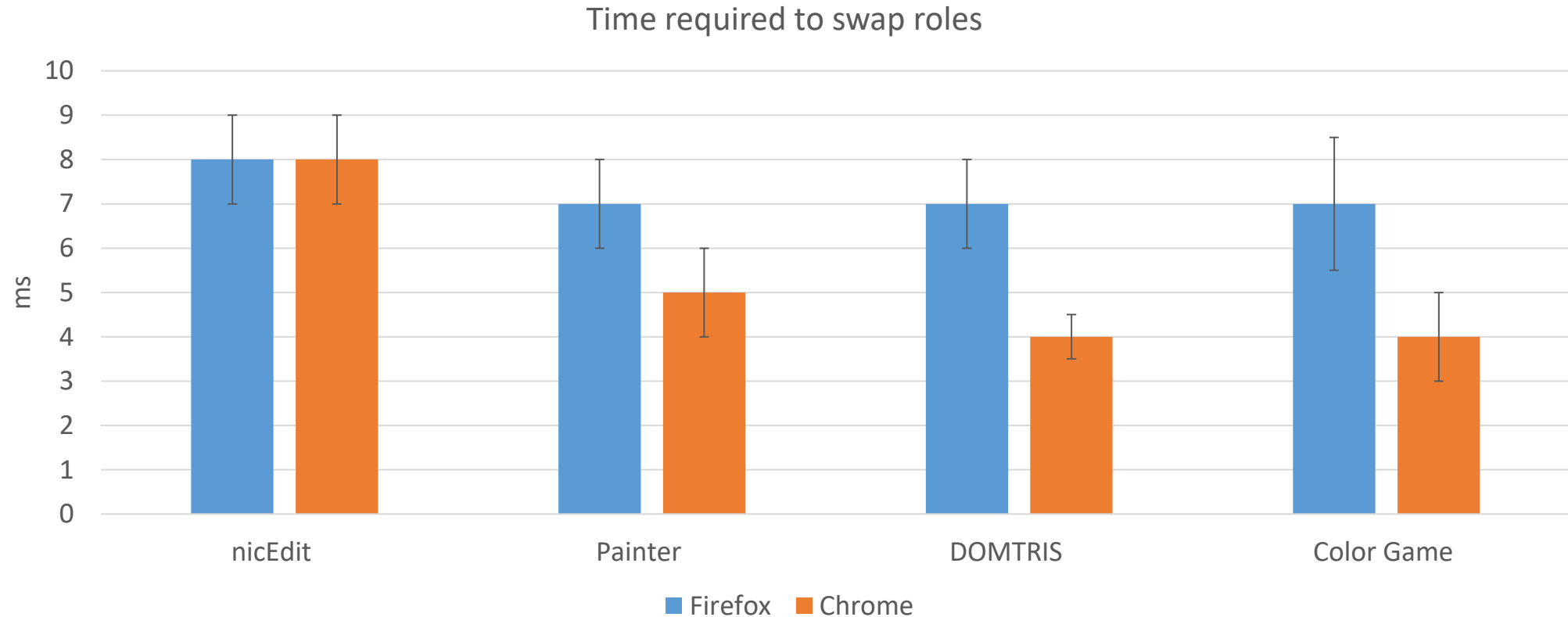
Old browser version

1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser
4. Swap roles

SINATRA phases

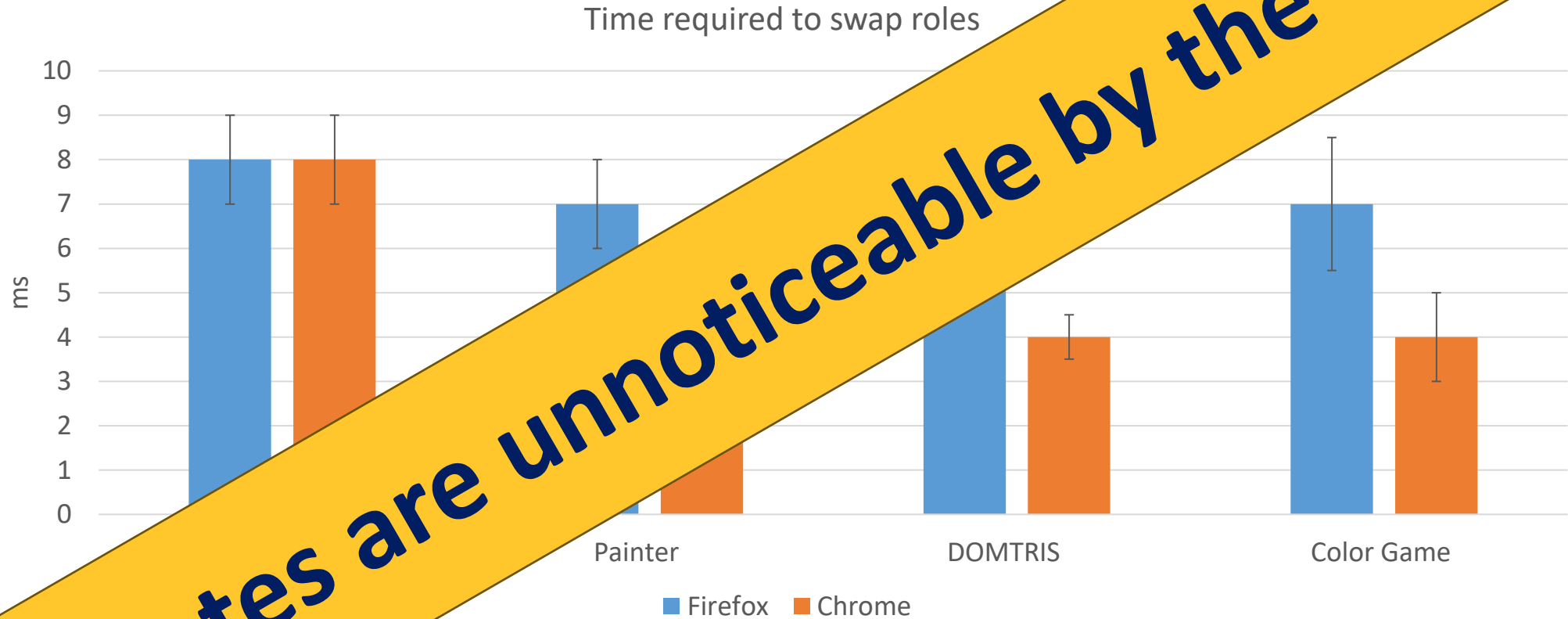


Pause introduced by SINATRA update



Users experience less than 10ms pause due to update

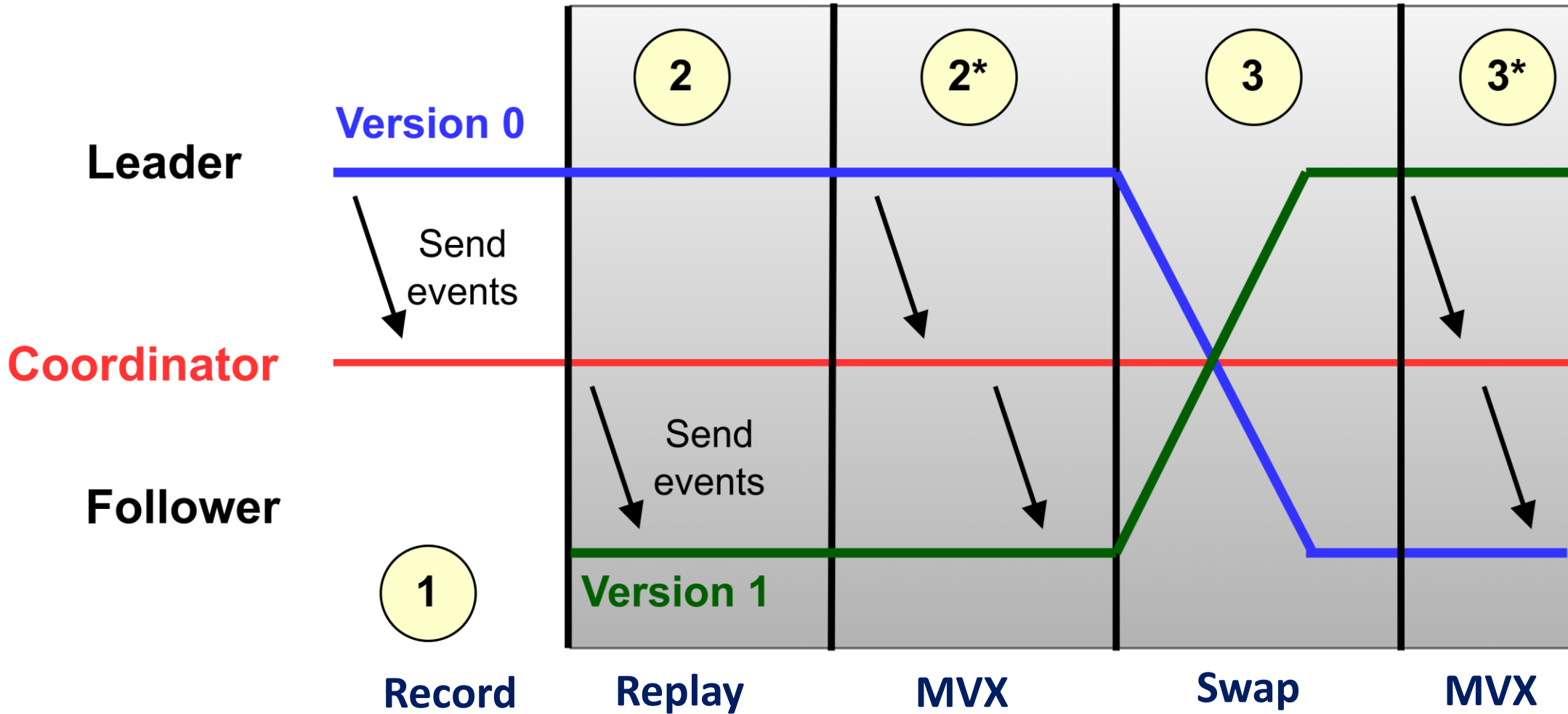
Pause introduced by SINATRA updates



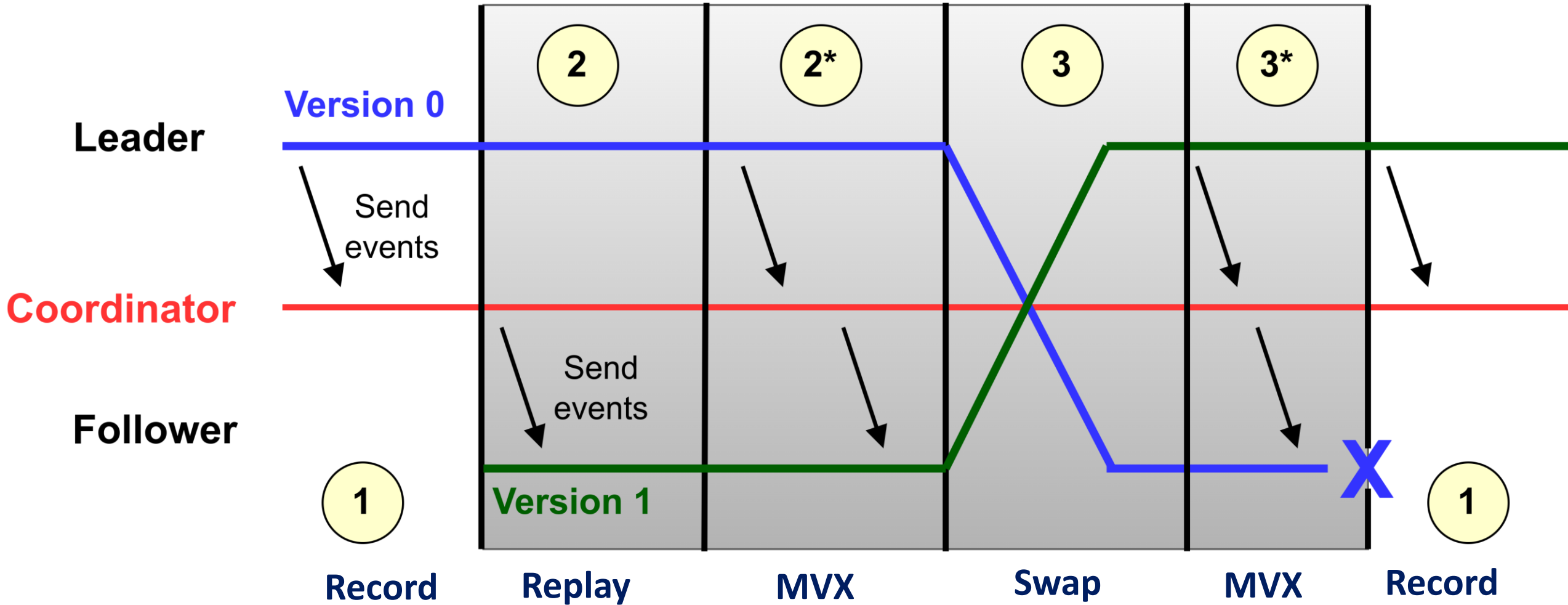
Updates are unnoticeable by the user

Users experience less than 10ms pause due to update

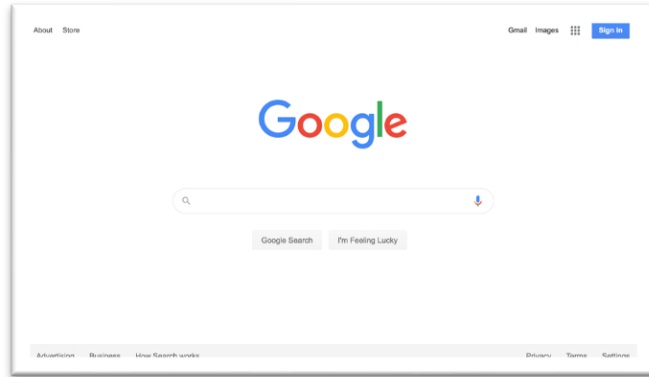
SINATRA phases



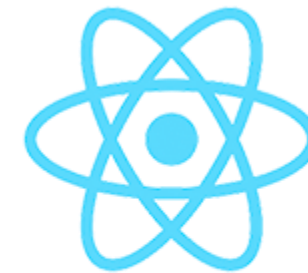
SINATRA phases



Realistic pages



JS Action



React

Realistic pages

- Captured 14h of traffic for high-volume twitter account
 - <https://twitter.com/TotalTrafficCHI>
 - Log sizes under 36MB



SINATRA is available!



zenodo



Conclusion



github.com/bitslab/sinatra

Fork me on Github

No good option

Don't update browser, get PWNED

Update browser, lose state, crash, etc.

BROWSER UPDATE

BROWSER UPDATE

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

13

SINATRA

Old browser version

1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

23

Intercepting Javascript Events

Fully implemented in Javascript

Browser agnostic

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

34

Pause introduced by SINATRA

Time required to swap roles

ms

■ Firefox ■ Chrome

Painter DOMTRIS Color Game

Users experience less than 10ms pause due to update

Updates are unnoticeable by the user

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

45

Realistic pages

ANGULAR

JS Action

React

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

49

Conclusion



github.com/bitslab/sinatra

Fork me on Github

No good option

Update browser, lose state, crash, etc.

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

13

SINATRA

Old browser version

1. Launch new browser version
2. Open same page, get same contents
3. Replay all events from old browser

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

23

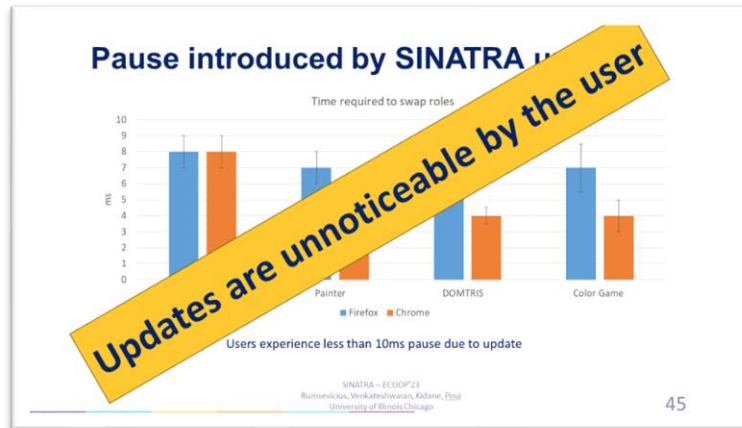
Intercepting Javascript Events

Fully implemented in Javascript

Browser agnostic

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

34



Realistic pages

SINATRA – ECOOP'23
Rumsevicius, Venkateshwaran, Kidane, Pina
University of Illinois Chicago

49

Thank you!
Questions?



CCF-2227183