



Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots

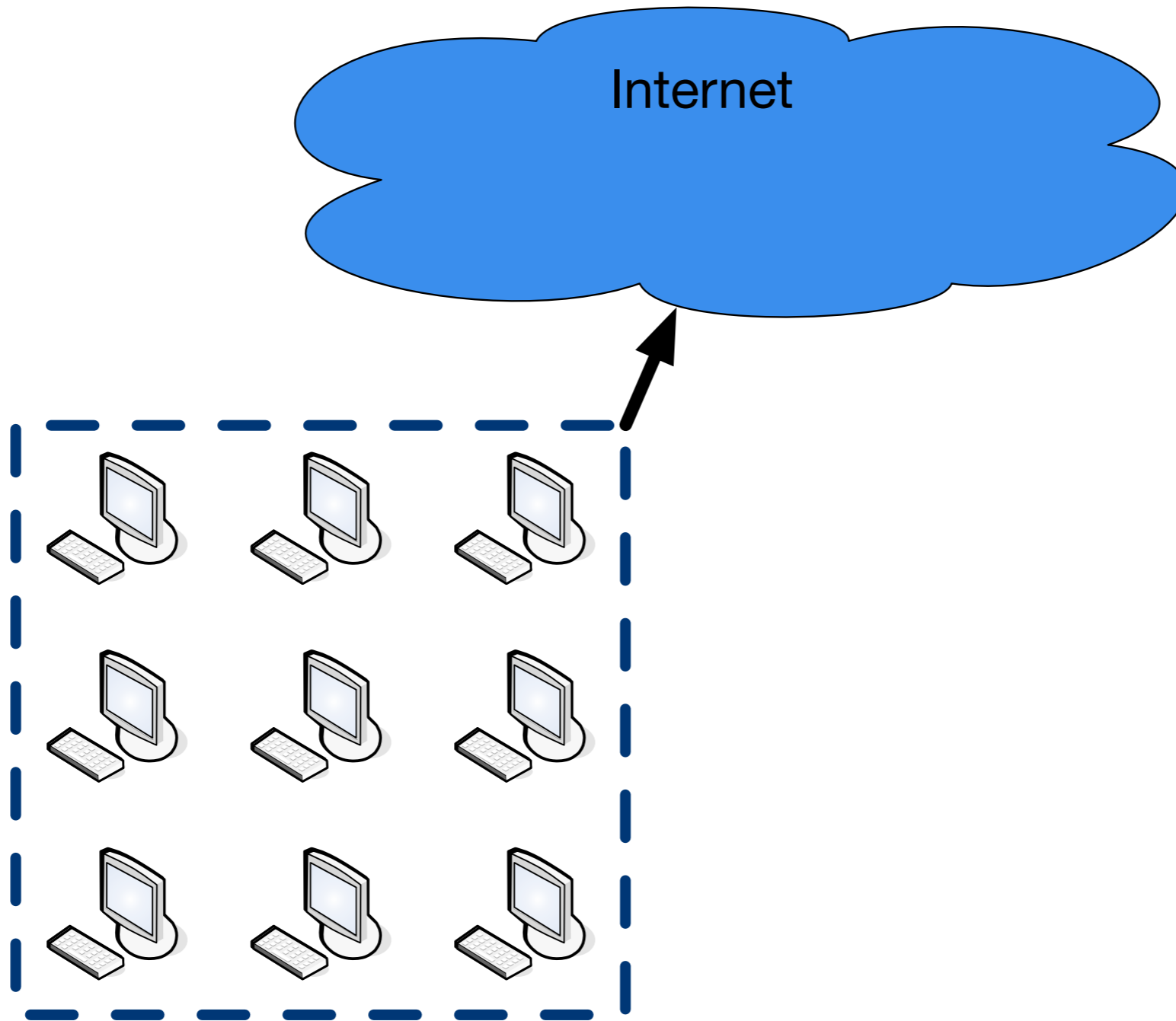
Phani Vadrevu*, Jienan Liu*, Bo Li*, Babak Rahbarinia⁺,
Kyu Hung Lee* and Roberto Perdisci*

* University of Georgia, Athens, USA

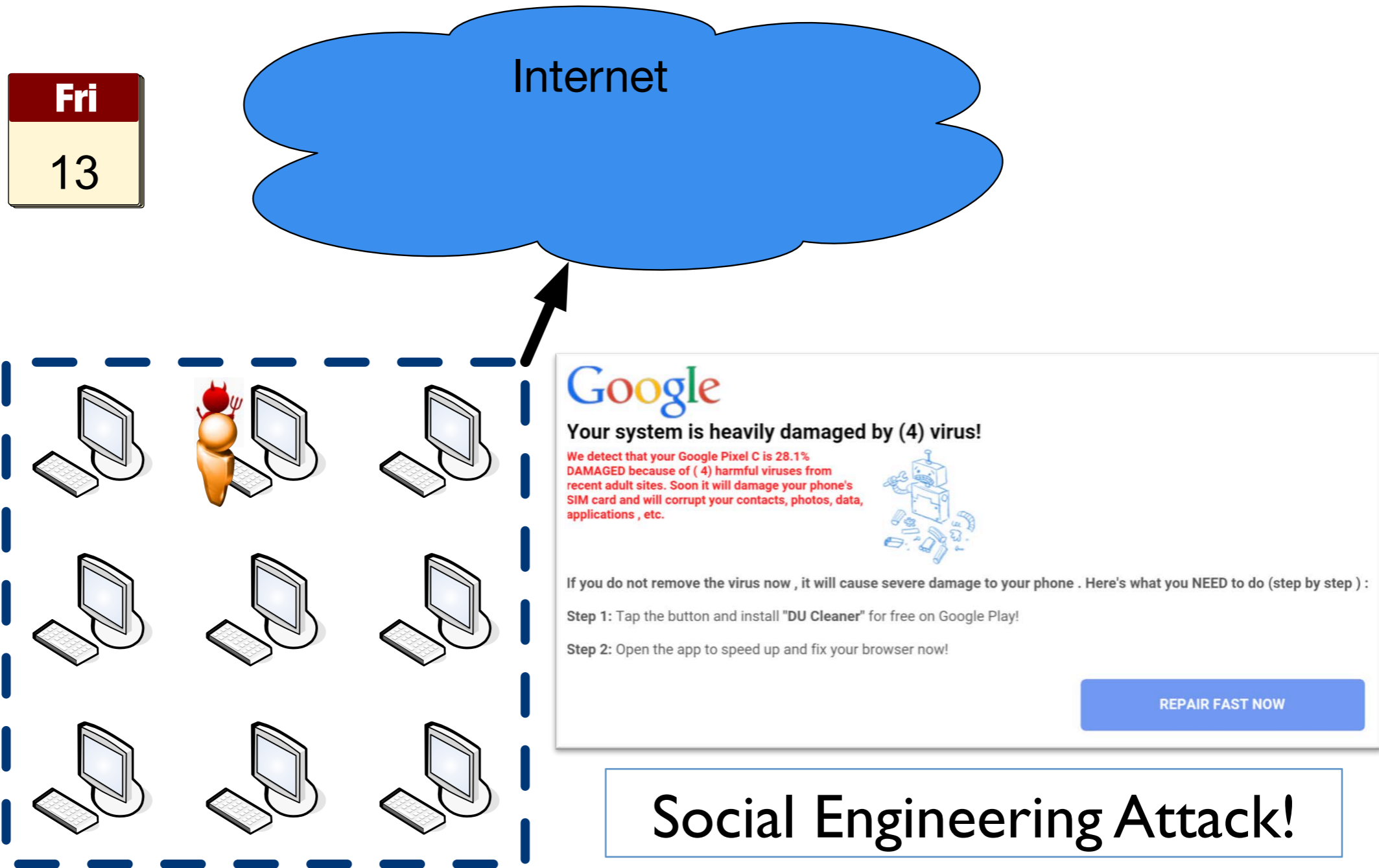
⁺ Auburn University in Montgomery, Alabama, USA



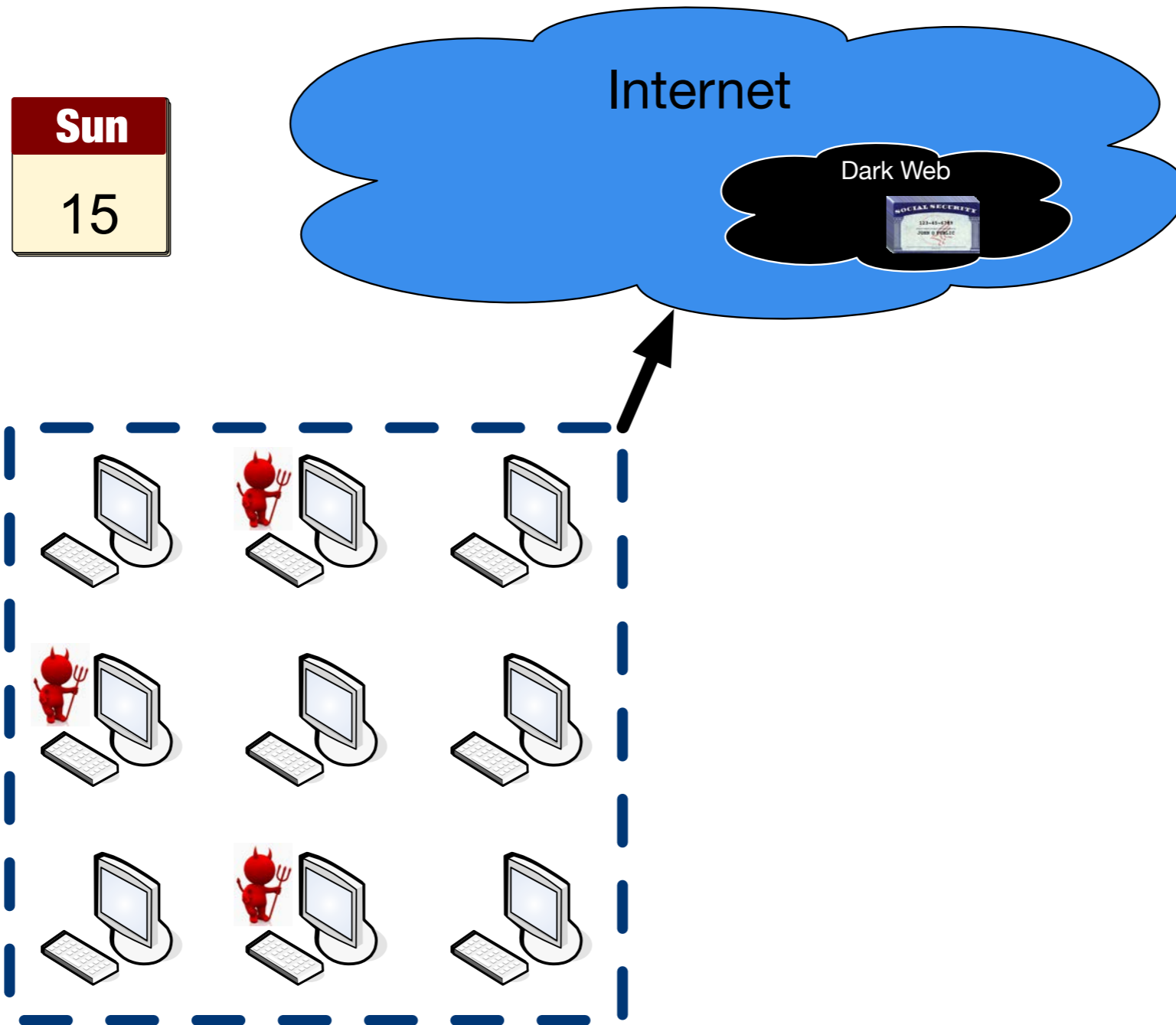
Case Study



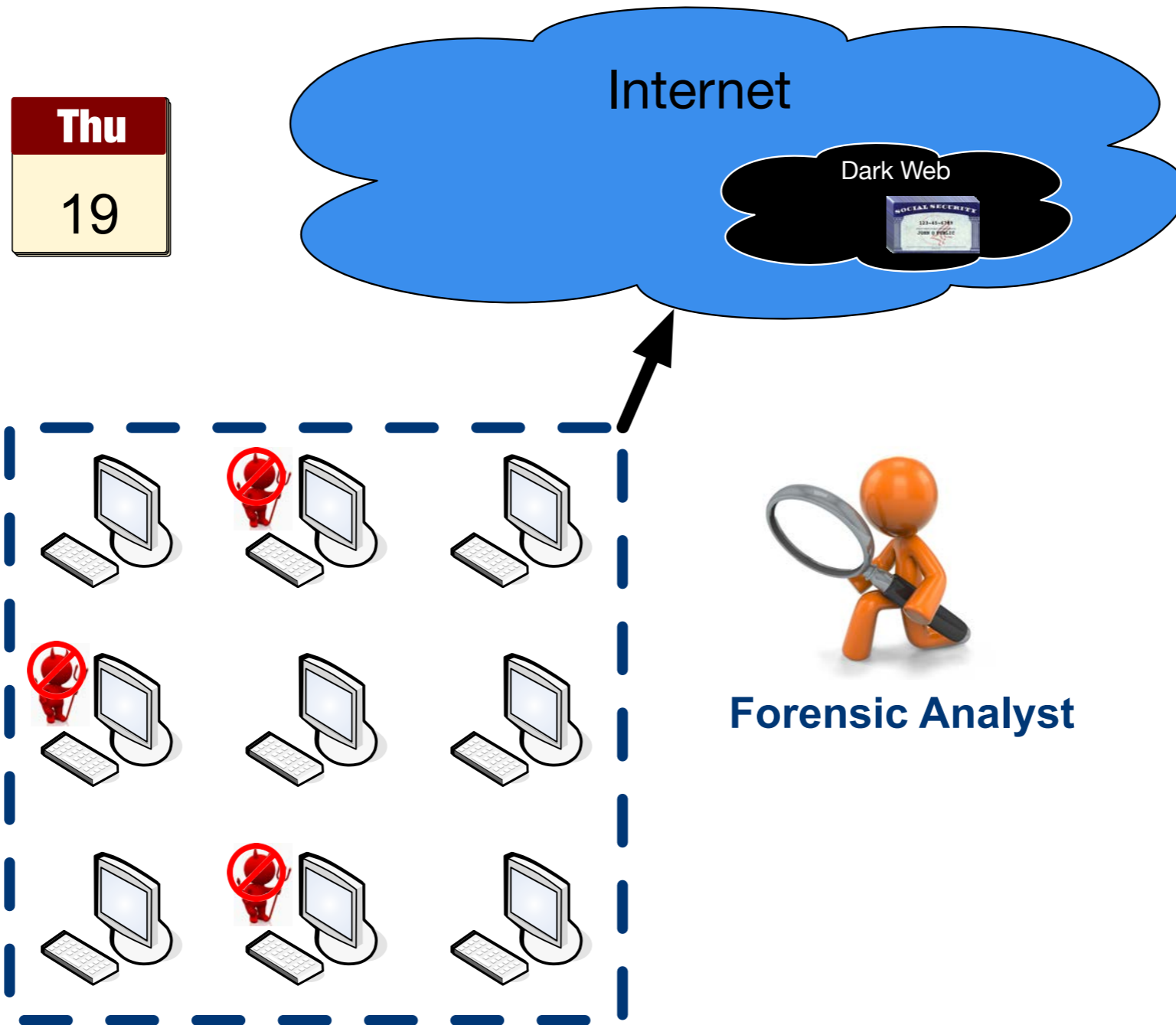
Case Study



Case Study

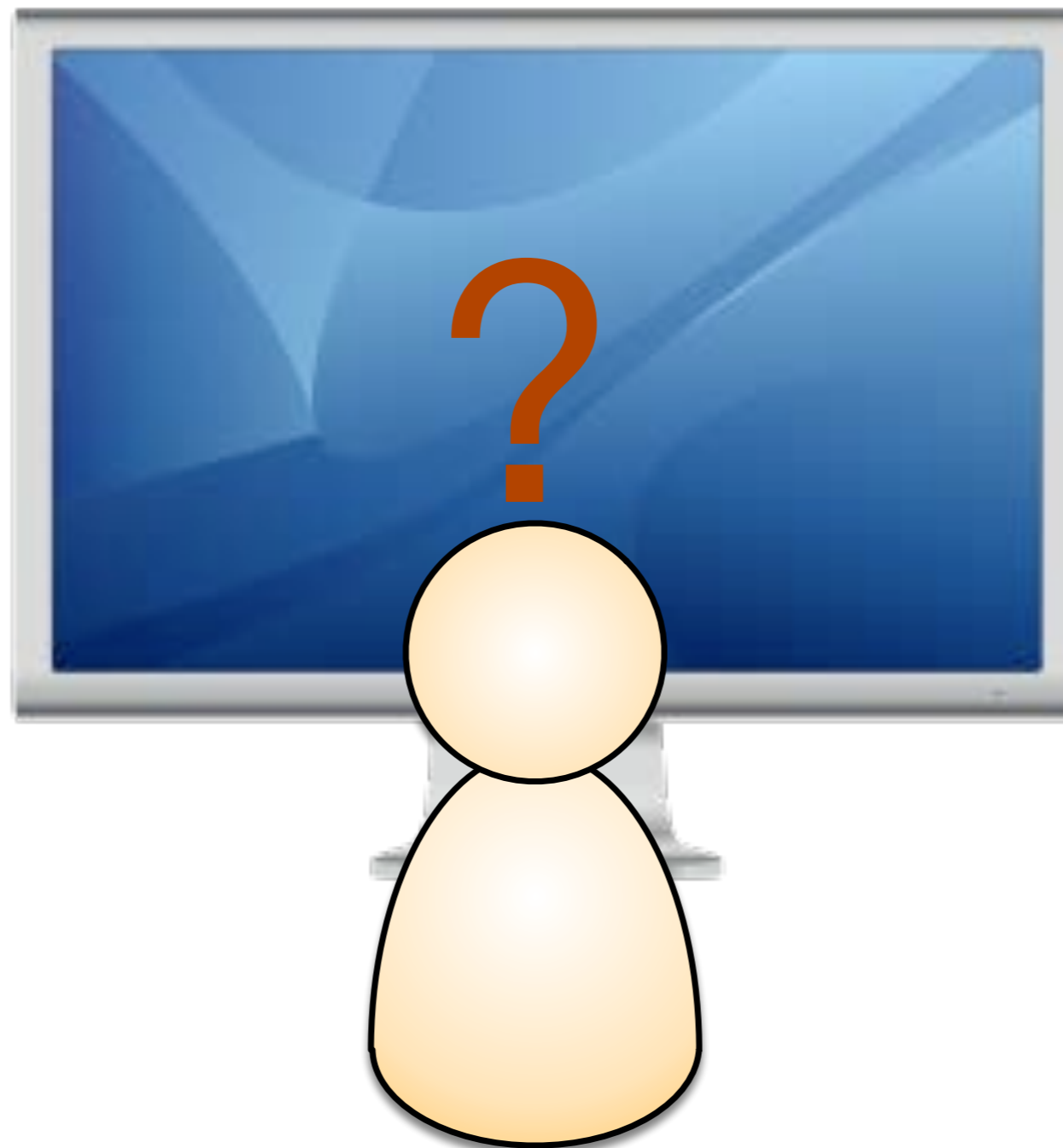


Case Study





We need ...



Helps in user training to improve awareness





Requirements

A tool that can record and reconstruct user-browser interactions and browser state.

1. Forensic Rigor

- Browser state should be fully captured **synchronously** i.e. before input is processed by the browser

2. Efficiency (always-on)

- HCI research states that a lag < **150 ms** is practically unnoticeable to end users^[1]

3. Transparency

- Should not be easily detected by adversaries

4. Portability

- Should work on all platforms (mobile)





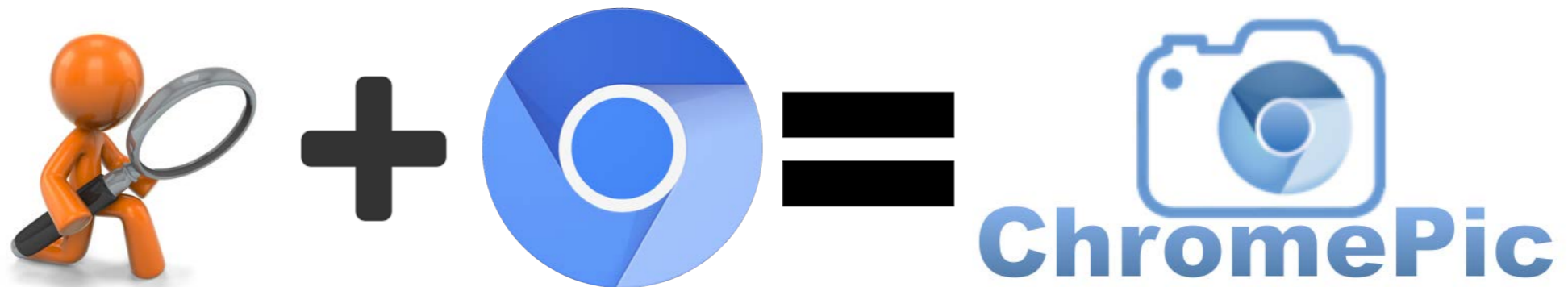
Related Work

- Network:
 - WebWitness (USENIX SEC 2014): DPI to reconstruct path to attack pages; **visual reconstruction not possible**
- Browser based record-and-replay:
 - WebCapsule (CCS 2015): Instrument Blink to record and replay all browser actions; **not fully deterministic and is complex**
- Whole system record-and-replay:
 - ReVirt (OSDI 2002): Record and guest OS's execution at an instruction level; **heavy-weight and difficult to deploy on mobile devices**



ChromePic

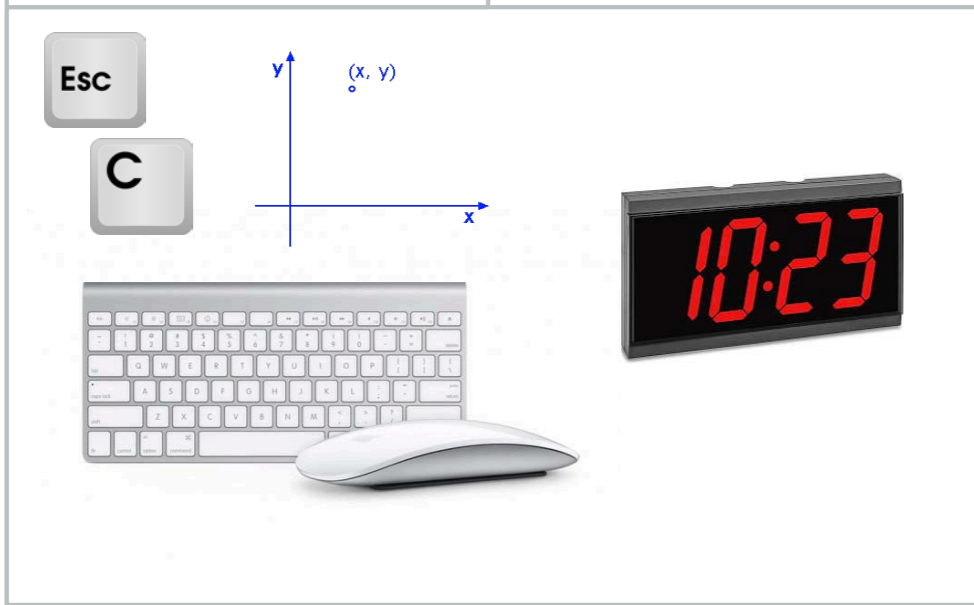
- An *always-on, lightweight, efficient and portable* forensic engine embedded inside the Chromium browser



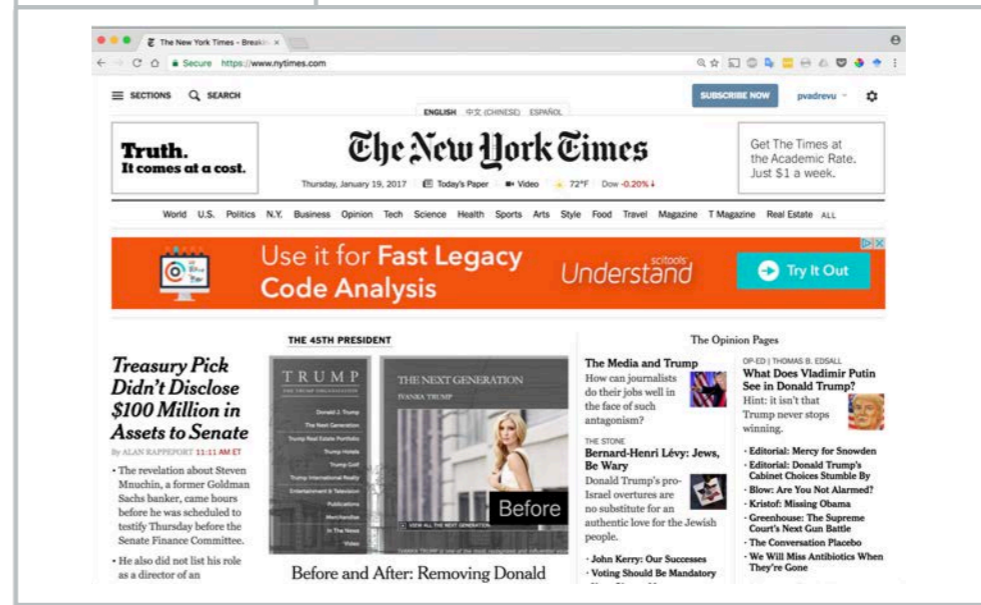
- It *synchronously* records user-browser interactions and the browser state into rich forensic logs called ***webshots***

Webshot

User Input, Timestamp



Screenshot



DOM Snapshots (for all frames)







Trigger Events



Trigger Events

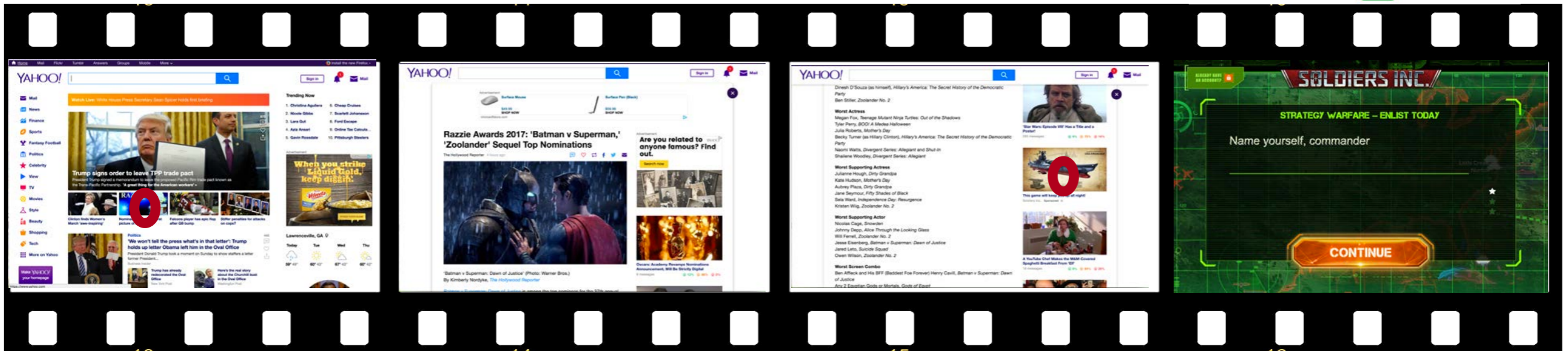
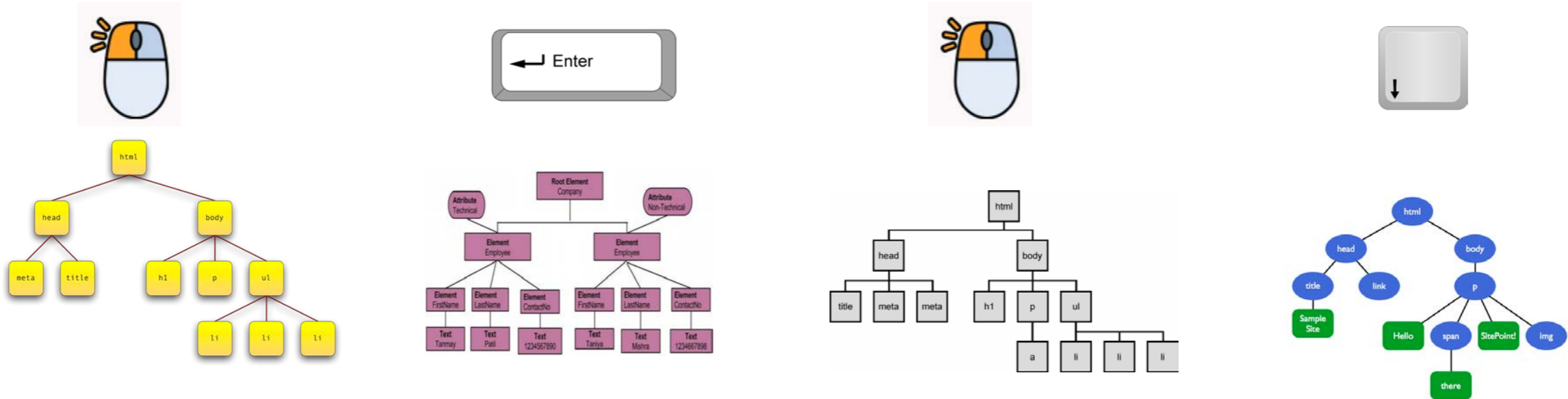


Mouse: left click, right click

Touch device: tap

Keyboard: return, space, tab, esc, back space, arrows

ChromePic in Action

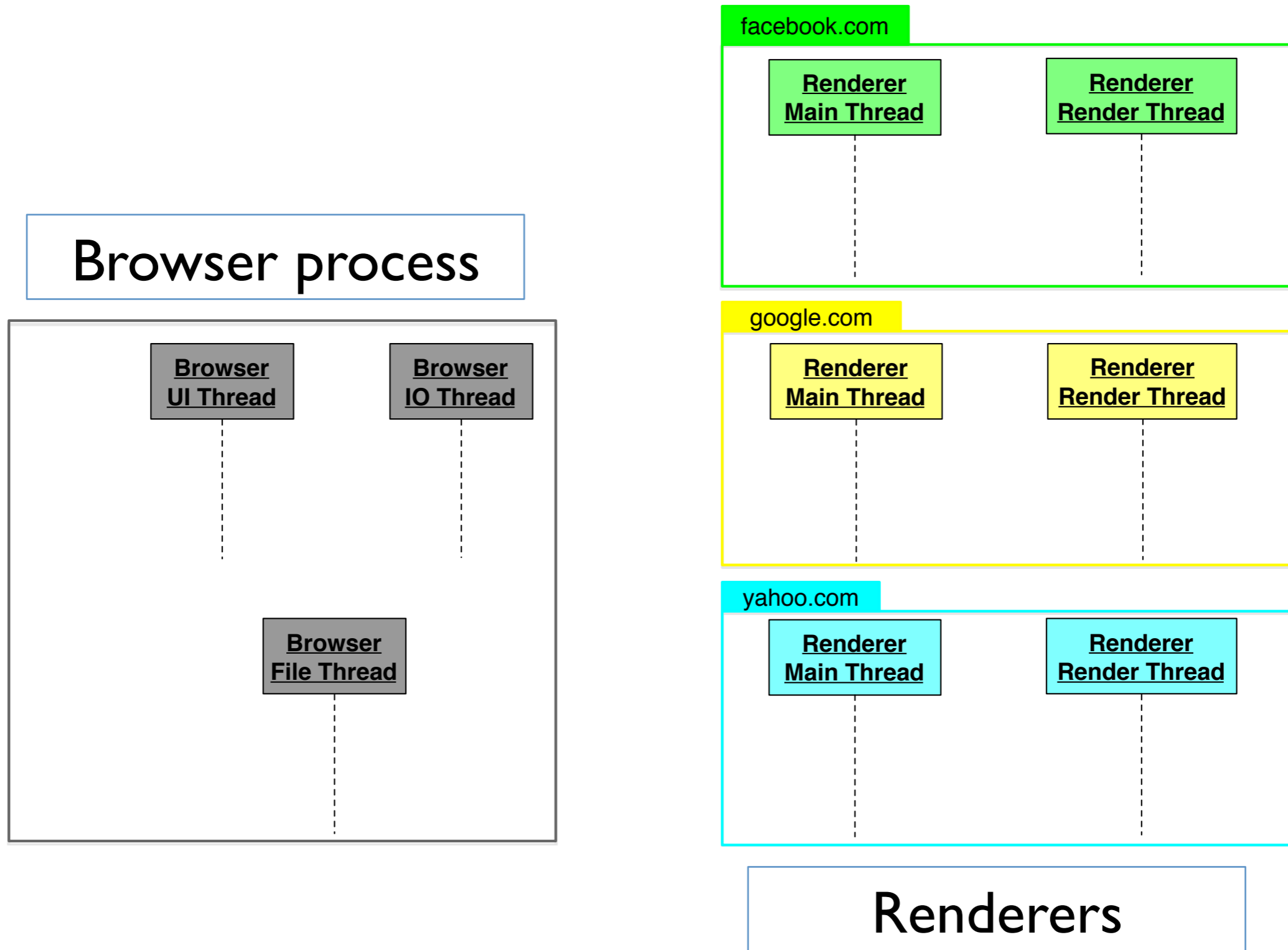


Building ChromePic

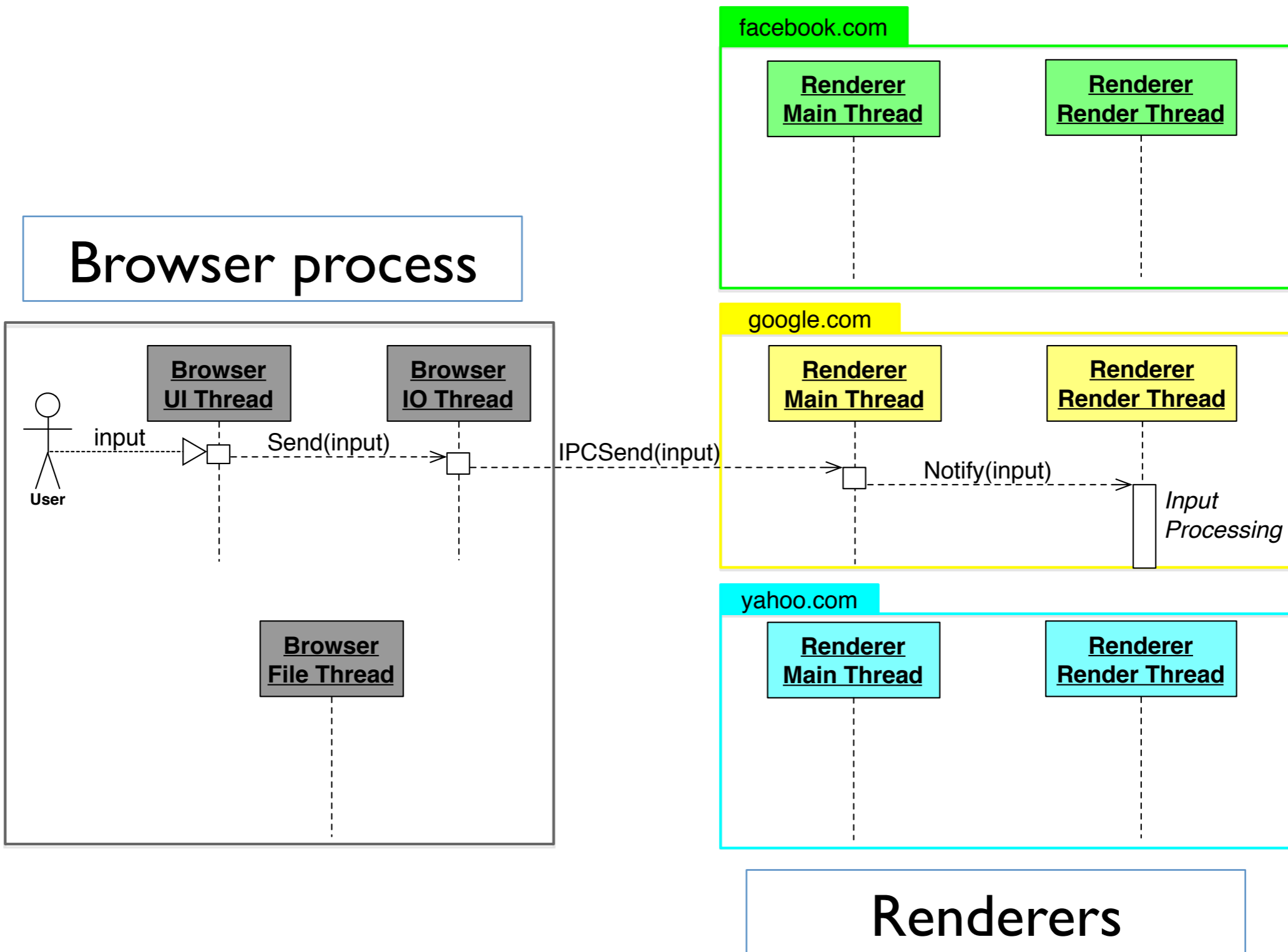
Extensions not viable 

Browser Instrumentation 

Chromium Architecture



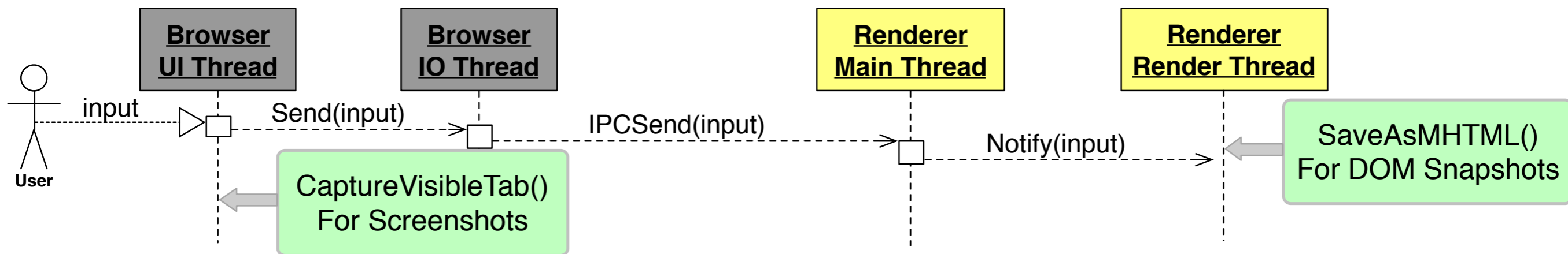
Chromium Architecture



Browser Instrumentation

Use as much underlying code as possible:

- `CaptureVisibleTab()` : asynchronous screenshots
- `SaveAsMHTML()` : asynchronous DOM snapshots

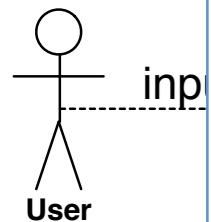


Browser Instrumentation

Use as much underlying code as possible:

- `CaptureVisibleTab()` : asynchronous screenshots
- `SaveAsMHTML()` : asynchronous DOM snapshots

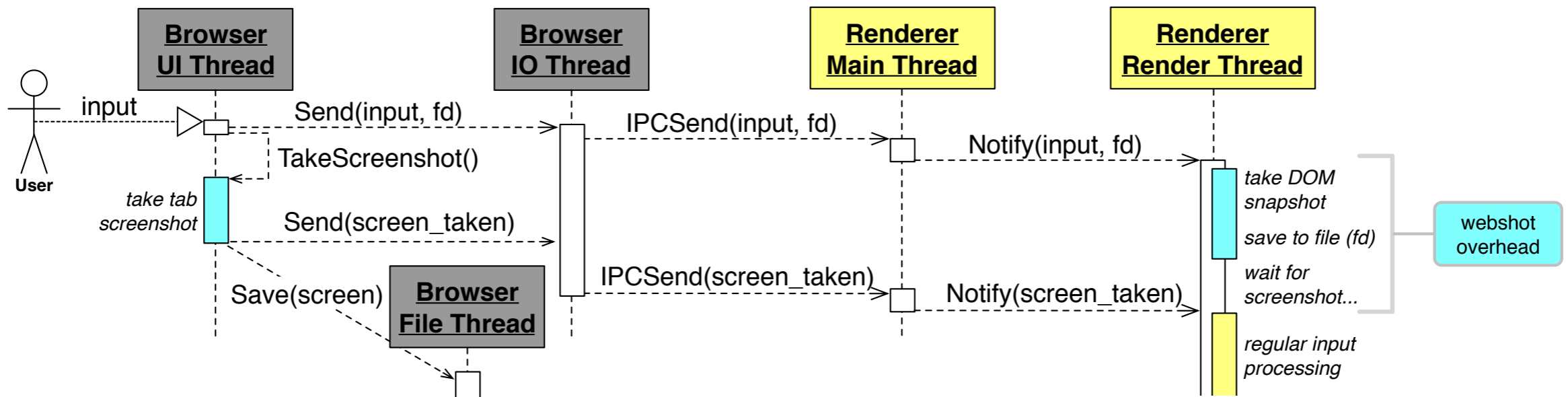
both are **asynchronous**
need synchronous and efficient
versions



MHTML() snapshots

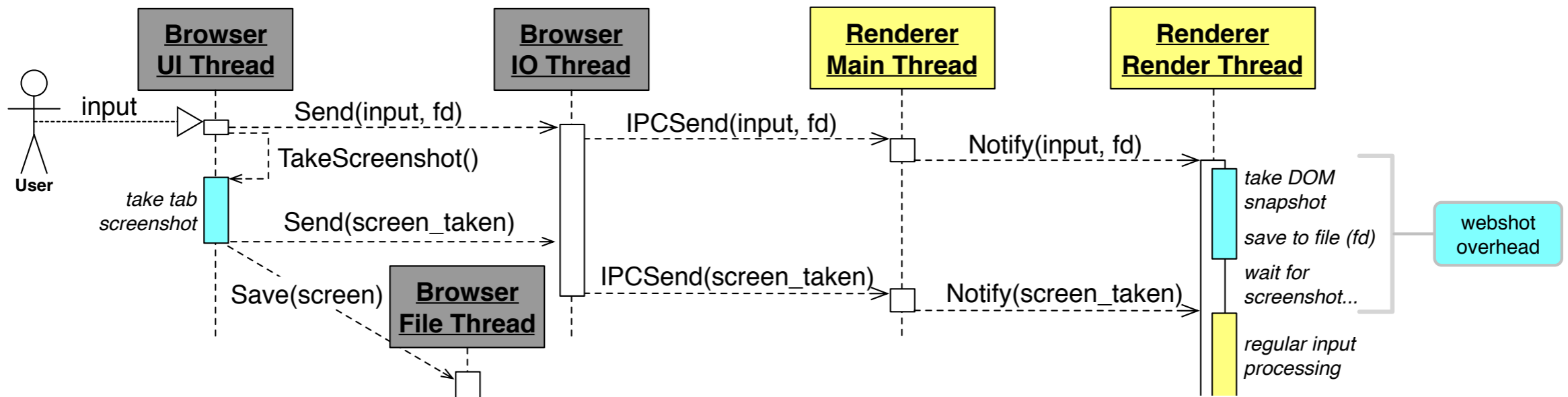
ChromePic Design

ChromePic Trigger Input Processing



ChromePic Design

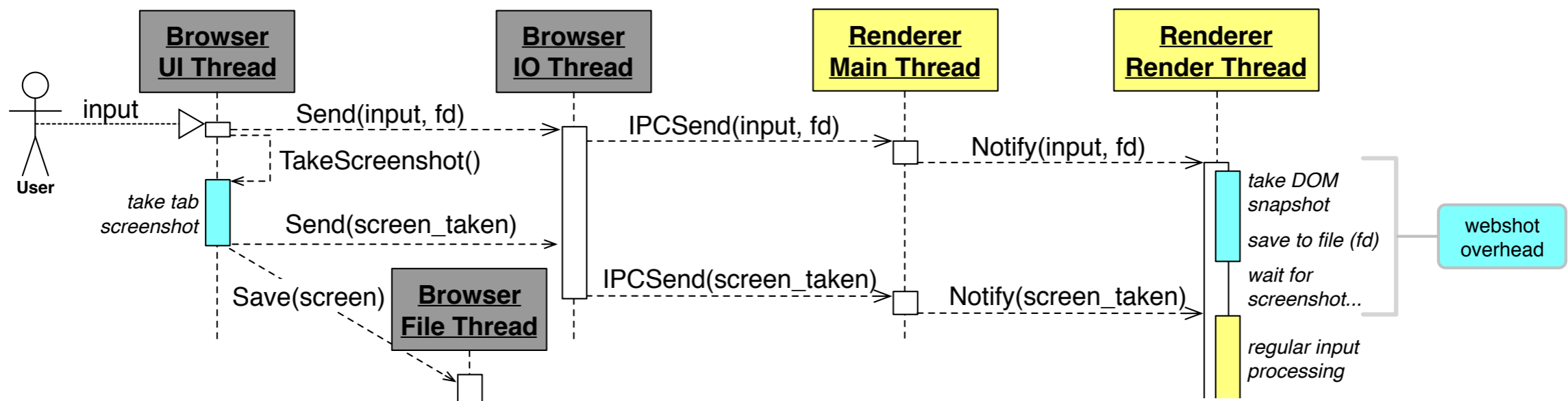
ChromePic Trigger Input Processing



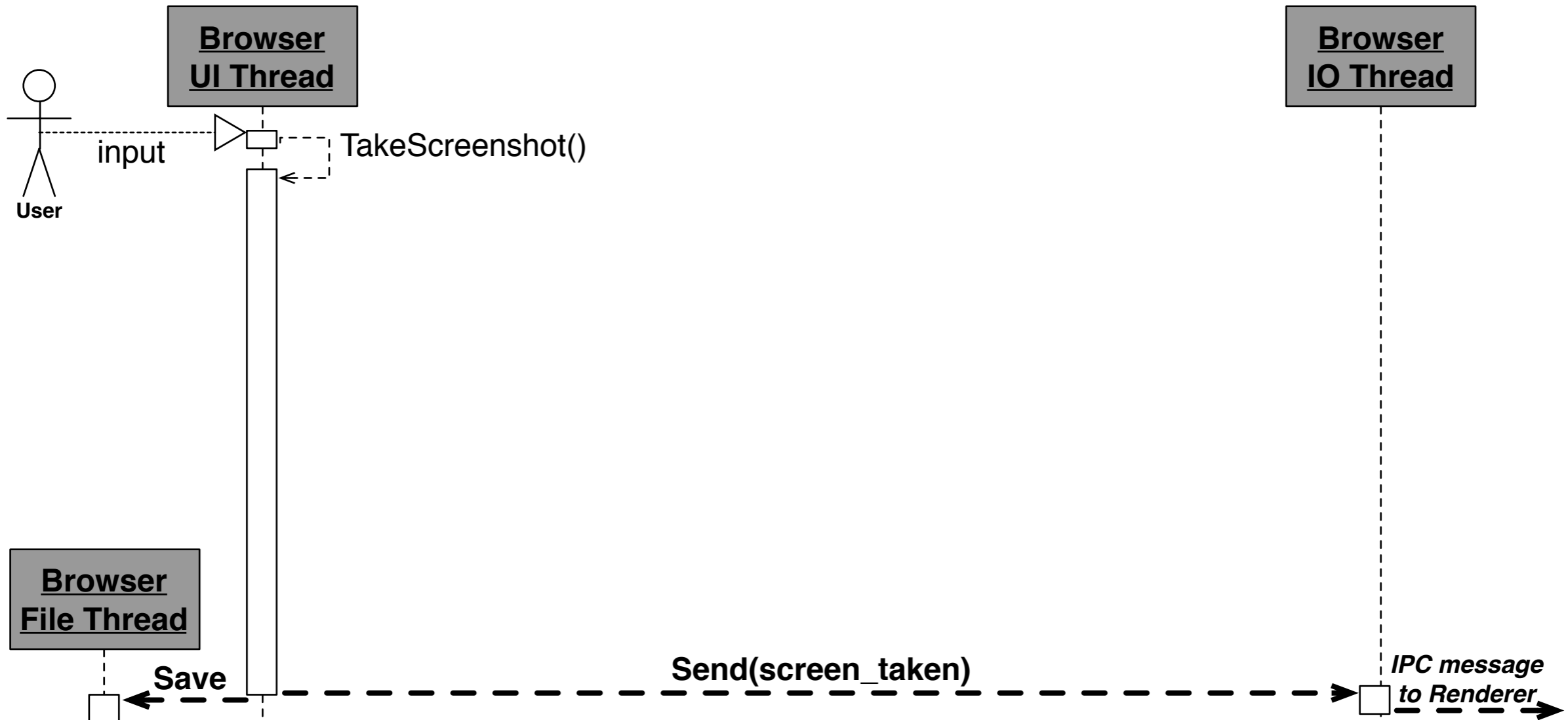
Synchronous by design

ChromePic Design

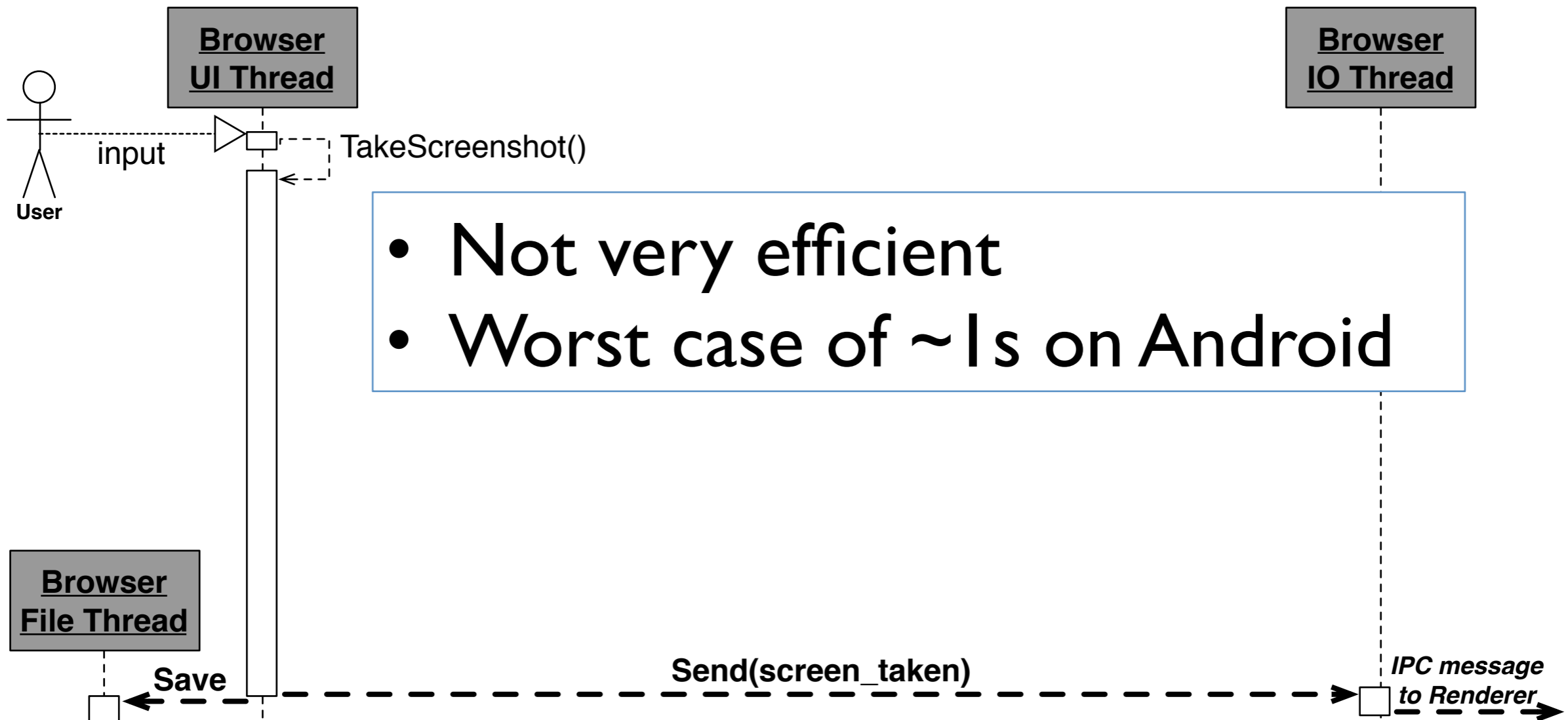
- Next efficiency needs to be ensured for both:
 - Screenshots
 - DOM Snapshots



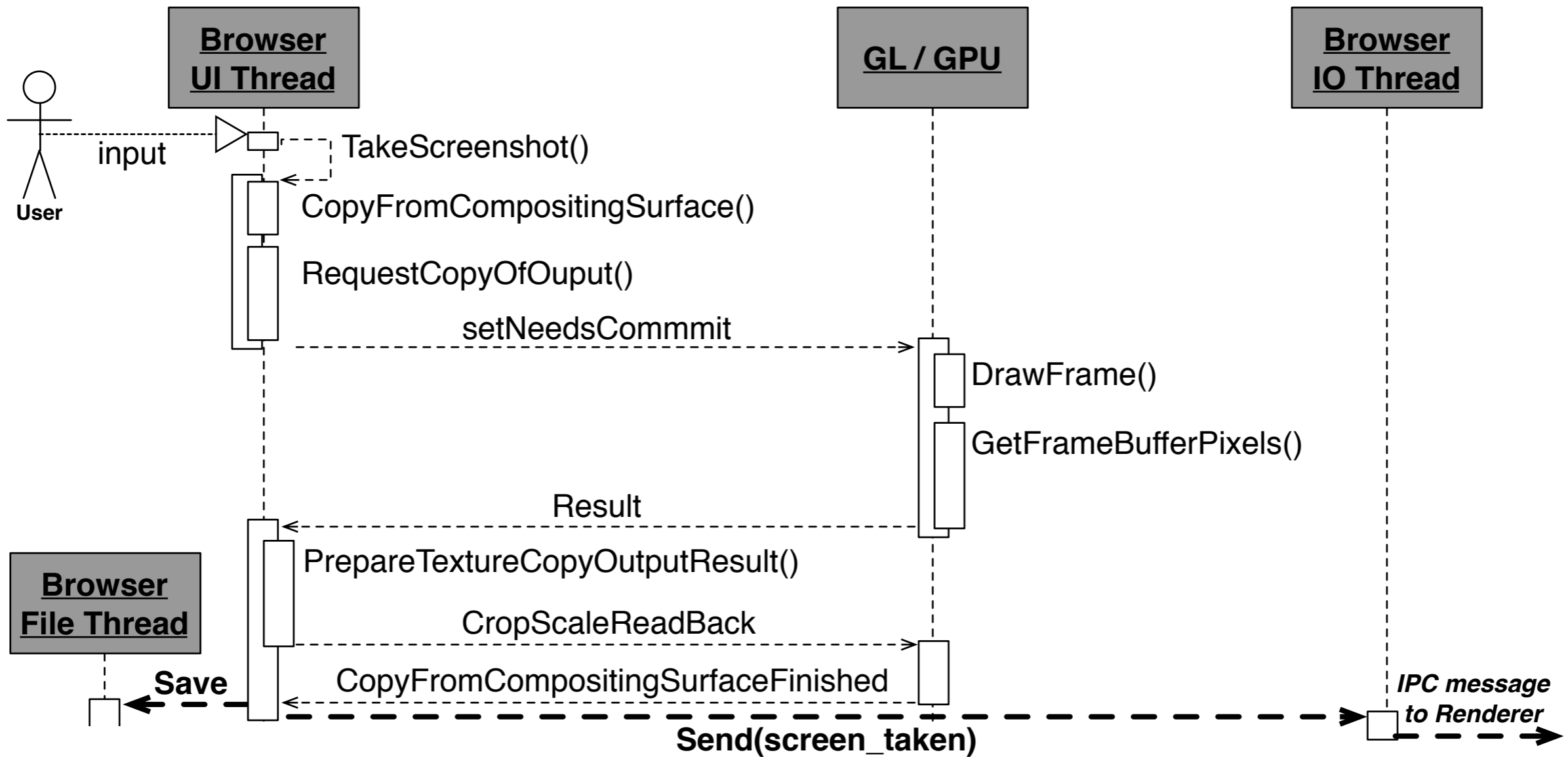
Taking screenshots



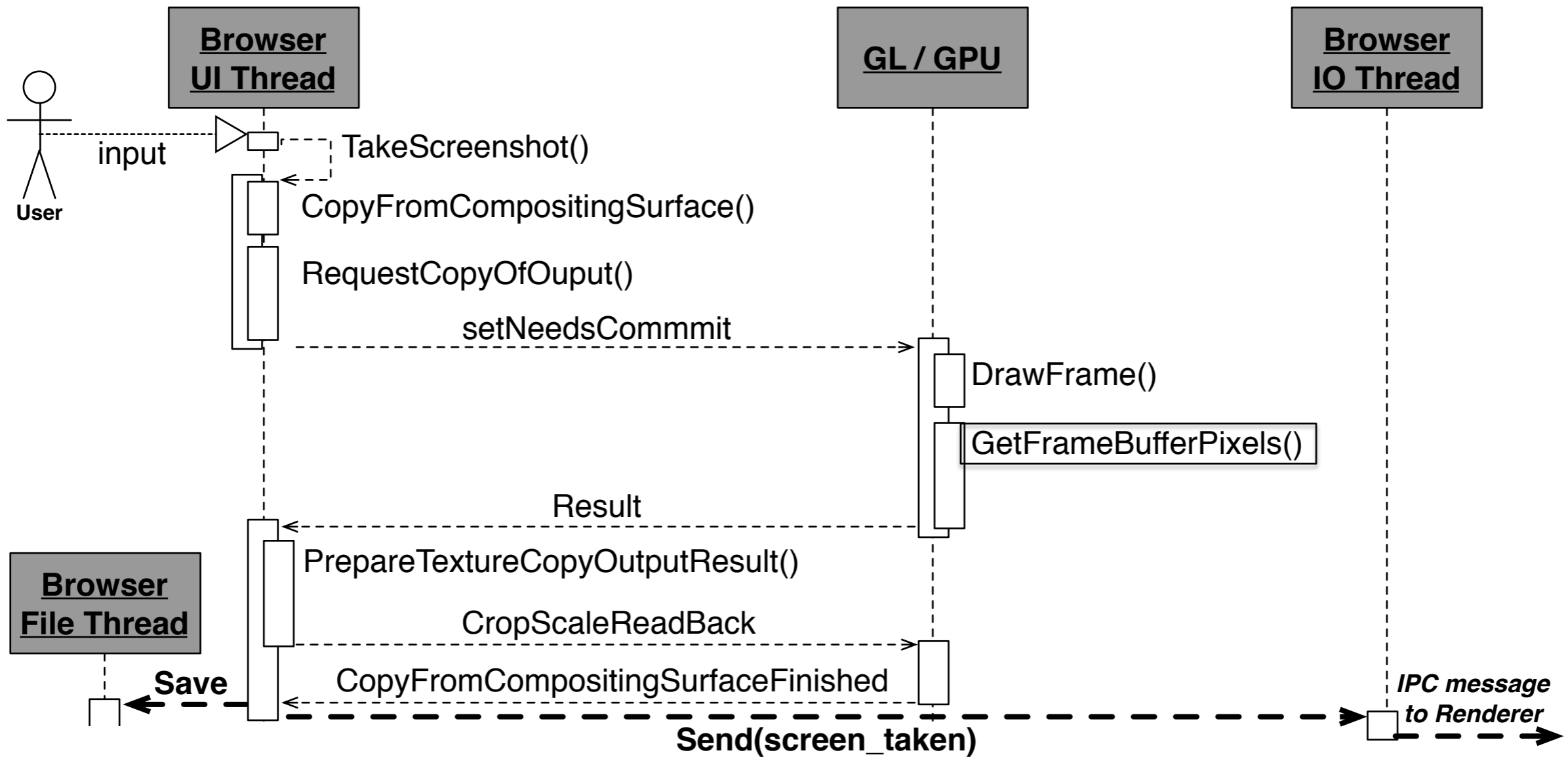
Taking screenshots



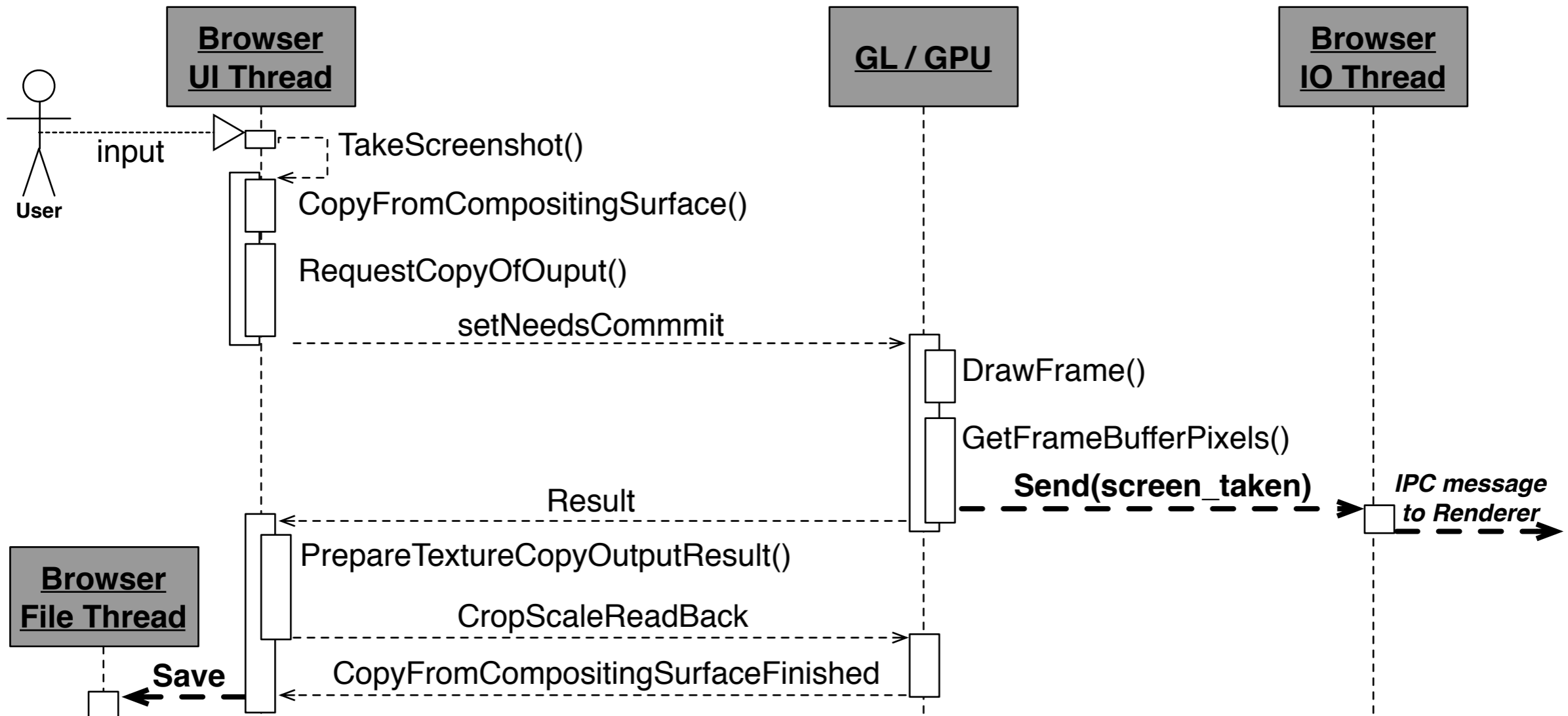
Taking screenshots



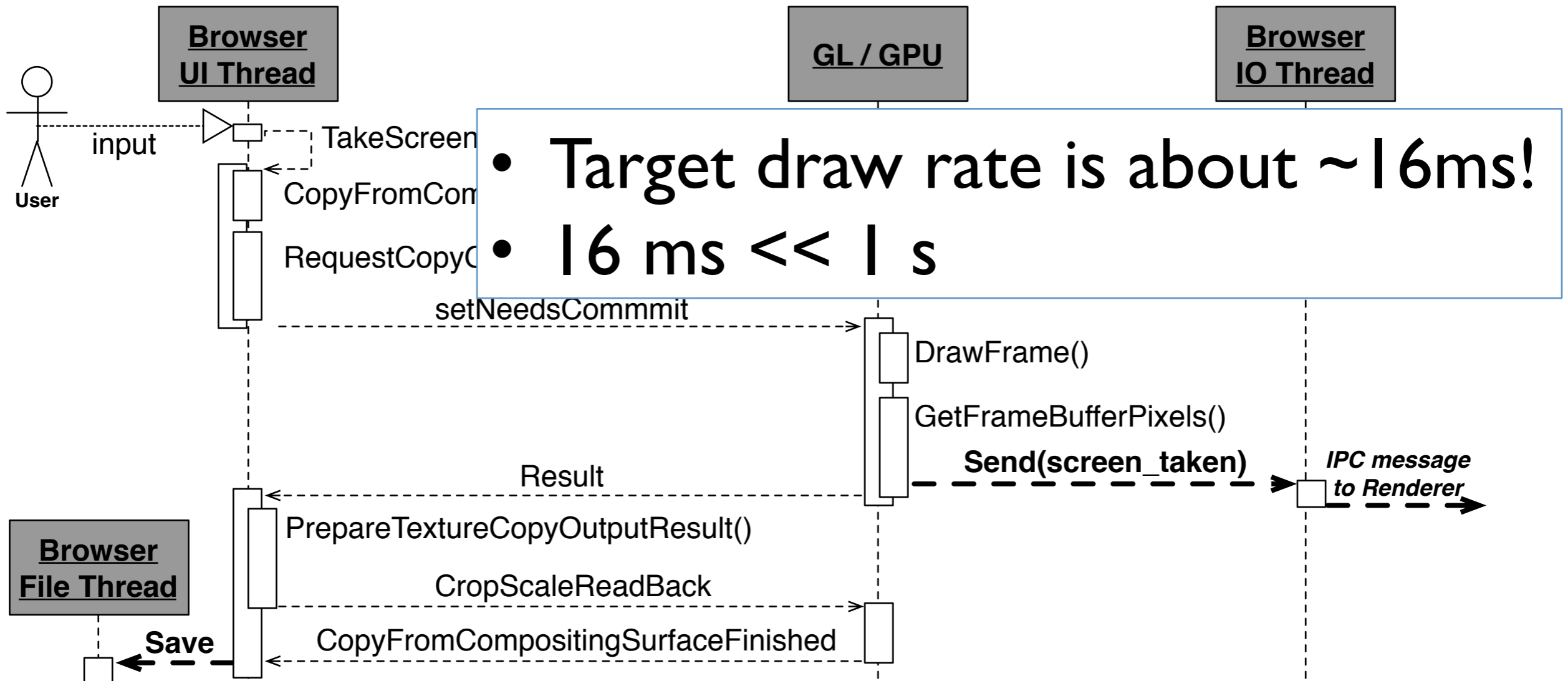
Taking screenshots



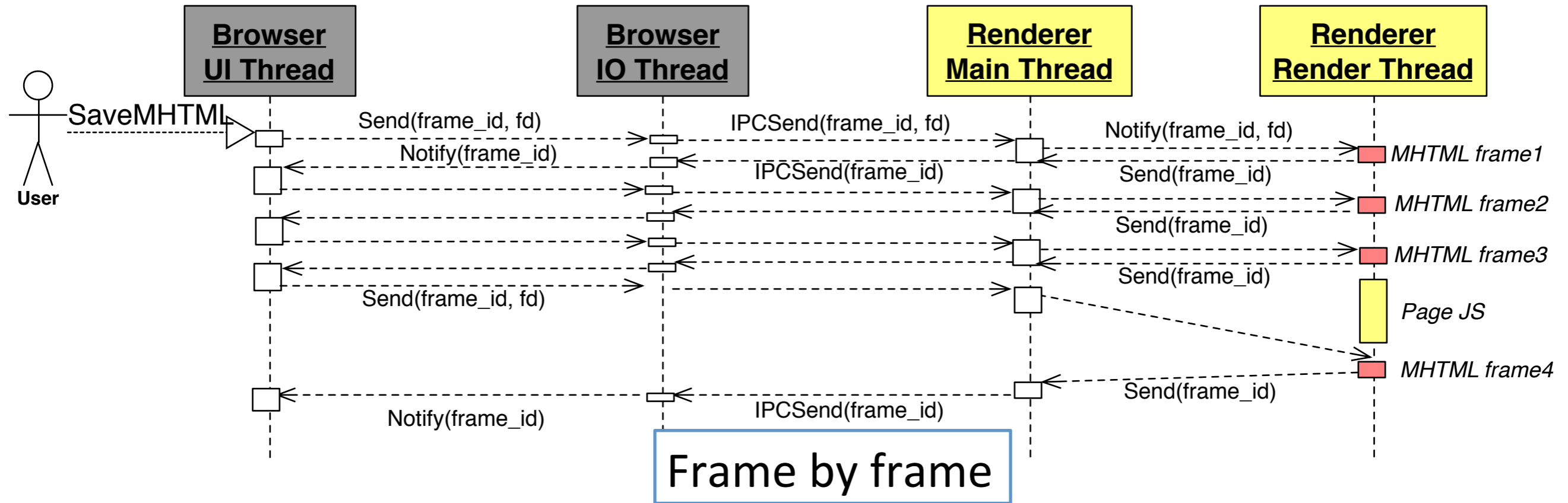
Efficient screenshots



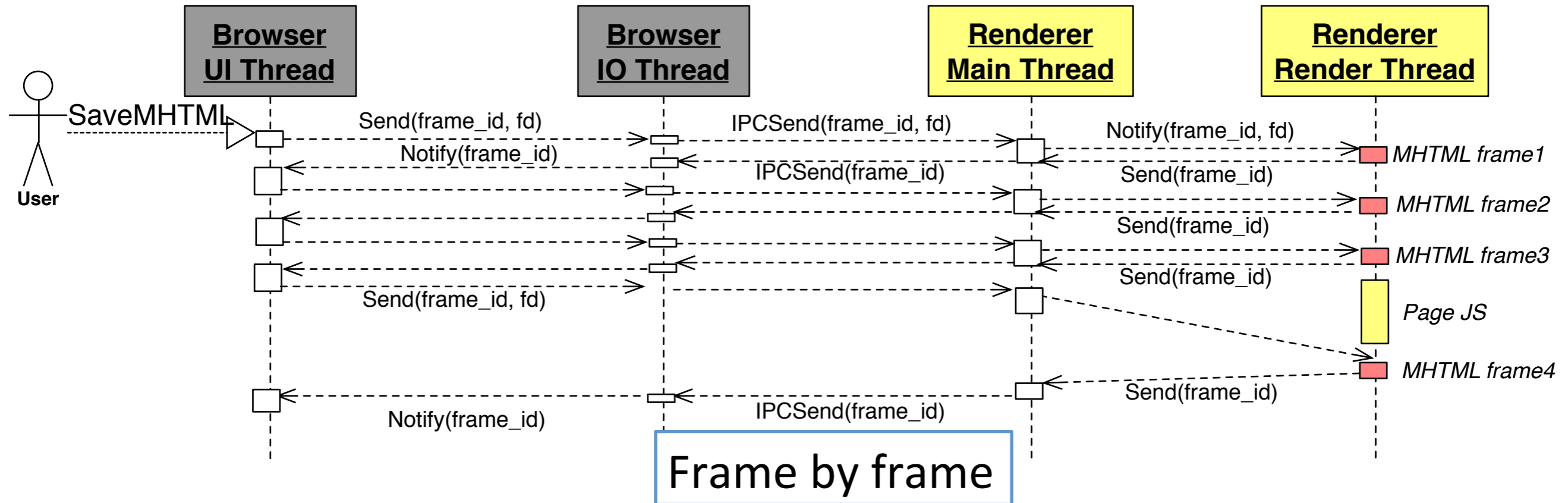
Efficient screenshots



Chromium MHTML Code

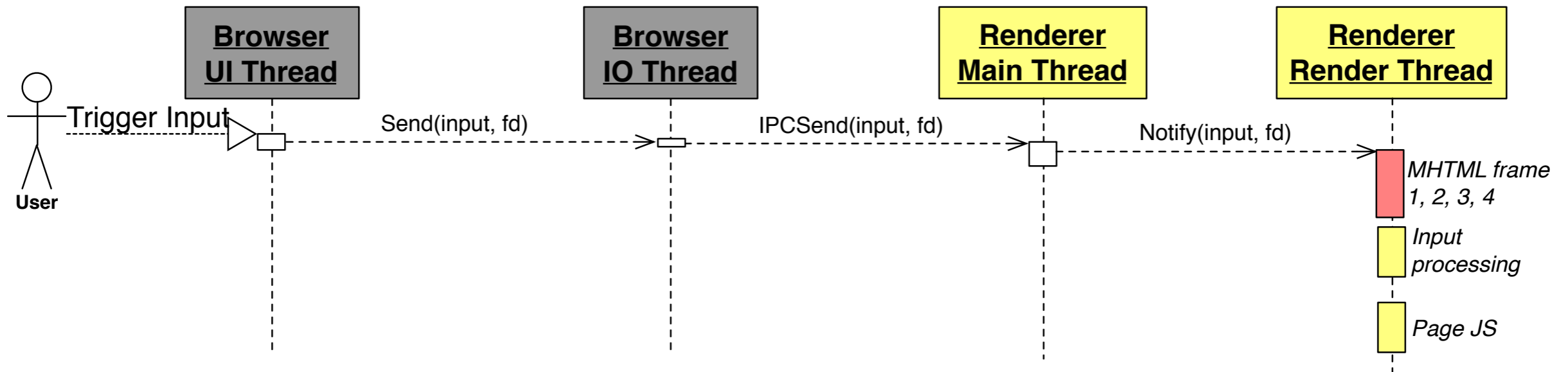


Chromium MHTML Code



“the render thread is a scary place”
 “on ARM, stalls can be seconds long”
 - Chromium Docs

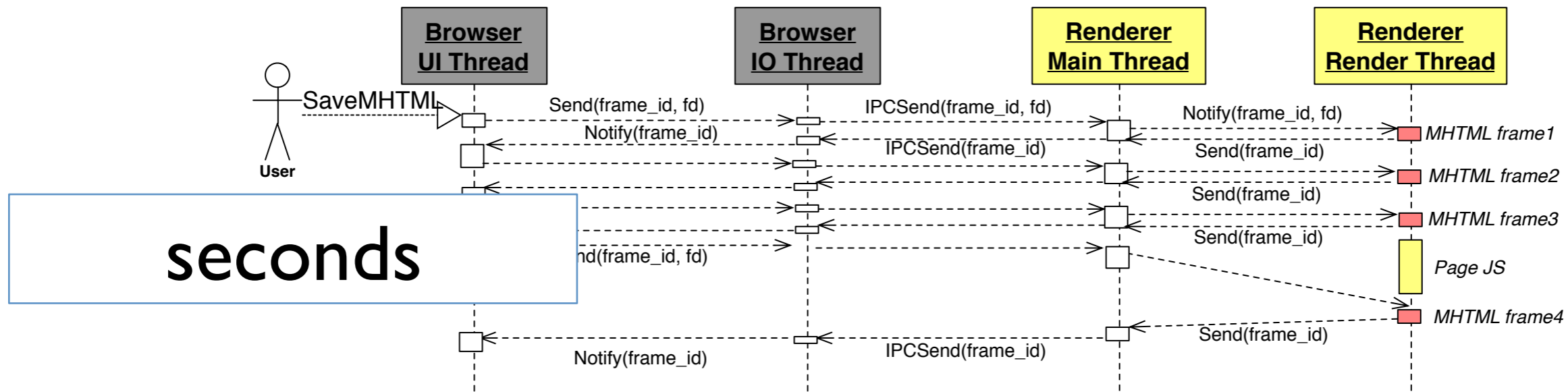
Efficient DOM Snapshots



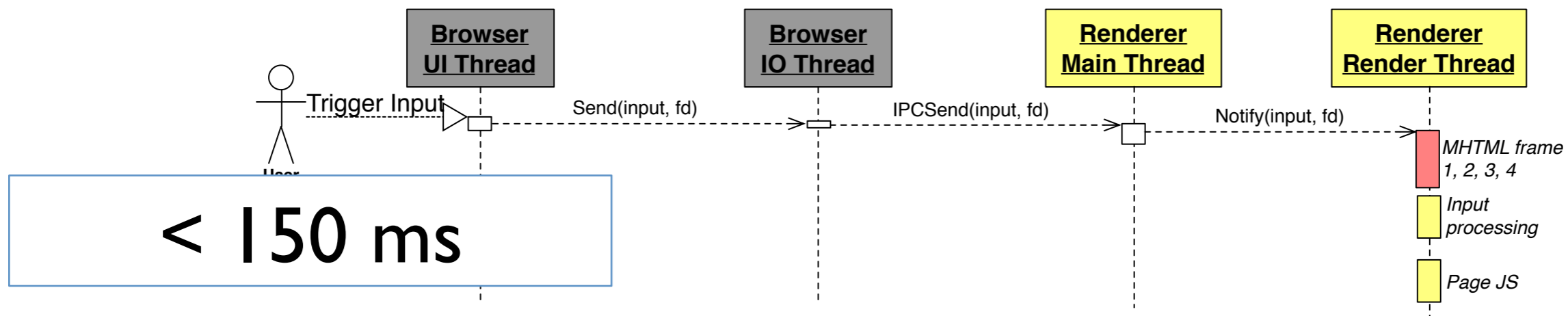
- Process all frame in a single task.
- Piggyback on input processing task.

DOM Snapshots: Comparison

Original MHTML Code



ChromePic DOM Snapshots

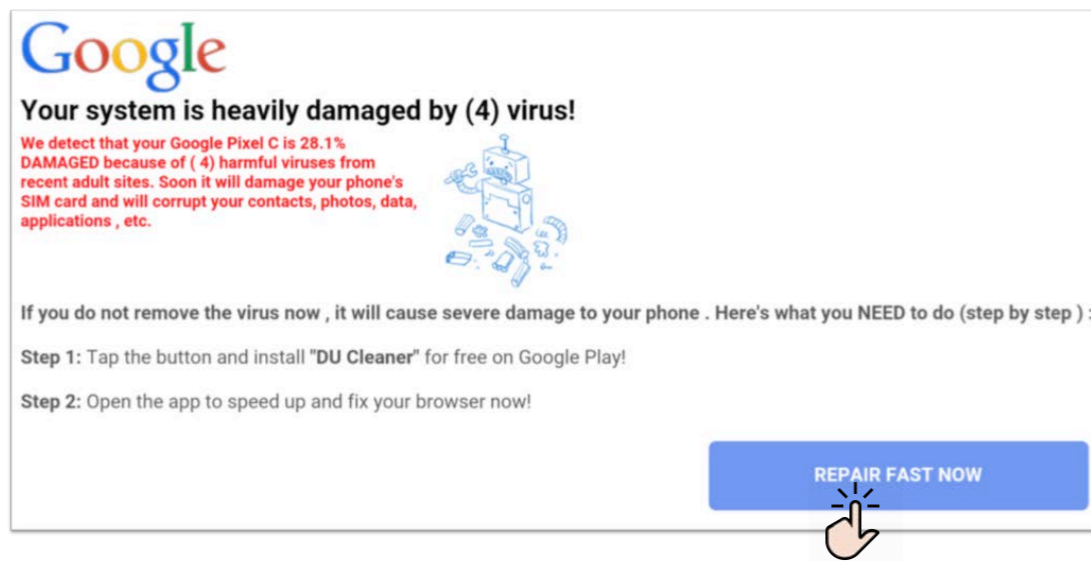
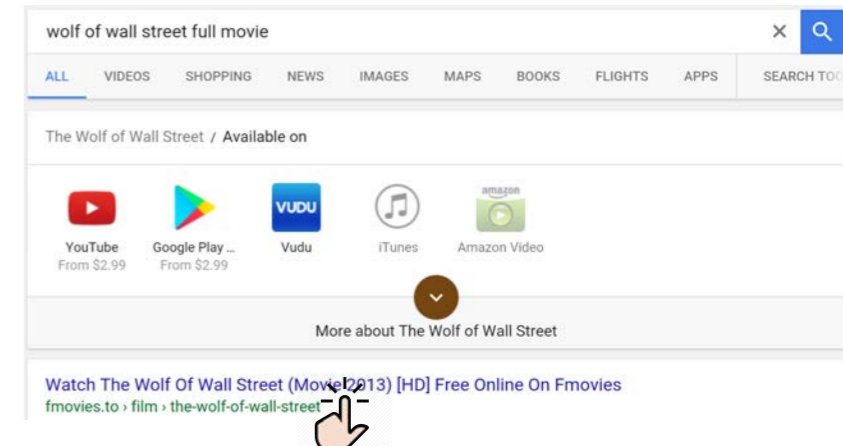
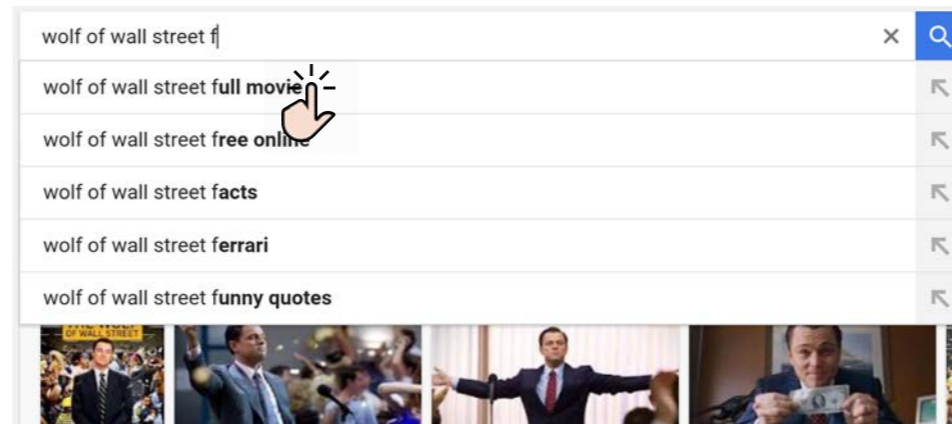
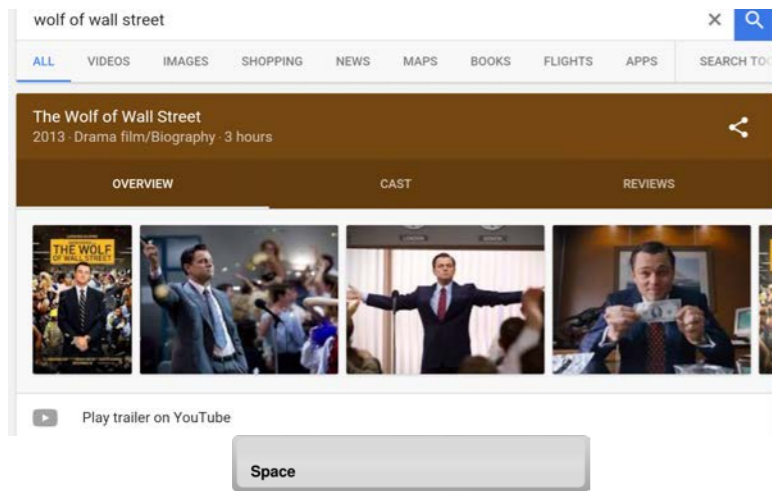


Evaluation

- Reconstructing attacks on users
- Used ChromePic on various UI attack pages
 1. An in-the-wild social engineering attack
 2. Real-world phishing pages
 3. Clickjacking attacks from WOOT '14 [2]



Social engineering attack






Alert Box (from DOM Snapshot)
WARNING ! This Google Pixel C is infected with viruses and your browser is seriously damaged. You need to remove viruses and make corrections immediately. It is necessary to remove and fix now. Don't close this window. ** If you leave , you will be at risk**



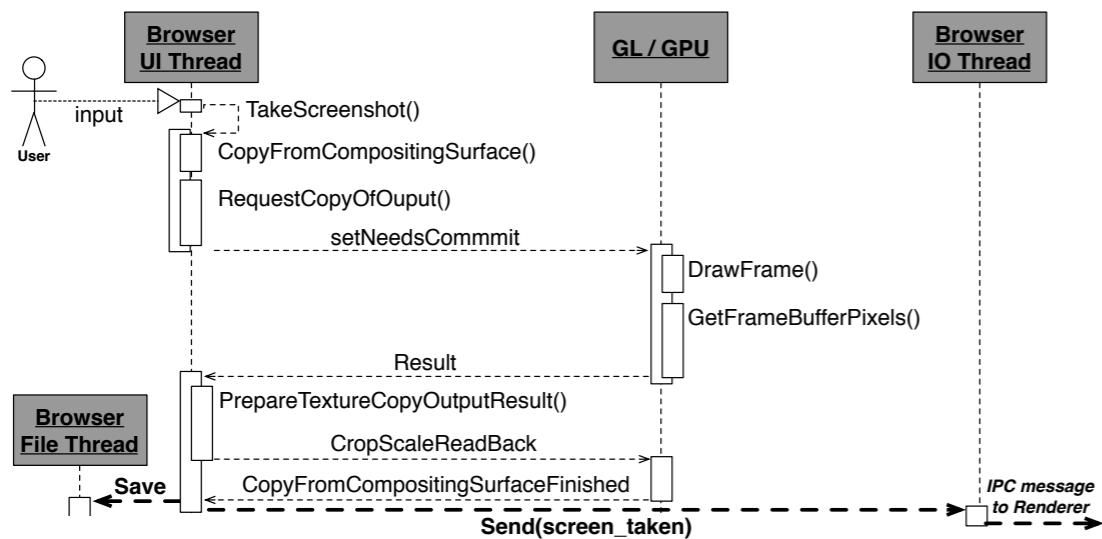
User Study

- **Measure performance on real user behavior**
- 15 minutes limit for each user/device

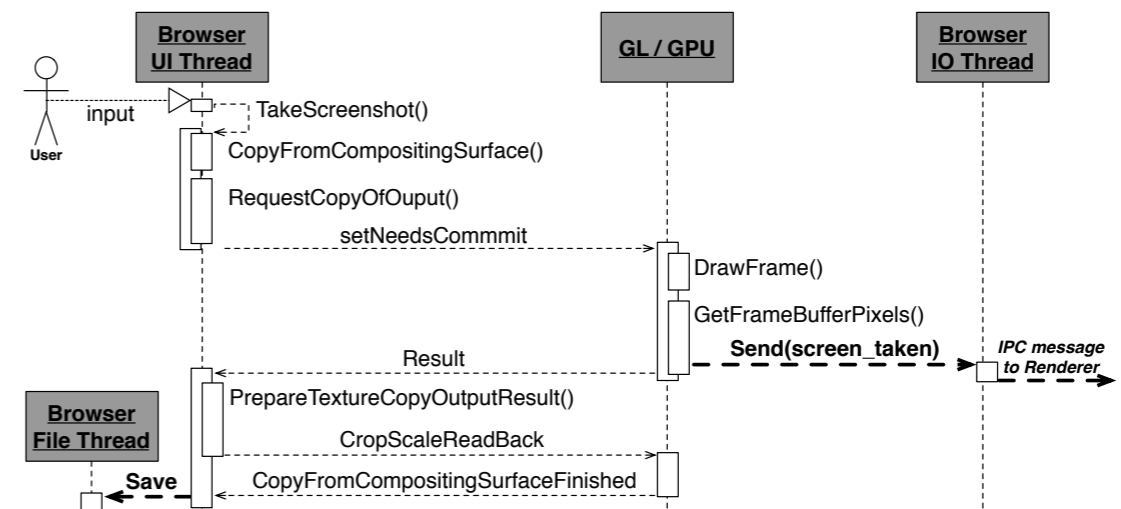
				Total
# Users	11	15	16	22 (unique)
Browsing Time (minutes)	286	346	363	995
# Domains	65	80	92	204 (unique)
# Webshots	1376	2145	2428	5949

Screenshot Overhead

Original Screenshot Code



ChromePic - Optimized



	Median(ms)	98% (ms)
Tablet	65.7	110
Laptop	36.2	71
Desktop	39	118

	Median(ms)	98% (ms)
Tablet	13	25.9
Laptop	5.38	27.7
Desktop	2.7	23.8

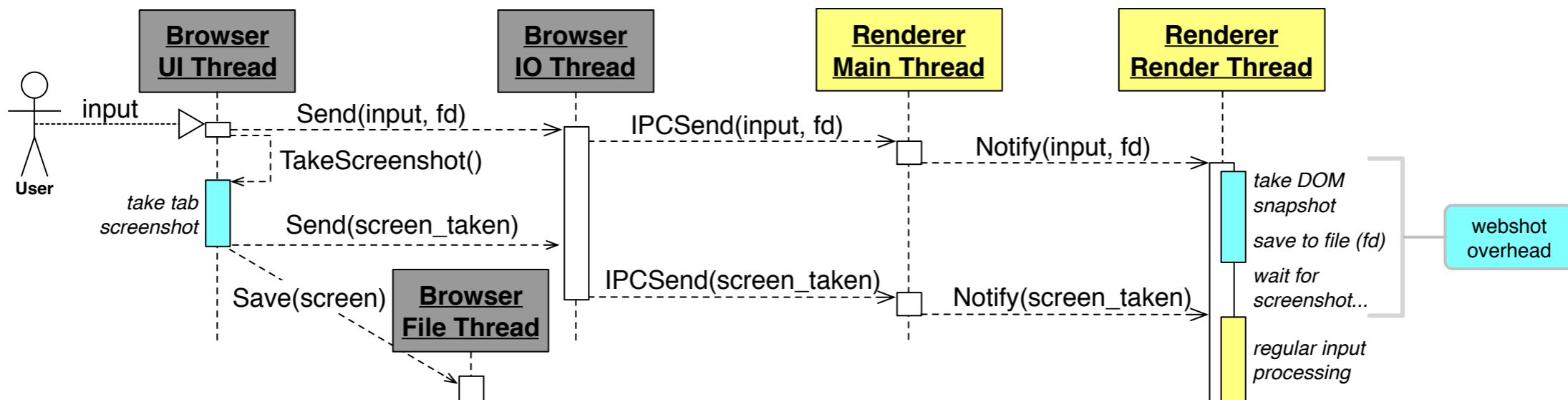
Total Webshot Overhead

Screenshot Overhead

	Median(ms)	98% (ms)
Tablet	13	25.9
Laptop	5.38	27.7
Desktop	2.7	23.8

DOM Snapshot Overhead

	Median(ms)	98% (ms)
Tablet	59.5	203
Laptop	33.3	109.6
Desktop	19	76.1



Total Webshot Overhead

Screenshot Overhead

	Median(ms)	98% (ms)
Tablet	13	25.9
Laptop	5.38	27.7
Desktop	2.7	23.8

DOM Snapshot Overhead

	Median(ms)	98% (ms)
Tablet	59.5	203
Laptop	33.3	109.6
Desktop	19	76.1

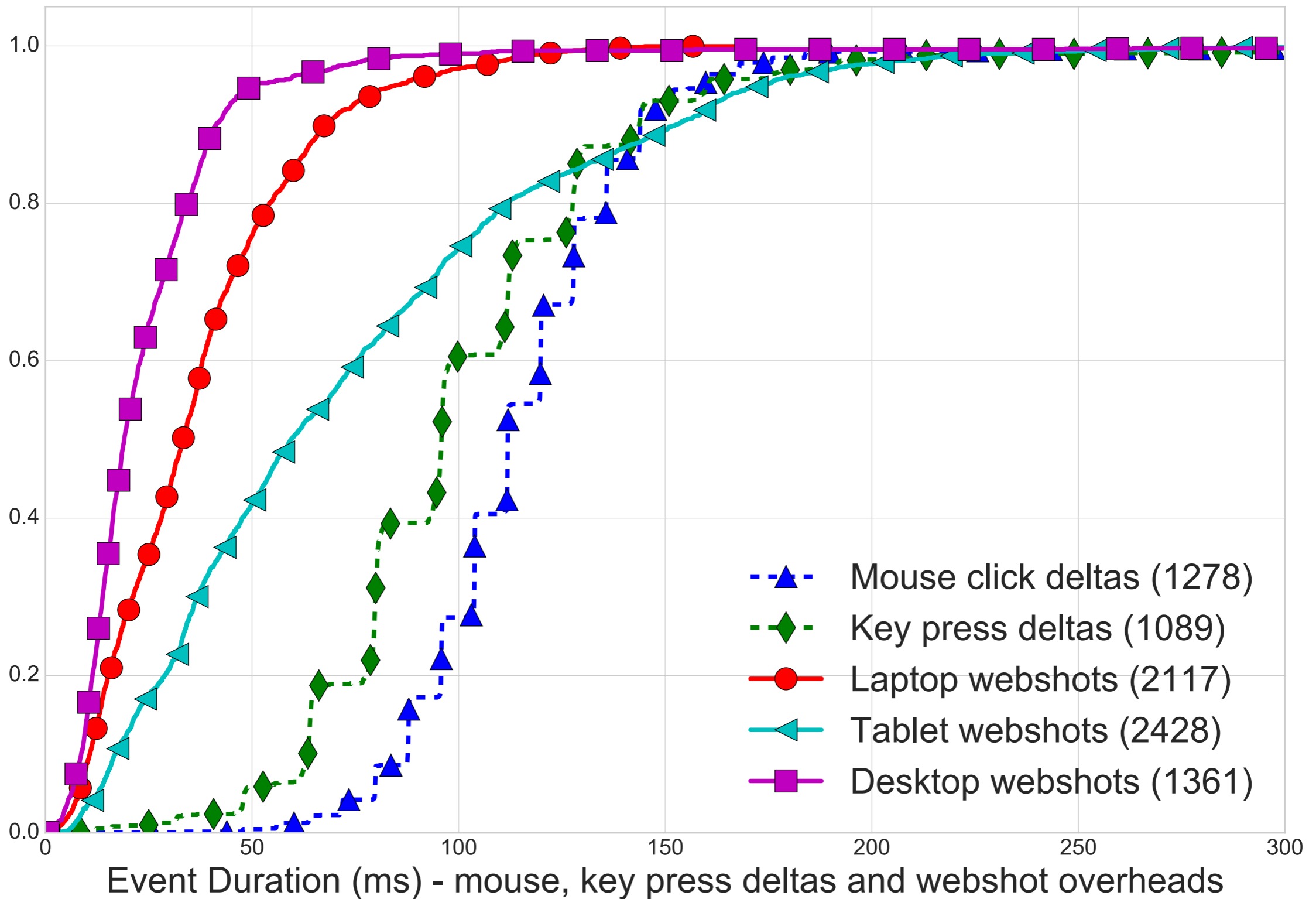
89% < 150 ms



< 150 ms



Performance Overhead



Storage

Platform	Uncompressed		Compressed	
	Screenshots	DOM	Screenshots	DOM
Android	6.80	11.62	0.31	0.54
Linux laptop	4.66	11.33	0.15	0.88
Linux desktop	2.31	8.07	0.09	0.83

Storage requirements in **MB/Minute**

- Maximum requirement of about **1.03 MB/minute** of active browsing
- At this rate, a **1000 employee** corporate network would generate **72 TB** of log data per year

Discussion on Privacy

- **Disable on HTTPS** connections using valid SSL certificates
- **Whitelist sensitive** websites
- Site-based encryption scheme based on a key-escrow agent.
 - Each site's data is encrypted with a **separate key**
 - When an incident happens, the investigator gets only **keys to the relevant sites**.
 - **Forward secure encryption schemes** can be used to extend this for devices that are not always connected to the key escrow agent

Conclusion

- ChromePic is a **lightweight and portable forensic engine**.
- It can accurately log important user inputs and the associated browser states.
- ChromePic can help **reconstruct real world UI attacks**.
- ChromePic has **imperceptible latency** and requires only **moderate disk space** for logs.



Thank You!



Source code to be released soon!

Binaries already available!!

<https://github.com/chromepic/chromepic-browser>

