Tales from the trenches:

Fingerprints on the Web

@igortolivei

WHOAMI

Why to track users?

- Analytics
- Target Ads
- Personalization
- Fraud detection
- Deanonymization

Reminiscences Of The Past

Cookies

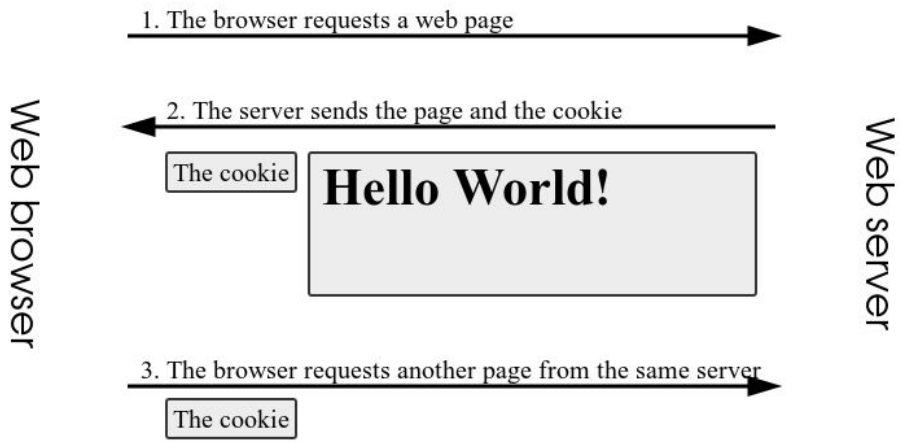
Reminiscences Of The Past - Cookies

Cookies are nuggets of data that can be stored on your PC (Browser) by a Web site and then accessed every time you go back to that site.

Internet 'Cookies' Raise a Batch of Privacy Concerns. Los Angeles Times. 1996

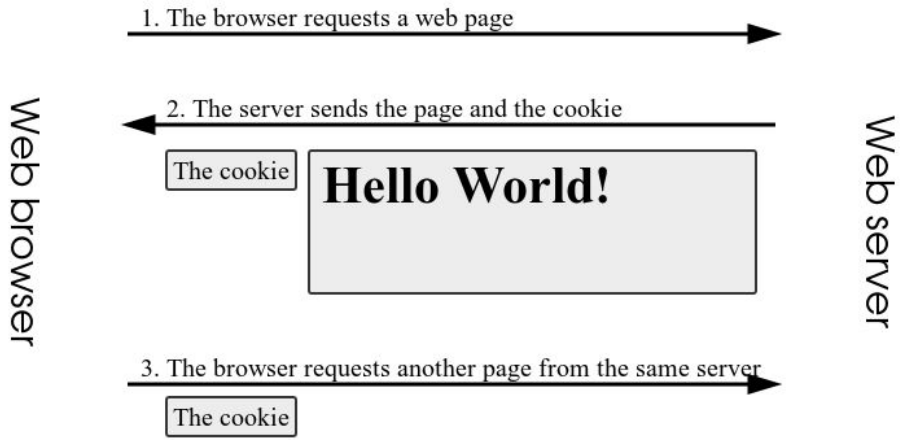
Reminiscences Of The Past - Cookies

- Browser Requests a web page



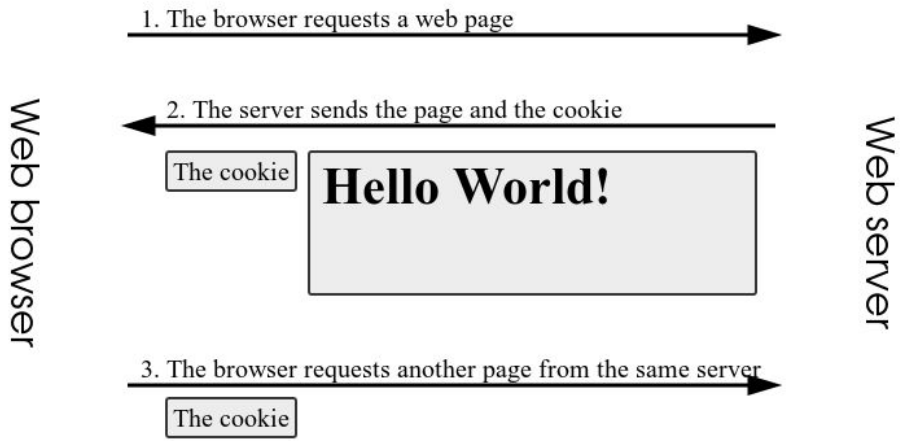
Reminiscences Of The Past - Cookies

- Browser Requests a web page
- The server sends the page and the cookie (Set-Cookie HTTP Header)



Reminiscences Of The Past - Cookies

- Browser Requests a web page
- The server sends the page and the cookie (Set-Cookie HTTP Header)
- The browser requests a new page from the same server



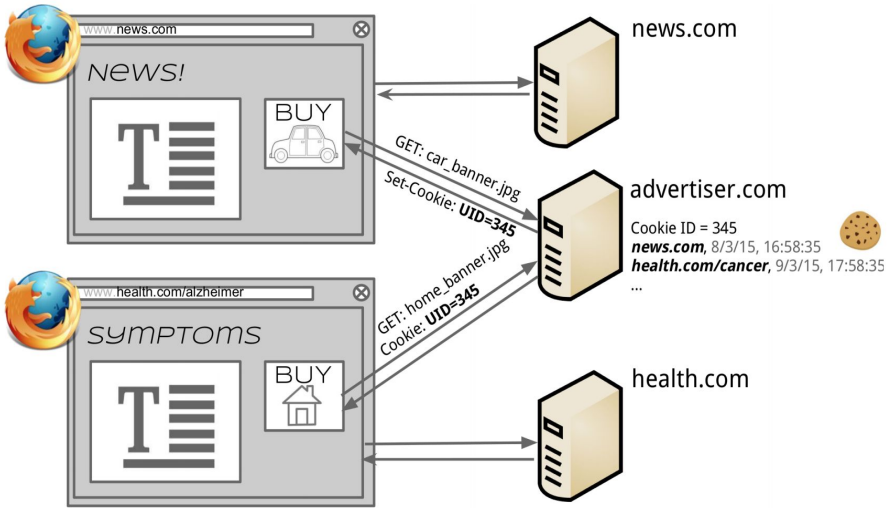
Reminiscences Of The Past

Cookie Apocalypse

In 1996 **Third Party Cookies** where being used in the wild.

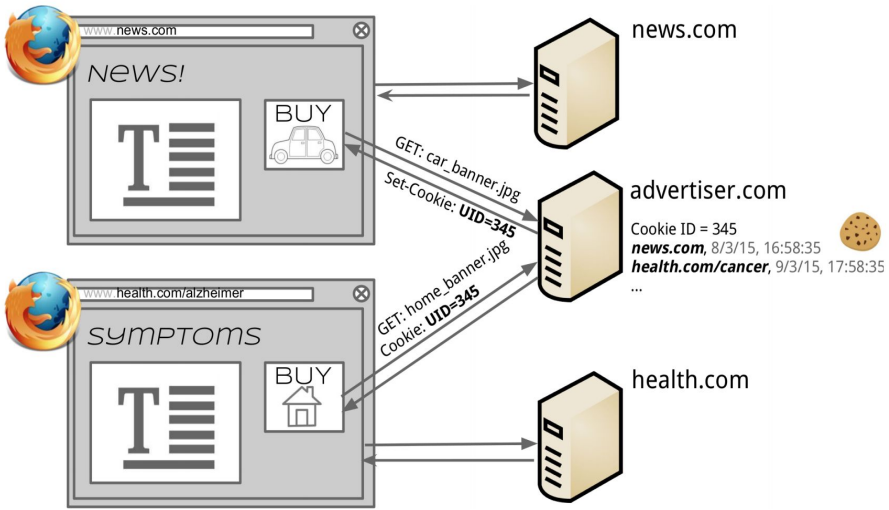
HTTP Cookies: Standards, Privacy, and Politics. DAVID M. KRISTOL. 2001.

- Browser requests the Web Page



Reminiscences Of The Past - Cookie Apocalypse

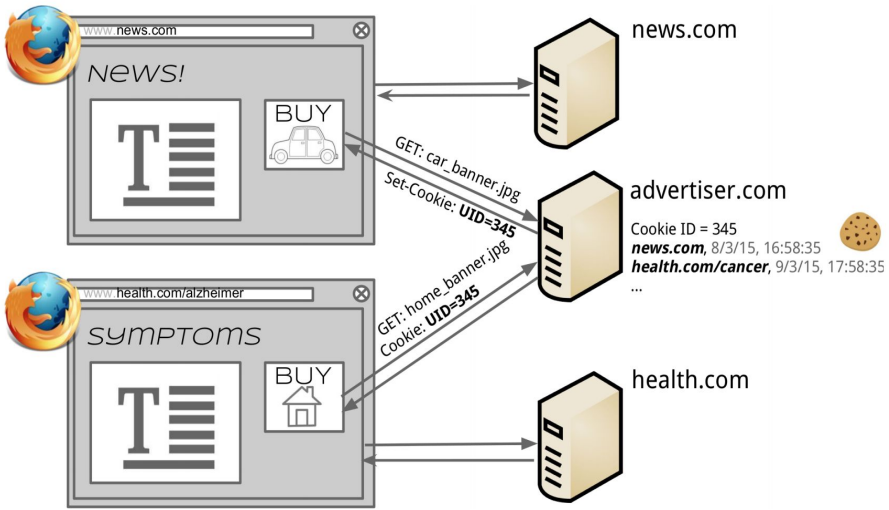
- Browser requests the Web Page
- The server sends the page and the cookie (Set-Cookie HTTP Header)



Online Tracking Technologies and Web Privacy. Günes Acar. 2017.

Reminiscences Of The Past - Cookie Apocalypse

- Browser requests the Web Page
- The server sends the page and the cookie (Set-Cookie HTTP Header)
- When the user visits either of the websites, the Browser will send the cookies to the advertiser



Online Tracking Technologies and Web Privacy. Günes Acar. 2017.

The Rage of the Ad Blockers

The Rage of the Ad Blockers

Browser Fingerprinting

- Request Behavior
- JavaScript
- CSS
- Plugins

- Request Behavior
- JavaScript
- CSS
- ~~Plugins~~

- # Accept-* Headers

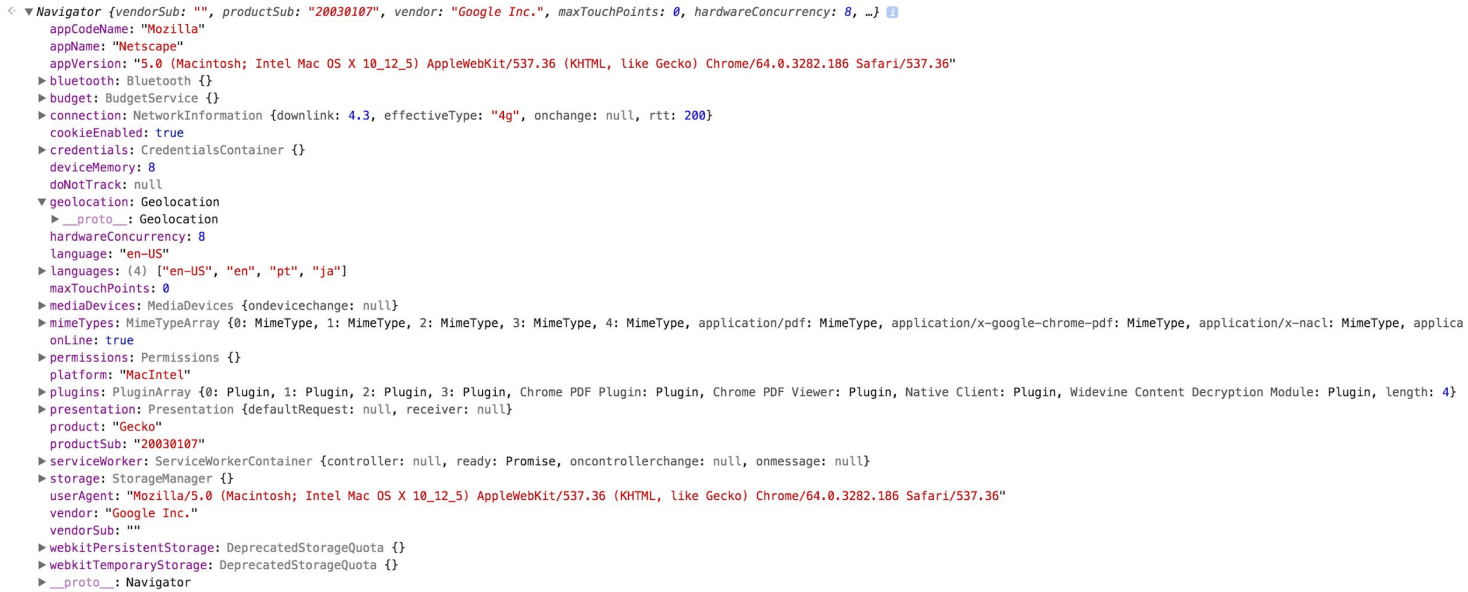
```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: deflate, gzip;q=1.0
```

- # User Agent

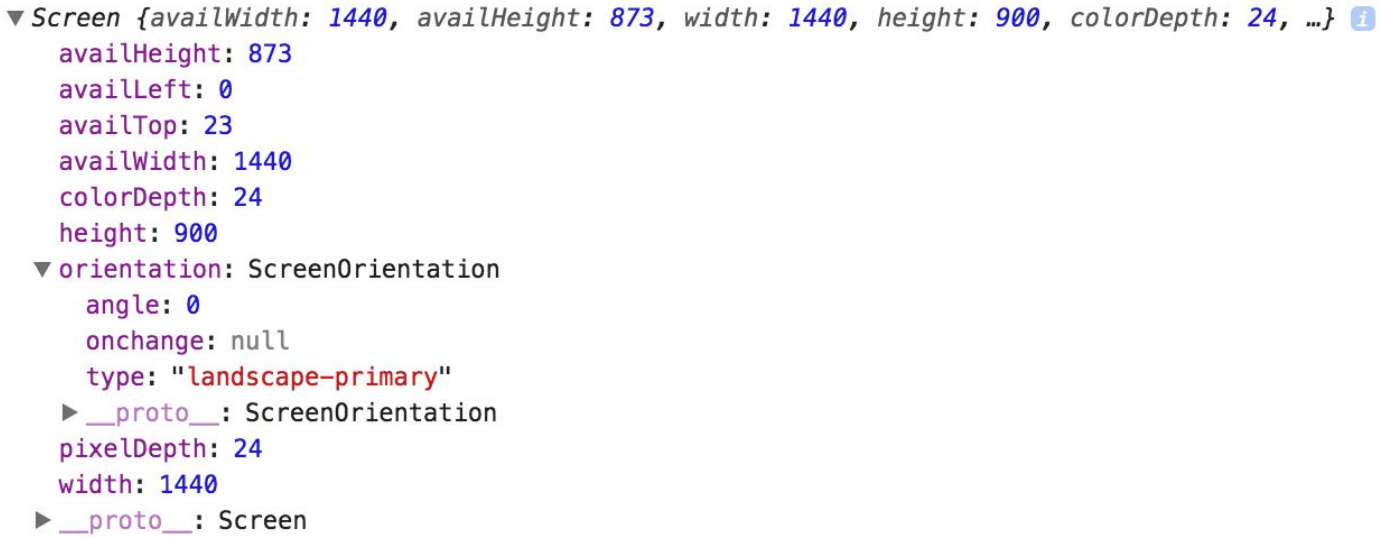
```
Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52
```

Behavior of JS Objects - Navigator



Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. Frederick Beyer. 2013.

Behavior of JS Objects - Screen



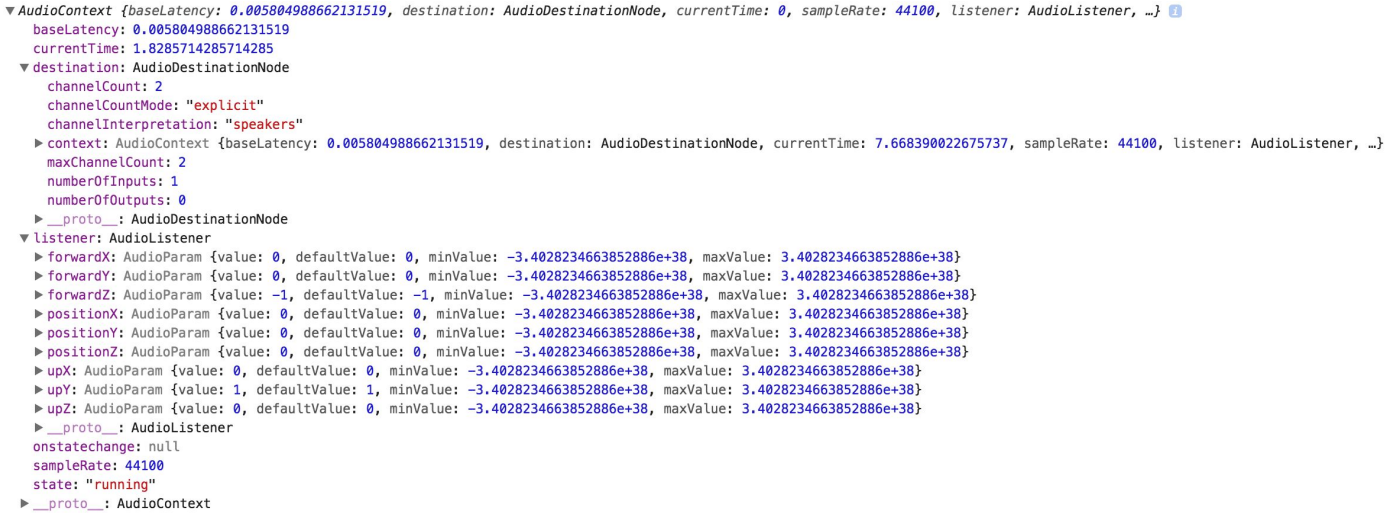
Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. Frederick Beyer. 2013.

. Mitigation

- We make the values uniform
- Locales, Dates, vendors ...

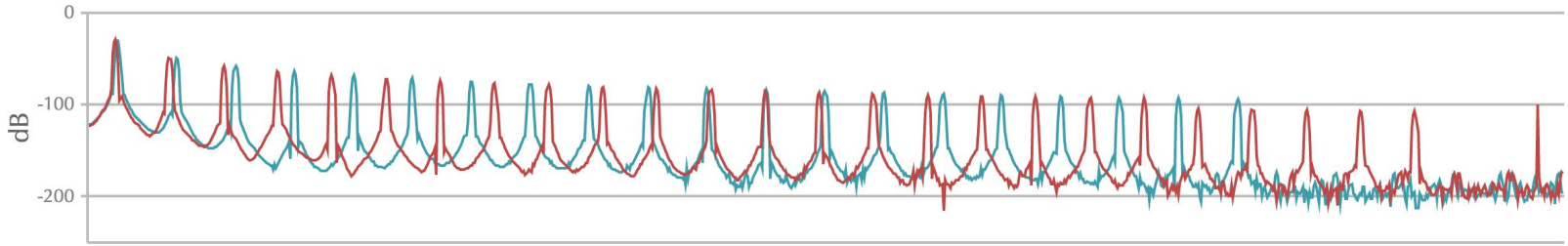
Browser Fingerprinting - JavaScript

- # WebAudio



Online tracking: A 1-million-site measurement and analysis. Steven Englehardt and Arvind Narayanan. 2016.

WebAudio



Online tracking: A 1-million-site measurement and analysis. Steven Englehardt and Arvind Narayanan. 2016.

Browser Fingerprinting - JavaScript

```
let cc_output = [];
let audioCtx = new window.AudioContext(),
    oscillator = audioCtx.createOscillator(),
    analyser = audioCtx.createAnalyser(),
    gain = audioCtx.createGain(),
    scriptProcessor = audioCtx.createScriptProcessor(4096, 1, 1);


gain.gain.value = 0; // Disable volume
oscillator.type = "triangle"; // Set oscillator to output triangle wave
oscillator.connect(analyser); // Connect oscillator output to analyser input
analyser.connect(scriptProcessor); // Connect analyser output to scriptProcessor input
scriptProcessor.connect(gain); // Connect scriptProcessor output to gain input
gain.connect(audioCtx.destination); // Connect gain output to audiocontext destination

scriptProcessor.onaudioprocess = function () {
    let bins = new Float32Array(analyser.frequencyBinCount);
    analyser.getFloatFrequencyData(bins);
    for (var i = 0; i < bins.length; i = i + 1) {
        cc_output.push(bins[i]);
    }
    //cc_output.extend(bins);
    analyser.disconnect();
    scriptProcessor.disconnect();
    gain.disconnect();

    console.log(cc_output)
};

oscillator.start(0);
```

- Mitigation
  - Too many things to make uniform
  - We disable it :(

- Timing Based Side Channels
  - JavaScript JIT

- Timing Based Side Channels
  - JavaScript JIT
  - CPU

- Timing Based Side Channels
  - JavaScript JIT
  - CPU
  - **Timing of computation**

Timing Based Side Channels

```
performance.now()
new Date().getTime()
audioContext.currentTime
canvasStream.currentTime
video.currentTime
audio.currentTime
new File([], "").lastModified
new File([], "").lastModifiedDate.getTime()
animation.startTime
animation.currentTime
animation.timeline.currentTime
document.timeline.currentTime
```

Timing Based Side Channels

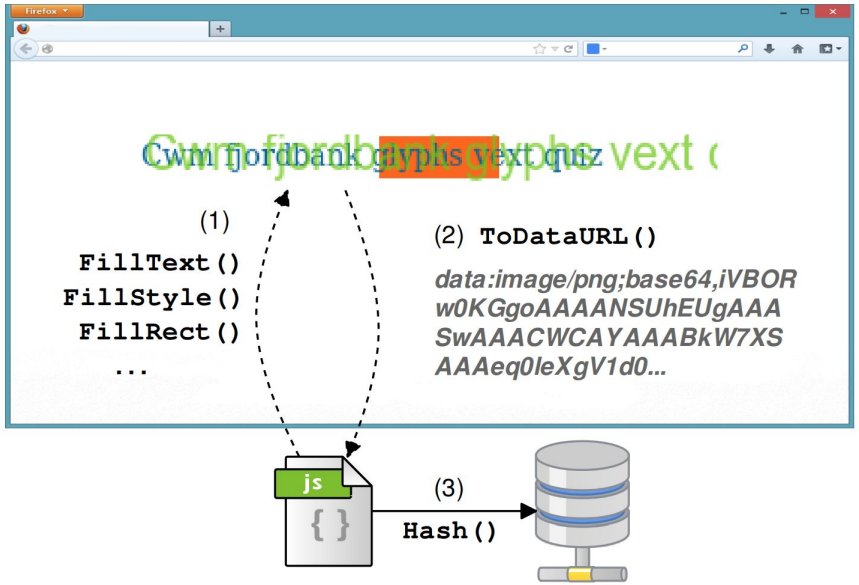
```
<html><body><img id="test" style="display: none">
<script>
  var test = document.getElementById('test');
  var start = new Date();
  test.onerror = function() {
    var end = new Date();
    alert("Total time: " + (end - start));
  }
  test.src = "http://www.example.com/page.html";
</script>
</body></html>
```

Exposing Private Information by Timing Web Applications. Andrew Bortz et al. 2007.

- Mitigation
  - Remove timers granularity: Clamp to 100ms

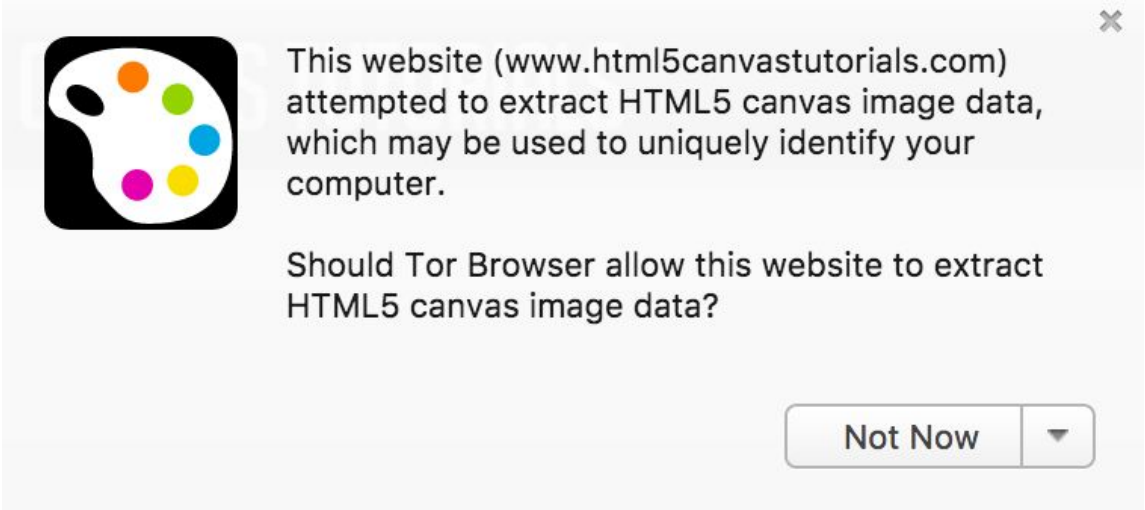
- Mitigation
  - Remove timers granularity: Clamp to 100ms
  - No silver bullet :(

Canvas2D

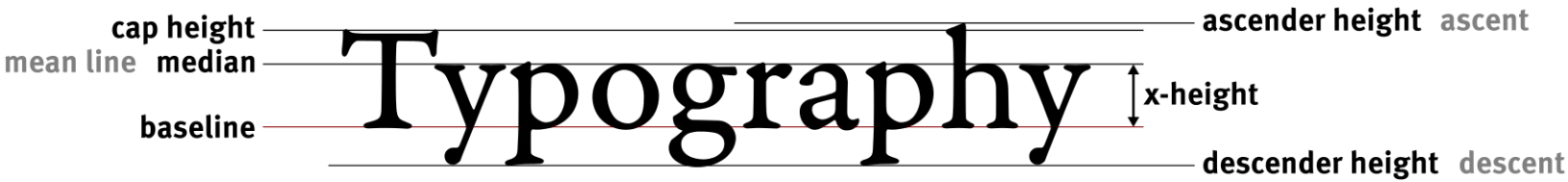

Cwm fjordbank glyphs vext quiz
(1)
FillText()
FillStyle()
FillRect()
...
(2) ToDataURL()

w0KGgoAAAANSUhEUgAAA
SwAAACWCAYAAAABkW7XS
AAAeq0leXgV1d0...
js
{ }
(3)
Hash()

Mitigation


This website (www.html5canvastutorials.com) attempted to extract HTML5 canvas image data, which may be used to uniquely identify your computer.
Should Tor Browser allow this website to extract HTML5 canvas image data?
Not Now

- Line Height
  - Ascender Height + Descender Height + Font size



https://trac.torproject.org/projects/tor/ticket/23104

- Line Height (Firefox)
  - Linux: 19px
  - Mac OS X: 19.5167px
  - Windows: 19.2px or 20px

https://trac.torproject.org/projects/tor/ticket/23104

- Mitigation
  - Use a default value of 1.2 (W3C)

- Media Queries
  - device-aspect-ratio
  - device-height
  - device-width

https://trac.torproject.org/projects/tor/ticket/2875

- Mitigation
  - We make the values uniform
  - E.g. aspect ratio = 1.0

And What About Cookies?!?

First Party Isolation (FPI)
OR
Cross Origin Identifier Unlikability

- First Party (URL based) Isolation of all browser identifier sources

- First Party (URL based) Isolation of all browser identifier sources
  - Cookies
  - Shared Workers
  - Blob
  - Storage

THANKS!

Use Tor (Browser)
Protect Your Privacy

@igortolivei (igt0)