EVERCOOKIE

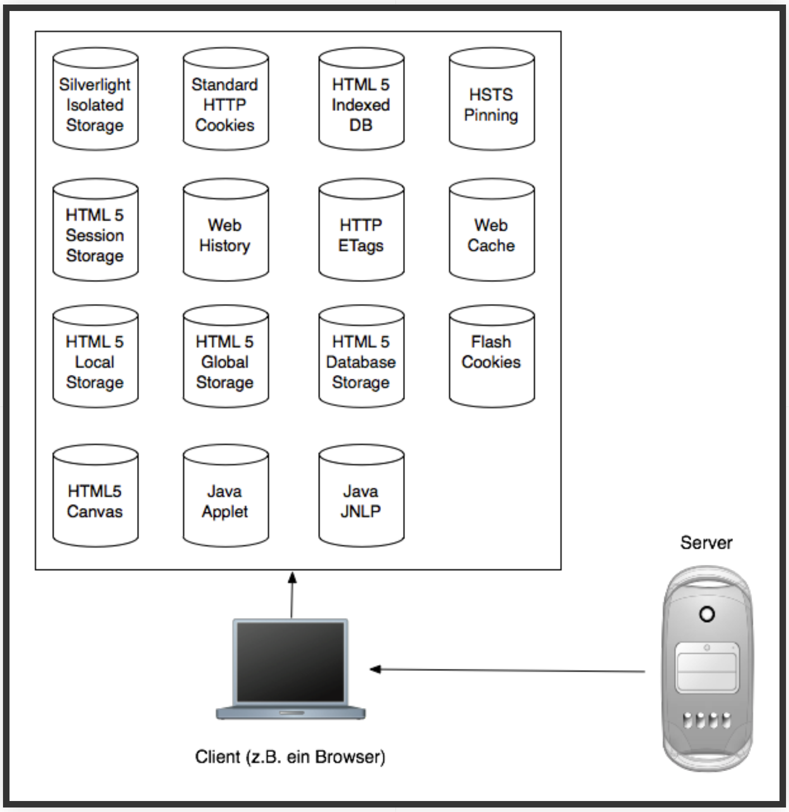
Meetup 11.10.2017 - Sergej Michel

WAS IST EIN HTTP COOKIE?

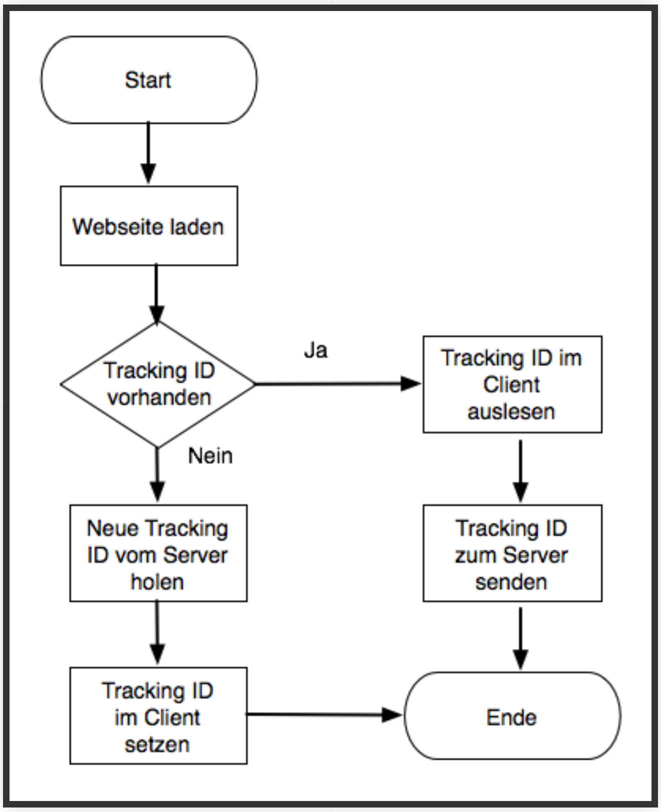
WAS IST EIN EVERCOOKIE?

WOFÜR WIRD EIN EVERCOOKIE VERWENDET?

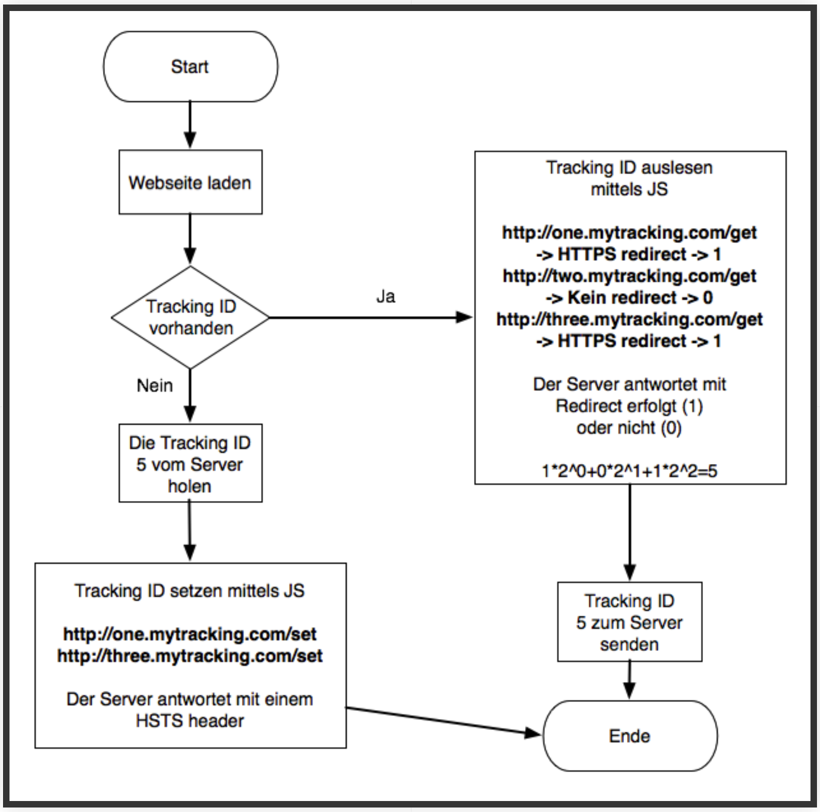
DIE BROWSER SPEICHERORTE



TRACKING ALGORITHMUS

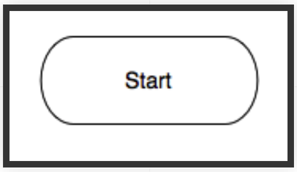

Start
Webseite laden
Tracking ID vorhanden
Ja
Nein
Tracking ID im Client auslesen
Neue Tracking ID vom Server holen
Tracking ID zum Server senden
Tracking ID im Client setzen
Ende

TRACKING ALGORITHMUS HSTS

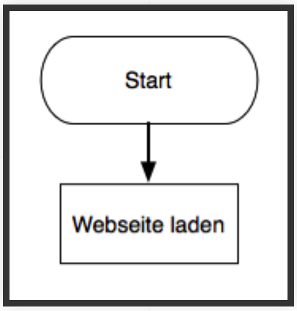


Start
Webseite laden
Tracking ID vorhanden
Ja
Nein
Die Tracking ID 5 vom Server holen
Tracking ID setzen mittels JS
http://one.mytracking.com/set
http://three.mytracking.com/set
Der Server antwortet mit einem HSTS header
Tracking ID auslesen mittels JS
http://one.mytracking.com/get -> HTTPS redirect -> 1
http://two.mytracking.com/get -> Kein redirect -> 0
http://three.mytracking.com/get -> HTTPS redirect -> 1
Der Server antwortet mit Redirect erfolgt (1) oder nicht (0)
1*2^0+0*2^1+1*2^2=5
Tracking ID 5 zum Server senden
Ende

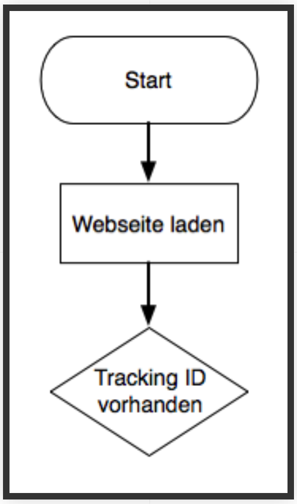
TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN



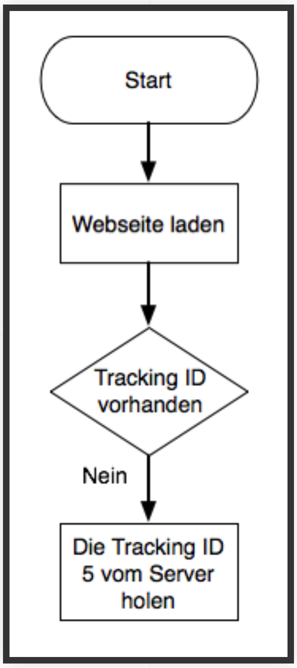
TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN



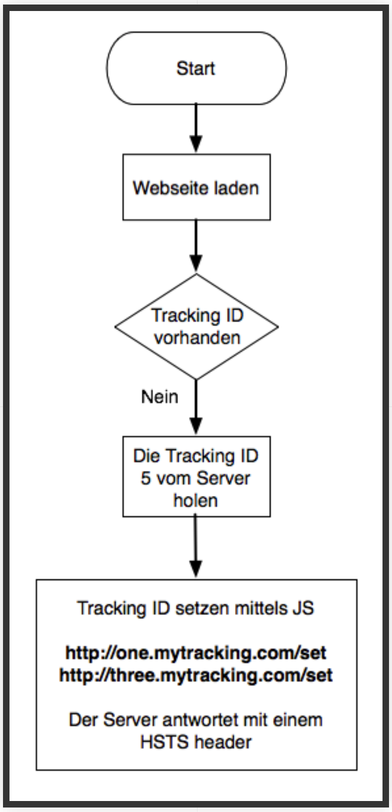
TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN



TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN

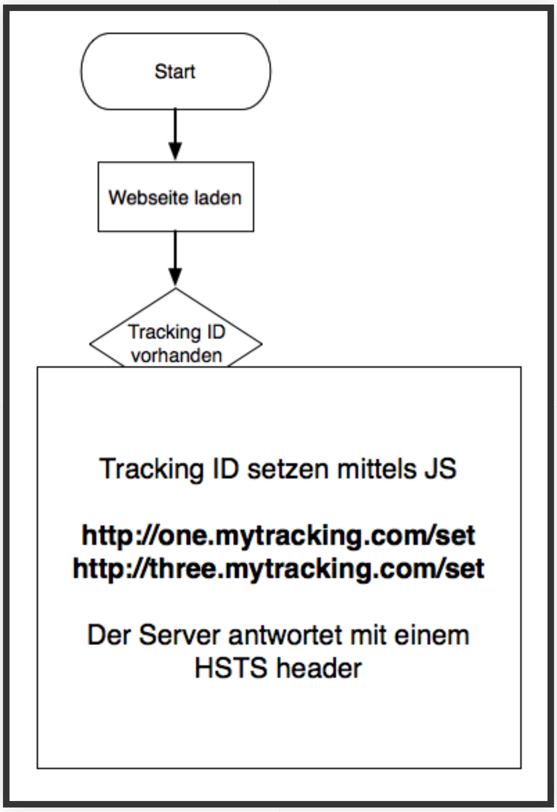


TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN



Start
Webseite laden
Tracking ID vorhanden
Nein
Die Tracking ID 5 vom Server holen
Tracking ID setzen mittels JS
http://one.mytracking.com/set
http://three.mytracking.com/set
Der Server antwortet mit einem HSTS header

TRACKING ALGORITHMUS HSTS TRACKING ID ANLEGEN

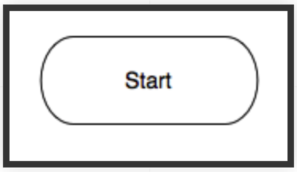


Tracking ID setzen mittels JS

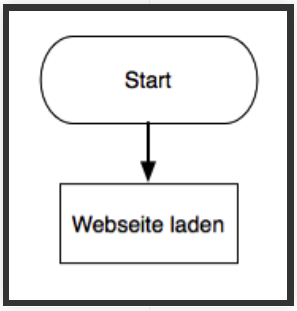
http://one.mytracking.com/set
http://three.mytracking.com/set

Der Server antwortet mit einem HSTS header

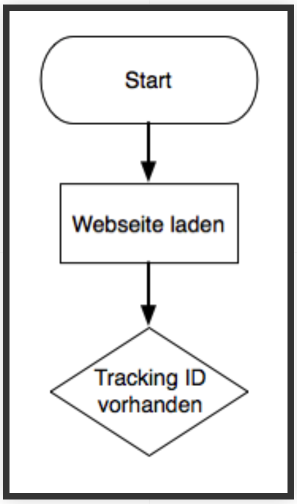
TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



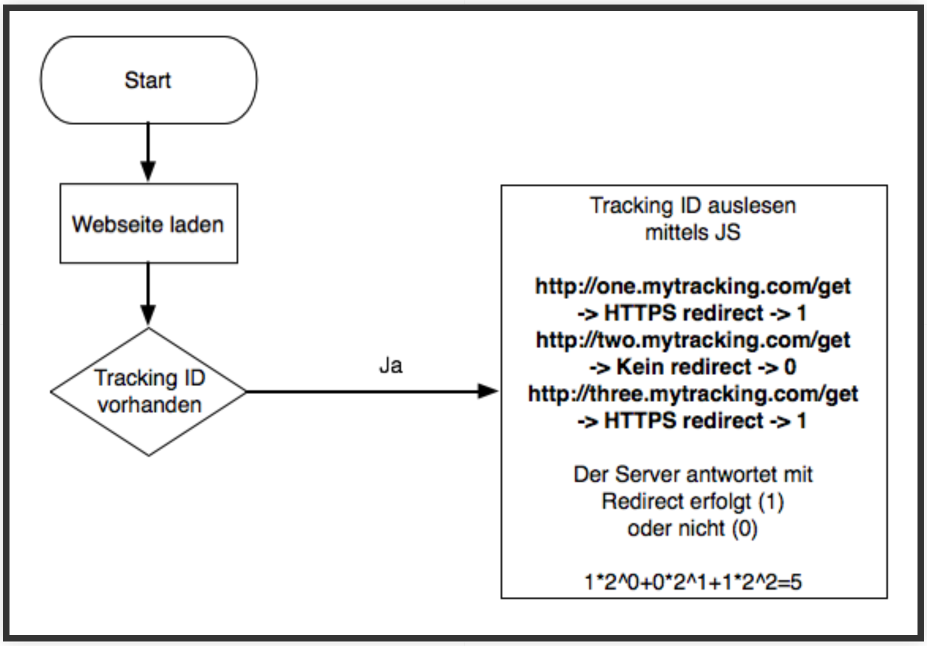
TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



Start

Webseite laden

Tracking ID vorhanden

Ja

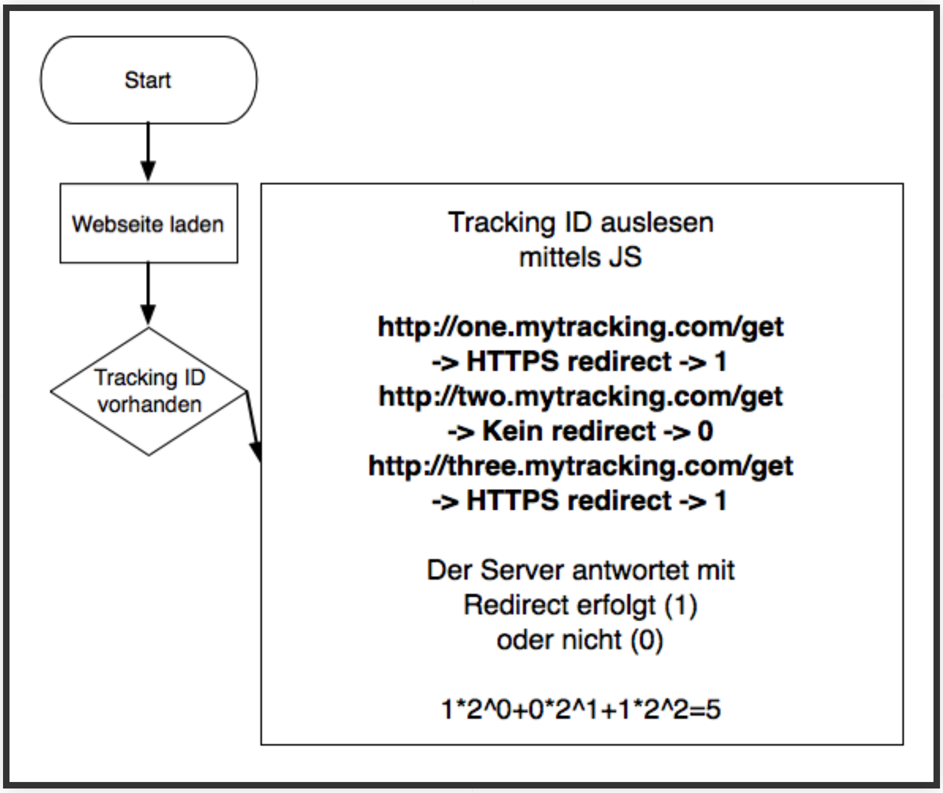
Tracking ID auslesen
mittels JS

http://one.mytracking.com/get
-> HTTPS redirect -> 1
http://two.mytracking.com/get
-> Kein redirect -> 0
http://three.mytracking.com/get
-> HTTPS redirect -> 1

Der Server antwortet mit
Redirect erfolgt (1)
oder nicht (0)

1*2^0+0*2^1+1*2^2=5

TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



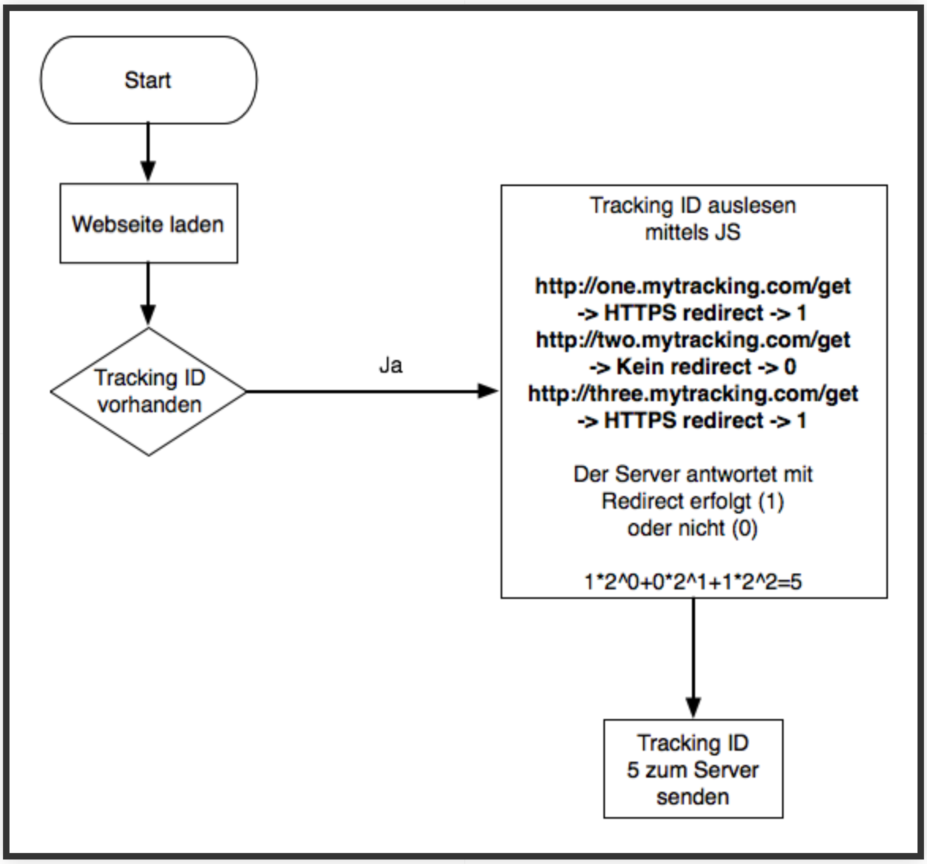
Tracking ID auslesen
mittels JS

http://one.mytracking.com/get
-> HTTPS redirect -> 1
http://two.mytracking.com/get
-> Kein redirect -> 0
http://three.mytracking.com/get
-> HTTPS redirect -> 1

Der Server antwortet mit
Redirect erfolgt (1)
oder nicht (0)

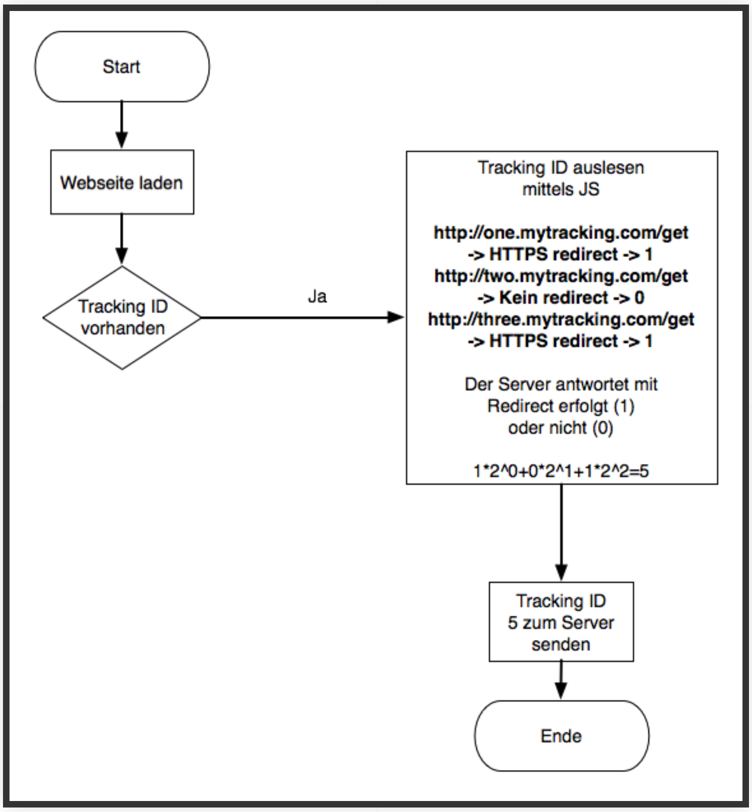
1*2^0+0*2^1+1*2^2=5

TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



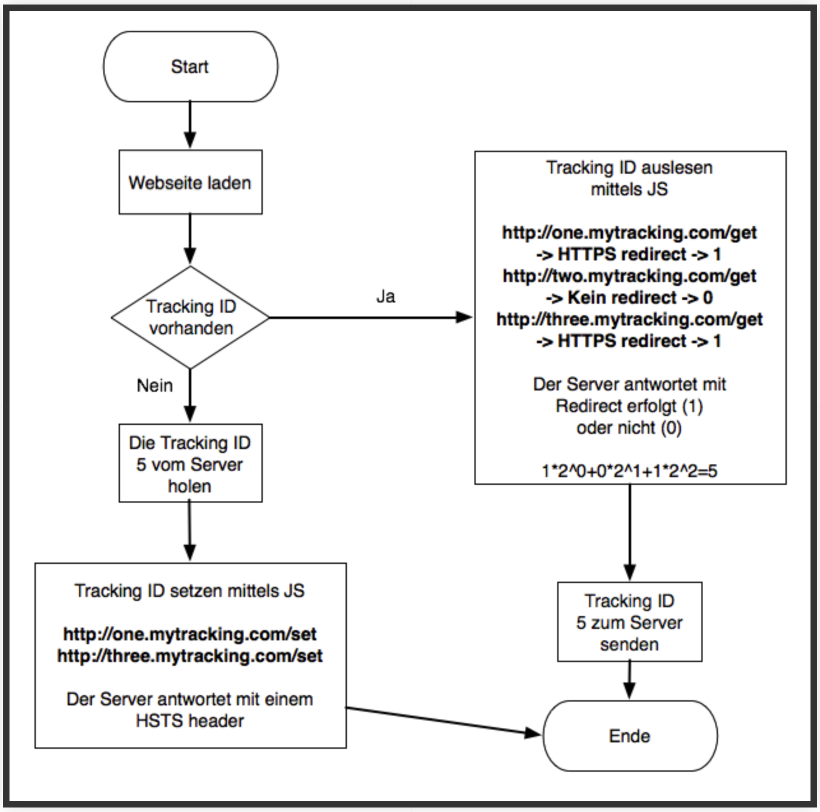
Start
Webseite laden
Tracking ID vorhanden
Ja
Tracking ID auslesen mittels JS
http://one.mytracking.com/get -> HTTPS redirect -> 1
http://two.mytracking.com/get -> Kein redirect -> 0
http://three.mytracking.com/get -> HTTPS redirect -> 1
Der Server antwortet mit Redirect erfolgt (1) oder nicht (0)
1*2^0+0*2^1+1*2^2=5
Tracking ID 5 zum Server senden

TRACKING ALGORITHMUS HSTS TRACKING ID LESEN



Start
Webseite laden
Tracking ID vorhanden
Ja
Tracking ID auslesen mittels JS
http://one.mytracking.com/get -> HTTPS redirect -> 1
http://two.mytracking.com/get -> Kein redirect -> 0
http://three.mytracking.com/get -> HTTPS redirect -> 1
Der Server antwortet mit Redirect erfolgt (1) oder nicht (0)
1*2^0+0*2^1+1*2^2=5
Tracking ID 5 zum Server senden
Ende

TRACKING ALGORITHMUS HSTS



Start

Webseite laden

Tracking ID vorhanden

Ja

Nein

Die Tracking ID 5 vom Server holen

Tracking ID setzen mittels JS

http://one.mytracking.com/set
http://three.mytracking.com/set

Der Server antwortet mit einem HSTS header

Tracking ID auslesen mittels JS

http://one.mytracking.com/get
-> HTTPS redirect -> 1
http://two.mytracking.com/get
-> Kein redirect -> 0
http://three.mytracking.com/get
-> HTTPS redirect -> 1

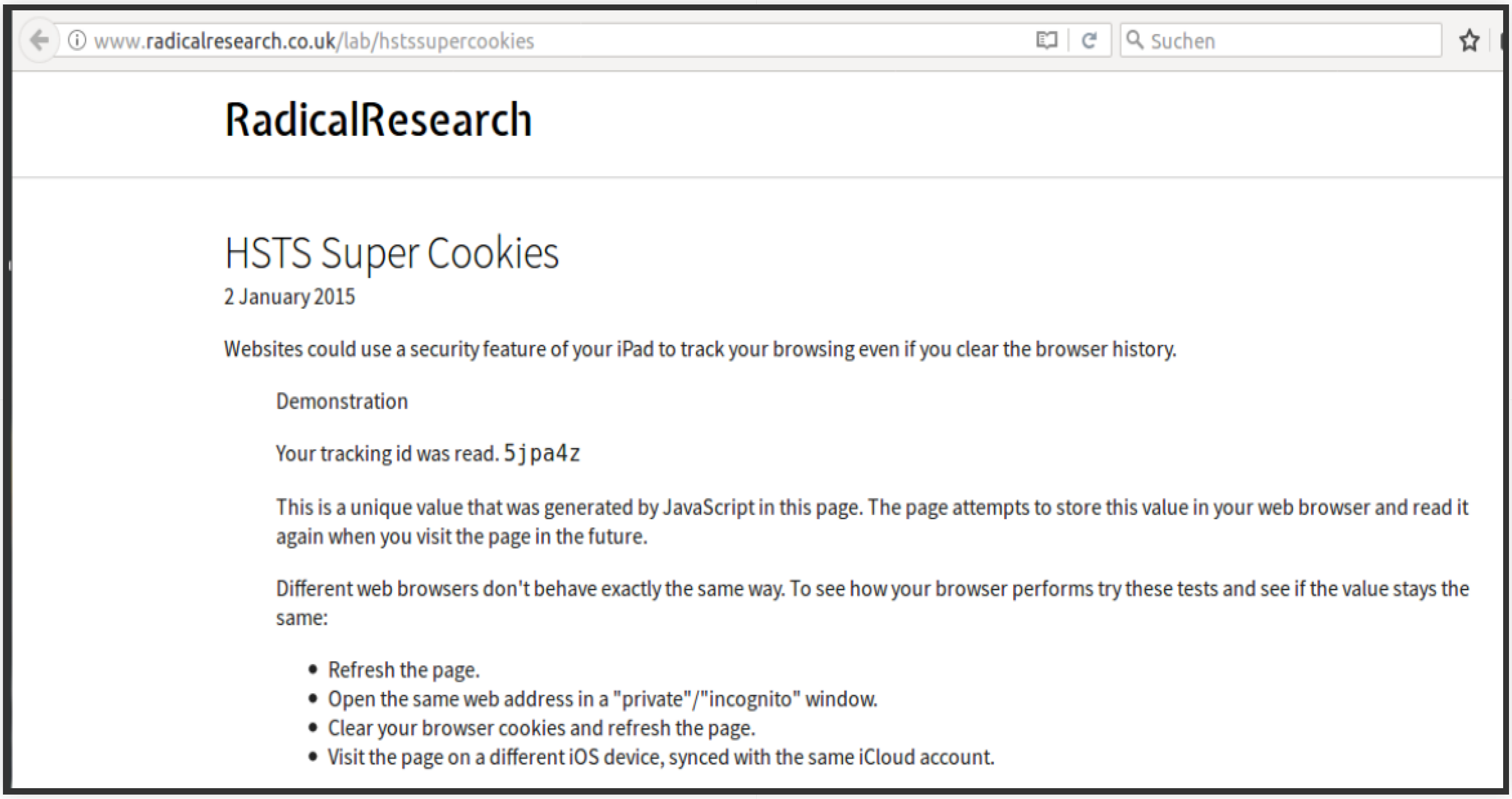
Der Server antwortet mit Redirect erfolgt (1) oder nicht (0)

1*2^0+0*2^1+1*2^2=5

Tracking ID 5 zum Server senden

Ende

http://www.radicalresearch.co.uk /lab/hstssupercookies



RadicalResearch

HSTS Super Cookies

2 January 2015

Websites could use a security feature of your iPad to track your browsing even if you clear the browser history.

Demonstration

Your tracking id was read. `5jpa4z`

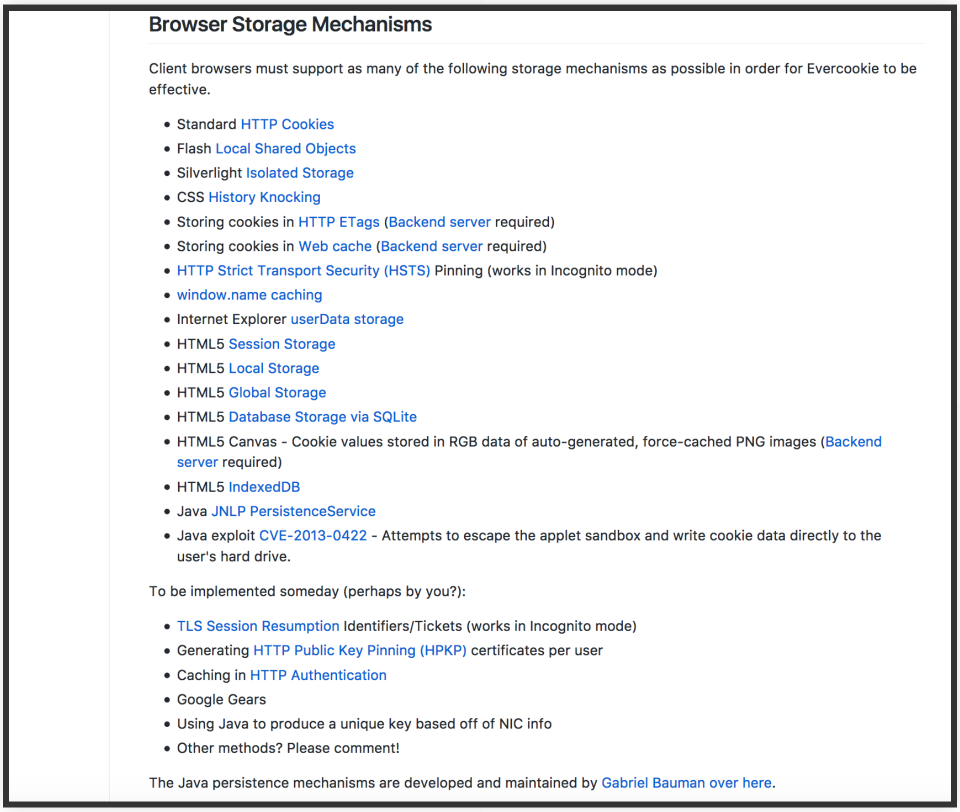
This is a unique value that was generated by JavaScript in this page. The page attempts to store this value in your web browser and read it again when you visit the page in the future.

Different web browsers don't behave exactly the same way. To see how your browser performs try these tests and see if the value stays the same:

- Refresh the page.
- Open the same web address in a "private"/"incognito" window.
- Clear your browser cookies and refresh the page.
- Visit the page on a different iOS device, synced with the same iCloud account.

Samy Kamkar

https://github.com/samyk/evercookie



Browser Storage Mechanisms

Client browsers must support as many of the following storage mechanisms as possible in order for Evercookie to be effective.

- Standard HTTP Cookies
- Flash Local Shared Objects
- Silverlight Isolated Storage
- CSS History Knocking
- Storing cookies in HTTP ETags (Backend server required)
- Storing cookies in Web cache (Backend server required)
- HTTP Strict Transport Security (HSTS) Pinning (works in Incognito mode)
- window.name caching
- Internet Explorer userData storage
- HTML5 Session Storage
- HTML5 Local Storage
- HTML5 Global Storage
- HTML5 Database Storage via SQLite
- HTML5 Canvas - Cookie values stored in RGB data of auto-generated, force-cached PNG images (Backend server required)
- HTML5 IndexedDB
- Java JNLP PersistenceService
- Java exploit CVE-2013-0422 - Attempts to escape the applet sandbox and write cookie data directly to the user's hard drive.

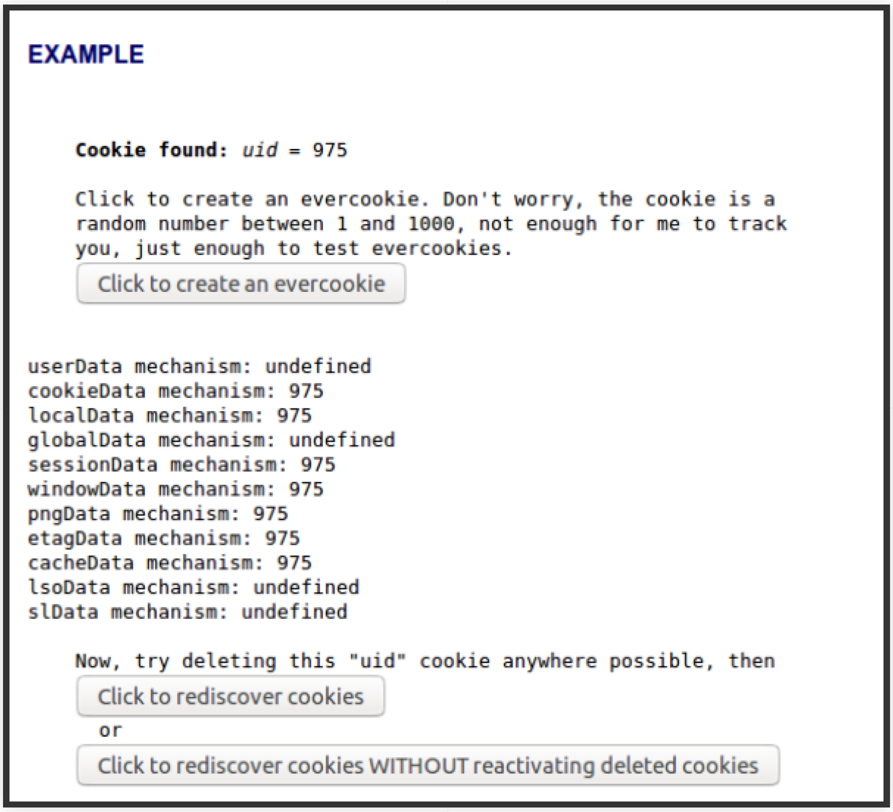
To be implemented someday (perhaps by you?):

- TLS Session Resumption Identifiers/Tickets (works in Incognito mode)
- Generating HTTP Public Key Pinning (HPKP) certificates per user
- Caching in HTTP Authentication
- Google Gears
- Using Java to produce a unique key based off of NIC info
- Other methods? Please comment!

The Java persistence mechanisms are developed and maintained by Gabriel Bauman over here.

SAMY KAMKAR - BEISPIEL

https://samy.pl/evercookie/



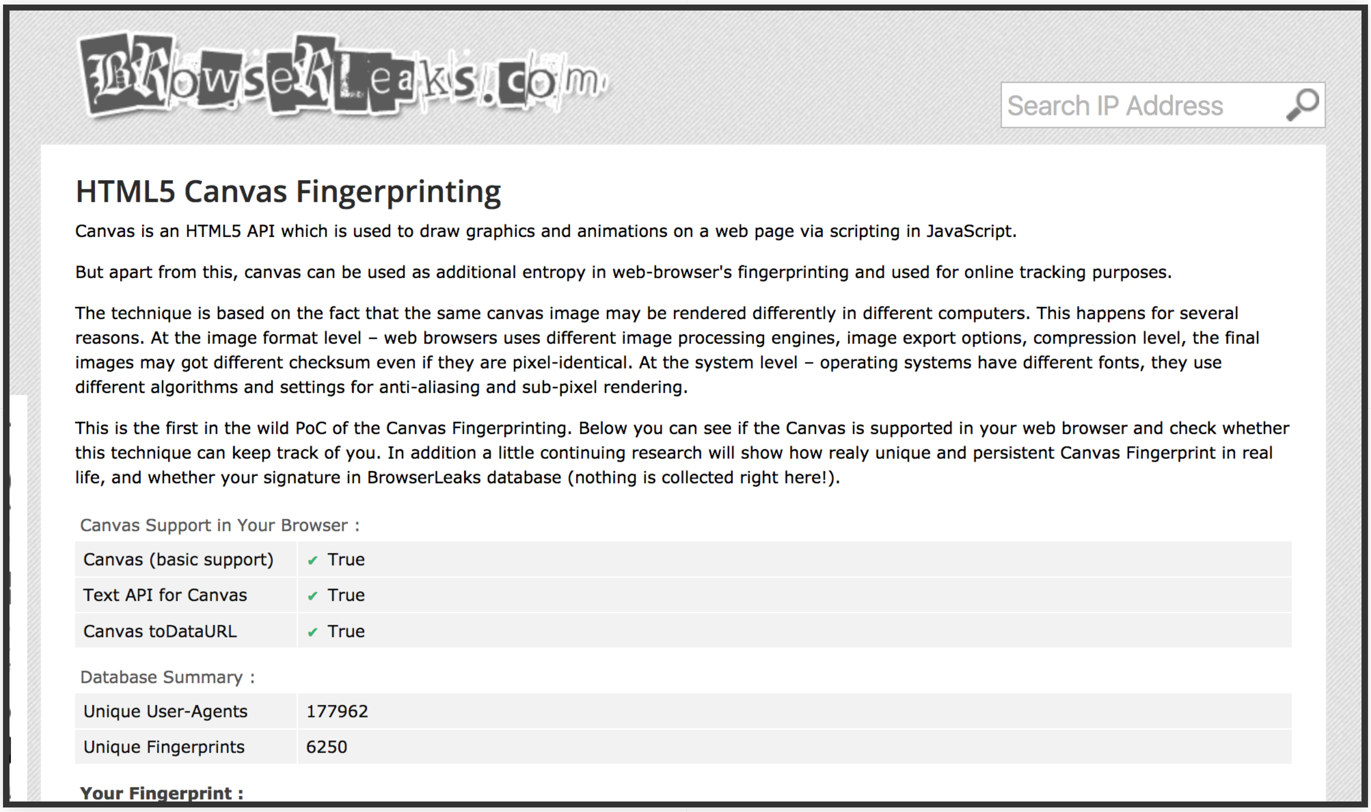
EXAMPLE

```
    Cookie found: uid = 975

    Click to create an evercookie. Don't worry, the cookie is a
    random number between 1 and 1000, not enough for me to track
    you, just enough to test evercookies.
```

```
userData mechanism: undefined
cookieData mechanism: 975
localData mechanism: 975
globalData mechanism: undefined
sessionData mechanism: 975
windowData mechanism: 975
pngData mechanism: 975
etagData mechanism: 975
cacheData mechanism: 975
lsoData mechanism: undefined
slData mechanism: undefined

    Now, try deleting this "uid" cookie anywhere possible, then
```

Click to rediscover cookies
or
Click to rediscover cookies WITHOUT reactivating deleted cookies

https://browserleaks.com/canvas



HTML5 Canvas Fingerprinting

Canvas is an HTML5 API which is used to draw graphics and animations on a web page via scripting in JavaScript.

But apart from this, canvas can be used as additional entropy in web-browser's fingerprinting and used for online tracking purposes.

The technique is based on the fact that the same canvas image may be rendered differently in different computers. This happens for several reasons. At the image format level – web browsers uses different image processing engines, image export options, compression level, the final images may got different checksum even if they are pixel-identical. At the system level – operating systems have different fonts, they use different algorithms and settings for anti-aliasing and sub-pixel rendering.

This is the first in the wild PoC of the Canvas Fingerprinting. Below you can see if the Canvas is supported in your web browser and check whether this technique can keep track of you. In addition a little continuing research will show how realy unique and persistent Canvas Fingerprint in real life, and whether your signature in BrowserLeaks database (nothing is collected right here!).

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	177962
Unique Fingerprints	6250

Your Fingerprint :

ZUSAMMENFASSUNG

FRAGEN?