Research by Samy Kamkar & Matt Stofko @ 24th Degree, Inc.
research@samy.pl / http://samy.pl
June 28, 2011

Summary

www.hulu.com sets various cookies on any user's computer that visits the website to identify the user and track other information. However, www.hulu.com specifically includes at least two persistent, respawning cookies that can be used to track the individual even after the user intentionally removes all HTTP cookies to prevent being tracked.

Both cookies are readable by www.hulu.com itself at any time, however the cookies are set by Javascript/Flash applications on different domains. One of these cookies is set from huluim.com, owned by Hulu, LLC, while the other is set from kissmetrics.com, a popular online analytics platform.

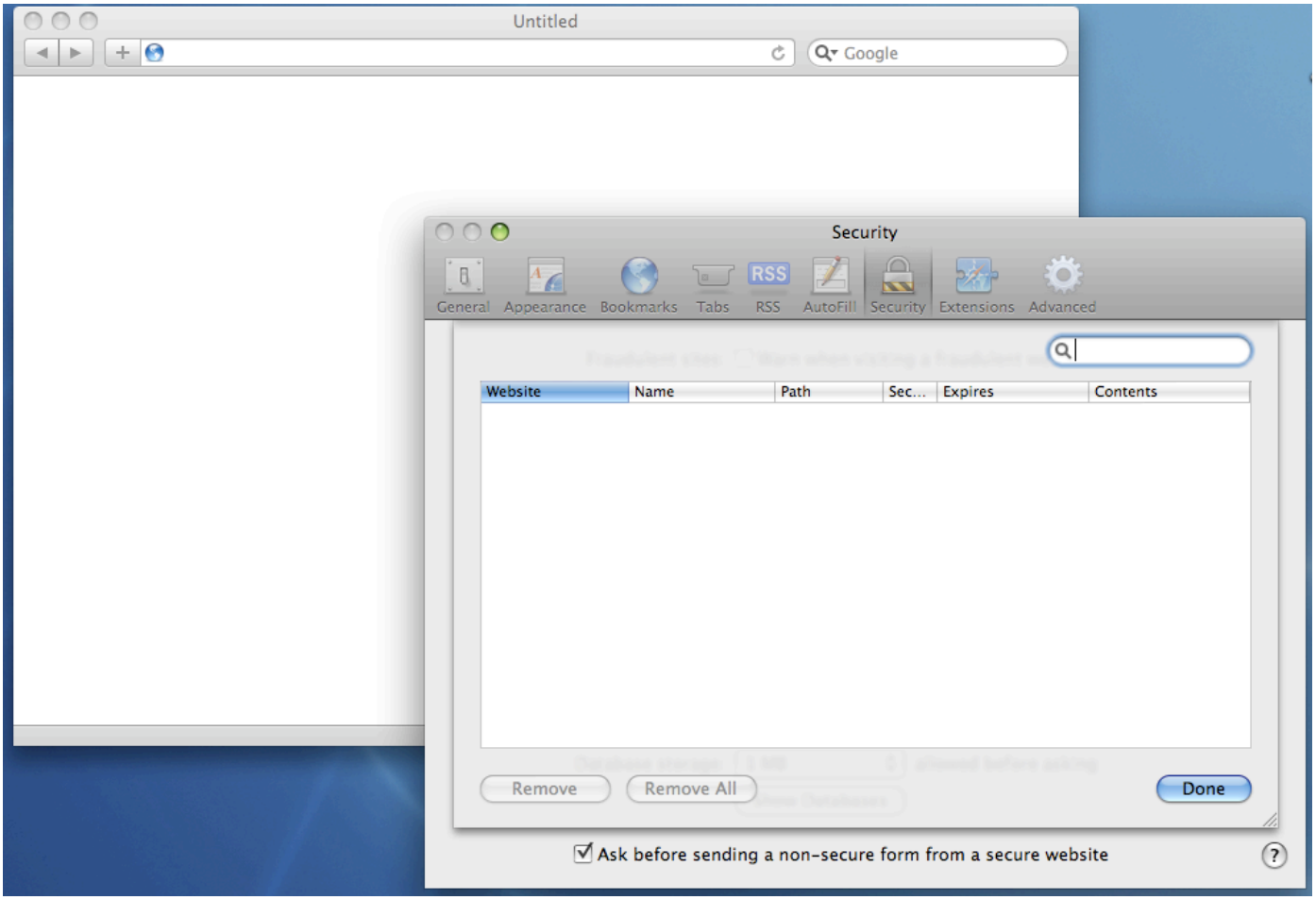
When visiting www.hulu.com and documenting the cookies set, then deleting all HTTP cookies and revisiting www.hulu.com, we find that the original values set in the cookies remain the same. This is because code on both huluim.com and kissmetrics.com are using HTML5 Local Storage and Flash Local Shared Objects (LSO) respectively to store the same unique identifiers in a different location. In this scenario, even when the original HTTP cookies have been deleted by the user, revisiting www.hulu.com allows the site to discover the original identifiers in HTML5 Local Storage and Flash LSO and then reset the HTTP cookies with the same value rather than a new, unique value evading the user's attempt to delete these unique identifiers.

The only way to acquire a new, unique value for these cookies is to delete not only the HTTP cookies are most web users are familiar with, but also to delete the related Flash LSOs and several HTML5 Local Storage objects which in many cases is quite complex for the average user.

These tests are confirmed in the Safari browser, however the same results have been found in other browsers.

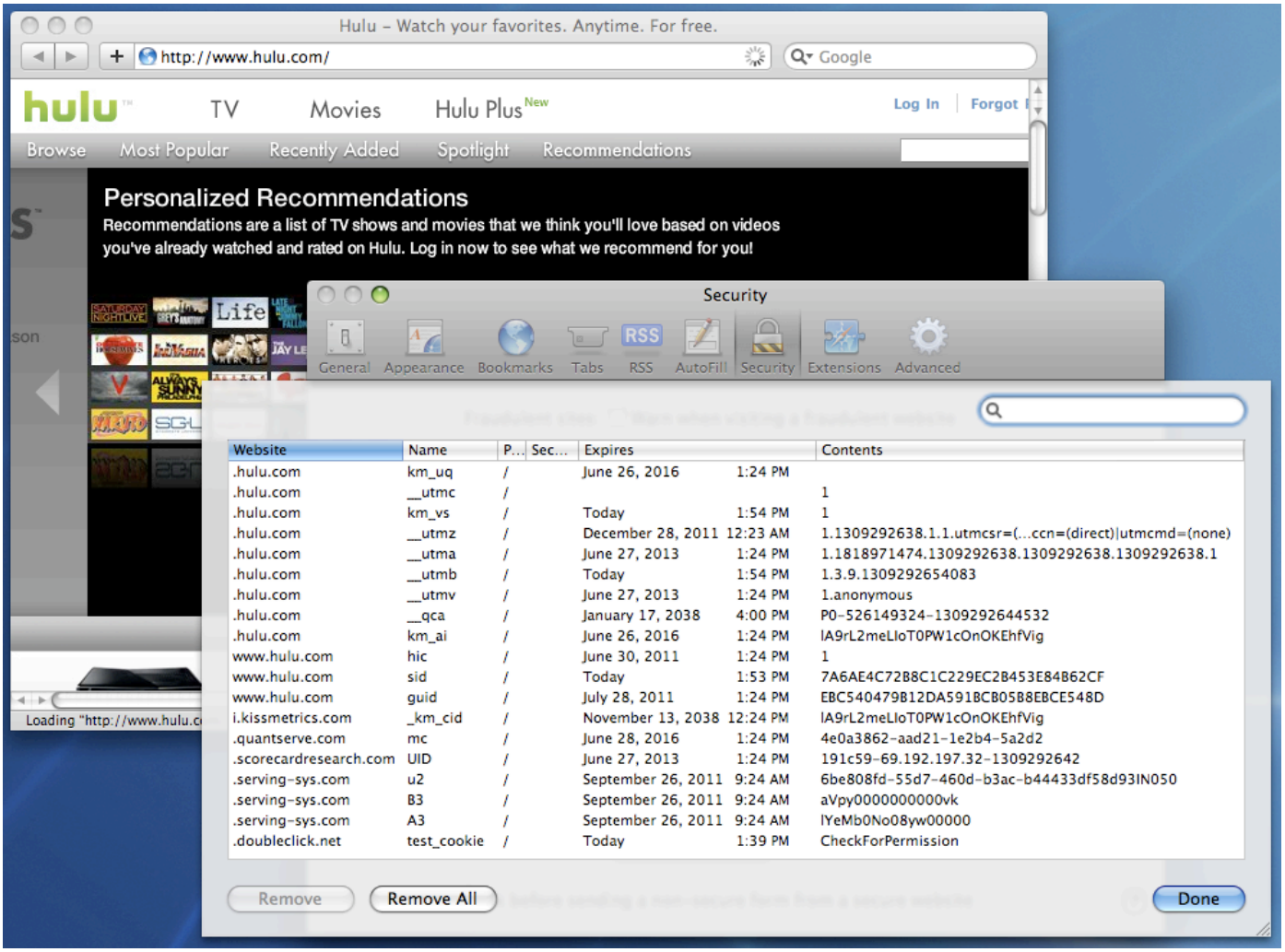
Initial Findings

Here is our clean Safari with no cookies:

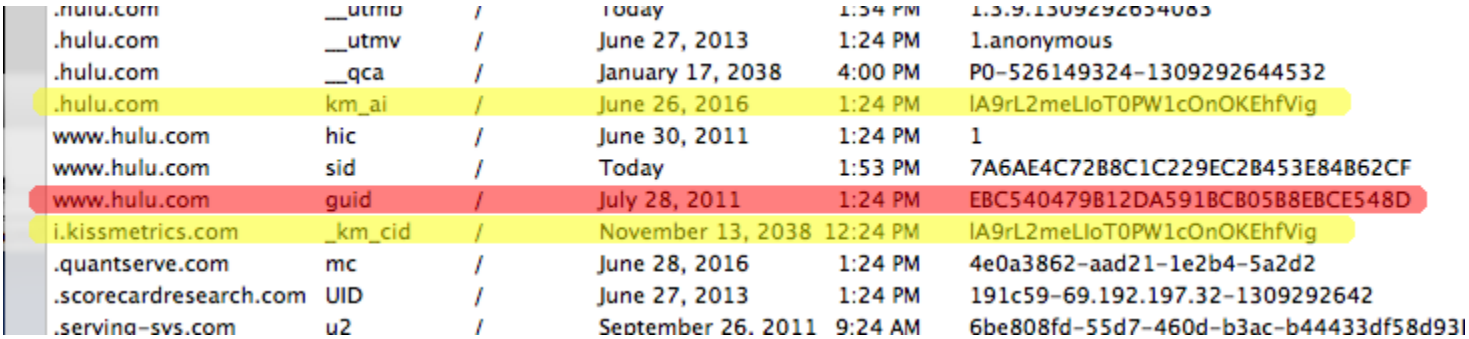


Research by Samy Kamkar & Matt Stofko @ 24th Degree, Inc.
http://samy.pl -- research@samy.pl

Upon an initial visit to http://www.hulu.com, the following cookies are set:

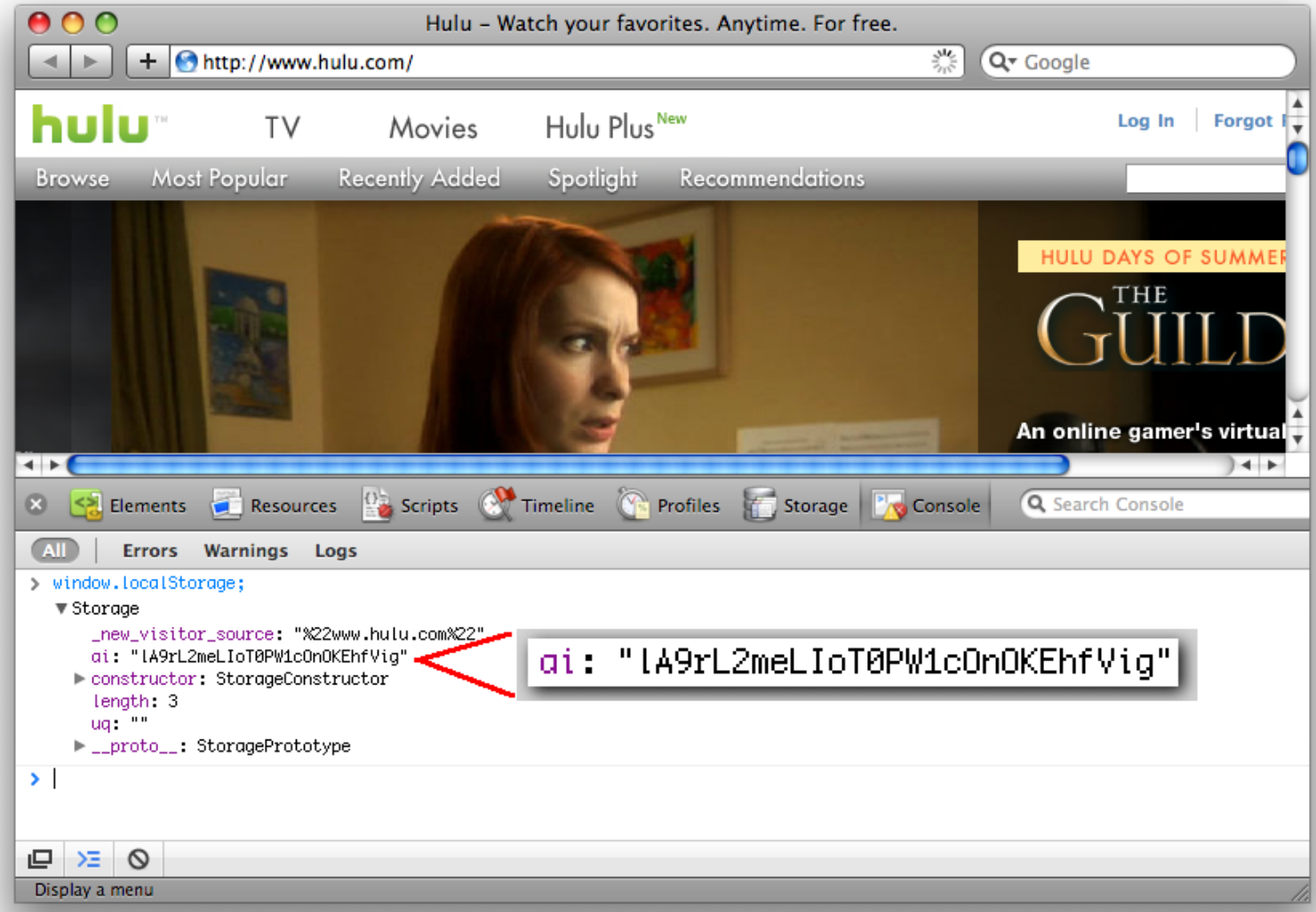


The three cookies we are interested in are highlighted below



Research by Samy Kamkar & Matt Stofko @ 24th Degree, Inc.
http://samy.pl -- research@samy.pl

The `km_ai` cookie has an identical value to the `_km_cid` cookie (as set by kissmetrics.com). It is also set in the browser's HTML5 Local Storage



We also have a cookie named `guid` as set by www.hulu.com.
The `guid` is interesting because it is also set in a Flash object (Flash LSO aka Flash cookie) which we extract using `strings`:

```
% strings Library/Preferences/Macromedia/Flash\ Player/
\#SharedObjects/*/www.hulu.com/*
OTCSO
BeaconService

computerguid
 EBC540479B12DA591BCB05B8EBCE548D
%
```

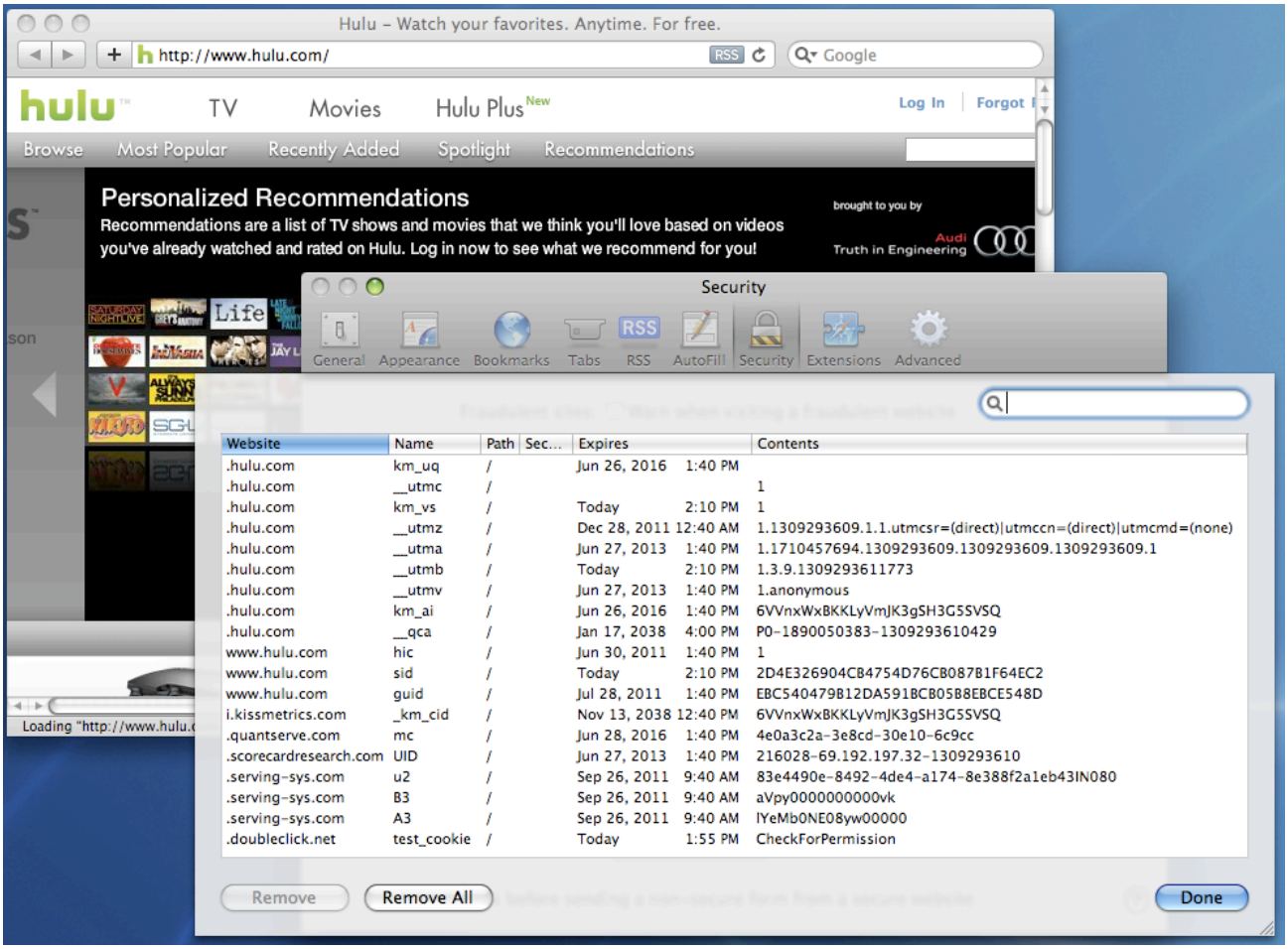
Flash LSOs (Flash Cookies) are not cleared when using the normal methods in a web browser to clear personal data, which is a sign this data in `guid` and `computerguid` will be used to identify a user against their wishes if they decide to delete their cookies.

The Test

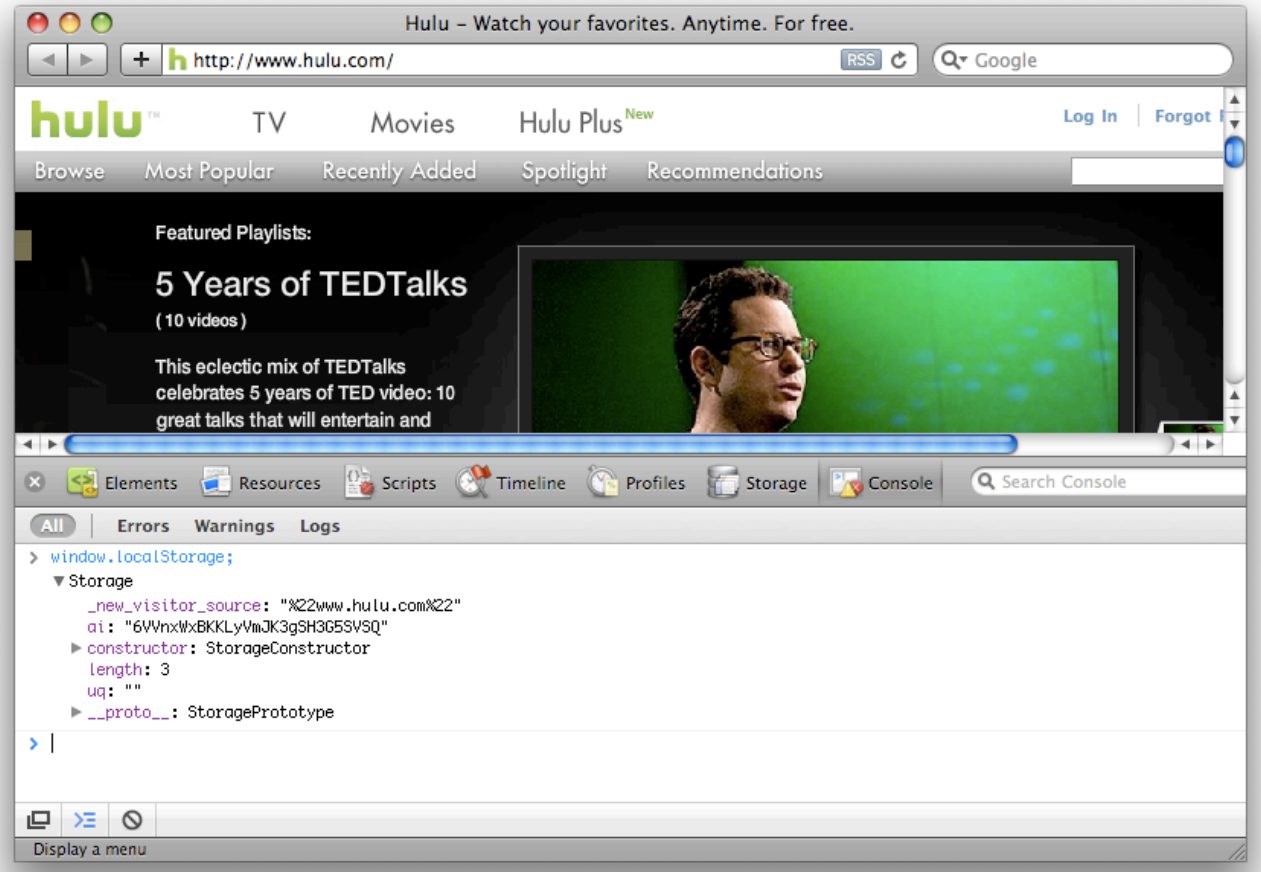
Now that we've identified the cookies we are interested in, a full reset of the browser is done to see how persistent they truly are.

After deleting all HTTP cookies, Flash LSOs, and HTML5 Local Storage, we revisit www.hulu.com. We can see this was successful in removing these cookies, as we now have new values. However this is not typical or practical for most web users and requires some level of expertise and knowledge to find and delete this data.

HTTP cookies:



HTML5 Local Storage:



Flash LSO:

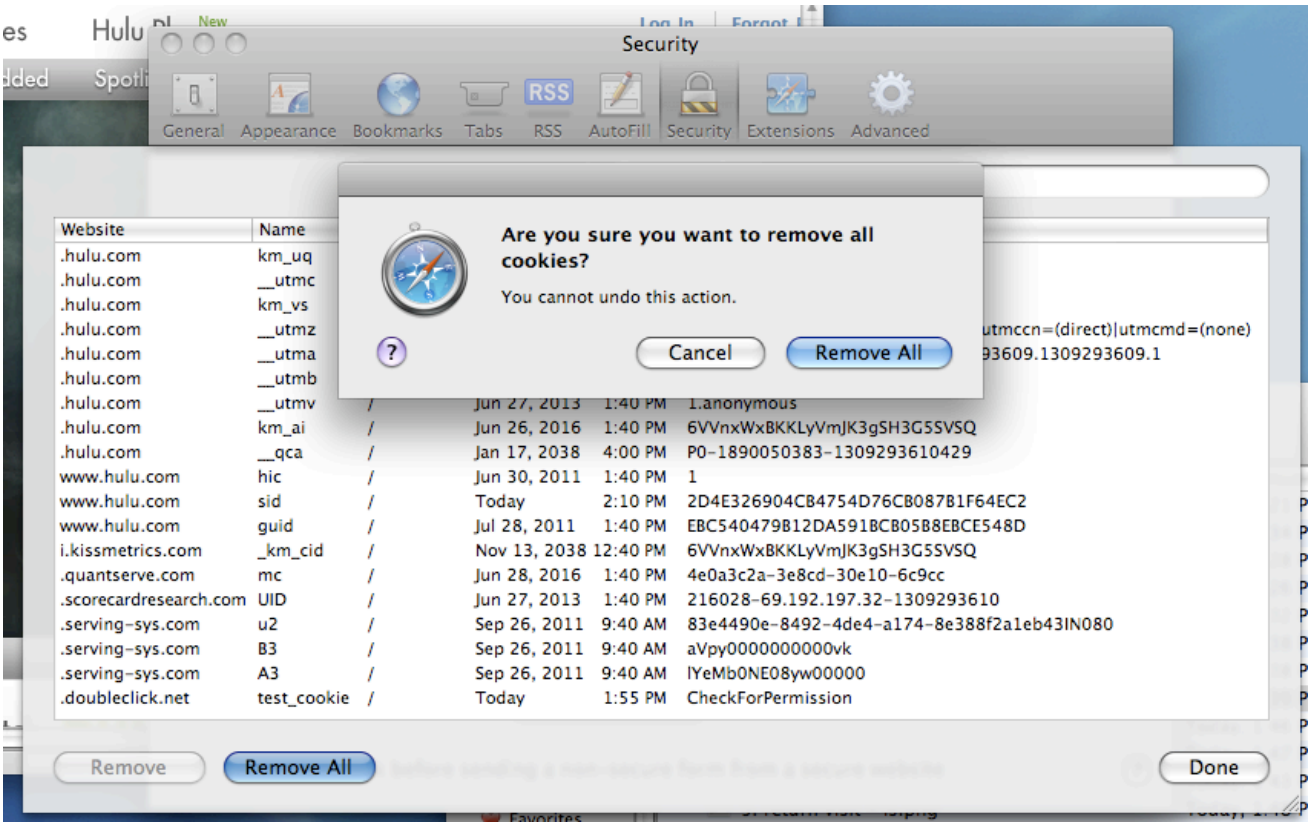
```
%  strings Library/Preferences/Macromedia/Flash\ Player/
\#SharedObjects/*/www.hulu.com/*
OTCSO
BeaconService

computerguid
 EBC540479B12DA591BCB05B8EBCE548D
%
```

In summary, this return visit to hulu.com set the following cookies:

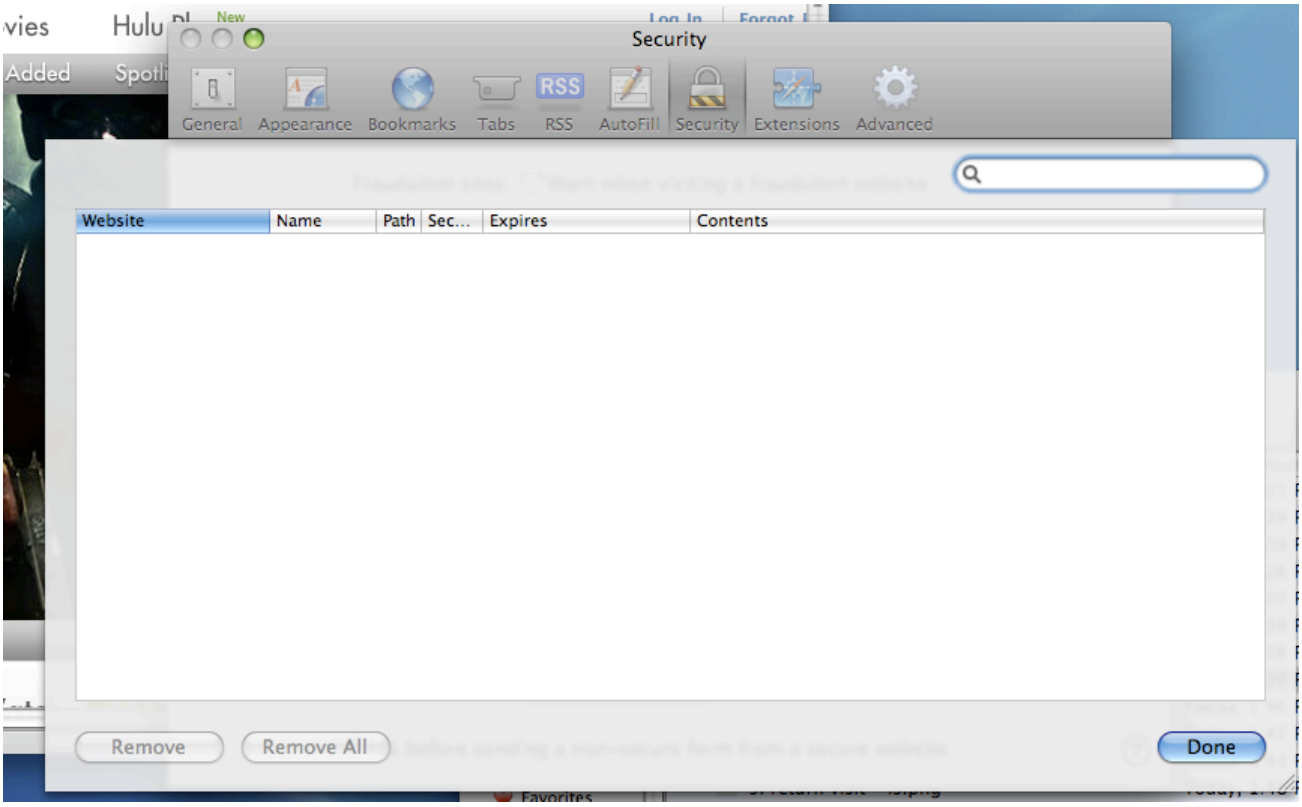
Name	Value	Domain	Type
guid	EBC540479B12DA591BCB05B8EBCE548D	www.hulu.com	HTTP
km_ai	6VVnxWxBKKLyVmJK3gSH3G5SVSQ	.hulu.com	HTTP
_km_cid	6VVnxWxBKKLyVmJK3gSH3G5SVSQ	i.kissmetrics.com	HTTP
computerguid	EBC540479B12DA591BCB05B8EBCE548D	www.hulu.com	Flash
ai	6VVnxWxBKKLyVmJK3gSH3G5SVSQ	www.hulu.com	HTML5 Local Storage

We now have two unique IDs stored in five different places. These were previously removed by doing a full reset of the browser (not typical for the average computer user as it can be a manual process or requires special software).

Now we use the built-in mechanism in Safari to remove all HTTP cookies, e.g.:

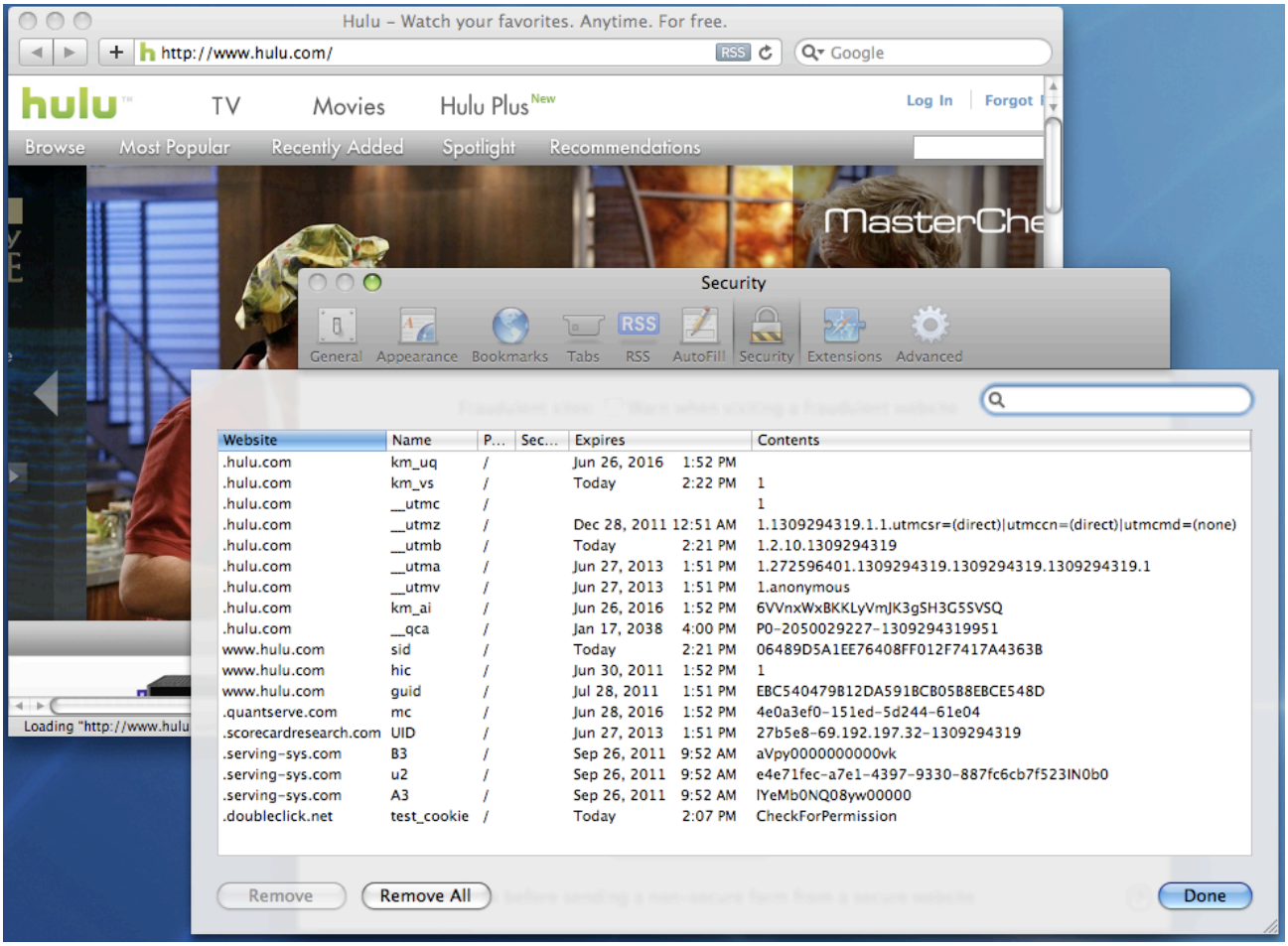


Our HTTP cookies are now empty:



Research by Samy Kamkar & Matt Stofko @ 24th Degree, Inc.
http://samy.pl -- research@samy.pl

We now revisit www.hulu.com:



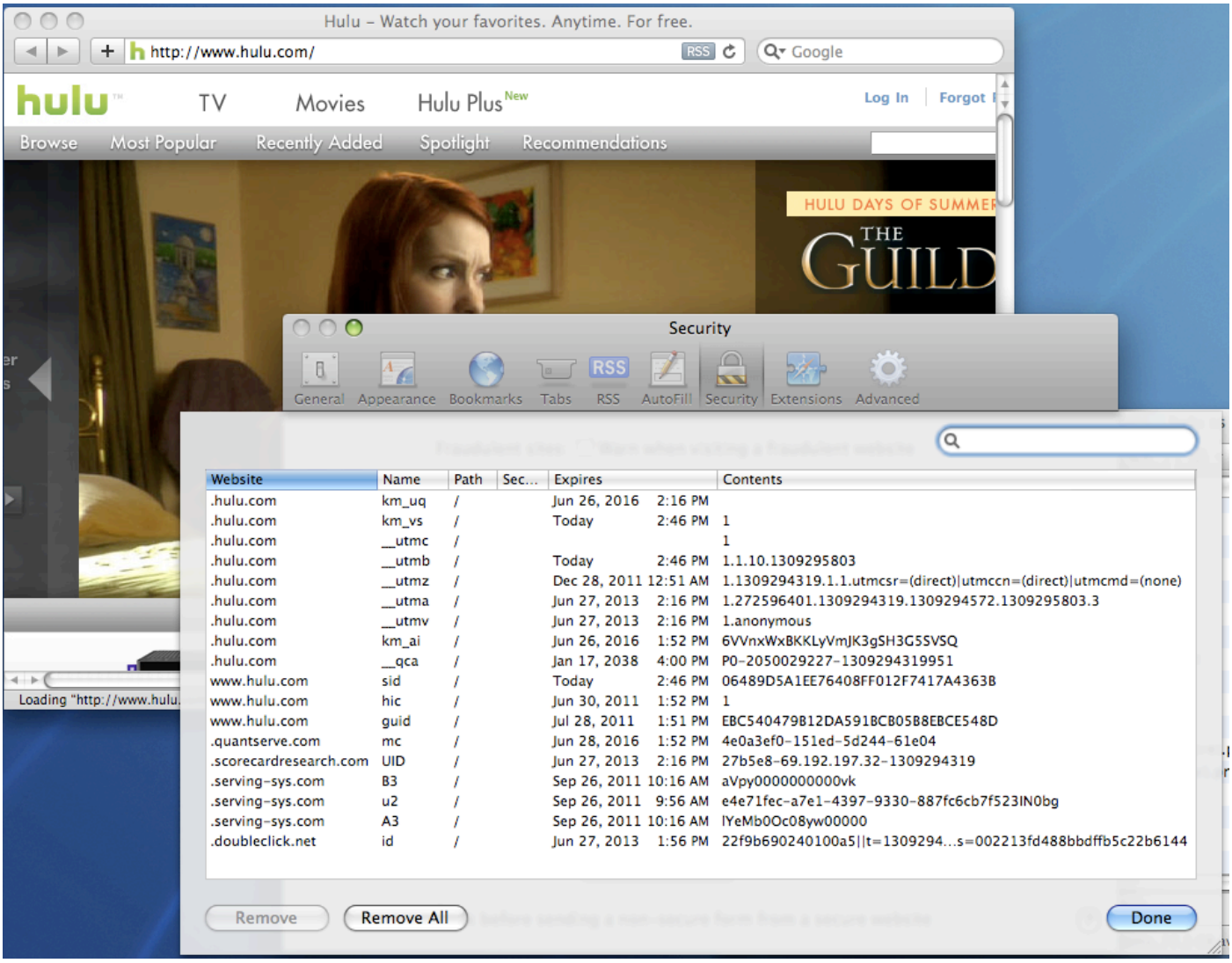
We can see the `km_ai` and `guid` cookies have returned with their old values that were set in the HTTP cookies originally, even after we've deleted them. This demonstrates that www.hulu.com is actively trying to keep the same unique ID for these specific cookies against the user's wishes.

Note the cookie set by kissmetric.com did not return, however the cookie of the same value from hulu.com did.

Now we will delete the Flash LSO for www.hulu.com, which contains the `computerguid` cookie (which is tied to the `guid` HTTP cookie).

```
% ls -dl Library/Preferences/Macromedia/Flash\ Player/\#SharedObjects/*/www.hulu.com
zsh: no matches found: Library/Preferences/Macromedia/Flash Player/#SharedObjects/*/www.hulu.com
```

Now return to www.hulu.com:



Notice our HTTP cookies are still intact.

Running the `strings` application on the www.hulu.com Flash LSO while the page was loading yields similar results as deleting the HTTP cookies in question:

(Initial load)

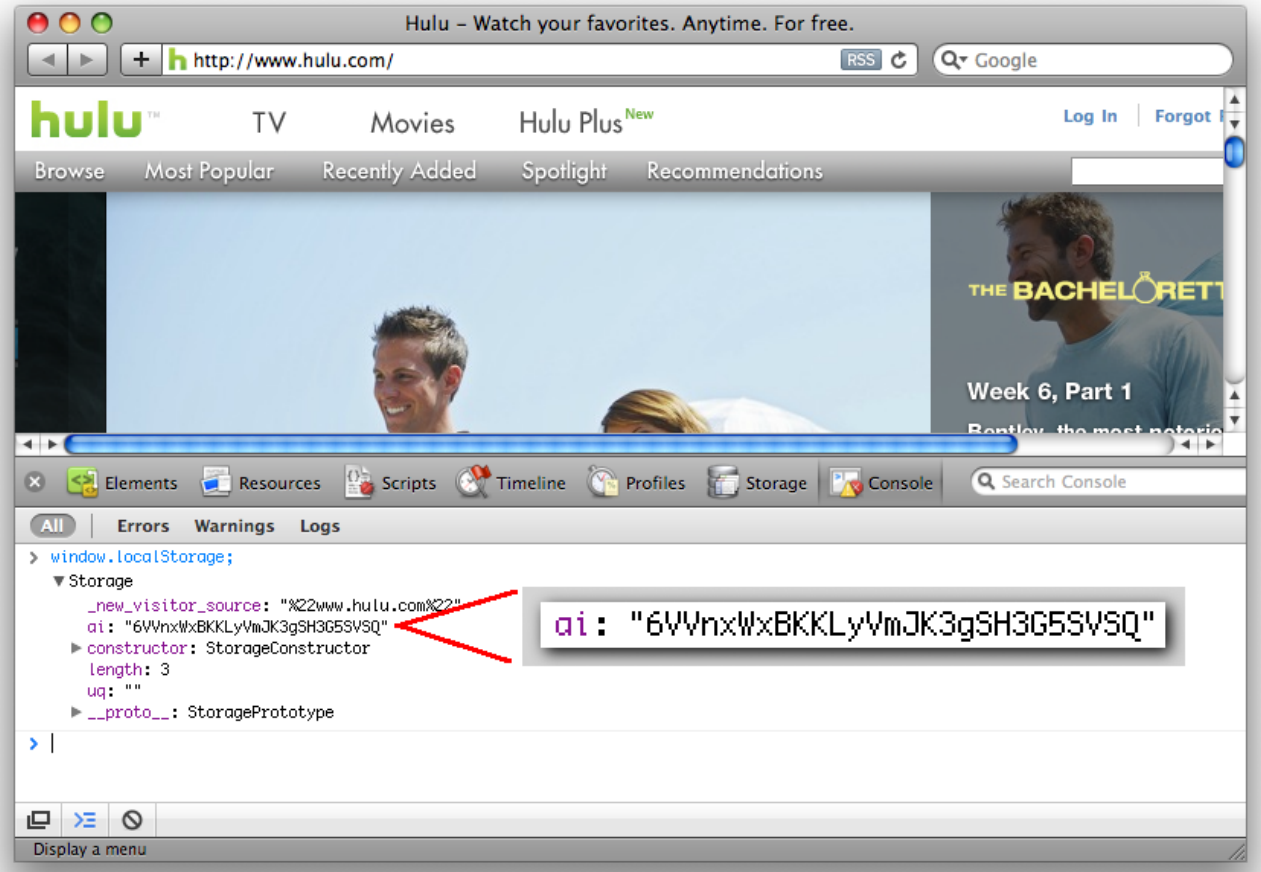
```
% strings Library/Preferences/Macromedia/Flash\ Player/
\#SharedObjects/*/www.hulu.com/*
OTCSO
BeaconService

computerguid
 DD28CE69282137025B3E58A691018079 (note the new ID while page loads)

(www.hulu.com is now finished loading)
% strings Library/Preferences/Macromedia/Flash\ Player/
\#SharedObjects/*/www.hulu.com/*
OTCSO
BeaconService

computerguid
 EBC540479B12DA591BCB05B8EBCE548D (original ID from the HTTP cookie)
%
```

This shows that www.hulu.com resets the Flash LSO `computerguid` cookie from the `guid` HTTP cookie if it exists, essentially respawning the Flash LSOs when possible.

Now doing the same for the HTML5 Local Storage and the `km_ai` cookie:

```
% ls Library/Safari/LocalStorage/http_www.hulu.com_0.localstorage
Library/Safari/LocalStorage/http_www.hulu.com_0.localstorage
% rm Library/Safari/LocalStorage/http_www.hulu.com_0.localstorage
% ls Library/Safari/LocalStorage/http_www.hulu.com_0.localstorage
ls: Library/Safari/LocalStorage/http_www.hulu.com_0.localstorage: No
such file or directory
```

Returning to www.hulu.com shows the HTML5 Local Storage value is also respawned from the HTTP cookie:



How the Cookies are Set

The `guid` cookie is set by JavaScript, referenced on ww.hulu.com by:

```
<script src="http://static.huluim.com/system/
hulu_102685_0624004225.js" type="text/javascript"></script>
```

This Javascript can be downloaded directly from: http://static.huluim.com/system/hulu_102685_0624004225.js

There is separate JavaScript on www.hulu.com that deals with the Flash LSOs (`computerguid` cookie)

```
<script type="text/javascript" charset="utf-8">/*<![CDATA[*/
  Event.observe(window, "load", function() {
    return;
    setTimeout(function() {
      var guidManager = $('pguid');
      if (guidManager) {
        var guid = guidManager.getGUID();

        if (Math.abs(Math.floor(parseInt(guid.substring(guid.length - 2), 16) / 2.55)
- 76) < 0.001) {

var so = new SWFObject("/fap.swf?cb=" + cbString(), "fap", "1", "1", "10.1");
          so.addParam("bgcolor", "#000000");
          so.addParam("wmode", "transparent");
          if (!VersionCheck.write(so, "fap-container")) {

var so2 = new SWFObject("/ver_beacon.swf?cb=" +
cbString(), "ver_beacon", "1", "1", "9");
            so2.addParam("bgcolor", "#000000");
            so2.addParam("wmode", "transparent");
            VersionCheck.write(so2, "fap-container")
          }
        }
      }
    }, 3000);
  });
/*]]>*/</script>
```

The `ai`, `km_ai`, and `_km_cid` cookies are set by this JavaScript, referenced on ww.hulu.com by `_kms('//doug1izaerwt3.cloudfront.net/5a68d120b211c810289fc36493663648821d58aa.1.js');`

The Javascript code can be downloaded directly from http://doug1izaerwt3.cloudfront.net/5a68d120b211c810289fc36493663648821d58aa.1.js

Additional Respawning KISSmetrics Sites

These sites were discovered to be using the `km_ai` respawning cookie from KISSmetrics:

about.me
adroll.com
assistly.com
atlassian.com
babypips.com
blueglass.com
bufferapp.com
crazyegg.com
designyoutrust.com
ehealthforum.com
favstar.fm
friend.ly
getharvest.com
goanimate.com
graphpaperpress.com
hasoffers.com
hootsuite.com
hulu.com
inspirationfeed.com
jobscore.com
kissmetrics.com
olark.com
peerindex.net
plancast.com
realmacsoftware.com
rockettheme.com
runkeeper.com
seomoz.org
shoedazzle.com
skitch.com
slidedeck.com
slideshare.net
spotify.com
squareup.com
suite101.com
suite101.de

Research by Samy Kamkar & Matt Stofko @ 24th Degree, Inc.
http://samy.pl -- research@samy.pl

suite101.net
wibiya.com
widgetbox.com
wikinvest.com
wikispaces.com