# Blog

## Flash Cookie Forensics

28 aug 2009

**Posted by Chad Tilbury**
**Filed under Computer Forensics, Evidence Analysis**

**10 comments**

Flash cookies have been a hot topic lately with the release of an excellent research paper titled Flash Cookies and Privacy. Flash Cookies, or local Shared Objects in Macromedia parlance, are a great example of a forensic artifact that has existed for a long time but was virtually ignored until someone decided to shine some light on it. Whenever I see new research about problematic privacy controls, I immediately get out my notepad, because I know that I am going to find some great artifacts that can help in my forensic investigations.

**First some basics:**

- Macromedia Flash has become ubiquitous on the web, providing features such as streaming video and a "rich client" experience. Many of the most popular sites on the web are dependent on Flash, and thus a high percentage of Internet users have installed the Flash plug-in.
- The Flash standard incorporates local Shared Objects (LSOs), which allow data (such as preferences) to be stored in the local Flash instance on a user's machine.
- LSOs are stored as individual files with a .SOL file extension. By default they are less than 100 kB in size and have no expiration (unlike traditional HTTP cookies).
- I have found .SOL files in two locations on the local system: %user profile%\Application Data\Macromedia\Flash Player **and** %user profile%\Application Data\Macromedia\Flash Player\#SharedObjects\\ (%user profile% is shorthand for where the user folders reside - typically C:\Documents and Settings\\ on a XP system). For Vista analysis, you will need to look in the Roaming folder within %user profile%.
- LSOs are not browser based, so there is currently no easy way for the average user to remove them (simply deleting the files does the job, but a user would need to know where they are located). This makes LSOs very persistent on the local system.

**Analysis**

For our purposes, the term Flash Cookies is an apt descriptor for LSOs since they give very similar information to what we find in traditional HTTP cookies. Those of you that have taken the SANS SEC 408 Computer Forensic Essentials course will recall that HTTP cookies can give us the following information:

Websites that were visited

Macromedia Flash requires that LSOs be stored hierarchically by domain. This is one way it is able to enforce the rule that each domain may only store up to 100k on the local system. From our perspective, this gives us a very handy means for quickly reviewing the sites visited.

**Figure 1: Directory listing displaying LSO domains**

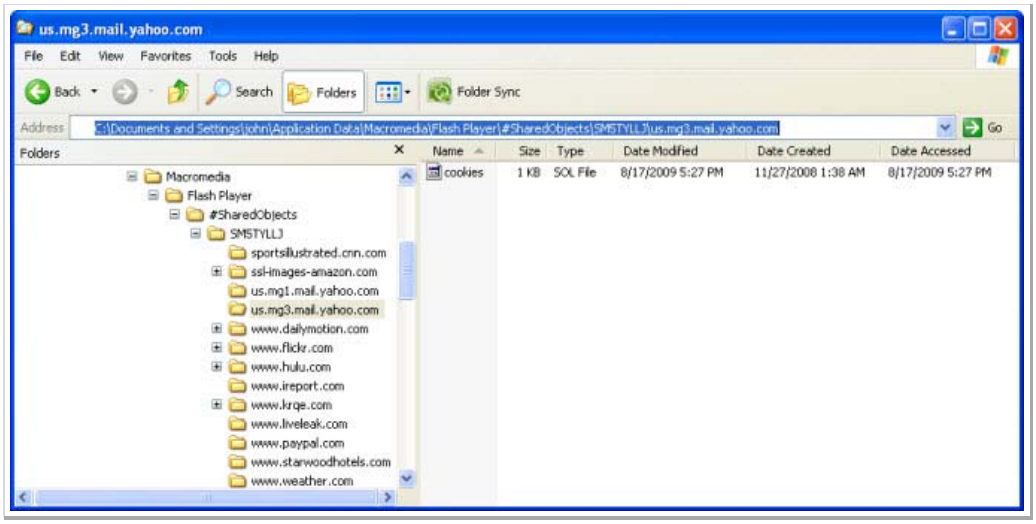
RSS

Search Blog:

Search

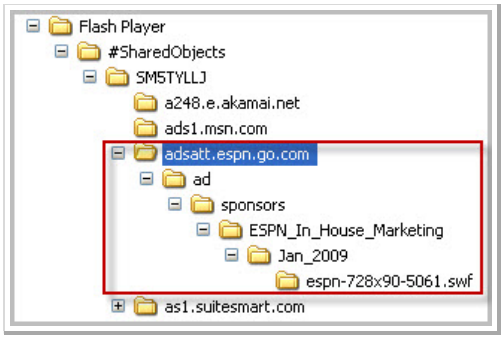
Categories

Advanced Persistent Threat (4)
apt (3)
artifact analysis (64)
Book Reviews (4)
Browser Forensics (29)
Case Leads (94)
Certification and License (9)
Challenge (7)
Community SANS Events (2)
Computer Forensic Hero (2)
Computer Forensics (486)
Computer Forensics and IR Summit (18)
DFIR Summit (1)
Digital Forensic Law (42)
Drive Encryption (15)
eDiscovery (43)
Email Investigations (15)
Ethics (7)
Evidence Acquisition (104)
Evidence Analysis (171)
Getting Started (15)
Incident Response (122)
Linux IR (24)
Malware Analysis (56)
Memory Analysis (39)
Mobile Device Forensics (47)
Network Forensics (39)
Registry Analysis (24)
Reporting (16)
Reverse Engineering (23)
SANS Institute (16)
SIFT Workstation (6)




One thing to note is that Flash based advertisements also have the ability to save LSOs. This is important because in some cases we can't necessarily conclude that it was the user's intent to access the domain. The origin of the LSO is often obvious (see Figure 2), but further testing or additional artifacts may be necessary to make any definitive conclusions.

**Figure 2: LSO saved from a Flash advertisement**




Local user account that visited the site

Recall that the .SOL files are located within the %user profile% folder, indicating the account that was logged in when the LSO was saved.

When thesite was first and last visited

Since the .SOL files are saved individually, we have a nice set of file system timestamps to utilize. On Windows XP (which has Access time stamping on by default) we can use the Access Time to tell us when the LSO was last read. This can potentially tell us when the site was last visited, but we have to be careful since I am not aware of any standard that *requires* an issuing site to read the LSO. It is certainly in their best interests and in my testing all appear to be doing so, but if the site does not read the LSO for some reason, the Access time will not be updated.

The .SOL file Creation Time can potentially tell us when the site was first visited. Again, we are not assured that the LSO was created on the first visit to the site, so it is difficult to be conclusive. A better way of looking at this would be the "first known visit to the site". Other artifacts on the system may be able to corroborate this time or indicate an even earlier visit time.

So looking again at Figure 1, we can see that the first known visit to mg3.mail.yahoo.com was 11/27/2008 at 1:38am and the last known visit was 8/17/2009 at 5:27pm (local machine time).

Data stored by the website

Flash specifically attempts to obfuscate data within each LSO by controlling the format and forcing a binary serialization of any stored data. That being said, if you find a relevant file, don't overlook this data area. I have found interesting tidbits such as text-based location information storedby aweather website.

**Tools**

While not recommended as a forensic tool (primarily because it requires installation / execution on a live system), the Better Privacy Firefox extension is a great tool for identifying (and removing) LSOs on your local system. One of the best ways to learn about forensic artifacts is by reviewing them on a system with known behavior (i.e. your own system). The Better Privacy plug-in allows you to easily review (and manage) LSOs on a live system.

**Figure 3: Better Privacy Firefox Plug-in Screenshot**

Specials (1)
Timeline Analysis (20)
Training (14)
Uncategorized (4)
USB Device Analysis (12)
Windows IR (50)
Write Blockers (13)

## Recent Posts

Digital Forensic Case Leads : Flame On! The most sophisticated malware since...the last one, Higher Ed data breach and PowerShell forensics.

How to Extract Flash Objects From Malicious MS Office Documents

New version of Nmap, 60TB hard drives on the way, attacker trends, & a dissected web attack

Digital Forensic Case Leads: A Volume Shadow Copies Toolset Updated, Malware Binary Files Analysis Became Easier, Media and Mobile Forensics Analysis, And A Man Stabs His Computer!

Digital Forensic Case Leads: Report from the Forensic Expert Witness Conference, Judge: Viewing CP might NOT be possession, Mac crypto bug helps forensicators

## Recent Comments

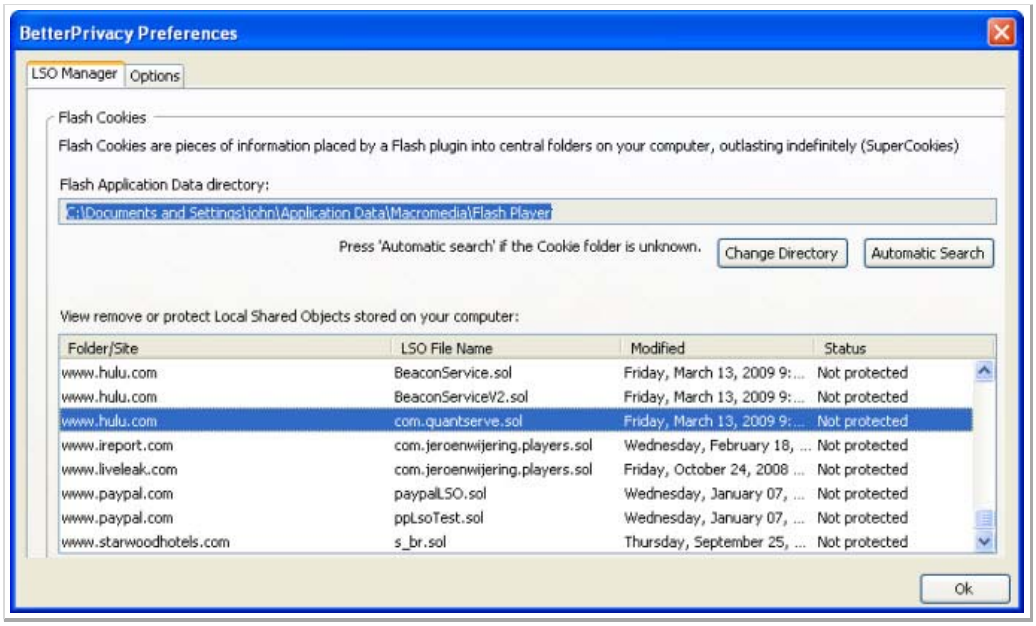
## Popular Posts

## Archives

Select Month

## Links

Log in
Entries RSS
Comments RSS
WordPress.com
WordPress.org




This is just a first look at Flash Cookies -- I encourage our readers to post any links or information they have discovered in the blog comments.

*Chad Tilbury, GCFA, has spent over ten years conducting computer crime investigations ranging from hacking to espionage to multi-million dollar fraud cases. He teaches FOR408 Windows Forensics and FOR508 Advanced Computer Forensic Analysis and Incident Response for the SANS Institute. Find him on Twitter @chadtilbury* or at http://ForensicMethods.com.

 Permalink | Comments RSS Feed - Post a comment | Trackback URL

10 Comments

### johnmccash

Here are some useful links for this topic:
http://forensicsfromthesausagefactory.blogspot.com/2009/04/adobe-flash-player-local-shared-objects.html
http://www.adobe.com/products/flashplayer/articles/lso/
http://en.wikipedia.org/wiki/Local_Shared_Object

### Vivek Rajan

Scary stuff considering that the LSO can resurrect browser cookies.

You can also use a shortcut for the directory %APPDATA%

I also found a folder %APPDATA%\macromedia\flashplayer\macromedia.com\support\flashplayer\sys If anyone is cleaning out the cookies they might miss this folder.

### Mike A.

The %APPDATA%\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol file contins Global prefernces set with the Adobe Flash Player Settings Manager (http://www.macromedia.com/support/documentation /en/flashplayer/help/settings_manager.html).

There are also files that contain Website specific preferences (e.g. %APPDATA%\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\#mail.google.com\settings.sol).

The settings.sol files are the ones you want to protect from deletion with BetterPrivacy or your preferences will be lost and restored to the default settings.

One discovery that I have found is even with everything deleted in %APPDATA%\Macromedia\Flash Player\#SharedObjects there is still a record of websites visited in the Global preferences file. The websites visited show up in the Adobe Flash Player Settings Manager and each site can be deleted individually.

### Dan Pixley

Don't be fooled by Firefox and Chrome's built-in private browsing either. They don't block Flash cookies:
http://danpixley.wordpress.com/2009/08/29/firefox-and-chrome-private-browsing-not-so-private/

### Aaron Ringo

On Mac:
Home->Library->Preferences->Macromedia->Flash Player->#SharedObjects-> and additionally
Home->Library->Preferences->Macromedia->Flash Player->macromedia.com->support->flashplayer->sys

They make you dig a little deep.

### hep-cat.de

Mac OS X: Flash-Cookies lschen...

Adobe Flash fllt nicht nur dadurch auf, dass es teilweise gravierende Sicherheitslcken enthlt und relativ hufig in alten und somit verwundbaren Versionen zum Einsatz kommt, sondern auch durch seine Unart Tracking-Cookies auf der Festplatte des Benu...

### laurence

most excellent analysis of tracking cookies, thanks.

### Rahul

Hi,
Excellent post from the forensics point of view. May I know that what would be the impact of removing these files from the macromedia folder ?

Thanks in advance.
Rahul Shrivastava.

### Clerkendweller

Thanks for pulling all this good information together into a single blog post (+comments).

### maxatwo

See http://www.maxa-tools.com/cookie.php for MAXA Cookie Manager, a windows tool that handles all kinds of cookies in a centralized way.
The Pro version allows to automatically handle cookies with White and Blacklists making sure you keep the ones you want, but delete the tracking cookies and web bugs.

## Post a Comment

*****Name

*****Email

Website

*****Anti-spam question:
Are rocks hard or soft?

*****Comment

Post Comment

* Indicates a required field.

## Latest Blog Posts

Digital Forensic Case Leads : Flame On! The most sophisticated malware sinc [...]
June 01, 2012 - 6:06 PM

How to Extract Flash Objects From Malicious MS Office Documents
May 29, 2012 - 8:33 PM

New version of Nmap, 60TB hard drives on the way, attacker trends, & a [...]
May 25, 2012 - 1:10 PM

## Latest Tweets @sansforensics

New #DFIR Blog Post: "Digital Forensic Case Leads : Flame On [...]
June 1, 2012 - 8:37 PM

Final Month before #DFIRSUMMIT - Register Now and get 10% of [...]
June 1, 2012 - 1:49 PM

Final Month before #DFIRSUMMIT - Register Now and get 10% of [...]
May 31, 2012 - 4:04 PM

## Latest Papers

Grow Your Own Forensic Tools: A Taxonomy of Python Libraries Helpful for Forensic Analysis
By Terrence OConnor

Integrating Forensic Investigation Methodology into eDiscovery
By Colin Chisholm

Mastering the Super Timeline With log2timeline
By Kristinn Gudjonsson

"This is awesome! We're seeing details that most people don't even know exist."
- John Wright, Info Tech, Inc.

"This course is filling in the blanks in my knowledge of how some things work. It is nice to know what the tools are doing."
- Douglas Couch, Purdue University

"I had taken several other forensic courses prior to this one, but none of them or their instructors made understanding forensic methodologies and techniques as clear and understandable as Rob Lee and this course has."
- Nathon Heck, Purdue