



MYSFACE
investigators.com



*MySpaceInvestigators.com is not associated with MySpace.com

MySpace.com Forensic Artifacts Keyword Searches:

By Sr. Detective Frank Zellers

Effective forensic examiners need the ability to perform keyword searches that yield specific, focused results. The more specific you can make your search strings, the more streamlined your results will be. When performing a keyword search for MySpace.com related artifacts, there are a few particularities to keep in mind. Once you understand the Myspace.com system of embedded syntax tags and messaging menus, you may be able to get more efficient search results.

Until recently, the most commonly used search strings for MySpace investigations included the terms, "friendID" or "FriendID=user-account-number." While these search terms are useful, they present a major disadvantage in that they often result in thousands of hits when greater specificity is needed. In my search for a better solution, I studied individual MySpace profiles by viewing source data as well as HTML syntax to look for common areas within the pages. I discovered that *ColdFusion* (the web application responsible for MySpace.com architecture) assigns a unique tag to each of the different pages within MySpace.

MySpace Data Tags

When viewing "Page Source Data" within the MySpace website, note that each area has its own unique data tag. The data tags are generated by the server website application, *ColdFusion*. *ColdFusion* Markup Language (CFML) includes a set of tags applied to web pages that allow users to interact with data sources, manipulate data, and display output. CFML tag syntax is similar to HTML element syntax. The data tags below appear in MySpace.com pages:

<!-- MailInbox -->	-User message inbox
<!-- MailReadMessage -->	- User mail message
<!-- MailReply -->	-User reply to message/ bulletin
<!-- Bulletin -->	- Bulletin inbox
<!-- BulletinRead -->	- Bulletin message
<!-- MailForward -->	-Forward mail message
<!-- MailTrashBox -->	- Messages in trash
<!-- UserViewComments -->	- User comments page
<!-- ViewFriends2 -->	- User friends page list
<!-- UserViewProfile -->	- User profile page
<!-- User -->	- User control panel
<!-- UserViewPicture -->	- User view pictures area
<!-- UserViewAlbums -->	- User picture album area
<!-- MailFriendRequests -->	-Incoming Friend Requests
<title>Myspace.com Blogs -	- MySpace Blog Pages

When these data tags are used as search strings, data can be recovered out of the user's internet cache folders and in unallocated areas on the hard drive. To illustrate this, the test on the following page was performed on a 1.5 GB HDD test image with relatively mild to light MySpace use.

Search Summary

Hits	First Searched	Last Searched	Search Text
5	04/22/08 10:18:23PM	04/22/08 10:18:23AM	<!-- MailInbox -->
1	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- MailReadMessage -->
2	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- MailReply -->
2	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- Bulletin -->
2	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- BulletinRead -->
1	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- MailForward -->
1	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- MailTrashBox -->
9	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- UserViewComments -->
5	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- ViewFriends2 -->
8	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- UserViewProfile -->
13	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- User -->
3	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- UserViewPicture -->
3	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- UserViewAlbums -->
2	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<!-- MailFriendRequests -->
3	04/22/08 10:18:23AM	04/22/08 10:18:23AM	<title>Myspace.com Blogs -
4,885	04/22/08 10:22:39AM	04/22/08 10:22:39AM	friendid=

Now compare the streamlined search results above to the aforementioned "friendid=" search term which resulted in about **4,885** search hits. By using the unique *ColdFusion* data tags, and the HTML syntax in the MySpace Blogs search example, you can organize your results into specific folders and significantly filter your search results. The MySpace blog search string "<title>Myspace.com Blogs --" represents HTML syntax out of the "title" of the blog web page. The actual *ColdFusion* tag associated with MySpace Blog pages is "<!-- -->". I recommended that you **do not** use the *ColdFusion* syntax tag of "<!-- -->" to conduct keyword searches. The reason is that the tag is associated with a multitude of other areas within MySpace.com user pages. The result would probably be search returns in the thousands.

Messaging Menus

There are data embedded in links within the MySpace messaging menu that can assist forensic examiners in locating cached web pages and data within unallocated areas on the hard drive. The messaging menu is found in the user control panel area which can only be accessed after the user has logged in to the website (see illustration below).

The image illustrates the MySpace messaging interface. On the left, a vertical menu contains various options. Arrows indicate the following mappings:


- Inbox → "mail.inbox"
- Sent → "main.sentbox"
- Saved → "mail.savebox"
- Trash → "mail.trashbox"
- Bulletin → "bulletin"

The main content area shows a smaller version of the menu and an inbox listing three messages:

Date:	From:	Status:	Subject:
Apr 11, 2008 10:12 AM	USEOFFORC...	Replied	LOOK OUT
Apr 11, 2008 10:02 AM	Crank	Replied	Dude..
Apr 11, 2008 10:00 AM	frank	Replied	Hello


Note: In each of the menu examples, the user **is not** identified by the "friendID" number. The user is alternatively identified by the assigned token as shown below.

User Inbox

 <http://messaging.myspace.com/index.cfm?fuseaction=mail.inbox&MyToken=a5d2388f-bfff-4839-bba9-c3f16b49ea6e>




User Sent Items

 <http://messaging.myspace.com/index.cfm?fuseaction=mail.sentbox&MyToken=21780d57-1dac-4c64-a34b-06385e984774>




User Saved Items (Drafts)

 <http://messaging.myspace.com/index.cfm?fuseaction=mail.savebox&MyToken=4b77e7c1-60c4-4f05-b1cd-f8136e137347>



User Trash

 <http://messaging.myspace.com/index.cfm?fuseaction=mail.trashbox&MyToken=209e8f91-82dc-4b19-81e9-a6c852e12aff>



It is unnecessary to use all of the menu search strings to locate suspect data; all of the messaging menus within a user messaging area are populated with the exact same data. For this reason, the use of just one of the search strings is sufficient. In the example below, the search strings, “mail.inbox”, and “mail.sentbox”, were used to conduct the search.

(1)	1,146	04/14/08 10:32:58PM	04/14/08 10:32:58PM	mail.inbox
(2)	77	04/15/08 05:12:18AM	04/15/08 05:12:18AM	mail.sentbox

The two search results are significantly different because of the amount of hits received by the respective search strings.

[Home](#) | [Browse](#) | [Search](#) | [Invite](#) | [Film](#) | [Mail](#) | [Blogs](#) | [Favorites](#) | [Forum](#) | [Groups](#) | [Events](#) | [MySpaceTV](#) | [Music](#) | [Comedy](#) | [Classifieds](#)



More specifically, the reason for the vast difference in search results is that link 1,

<<http://messaging.myspace.com/index.cfm?fuseraction=mail.inbox>>, is also embedded as a link in the main MySpace navigation bar.

In each of the above examples, there is no guarantee that ALL of the data searched for will be retrieved. Fragmented data in unallocated areas of the hard disk area may not have captured the data containing the aforementioned *ColdFusion* and HTML syntax tags. I suggest that examiners use as many search strings as possible to yield the most effective results.

Data Carving

Data carving can be accomplished by using a variety of different computer forensic software applications. The Investigator should look for certain HTML syntax that is usually located above the *ColdFusion* data tags to begin data carving. In this example, the tag, <!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0” appears directly above the user control panel area *ColdFusion* syntax tag, “<!-- user -->”

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
<!--AJAX-->
<html xmlns="http://www.w3.org/1999/xhtml">
<!-- ELS2MWEBNET2133 -->
<!-- User -->|
<head id="ct100_Head1"><title>
```

Examiners should end the data carving by looking for the ensuing “</html>” tag. This requires that you manually look for the HTML syntax. There is no predetermined file offset associated with the end HTML tag, “</html>”.

```
</body>
</html>
```

Obtaining Data through MySpaceIM (Instant Messaging)

Forensic examiners can retrieve important data through an understanding of how to manipulate *MySpaceIM with Skype* (a downloadable program that allows MySpace users to instant message through text and to make free calls over the internet). The MySpace Instant Messenger needs to be installed in order to use the MySpace IM service.

Once installed, MySpaceIM creates the following folder structure:

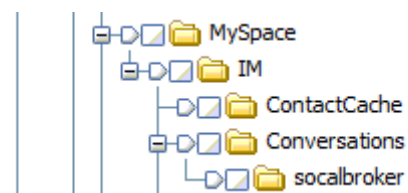


Win XP systems:

C:\Documents and Settings\Application Data\My Space\IM*. * (subdirectories)

C:\Program Files\My Space\IM Skins*. * (subdirectories)

Windows XP Example (Application Data)



Windows Vista Systems:

C:\Users\\AppData\My Space\IM\ *. * (subdirectories)

C:\Program Files\My Space\ Skins*. * (subdirectories)

A folder titled, "Conversations" appears under the first set of subdirectories (shown above, right). The Conversations subdirectory will have the MySpace screen name used by each person who logged onto that computer using MySpace IM. Each screen name folder contains files with the MySpace screen name of the person with whom they messaged (ex: mscrook.txn.). These .txn files, when opened*, show the IM conversation between the user on the computer and each person he/she has texted. The .txn files are appended to show both sides of every typed conversation the user has ever had on this computer.

***To view the .txn files, copy them out and re-name each to .htm. Then use Internet Explorer to view them.**



387 Magnolia Ave. #103 – Corona, CA 92879-3308

PH: (951) 848-0839 FX: (951) 737-0797 EM: Frank@inlanddirect.com

Web: <http://www.inlanddirect.com>

*Disclaimer: The information regarding the embedded link and search string data information in this training article was as a result of research & development conducted by the author. The information pertaining to MySpace IM is open source information which can be located at <http://www.myspaceinvestigators.com> in the forums area, the Guidance Software website in their associated forums area, and various CFE internet resources. The author does not take credit for research regarding this information. This is an "OPEN SOURCE DOCUMENT" Please feel free to distribute it as you please.