

# Getting Facebook into Evidence – A Technical Perspective

---

*By: Larry E. Daniel, EnCE, DFCP, BCE, Digital Forensics Examiner*

There are many legal arguments for and against getting Facebook information in to evidence. While comments may be made in this paper regarding the legal arguments, along with references to case law and other legal sources, this is primarily a paper regarding the collection, preservation and authentication of Facebook evidence from a digital forensics perspective.

The challenge with any kind of electronic or digital evidence is authenticating the evidence so it can stand as a foundation for admittance of the evidence in a court of law. This foundation from a technical perspective involves being able to show the court that the evidence is identical to the original and was collected in a forensically sound manner.

The best method for getting any evidence is to get it from the original source. In the case of Facebook evidence, Facebook itself would be considered the best source as Facebook is the custodian of the data.

However, there are many challenges to getting original Facebook evidence since Facebook and other social media entities are protected from disclosing information by the Stored Communications Act and are not subject to civil subpoenas for content nor will they respond to criminal subpoenas unless they originate from a law enforcement agency. This means that criminal defense attorneys are severely handicapped by the stance that Facebook is not required to respond to subpoenas for content unless they are from a law enforcement agency.

Rather than focusing on the legal aspects, I will be sticking to the technical aspects of Facebook evidence.

## Part 1: Creation and Authentication of User Accounts – The Weakest Link

All of the social media providers such as Facebook have a Terms of Service that a person must agree to during the account creation process. You can review the Facebook terms of service at this link:

<https://www.facebook.com/legal/terms>

Regarding the account creation and security;

### 1. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.

3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline for your own commercial gain (such as selling your status update to an advertiser).
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

While the terms of service specifically prohibit persons from providing false information to Facebook or creating an account for someone other than themselves, these terms are not enforceable from a technical standpoint.

### **Creating a fake Facebook account:**

Step 1: Get a free email address from Yahoo or Hotmail, etc. There is no verification of identity when these accounts are created.

Step 2: Go to Facebook and create a new account. Use your free email address as your contact email for verification.

Viola! You now have a Facebook account with no attachment to you in any way. There is no method for verifying anyone's actual identity on Facebook or any other social media site simply by viewing the profile page online. You can grab anyone's picture, company logo, email address, phone number from various sources on the internet to construct this fake Facebook profile. It is even possible to construct multiple Facebook profiles and connect them together as "friends" even if they are all under the control of a single person.

What this means in terms of getting Facebook content into evidence is that simply viewing a Facebook profile and printing out what you see on the screen has no method of verification that the person portrayed in the profile is in fact that person at all.

## **Part 2: Authentication of Facebook Evidence**

### **Linking a Facebook account to a person:**

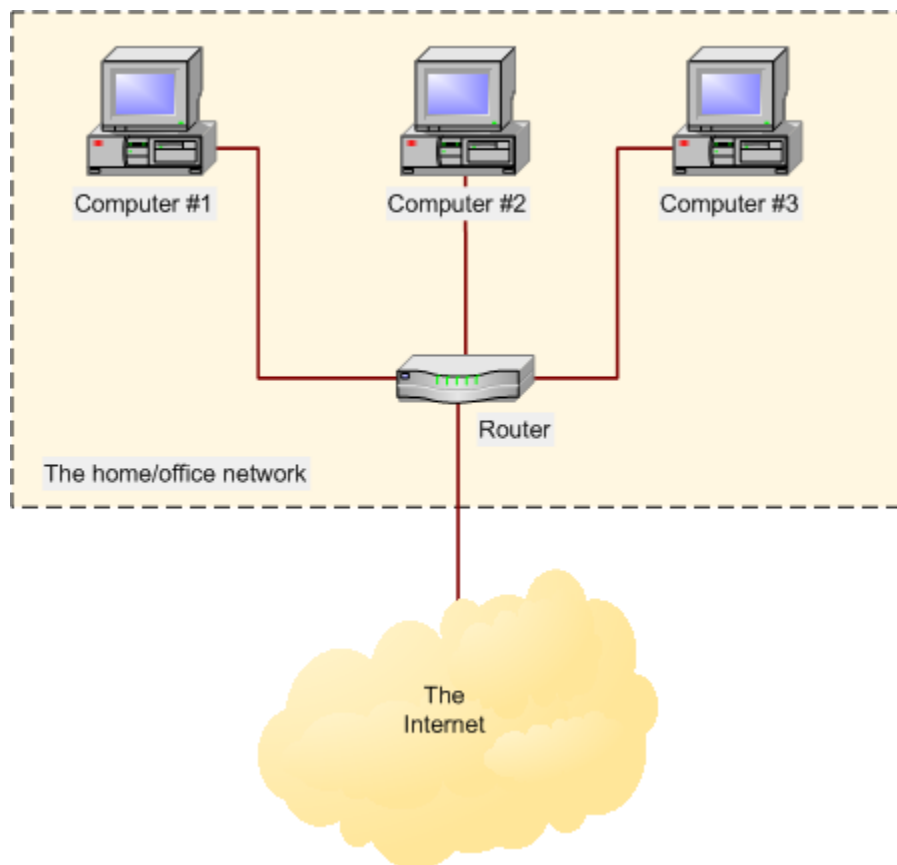
#### **What about the IP address used to create the profile?**

One way to potentially link a Facebook account to a person is to get from Facebook the access logs for the account. This would include the creation date and time for the profile and the IP address that was used to access the internet to create the profile.

An IP address is a numerical address that is used for internet access the same way that a telephone number is used to access the public telephone network.

When you connect to the internet your computer will always has an IP address associated with it in some way. However, the IP address rarely connected directly to a computer, but in fact is normally an address for a device between your computer and the internet, called a router.

So the best you can do with an IP address is to find out the location and subscriber information for a router, not a specific computer.



Why is this important? Knowing the address for a router can be of limited use for the following reasons:

1. The router is in a public space such as a coffee shop, library, McDonald's etc.
2. The router may belong to a business with dozens to hundreds of computer connected via that same IP address.
3. The router is in a hotel or other area with shared internet access.
4. The router may be in a person's home. If this is the case, then verification that the router is secured from unauthorized access can become an issue.

If the router is in a person's home, specifically the person who allegedly posted the evidence items on Facebook, then a subsequent subpoena to the internet provider is required to find this out by verifying the subscriber information. Having the subscriber information would potentially show that the subscriber for the IP address at the time of the posting or account creation is the same as the person who made the posting.

To do this you would need to perform the following steps in order:

1. Get the Facebook ID for the account of interest.
2. Subpoena Facebook for activity logs to include the date, time and IP address information for a specific period of time.
3. Locate the IP address for the date and time of interest.
4. Locate the owner of the IP address, i.e. Time Warner, Comcast, etc.
5. Subpoena the owner of the IP address for the IP address for the specific date and time of interest to get the subscriber information.

If there are different IP addresses for the dates and times you are interested in, the above steps would need to be repeated for each of them.

If you get a "hit" i.e. the date and time and IP address links up with the date and time of the posting you are interested in and the person's home address, you have gone a long way toward being able to support the posting was in fact created by the person.

IP Log Example:

```
Created on: 2006/01/18-23:55:42-UTC
IP: 12.208.12.248, on 2006/01/18-23:55:41-UTC
Language Code: en
SMS: [US]
Nickname:

Date/Time                Event                IP
2011/03/25-12:37:06-UTC   Login                138.162.8.58
2011/03/25-12:12:31-UTC   Login                96.255.98.133
2011/03/24-13:12:36-UTC   Login                96.255.98.133
2011/03/23-23:37:04-UTC   Login                96.255.98.133
2011/03/23-21:46:14-UTC   Login                96.255.98.133
2011/03/23-21:45:33-UTC   Login                96.255.98.133
```

*This type of subpoena response would show as in the image above, the creation IP address with the date and time, along with the login accesses to the profile with the dates, times and IP addresses. This would also show the email address used to create the profile and the profile ID or name associated with the profile account.*

## Part 3: Better Sources of Evidence for Facebook

***The best sources of evidence for Facebook postings are from locations that can be tied directly to a computer user or account owner.***

There are typically two excellent sources of information for a Facebook posting or content that is easy to authenticate.

### One: From Facebook via consent.

If you can obtain voluntary consent from the owner of the account, you can use the following form to get information from Facebook. While this may or may not work in your particular case, it would be the best evidence from an authentication standpoint.

#### Consent to Release Private Facebook Information

I, [LEGAL NAME] , am an account holder with Facebook, Inc. My profile user ID is [UID/ALIAS] and my login email address is: [USER LOGIN EMAIL

– please do not include your password]. I do hereby voluntarily authorize Facebook to release the reasonably available data as check-marked below, from my Facebook account profile for the period of [ date range ]

I hereby indemnify Facebook, Inc. against all claims for damages, compensation and/or costs in respect to damage or loss to a third party caused by, or arising out of, or being incidental to release of my data.

My data should be released to\*\*\*:

[CONTACT NAME, PHONE NUMBER, FAX NUMBER, ADDRESS and E-MAIL ADDRESS –

\*\*\*please note that user data will be sent to the user or the user’s legal representative]

Please release the following data: [check all the boxes that you are requesting]

- Profile information
- Recent logins (recent means the past 2-3 days from process date)
- Status Updates
- Notes
- Mini-feed
- Shares
- Wallposts
- Friends List
- Groups
- Events
- Videos

- \_ Applications
- \_ Facebook Message Inbox (received messages)
- \_ Facebook Message Outbox (sent messages)
- \_ Photos and users' comments (ALL photos available will be sent if this box checked)

\_\_\_\_\_  
Affiant's Name (USER please print) Affiant's Signature

Date \_\_\_\_\_

Notary Public/Individual Duly Authorized to Administer Oath:

[THIS CONSENT MUST BE NOTARIZED. See attached]

\_\_\_\_\_  
Affiant's Name (USER please print) Affiant's Signature

Date \_\_\_\_\_

State of \_\_\_\_\_

County of \_\_\_\_\_

Subscribed and sworn to (or affirmed) before me on this \_\_\_\_ day of \_\_\_\_\_,  
20\_\_\_\_, by \_\_\_\_\_, proved to me on the basis of  
satisfactory evidence to be the person(s) who appeared before me.

(Seal) Signature \_\_\_\_\_

---

The second way to get evidence from Facebook via consent is when the owner of the profile gives consent for the profile to be accessed for the purpose of collecting information from the profile. If you are able to get consent to access the profile by logging into the profile with the provided username and password, it is best to have a third party such as a forensic examiner, perform the collection of the data.

When you have access to the profile, you can use the Download Archive function on their Facebook Accounting Settings page to download everything in the profile including:

Active Sessions

Account Status Changes

Address Book

City and Hometown info

Datr Authentication cookies. (These can be potentially tied back to a device.)

Email addresses

Family Members that are connected to the profile

Notifications Settings

Phone Numbers

Recognized Devices (Any device such as a phone connected to the profile.)

In addition to the above, you can also get the following information by downloading it from the profile. Even if you cannot get consent to collect the data via these downloads, you can ask for the download to occur via a discovery production order. **Note that these downloads would only include the current profile and would not show what was deleted from the profile prior to download.**



- Profile**
- Wall
- Photos
- Friends
- Notes
- Messages

## Larry Daniel

Facebook Profile: <http://www.facebook.com/larry.daniel>

Current City: Raleigh, North Carolina

Website: [www.exforensics.com](http://www.exforensics.com)  
[www.guardiandf.com](http://www.guardiandf.com)  
[www.blogtalkradio.com/talkforensics](http://www.blogtalkradio.com/talkforensics)

Email: [larry@guardiandf.com](mailto:larry@guardiandf.com)

Birthday: 10/08/1958

Sex: Male

Relationship Status: Married - Erna Stromsland Daniel

Hometown: Memphis, Tennessee

Family: Destiny Porter Daniel (daughter)  
Lars Daniel (son)  
Geoff Daniel (son)  
Leslie Denton (sister)  
Ny Daniel (daughter)

Employers: Guardian Digital Forensics 1998-05 - Present  
Digital Forensics Consultant  
Computer forensics for civil and criminal cases. Expert witness testimony for computer forensics.

Political Views: Moderate

Religious Views: Reformed

Favorite Quotations: 8 He has told you, O man, what is good;  
and what does the Lord require of you but to do justice, and to love kindness,  
and to walk humbly with your God?  
  
Micah 6:8  
  
It is absurd for the Evolutionist to complain that it is unthinkable for an  
admittedly unthinkable God to make everything out of nothing, and then  
pretend that it is more thinkable that nothing should turn itself into everything.  
G.K. Chesterton  
  
Every time you make a choice, you are turning the central part of you, the part  
that chooses, into something a little different from what it was before. C. S.  
Lewis  
  
Too many of us have a Christian vocabulary rather than a Christian  
experience. We think we are doing our duty when we're only talking about it.  
Charles F Banning

Other: EverQuest 2, San Diego Chargers, Peninsula Cleaning Solutions, NACDL,  
Microsoft U.S. Partner Community, FindLaw, Super Lawyers, NFSTC -  
[www.NamUs.gov](http://www.NamUs.gov), Law Offices of Mary Frances Prevost, Carey's Variety  
Store, Visual Studio LightSwitch, River of Life, Rebecca's Hope Christian  
Center

Music: Eclectic Taste

Bio: 8 He has told you, O man, what is good;  
and what does the Lord require of you but to do justice, and to love kindness,  
and to walk humbly with your God?  
  
Micah 6:8

Television: Grimm, The Voice, Firefly, The Big Bang Theory, Eureka

Groups: Missing, Vote for Clayton High School's Lip Dub Video, Forensics



## Friends List:

Larry Daniel - Friends

Page 1 of 4



[Profile](#)

[Wall](#)

[Photos](#)

**Friends**

[Notes](#)

[Messages](#)

## Larry Daniel

---

Aimee Hatchell  
Alan Swartz  
Alex Nelson  
Allen Alexander Lee  
Anecia Lee  
Angelina Ward  
Annie Aguzzi  
Ben Levitan  
Benny Oakes  
Bob Kastl  
Brett Norris  
BringThem Home  
Bruce McCarthy  
Burt Smith  
Butch Lawter  
Carol Cooke Spencer  
Carol Sirk  
Carolynn Boeh  
Cary A. Disney  
Catherine Mambretti

## Wall Posts:



Profile

Wall

Photos

Friends

Notes

Messages

## Larry Daniel

Larry Daniel Games/Toys



EverQuest 2

ESRB Rating: TEEN with use of Alcohol, Violence, and Suggestive Themes. About EQII: EverQuest® II is the next...

📅 June 7, 2012 at 7:20 pm

Larry Daniel Interesting...According to Google, my book is in 106 libraries in 19 countries. <http://ow.ly/9Dzq3>



Digital Forensics for Legal Professionals, 1st Edition | Larry Daniel...

Elsevier Store: Digital Forensics for Legal Professionals, 1st Edition from Larry Daniel, Lars Daniel. ISBN-9781597496438, Printbook . Published: 2011

📅 March 13, 2012 at 5:45 pm

5 people like this

Larry Daniel

📅 March 10, 2012 at 11:14 pm

Larry Daniel I did my television interview with Consumer Reports this morning. :) Once they give me notice of where it will air, I will post a link.

📅 March 6, 2012 at 2:43 pm

10 people like this

Larry Daniel Consumer Reports called me today from New York. They are sending a camera crew to my office next week to interview me about computer and cell phone privacy issues. Should be fun. :)

📅 February 29, 2012 at 7:39 pm

9 people like this

## Messages:



## Larry Daniel

Unknown

June 7, 2012 at 7:22 pm

Larry Daniel

June 7, 2012 at 7:22 pm

Wow, I am so sorry I did not get this message in time. I do not check my Facebook very often. I hope the race worked out great for everyone.

Unknown

March 21, 2012 at 10:16 am

Profile

Wall

Photos

Friends

Notes

Messages

Downloaded by Larry Daniel (<http://www.facebook.com/larry.daniel>) on July 9, 2012 at 11:51 am

## Two: From a computer or device that is in control of the person posting to Facebook.

When you have access to a computer owned, controlled and used by the poster of information, it may be possible to recover the actual Facebook page of interest. In many cases Facebook users also receive notifications on their smart phone or pad computers in addition to the computer they use. All of this can potentially be recovered using forensic software.

If recovery of the actual page is not possible, other pages from the profile may be recoverable to establish that the person is the owner of the profile and accesses it on a regular basis. Also, the internet history from the computer may also provide dates and times that the Facebook profile were accessed from the computer.

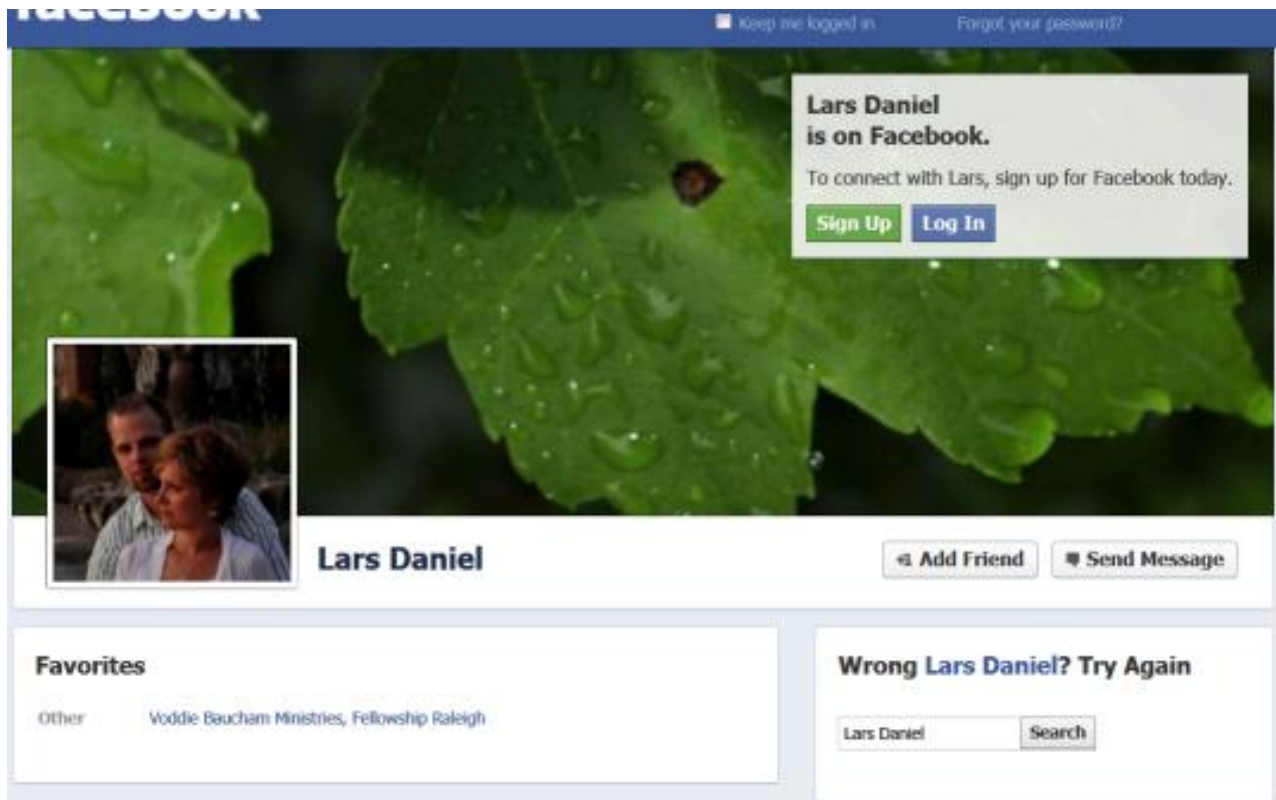
Here is an example of an internet history record from an actual case, pointing to a Facebook profile:

The following Facebook profile was accessed from the computer:

Last Accessed	Profile Name	Url Name
06/10/11 11:16:40PM	john	http://www.facebook.com/ajax/presence/notifications_read.php?time=1307764300&user=111111111&version=2&render=1&locale=en_US&__a=1

*The user ID has been changed for this example.*

If you have internet history showing an access to a Facebook page, you can then go to the Facebook profile and see what you can see. Even if the profile is protected, there will be at least a public page you can capture. Below is the public profile for my son's Facebook page:



*By using the link from the internet history from the person's computer and linking to the Facebook profile, you can establish that the computer was used to access the profile.*

**Facebook Login History:**

The follow image is an example of the Facebook login history available to the account owner from their Facebook profile page. This type of information, as well as all of the person's profile content can be downloaded by the user by requesting it from Facebook using the Download Archive function on their Facebook Accounting Settings page.

## Login History



## Larry Daniel

---

	IP	Time	Site
<a href="#">Account status changes</a>	174.99.51.10	Today at 9:33am	www.facebook.com
<a href="#">Active Sessions</a>	174.99.51.10	Today at 9:23am	www.facebook.com
<a href="#">Apps You Admin</a>	174.99.51.10	Today at 8:57am	www.facebook.com
<a href="#">Pages You Admin</a>	174.99.51.10	Today at 7:07am	www.facebook.com
<a href="#">Address</a>	174.99.51.10	Tuesday, July 3, 2012 at 1:48pm	www.facebook.com
	174.99.51.10	Thursday, June 28, 2012 at 12:46pm	
	174.99.51.10	Tuesday, June 26, 2012 at 11:35am	www.facebook.com
	174.99.51.10	Thursday, June 7, 2012 at 4:20pm	www.facebook.com
	174.99.51.10	Sunday, March 18, 2012 at 4:01am	www.facebook.com
	174.99.51.10	Wednesday, March 14, 2012 at 7:40pm	www.facebook.com
	70.154.107.136	Tuesday, March 13, 2012 at 2:50pm	www.facebook.com

### Recovered Facebook pages from the computer hard drive:

If you are unable to get evidence directly from Facebook, then the next best thing is to recover Facebook pages directly from the person's computer hard drive. Forensic tools can allow an examiner to recover web pages from a computer hard drive and show them in their original condition, just as the user saw them on the computer monitor.


In order to do this, you will have to have the computer that was used to either view or post to Facebook.

### Facebook Notification Emails:

Facebook sends notification emails for activities that occur on a user's profile. These emails can be recovered in many cases from the user's computer hard drive.

#### Jose Baez is at CBS Inside Edition

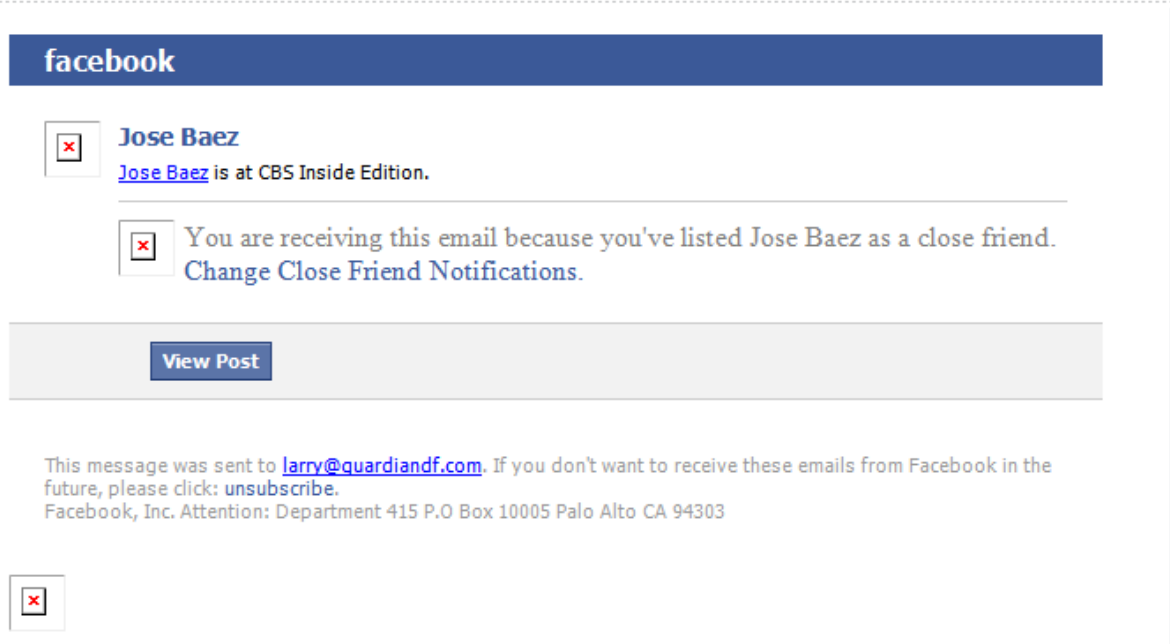
Facebook <notification+ke4grqxn@facebookmail.com>

 If there are problems with how this message is displayed, click here to view it in a web browser.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Sent: Mon 7/9/2012 12:32 PM

To: Larry Daniel



The screenshot shows an email interface with a blue header bar containing the word "facebook". Below the header, there is a notification from "Jose Baez" with a broken image icon. The notification text reads: "Jose Baez is at CBS Inside Edition." Below this, another notification with a broken image icon states: "You are receiving this email because you've listed Jose Baez as a close friend. Change Close Friend Notifications." A "View Post" button is visible below the notifications. At the bottom of the email content, there is a footer with the text: "This message was sent to larry@guardiandf.com. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe. Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303". There is also a broken image icon at the very bottom of the email content area.

## Part 4: Best Practices

Your best option to make sure that you will be able to get and use Facebook evidence is to preserve everything you can.

Even if the user says that they deleted their Facebook account, Facebook will retain all of the information and content for 90 days from deletion in order to give the user time to change their mind.

1. **Use preservation letters:** While you may not be able to obtain content from Facebook via a subpoena, sending them a preservation letter is one of your best options to prevent loss of evidence. You probably won't know in advance if you may be able to get voluntary or compelled consent to access and download the content from a Facebook profile. Even if you are not after content, a preservation letter to Facebook can help you in the preservation of user access logs and account creation information.

Also, use preservation letters to opposing parties to try to preserve computers, smart phone evidence and the Facebook profile itself. |

2. **Preserve all devices:** If you are working with an employer who has an employee's computer, attempt to get a forensic copy of the hard drive for preservation of the evidence. At the least, try to get them to turn over the computer hard drive for preservation until a forensic copy can be made of the original hard drive. It is also critical to preserve smart phones, iPads and any other device that can connect to the internet as Facebook can be present on all of those platforms as an "App."
3. **Use Forensic Experts:** You can use digital forensic experts to assist with the collection, preservation and authentication of Facebook evidence not only from computers, iPads, phones and other devices, but also from the internet itself.

Also, while the forensic expert may not be able to recover the actual Facebook web page from the hard drive or other device storage, he or she may be able to get IP address information that can later tie the person of interest to a Facebook profile.

IP address information can be obtained from internet history on the hard drive or device, the IP address assigned to the computer, as well as potentially from email or Facebook chat histories that may be resident on the storage media of the computer for device.

## **Part 5: What an expert cannot do**

An expert cannot authenticate a print out of a web page any more than any other witness. The reason is that a print out of a Facebook profile provides no external method for authentication on its own merit. A Facebook profile can easily be created for the purpose of framing or de-faming someone else. This is why it may be difficult to get Facebook content into evidence if there is no method for authenticating that the Facebook profile in is fact real, created by the person alleged, and that the profile was not hacked or tampered with y a third party.