



Annual ADFSL Conference on Digital Forensics, Security and Law

2009
Proceedings


May 22nd, 9:00 AM

Methodology for Investigating Individuals Online Social Networking Persona

Jonathan T. Rajewski

Champlain College, Burlington, Vermont 05403, jtrajewski@gmail.com

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Rajewski, Jonathan T., "Methodology for Investigating Individuals Online Social Networking Persona" (2009). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3.
<https://commons.erau.edu/adfsl/2009/friday/3>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



Methodology for Investigating Individuals Online Social Networking Persona

Jonathan T. Rajewski
Champlain College
Burlington, Vermont 05403
Jonathan.Rajewski@champlain.edu
jtrajewski@gmail.com

ABSTRACT

When investigators from either the private or public sector review digital data surrounding a case for evidentiary value, they typically conduct a systematic categorization process to identify the relevant digital devices. Armed with the proper methodology to accomplish this task, investigators can quickly recognize the appropriate digital devices for forensic processing and review. This paper purposes a methodology for investigating an individual's online social networking persona.

Keywords: Social Networking, Web 2.0, Internet Investigations, Online Social Networking Community

1. INTRODUCTION TO THE ONLINE SOCIAL NETWORKING COMMUNITY

Online Social Networking Communities (OSNC) are utilized by nearly 45 percent of all active Internet users (Nielsen/NetRatings, 2006), which equates to approximately four hundred sixty million people (Internet World Stats, 2007). The top ten online social networking sites grew nearly 47 percent over the past few years. This trend has been on the rise and doesn't show any signs of declination (Nielsen/NetRatings, 2006).

So what are Online Social Networking Communities? The concept of "Online Social Networking" is not new. When the notion of "Online Social Networking" was combined with "Community" it evolved to what we now know as the concept of "Web 2.0".

Web 2.0 is concept that explains the evolution of how people use the Internet. *Table 1* contains a comparative example of websites which are considered Web 1.0 and Web 2.0.

Table 1. Web 1.0 vs. Web 2.0 Websites

Web 1.0		Web 2.0
DoubleClick	-->	Google AdSense
Ofoto	-->	Flickr
Akamai	-->	BitTorrent
mp3.com	-->	Napster
Britannica Online	-->	Wikipedia
personal websites	-->	blogging
evite	-->	upcoming.org and EVDB
domain name speculation	-->	search engine optimization
page views	-->	cost per click
screen scraping	-->	web services
publishing	-->	participation
content management systems	-->	wikis
directories (taxonomy)	-->	tagging ("folksonomy")
stickiness	-->	syndication

(O'Reilly, 2005)

To further describe OSNCs, or its synonymous term Web 2.0's, conceptualize how the Internet revolutionized the world – online banking, search engines, email, instant communication methods, and the list goes on. Now, imagine traditional everyday social interaction – such as: greeting your spouse or co-worker in the morning. Combine the two, and you have the phenomenon known as Web 2.0 or Online Social Networking Communities.

Traditional Online Social Interaction + Community = Web 2.0

2. DIFFERENT TYPES OF ONLINE SOCIAL NETWORKING COMMUNITIES

By design, there are numerous types of OSNCs. Each OSNC provides unique features and opportunities for its users. Below are several popular examples which investigators will typically encounter during an investigation:

- 1) Blog – Users have the ability to publically (can also be privately) publish their thoughts on a particular topic. Unlike the traditional news article published on physical paper, Blogs are posted on the Internet for everyone or a specific user group to see (Kazakoff, 2009). In the past, Internet users may have created a website to achieve an equivalent goal, but with open source software solutions such as Wordpress (WordPress, 2008) being introduced to the market, users now have a scalable and easily manageable solution to communicate to the masses.
- 2) Digital Photograph Hosting – Users have the ability to save photos to Internet based repositories for “everyone” or a select group to view. Websites such as Flickr.com (Flickr, 2008) and Photobucket.com (Photobucket, 2008) have created a seamless process for users to share their photos with the world.
- 3) Video Hosting – Users have the ability to take videos in the real world and save them in an online storage area to ultimately share them with the world. Websites such as YouTube! (YouTube, 2008) and Google Video (<http://video.google.com/>, 2008) have pioneered the industry and made this process a very scalable and easy function for the end user.
- 4) Online Collaboration – These websites foster online communication with users across the world. Essentially, users have a unique persona and are encouraged to collaborate with the community. Some examples of these websites are web based message boards, Facebook (Facebook, 2008) and Myspace (Myspace, 2008)

There are a plethora of OSNCs available to explore. The examples listed above have both communal and exclusive features that should be explored in every investigation.

3. HOW TO UTILIZE ONLINE SOCIAL NETWORKING COMMUNITIES

When people decide to join an OSNC, they typically embark on an OSNC selection process. This procedure is typically carried out by either querying an Internet search engine or by learning about a specific OSNC from another person. To describe this further, if an accountant in the real world sought out to join a club or professional organization relating to their industry, they might read a trade magazine or ask a colleague which organizations they belong to. The same is true in the selection process of online communities. If one wishes to join an OSNC that discusses “Microsoft Windows Vista”, they might use an internet search engine or a colleagues advice to find one.

Typically, upon selecting an OSNC, a user must “register”. This process allows users participating in OSNCs to uniquely identify and authenticate themselves. In order for users to successfully complete the registration process, they typically have to provide at least two things to the OSNC:

- 1) A distinctive username or screen name – This is the “unique identifier” will help differentiate users on in the OSNC;
- 2) An email address – This is often the “communication” method the OSNC will use with the user. An email address is typically used to authorize the registration process.

In the real world, communities can put more of a focus on credentials or who is authorized to access a particular social group, same is true for OSNCs. That said, once the registration process is complete, a user is permitted to start online collaboration. Also, just as in the real world, when a participant is no longer welcome in a social community, they can be removed just as easily as they were introduced.

4. CONSIDERING ONLINE SOCIAL NETWORKING COMMUNITIES AS DATA SOURCES IN INVESTIGATIONS

Investigations are typically geared to the incident presented to those conducting the investigation. Oftentimes there is a framework for investigations that stays uniform (How Should We Conduct Investigations?, 2007), yet when investigations into OSNCs are conducted, one must take due care even when exigency is presented. For example, if exigency is a factor during an investigation, such as a person’s life in immanent danger, the typical process of conducting an investigation is modified based on the needs of the investigation.

In the recent investigation into the death of 12-year-old Vermonter, Brook Bennett, police reported that MySpace, a widely used OSNC, may have been used to arrange a meeting with someone she had been communicating with (Slota, 2008). This example demonstrates that when OSNCs are considered in investigations, additional relevant data can be added to the investigation, which may not have been available via traditional information gathering techniques.

The Brooke Bennett example and others alike are reasons enough to arm investigators with a proven methodology to investigate an individual’s online social networking persona.

5. INVESTIGATING ONLINE SOCIAL NETWORKING COMMUNITIES

The Online Social Networking Community is a very large and oftentimes overlooked source for evidence in an investigation. Thousands of OSNCs are available on the Internet to choose from. Investigators must be armed with a systematic and intelligent approach when investigating such data sources.

In reality, a new OSNC can be created by anyone who has the means and access to the internet. Staying current with every new community created would be an unrealistic task for investigators. Therefore, a high level understanding on how these communities work is an essential part of the process.

Due to the nature of how Electronically Stored Information (ESI) is stored on a social networking or online community website, it’s critical for investigators to be equipped with the proper knowledge and tools necessary to quickly locate and interrogate the digital data residing on them.

A conceptual understanding of the data available to investigators is key to realizing the vast amount of information available from an OSNC. Typically, there are at least two data sources to consider when investigating an OSNC:

1) The OSNC facing the internet – This is normally what investigators will find after visiting a suspects OSNC. The information found on these pages are active and can be changed at any time.

2) The OSNC subscriber records – This data usually consists of successful user authentication access times with Internet Protocol (IP) addresses and registration email addresses. This data is typically stored by the OSNC and cannot be accessed without court authorization.

6. IDENTIFY IF A SUSPECT ACCESSED/UTILIZED A SOCIAL NETWORKING AND/OR ONLINE COMMUNITY

There are five guidelines that should be followed when investigating an individual's online social networking persona. In essence, these steps will help mitigate the risks associated with an online investigation and identify which steps to take in what order. Some of the steps can be added or subtracted based on the nature of the investigation, but the following are three guidelines that should be followed:

- 1) Recognize the risks of searching for a personal on an OSNC
- 2) Ensure that the investigator appears anonymous to the internet
- 3) Determine which OSNCs to search
- 4) Probe OSNCs for potential evidence
- 5) Collect potential evidence



Step 1 – Recognize the risks of searching for a persona on an OSNC

It's imperative, that investigators take the same due care when investigating OSNC's as they do when investigating a suspect in the real world. Keep in mind, that a single visit to an OSNC can compromise the entire investigation and it's critical to ensure anonymity. A gross example of this would be if Law Enforcement drove a marked police cruiser to a drug house to conduct an undercover drug buy. Not

only would the drug dealers refuse to sell the drugs, but also they would most likely move to another house.

Another example for investigators to be conscious of is services that claim to uncover ones online persona. It's critical that the investigator always conduct independent tests prior to using such services. A specific example that, at the time of this publications writing, is the web service called "Yo Name" (<http://www.yoname.com/>) which advertises the ability to "search across social networks, blogs and more". This service does what it purports to do (Figure 1), but it also will notify the person being searched via email.



Figure 1. www.Yoname.com search

Step 2- Ensure that the investigator appears anonymous to the internet

When conducting an investigation into an OSNC, investigators must appear anonymous to the Internet. Just because one is using a work computer and work Internet connection with a fictitious OSNC alias, this does not ensure anonymity.

To ensure anonymity, investigators should seek out the following:

- 1) Dedicated computer¹ with a normal system configuration²
- 2) Dedicated undercover internet connection³

In figure 2, you will find a typical network topology diagram that satisfies Step 2.

¹ A "dedicated computer" is a computer that is only used for a predefined task

² A "normal system configuration" includes commonly available software and hardware.

³ A "Dedicated undercover internet connection" is one that was purchased with an undercover identity. Typically these internet connections are Cable/DSL connections. It's becoming more prevalent to purchase mobile carrier "Air Cards" due to their portable nature.

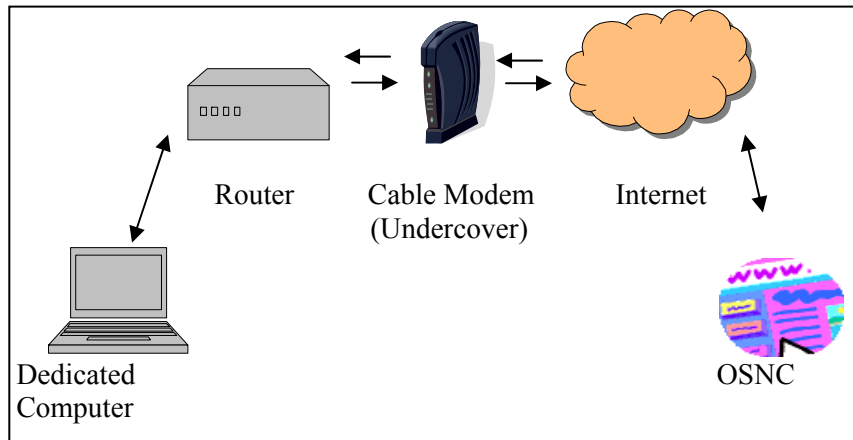


Figure 2 – Ideal network topology

Step 3 – Determine which OSNCs to search

After completing Steps One and Two, investigators will need to begin the process to determine if a suspect has an online persona within an OSNC. Due to the anonymous nature of the Internet, without analyzing the suspect’s digital device or knowing their specific persona, this can be a very challenging if not an impossible task. With that being said, it’s in the best interest of an investigator to use an educated approach when trying to track down the suspect.

The Top 10 social networking websites would be a good first choice for an investigator to explore (Table 2). The ability for a social networking site to retain its users should also influence your investigative methods (Table 3).

Table 2. Top Social Networking Sites for April 2006

Site	# Unique Visitors April 2006
MySpace	38,359,000
Blogger	18,508,000
Classmates Online	12,865,000
YouTube	12,505,000
MSN Groups	10,570,000
AOL Hometown	9,590,000
Yahoo! Groups	9,165,000
MSN Spaces	7,165,000
Six Apart TypePad	6,711,000
Xanga.com	6,631,000

Source: (Nielsen/NetRatings, 2006)

Table 3. Top 5 Social Networking Sites ranked according to Retention Rate, April 2006

Brand	Retention Rate (%)
MySpace	67.04
MSN Groups	57.62
Facebook	51.73
Xanga.com	48.92
MSN Spaces	47.33

Source: (Nielsen/NetRatings, 2006)

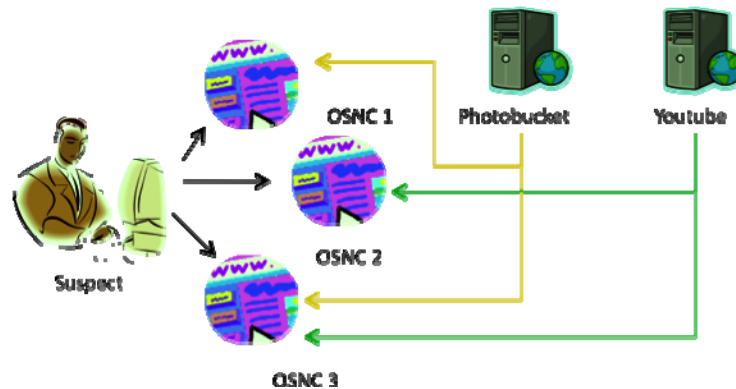
Due to the ever-evolving/changing OSNCs, it’s critical to stay mindful of current and up-and-coming social networks. A simple query of international news sites, intelligence groups and/or high school lunchrooms could reveal real time trends and data sources to consider.

Step 4 - Probe OSNCs for potential evidence

Now that the investigator identified the statistically leading websites where suspects may be partaking in online social networking, gathering known unique information about the suspect is critical to this process. In other words, in order to find a particular straw in the haystack, you need to know something about it. For example, if an investigation uncovers the that suspect “Johna Doeet” had a dog named “fluffy”, an email address – fluffy1992fluffy@aol.com and a mobile phone number of 212-244-9089 you would have several great keyword combinations to use. For example:

	Keyword
1	Johna
2	Doet
3	Johna+doet
4	Fluffy
5	Fluffy1992
6	Fluffy1992fluffy
7	Fluffy1992fluffy@aol.com
8	212-244-9089

Another technique to utilize is when the investigator learns of one OSNC persona and is trying to locate another. Using data from the known persona can aid in the search. For example, leaning where one stores their photographs or videos can help the investigator discover an unknown persona. Online photo and video storage websites allow users to store a large amount of data, which oftentimes equates to over one gigabyte in size. This presents the suspect with the convenient opportunity to only use one photo sharing website, of which the investigator can exploit to link unknown personas back to an individual. See *Figure 3* for an example. In *Figure 3*, the suspect has three OSNCs. The investigator identified the Photobucket account using traditional search techniques and used the data collected to search OSNC1 and OSNC3 to help identify the hidden persona. Also, after reviewing OSNC3, the investigator located an unknown Youtube account which later linked was linked to OSNC2.



Typically, every online community and social networking website will have a search function. Some are more powerful than others, but please be advised that some communities permit only registered users to utilize the search feature. Please note the necessary steps to ensure anonymity still apply to these searches.

Another feature that is a great resource with which to conduct investigations into online personas is Google. Correctly implementing Google's powerful indexing/search engine to your investigative arsenal is key to an investigation. Two features which will be discussed in this paper are "Google Alerts" and Google's Advanced Search features.

A Google Alert is a feature of Google that will send an email to the requesting person when a specific text string is indexed by Google (Google, 2007). This feature alone is very powerful, but will only alert the requestor from the time they configure the alert forward, not retroactively.

The second Google feature that is very helpful in an online investigation is Google's advanced search features. One in particular is the ability to search an entire website from the Google website by using the following string:

apple site:www.cnn.com

The above search term will search the website www.cnn.com for the term "apple". As you can see this is a very powerful feature to be aware of.

To access Google's advanced search features, please click the "Advanced Search" link by the search bar.⁴

Aside from the educated statistical approach, if the investigator has access to the digital devices suspected of being utilized to access OSNCs, the next immediate step would be to contact a competent digital forensic examiner to review the digital devices. Such digital devices of interest include but are not limited to: laptops, desktops, mobile telephone devices, media players. Due to the nature of how technology is ever changing, it may be appropriate on a case-by-case basis, to consult with a technology specialist (or an expert of the like) to ensure that you exhausted your search of available digital devices.

A knowledgeable digital forensic examiner should be able to determine which if any OSNC was utilized and persona used on each.

⁴ There are several books and publications available on leveraging the power of the Google search engine.

Step 5: Collect potential evidence

Once the investigator identifies potential evidence it's critical to collect the information and preserve it as soon as possible. Due to the OSNC's typically storing active content on their websites, as soon as a change is made, its immediately made and there are no backups available.

There are two recommended steps to be followed by investigators when collecting potential evidence from OSNCs. The first of which should be done under most instances and the second should be done when needed.

1) Use a tool to collect/save/copy/print the content from the OSNC. One example is a tool called Camtasia⁵ that enables an investigator to save a video capture of the data presented on the computer monitor. Another tool noteworthy of mentioning is HTTrack⁶. According to the vendors website, the software allows investigators to "download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system."

2) Investigators can obtain court authorization to acquire the content and logs associated with an OSNC persona. The results of such a request can yield information not available from the "internet facing" OSNC. For example, the investigator will be typically presented with registration email addresses, Internet Protocol (IP) logs with dates/times of persona activity.

7. CONCLUSIONS AND OBSERVATIONS

In both private and public sector investigations, OSNC's can provide a great amount of evidentiary information. Arming an investigator with the purposed methodology detailed in this paper, initiates the process of potentially discovering more information about a suspect or targeted individual.

REFERENCES

Facebook. (2008, January 28). *Facebook*. Retrieved January 28, 2008, from Facebook: <http://www.facebook.com/>

Flickr. (2008, January 28). *Flickr*. Retrieved January 28, 2008, from Flickr: <http://www.flickr.com/>

Google. (2007, 11 28). *Google Alerts*. Retrieved 11 2008, 2007, from Google.com: www.google.com/alerts

Heckers, J. (2007, 11 19). *Three areas management must handle with delicacy*. Retrieved 11 28, 2007, from [bizjournals: http://www.bizjournals.com/business_resources/hr_careers/business_advice/employment/2007/11/19/column9.html](http://www.bizjournals.com/business_resources/hr_careers/business_advice/employment/2007/11/19/column9.html)

How Should We Conduct Investigations? (2007, December). *Directorship* , 10-11.

<http://video.google.com/>. (2008, January 28). <http://video.google.com/>. Retrieved January 28, 2008, from <http://video.google.com/>: <http://video.google.com/>

⁵ Camtasia is a product of TechSmith and can be reviewed at <http://www.techsmith.com/camtasia.asp>

⁶ HTTrack can be reviewed at <http://www.httrack.com/>

Internet World Stats. (2007, 11 11). *Internet Growth Statistics*. Retrieved 11 28, 2007, from www.internetworldstats.com: <http://www.internetworldstats.com/emarketing.htm>

Kazakoff, L. (2009, Spring). Care and feeding of blogs. *The Masthead* , p. 3.

Myspace. (2008, January 28). *Myspace*. Retrieved January 28, 2008, from Myspace: <http://www.myspace.com/>

Nielsen/NetRatings. (2006, 5 11). www.nielsen-netratings.com. Retrieved 11 28, 2007, from Nielsen/NetRatings: http://www.nielsen-netratings.com/pr/pr_060511.pdf

O'Reilly, T. (2005, 09 30). *What Is Web 2.0*. Retrieved 03 05, 2008, from Oreilly Net: <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>

Photobucket. (2008, January 28). *Photobucket*. Retrieved January 28, 2008, from Photobucket: <http://photobucket.com/>

WordPress. (2008, January 28). Retrieved January 28, 2008, from WordPress: <http://wordpress.org/>

YouTube. (2008, January 28). *YouTube*. Retrieved January 28, 2008, from YouTube: <http://youtube.com/>

ACKNOWLEDGEMENTS

This project was partially supported by Grant No. 2004-MU-MU-K001 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

AUTHOR BIOGRAPHY

Jonathan T. Rajewski is a Computer & Digital Forensics instructor at Champlain College and a Computer Forensic Examiner with the Vermont Internet Crimes Task Force in Burlington, Vermont. He has experience with both civil and criminal digital forensic investigations and in providing expert written and oral digital forensic testimony. He has served many high profile confidential clients and has worked alongside both international and local, state/federal governmental entities. Jonathan holds a B.S in Economic Crime Investigation and the following professional certifications: Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCe), Certified Fraud Examiner (CFE) and Certified Information Systems Security Professional (CISSP).