



Annual ADFSL Conference on Digital Forensics, Security and Law

2015
Proceedings

May 21st, 11:30 AM

Tracking Criminals on Facebook: A Case Study From A Digital Forensics REU Program


Daniel Weiss

University of Arizona, dweiss@email.arizona.edu

Gary Warner

University of Alabama at Birmingham, Director of Research in Computer Forensics

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

 Part of the [Aviation Safety and Security Commons](#), [Computer Law Commons](#), [Defense and Security Studies Commons](#), [Forensic Science and Technology Commons](#), [Information Security Commons](#), [National Security Law Commons](#), [OS and Networks Commons](#), [Other Computer Sciences Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Scholarly Commons Citation

Weiss, Daniel and Warner, Gary, "Tracking Criminals on Facebook: A Case Study From A Digital Forensics REU Program" (2015). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 4.
<https://commons.erau.edu/adfsl/2015/thursday/4>

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



TRACKING CRIMINALS ON FACEBOOK: A CASE STUDY FROM A DIGITAL FORENSICS REU PROGRAM

Daniel Weiss
University of Arizona
dweiss@email.arizona.edu

Gary Warner
University of Alabama at Birmingham
Director of Research in Computer Forensics
gar@cis.uab.edu

ABSTRACT

The 2014 Digital Forensics Research Experience for Undergraduates (REU) Program at the University of Alabama at Birmingham (UAB) focused its summer efforts on tracking criminal forums and Facebook groups. The UAB-REU Facebook team was provided with a list of about 60 known criminal groups on Facebook, with a goal to track illegal information posted in these groups and ultimately store the information in a searchable database for use by digital forensic analysts. Over the course of about eight weeks, the UAB-REU Facebook team created a database with over 400 Facebook groups conducting criminal activity along with over 100,000 unique users within these groups. As of November 2014, students involved in the research project with Advisor Gary Warner at UAB continued running the automated fetchers since my summer projected completed. Working with U.S. Federal Law Enforcement agencies, there have been at least NINE CONFIRMED ARRESTS of individuals associated with the illegal activities tracked on Facebook. This paper will discuss the methods used to collect the information, store it in a database and analyze the data. The paper will also present possible future uses of the Facebook criminal activity-monitoring tool.

Keywords: social media, criminal organizations, online crime, social network monitoring

1. INTRODUCTION

For the past five years, the UAB Computer Forensics Research Lab has participated in the National Science Foundation Research Experience for Undergrads (REU) program. During the summer of 2014, the Digital Forensics REU team focused on developing tools for automating the gathering and analysis of the communications between criminals in online forums and on Facebook groups. The UAB-REU summer 2014 research project created a searchable database that keeps track of the growing criminal activity on Facebook. Our case study has a growing database that can keep track of everything on a Facebook group from posts, comments, likes, as well as the user who posted the respective post, the time it was posted, and any image that was posted in a post or comment. This data can be used to draw connections between active users within different

groups and lead to arrests if proven criminal acts were performed. Many of the messages that we stored within the database contained credit card numbers associated with other personal information as well.

2. LITERATURE REVIEW

Previous REU cohorts have examined the methods in which criminals learn and encourage one another's criminal behavior through online social interaction in the area of phishing. (Levin, Richardson, Warner, & Kerley, 2012) Others have explored the role of online social media networks in the creation and execution of large international markets for stolen data and identities. Several researchers have examined online web forums that were designed primarily to support international trade in stolen goods and identities. (Holt & Smirnova, 2014), (Motoyama, McCoy,

Levchenko, Savage, & Voelker, 2011), (Merces, 2011) As criminals and terrorist grow more brazen, they have realized that the use of secretive online forums is not necessary when Facebook traffic is largely unregulated and unmoderated and represents minimal risk of prosecution or incarceration. The House Homeland Security Committee held hearings on “Jihadist Use of Social Media” in 2011 where testimony included “The Antisocial Network” where it was remarked how little concern adversaries have about discovery. (Kohlman, 2011)

The Law Reviews and Journals are beginning to fill with articles about the use of evidence from social media in the courts. Many of the opinions expressed in those articles helped to make the case for the existence of this project. One current trend in this debate is whether messages shared “quasi-privately” only to a chosen community of friend’s withstood Fourth Amendment challenges regarding expectations of privacy. (Sholl, 2013) Others have argued about the admissibility of such evidence, partly with regards to whether it constituted heresay under Federal Rules of Evidence. (Holt & San Pedro, 2014) Still others argue about the authentication of the evidence and how to prove the origins and identify of the poster. (Griffith, Winter 2012).

To address all of these concerns, evidence would need to be gathered in a repeatable and automated way that preserved the timestamp and ‘userid’ of the creator of the evidence, and only from pages that could be shown to be publicly “Open.”

3. FACEBOOK AS OPEN SOURCE INTELLIGENCE

3.1. Problem Statement Summary

The UAB-REU Facebook team was given a list of known criminal groups on Facebook, and was asked to track these groups over the summer of 2014. Specifically, the following was to be accomplished by the end of the summer. Can we quickly decide if a Facebook group is discussing criminal activity and if so, can we characterize what types of activities they do or targets they are after. For example is the criminal activity credit

card fraud, stolen electronics, shipping of illegal or stolen items, viruses, malware, botnets, spamming, and even terrorists organizations or supporters of terrorists. We also wanted to be able to identify the most influential, and or important people, and or most active users within a group. By the end of summer our goal was to be tracking at least 200 criminal Facebook groups. With these goals in mind we set out to develop code to request and retrieve the wanted information from Facebook, and store the information into a searchable database where we could easily query the data for further investigations.

3.2. Facebook’s Graph Application Programming Interface (API)

The API is on the developer side of Facebook and is a great tool that we used over the summer project. “The graph API is the primary way to get data in and out of Facebook’s social graph (network).”¹ Essentially the Graph API allows a user to post, delete, and also get information to and from Facebook. The graph API was a tremendous asset for our team because it allowed us to query many useful searches directly without having to perform many iterations to gather wanted information, however to do so an Access Token was required.

3.2.1. The Basics

The Graph API is a representation of the information on Facebook, which is composed of nodes, edges, and fields. Nodes are basically the “things” on Facebook. Ex. Users, Photos, Posts. Edges are the connections between nodes, such as a comment or a like on a photo. Fields are the information about nodes. For example, a node that is a user can have a field such as their birthday or hometown.

3.2.2. Using the Graph API to find more criminal groups

To find more criminal Facebook groups, we used the Graph API, and searched for groups with specific keywords. Group names that had the word such as “Hacker” or “CVV” within their

¹ Graph API Overview
<https://developers.facebook.com/docs/graph-api/overview>

name were added to our list of criminal groups. Even though it was not for sure that these groups were criminal our database queries later on would tell us. Figure 1 below shows the Graph API

searching for all groups with the word “Hacking” in its’ name. Our team developed a “Bag of Words” which essentially was a list of keywords that we used to find new Facebook groups.

The screenshot shows the Graph API Explorer interface. At the top, there's a header with 'Graph API Explorer' and 'Application: [?] Graph API Explorer'. Below that, an 'Access Token' field contains a long alphanumeric string. The main area has two tabs: 'Graph API' and 'FQL Query'. A 'GET' dropdown is visible. The URL bar shows a search query: `→ /v2.0/search?type=group&q=Hacking&access_token=`, which is highlighted with a red box. An arrow labeled 'Keyword Search' points to this box. Below the URL bar, there's a section for 'Node: search' with checkboxes for 'q (Hacking)', 'type (group)', and 'access_token'. To the right, a JSON response is displayed, listing several groups with their names and IDs.

```

{
  "data": [
    {
      "name": "Hacking News And Tutorials",
      "id": "280648318751472"
    },
    {
      "name": "HackingMexico",
      "id": "415634755176912"
    },
    {
      "name": "Hacking",
      "id": "678674505545853"
    },
    {
      "name": "HackingMexico-FRAUDE",
      "id": "243478312496400"
    },
    {
      "name": "Hacking",
      "id": "433051603501364"
    },
    {
      "name": "Hacking tricks",
      "id": "340924266032625"
    }
  ]
}

```

Figure 1 Graph API Search

Source: <https://developers.facebook.com>

3.2.3. Facebook Privacy

The Graph API is a very handy tool that Facebook has allowed the public to use. However, Facebook privacy still comes into play when using the API. Facebook groups that have a Privacy status of Open, meaning anyone can see the group and join it, or a status of Closed, meaning anyone can see the group but must request to join the group can be seen through the Graph API. A group that is secret will not show up on the API. A secret group has no record of existing through any means of searches; the only way to be in a secret group is

by getting invited to join the group. Of course being in a closed or secret group allows users to see everything going on within the group making the group ‘Open’ to the users within. Figure 2 and Figure 3 below are examples of an open and a closed group. Notice the difference in the amount of information between the Open and Closed group. Figure 4 below is an example of a closed group that the current Facebook user on the Graph API was a member of. Notice that it now looks like an open group.

The screenshot shows a web browser interface for the Facebook Graph API. At the top, there is a search bar with the URL `https://graph.facebook.com/v2.0/563652277096630` and a 'Submit' button. Below the search bar, there is a link to 'Learn more about the Graph API syntax.' The main content area is divided into two panels. The left panel shows the node ID '563652277096630' and a search field with the text '+ Search for a field'. The right panel displays a JSON response from the API:

```
{
  "id": "563652277096630",
  "owner": {
    "id": "327410144075244",
    "name": "Beef Cent"
  },
  "name": "BEEF GH ***CCV STRONG CARDS*** KILL THEM ALL****T-MOBILE****MORE STORES****",
  "venue": {
    "street": ""
  },
  "privacy": "OPEN",
  "icon": "https://fbstatic-a.akamaihd.net/rsrc.php/v2/yy/r/LYLLqQ00kcP.png",
  "updated_time": "2014-07-21T15:35:44+0000",
  "email": "563652277096630@groups.facebook.com"
}
```

Figure 2 Open Group Example
Source: <https://developers.facebook.com>

The screenshot shows a web browser interface for the Facebook Graph API. At the top, there is a search bar with the URL `https://graph.facebook.com/v2.0/217979238297595?fields=members` and a 'Submit' button. Below the search bar, there is a link to 'Learn more about the Graph API syntax.' The main content area is divided into two panels. The left panel shows the node ID '217979238297595' and a search field with the text '+ Search for a field'. Below the search field, there is a checkbox labeled 'members' which is checked. The right panel displays a JSON response from the API:

```
{
  "id": "217979238297595"
}
```

Figure 3 Closed Group non-Member Example
Source: <https://developers.facebook.com>

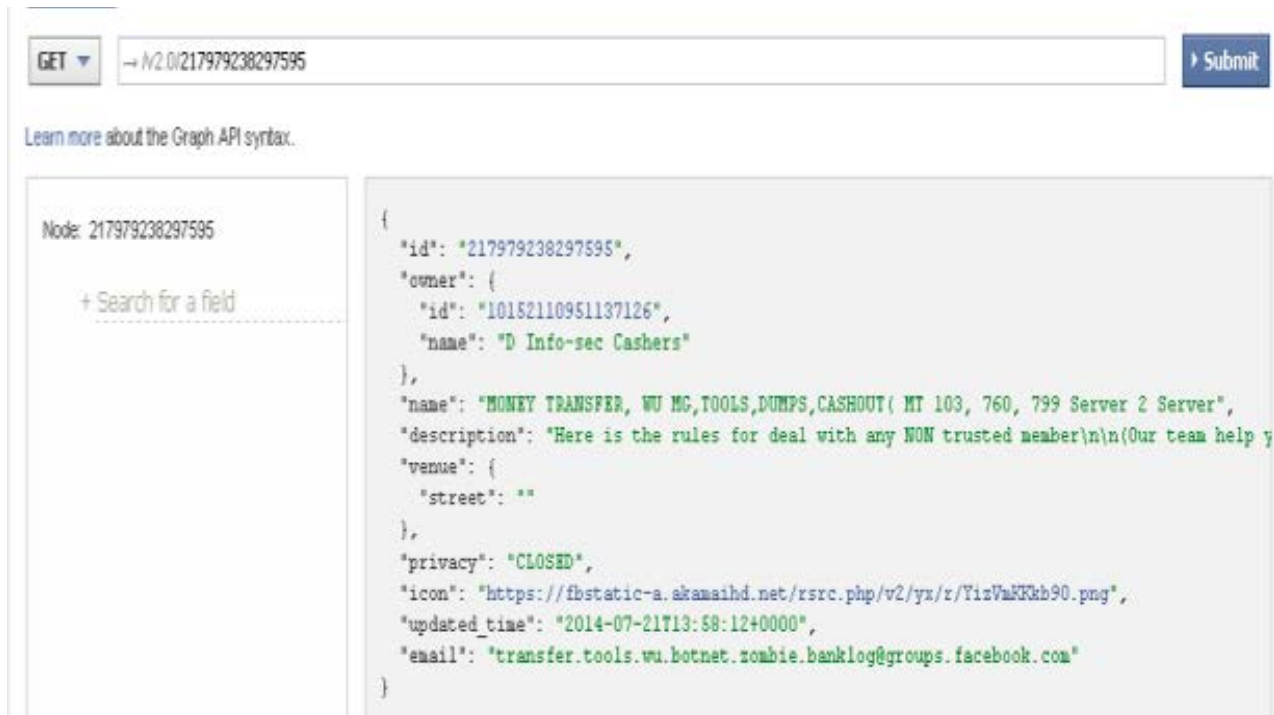


Figure 4 Closed Group Member Example

Source: <https://developers.facebook.com>

3.2.4. Aliases

When collecting group ID numbers to run through the fetcher we realized that we were only able to pull information from a group that was open. To fix this issue we created Facebook aliases that looked like cyber criminals. We made two main accounts in particular and tried joining as many of the closed groups that we had found through the Graph API as possible. As a matter of fact it was not very hard to get accepted to a number of these groups. Once accepted into these groups we would run the Graph API with our alias' Access Token and then run the fetcher. This was a huge step in our summer research as it allowed us to gather a considerably larger amount of data.

4. CODE IMPLEMENTATION

4.1. Automation of the Graph API

The program for extracting the information from Facebook was written in Java. The code used a library package called RestFB, which allowed for direct access to the Graph API while in Java. We would supply the Graph API with a Group ID

number and then would retrieve all of the group's members, posts, comments, likes, pictures, etc.

4.2. The Database

Our team created an SQL database to store the data retrieved from Facebook and make it easy to search for wanted results. In SQL, several different tables were created to easily make connections between users and groups. Within Java we coded to put all of the comments within its own SQL searchable table for example. Similarly tables were used to store information for images, posts, and groups. We created a user group's table that allowed us to connect users to multiple groups because there were many instances where the same user belonged to more than one group in our database, and this allowed for a connection between the two.

5. RESULTS

Within the database we ran queries to achieve the goals we set out in the beginning of the summer. We were able to determine if a Facebook group was talking about criminal activity, what kind of activity, and the 'big' players within those groups

as well. By the end of the summer after about two weeks of data collection, the database had over 400 criminal groups that we were tracking and fetching information from. Within those 400 groups, there were over 100,000 unique users in those groups, about 50,000 posts, and about 40,000 comments on posts.

keyword. The query searched for posts containing the word 'fbi'. Many other related queries searched for posts containing the words 'cia' or 'vbv'(Verified By Visa, a common term used by credit card criminals.) i.e. and counted the number of occurrences, displaying then the top ten groups.

The following query looked for messages within the group's posts' that contained a certain

Table 1: Results for the 'fbi' query

count	Groupid	name
19	183381435133188	SPAMER's
11	229655640389234	KING OF HACKER
10	505516012807000	DDOS
9	230749693747529	! P4K OR4Kz4I H4CkERX !
8	465238643517306	Bestbikes Grupo ventas Nacional
8	165155633573484	WESTERN UNION
7	290630927627110	Genius Hackers
6	126115430891994	SaDaM Khakwani All Hacking TrickXx & Tip\$
6	112852328867059	HACKERS SPOTTED :)))
6	14929934514034	Hack With Stylee (Hacking Zone)

The following query searched for messages that contained a string of 15 or 16 digits, because that was our credit card number identifier if groups were sharing stolen credit cards with one another.

The query below shows the results for the top four group's sharing Visa credit cards. Our query searched for the number four followed by another 15 digits 0-9.

Table 2: Results for the Visa query

count	Fb_group.Groupid	Fb_group.name
432	435715723187958	PRO SHOPPER'S TUT AND BINS AND STORES
402	563652277096630	REEF GH ***CCV STRONG CARDS*** KILL THEM ALL
376	384945978297975	PRO SHOPPERS ***KILL, WAL,KMAR,SEAR, AND BEST

256	1422518178033504	*** KILL CREDIT CARD***
-----	------------------	-------------------------

The following query took a group that talked about visa credit card numbers frequently and displayed

the message along with the user who posted it. (Card numbers have been altered for privacy.)

Table 3: Results for the Visa query

userid	name	substring
100008366380917	Nana Less	4266841341509999 02/17 597 Sue Lowe 123 sixth street Calvin LA 71410
100008366380917	Nana Less	4185866411539999 06/16 417 Debra Duhon 300 Big Pasture Rd Lake Charles LA
100000835312440	Okoeokoso More-vimlated Vim-carders	high balance cc 4347696620159999 1016 919 Cynthia Kroecker 11817 SW 1 st Yukon OK 73099
100005869085570	Undergrad Carder	428208712259999 1014 578 Martin Ibarra 1108 E ORTEGA ST Santa Barbara C

6. FUTURE USES

After just a short eight weeks in this REU program, and after only two weeks of actual data collection, results were huge. As of November 2014, students involved in the research project with Advisor Gary Warner at UAB continued running the automated fetchers since my summer projected completed. After the REU program completed for the summer, the tool became the anchor of a new Open Source Intelligence effort within the lab. The database now contains over a half million Facebook messages and replies and is monitoring more than 900 Facebook groups. The most prolific of these groups that were found to be dedicated to criminal activity have logged well over 5,000 messages each from as many as 1,800 distinct Facebook users. The tool has been used to learn more about criminal groups for many Federal, state, and local law enforcement investigations. Original conceived to assist in cybercrime cases, investigations have included tracking of many types of Facebook groups including “carders” (criminals who steal and trade

credit cards), “booters” (criminals who sell DDOSing services), online sexual harassment via webcam-controlling botnets, street gangs selling illegal drugs and weapons, and counter-terrorism investigations. Hundreds of Facebook groups have been reported and terminated, while others are left intact to identify ring-leaders and, working with major US-based shipping companies and retailers, to intercept the shipment of stolen packages. Working with an inter-agency task force on violent crime, Facebook evidence from this project was used to document relationships between criminals as well as proof of weapons and drug possession from photos shared on Facebook in support of a RICO case that led to nine felony arrests.

The project has also led to additional publications that have been focused on image analysis of the profile pictures. Hackers often use Guy Fawkes masks in profiles pictures, carders often have images of credit cards in their profile pictures, and jihadists often have Islamic State flags on their profile pictures. In addition to keyword clues,

these new image analysis tools allow a group to be quickly categorized, even when the language used in the messages is not understood by the analyst. Implementation of a tool like this would have a great impact on the cyber world, as it would aid in the capture of cyber criminals.

7. CONCLUSION

The 2014 Digital Forensics REU program at UAB provided students with the opportunity to develop real world applications with valuable outcomes. Our 2014 project identified criminal activity on Facebook, collected evidence and ultimately helped prosecute and punish criminals. The UAB-REU Facebook team created a searchable database that could be used by law enforcement and intelligence agencies, as well as private sector shipping companies, banks, and credit card companies to identify criminal activity and work with law enforcement to prosecute those responsible for the illegal activity.

REFERENCES

1. BIBLIOGRAPHY

- Allen, M. (2010). Retrieved from restfb.com
- Burgess, E., & Metz, E. (2008). Applying Google Mini search appliance for document discoverability. *Online*, 32(4), 25-27.
- Chan, A. (2009, July). *Google to the (E-Discovery) rescue?* Retrieved January 11, 2013, from eDiscovery: <http://ediscovery.quarles.com/2009/07/articles/information-technology/google-to-the-ediscovery-rescue/>
- Cheek, J. M., & Buss, A. H. (1981). Shyness and sociability. *Journal of personality and social psychology*, 41(2), 330.
- Clark, J. (2005). *AnandTech Search goes Google*. Retrieved January 11, 2013, from anandtech.com: <http://www.anandtech.com/show/1781/3>
- Claypool, M., Le, P., Wased, M., & Brown, D. (2001). Implicit interest indicators. *Proceedings of the 6th international conference on Intelligent user interfaces* (pp. 33-40). ACM.
- Colombini, C., & Colella, A. (2013). Digital profiling: A computer forensics approach. *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, 330-343.
- Colombini, C., Colella, A., & Italian Army. (2012). Digital scene of crime: technique of profiling users. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*.
- Compton, D., & Hamilton, J. (2011). An Examination of the Techniques and Implications of the Crowd-sourced Collection of Forensic Data. *Third International Conference on Privacy, Security, Risk and Trust (PASSAT)* (pp. 892-895). IEEE.
- Cuff, J. (2009). Key trends and developments of rights information management systems—An interview with Jim Cuff of Iron Mountain Digital. *Journal of Digital Asset Management*, 5(2), 98-110.
- Denning, D. E., & Baugh Jr., W. E. (1999). Hiding crimes in cyberspace. *Information, Communication & Society*, 2(3), 251-276.
- Ericsson, K. A., Krampe, R. T., & Tesch-Römer, C. (1993). The role of deliberate practice in the acquisition of expert performance. *Psychological Review*, 100(3), 363.
- Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.
- Garrison, J. (2012, December 11). *Google Mini Search Appliance Teardown*. Retrieved July 8, 2013, from <http://1n73r.net/2012/12/11/google-mini-search-appliance-teardown/>
- Gaw, S., & Felten, E. (2006). Password management strategies for online

- accounts. *Proceedings of the second symposium on Usable privacy and security* (pp. 44-45). ACM.
- Google. (2013a). *Google Mini Help*. Retrieved January 11, 2013, from Google Web Site: <http://support.google.com/mini/?hl=en#topic=219>
- Google. (2013b). *Google Mini: Information*. Retrieved January 11, 2013, from Google web site: http://lp.google-mkto.com/NORTHAMSearchLCSMiniEndofLife_GoogleMiniFAQs.html
- Google. (2013c). *Google Mini Report Overview*. Retrieved January 11, 2013, from Google web site: http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.ie/en/ie/enterprise/mini/library/MiniReports.pdf
- Google. (2013d). *First-Time Startup of a Google Search Appliance*. Retrieved January 15, 2013, from Google web site: <https://developers.google.com/search-appliance/documentation/50/installation/InstallationGuide#FirstTime>
- Google. (2013e). *Google Mini Help Center*. Retrieved June 30, 2013, from Google web site: https://developers.google.com/search-appliance/documentation/50/help_mini/home
- Google. (2013f). *Google Mini License Agreement v3.0*. Retrieved July 8, 2013, from Google web site: <http://1n73r.net/wp-content/uploads/2012/12/google-mini-eula.pdf>
- Grabosky, P. (2000). Computer crime: A criminological overview. *Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. Vienna.
- Griffith, H. L. (Winter 2012). Understanding and Authenticating Evidence from Social Networking Sites. *Washington Journal of Law, Technology & Arts*.
- Herley, C. (2012). Why do Nigerian Scammers say they are from Nigeria? *WEIS*.
- Holt, M. R., & San Pedro, V. (2014). Social Media Evidence: What you can't use won't help you - Practical considerations for using evidence gathered on the Internet. *The Florida Bar Journal*.
- Holt, T. J., & Smirnova, O. (2014). *Examining the Structure, Organization and Processes of the International Market for Stolen Data*. Washington DC: National Criminal Justice Reference Service.
- Jenkins, C., Corritore, C. L., & Weidenbeck, S. (2003). Patterns of information seeking on the Web: A qualitative study of domain expertise and Web expertise. *IT & Society*, 1(3), 64-89.
- Kohlman, E. (2011, 12 6). *The Antisocial Network: countering the use of online social networking technologies by foreign terrorist organizations*. Retrieved from House.gov: [homeland.house.gov/sites/homeland.house.gov/files/Testimony Kohlmann\[1\].pdf](http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Kohlmann%2012-06-12.pdf)
- Krone, T. (2004). *A typology of online child pornography offending*. Australian Institute of Criminology.
- Larrieu, T. (2009). *Crawling the Control System*. No. JLAB-ACO-09-1072; DOE/OR/23177-1007. Newport News, VA: Thomas Jefferson National Accelerator Facility.
- LaTulippe, T. (2011). Working Inside the Box: An Example of Google Desktop Search in a Forensic Examination. *Journal of Digital Forensics, Security and Law*, 6(4), 11-18.
- Levin, R., Richardson, J., Warner, G., & Kerley, K. (2012). Explaining Cybercrime through the Lens of Differential Association Theory. *eCrime Researchers Summit* (pp. 1-9). Las Croabas, Puerto Rico: IEEE.
- McElhaney, S., & Ghani, S. (2008). Enterprise Search and Automated Testing. *Governance, Risk, and Compliance Handbook: Technology, Finance,*

- Environmental, and International Guidance and Best Practices*, 267.
- Merces, F. (2011). *The Brazilian Underground Market: The Market for Cybercriminal Wannabes?* Retrieved from Trend Micro: www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf
- Merritt, K., Smith, D., & Renzo, J. (2005). An investigation of self-reported computer literacy: Is it reliable. *Issues in Information Systems*, 6(1), 289-295.
- Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. *2011 ACM SIGCOMM conference on Internet measurement* (pp. 71-80). NY: ACM.
- Ngo, F. T., & Parternoster, R. (2011). Cybercrime victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 5(1), 773-793.
- Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation*, 2(4), 261-267.
- Orr, E., Sisic, M., Ross, C., Simmering, M. G., Arseneault, J. M., & Orr, R. R. (2009). The influence of shyness on the use of Facebook in an undergraduate sample. *CyberPsychology & Behavior*, 12(3), 337-340.
- Radianti, J., Rich, E., & Gonzalez, J. J. (2009). Vulnerability black markets: Empirical evidence and scenario simulation. *42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.
- Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, 3(2), 97-102.
- Rogers, M. K. (2010). The Psyche of Cybercriminals: A Psycho-Social Perspective. In *Cybercrimes: A Multidisciplinary Analysis* (pp. 217-235). Springer Berlin Heidelberg.
- Scealy, M., Phillips, J. G., & Stevenson, R. (2002). Shyness and anxiety as predictors of patterns of Internet usage. *CyberPsychology & Behavior*, 5(6), 507-515.
- Sholl, E. W. (2013). Exhibit Facebook: The Discoverability and Admission of Social Media Evidence. *Tulane Journal of Technology and Intellectual Property*.
- Topalli, V. (2004). Criminal expertise and offender decision-making: An experimental analysis of how offenders and non-offenders differentially perceive social stimuli. *British Journal of Criminology*, 45(3), 269-295.
- United States Government. (2013, September 27). *Criminal Complaint*. Retrieved October 11, 2013, from <http://www.scribd.com/doc/172773407/Ubriicht-Criminal-Complaint-Silk-Road>
- Warren, P., & Streeter, M. (2006). Cyber alert: How the world is under attack from a new form of crime. Vision Paperbacks.
- Wright, R., Logie, R. H., & Decker, S. H. (1995). Criminal expertise and offender decision making: An experimental study of the target selection process in residential burglary. *Journal of Research in Crime and Delinquency*, 32(1), 39-53.