Cyber Profiling: Using Instant Messaging Author Writeprints for Cybercrime Investigations

By Angela Orebaugh, Jason Kinser, and Jeremy Allnutt

The explosive growth in the use of instant messaging (IM) communication in both personal and professional environments has resulted in an increased risk to proprietary, sensitive, and personal information and safety due to the influx of IM-assisted cybercrimes, such as phishing, social engineering, threatening, cyber bullying, hate speech and crimes, child exploitation, sexual harassment, and illegal sales and distribution of software. IM-assisted cybercrimes are continuing to make the news with child exploitation, cyber bullying, and scamming leading last month's headlines. Instant messaging's anonymity and use of virtual identities hinders social accountability and presents a critical challenge for cybercrime investigation. Cyber forensic techniques are needed to assist cybercrime decision support tools in collecting and analyzing digital evidence, discovering characteristics about the cyber criminal, and assisting in identifying cyber criminal suspects.

Introduction

The anonymous nature of the Internet allows online criminals to use virtual identities to hide their true identity to facilitate cybercrimes. Although central IM servers authenticate users upon login, there is no means of authenticating or validating peers (buddies). Current IM products are not addressing the anonymity and ease of impersonation over instant messaging. Author writeprints can provide cybercrime investigators a unique tool for analyzing IM-assisted cybercrimes. Writeprints are based on behavioral biometrics, which are persistent personal traits and patterns of behavior that may be collected and analyzed to aid a cybercrime investigation. (Li et al., 2006) Instant messaging behavioral biometrics include online writing habits, known as stylometric features, which may be used to create an author writeprint to assist in identifying an author, or characteristics of an author, of a set of instant messages. The writeprint is a digital fingerprint that represents an author's distinguishing stylometric features that occur in his/her computer-mediated communications. Writeprints may be used as input to a criminal cyberprofile and as an element of a multimodal system for cybercrime investigations. Writeprints can be used in conjunction with other evidence, criminal investigation techniques, and biometrics techniques to reduce the potential suspect space to a certain subset of suspects; identify the most plausible author of an IM conversation from a group of suspects; link related crimes; develop an interview and interrogation strategy; and gather convincing digital evidence to justify search and seizure and provide probable cause.

Instant Messaging and Cybercrime

Instant messaging's anonymity hinders social accountability and leads to IM-assisted cybercrime facilitated by the following:

- Users can create any virtual identity,
- Users can log in from anywhere,
- Files can be transmitted, and
- Communication is often transmitted unencrypted.

In IM communications, criminals use virtual identities to hide their true identity. They can use multiple screen names or impersonate other users with the intention of harassing or deceiving unsuspecting victims. Criminals may also supply false information on their virtual identities, for example a male user may configure his virtual identity to appear as female. Since most IM systems use the public Internet, the risk is high that usernames and passwords may be intercepted, or an attacker may hijack a connection or launch a man-in-the-middle (MITM) attack. With hijacking and MITM attacks, the victim user thinks he/she is communicating with a buddy but is really communicating with the attacker masquerading as the victim's buddy. Instant messaging's anonymity allows cyber criminals such as pedophiles, scam artists, and stalkers to make contact with their victims and get to know those they target for their crimes (Cross, 2008). IM-assisted cybercrimes, such as phishing, social engineering, threatening, cyber bullying, hate speech and crimes, child exploitation, sexual harassment, and illegal sales and distribution of software are continuing to increase (Moores and Dhillon, 2000). Additionally, criminals such as terrorist groups, gangs, and cyber intruders use IM to communicate (Abbasi and Chen, 2005). Criminals also use IM to transmit worms, viruses, Trojan horses, and other malware over the Internet.

With increasing IM cybercrime, there is a growing need for techniques to assist in identifying online criminal suspects as part of the criminal investigation. Cyber forensics is the application of investigation and analysis techniques to gather evidence suitable for presentation in a court of law with the goal of discovering the crime that took place and who was responsible (Bassett et al., 2006). With IM communications, it is necessary to have cyber forensics techniques to assist in determining the IM user's real identity and collect digital evidence for investigators and law enforcement.

Behavioral Biometrics Writeprints for Authorship Analysis

Determining an IM user's real identity relies on the fact that humans are creatures of habit and have certain persistent personal traits and patterns of behavior, known as behavioral biometrics (Revett, 2008). Online writing habits, known as stylometric features, include composition syntax and layout, vocabulary patterns, unique language usage, and other stylistic traits. Thus, certain stylometric features may be used to create an author writeprint to help identify an author of a particular piece of work (De Vel et al., 2001). A writeprint represents an author's distinguishing stylometric features that occur in his/her instant messaging communications. These stylometric features may include average word length, use of punctuation and special characters, use of abbreviations, and other stylistic traits. Writeprints can provide cybercrime investigators a unique behavioral biometric tool for analyzing IM-assisted cybercrimes. Writeprints can be used as input to a criminal cyberprofile and as an element of a multimodal system to perform cyber forensics and cybercrime investigations.

Instant messaging communications contain several stylometric features for authorship analysis research. Certain IM specific features such as message structure, unusual language usage, and special stylistic markers are useful in forming a suitable writeprint feature set for authorship analysis (Zheng et al., 2006). The style of IM messages is very different than that of any other text used in traditional literature or other forms of computer-mediated communication. The real time, casual nature of IM messages produces text that is conversational in style and reflects the author's true writing style and vocabulary (Kucukyilmaz et al., 2008). Significant characteristics of IM are the use of special linguistic elements such as abbreviations, and computer and Internet terms, known as netlingo. The textual nature of IM also creates a need to exhibit emotions. Emotion icons, called emoticons, are sequences of punctuation marks commonly used to represent feelings within computer-mediated text (Kucukyilmaz et al., 2008). An author's IM writeprint may be derived from network packet captures or application data logged during an instant messaging conversation. Although some types of digital evidence, such as source IP addresses, file timestamps, and metadata may be easily manipulated, author writeprints based on behavioral biometrics are unique to an individual and difficult to imitate.

Creating IM Writeprints

A stylometric feature set is composed of a predefined set of measurable writing style attributes. Given t predefined features, each set of IM messages for a given author can be represented as a t-dimensional vector, called a writeprint. Figure 1 presents a stylometric feature set for a 356-dimensional vector writeprint with lexical, syntactic, and structural features. (Orebaugh et al., 2014) The number of features in each category is shown in parenthesis.

Lexical features mainly consist of count totals and are further broken down into emoticons, abbreviations, word-based, and character-based features. Syntactic features include punctuation and function words in order to capture an author's habits of organizing sentences. Function words include conjunctions, prepositions, and other words that carry little meaning when used alone, such as "the" or "of". They

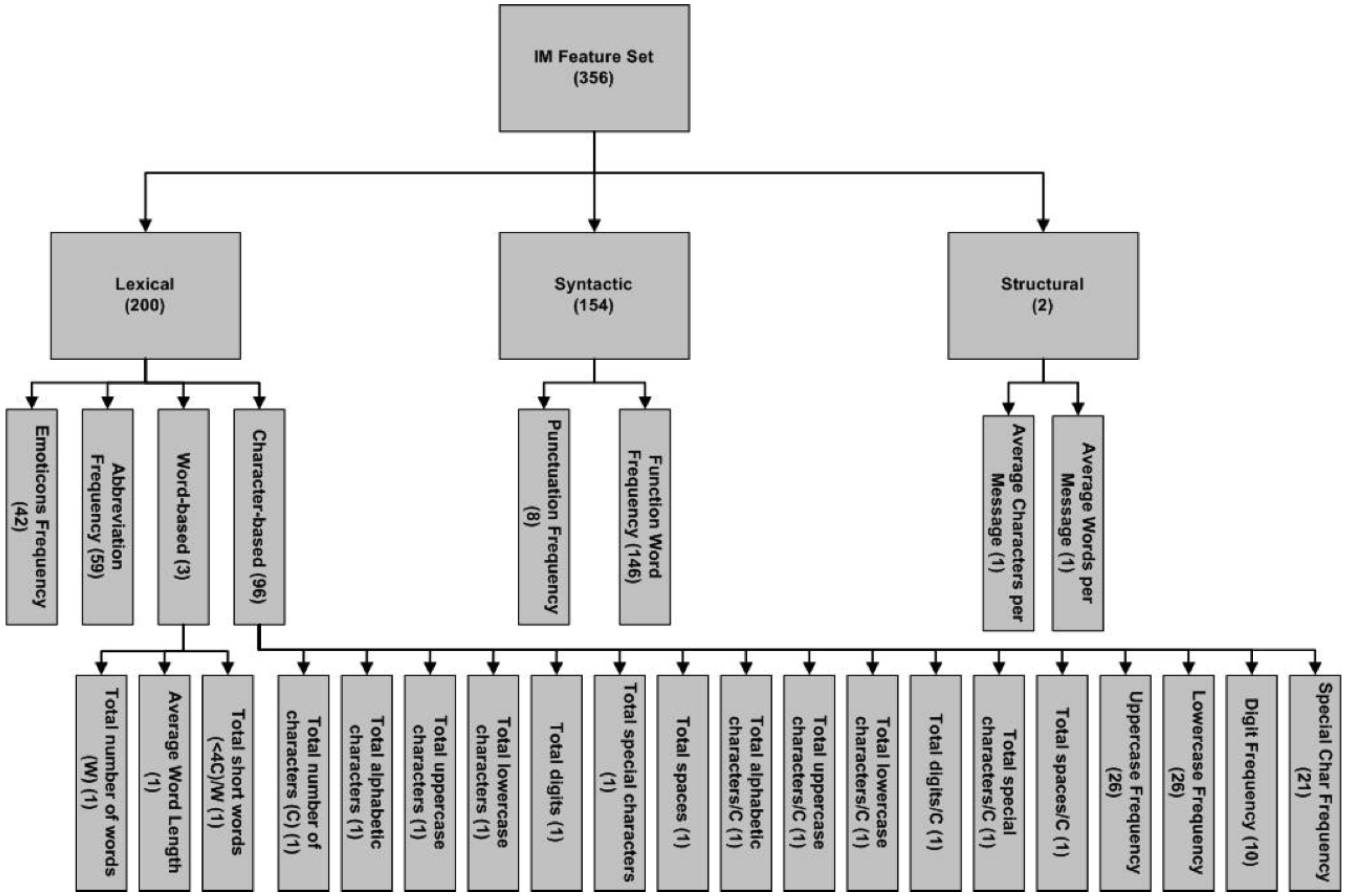

IM Feature Set (356)
Lexical (200)
Syntactic (154)
Structural (2)
Emoticons Frequency (42)
Abbreviation Frequency (59)
Word-based (3)
Character-based (96)
Punctuation Frequency (8)
Function Word Frequency (146)
Average Characters per Message (1)
Average Words per Message (1)
Total number of words (W) (1)
Average Word Length (1)
Total short words (<4C)/W (1)
Total number of characters (C) (1)
Total alphabetic characters (1)
Total uppercase characters (1)
Total lowercase characters (1)
Total digits (1)
Total special characters (1)
Total spaces (1)
Total alphabetic characters/C (1)
Total uppercase characters/C (1)
Total lowercase characters/C (1)
Total digits/C (1)
Total special characters/C (1)
Total spaces/C (1)
Uppercase Frequency (26)
Lowercase Frequency (26)
Digit Frequency (10)
Special Char Frequency (21)

Figure 1. IM Writeprint Feature Set

provide relationships to content words in the sentence, such as "ball" or "bounce". Analyzing function words as opposed to content words allows topic-independent results that reflect an author's preferred ways to express himself or herself and form sentences. Structural features capture the way an author organizes the layout of text. With IM communications there are no standard headers, greetings, farewells, or signatures, leaving simply the average characters and words per message in terms of structural layout. A list of function words, abbreviations, and emoticons are included in Appendix A.

Writeprints are created by generating totals for each stylometric feature, resulting in the output of a writeprint (W_x) for a set of messages $\{M_1,\ldots,M_p\}$ for an author (A_n) or author category (C_m). A writeprint may be viewed in a comma-separated value (CSV) format where each value represents a total for a specific feature. An example writeprint for an author A_n using a selected feature set $\{F_1,\ldots,F_q\}$, where q =100, for a set of messages $\{M_1,\ldots,M_p\}$ looks like the following:

```
105,1,0,0,4,0,1250,0,4,0,18,
8,1,2,0,0,0,0,1,9,0,14,31,6.
78,3.71,23,0,67,4,25,5,0,117
,5,0,1,4,0,0,23,0,0,0,8,0,23
,1,3,0,27,50,0,0,1550,0,7,0,
0,0,1,0,1250,33,0,13,1,0,0,0
,2,85,0,0,0,4,0,0,0,0,0,96,1
,0,0,0,13,0,3,0,10,0,2,0,0,0
,1,2,16,0,0.806
```

After writeprints are generated they may then be normalized, standardized, and input into various statistical models for analysis. Figure 2 shows the output of the Principal Component Analysis (PCA) model for writeprints for seven authors. (Orebaugh et al., 2014) The figure shows the first 3 principal components for multiple author conversations, mapped in three-dimensional space. In this example, each author has a relatively well-defined cluster representing his or her writeprint. Different authors separate from each other, while multiple conversations of an author cluster together.

This type of example may be used in an investigation to show that sample evidentiary writeprints do or do not overlap with certain suspect writperints, thus helping investigators narrow the suspect space, develop an interrogation strategy, link related crimes, or justify probable cause.

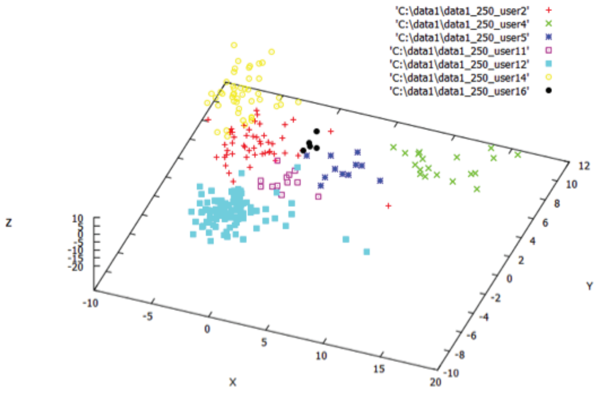


Figure 2. IM Writeprint PCA Output

Cybercrime Investigations and IM

Many disciplines including psychology, philosophy, sociology, criminology, law, knowledge management, and computer science have studied the criminal investigation process. Although cybercrime is a relatively new form of crime that has rapidly evolved over the last few decades, cybercrime investigations and traditional criminal investigations share the same goal – to gather information. Figure 3 illustrates the traditional criminal investigation process as presented in *Scene of the Cybercrime* (Cross, 2008).

The investigator first determines if an act has violated the law and warrants an investigation. Next, evidence is collected and analyzed, including tangible evidence such as hard drives and electronic devices, and the digital evidence they contain. Cybercrime investigations for IM rely on instant messaging exchanges, or conversations, as digital evidence. The sources for IM digital evidence include both data and meta-data. The data includes the IM text and the meta-data includes other related evidence such as the IM client version, timestamps, the length of time the user has been logged on, etc. The next step involves seeking expert advice if necessary. Often times in cybercrime cases the investigator needs to seek expert advice on the technical aspects of the crime. Experts may be on staff, or may be located from professional organizations, consultants, or the academic community. For IM related cybercrimes expert witnesses may include linguists, communication experts, or social psychologists. The next step of interviewing witnesses and interrogating suspects is an ongoing process throughout the investigation as new witnesses and suspects are discovered. Throughout this stage suspects are eliminated and the most plausible suspect is identified. Next, the investigator begins preparing the case file to include the initial incident report, evidence, other reports such as lab reports, written statements, and other relevant information. Once the case

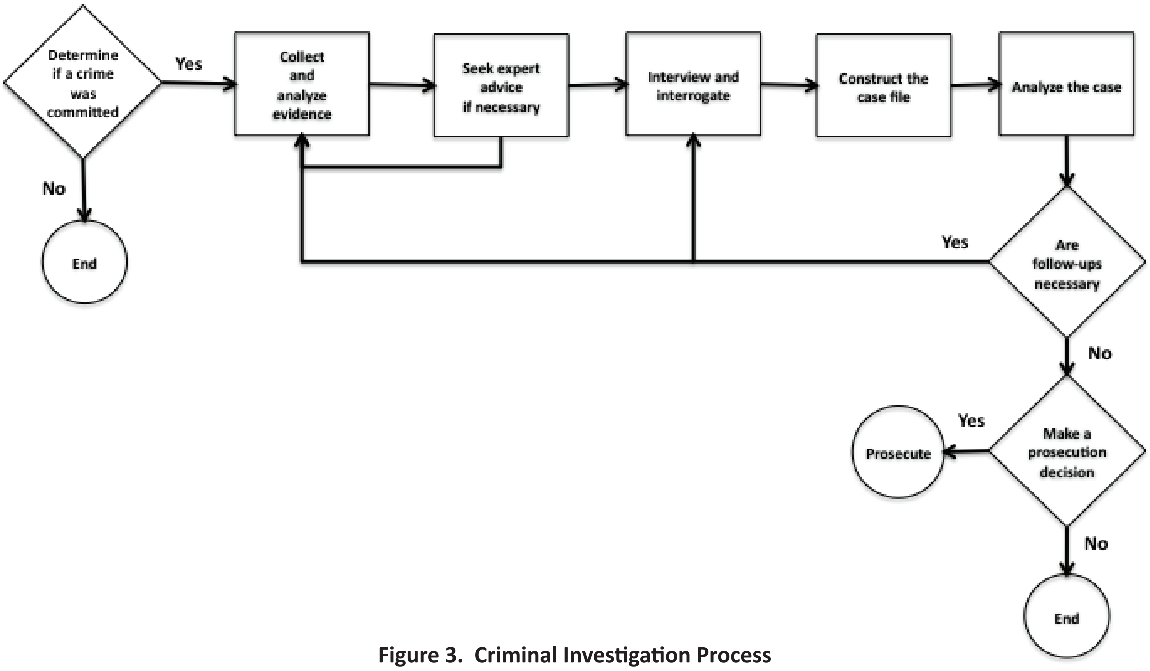

Determine if a crime was committed
Yes
No
End
Collect and analyze evidence
Seek expert advice if necessary
Interview and interrogate
Construct the case file
Analyze the case
Yes
Are follow-ups necessary
No
Yes
Prosecute
Make a prosecution decision
No
End

Figure 3. Criminal Investigation Process

file is constructed it is analyzed to determine weaknesses and to identify additional information needed for prosecution. This analysis leads to any follow-up investigations that need to occur including collecting additional evidence and interviewing witnesses again. Once the case is considered complete the prosecutor will decide whether to bring the case to trial and how to proceed. There is no standard accuracy measure or probability threshold for authorship attribution evidence; the investigator only needs probable cause to initiate a warrant or arrest. In addition, evidence admissibility varies by jurisdiction. In cases where digital evidence is not admissible, expert witnesses are often called upon to provide their expertise and interpretation. In the court of law, the jury only needs reasonable doubt to determine a defendant's guilt or innocence. Some relevant criminal cases were investigated and prosecuted based on text message abbreviations, sentence length, and punctuation (Leafe, 2009).

Criminal Profiling and IM

Criminal profiling is an investigative method that has been used in traditional criminal investigations that can also be applied to cybercrime investigations, known as cyberprofiling. Cross defines traditional criminal profiling is the "art and science of developing a description of a criminal's characteristics (physical, intellectual, and emotional) based on information collected at the scene of the crime" (Cross, 2008). Criminal profiling often uses patterns and correlations among criminal activity and different crimes to construct a profile. Criminal profiling is used to assist with the investigative process, reduce the potential suspect space to a certain subset of suspects, link related crimes, and develop an interview and interrogation strategy (Casey, 1999). It is important to note that a criminal profile will only provide generalities about the type of person who committed a crime, it will not identify a specific individual. Criminal profiling is one method among many for assisting with criminal investigations and building a case file. The profile cannot exist as evidence, rather it provides information to allow investigators to focus on the right suspects and begin to gather additional evidence (Cross, 2008). A criminal profile can be used in court in conjunction with expert witness testimony. "An expert witness can reference a criminal profile as the basis of an opinion that there is a high probability of a link between a particular suspect and a particular crime" (Cross, 2008). An IM author writeprint may be used as input to a criminal profile.

The FBI is credited with formalizing the criminal profiling process. The FBI's Behavioral Science Unit (BSU) "focuses on developing new and innovative investigative approaches and techniques to solve crimes by studying offenders and their behaviors and motivations" (FBI, 2014). The BSU has been assisting local, state, and federal agencies in narrowing investigations by providing criminal profiles since the 1970s (Doublas et al., 2014). The FBI BSU has created the six-step criminal profile generating process shown in Table 1.

Table 1. FBI BSU Criminal Profile Process

FBI BSU Criminal Profile Process	
1. Profiling Inputs	The first step collects profiling inputs including comprehensive information about the crime and all evidence collected, both tangible, physical evidence and digital evidence.
2. Decision Process Models	This step analyzes the information and evidence to determine patterns and possible linkages to other crimes.
3. Crime Assessment	The crime scene is reconstructed and analyzed to determine the sequence of events and other information about the crime.
4. Criminal Profile	The first three steps are combined to create a criminal profile, often incorporating the motives, physical qualities, and personality of the perpetrator. The criminal profile is also used to create an interrogation strategy for the suspects.
5. The Investigation	Investigators and others use the profile to learn more information and identify suspects. Suspects matching the profile are evaluated. The profile may be reassessed if no leads or suspects are identified.
6. The Apprehension	The last stage occurs when investigators believe they have identified the most plausible suspect likely to be the perpetrator. A warrant is obtained for the arrest of the individual, usually followed by a trial (Doublas et al., 2014).

The FBI criminal profile generating process may be easily applied in a cybercrime investigation to perform cyberprofiling. Various types of digital and non-digital evidence may be combined as profile inputs, including, email, IM conversations, network packet captures, account activity information, and physical evidence. A cybercriminal's profile may include a number of traits such as time and location of computer access, types of computer attacks launched by the attacker, programs and attack tools used, writeprints, and targets of the cybercrime whether they be human or electronic (networks, satellites, phones, computer systems, etc.).

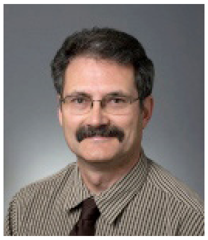
In the context of IM-assisted cybercrime, cyberprofiling uses IM data such as the conversation logs, IM client version, timestamps, the length of time the user has been logged on, etc. IM writeprints may be used in conjunction with other evidence and investigative techniques to build or validate a criminal profile; reduce the potential suspect space to a certain subset of suspects; link related crimes; develop an interview and interrogation strategy; and gather convincing digital evidence to justify search and seizure and provide probable cause.

Conclusion

As cybercrimes continue to increase, new cyber forensics techniques are needed to combat the constant challenge of Internet anonymity. The IM writeprint technique may be used to assist cybercrime decision support tools in collecting and analyzing digital evidence, discovering characteristics about the cyber criminal, and assisting in identifying cyber criminal suspects. Future areas of research include implementing the IM writeprint taxonomy on past and/or ongoing investigation data for further analysis and modification. Additionally, this research would benefit from a feasibility analysis of various sociolinguistic writeprint categories (such as gender and age). Lastly, the IM writeprint taxonomy may be modified and applied to other communication mediums such as text, Twitter, and Facebook.

About the Authors

Dr. Angela Orebaugh is Fellow and Chief Scientist at Booz Allen Hamilton. She received her Ph.D. from George Mason University with a concentration in Information Security. Her current research interests include behavioral biometrics and the Internet of Things.



Dr. Jason Kinser is an Associate Professor in the School of Physics, Astronomy, and Computational Sciences at George Mason University. His current research interests include classification of regions in lung scans to detect idiopathic pulmonary fibrosis.

Dr. Jeremy Allnutt is a Professor in the Electrical and Computer Engineering Department at George Mason University with a focus in communications and signal processing, computer networking, and telecommunications.

References

1. Cross, Michael. *Scene of the Cybercrime*. Syngress Publishing, (2008): 679-690
2. Moores, Trevor, and Gurpreet Dhillon. "Software piracy: a view from Hong Kong." *Communications of the ACM* 43.12 (2000): 88-93.
3. Abbasi, Ahmed, and Hsinchun Chen. "Applying authorship analysis to extremist-group web forum messages." *Intelligent Systems*, IEEE 20.5 (2005): 67-75.
4. Bassett, Richard, Linda Bass, and Paul O'Brien. "Computer forensics: An essential ingredient for cyber security." *Journal of Information Science and Technology* 3.1 (2006): 22-32.
5. Revett, Kenneth. *Behavioral biometrics: a remote access approach*. Wiley Publishing, (2008): 1-2.
6. De Vel, Olivier, Alison Anderson, Malcolm Corney, and George Mohay. "Mining e-mail content for author identification forensics." *ACM Sigmod Record* 30.4 (2001): 55-64.
7. Zheng, Rong, Jiexun Li, Hsinchun Chen, and Zan Huang. "A framework for authorship identification of online messages: Writing-style features and classification techniques." *Journal of the American Society for Information Science and Technology* 57.3 (2006): 378-393.
8. Kucukyilmaz, Tayfun, B. Cambazoglu, Cevdet Aykanat, and Fazli Can. "Chat mining: Predicting user and message attributes in computer-mediated communication." *Information Processing & Management* 44.4 (2008): 1448-1466.
9. Leafe, David. "Dear Garry. I've decided to end it all: The full stop that trapped a killer." *Daily Mail* (2009).
10. Casey, E. "Cyberpatterns: criminal behavior on the Internet." *Criminal profiling: An introduction to behavioral evidence analysis* (1999): 361-378.
11. Federal Bureau of Investigation, Behavioral Science Unit website. http://www.fbi.gov/hq/td/academy/bsu/bsu.htm. (accessed March 4, 2014)
12. Doublas, John E., Robert K. Ressler, Ann W. Burgess, and Carol R. Hartman. "Criminal profiling from crime scene analysis." *Behavioral Sciences & the Law* 4.4 (1986): 401-421.
13. Li, Jiexun, Rong Sheng, and Hsinchun Chen. "From Fingerprint to Writeprint." *Communications of the ACM* 49.4 (2006): 76-82
14. Orebaugh, Angela, Jason Kinser, and Jeremy Allnutt. "Visualizing Instant Messaging Author Writeprints for Forensic Analysis," In Proceedings of Conference on Digital Forensics, Security and Law, Richmond VA (2014): 191-213