iForensics: Forensic Analysis of Instant Messaging on Smart Phones

Mohammad Iftekhar Husain and Ramalingam Sridhar

University at Buffalo, State University of New York, Buffalo, NY 14260-2000
{imhusain,rsridhar}@buffalo.edu

Abstract. Smart phones with Internet capability are growing in popularity, due to many of their useful capabilities. Among other handy features of smart phones, Instant Messaging (IM) is very popular due to the level of convenience it provides in interpersonal communications. As the usage of IM on smart phone is increasing rapidly, it is important to take measures in advance from forensic standpoint forecasting the potential use of it in cyber crimes such as the cyber stalking and cyber bullying. Although, current IM applications for smart phones are in most cases a downsized version of the one used on traditional computers, diverse structure of file systems and storage device on different smart phones pose unique challenges to forensic examiners for recovering digital evidences of a conversation under investigation. In this work, we study and report the forensic analysis of three different IMs: AIM, Yahoo! Messenger and Google Talk, (both client based and web based version) on Apple iPhone. Our results show that the forensic analysis of IMs on smart phones has significant value and needs further attention.

Keywords: smart phone forensics, instant messaging, chat forensics, iPhone forensics.

1 Introduction

Instant Messaging (IM) is the process of exchanging text messages in (pseudo) real time between two or more people pre-registered and logged into an instant messaging service provider such as AIM [4], Yahoo! [3] and Google [5]. Sometimes, the term "text chat" or simply "chat" is used to indicate IM. IMs started as simple UNIX command line utility and had grown into a giant IT market with fancy user interfaces that include many more feature than simple text chat. In fact, most of the top IM service providers have subscribers at a level of multiple million. Previously, IM service providers required users to download IM application (clients) on their local machines and use those applications for instant messaging. Recently, a new paradigm, called Volatile Instant Messaging (VIM) had been introduced where the participants can enjoy instant messaging by just using a web browser without installing any application on the user's local system.

Smart phones with Internet capability are adopting IM very fast. A recent report from Telephia Mobile Internet Report [13] showed that approximately 7.9 million

S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 9–18, 2010.

mobile users connected to Yahoo! Messenger from their wireless device in December 2005, which was about 4 percent of all wireless subscribers. AOL Instant Messenger attained 3.6 percent with a number of wireless customers at more than 7.3 million.

Although, IM is a convenient way to communicate with online friends and family, it is also an increasingly popular way for cyber criminals to distribute malwares, stalk or bully a person online, and to commit fraud. IM is a convenient choice for such criminals because they can use network ports that are already open for the IM client instead of having to open suspicious new ports which might be blocked by firewalls. Cyber criminals utilize IM's convenient presence features and find potential victims simply by choosing from an updated directory of buddy (friend) lists. This way, the cyber criminals also get to know each time their victims' computers are online. In fact, recently a Melbourne woman was sentenced for a year for cyber stalking and cyber bullying a US singer [25].

To solve IM based cyber crimes, investigators need to perform forensic analysis of suspect device to find digital evidences. The advantage of client-based IMs is that much of conversation related information can be recovered from the suspect device. Recent reports [16], [17] show that forensic analysis of IM programs can provide various digital evidences such as conversation log, screen name and buddy list. However, web-based Volatile IMs (VIMs) require different forensic approach because when the user closes the web browser or shuts down the machine, most of the information related to the conversation is not retained in VIM.

The Apple iPhone [1] is among the most popular smart phones on the market, since its release in July, 2007. Smart phones have been able to perform similar functionalities that iPhone does for a while; but the addition of touch screen and virtual keyboard were behind its high popularity. The iPhone 3rd Generation Cellular Communication device, widely known as iPhone 3G was released in July, 2008 which featured GPS service and faster Internet connection. This device with high speed Internet supports both traditional client-based IM and web-based VIM. Although, traditional IMs store significant information on local system, due to the unique device structure and system obfuscation of iPhone, recovering evidences even from traditional client-based IMs are challenging. Locating digital evidences from web-based IMs on smart phones are more difficult due to the volatile nature of the communication. Existing methods of iPhone forensics [14], [15] mostly rely upon altering the firmware of iPhone to access the storage area using a method widely known as "Jailbreaking" [10]. However, this violates the ACPO (Association of Chief Police Officers) guideline for computer forensics and electronic evidence [21], which clearly states that "*No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may be subsequently be relied upon in court.*" This paper investigates the recovery of forensic evidences from IM conversations on an iPhone without altering the firmware and keeping the analysis legally sound. Artifacts and other forensically-significant piece of information that can be recovered from three popular IMs: AIM, Yahoo! and Google, are also examined in details.

2 Literature Review

2.1 IMs for iPhone

Traditional IMs rely on the existence of an installed client application. Yahoo! [3] and AIM [4] provide traditional IM applications for iPhone. These programs require the user to enter an online screen name and password from a previously registered account. Both of these providers have web-based VIM, AIM Express [11] and Yahoo! webmessenger [12] respectively. However, Google only have the web-based Google Talk gadget [5] optimized for iPhone.

2.2 iPhone Internals

The iPhone OS is an optimized version of OS X [33] based on BSD. Updates to the OS are provided through iTunes via an interface called the Apple File Communication Protocol (AFC). However, the AFC and iTunes are not allowed to access the entire iPhone storage area. Instead access and view are limited to certain files on the iPhone, mostly those located in the Media folder on the second partition of the device other than the system partition.

2.3 Prior Art on IM and iPhone Forensics

Hurbaneck [16] provides a useful discussion on messaging forensics both on traditional computers and mobile devices from broad perspective. The presenters focused mainly on enterprise policy and legal issues related to the messaging service. A nice introduction to MSN messenger and Windows Live Messenger forensics is provided in [18] with detailed screenshots. A forensic examination of Yahoo Messenger is reported in [19] for traditional computers. Kiley *et al* [20] presents an interesting and first of its kind work in the area of VIM. The authors have studied four popular VIMs and presented an investigative framework for volatile messaging forensics. The platform was traditional computers for this study as well.

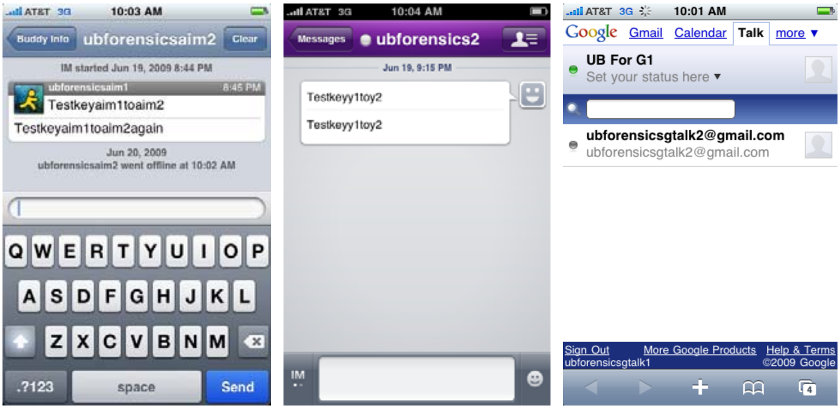
Also, several forensic companies have released tools to forensically examine an iPhone: “Aesco” [22] from Radio Tactics, “Device Seizure” [23] by Paraben Forensic Tools and “Wolf” [24] from Sixth Legion. Each of these applications retrieves SMS, Call Records, Contacts as well as other information. Aesco supports both iPhone and iPhone 3G forensics. It also mentions file system support for iPhone, but it is not clear whether this includes system files or requires “jailbreaking” of the device. Device Seizure supports both jailbroken and non-jailbroken firmware for forensic analysis. However, with a non-jailbroken firmware, it can only analyze the media files. Wolf is primarily an iPhone focused forensic tool. A unique feature of Wolf is that it can retrieve the information from the Internet history of built-in Safari browser of the iPhone. However, none of these commercially available tools address IM forensics in their product information and to the best of our knowledge none of prior art addresses IM forensics issues for iPhone without “jailbreaking” the device.

3 Methodology

This paper reports the result of forensic analyses of three IM programs on an Apple iPhone 3G provided by AIM (version 2.0.2.4), Yahoo! (version 1.1), and Google (version 2009). The iPhone firmware version was 2.2.1 and 16 GB storage. We have tested both the traditional IM application that requires the download and installation of provider softwares and web-based VIM application that does not require software installation. Default iPhone web browser Safari (customized for iPhone [26]) was used to test the VIM applications. We have chosen these IM services based on their popularity at the Apple App Store [27].

3.1 Creation of Test Data

For this study, test data was created by sending two consecutive messages for each IM program. The communication was limited between two participants. One participant was logged in on an iPhone and another participant was using a Windows based machine. The conversations were initiated from the participant on the iPhone. Unique phrases were used for each conversation for the ease of identification as shown in Table 1.



ubforensicsaim2

IM started Jun 19, 2009 8:44 PM

ubforensicsaim1 8:45 PM

Testkeyaim1toaim2

Testkeyaim1toaim2again

Jun 20, 2009
ubforensicsaim2 went offline at 10:02 AM

ubforensics2

Jun 19, 9:15 PM

Testkeyy1toy2

Testkeyy1toy2

UB For G1

Set your status here

ubforensicsgtalk2@gmail.com
ubforensicsgtalk2@gmail.com

ubforensicsgtalk1

Fig. 1. Three IMs on iPhone: AIM, Yahoo! and Google (left to right)

3.2 Data Acquisition from iPhone

Apple iPhone forensics is a relatively new field and the standard and procedures are yet to be finalized. Still, many researchers [7], [8], [9] are trying to understand and explore different parts of an iPhone. Considering the methods explored so far, there are two ways to acquire data from an iPhone: logical acquisition via iTunes backup and acquiring a physical image.

Table 1. Screen names and unique phrases used for IM conversations

Category	AIM	Yahoo!	Google
Unique Phrase	Testkeyaim1toaim2	Testkeyy1toy2	Testkeyg1tog2
Screen name on iPhone	ubforensicsaim1	ubforensic1	ubforensicsgtalk1
Screen name on Windows	ubforensicsaim2	ubforensics2	ubforensicsgtalk2

Logical acquisition is based on acquiring the iPhone backup data from a machine on which the synchronized iTunes exists. Alternatively, an investigator can force backup an iPhone to a forensic examination machine using iTunes and a method discussed in this paper shortly. While for forensic purpose, the obvious choice is to get a physical image of the device and then perform the analysis, Apple has not yet released any publicly available tool for forensic experts for this purpose. As mentioned earlier, there are methods such as "jailbreaking", to acquire physical image, but according to ACPO guideline for computer forensics and electronic evidence, this kind of acquisition might not be acceptable on legal platforms because it alters the original system configuration data. For that reason, in this paper, we will use the logical acquisition method to acquire the data necessary for IM forensics to increase the validity of this analysis on legal venues.

3.2.1 Logical Acquisition via iTunes Backup

On a Windows machine, the iTunes software saves logical copies of files on iPhone at:C:/Users/*UserName*/AppData/Roaming/AppleComputer/MobileSync/Backup. By right-clicking on the device icon when the iPhone is connected to a computer via iTunes, one can choose the backup option to backup a logical copy of iPhone data. However, sometimes it is difficult to recover some deleted files from this kind of backup. After the backup is acquired, "MobileSyncBrowser" [2] can be used to parse the data. The parsed data are mostly in the form of .db (database) and .plist (Apple Property List) [28] format. "SQLite Database Browser" [29] and "plist Editor for Windows" [30] were used to analyze these files respectively.

4 Results

Table 2 shows the usability experience of both the traditional client-based IM and web-based VIM from AIM, Yahoo! and Google on iPhone.

The web-based VIM client of AIM is available at [11]. However, this widget could not be accessed using the default Safari browser on iPhone as it does not support

Table 2. Usability of IMs and VIMs on iPhone

Program	Web-based VIM	Client-based IM
AIM	No, requires Flash	Yes, application available
Yahoo!	No, requires Flash	Yes, application available
Google	Yes, web gadget available	No, application not available

Flash at this point. For the same reason, Yahoo! webmessenger available at [12] cannot be used on iPhone. However, a Flash installer for iPhone is currently under consideration by Apple [31]. If it is available in future, web-based VIMs that require Flash might be used from iPhone. On the other hand, Google does not provide any client-based IM application for iPhone. It only provides web-based VIM talk gadget support which works fine with default Safari browser on iPhone.

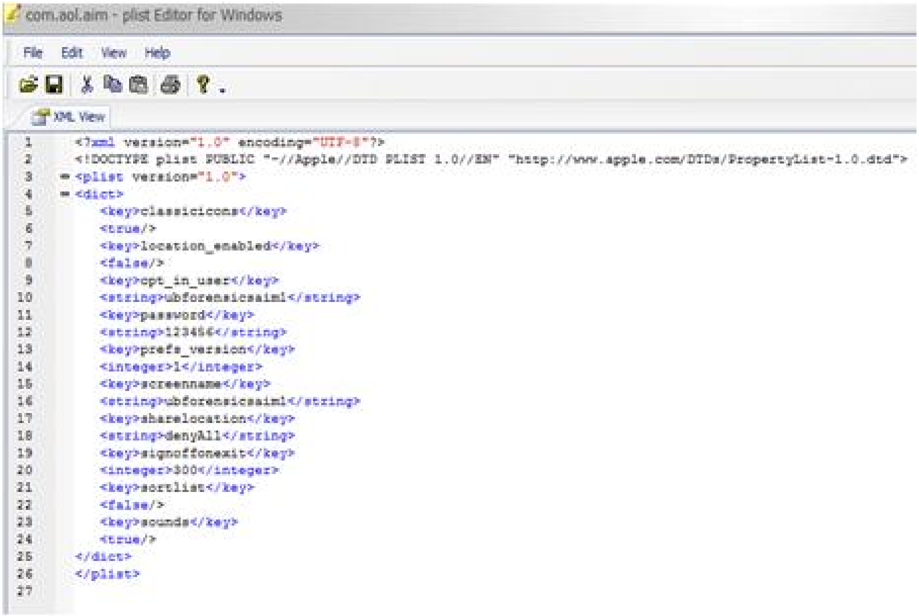
A summary of evidences with IM forensic value found on the iPhone after logical acquisition and analysis of data is shown in Table 3.

Table 3. Summary IM forensic evidence found on IPhone

Program	Unique Phrase	Timestamp	Screen Names	Plain Text Password	Buddy List
AIM	Yes	Yes	Yes	Yes	Yes
Yahoo!	Yes	Yes	Yes	No	Yes
Google	No	No	No	No	No

4.1 AIM

AIM screen name and password (in plain text!) was found in /lib/preferences/com.aol.aim.plist file which is shown in Figure 2. Account information was found in



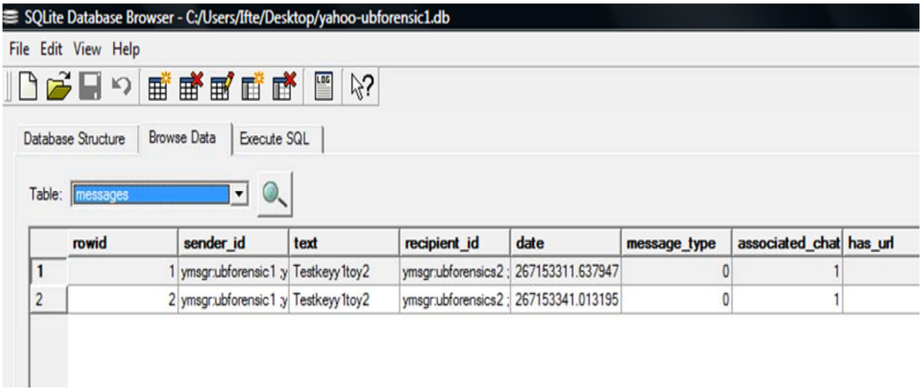
```
  <?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
= <plist version="1.0">
= <dict>
      <key>classicicons</key>
      <true/>
      <key>location_enabled</key>
      <false/>
      <key>opt_in_user</key>
      <string>ubforensicsaim1</string>
      <key>password</key>
      <string>123456</string>
      <key>prefs_version</key>
      <integer>1</integer>
      <key>screenname</key>
      <string>ubforensicsaim1</string>
      <key>sharelocation</key>
      <string>denyAll</string>
      <key>signoffonexit</key>
      <integer>300</integer>
      <key>sortlist</key>
      <false/>
      <key>sounds</key>
      <true/>
  </dict>
  </plist>
```

Fig. 2. AIM screen name and Password in plain text

/documents/Accounts.accounts file. Conversation detail with timestamp and unique phrase was found in /documents/ *accountname*.conversations.plist file. The file /documents/*accountname*.sessions. plist contains information on buddy list.

4.2 Yahoo! Messenger

Encrypted password and Yahoo! ID were found in /lib/preferences/ com.yahoo.messenger.plist file. This file also contains the time when a particular user last accessed the IM service from the iPhone. Conversations with timestamps are found in /documents/yahoo-*accountname*.db file as shown in Figure 3. /documents/ yAddressBook_*accountname*.xml contains the buddy list. Evidences from the conversation are also found at the session.log.db file.



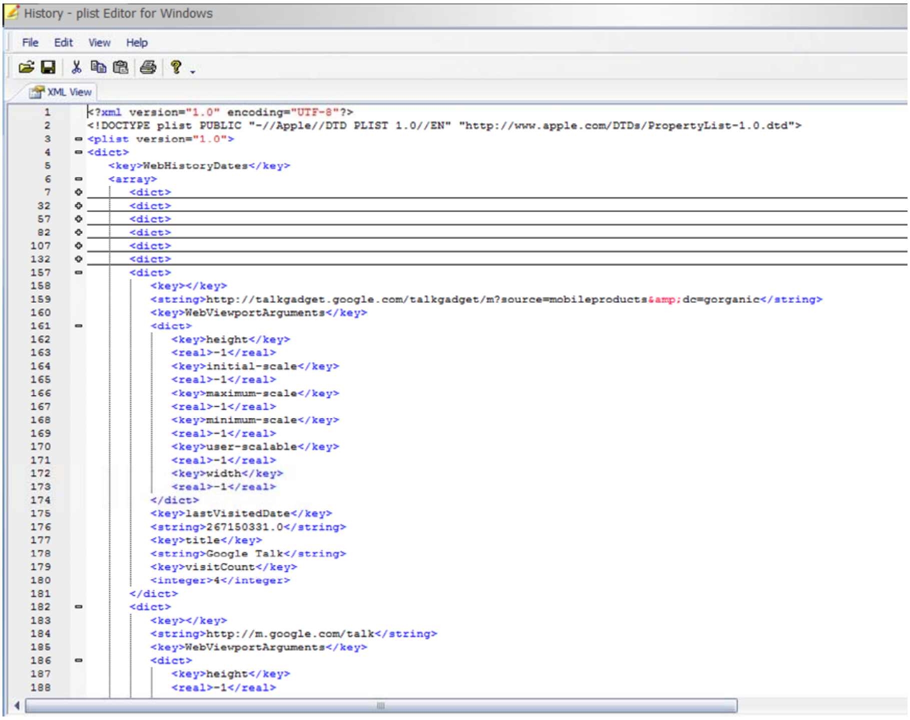
	rowid	sender_id	text	recipient_id	date	message_type	associated_chat	has_url
1	1	ymsgr:ubforensic1 ;y	Testkeyy1toy2	ymsgr:ubforensics2 ;	267153311.637947	0	1	
2	2	ymsgr:ubforensic1 ;y	Testkeyy1toy2	ymsgr:ubforensics2 ;	267153341.013195	0	1	

Fig. 3. Recovered Yahoo! Messenger conversation

4.3 Google Talk

Google Talk gadget is a web-based VIM and it was difficult to find direct evidences from the conversation. However, there are several indirect methods that lead to the proof of a conversation. For example, Google stores a copy of the chat on the Gmail (E-mail service from Google) account of conversation participants, unless they have chose “Off the record” mode [32]. Also, by searching the /lib/Mail/Accounts.plist file, it is possible to identify whether the owner of the iPhone is the account holder of a particular Google account.

This is also true for AOL and Yahoo! if the phone owner was using inbuilt mail application of the iPhone. However, the temporary Internet files and caches of Safari browser didn’t contain much information accept the fact that Google Talk web gadget was accessed from that particular iPhone at a certain time. These files can be found at /lib/Safari/History.plist file (figure 4).



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>WebHistoryDates</key>
    <array>
        <dict>
        <dict>
        <dict>
        <dict>
        <dict>
        <dict>
        <dict>
            <key></key>
            <string>http://talkgadget.google.com/talkgadget/m?source=mobileproducts&amp;dc=gorganic</string>
            <key>WebViewportArguments</key>
            <dict>
                <key>height</key>
                <real>-1</real>
                <key>initial-scale</key>
                <real>-1</real>
                <key>maximum-scale</key>
                <real>-1</real>
                <key>minimum-scale</key>
                <real>-1</real>
                <key>user-scalable</key>
                <real>-1</real>
                <key>width</key>
                <real>-1</real>
            </dict>
            <key>lastVisitedDate</key>
            <string>267150331.0</string>
            <key>title</key>
            <string>Google Talk</string>
            <key>visitCount</key>
            <integer>4</integer>
        </dict>
        <dict>
            <key></key>
            <string>http://m.google.com/talk</string>
            <key>WebViewportArguments</key>
            <dict>
                <key>height</key>
                <real>-1</real>
```

Fig. 4. History file of Safari web browser

5 Conclusion

Forensic examination of Instant Messaging on smart phones such as iPhone pose a new challenge for the investigators as well as researchers due to the uniqueness of file system, lack of standard methods and tools for system exploration. In this study, we have investigated forensic evidences from three popular IMs used on an iPhone without altering the firmware and keeping the evidences acceptable at legal platforms according to ACPO guidelines. Our results have shown that various useful artifacts related to IMs can be recovered from the iPhone, including username, password, buddy list, last log-in time, and conversation timestamp as well as conversation details. In some cases, multiple instances of information were found which might strengthen the investigation as well as lead to further evidences. Our methodology and results showed significant promise and will contribute to further research in this field.

References

1. Apple-iPhone-Mobile phone, iPod and Internet device, `http://www.apple.com/iphone/`
2. Vaughn, S.C.: MobileSyncBrowser, `http://homepage.mac.com/vaughn/msync/`

3. Yahoo! Messenger for the iPhone, http://messenger.yahoo.com/platform/iphone/
4. AIM on iPhone - Discover AOL, http://daol.aol.com/software/mac/iphone/aim
5. Google Mobile | Talk for your iPhone, http://www.google.com/mobile/apple/talk.html
6. Mac OS X Forensics, http://www.macosxforensics.com/index.html
7. Richardson, W.: How To Mount Your iPhone Filesystem On Your Desktop In Ubuntu (2007), http://www.fsckin.com/2007/09/23/how-to-mount-your-iphonefilesystem-on-your-desktop-in-ubuntu/
8. Singh, A.: MacFuse, http://code.google.com/p/macfuse/
9. Colyer, M.: iFuse and libiphone (2009), http://matt.colyer.name/projects/iphone-linux/index.php?title=Main_Page
10. How to Jailbreak Your iPhone in Under a Minute, http://www.appleiphonereview.com/iphone-tutorials/iphone-jailbreak/
11. Web IM-AIM Express, http://www.aim.com/aimexpress.adp
12. Yahoo Messenger for the Web, http://webmessenger.yahoo.com
13. Telephia Mobile Internet Report, http://www.telephia.com/documents/InternetandDeviceReleaseJune2006v68.14.06FINAL.pdf
14. Zdziarski, J.: iPhone Forensics. O'reilly Media, California (2008)
15. Punja, S.G., Mislan, R.P.: Mobile Device Analysis. Small Scale Digital Device Forensics Journal 2(1), 1–16 (2008)
16. Hurbanek, T.B.: Messaging: A forensic view, http://www.cscic.state.ny.us/security/conferences/security/2006/presentations/hurbanek.cfm
17. Reust, J.: AOL Instant Messenger Trace Evidence. Digital Investigation 3(4), 238–243 (2006)
18. Parsonage, H.: The Forensic Recovery of Instant Messages from MSN Messenger and Windows Live Messenger (2008), http://computerforensics.parsonage.co.uk/downloads/MSNandLiveMessengerArtefactsOfConversations.pdf
19. Dickson, M.: An examination into Yahoo Messenger 7.0. Digital Investigation 3(3), 159–165 (2006)
20. Kiley, M., Dankner, S., Rogers, M.: Forensic Analysis of Volatile Instant Messaging. Advances in Digital Forensics 4, 129–138 (2008)
21. Computer Investigation, Electronic Evidence - ACPO Guideline (2009), http://www.dataclinic.co.uk/computer-ACPO.htm
22. Aesco, Radio Tactics Limited, http://www.radio-tactics.com/?pageid=phonedatabasehandle&man=Apple
23. Device Seizure, Paraben Forensic Tools, http://www.paraben-forensics.com/cell_models.html
24. Wolf, Sixth Legion, http://www.sixthlegion.com/
25. Cyber stalking and online libel, http://www.abc.net.au/rn/lawreport/stories/2009/2584563.htm

26. Berka, J.: iPhone Safari isn't Safari 3.0, http://arstechnica.com/apple/news/2007/07/iphone-safari-isnt-safari-3-0-and-other-development-surprises.ars
27. Apple App Store, http://www.apple.com/iphone/apps-for-iphone/
28. PLIST, http://developer.apple.com/documentation/Darwin/Reference/ManPages/man5/plist.5.html
29. SQLite Database Browser, http://sqlitebrowser.sourceforge.net/
30. plist Editor for Windows, http://www.iPodRobot.com/download.htm
31. Flash installer for iPhone, http://www.geek.com/articles/apple/developer-creates-flash-for-iphone-but-will-it-make-it-to-the-app-store-20090428/
32. Google Talk, Off the record, http://www.google.com/talk/chathistory.html#offrecord
33. Mac OS X, http://www.apple.com/macosx/