# Text Message Preservation

**by Sharon D. Nelson, Esq., John W. Simek and Jesse M. Lindmar**


With an average of 193.1 billion text messages sent every month in the United States, the importance and use of text messages in litigation is ever-increasing. As a consequence, the importance of text message preservation for e-discovery is also growing. Understanding how text messages can be preserved and the pitfalls to avoid is essential. While we recommend engaging the services of a digital forensics service provider who is familiar with the complexities of mobile phone forensics, there are certain situations in which the end-user can at least create a preserved, forensically sound copy that a digital forensics expert can later access and produce data from.

For the purpose of this article, we are assuming that the text messages are sent or received by a mobile telephone. We'll start by lumping most of the mobile phones in use today into two major categories: Smartphones and Feature Phones. The most popular Smartphones would include Apple's *iPhone*, Google's *Android*, Microsoft's *Windows Phone*, and RIM's *BlackBerry* devices. Feature phones are pretty much everything else; having some of the basic "features" of smartphones, but lacking in overall integration with the phone's operating system and hardware, and with limited user-customization options.

**Feature Phones**

For feature phones, the end-user is limited as to their preservation options. Depending on the service provider, the feature phone may or may not be equipped with a *Subscriber Identity Module* (SIM) card. The SIM card contains information that will validate the phone on the service provider's network, but can also be used as a repository for received text messages. Text messages can also be stored on the phone itself, and in some situations, messages are stored on the phone and SIM card. There are a number of SIM card readers and software products that, when used together, allow a user to explore and manage the contents of a SIM card. However, if the user doesn't fully understand how to use the hardware/software safely, he or she could just as easily alter or permanently erase the very data they are trying to preserve.

There are several products used within the forensic community to preserve text messages from many feature phones – from both a SIM card and the phone itself. This will result in an electronic copy of the text messages being extracted from the SIM card and/or phone, and will include not only the content of the message, but also the date and time the text message was sent/received and information about the sender (phone number and/or contact information for a phone number if the user has added them to the phones address book). Furthermore, SIM cards and many feature phones have a limited number of "slots" to store text messages, and the number of slots will vary across manufacturers and can even vary across similar phone models from the same manufacturer. When these slots are full, the phone will begin to overwrite the older text messages with the newer ones – a process that renders the older messages unrecoverable. With an average user sending or receiving sixty text messages per day, the likelihood of this happening increases dramatically.

For a digital forensic expert, the ability to recover deleted text messages from a feature phone is dependent on the make/model of the phone, the length of time that has passed since the messages were deleted, the number of new text messages that have been sent/received since the messages were

deleted, and whether the deleted messages have been overwritten. Furthermore, the make/model of phone will need to be supported by the forensic hardware/software the expert uses – if the hardware/software cannot communicate with the phone, the data cannot be accessed and preserved. Recovery from a SIM card is a little more straightforward as its architecture is standard; however, the same usage rules apply to it.

This is why we never make promises about what we can recover. It is more or less a crap shoot every doggone time.

**Smartphones**

For smartphones, and depending on the make and model of phone, there are several options for preserving text messages. Although a smartphone may be equipped with a SIM card, text messages are not typically stored there. Instead they are stored in a database file or another organized collection format, located on the phone itself – it is this file(s) that will specifically need to be preserved.

The *iPhone*, in conjunction with *iTunes* (*Apple's* software program for playing, downloading, saving, and organizing multimedia files on a computer or *Apple iOS* device), will allow an end-user to create a backup of the existing user-data from the phone – including the database file that stores the text messages. When the user connects the phone to *iTunes*, this backup will typically happen automatically, but a user can also initiate the backup at any time. *iTunes* will only store one backup at a time, so creating a new backup will cause the deletion of a previously created backup. The backup file will be buried in a system area of the computer used to create the backup, but with a little assistance it can be located. A user won't be able to access the data in the backup without special software, but a qualified digital forensics expert will be able to open the backup, access the text message database, and extract the necessary text messages. To a degree, deleted text messages may also be recoverable from the existing text message database. However, if a significant amount of time has passed, and depending on the user's text messaging habits, deleted text messages will not be recoverable via this method. A digital forensics expert will need to create a more thorough backup of the phone that will allow them to potentially recover deleted text messages using more advanced techniques.

Similar to the *iPhone*, *BlackBerrys* also allow for a backup to be created that will contain existing text messages. This backup can be created using the *BlackBerry Desktop Manager* software that comes with the phone or is available for download from the *BlackBerry* website. Unlike the iPhone, multiple backup files will exist on the computer used with the Desktop Manager. Like the *iPhone* backup, a user won't be able to access the data in the backup without special software, but a qualified digital forensics expert will be able to open the backup and extract the necessary text messages. Deleted text messages can only be recovered using a combination of specialized hardware and software used by digital forensic service providers specializing in mobile phone forensics. In some situations, only the removal and analysis of the phone's memory chip, a process that will destroy the phone, will allow for the recovery of deleted text messages. For obvious reasons, this route is ordinarily something undertaken primarily by law enforcement.

*Google Android* and *Windows Phone* smartphones do not have a native method for preserving text messages. A digital forensics expert will use tools and techniques specific to the type of phone they encounter. However, for the end-user, there are several third-party applications that advertise the ability to backup existing text messages from these devices. Any application the end-user chooses

should offer the ability to export the messages and their attributes into an uneditable format, so there is no question as to their authenticity.

Not all makes/models of phones are supported by forensic products and electronic versions of the existing text messages are not always obtainable. In these situations, even the best forensic examiner will be forced to painstakingly take digital photographs of the existing text messages as they natively appear on the mobile phone. And yes, these are admissible in court. As far as deleted text messages are concerned, if they still exist on the phone, even in a fragmented form, a digital forensic expert should be able to recover them as long as the analysis computer can communicate with the phone.

Regardless of the method used, it should not alter any of the original text messages, the process and results must be reproducible and the preserved information must be identical to the original source information. Although an end-user may be able to assist with some of the initial stages of text message preservation, a digital forensics expert will be able to extract and produce verified and accurate text message data from the preservation data set. In most situations, engaging a digital forensics expert to complete the entire project life-cycle – from preservation to production – will allow for a more accurate and defensible use of text message data.

The temptation to DIY this sort of project should be resisted. If you're going to throw the dice and gamble monies on the recovery of text messages, hiring an expert will give you the best odds of rolling a seven.

*The authors are the President, Vice President and Director of Computer Forensics at Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax)* sensei@senseient.com *(e-mail)*, http://www.senseient.com.