Recovery: Deleted Short Messages from SIM Memory

Bharat Bhanjana

Syscom Corporation Ltd

Abstract- In this paper, SIM Storage Memory that is used to store Short Message Service (SMS) is discussed. In addition, different behaviours implemented by mobile manufacturers to delete a message from SIM Memory are also studied. Two solutions for recovering the deleted message (from SIM Memory) are proposed based on the FREE MEMORY available in SIM Card.

Index Terms- Electrically Erasable Programmable Read-Only Memory (EEPROM), Subscriber Identity Module (SIM), Short Message Service (SMS).

I. Introduction

Short Message Service is the service of delivering messages over the mobile networks. It is a service through which messages (text only) can be transferred between mobiles. There are storage locations for the messages on mobile as well as on SIM Cards. On SIM card, there is an elementary file used for storing messages named as SMS File.

II. Types of Memory Used for Storing Messages

There are two types of memory that are being used for storing messages:

1. Phone Memory
2. SIM Memory

In this paper, I will be focusing on later one i.e. SIM MEMORY. In SIM Cards, there is a special elementary file named EF SMS File (7F10/6F3C) which is used to store SMS. Here is the structure of file:

Table I: SMS File Structure

File ID: 6F3C	**Structure**: Linear Fixed	**Record Length**: 176 Bytes
Access Condition: **Read**: PIN1 **Update**: PIN1 **Invalidate**: ADM **Rehabilitate**: ADM		
Bytes	**Description**	**Length**
1	Status Byte	1 byte
2-176	Remainder	175 bytes

The first byte of SMS file is Status Byte. This byte tells about the status of the SIM messages i.e. whether the message is deleted/unread/saved or read.

Following is the structure of the status byte:

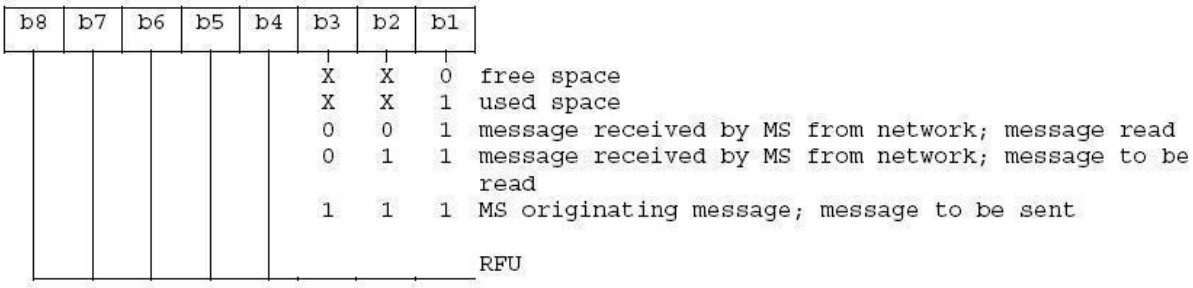

Figure 1: Structure of Status Byte

III. Deletion of Messages

To understand the concept of recovering messages from SIM Memory, first there is a need to understand how messages are deleted. There are different behaviours implemented by Mobile Phones. Below are some of the different behaviours that mobile phones implement:

1. Some mobile phones delete the message by changing the status byte (first byte) to 00. This means that the data of message is still present only the record is being set as free space. And when there is any new incoming message this first byte will indicate this space as free space that can be used to store that new message.

For e.g.: Let us say there are 4 messages present in SIM Memory

Table II: Four Messages in SIM Memory

Record Number	Status Byte	Remainder
01	01 (Used Space)	Data Part of SMS
02	01 (Used Space)	Data Part of SMS
03	01 (Used Space)	Data Part of SMS
04	01 (Used Space)	Data Part of SMS

The user deleted the second message. With this deletion the data of file will now looks like:

Table III: Deleted 2nd Record (Status Byte)

Record Number	Status Byte	Remainder
01	01 (Used Space)	Data Part of SMS
02	00 (Free Space)	Data Part of SMS (Not Erased)
03	01 (Used Space)	Data Part of SMS
04	01 (Used Space)	Data Part of SMS

2. Some mobile phones delete the message by updating the whole record with 00FF…FF. This means they clear both status byte as well as the data.

For e.g.: If the same message is deleted using this behaviour then the data of SMS File will look like:

Table IV: Deleted 2nd Record (Whole Record)

Record Number	Status Byte	Remainder
01	01 (Used Space)	Data Part of SMS
02	00 (Free Space)	FFFFFFFFFF ….FFF (Erased)
03	01 (Used Space)	Data Part of SMS
04	01 (Used Space)	Data Part of SMS

The table below shows behaviour of some of the mobile brands when a message gets deleted from SIM Memory:

Table V: Behaviour of Mobile Phones on deleting a message from SIM Memory

Brands	Deletion of a message by updating Status Byte	Deletion of a message by updating full record
Nokia	□	×
Samsung	×	□
LG	×	□
HTC	×	□

IV. Proposed Solution

Below are the two solutions that can be used to recover the deleted message from SIM Memory. The choice of the solution depends upon the memory available. Here the word "memory available" means that the memory that is being available in the SIM Card after fulfilling the customer's requirement i.e. Free EEPROM.

1st Solution: In case the memory is available after fulfilling the customer's requirements.

In case there is memory available in SIM Card, then a file (let's say X) having same structure as SMS File (6F3C) can be created on SIM Card. In case a new message is added in SMS File (6F3C) then an application on SIM Card will copy that new message into the file(X) so that in future if user deletes the message then there is a copy of that message available. Using the same application the message can be copied back into the SMS File. In this way the message deleted is recovered.

The number of messages to be stored for recovery depends upon the number of records of file (X) created. Thus if we say that the user wants to store last 10 incoming messages for recovering, then the number of records of the file(X) created should be 10. And in case the file(X) gets full then at this time on receiving new message the oldest message saved in file(X) will get replaced by the new one. So using this solution the recovering of message is possible regardless of the deletion behaviour.

2nd Solution: In case there is less memory available after fulfilling the customer's requirements.

In case there is not enough memory in SIM Card to create a file, then in this case an application can be integrated on SIM Memory. This application will be responsible for updating the status byte of messages to read/un-read from deleted. Thus, if the mobile phone updates only the status byte of message to 00 (deleted) then there is an option available to recover the same until a new message comes and over-rides this memory.

Please note that this solution only works for the mobile phones having behaviour of updating the status byte for deletion and that too only till the time when no new incoming message over-rides that deleted message.

V. Conclusion

The above proposed 1st Solution (where there is some memory available in SIM Card) can be implemented effectively since having a file on SIM Card will not going to be cost customers when the benefit looks like recovering of deleted message. The reasons for proposing the first solution are:

1. The current solution will be completely independent of the mobile behaviour of updating the SMS File on deletion. Thus the implementation can be adopted irrespective of the mobile behaviour i.e. whether it updates first byte or whole record.
2. In today's scenario there are very less number of mobile brands that updates only status byte for deleting a message from SIM Memory.

Acknowledgment

I would like to acknowledge my co-workers for supporting and encouraging me through out the course work.

References

[1] 3GPP TS 11.11 version 8.14.0 Release 1999

Authors

First Author – Bharat Bhanjana, **Qualification /Experience:** Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards., **Email Address:** b.bhanjana@gmail.com