

RECOVERING DELETED DATA FROM FAT PARTITIONS WITHIN MOBILE PHONE HANDSETS USING TRADITIONAL IMAGING TECHNIQUES

KEVIN MANSELL
CONTROL-F LTD.
KEVIN.MANSELL@CONTROLF.CO.UK

DARREN LOLE & FIONA LITCHFIELD
SERVICE POLICE CRIME BUREAU
ROYAL MILITARY POLICE

Although techniques for retrieving deleted SMS from SIM cards are well established, the ability to retrieve deleted data from flash memory within mobile phone handsets is a recent development. Commercial phone forensic tools are now available which can “dump” the contents of mobile phone memory and allow users to retrieve deleted data. This paper looks at how deleted and unallocated data can be quickly and easily retrieved from the internal memory of certain mobile phone handsets using easily accessible data cables and computer forensic imaging tools. Such techniques can be used to recover critical evidence from handsets which may previously have been inaccessible.

INTRODUCTION

Since evolving into a discipline in its own right within the last 3 – 4 years, mobile phone forensics has clearly demonstrated its value in criminal investigations. However, although SIM cards and memory cards can be removed from handsets and examined in a controlled way, the acquisition of data from the flash memory contained within the handset itself has been a far less forensically sound process than most practitioners would like. Specifically, phone forensic tools have relied on “logical acquisition” techniques whereby the handset is switched on and data is retrieved by means of communication with the device’s operating system (e.g. using protocols such as OBEX and SyncML). The single biggest drawback of such an approach is that deleted data cannot be retrieved from the handset.

For some time, phone examiners have been hoping for advancements in their toolset which would allow them to move closer towards the more forensically sound processes used when imaging and recovering evidence from computers; for example:

- Being able to create an image of the contents of the handset memory (thereby capturing live and deleted data)
- Preventing changes to the handset data during the acquisition process

Over approximately the last two years, some phone examiners have been using “flasher” boxes like the SHU Box [1] and SaraSoft software in order to “dump” the memory of the mobile phone¹. This, in combination with analysis software tools such as Pandora’s Box [2], has allowed phone examiners to recover deleted data from some mobile phone handsets. Although a positive step forward, devices such as the SHU Box are far from ideal tools for the forensic examiner in that they were not designed to be used for evidence recovery and have the ability to write data back to the device (e.g. completely remove all user data from the phone).

¹ Such techniques are often referred to as “hex dumps” or “physical acquisitions”



Fig 1 - SHU box

Phone forensic tool vendors have recently started to offer tools which are capable of retrieving deleted handset data but which do not allow data to be changed on the device. For example, Micro Systemation's XACT product [3] acquires and decodes handset memory contents for a range of different handsets.

Like their computer forensic counterparts, mobile phone examiners understand the value (and necessity) of having more than one tool in their "toolbox". This paper introduces a technique which can complement existing logical and physical acquisition tools. The technique described has been used to image the flash memory contained within certain Nokia, Sony Ericsson and Motorola handsets and recover live, deleted and unallocated data using existing computer and phone forensic tools.

Although some phone examiners may already be using such techniques, they are not in common use today. The authors believe that their adoption would increase the quality of phone examinations and would also enhance the forensic community's understanding of how such devices operate.

TECHNIQUE OVERVIEW

The techniques described here have been found to work with certain Nokia, Sony Ericsson and Motorola handsets, but by no means all handset makes and models. The handsets for which this technique works are all phones whose memory can be mounted as a USB storage device within Windows (the handsets in question appear to

use a FAT file system [4] within part of the device memory)

The technique is extremely simple:

1. Remove any media card from the handset (to prevent possible confusion between the media card and the handset's internal memory)
2. Use an appropriate write blocker (hardware or software) to prevent data being written to the phone once connected
3. With the handset OFF, connect a USB data cable from the handset to a Windows PC (note that this assumes that any drivers for the cable or handset have already been installed)
4. At this point the handset may detect the presence of the USB cable and automatically enter a "file transfer" mode
5. Windows should detect the handset memory and mount it as a drive under Windows (see Fig 2). If this does not happen then it is possible that the handset will not be accessible using this technique. A Windows "auto-play" prompt may appear which can be dismissed.

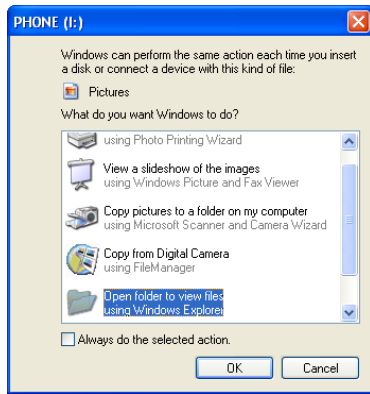


Fig 2 - Windows detects the phone as a storage device

6. Use an appropriate disk imaging tool to image the mounted drive and generate a hash of the acquisition process

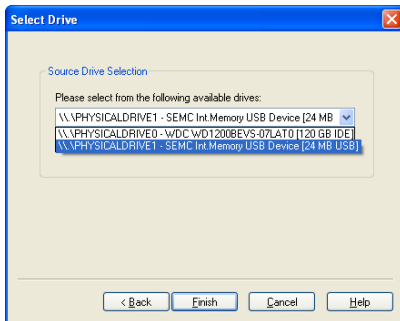


Fig 3 - FTK Imager "sees" the handset memory as a physical drive

7. Analyse the contents of the drive image using existing computer forensics tools

EXAMPLE 1: NOKIA 6500 CLASSIC

The technique described above was tested with a Nokia 6500 Classic. The 6500 Classic is a Series 40 Nokia handset with 1GB internal memory, but no removable media card. The handset contained a number of live images, one of which was deleted for the purposes of this test.

The handset was turned off and then connected to a PC running Windows Vista using the micro USB data cable supplied with the handset. When connected to the PC, the handset screen illuminated but remained blank (the handset did not “start up”). Windows detected the handset as a USB storage device and displayed an “Autoplay” window which was dismissed.

A ‘dd’ image of the handset’s FAT16 partition was created using AccessData’s FTK Imager [5] and the resulting hash noted. The handset was then disconnected from the PC.

The ‘dd’ image was then mounted as a drive letter under Windows using Mount Image Pro [6]. Recover My Files [6] was used to recover deleted and unallocated data from the mounted drive image.

Recover My Files successfully recovered the deleted picture and classified it as a “Lost File” indicating that it was recovered from unallocated space. Further analysis of the contents of the device image revealed that a directory entry for the file was present, however neither Recover My Files or FTK Imager seemed to recognise the directory entry (the file was not visible within FTK Imager’s file/folder browser window).

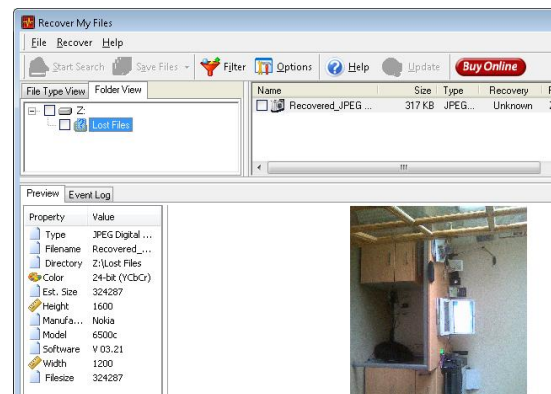


Fig 4 - Recover My Files retrieval of deleted picture from Nokia 6500 Classic

still a step forward from only being able to see live data.

EXAMPLE 2: SONY ERICSSON W300I

The technique described above was tested with a Sony Ericsson W300i. The results were less favourable than with the Nokia 6500 Classic, but they are included here as they raise interesting questions about the operation of the device.

The internal handset memory contained a number of photos, one of which was deleted for test purposes. The handset was turned off and the media card removed from the device. The handset was connected to a Windows XP PC using the corresponding Micro Systemation .XRY [7] data cable (.XRY was already installed on the PC so all necessary drivers were available). The driver installation under Windows completed successfully and the handset display showed the handset entering “File Transfer” mode.

Windows mounted the handset memory as a drive letter under Windows. SAFEBlockXP [8], a software write blocker was used to disable writing to the phone memory. This was tested by trying to create a new text file on the device. Windows generated an error saying that the device was write protected which indicated that the write protection was functioning correctly.

A ‘dd’ image of the handset’s FAT16 partition was created using MicroSystemation’s XACT product. The image was then decoded (read) using XACT and the file system analysed. Analysis of the handset image revealed filenames for a mixture of live and deleted files. However, when the deleted files were inspected, the files were found to be completely empty (all zeros). The same results were seen when analyzing the device image in FTK Imager. As such, although it could be seen that a file of a certain name had been deleted, the contents of the file were not available. This is obviously disappointing, but

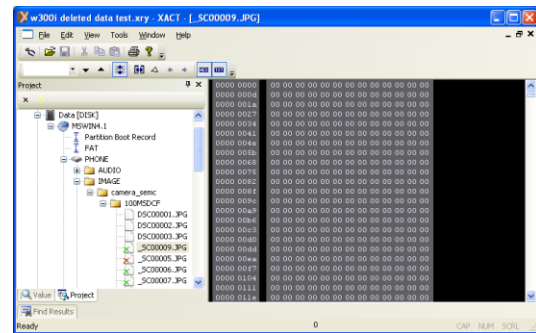


Fig 5 - Deleted files from W300i are listed but contain no data

The same “zeroed file” effect has also been seen with a Sony Ericsson K310i. One possible explanation for this effect is that the device is actually erasing the file data when the file is deleted by the user instead of simply modifying the directory entry as happens with a FAT partition in Microsoft Windows [9].

CONCLUSIONS

The tests described within this paper have demonstrated that deleted and unallocated data can be retrieved from mobile phone handset memory simply by connecting the handset to a PC via a data cable and imaging the resulting mounted drive.

The technique can only be used on specific handsets, and further research is required to establish what types of data can be retrieved from which handsets. It is worth stating that this approach has already been used in criminal investigations to recover evidence that would have otherwise been unrecoverable. As such, the authors hope that this paper encourages others to test it, evaluate its benefit within mobile phone forensic investigations and to share their findings within the forensic community.

REFERENCES

- [1] SHU Box
[http://www.fonefunshop.co.uk/Unlocking/h
su.htm](http://www.fonefunshop.co.uk/Unlocking/h
su.htm)
- [2] Pandora's Box
[http://www.hex-
dump.com/PB/pandora/pandora.html](http://www.hex-
dump.com/PB/pandora/pandora.html)
- [3] Micro Systemation XACT
[http://www.msab.com/en/mobile-forensic-
products/XACT-mobile-forensic-application/](http://www.msab.com/en/mobile-forensic-
products/XACT-mobile-forensic-application/)
- [4] Microsoft FAT32 Specification
[http://www.microsoft.com/whdc/system/pla
tform/firmware/fatgen.mspx](http://www.microsoft.com/whdc/system/pla
tform/firmware/fatgen.mspx)
- [5] Access Data FTK Imager,
<http://www.accessdata.com/>
- [6] GetData Mount Image Pro and Recover My
Files
<http://www.getdata.com>
- [7] Micro Systemation .XRY
[http://www.msab.com/en/mobile-forensic-
products/XRY-Mobile-Version-Forensic-
Software/](http://www.msab.com/en/mobile-forensic-
products/XRY-Mobile-Version-Forensic-
Software/)
- [8] ForensicSoft SAFEBlockXP
<http://www.forensicsoft.com/>
- [9] File System Forensic Analysis, B. Carrier
(Addison Wesley, 2005)