3-12-2007

The effectiveness of investigative tools for Secure Digital (SD) Memory Card forensics

Haitham Al-Hajri
Edith Cowan University

Patricia Williams
Edith Cowan University, trish.williams@ecu.edu.au

DOI: 10.4225/75/57ad3c637ff27
5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.

The effectiveness of investigative tools for Secure Digital (SD) Memory Card forensics

Haitham Al-Hajri
Edith Cowan University
halhajri@student.ecu.edu.au

Patricia A H Williams
Edith Cowan University
trish.williams@ecu.edu.au

Abstract

There are many freeware based tools that can be downloaded from the World Wide Web. This paper reports the retrieval results of using these tools on digital images which have been deleted from Secure Digital (SD) cards. Since SD cards and USB flash drives are considered solid state technology, the tools selected are specifically for solid state drives. This research helps classify the selection of the most effective freeware tools that could be used to recover lost or deleted images. Further, it includes some of the issues that would face forensic examiners undertaking such investigations. The tools were tested using the Windows environment and did not require any specific forensics background in order to retrieve the images. The testing procedures included retrieval time and the state of the deleted image, viewable or damaged (corrupt). A review of tool functionality is given together with the most effective tools useful in retrieving images from deleted Secure Digital cards.

Keywords

Forensics, retrieval, secure digital (SD), solid state disks, removal media, freeware based tools.

INTRODUCTION

Digital storage devices have developed rapidly over the past five years which includes storage size, physical size and shape. In computer security it is accepted that technology can be used for illegal purposes when its fall into criminal hands even if the technology was designed for a purely different purpose. One popular type of storage device is the Secure Digital (SD) Card, which is part of the 'solid state' family of technologies. Therefore a number of tools have been developed to recover data from solid state disks. Most of the currently available tools are commercially developed and therefore are expensive. The purpose of the paper is to test the ability of freeware tools to recover deleted digital images from SD cards. Some of the tools have the ability to retrieve other file formats and these are noted in the results. The tools selected for testing are all freeware based tools that are comparable in functionality to the commercial tools. This paper investigates the effectiveness of some of these freeware tools obtainable from the World Wide Web.

TESTING SCENARIO

Experiment procedure

The experiment was carried on an 256 MB Secure Digital card that had been used to store 101 photos along with other document such as word, PDF and other file formats. The procedure for the investigation was as follows:

- The testing tools were installed in a stable, clean windows environment;
- The SD card was hashed before and after using the tools for analyses of the card;

SD Card Integrity

In order to ensure the integrity of the SD card, an initial analysis of the card was undertaken to ensure that the card did not contain any files. A format utility from Windows XP was utilized to format the new SD card. After verifying that the card was clean, a number of files such as MSWord and PDF were saved to it together with 101 digital images. Before beginning the analysis with each tool, an MD5 hash was generated from the card to compare it with the original hash to ensure that running the tools had not affected the state of the SD card. The hash value of each image was not taken because the aim of the experiment was to analyse the ability of the tools to recover the digital photos in a viewable format, not test the images themselves. Maintaining the integrity of

the SD card whilst examining the effect of the tools was a priority to provide an equitable testing environment for each tool.

Cleaning the SD card

The SD card was formatted using the simple deletion function in Windows. No secure deletion tool was used on the SD card so that the capability of the tools to recover standard deleted images could be tested.

Testing Schema

All tools were tested on the same Secure Digital (SD) card, on a Windows environment machine using a Windows Picture and Fax Viewer (a standard tool in Windows). The targeted data was deleted photos regardless of the different file formats in which they were saved. The goal was to recover photographs in a viewable state. The selected tools used are user friendly and able to be operated without the need of manual or background knowledge on digital forensics. The experiments tested the ability of the tools to recover photos and assessed whether they were viewable or corrupt, in addition it assessed how long it took to recover the images.

The following section presents a background of each tool, software details, functional overview and the test results.

Testing Environment

1. SD card 256 MB
2. SD Card 128 MB for backup and testing purposes.
3. Two card reader via USB port
4. Stop watch (recording the time run)
5. Windows environment machine (computer).

TOOL BACKGROUND

This section gives a background on each tool selected. It includes a brief description of the software, an example of the interface and the tool functionality.

MjM Free Photo Recovery Software

This software claims that it has the ability of recovering images from memory cards that have been deleted or formatted. The tool automatically locates the memory card once its been plugged in the card reader and is then ready to scan. It displays what is contained on the card as thumbnail images. It can view photos in full size or recover them all. An example of the type of testing that MjM Data Recovery Ltd has previously conducted on the tool is:

> During our review, we first deleted all images from the card via Windows - the program found and recovered all of them. We then formatted the card in the camera and restarted the search - and again it found them all (recovery results after formatting may vary depending on the formatting method used by the camera). Works with Compact Flash, Smart Media, Memory Sticks and other media storage cards. (MjM,2007)

Software Details

Publisher	MjM Data Recovery Ltd
File Size	3053 kb
Version & Last Updated	0.12 beta - Dec 29, 2006
License	Freeware
Windows	98/ME/2000/XP
Site	http://www.snapfiles.com/get/mjmphotorecovery.htm

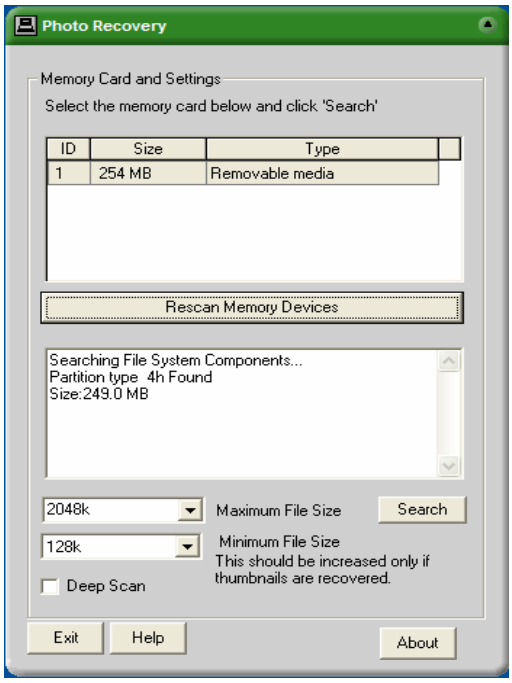

Figure 1. MjM (single card)

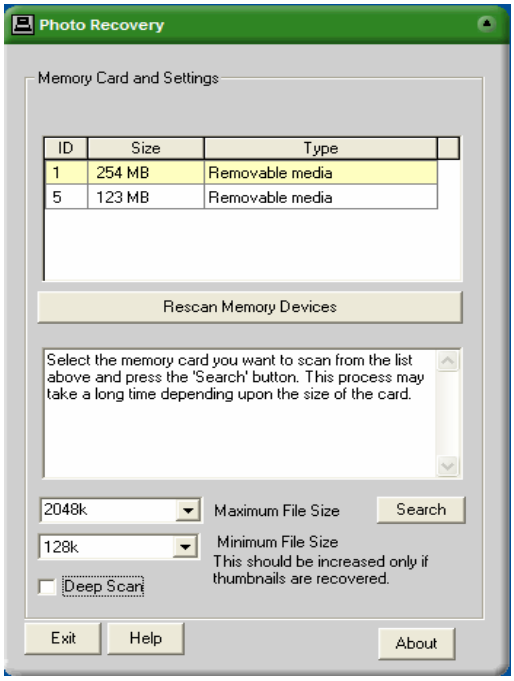

Figure 2. MjM (dual cards)

Tool Functionality

The interface is simple as shown in Figure 1. It contains a number of sections in each terminal window and in the test displayed memory card details as shown in Figure 1. The top screen shot indicates that it recognized the presence of removal media SD card 256 MB, but it is just shown as 254 MB. Between the two windows there was memory rescanning function to scan for added memory cards if applicable. In this case the second card reader had been added, an SD card 128 MB to test the ability of the tool to handle added memory cards. The tool recognized the added memory card and displayed this as 123 MB removable media, as shown in Figure 2. The second window displayed a massage to inform the user to select the memory device to be tested as shown in Figure 2.

The tool uses a drop down menu to select the size of the file with the maximum and minimum file size by default maximum (2048k) and minimum (128k). The tool supports a deep scan functionality where the user ticks the box will display a massage context saying "deep can only needs to be used if you photos do not show using default settings ,using a normal scan or if the memory file system is corrupt" as shown in Figure 3.

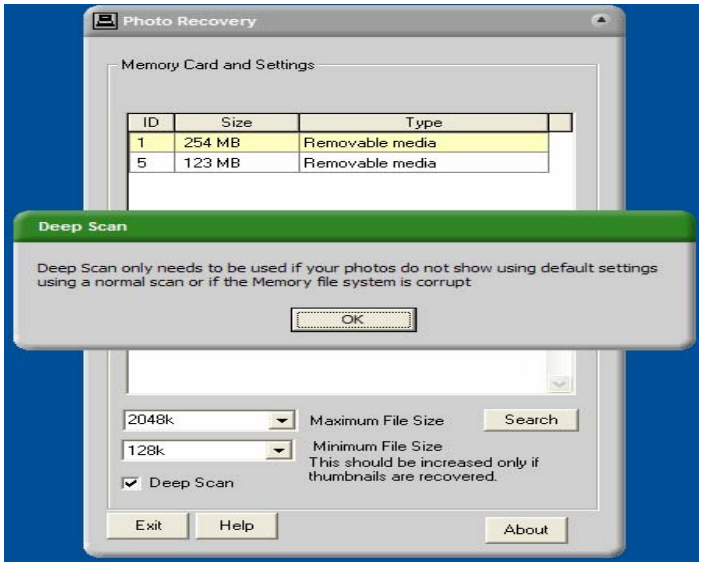

Figure 3. MjM (Deep scan option)

PC Inspector Smart Recovery

PC Inspector Smart Recovery is an inspection based program to look at removable media such as secure digital and multimedia cards. This tool been advertised to work with any removable media from digital cameras and recover any files that have been deleted (GmbH, 2007).

Software Details

Publisher	CONVAR DEUTSCHLAND GmbH
File Size	Size 6233 kb
Version & Last Updated	3.0 - Jun 27, 2004
License	Freeware
Windows	98/ME/2000/XP/vista
Site:	http://www.snapfiles.com/get/smartrecovery.html

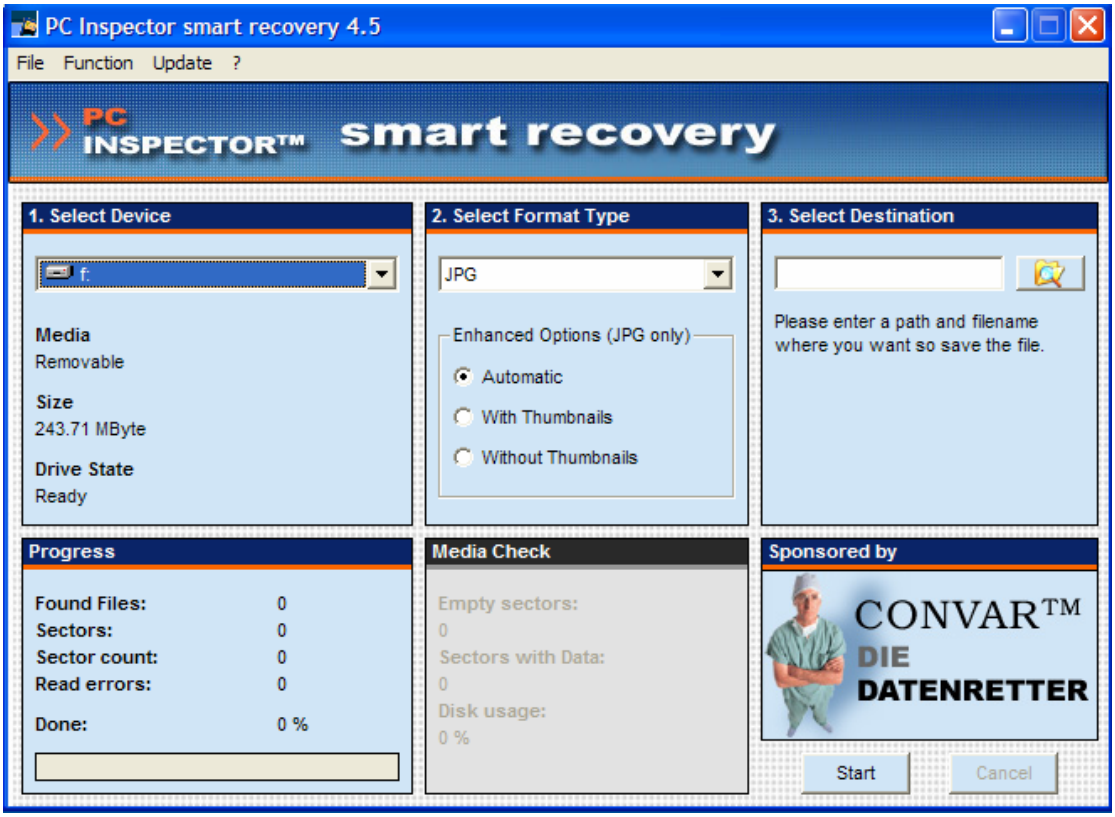

Figure 4. PC Inspector (main page)

Tool functionality

The interface of the tool is simple. It consists of two drop down menus and a browser bar to select the destination of the retrieved images. The first drop down menu is it to select the removable drive intended for inspection and retrieval. The device selection details the device such as the size of media drive and if it is fixed or removable. Whilst a second drop down menu offers selection of the format of the files intend to be retrieved as shown in Figure 4. Since this paper will look in to the effectiveness of the tool in retrieving images from an SD card, the tool was set to recover JPG photo format. In selecting the JPG format, an extra service becomes available, called enhanced options to display with or without thumbnail images. The tool supports different image format however for the purpose of this investigation the tool recovered JPG files only.

Art Plus Digital Photo Recovery

Art Plus digital photo recovery tool claims that it can recover images from formatted or corrupted memory cards. The software has the ability to retrieve images from different memory card types. Moreover it has the ability to retrieve number of other media formats. The tool claims that it has the ability to "Read corrupted cards

(even if they're not recognized by Windows)" in addition the current Version 2.3 may include unspecified updates, enhancements, or bug fixes (Art Plus, 2007).

Software Details

Publisher	Art Plus Marketing & Publishing
File Size	9 912 kB
Version & Last Updated	2.3 - unknown
License	Freeware
Windows	98/ME/2000/XP

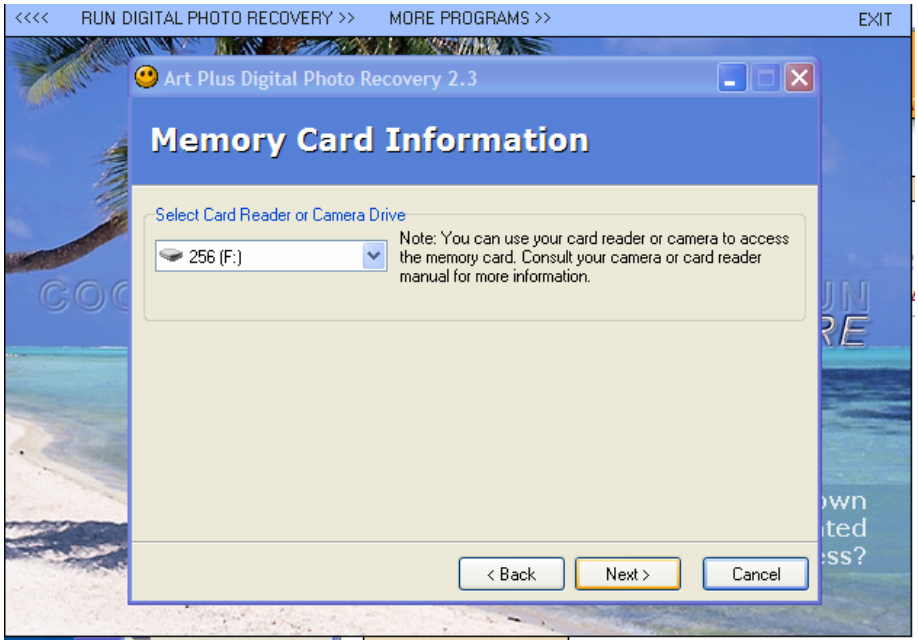

Figure 5. Art Plus (main page)

Tool Functionality

The software is self executable with no need for user specified installation. It contains a drop down menu to choose the removable drive to perform the retrieval on as shown in Figure 5. The subsequent window asks the user to select the target folder where the retrieved files will be saved. The last window displays the retrieved files and has the option to view the targeted folder or to process anther removable media card as shown in Figure 6.

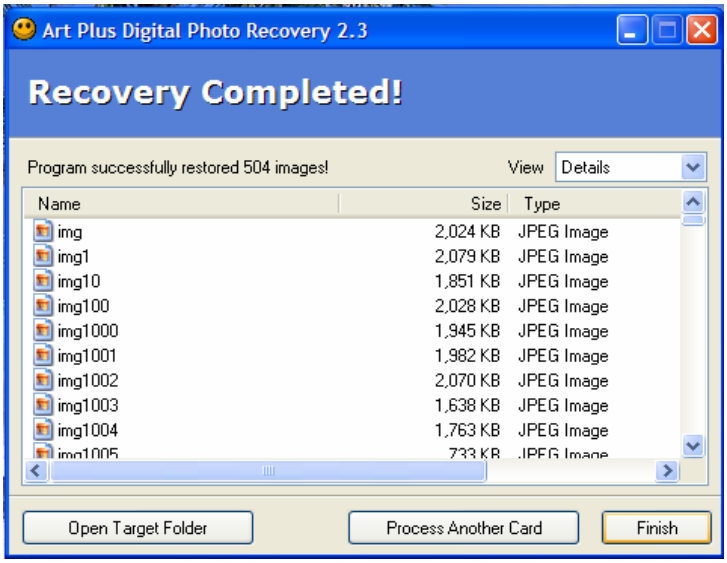

Figure 6. Art Plus (retrieved files)

Free Undelete 2.0

Free undelete is a recovery program that has been developed to retrieve files that has been deleted on an NTFS FAT32 or FAT16 file system. (Recoveronix Ltd, 2007)

Software Details

Publisher	Recoveronix Ltd
File Size	705 kB
Version & Last updated	2.0 – Unknown
License	Freeware
Windows	98/ME/2000/XP

Tool Functionality

The tool interface is simple with two main display windows. The left hand side window displays the removable media drives, where the user can select the memory card to scan. A second window displays the files that have been retrieved. The bottom of the tool window contains a search filter box where user can specify what type of files to view and the destination folder for the retrieved files as shown in Figure 7.

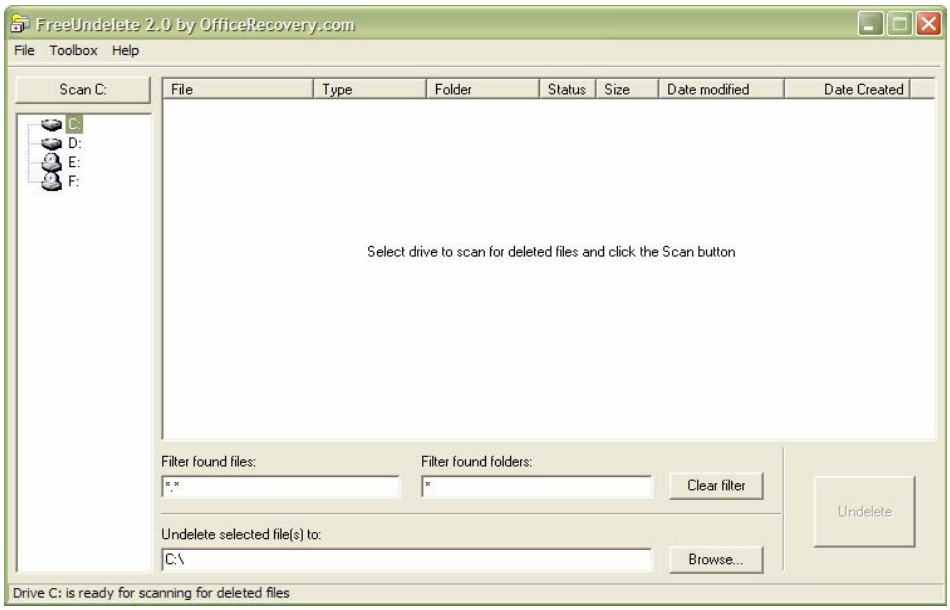

Figure 7. FreeUndelete (main page)

Recuva – File Recovery

Recuva is recovery tool that works in the Windows environment. It recovers files that has been deleted from camera memory cards even if they have been emptied from the recycle bin. The software claims that it can retrieve files that have been affected and deleted by bugs or viruses. (Recuva, 2007)

Software Details

Publisher	recuva -file recovery
File Size	282 kB
Version & Last Updated	v1.06.132- 1st October 2007
License	Freeware
Windows	98/ME/2000/XP

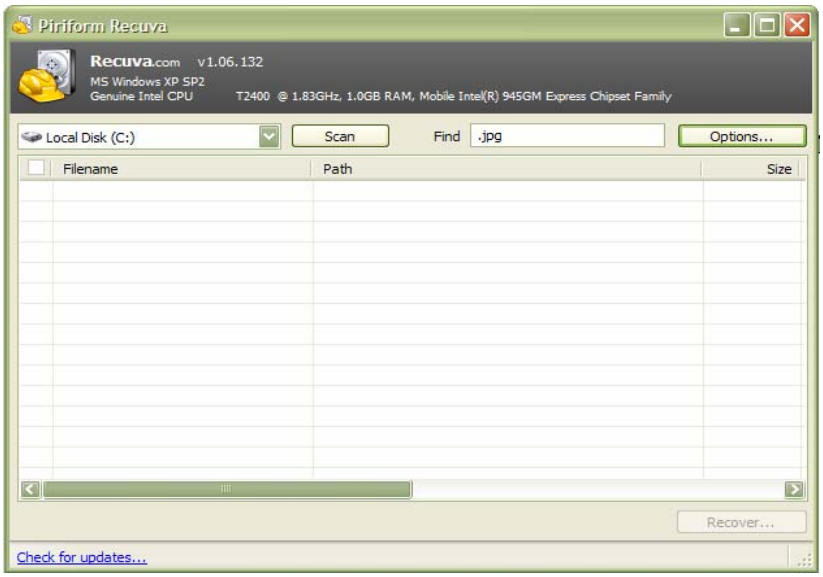

Figure 8. Recuva (main interface)

Tool functionality

The interface is easy to follow. It has a drop down menu to select the memory card to scan, as shown in Figure 8. The option button contains settings that help the user to customize the view. When the scan is complete the recover button is displayed in the bottom right hand corner to select the folder where the recovered files will be saved as shown in Figure 9. In the banner of the tool the details of the machine specification are displayed along with operating system type.

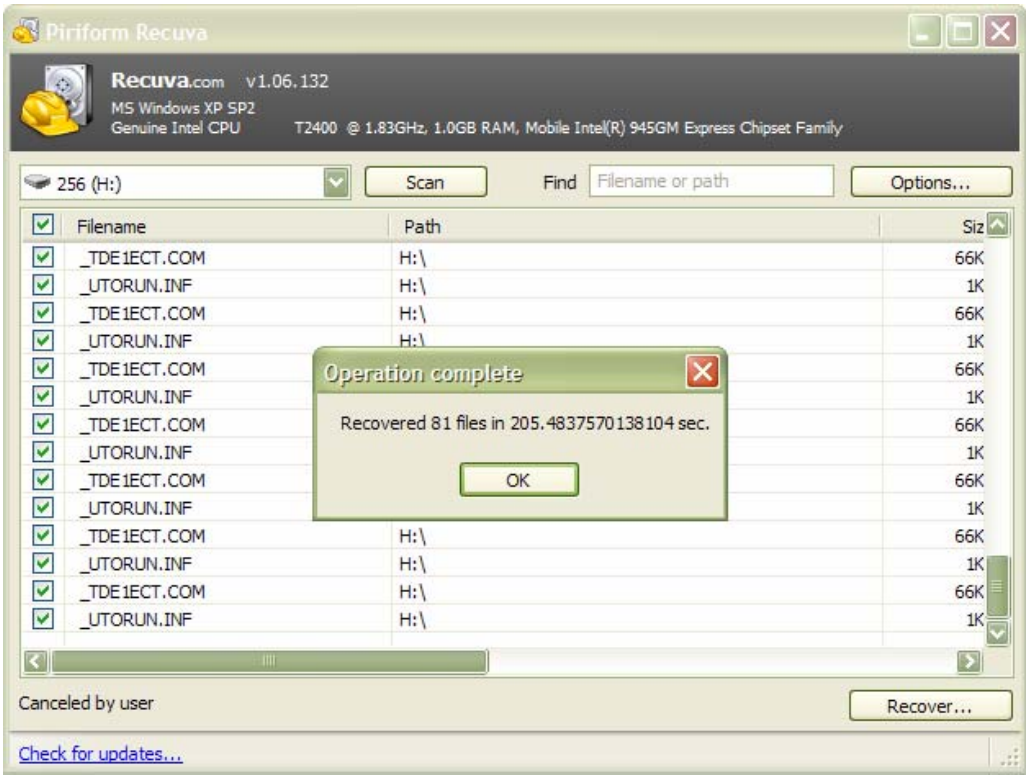

Figure 9. Recuva (scanned files)

Soft Perfect File Recovery

The tool is designed to retrieve accidentally deleted files from different storage devices. It supports CF, SD, MMC and flash drives, in addition to other storage formats ranging from FAT12 to FAT32 along with NTFS. This software is self executable and needs no user installation (Softreaserch, 2006).

Software Details

Publisher	SoftPerfect Research
File Size	248 kB
Version & Last Updated	1.1 - March 14, 2007
License	Freeware
Windows	98/ME/2000/XP/vista

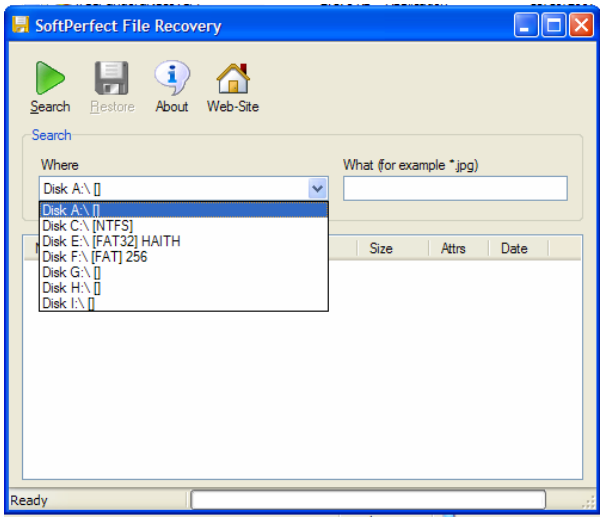

Figure 10. SoftPerfect (main page)

Tool Functionality

The tool is self executable and simple to use. The tool has a drop down menu to select the removable media for scanning and file retrieval, together with a search facility to specify what type of file to retrieve. The main window displays the findings from the memory card as shown in Figure 10. Once the files are displayed, the user can select the files to be restored and click on the restore button to select the destination of the retrieved files as shown in Figure 11.

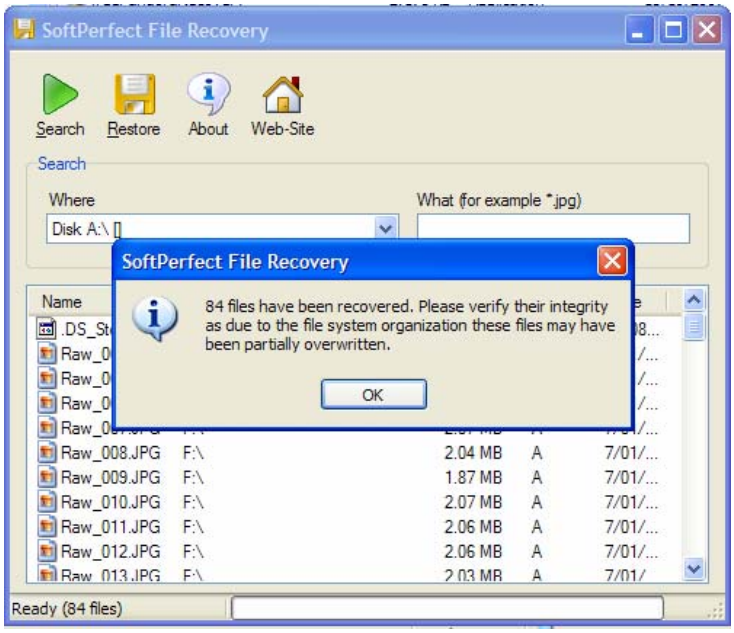

Figure 11. SoftPerfect (retrieved files)

Undelete Plus

Undelete plus is another recovery tool advertised as fast and effective retrieval of data which has been deleted. It is effective for files that have been removed from the recycle bin and after a system restart. It also supports removable media such as flash drives and secure digital memory cards. (FDRLab, 2007)

Software Details

Publisher	FDRLab Data Recovery Centre
File Size	1.06 MB
Version & Last Updated	3.0 - August,21 2007
License	Freeware
Windows	98/ME/2000/XP/vista
Site	http://www.undelete-plus.com/

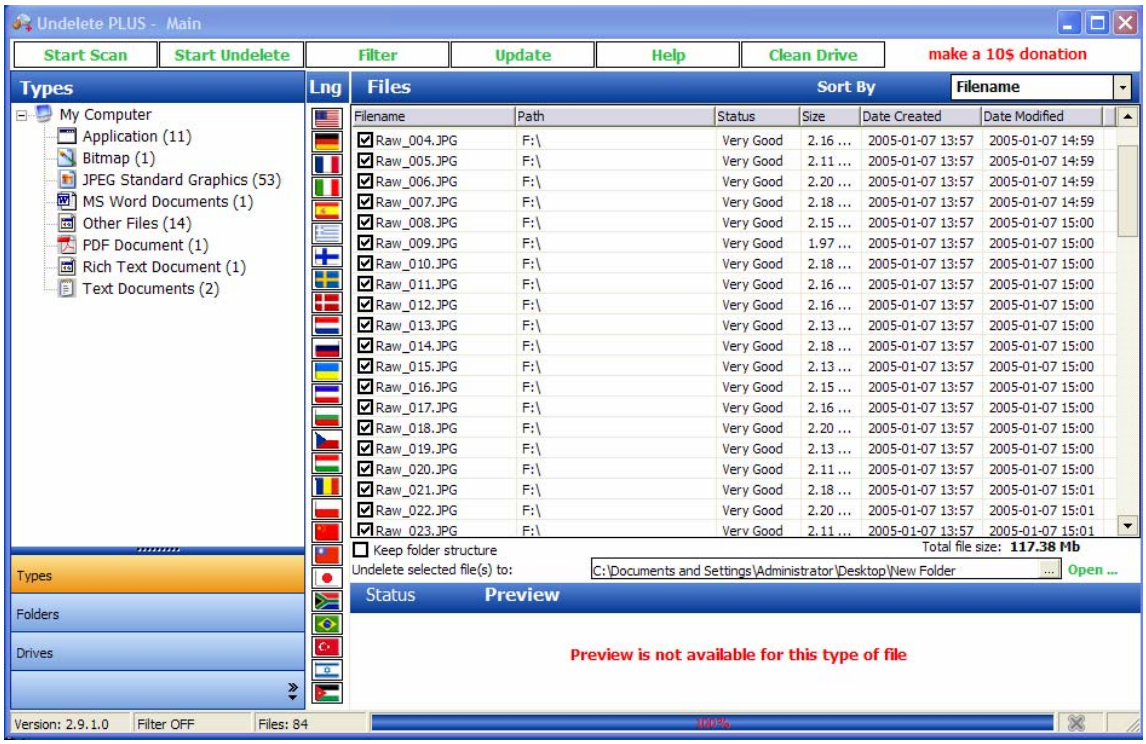

Figure 12. UndeletePlus (retrieved files)

Tool Functionality

The tool has a lot of functions. The tool displays all storage media available for the user can select the drive to recover form. Once selected a list of file extensions is displayed, followed by the number of files that have been retrieved for each extension. The tool supports multiple languages and each country flag displayed can demonstrate the language spoken in that country as shown in Figure 12. This tool supports filtering so the user can customize the search and retrieval options. It also supports cleaning the drive so the drive will be cleaned for future use.

RESULTS

Table 1. Results of test scans

Software	Time to Scan/ Retrieve	Number of retrieved files	Number of damaged files (Non Viewable)	Supported formats	Issues
MjM Data Recovery Ltd	39 min 36 sec	132	4	JPG	The scale of the minimum file size is 64k also takes very long time to recover the files
Pc inspector smart recovery	23 min 2 sec	135 files, no folders	4	Multimedia only such as photos, sounds and videos	The tool will retrieve all the files at once , it does not support selecting option to retrieve selected files
Art Plus Marketing & Publishing	21 min 22 sec	504 files	372	JPG	It retrieved 8kb file identified as jpg but cant be viewed out of 504 files 133 viewable file could be retrieved
Free undelete 2.0	17 min 34 sec	21 files and 5 folders	All	JPG and number of unknown files	The images retrieved where not viewable
Recuva –file Recovery	3 min 21 sec	81	All	unknown	The tool did not successfully retrieve the viewable images also a miss match of the displayed retrieved files and actual files in the saved folder ,in this case the tool displayed that it has retrieved 81 files, but the recovered folder shows 64 files
Soft Perfect Research	1 min 4 sec	84 files	All	JPG, DOC, PDF and some unknown formats	The images where not viewable
Undelete plus	1 min 4 sec	57 files	All	JPG, DOC, PDF,TXT and some unknown formats	The images where corrupt and did not open the word nor the PDF file.

DISCUSSION

MjM Data Recovery Ltd

The tool recovered the photos in viewable format. Four images were partially corrupt and the rest where viewable. The tool took the longest time of all the tools tested to recover the images but it was complete. The only drawback was the scale of the images at 64k with some thumbnails smaller than 10k and usually they do not get corrupt because they are easy to recover.

PC Inspector –Smart recovery

This tools was also reasonably successful and took 23 minutes to scan and recover the files. The total number of files found was 135 files and only 4 files where corrupt but could still be viewed as thumbnails. This tool only worked with multimedia file format, which makes it very good tool to recover images from solid state drives.

Art Plus

The tool took 21 minutes to recover the files, however it did 504 files. 372 of these files where only 8 kb and could not be viewed with the remaining 132 files viewable. This matched the files that were recovered by the MJM tool. However this tool took half as much time to retrieve more files.

FreeUndelete 2.0

The tool took some time to scan the files. It retrieved 21 files and 5 folders, but these were not viewable. Other file formats were recovered, however the folders contained different file format than the photos.

Recuva

This tool was fast, but unfortunately it did not retrieve as many files as the other programs. In addition, the files were not viewable. It was able to retrieve some other files however these were not identified as it was out of scope of this paper. The display of the retrieved images did not match the actual retrieved files on the saved folder.

Soft Perfect

Very fast tool which only took one minute to scan and retrieve 84 files. Unfortunately the files where not viewable. It did retrieve other file formats such as word and PDF.

Undelete Plus

This was another fast tool which only took one minute to scan and retrieve files. It recovered 57 files, but the photos where not viewable. Other formats where recovered such as PDF, TXT and other unknown formats. These files were not examined.

CONCLUSION

This paper tested eight freeware tools, obtained from the internet, to retrieve deleted photos in a viewable format. The results show that the faster tools did not retrieve the photos in a viewable format. However, the faster tools did retrieve some evidence of photos had been present on the SD card and that subsequent forensic examination of these files would be warranted. As such these tools would be useful as an initial rapid analysis of the removable media which would then need further analysis using other tools to recover the viewable images from the memory device. As it has been shown not all of the tools works in the same approach, neither do they recover the identical amount of files. Out of eight tools, three of the tools have successfully retrieved images in a viewable format. The tools have retrieved photos that can not be viewed on the Windows platform, however they may be viewable on other operating systems or photos viewer programs. Future research will look at using a known secure file deletion tool on the card and then rerunning the tests to see how effective they are under secure deletion conditions.

REFERENCES

ArtPlus. (2007). *Free Art Plus Digital Photo Recovery*. Retrieved 15 November 2007, from http://www.artplus.hr/adapps/eng/dpr.htm

FDRLab. (2007). *Undelete Plus. Free file recovery software. Retrieve accidentally deleted files.* Retrieved 15 November 2007, from http://www.undelete-plus.com/

GmbH. (2007). *PC Inspector Smart Recovery download and review - recover digital camera files from SnapFiles.* Retrieved 15 November 2007, from http://www.snapfiles.com/get/smartrecovery.html

MjM. (2007). *MjM Free Photo Recovery Software download and review - recover images from media cards from SnapFiles*. Retrieved 15 November 2007, from http://www.snapfiles.com/get/mjmphotorecovery.html

RecoveronixLtd. (2007). *Undelete Plus. Free file recovery software. Retrieve accidentally deleted files.* Retrieved 15 November 2007, from http://www.undelete-plus.com/

Recuva. (2007). *Recuva - Undelete, Unerase, File Recovery - Home.* Retrieved 15 November 2007, from http://www.recuva.com/

Softreaserch. (2007). *Restore accidentally deleted files from FAT and NTFS volumes.* Retrieved 15 November 2007, from http://www.softperfect.com/products/filerecovery/

COPYRIGHT