12-3-2012

The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia

Patryk Szewczyk
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University

DOI: 10.4225/75/57b3d443fb870
10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

THE 2012 INVESTIGATION INTO REMNANT DATA ON SECOND HAND MEMORY CARDS SOLD IN AUSTRALIA

Patryk Szewczyk and Krishnun Sansurooah
SRI - Security Research Institute, Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au; k.sansurooah@ecu.edu.au

Abstract

This study investigates the remnant data on memory cards that were purchased through Australian second hand auctions sites in 2012. Memory cards are increasing in capacity and are commonly used amongst many consumer orientated electronic devices including mobile phones, tablet computers, cameras and multimedia devices. This study examined 78 second hand memory cards. The investigation shows that confidential data is present on many of the memory cards and that in many instances there is no evidence to suggest that the seller attempted to erase data. In many instances the sellers are asking the buyer to erase the data on the memory card. It is evident through this research that consumers are not appropriately informed of the dangers of disposing of personal media through second hand auction sites. Subsequently consumers do not take the appropriate actions to remove data.

Keywords
Digital forensics, memory cards, flash memory, remnant data, eBay

INTRODUCTION

Memory cards are inexpensive, versatile and are used in a vast array of consumer electronic devices. Vendors have traditionally manufactured personal electronic devices (e.g. mobile phones, tablet computers) with internal storage limitations. However, this can often be increased by an end-user through the use of an additional memory card. Small capacity memory cards create limitations on the amount and type of data that can be stored. However, recently emerging large capacity memory cards can be used to store and potentially clone the contents of an end-user's personal computer. Subsequently, end-users benefit from being able to carry their important data with them at all times.

Two predominant electronics devices permitting the use of additional memory cards include smart phones and tablet computers. There is speculation that tablet computers sales will exceed traditional notebook and desktop sales by 2015 (Tofel, 2010). Such speculation is becoming a reality sooner than people may have envisioned. Corporations who believed Ultrabook computers would encourage consumers to stick to traditional computers, have now realised that consumers are choosing tablet computers as desktop and notebook replacements (Pepitone, 2012). Android based smart phones are also dominating the market in 2012, accounting for nearly seventy percent of all phone sales (Wasserman, 2012). Android devices generally include expansion slot interfaces for memory cards. Both of these devices allow the end-user to utilise the device as if it were a personal computer, and easily interchange or upgrade the storage capacity through the use of memory cards.

With the ease of upgrading the storage capacity of the aforementioned devices, consumers may continually upgrade their device, and then sell their obsolete memory cards through second hand auction sites. However, unless proper precautions are taken to erase the data on the memory card, confidential data could be acquired and misused if in the wrong hands. The issue of remnant data on second hand storage devices is an ongoing issue. Research has clearly shown that regardless of the storage medium (hard disks, flash drives, memory cards) that end-users continually dispose of these devices in an inappropriate and insecure manner, leaving confidential data intact (Szewczyk & Sansurooah, 2011; Valli, 2004; Valli & Woodward, 2008). The issue has become so significant that approximately one in three persistent storage devices sold through eBay contains some confidential data (Bhat & Quadri, 2012). This study investigates if the issue of remnant data on memory cards sold on second hand auction remains a problem in Australia despite continues media attention.

RESEARCH PROCEDURE

Between December 2011 and October 2012, 78 second hand memory cards were procured and analysed, providing a representative view of remnant data on memory cards in Australia. All of the memory cards were purchased through the second hand auction site eBay – Australia. Memory cards were located and purchased in each of the eBay categories of mobile phones, cameras, and video games. For the purpose of this research a second hand memory card constitutes an item in which the seller on eBay claims that it has previously been used, and has subsequently listed the item as either *used* or *refurbished*. In some instances the memory cards were purchased in small bulk lots as the seller had two or three cards for sale simultaneously. The table below shows the final breakdown of the types of memory acquired in 2012 versus 2011 (Szewczyk & Sansurooah, 2011). Most consumer electronic devices still utilise either microSD or standard SD cards. As a result it was expected that these two formats would have dominated the types of memory cards purchased.

Table 1 Comparison of memory card types purchased

Memory Card Type	Quantity Purchased 2011	Quantity Purchased 2012
microSD Card	64 (55%)	45 (58%)
miniSD Card	4 (3%)	0
SD Card	13 (11%)	26 (33%)
Memory Stick Pro Duo	8 (6%)	2 (3%)
M2 Card	18 (15%)	2 (3%)
Compact Flash Card	12 (10%)	2 (3%)

To avoid alerting sellers to the fact that the memory cards could be utilised for research purposes, multiple eBay aliases were utilised to conduct the transactions. In turn it was anticipated that this would reduce the chances that the sellers would take additional precautions to erase data from the memory cards. Unfortunately, the number of second hand memory cards purchased on eBay this year was lower than the number procured in 2011 (Szewczyk & Sansurooah, 2011).

Daily email notifications were received regarding newly listed *used* memory cards. This allowed each memory card to be bid on with the anticipation to purchase every listed item. In 2011, approximately ninety-six percent of all memory cards listed in the eight month period were purchased. Due to project budget constraints, and a large un-justified interest in individuals purchasing memory cards from eBay, only seventy-one percent of all second hand memory cards were purchased. The storage capacities of memory cards have also changed considerably compared to 2011. Table 2 compares the size of memory cards procured in 2011 and 2012. The size of current memory card capacities has reached the point where end-users can store a vast amount of files. Large capacity memory cards have the potential to encompass a significant quantity of confidential data and subsequently were bid on aggressively through the second hand auction site.

Table 2 Number of Memory Cards Purchased

Size of Memory Card	Quantity Purchased in 2011	Quantity Purchased in 2012
32 MB	1 (1%)	0
64 MB	9 (8%)	0
128 MB	13 (11%)	2 (3%)
256 MB	9 (8%)	0
512 MB	19 (16%)	0
1 GB	38 (32%)	17 (22%)
2 GB	26 (22%)	20 (26%)
4 GB	3 (3%)	14 (18%)
8 GB	1 (1%)	15 (19%)
16 GB	0	6 (8%)
32 GB	0	3(4%)

The research investigation leveraged the tools and techniques used in previous similar studies undertaken on hard disks and USB drives (Jones, Valli & Dabibi, 2009; Valli & Woodward, 2008). This same methodology was utilised to investigate the memory card sample in the 2011 study, and proved both effective and efficient in acquiring confidential data (Szewczyk & Sansurooah, 2011). A raw *dd* image was created of each memory card utilising FTK Imager 3.1.1 (FTK Imager, 2012). Recovery and analysis was subsequently undertaken through

WinHex 15, using the *File Recovery by Type* function (Reischmann, 2011) and further validated through Autopsy 3.0.0b5 (Carrier, 2012).

Given the media publicity of end-users disposing of memory cards inappropriately (DeCeglie, 2011) and the warnings given by eBay to erase data (eBay, 2011) the researchers were hopeful that the amount of confidential data would have diminished significantly compared to previous years. However, despite these warnings the realistic expectations were that the problem of inappropriate memory card disposal would remain the same if not increase in the 2012 investigation.

REMNANT DATA RESULTS

Twenty-nine percent (23) of the memory cards were not recoverable. As a result it would appear that the seller may have taken the appropriate precautions to remove any data. This is a positive aspect in that the 2011 analysis of second hand memory cards showed that only twelve percent were not recoverable (Szewczyk & Sansurooah, 2011). Nineteen percent (15) of memory cards had their data deleted, but were easily recoverable. The 2011 had as many as seventy-four percent (58) of memory cards with data deleted. Overall, in 2011 approximately eighty-seven percent (104) of memory cards investigated showed that the seller took some action to remove the data. In 2012, this figure has dropped considerably with only forty-nine percent (38) of memory cards investigated showing attempts to remove confidential data. Fifty-one percent (40) of memory cards purchased had all data in-tact with no evidence to suggest that the seller attempted to remove the data. Table 3 portrays the breakdown of the types of information that were recovered from the 78 memory cards in 2012.

Information Types Recovered	**Number of Cards**
Multimedia (audio, video)	41 (53%)
Photographic images	28 (36%)
Private personal documentation	15 (19%)
Sexualised images	13 (17%)
Private business documentation	11 (14%)
Business cards (e.g. vCard)	11 (14%)
Tertiary institution documents	7 (9%)
Resumes	4 (5%)
Pornography	4 (5%)
Government documents	2 (3%)

Work related information appeared quite low in the majority of investigation. However, private personal information was considerably high with the memory cards encompassing a variety of files with personally identifiable information and financial data. The notable recovered memory cards have been shown below. The case numbers reflect the order of analysis and do not in any way reflect the purchasing order or type of data that had been recovered. Throughout 2012, the authors' identified six notable memory cards which encompassed sufficient confidential information to cause fraud or embarrassment to the owner.

- Case 17 had been deleted but data was recovered. The memory card predominantly contained multimedia files and amongst other things a directory named *trash*. The *trash* directory encompassed two scanned images of two current credit cards from a large Australian bank. The directory also contained a text file with the heading PayPal and bank. Both of the aforementioned headings contained what looked like login credentials to access the specific online account. The auction sites' sellers name corresponded to the names on the credit cards.

- Case 24 had been deleted but data was recovered. The memory card contained files for a personal business website with a detailed personal background of the business owner. The memory card also contained homemade sexualised images and movies.

- Case 31 had not been deleted and all files were intact. The memory card contained tertiary institution documents. The sellers' name matched the name on all the files. Amongst the files were university dissertation drafts, unpublished research papers, and undergraduate degree grade transcripts.

- Case 33 had been deleted but data was recovered. The memory card contained in excess of 2600 family holiday photos. In addition there was a half completed resume and a scanned Australian university degree parchment.

- Case 63 had been deleted but data was recovered. The memory card contained various multimedia files and amongst other things documents pertaining to work being undertaken in a government department. The name of the department and author of the many documents was clearly identifiable. In this particular instance the seller also included a short, hand written note stating their card reader was broken and subsequently could not erase the memory card and that buyer should do this prior to usage. The seller also made it clear that that opening, viewing or copying any of the files is deemed illegal.

- Case 71 had been deleted and encompassed a vast array of personal files. These files included; a personal resume, job application letters, utility bills, multimedia files, personal photos, and personal financial transactions stored within an excel spreadsheet.

Compared with last year's memory card investigation there was a significant increase in the number of suggestive images located on memory cards. With two-thirds of teenagers and adults sexting world wide (Henderson, 2011) this is no real surprise. Unfortunately this year's investigation revealed that in approximately seventy percent of cases, the seller had not taken any action to remove any of the suggestive images. Although the suggestive images were concealed amongst other files, they could still be obtained by an individual with the right skill set.

It appears that sellers are becoming increasingly lazy when it comes to erasing their own confidential data. Nineteen sellers (24%) included either a hand written or printed note stating that the memory card needs to be erased/formatted prior to usage. Not only does this encourage the buyer to potentially snoop through the memory card data, it also presents a significant privacy issue for the seller. Sellers may be ignorant to the fact that someone could misuse their confidential data. There could also be the issue of how much time a seller is willing to dedicate to prepare a memory card for shipping after a sale. The average cost of the seventy-eight memory cards procured was $10.94 per card. The eBay list fee is $0.30 and the final value fee is set at 7.90% (eBay, 2012) coupled with the PayPal fee of 2.4% + $0.30 (PayPal, 2012) for receiving payment. Assuming the seller uses basic postage options, the sellers are left with approximately $7.50. With a small financial reward for selling an item, sellers may simply see no incentive to waste more time than required to erase the memory card. There could also be issue whereby sellers do not actually see the value in the data stored on the memory card.

Whilst eBay warns and advices sellers to remove personal data from the memory card prior to sale, the support ends there. A search through eBay shows there is no additional supportive information by which to guide an end-user through the process of wiping a memory card. The Australian Government has created two informative websites for online security namely Cyber Smart (CyberSmart, 2012) and Stay Smart Online (StaySmartOnline, 2012). The websites do contain information on protecting individuals online, but do not encompass any information on how to remove private data from a persistent storage medium prior to sale. With consumers continually upgrading and replacing their electronic devices, one would assume that there would be an abundance of information on wiping data. Subsequently, it is of no surprise that end-users on second hand auction sites are selling storage devices with confidential data in tact when there is simply insufficient guidance by which to mitigate this issue.

The increased capacity of modern memory cards, is allowing consumers to store a vast array of personal files. This investigation has identified that unlike the previous investigation (Szewczyk & Sansurooah, 2011) there is now a much larger spectrum of file types across these memory cards. Multimedia files were predominant with pirated movies being common on the larger capacity cards. Approximately fifty percent (43) of memory cards contained at least one private or business related document. This included covering letters, reports, resumes, business spreadsheets, presentations and banking documents. As tablet computers increase in sales coupled with ever increasing memory card capacities, it is only assumed that memory cards may replace traditional hard disks as a persistent storage medium.

It is anticipated that the trend of private or business related documents will continue to escalate on memory cards. Many financial institutions, Government and utility departments utilise paperless bills and statements. These departments often offer incentives to customers should they choose paperless correspondence. Subsequently bills, receipts, and informative letters are often emailed to customers. Coupled with consumers utilising tablet computers more often, many of these potentially confidential documents may continue to find themselves stored on the memory cards utilised within these devices.

CONCLUSION

It has been continually reported that Australian cyber crime has reached epidemic proportions (Offner, 2012; Roberts, 2010). Amongst all cyber crime issues this investigation shows that there is a significant issue in how persistent storage is disposed of. Consumers are also becoming lazier in asking the buyer to erase data on behalf of the seller, only further encouraging the buyer to scrutinise the memory card.

There are a number of potential solutions which second hand auction sites could utilise to encourage proper wiping of persistent storage mediums prior to sale. Scare tactics are a potential solution to demonstrate to sellers the dangers of not erasing data. Simplistic step-by-step procedures to educate end-users could also aid in allowing sellers to take proper precautions. Being a global leader in the second hand auction market, eBay itself should provide (novice) sellers with sufficient information to carry out the erasing process effectively. Ignoring this issue will only further increase the size of the issue especially as additional novice sellers enter the market to quickly and easily dispose of their obsolete electronic devices.

This research investigation will be repeated in subsequent years. The issue of memory card disposal will not diminish quickly, especially as tablet computers and smart phones become common practice. The large capacity memory cards will also allow a significant amount of data to be stored potentially negating the need for a laptop or desktop computer entirely. National publicity (DeCeglie, 2011) from this research in previous years has thus far shown to have little impact on sellers' behaviours. Subsequently, online, print, and television media may also play a vital role in raising awareness of not only cyber crime, but also the now very problematic issue of inappropriate persistent storage disposal.

REFERENCES

Bhat, W. A., & Quadri, S. M. K. (2012). After-deletion data recovery: myths and solutions. *Computer Fraud & Security, 2012*(4), 17-20.

Carrier, B. (2012). The Sleuth Kit. Retrieved September 20, 2012, from http://www.sleuthkit.org/autopsy/download.php

CyberSmart. (2012). CyberSmart - Internet and mobile safety advice and activities Retrieved September 13, 2012, from http://www.cybersmart.gov.au/

DeCeglie, A. (2011). Your secrets exposed: Hidden danger in old memory card sales. *The Sunday Times*.

eBay. (2011). Advice for selling mobiles phones safely on eBay. Retrieved January 20, 2011, from http://pages.ebay.co.uk/buy/guides/mobile-phone-advice/#1

eBay. (2012). eBay Final value fees. Retrieved October 1, 2012, from http://pages.ebay.com.au/help/sell/fees.html#final

FTK Imager. (2012). Forensic Toolkit Imager. Retrieved September 20, 2012, from http://accessdata.com/support/adownloads#FTKImager

Henderson, L. (2011). Sexting and Sexual Relationships Among Teens and Young Adults. *McNair Scholars Research Journal, 7*(1), 1-9.

Jones, A., Valli, C., & Dabibi, G. (2009). *The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market.* Paper presented at the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Offner, S. (2012). Could you be Australia's next cyber crime victim? Retrieved June 15, 2012, from http://newsroom.unsw.edu.au/news/law/could-you-be-australia%E2%80%99s-next-cyber-crime-victim

PayPal. (2012). Transaction Fees for Domestic Payments. Retrieved October 1, 2012, from https://www.paypal-australia.com.au/business/manage-my-payments/transaction-fees

Pepitone, J. (2012). Ultrabook sales forecast slashed in half for 2012. Retrieved October 1, 2012, from http://money.cnn.com/2012/10/01/technology/ultrabook-sales-forecast/index.html

Reischmann, S. (2011). X-Ways Software Technology. Retrieved March 23, 2011, from http://www.winhex.com/winhex/

Roberts, G. (2010). Australia a top 10 target for cyber crime. Retrieved April 14, 2012, from http://www.abc.net.au/worldtoday/content/2010/s2800551.htm

StaySmartOnline. (2012). Stay Smart Online - About Retrieved October 9, 2012, from http://www.staysmartonline.gov.au/about

Szewczyk, P., & Sansurooah, K. (2011). *A 2011 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia.* Paper presented at the 9th Australian Digital Forensics Conference, Citigate Hotel, Perth, Western Australia.

Tofel, K. C. (2010). 3 Reasons Tablets Will Take 1 in 4 PC Sales By 2015. Retrieved September 18, 2011, from http://gigaom.com/mobile/3-reasons-tablets-will-take-1-in-4-pc-sales-by-2015/

Valli, C. (2004). *Throwing Out the Enterprise with the Hard Disk.* Paper presented at the 2nd Australian Digital Forensics Conference, Esplanade Hotel in Fremantle, Western Australia.

Valli, C., & Woodward, A. (2008). *The 2008 Australian study of remnant data contained on 2nd hand hard disk: the saga continues.* Paper presented at the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Wasserman, T. (2012). Android Was in 68.1% of Smartphones Shipped in Q2. Retrieved October 1, 2012, from http://mashable.com/2012/08/08/android-smartphone-marketshare/