Survey of Data remaining on Second Hand Memory Cards in the UK

A Jones
Cyber Security Centre
University of Hertfordshire
Edith Cowan University
a.jones26@herts.ac.uk

O Angelopoulou
Cyber Security Centre
University of Hertfordshire
o.angelopoulou@herts.ac.uk

L Noriega
Cyber Security Centre
University of Hertfordshire
l.noriega@herts.ac.uk

Abstract

This study was an investigation into the level and type of information that remained on memory cards (SD, Micro SD)[1] that were purchased from the second hand market in the UK in 2018. The storage capacity of memory cards has continued to increase in capacity at a rapid rate and had reached 512GB at the time of the study. Memory cards are now commonly used in a wide range of consumer devices, but are used, in the main, in mobile phones, tablet computers, cameras, Satellite Navigation (SatNav) systems, dashboard cameras (dashcams), drones and multimedia devices. This study was carried out on 100 second hand memory cards. The aim of the study was to determine the proportion of memory cards that still contained data and of those that did, what type of data they contained. The study also looked, where data was found, at whether any attempt had been made to remove it. The investigation showed that sensitive and personal data was present on 67 percent of the memory cards. While some of the memory cards showed evidence of attempts to remove the data, in many instances there was no such evidence to suggest that the seller had made any attempted to remove it.

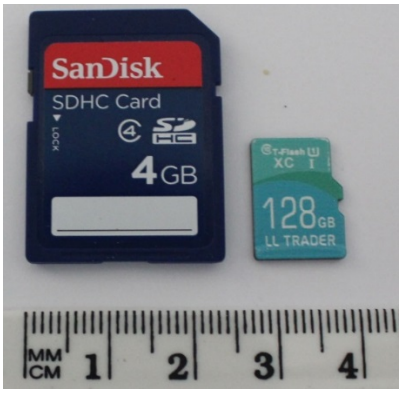
Keywords: Memory cards, flash memory, residual data, Digital forensics, eBay

INTRODUCTION

Memory cards, in particular the micro SD card, which has become the industry standard, provide a convenient, small and inexpensive option for data storage. Because of their size and minimal weight, they provide an extremely versatile data storage option and as a result, are now used in a large range of consumer electronic devices. Figure 1 below shows the SD and Micro SD card formats that were used during this research. While, historically, there have been cards available on other formats, none were found to be for sale during the period of the research.

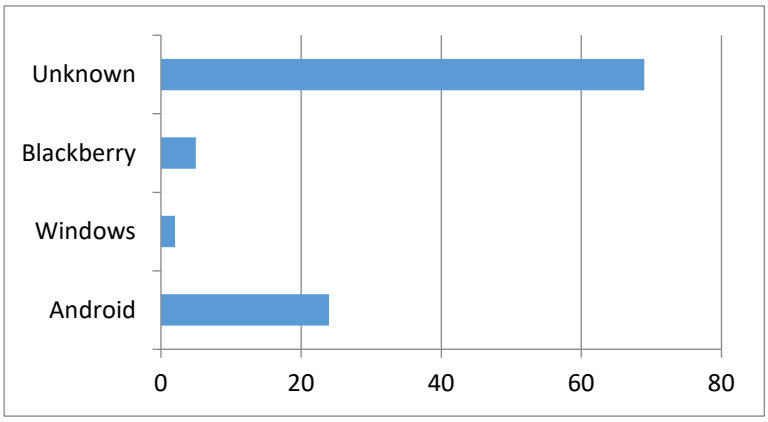
[1] Secure Digital (SD) is a non-volatile memory card format developed by the SD Card Association (SDA) for use in portable devices.

Figure 1 – SD and Micro SD cards



In addition to their use in a whole range of mobile devices, the emergence of the large capacity memory cards have now reached the size that makes them a viable option for the backing up of the contents of a user's personal computer. The storage capacity of a Micro SD card (up to 512GB) is now equal to or greater than the capacity of most home use laptop computers. This gives the users the benefit of being able to back up and carry their sensitive or important data with them at all times, without the need for a bulky and weighty external disk drive. At the present time the two main types of device in which memory cards appear to have been used are smart phones and tablet computers, although during this research examples were also found of them being used in SatNav systems, dashcams and drones. While the Apple iphone and ipad do not have slots to allow for the use of memory cards, almost all other mobile devices do. The market share of the different operating systems in the UK in March 2018 was the Apple iOS at 53.3%, devices with the Android operating system at 44.4% and other operating systems (Windows and Blackberry) at a combined 1.2 percent (Statistica, 2018). Table 1 below shows the breakdown of operating systems that could be identified during the study.

Table 1 - Operating System identified on media in the study



As with any other type of storage media, unless proper precautions are taken to erase the data on the memory card, sensitive data can remain and could be misused if the buyer has malicious intentions. The issue of remnant data on second hand storage media is ongoing and had been researched for more than a decade (Jones et al, 2005, Jones et al, 2009, Szewczyk and Sansurooah,

2012). Prior research has shown that all types of storage medium, such as hard disks, USB thumb drives, memory cards that end-users dispose of are likely to contain confidential or sensitive data if the appropriate measures are not taken to remove it.

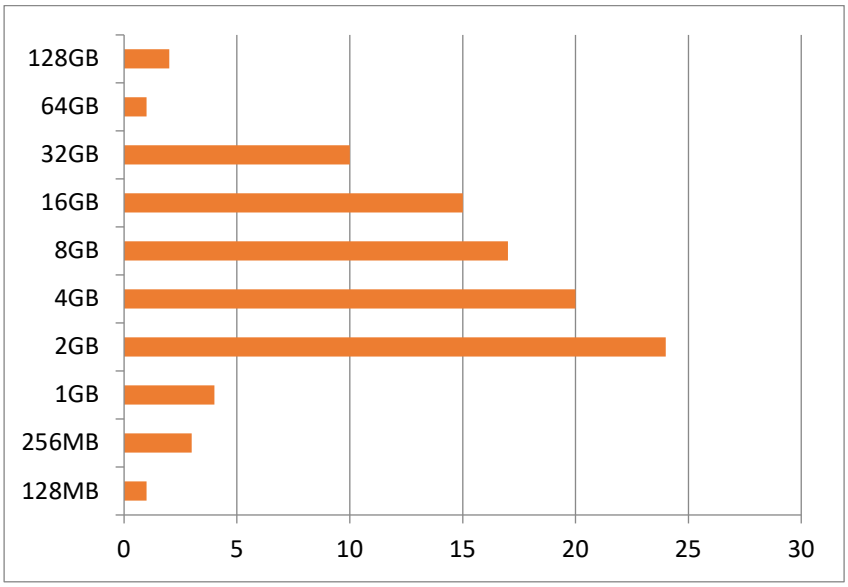
With the increasing capacity of memory cards, confidential and sensitive data that remains on media is becoming an ever more significant issue. This study investigates whether the issue of remnant data on memory cards sold on second hand market remains a problem in the UK despite the ongoing news media attention with regard to the issue.

RESEARCH PROCEDURE

Between January and May 2018, 100 second hand memory cards were purchased from a range of second hand sources, primarily via Ebay, but also from conventional auctions and second hand shops. The memory cards were then processed and analysed in a forensically sound manner. The majority of the cards were purchased singly, although on a small number of occasions, the memory cards were purchased in small lots as the seller had more than one card for sale at the same time. While it is acknowledged that other card formats still exist, the cards that were purchased were all either SD cards or Micro SD cards, as these were the only types that were on sale during the period. The cards were purchased over a four-month period in order to prevent any distortion in the market and also in order not to alert potential sellers of one organisation purchasing a large number of memory cards.

The storage capacity of the memory cards varied considerably and Table 2 below shows the spread if capacity of the cards purchased. At the time of writing this report, the maximum capacity of Micro SD memory cards was 512GB.

Table 2 - Storage capacity of memory cards purchased



This research used the same tools and methodology and techniques that had been used in previous studies undertaken on hard disks, USB drives and memory cards (Valli, 2004, Jones, Meyler, Gooch & Mee, 2005, Jones, Dardick, Davies, Sutherland & Valli 2008, Valli & Woodward, 2008, Jones, Valli & Dabibi, 2009; Szewczyk & Sansurooah, 2012, Jones, Angelopoulou, Vidalis & Janicke, 2016).

An image of each memory card was created utilising FTK Imager 4.2.0.13. While not necessary to obtain an image of the device, this tool was used in order to follow best digital forensic practice so

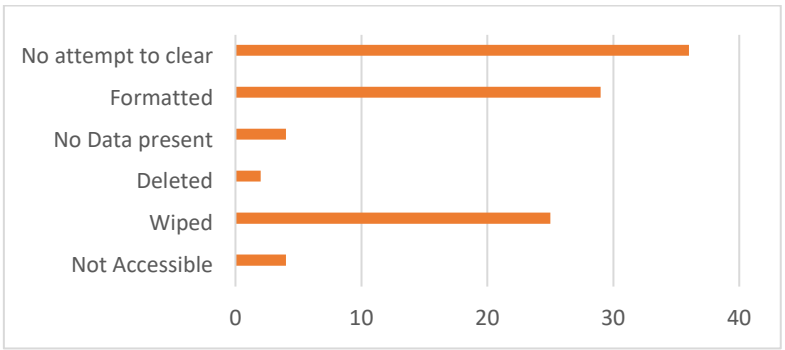
that all future analysis could be carried out on the image and the original could be preserved without modification. The subsequent analysis was conducted using WinHex 15, and the OSforensics tool (Version 5.2.1007), both of which are publicly available, free and can be downloaded from the internet.

While a number of studies have been carried out into residual data on second hand computer hard disks and mobile phones at institutions around the world over a period of more than a decade, only one similar study has been carried out into residual data on memory cards, and this took place in Australia in 2011-12 (Szewczyk & Sansurooah, 2012). In the 6 years since that study, the types of memory cards in common use and the storage capacity of the cards has changed significantly. Since the initial second hand hard disk study in 2005, there have been a number of studies and innumerable media reports on the issue of data leakage and advice on the care that is needed regarding the destruction of data when disposing of storage media. However it appears that users are still not taking appropriate measures to remove data. There may be a number of reasons for this, including the widespread belief that deleting data or performing a quick format of the media will actually remove the data. On other occasions it might be simply a human error, where the users do not consider the content of the device they decide to sell in the second hand market.

REMNANT DATA RESULTS

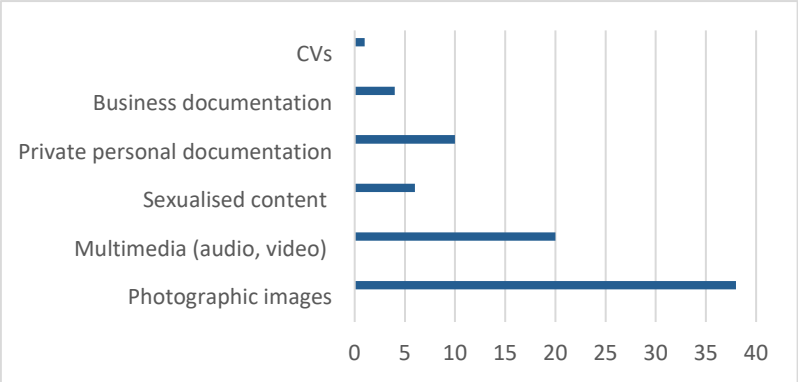
Of the 100 memory cards that were purchased, 4 percent were not accessible and could not be read using the tools available. These may have been accidentally or purposely made inoperable. Of the remainder, 25 appeared to have been wiped using a data erasing tool and it would appear that the sellers have taken the appropriate precautions to remove any data as the storage area had been overwritten with 0s or another character. 29 appeared to have been formatted, but data could still be recovered with minimal effort. 2 appeared to have had the data deleted but, again, it could easily be recovered. Another 4 had no data present, but the reason for this could not be determined. 36 did not appear to have had any steps taken to remove the data. Table 3 below shows the percentages for each of the groups.

Table 3 – Percentage for each group.



Overall, data could easily be recovered from 65 percent of the memory cards that were obtained. Of these, the previous owner could be identified in 23 of the cases. Table 4 shows the breakdown of the types of information that was found on the memory cards.

Table 4 – Types of Data Recovered



As might be expected, with the majority of the memory cards having been used in mobile phones and tablet computers, the majority of the information that was recovered was personal to the previous owner. There were however a small number of memory cards that had been used in a business environment. Again, as might be expected, the vast majority of the data recovered was in the form of photographs and video clips.

Notable examples of the type of data recovered from the memory cards is shown in the cases below. Overall, the number of cases where the data recovered from the memory cards was sufficient to identify the previous owner was relatively low, but this is consistent with the type of data expected to be found on a memory card.

Cases

01. A large number of photos, some of an intimate nature, from a female student at a University in the UK. Also included was a photo of the owner's passport. SD card probably from Tablet computer.

02. A number of selfie photos from a female owner together with an email address, phone number, names and phone numbers of friends. SD card probably from smart phone.

03. The name of the owner and email addresses, family photos. SD card probably from smart phone.

04. The name of the owner, home address, phone number, email address, vehicle reg no. credit card pin number from a university student in the UK. SD card probably from smart phone.

05. A male owner, probably in his late 50s. The card included pornography, holiday and hobby photos, vehicle reg no. SD card probably from smart phone.

06. Several navigation files, a large number of pictures for articles to be sold on eBay, an invoice with the owner's name and address, and also large number of .pdf files. SD card probably from Tablet computer.

07. The email address of the female owner. Also, a large number of family photos including several of a man in military uniform, plenty of farm photos, vehicle registration number name of husband and livestock .pdf files. SD card probably from Tablet computer.

08. Videos, photos, 2 medical case reports from an Indian Journal and a planning application for land at an old hospital near Norwich. SD card probably from Tablet computer.

09. The first name of the owner, several nude photos of male and female, as well as videos of dog training, a visit to a zoo, a young man (cadet) in military uniform at Wathgill army camp Caterick. SD card probably from smart phone.

10. Document headers referring to SeaBank Chapel, Kings Lynn and a response to queries raised at Gt Yarmouth and Waveney Contract meeting on 6/11/2015. SD card probably from Tablet computer.

11. The name of the young female owner and details of the area in which she lives and a number of friends, as well as images and texts, references to Newcastle upon Tyne, Bradford, Leeds, a photo of a man in RAF uniform, , a huge number of selfies, photos of family, intimate photos, Instagram, snapchat. SD card probably from smart phone.12. Contains vCard contact lists with names and phone numbers, football videos, small number of football photos. SD card probably from smart phone.

13. Contains images of pornography, bondage, beach scenes, possibly photos of owner, References to Bridgend, vehicle registration number, email address, music, some web browsing details. SD card probably from smart phone.

14. A CV with name and address, phone number and email address, reference to a lapsed security clearance and html documents. SD card probably from smart phone.

The assessment of the device that the SD card had been used in is subjective and based on the type and volume of data recovered. It was also clear from the data that was recovered, that in a number of cases the memory card had come from the device of pre-teen children.

This study has presented a surprisingly similar proportion of items of media that still contain data (67 percent) to that of the 2012 study in Australia (Szewczyk and Sansurooah, 2012), which found data on 70 percent of the media. This would indicate that, despite the news media exposure of the issue and the advice from a range of sources from governments and the news media to security product vendors, sellers are either not responding to the warnings or disregarding them. While the sellers had, in some cases stated that the media had been formatted or wiped, in other cases they had included a disclaimer saying that there may be data present and that they buyer should remove it. On one day during the research period, a sample of 100 adverts for the sale of second hand micro-sd cards were examined and 12 of the sellers stated that the media had been wiped, 31 claimed that the media had been formatted, 46 made no comment about the state of the media and, shockingly, 11 of the sellers stated that there was data present on the media.

The average cost of the one hundred memory cards obtained was just £5.50 per card. With such a small financial return for selling a memory card, it is possible that the seller perceive them as low value items and do not consider the potential value of any data that they might contain. Recent reports indicates that business cybercrime in the UK has increased by 63% in the last year (Ashford, 2018), whilst at the same time there has been a 15% decrease in fraud and computer misuse in the UK (ONS, 2018).

The UK government promotes good information security and media disposal through a number of resources, including Get Safe Online, (Get safe Online, 2018), the National Cyber Security Centre (NCSC)(2016) and through advice from the Chambers of Commerce and the police. While there is plenty of good advice, it was noticeable that it was not necessarily easy to find it – for example the NCSC guidance is under the heading of ‘Secure sanitisation of storage media’ (NCSC, 2016), which the average end user is unlikely to find. An online search for information on data erasure, however,

produces a wealth of advice from a range of sources (BT, 2018, Business insider, 2018, Computer Weekly, 2018, TunesBro, 2018, Remo Software, 2018, DoYourData, 2018).

Given the short life cycle of current digital devices, in particular with smart phones, users are regularly replacing and upgrading their mobile devices, it is perhaps strange that the service providers and vendors are not making available the advice and tools that would enable users to erase their personal and sensitive data easily. Such advice as there is tends to relate to undertaking a factory reset of the device but ignores the removable media that may have been used.

It is noticeable that in this study, for the first time, memory cards from drones, dashcams and satellite navigation systems have been identified. As the diversity of devices that utilise memory cards increases, so will the diversity of data available and the potential for the exposure of personal information. For example, from the Satellite Navigation system (SatNav), it is possible to determine the home location of the user and also the routes that they regularly use and locations that they have identified as being of interest, which may include their place of work and the homes of family and friends.

RECOMMENDATION

It is recommended that the government, academia, the news media, mobile service providers and the vendors of relevant tools find new and better methods to explain to users the potential risks of failing to erase data from storage media and also to make suitable tools more easily available.

CONCLUSIONS

The level of reported cybercrime in the UK has continued to rise over the last decade with regular news media reports on the latest crimes and trends, for example (Treanor, 2017), reported that fraud in the UK had exceeded £1Bn in value in 2017, and the Office for National Statistics (ONS) produced figures that showed that there had been an estimated 5.6 million instances of fraud and computer misuse in the 12 months running up to June 2016 (ONS, 2016)**.** Given the range and level of publicity with regard to data breaches and the loss of personal information that has regularly been in the news media for more than 10 years it is difficult to understand why so many users still fail to remove the data on the media that they are selling as there is a wide availability of both commercial and free tools that can be used for the destruction of data on media adequately.

It is intended that this research will be repeated on a periodic basis in subsequent years. The problems arising from the disposal of memory cards will only increase as the size of the media and the range of devices that they can be used in continues to grow. As the capacity of the memory cards continues to increase, so does the potential for greater volumes of confidential and sensitive personal data to be exposed

It is evident from this research that the end users of these memory cards are still not well enough informed of the dangers of not ensuring that data has been properly erased when disposing of media that has been used in personal or business devices and that the users do not take the appropriate actions to permanently remove data from the media before they dispose of it.

During the coming year the research team will be conducting three further studies into second hand hard disks, second hand USB storage sticks and mobile devices. Once the full set of studies has been carried out, it will be possible to look at the data remaining on all types of storage media and identify whether there are any significant differences in the data contained.

ACKNOWLEDGEMENTS

The funding for the purchase of the MSD cards was generously provided by Comparitech.com, a company that carries out reviews of technologies.

REFERENCES

Ashford W, (2018), Business cyber crime up 63%, UK stats show, https://www.computerweekly.com/news/252433873/Business-cyber-crime-up-63-UK-stats-show

BT, (2018) Selling your computer? How to wipe your PC with Windows 10, http://home.bt.com/tech-gadgets/computing/windows-10/how-to-wipe-your-pc-with-windows-10-11364002707321

Business Insider, (2018). How To Erase Your Data So No One Can Ever Recover It, http://www.businessinsider.com/how-to-erase-your-data-so-no-one-can-ever-recover-it-2010-3?IR=T

Caloyannides, M. A.: Digital "Evidence" is Often Evidence of Nothing. In Kanellis, P. et al., editors: Digital Crime and Forensic Science. Idea Group Publishing, 2006

Computer Weekly, (2018). How to clear your data off a device, https://www.computerworld.com/article/2505470/data-center/data-center-how-to-clear-your-data-off-a-device.html

DoYourData, (2016), How to Permanently Erase Files from Micro SD Card?, https://www.doyourdata.com/erase-data/erase-files-from-micro-sd-card.html

Get Safe Online, (2018), Safe Computer Disposal https://www.getsafeonline.org/protecting-your-computer/safe-computer-disposal/

Jones A, Mee V, Meyler C, Gooch J (2005), Analysis of Data Recovered from Computer Disks released for sale by organisations. Journal of Information Warfare, 4(2), 45-53.

Jones, Dardick, Davies, Sutherland and Valli, (2008), The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, Http://www.jiclt.com/index.php/jiclt/article/view/80

Jones, Valli, Dardick, Sutherland, Dabibi, Davies, (2009), The 2009 Analysis of Information Remaining on Disks Offered on the Second Hand Market

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

Jones, Angelopoulou, Vidalis & Janicke, (2016), The 2016 Hard Disk Study on Information Available on the Second Hand Market in the UK, 16th European Conference on Cyber Warfare and Security (ECCWS2017).

Luehr, P.H.: Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts. Criminal Justice, 20 2005, Nr. 3, pp. 14–23

NCSC, (2016), Secure sanitisation of storage media, https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

Office of National Statistics, (2018), Overview of fraud and computer misuse statistics for England and Wales, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

Office for National Statistics. (2016) Cyber Security Breaches Survey 2016. [ONLINE] Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables. (Accessed 21 March 2018).

Remo Software, (2018), How To Erase Memory Card, https://www.remosoftware.com/how-to-erase-memory-card

Statista, (2018). Market share held by mobile operating systems in the United Kingdom (UK) from December 2011 to March 2018, https://www.statista.com/statistics/271240/android-market-share-in-the-united-kingdom-uk/

Szewczyk P, Sansurooah K, (2012), The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1109&context=adf (accessed 15 May 2018)

Treanor, J., (2017), UK fraud hits record £1.1bn as cybercrime soars,https://www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg

TunesBro, (2018), How to Permanently Deleted Data from Memory Card, https://www.tunesbro.com/erase-data-from-memory-card.html

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.

TunesBro, (2018), How to Permanently Deleted Data from Memory Card, https://www.tunesbro.com/erase-data-from-memory-card.html