# 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

The University of Hertfordshire has carried out a study into the volume and nature of data found on memory cards (SD, Micro SD)[1] purchased from the second hand market in the UK in 2018. These cards are commonly used in a wide range of consumer multimedia devices, including mobile phones, tablet computers, cameras, satellite navigation (SatNav) systems, dashboard cameras (dashcams), drones and other products. One hundred second hand memory cards were purchased, and their contents analysed to determine the amount and type of data discovered, and whether any attempt had been made to clear the data prior to sale. Sensitive and personal data was found on 65% of the memory cards and while there was evidence of attempts to remove the data in some cases, there were many cases were no attempt at removal had been made.

## INTRODUCTION

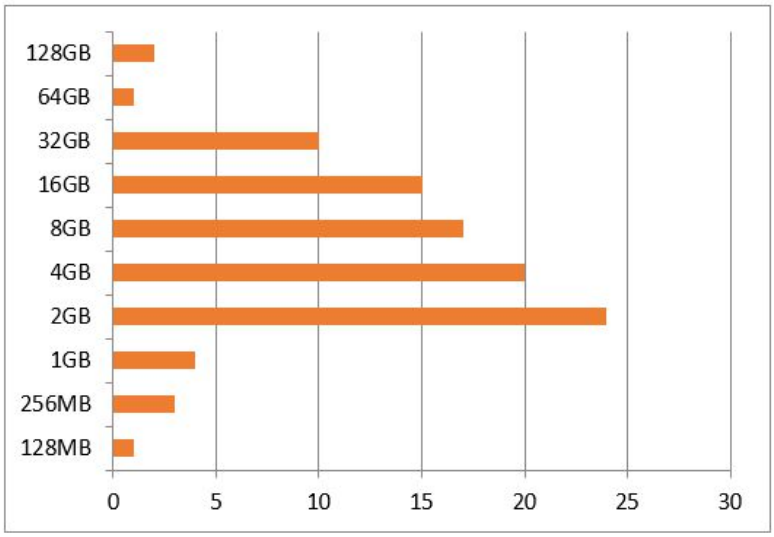
Memory cards, in particular the micro SD card (which has become the industry standard), provide a versatile, small and inexpensive option for data storage. Their convenience has led to their use in a wide range of electronic consumer devices, and the recent availability of large capacity memory cards makes them viable as a backup medium for personal computers. Currently they are providing a highly portable means of keeping sensitive and important data with a user, and a less bulky alternative to external disk drives. At present memory cards are mainly found in smart phones and tablet computers, although research has shown that SatNav

systems, dashcams and drones are using them. While iPhones and iPads lack the slots for memory cards, most other mobile devices produced in recent years do.
As with all storage media sold on the second-hand market, sensitive data can remain and could be misused if a buyer so wished, unless appropriate precautions are taken to erase the data prior to sale. This *remnant data* issue has been the subject of ongoing research for over a decade, and it has been shown that all types of storage medium (hard disks, USB thumb drives, memory cards) sold second hand, are likely to contain confidential or sensitive data. As storage capacity increases, second-hand memory cards are likely to provide a rich source of information, if adequate steps are not taken to remove the data prior to sale. 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 media focus on cybercrime and the security of personal data.

## RESEARCH PROCEDURE

Between January and May 2018, 100 second hand memory cards were purchased from second hand sources, including Ebay, conventional auctions and second hand shops. The memory cards were then processed and analysed. Most of the cards were purchased singly, although on a small number of occasions, the memory cards were purchased in small lots where 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 purchased were all either SD cards or Micro SD cards, as these were the only types on sale during the four month study period, the duration of which served to minimise any distortion in the market. It also sought to avoid alerting potential sellers that a single organisation was purchasing a large number of memory cards.
The storage capacity of the purchased memory cards varied considerably and Table 1 shows the spread of the capacities of the cards purchased. The current maximum capacity (at the time of writing) of memory cards is 512GB.

**Table 1 - Storage capacity of memory cards purchased**




A forensic *image* (a bit-by-bit copy) 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. Analysis was conducted using WinHex 15, and the OSforensics tool Version 5.2.1007, both of which are publicly available and can be downloaded from the internet.

Since the initial study into remnant data on second-hand hard disks study carried out in 2005, there have been innumerable media reports on the issue of data leakage and advice on the care that is needed in ensuring the destruction of data when disposing of storage media. The question remains as to whether it has had any effect.

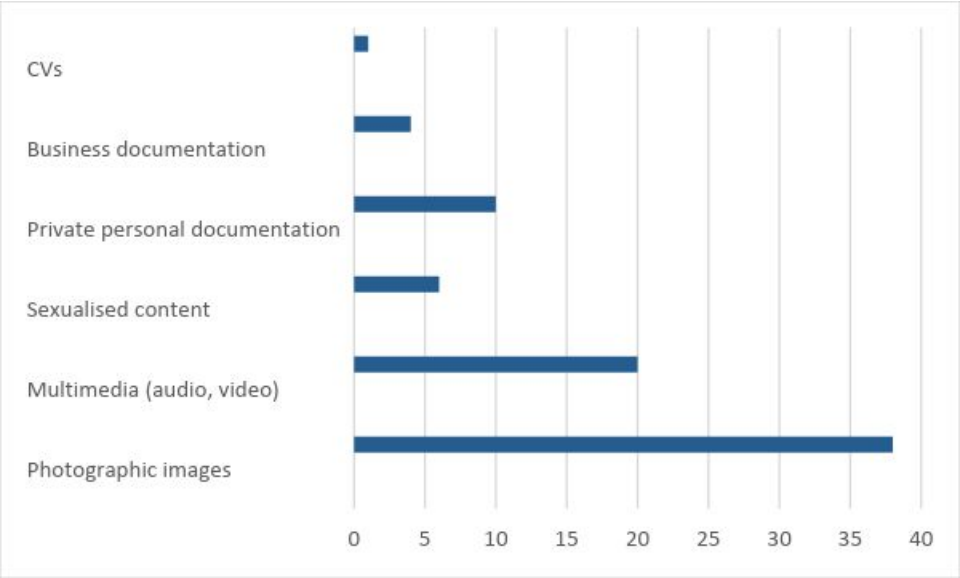
From this research, it appears that users are still not taking appropriate measures to remove data. There may be a number of reasons for this, including the widespread belief that deleting data or carrying out a quick format of the media will actually remove the data.

**REMNANT DATA RESULTS**

Of the 100 memory cards that were purchased, 4 were not accessible and could not be read using the tools cited. These may have been accidentally or deliberately rendered inoperable. Of the remainder: 25 appeared to have been wiped using a data erasing tool (the storage area had been overwritten and all of the data elements were set to 0 or another character) and it would appear that the sellers have taken the appropriate precautions to remove any data; 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.

Overall, data could easily be recovered from 65 percent of the memory cards that were obtained. Table 4 shows the breakdown of the types of information that was found on the memory cards.

**Table 2 – Types of Data Recovered**




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

Notable examples of the type of data recovered from the memory cards is shown below. Overall, the number of cases where the data recovered was sufficient to identify the previous owner directly was relatively low. It is worth remembering however that other information such as image content, metadata and locations can be used to derive personal or sensitive information.

**Cases**

01. A large number of photographs, some of an intimate nature, from a female student at a University in the UK. Also included was a photograph of the owner's passport.
02. A number of photographs (selfies) of the female owner together with an email address, phone number, names and phone numbers of friends.
03. The name of the owner and email addresses, family photographs
04. The name of the owner, home address, phone number, email address, vehicle registration number, credit card pin number from a university student in the UK.

05. Pornography, holiday and hobby photographs, vehicle register number. From the photographs recovered, the owner is male and probably in his late 50s.
06. Navigation files, a large number of pictures for articles to be sold on Ebay, an invoice with the owners name and address, large number of .pdf files
07. Email address of female owner. Large number of family photographs including a number of a man in military uniform, farm photographs, vehicle registration number, name of husband, livestock .pdfs
08. Images and text, young female, photograph of man in RAF uniform, names of the owner and a number of friends, huge number of Selfies, photographs of family, intimate photographs, Instagram, snapchat.
09. Contains vcard contact lists with names and phone numbers, football videos, small number of football photographs
10. Pornography, beach scenes - possible photographs of owner, vehicle registration number, email address, music, some web browsing history.
11. A CV with name and address, phone number and email address, reference to a lapsed security clearance, html documents.
It was clear from the recovered data, that in a number of cases the memory card had come from devices previously owned by pre-teen children.

Despite advice from various governments and media organisations, and the media exposure of the issue, the message about data security risks from remnant data is being ignored. Vendors/sellers are either not responding to the warnings are disregarding them. While the sellers had, in some cases, claimed prior to sale 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.

The average cost of the memory cards obtained was just £5.50 per unit. With such a small financial return for selling a memory card, it would appear that sellers do not appreciate that there is a significant difference between the selling price of the card and the value of any data it may contain.

Recent reports indicates that business cybercrime has increased by 63% in the last year, while at the same time there has been a 15% decrease in fraud and computer misuse in the UK. 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 through the police. While there is plenty of good advice available, it was noticeable that it was not necessarily easy to find – 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, with users regularly replacing and upgrading their mobile devices, it is perhaps an omission that better advice on data disposal tools (factory reset options or encryption) and advice are not issued by the original vendors.

It is noticeable that this study has identified memory cards from drones, dashcams and satellite navigation systems for the first time. As the diversity of devices deploying memory cards increases, so will the diversity of data available and enhance the potential for the exposure of personal information. For example satellite navigation systems (SatNav) data can be used 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.

## 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 regarding the public exposure of personal information that has been the subject of media attention 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 widely availability software (both proprietary and free) that can be used for the secure deletion of data prior to resale.** It is proposed to repeat this study periodically in subsequent years. The problems arising from the disposal of memory cards are likely to increase as the capacity of the cards and the range of devices using them continues to increase. Greater memory storage allows for greater volumes of personal and sensitive data to be exposed.

The diligent removal of data on resold storage media brings a social benefit in that it can, if reduced/eliminated, reduce the opportunity for, and also facilitate convictions in a whole range of computer crimes.

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

## REFERENCES

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

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/

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

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).

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

---

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