2012

The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE

Andy Jones
Edith Cowan University

Thomas Martin
Khalifa University of Science

Mohammed Alzaabi
Khalifa University of Science

DOI: 10.4225/75/57b3b239fb863
Originally published in the Proceedings of the 10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

THE 2012 ANALYSIS OF INFORMATION REMAINING ON COMPUTER HARD DISKS OFFERED FOR SALE ON THE SECOND HAND MARKET IN THE UAE

Andy Jones[1,2,3], Thomas Martin[1], Mohammed Alzaabi[1]
[1]Khalifa University of Science, Technology and Research, Abu Dhabi,UAE
[2] SRI - Security Research Institute, Edith Cowan University, Perth, Western Australia
[3]University of South Australia, Adelaide, South Australia
Andrew.jones@kustar.ac.ae

Abstract

The growth in the use of computers in all aspects of our lives has continued to increase to the point where desktop, laptop, netbook or tablet computers are now almost essential in the way that we communicate and work. As a result of this, and the fact that these devices have a limited lifespan, enormous numbers of computers are being disposed of at the end of their useful life by individuals or/and organisations. As the cost of computing has reduced, the level of 'consumerisation' has increased together with the requirement for mobility. This has led to an increasing use of these devices both in the work environment and for personal data, which has resulted in computers containing high levels of both personal and corporate data. Computers have a relatively short life and are replaced on a regular basis. If not properly cleansed of data when they are released into the public domain they may contain data that is sensitive to the organisation or the individual and which may be relatively up to date. This problem is further exacerbated by the increasing popularity and use of smart phones, which may also contain significant storage capacity. This research describes the first survey of data remaining on computer hard disks sold on the second hand market in the United Arab Emirates (UAE). Similar studies have been carried over the last six years in the United Kingdom, Australia, USA, Germany and France. This research was undertaken to gain insight into the volumes of data found on disks purchased in the UAE compared to other regions of the world and to gain an understanding of the relative level of the problem of residual data in the UAE. The study was carried out by Khalifa University of Science, Technology and Research and was sponsored by Verizon Ltd, a security management and consultancy company.The core methodology of the research that was adopted for the study was the same as has been used for the other studies referred to above. The methodology included the acquisition of a number of second hand computer disks from a range of sources and then analysing them to determine whether any data could be recovered from the disk and if so, whether the data that it contained could be used to determine the previous owner or user. If information was found on the disks and the previous user or owner could be identified, the research examined whether it was of a sensitive nature or in a sufficient volume to represent a risk.

Keywords
Computer forensics, disk analysis, data recovery, data disposal, data destruction, data leakage, privacy.

INTRODUCTION

This research was undertaken to gain an understanding of the level and types of information that remained on computer disks that had been offered for sale on the second hand market in the UAE. The research revealed that, contrary to the results of studies carried out over the last six years in other parts of the world, only a small proportion of the disks that were examined contained significant data. To the best of our knowledge no such similar study has previously been carried out in the region.

The research undertaken was sponsored by Verizon Ltd which funded the purchase of the computer disks. The aim of the research was to determine whether any data remained on second hand computer disks and if it did, the potential sensitivity of the information to the previous owner. The research was conducted under the same conditions that had been used during previous second hand disk and hand held mobile devices studies, carried out by the University of Glamorgan, Edith Cowan University, Longwood University and British Telecommunication, using common and easily available tools that equated to the undelete and unformat commands in older versions of Windows and a hexadecimal editor. The results of the research are that a number of observations can be made with regard to the level and type of information remaining on second hand computer disks and a number of conclusions and recommendations have been made on ways to improve the situation with regard to data remaining on second hand computer disks.

This paper, the report on the first of what is intended to be a series of surveys, contains the results of the 2012 research that was carried out by the Cyber operations Centre of Excellence at Khalifa University in Abu Dhabi in the UAE.

THE RESEARCH

To ensure that the results of the research provide a realistic and scientifically sound view of the situation, 43 second hand computer disks were obtained. All of the computer disks used in the research were purchased on SOUQ.com or in computer or mobile phone shops in four of the Emirates. The computer disks were purchased discretely either singly or in small lots by a number of purchasers. This procedure was adopted in order to minimise the possibility of the sellers becoming aware of the purpose for which the computer disks were being obtained and to ensure that the actions of one seller did not have a disproportionate effect on the results of the study.

The computer disks were supplied 'blind' to the researchers. This means that the research had no indication of the source of the computer disks that they were analysing. The only identifying mark on the computer disks that were provided to the researchers was a unique sequential serial number so that there was no indication of where or how they had been obtained. The research methodology used was the same as that used in the second hand disk study research (Jones et al. 2005, 2006. 2009, 2009a), with each computer disk being forensically imaged using commercially available software (Guidance Encase or Access Data Forensic Tool Kit (FTK)) and then stored in secure storage areas. The analysis was then undertaken on the images of the computer disks that had been created. There were two main reasons for the adoption of this time consuming step. The first was to preserve the original media in its original state and store it in a secure area in case criminal activity was discovered and there was a requirement to pass it on to law enforcement. By adopting this procedure, the chain of custody was preserved for any investigation by law enforcement. This allowed the research to be carried out in a non-intrusive manner that did not affect or change the original data. Also, if any anomalies were detected with the image, it would be possible to validate the data against a second image created from the original.

The tools used in this study to analyse the computer disks were fundamentally the same as those used in previous disk and mobile hand held device studies (although the versions of the tools may have changed). The tools performed similar functions to the Windows unformat and undelete commands and a hexadecimal editor (which can be used to view any information that exists in the unallocated portion of the computer disk). Tools that perform this type of functionality are free and readily available: examples include forensic analysis tools such as Autopsy (Version 2.08) and the Linux based Helix software. Freeware Hexadecimal editors include `XVI32 and ftweak-hex.` These tools can be used effectively without significant levels of skill or knowledge.

The objectives of the research were the same as those defined for the previous disk and hand held mobile device studies: firstly to determine whether the computer disks that were obtained in the UAE had been effectively cleansed of data or whether they still contained information that was either visible or easily recoverable with the tools identified above. The second objective of the research was to identify whether there was information that could be used to identify the organisation or individual(s) that had used the computer disks.

The initial results indicate that the level and type of information found on computer disks in the UAE was much lower than that found in previous studies of other.

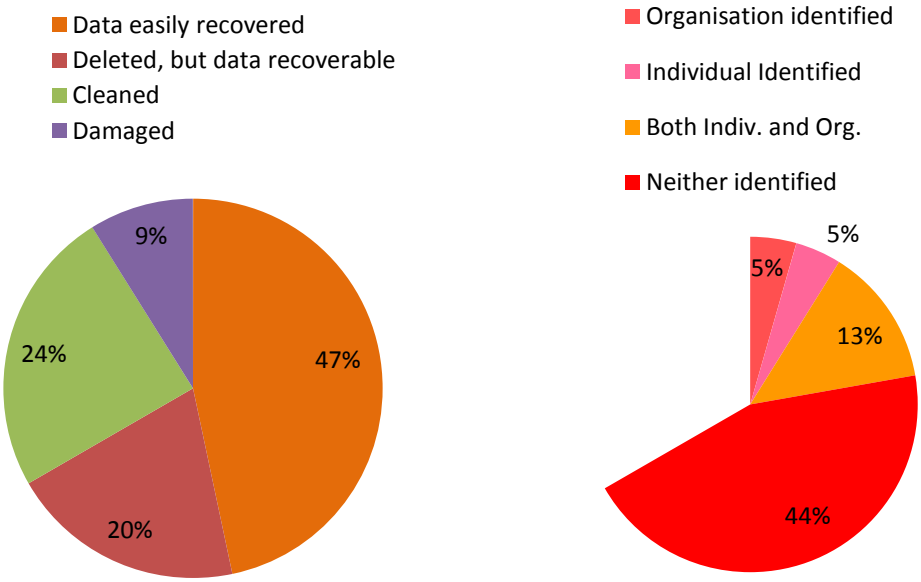
THE RESEARCH RESULTS

This section details the results for the study for the 45 computer disks obtained in the UAE:

- 4 disks (9%) were damaged and as a result, unreadable.
- 11 (24%) had been effectively cleaned and contained no recoverable data
- 9 (20% of the readable computer disks) had been deleted or formatted, but still contained recoverable data.
- 21 (47% of the readable computer disks) contained data that could be easily recovered, 8 (17%) contained sufficient information for the organisation that they had come from to be identified. 8 (17%) contained sufficient information for individuals to be identified.

Figure 1 below shows these results in a graphical format.

Figure 1: Graphical representation of the analysis results



This compares well with the latest (2009) survey results from the other regions (including the USA, UK, Europe and Australia) which is shown in Figure 2 below.

Figure 2: Graphical representation of the analysis results from the 2009 survey carried out in the USA, UK, Europe and Australia (figures for data present are percentages of the number of disks that had not been wiped/faulty)

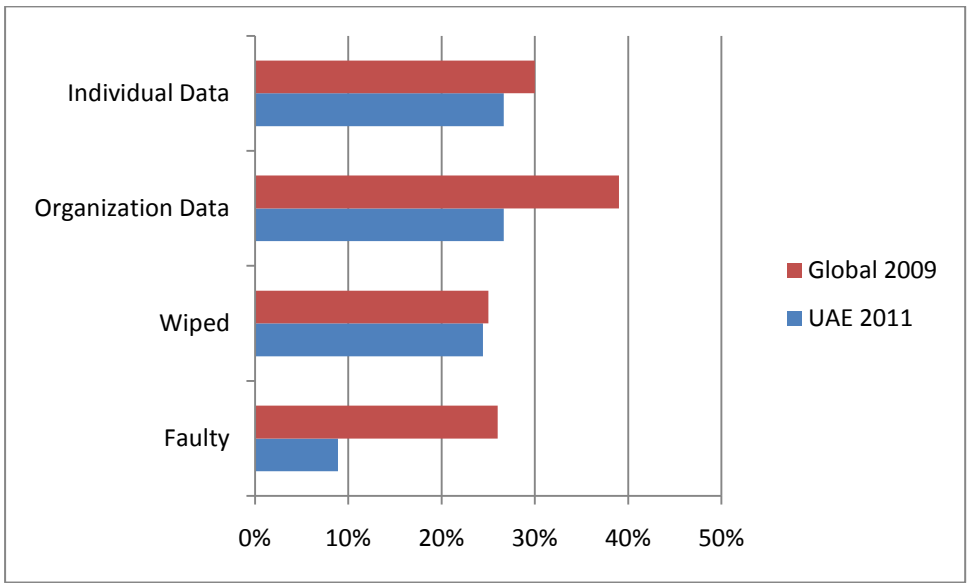
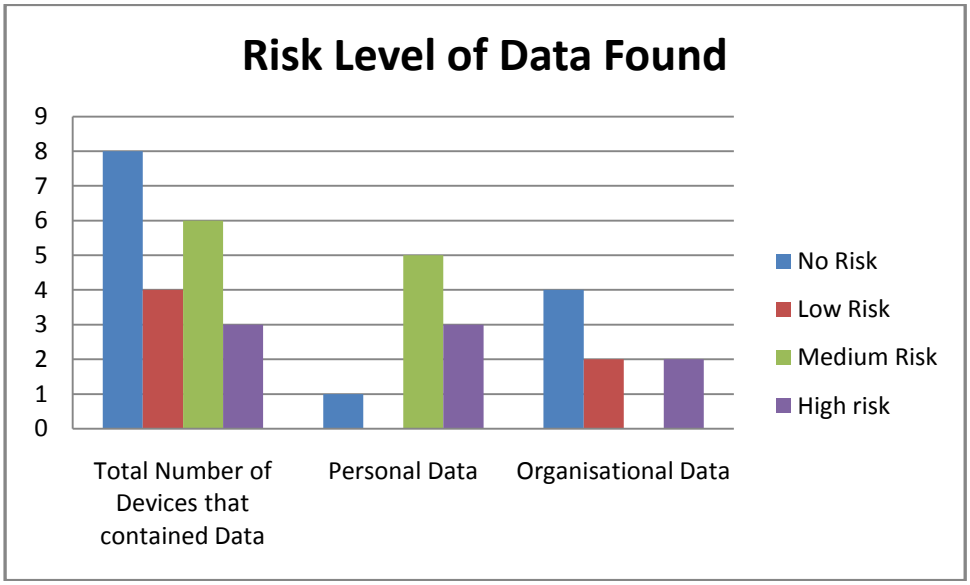


Figure 3 below shows an assessment of the level of risk that the data recovered would pose to the individual or the organisation.

Figure 3: Assessment of level of Risk of the data recovered



This is the first study that has been carried out in the UAE and it is not possible to draw any conclusions on possible trends, however, it is possible to compare the results with those from recent studies in other regions.

A range of types of information were found on the disks that were examined. From the tables above, it can clearly be seen that the volumes of information that were found were significantly lower than has been found in research in other regions. There were also clearly discernible trends in the data that was recovered.

Information that could have a potentially damaging commercial impact or pose a threat to the identity and privacy of the individuals involved was recovered as a result of the analysis. One notable piece of information that was recovered from a number of the disks studied was copies of passports. This may well be a direct result of the requirement to produce copies of passports to obtain access to a range of services in the UAE. An indication of the quantity and type of material that was recovered, originating from commercial and private individuals is detailed below:

- One of the disks contained a full CV for the previous owner written in Arabic.
- One disk contained Bank account Numbers, Passport scans, a possible set of encryption keys and an invoice.
- One disk contained a copy of a passport, visa and family photos taken in Sharjah and Dubai. It also contained a Trading Register Certificate for a Photocopier Warehouse with details of the amount of capital, the address, name and fax no.
- One disk from a well known international consultancy provider based in Dubai contained invoices with account numbers and a phone bill with call details. The disk also contained a shipping manifest of cargo worth AED 287,000. It also contained a letter describing an incident where a reversing vehicle had caused an employee to fall and dislocate his shoulder.
- One disk contained an unsigned letter granting power of attorney, CVs, details of bank transfers and loans, credit card numbers, scanned copies of passports and passport numbers. The disk also contained a government proposal and a letter of recommendation. Also present on the disk were a number of online chat conversations. In one of these, one of the correspondents asking for a naked photo of the other. Other chat sessions talked about "snaps go to the police" and "letters which i wrote to u b4 our marriage reached to my boss".
- Another disk contained a CV, a number of interviews that seem to be part of study on the "Impact of Globalisation upon the Definition of Ethics in UAE" and to find out the 'Reasons behind the Changing Ethical Standards in (UAE) with a focus upon Socio Economic influence of Globalization". One interview of a family in Abu Dhabi has details of finances, health, children's education and well being, and other details of the family and extended family. Another interview had an extensive list of a family's health problems (high blood pressure, TB, Hepatitis E, circulation problems). The disk also contained permission note for parents (including the parents home and mobile numbers), a User name and password for an airline frequent flyer programme. Interestingly, one completed survey form by the

owner of the disk has a disclaimer at the bottom "The information provided through this survey form will be kept confidential and the detail will not be circulated to any other surveying institution."

One interesting finding of the research was the number of disks that had apparently come from gaming computers with a total of 6 readable disks that had a large number of games loaded but little other information.

Technology, for the most part, has kept pace with the need to protect information to an appropriate level while it is in use and to destroy it effectively when it is no longer required. The observed failures from commercial organisations seem to be a result of a lack of corporate policies and procedures for the protection and subsequent disposal of obsolete computer disks or a failure to effectively implement these policies where they do exist. For private users, the cause is more likely to be a lack of awareness of the risk arising from failing to erase such information. Equally, they may not be aware of the availability of the tools and techniques to ensure that data is properly erased when it is no longer required.

The subject of the effective erasure of data was first highlighted in a 1996 conference paper (Gutmann 1996) that reported research on the secure deletion of data. A second paper (Gutmann 2001) examined 'Data Remanence in Semiconductor Devices' and a further paper (Garfinkel and Shelat 2003) looked at the measures that could be taken to 'sanitize' computer disks. In the period since the issue was first raised there has been an ongoing series of news reports on high profile cases where personal or organisational information has been found in the public domain. There has also been increasing publicity and awareness of the issue of identity theft and the guidance on how to protect both personal and organisational information.

There are now a good range of tools that can be used to effectively erase data from computer disks. However there appears to be an ongoing issue with making the users aware of the problem. With the ever increasing levels of theft of both corporate and personal information that are being reported (Bickle 2012), (Fox News 2012), (Constantin 2012), (Markoff and Barboza 2012) and the availability of suitable tools to erase data, it is difficult to explain the amount of information that has been found in this survey. It is clear that further investigation needs to be carried out to understand the underlying cause.

For those computer disks that were for personal use, the results indicate that there is an issue with awareness and education of the users as to what information is sensitive and how they can ensure that it is destroyed. For the most part the disks are used to store music, photographs and other, often small items of information that the user will not necessarily consider to be significant. The items of information that were consistently found on the disks that are considered to be of high risk were copies of passports, visas and bank account details.

For the disks that contained commercial information, there was a range of information on the companies' operations and customers. This would be embarrassing and potentially damaging to the business if the knowledge that they had released it into the public domain became known.

CONCLUSIONS

The issue of the use and subsequent disposal of computer hard disks is a significant problem, and is bound to grow as identity theft becomes more prevalent.. The results of the survey in the UAE show that the volume and type of information that was found are significantly less than those found in studies in other regions, with more disks having had the data effectively erased beyond easy recovery. However, because of local customs and requirements, where personal information was recovered it was potentially highly damaging. The results of this first survey to be carried out in the UAE compare very favourably with the results of previous studies in other regions.

A number of the disks examined were found to contain sensitive corporate or personal information and the consequence of failing to remove or erase this data is that it continues to be available to anyone that might seek to exploit it. There is ongoing clear requirement that staff within organisations be given the appropriate awareness, education and training programmes. They need to be able to ensure that computer disks and other media is properly managed and that the data that they contain is protected properly while in use and then erased before the disks are disposed of. For the disks from personal computers, there is a need for the owner to be educated with regard to the potential risks caused by the information and the steps that they can take to effectively erase the data when they dispose of the computer.

RECOMMENDATIONS

There are a number of measures that can be taken by both individuals and organisations to reduce the volume of sensitive information that is inadvertently given away when they dispose of computer disks. These include:

1. **Education -** A public awareness campaign by Government, the media, commerce and/or academia.
2. **Risk Assessment –** The organisation carries out risk assessments to determine sensitivity of the information that may be stored on the computer disks that are being disposed of.
3. **Roles and Responsibilities –** The assigning of the roles and responsibilities to those individuals responsible for issuing, managing and disposing of computer disks.
4. **Best Practices -** The introduction of procedures within organisations to ensure that computer disks are disposed of in an appropriate manner.
5. **Physical Destruction -** Where appropriate, the physical destruction of the computer disks.
6. **Encryption -** The encryption of the computer disks to ensure that information cannot be easily recovered in the event of their loss, theft or disposal.
7. **Data Erasure –** Provide access to the tools and facilities to enable individuals to effectively remove the information from their computer disks

Authors

Dr. Andy Jones is currently the Program Chair for the M.Sc. in Information Security at Khalifa University in Abu Dhabi in the UAE. Prior to this he was Head of Security Technology Research at the Security Research Centre at British Telecommunications (BT) where he led the research into the risk management methods, anomaly detection and computer forensics. He holds a post as an adjunct professor at Edith Cowan University in Australia, where significant research is being carried out into wireless networking, RFID vulnerabilities and computer and mobile device forensics and also as an adjunct professor at the University of South Australia.

Dr Thomas Martin is currently a lecturer for the M.Sc. in Information Security at Khalifa University in Abu Dhabi in the UAE. He has such courses as Introduction to Cryptography, Computer & Network Security and Identity Management. His research interests include: Cryptography, Multi-party communications, Digital Rights Management, Identity Management, Penetration Testing, Risk Assessment and Computer Forensics. Before joining Khalifa University, he worked as a researcher at BT, developing several security related patents, as well as participating in such projects as the EU FP7 MASTER Project (Managing Assurance, Security and Trust for sERvices).

Eng. Mohammed Alzaabi is a PhD Candidate in the Computer Engineering Department at Khalifa University of Science, Technology, and Research. He obtained his MS degree in information security from Khalifa University in 2010. He obtained his BS degree in computer engineering from the same university in 2009. Eng. Alzaabi primary research interests include Digital Forensics, Network Security, and Cloud Computing.

REFERENCES

Bickle M, *MasterCard and Visa Data Theft Brings Concern to a Wide Profile of Card Holders*, http://www.forbes.com/sites/prospernow/2012/04/02/mastercard-and-visa-data-theft-brings-concern-to-a-wide-profile-of-card-holders/, (accessed 04 Jul 2012)

Fox News, *Hackers steal hundreds of thousands of Social Security numbers*, http://www.foxnews.com/tech/2012/04/10/hackers-steal-hundreds-thousands-social-security-numbers/#ixzz1zdGcK4NI (accessed 04 Jul 2012)

Constantin, L., *Researchers Identify Stuxnet-like Cyberespionage Malware Called 'Flame'* http://www.pcworld.com/article/256370/researchers_identify_stuxnetlike_cyberespionage_malware_called_flame.html (accessed 04 Jul 2012)

Garfinkel, S., and Shelat, A., "*Remembrance of Data Passed: A Study of Disk Sanitization Practices*," IEEE Security and Privacy, January/February 2003, http://faculty.ksu.edu.sa/meshekah/CSC429%20Slides/disksanit.pdf (accessed 02 Jul 2012)

Guttman, P,. *Secure Deletion of Data from Magnetic and Solid-State Memory*, Sixth USENIX Security Symposium Proceedings, San Jose, California, 1996, http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (accessed 01 Jul 2012)

Guttman, P,. *Data Remanence in Semiconductor Devices*, Usenix Security 2001 paper, http://static.usenix.org/events/sec01/full_papers/gutmann/gutmann.pdf / (accessed 01 Jul 2012)

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

Jones, A., Valli, C., Sutherland, I., and Thomas, P,(2006), *The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market*, Journal of Digital Forensics, Security and Law, (2006) 1(3), 23-36.

Jones, A., Valli, C., Sutherland, I., and Dardick, G., (2008), *The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market,* International Journal of Liability and Scientific Enquiry 2009 - Vol. 2, No.1 pp. 53 – 68.

Jones, A., Valli, C., Sutherland, I., Dardick, G. Davies G,, *The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market*, Journal of International Commercial Law and Technology, Vol. 4, No 3 (2009a)

Markoff J., Barboza D., *Researchers Trace Data Theft to Intruders in China* http://www.nytimes.com/2010/04/06/science/06cyber.html?_r=1&pagewanted=all