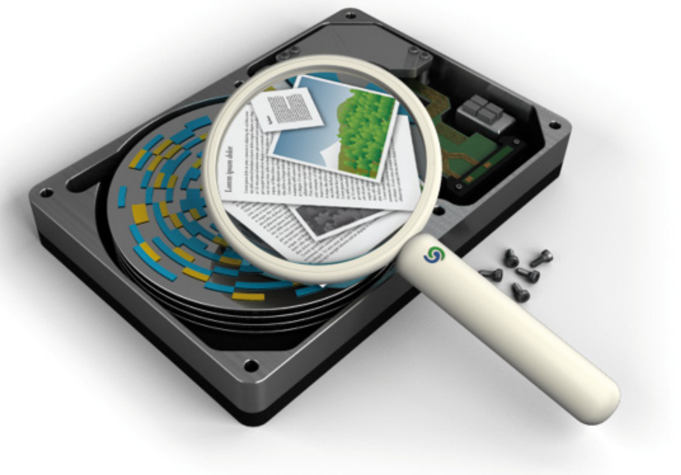
Data Protection on Used Hard Disks

Data Data Everywhere



Dipl.-Inform. Olaf Kehrer • O&O Software GmbH, Berlin • September 2007

Study on data protection and security on used hard drives and memory cards in Germany and the USA

When files are deleted, it doesn't mean that data are gone. That this simple fact is not known to many users of computer systems and digital cameras has once again lead to alarming results in this year's study. On virtually all of the hard drives purchased using online auctions, recovered personal and company data were found that should never have seen the light of day. Two-thirds of the storage media still contained the data of their predecessor although almost all of those former owners were convinced their data had been deleted. Barely any of them were aware that deletion of data in Windows or on a digital camera is not a permanent matter. Beyond presenting its research results, this study sheds light on the probable causes and background information regarding this very serious IT data security issue. Extensive solutions are also presented for preventing this dangerous and invisible form of data transmission.

The release of Windows Vista brought with it a new set of hardware requirements for computers. Many PC users were required to upgrade their hardware or even purchase a new computer. However, what happens to the old computer? Private users will generally sell or give away their old computers. Companies, on the other hand, choose to decommission their old IT equipment and return it back to their Leasing provider or dispose of it themselves. However, did you know that the data on insecurely deleted hard disks can be easily recovered with just a few clicks of the mouse? Unbeknownst to their owners, private and company data can change hands very easily, potentially causing tremendous damages.

As part of our research for this study, almost 400 hard disk drives were purchased via online auctions in 2006 and 2007. Each of the these storage volumes werethoroughly analyzed to see if they still contained data or had already been securely deleted. More than 66 % of the hard drives had not been deleted, making the previous owner's data easily accessible using specialized data recovery software.

In the Internet age, security is a Number One issue. Reports of attacks on Online Banking accounts through Phishing schemes seem commonplace. Even traditional media sources, such as newspapers, now warn about new and quickly spreading E-mail viruses, which have contributed to an overall increased awareness among computer users. Moreover, the collection and mining of user data by so-calledSpyware are receiving more and more attention on the part of the public and criminal authorities.

However, what happens to the private and company data, when a computer is no longer in use, sold or given away? More users are simply not conscious of the fact that, without taking the appropriate preventative measures, potentially damaging information can easily be transferred into unknown hands.

Study

For this study, a total of 395 data storage volumes were purchased by online auction over a course of 18 months and analyzed. Out of those 395 hard drives, 80 originated from the United States, allowing for an international comparison.

In total, the purchased hard disks had a combined capacity of more than 15 Terabytes (15,116 GB). Out of the 280 hard disks, 59 were defective, about 21 % of the total test group. These defective hard disks were excluded from testing, as repairs would have meant a larger than acceptable use of resources. A normal PC user would generally have only limited access to such repairs, making their inclusion in the study irrelevant.

After the discovery of countless digital photos from private users, the analysis of would-be deleted data was expanded to include 115 memory cards,USB Sticks and digital cameras. The data on these storage media were astoundingly intact and easily included into the analysis results.

Results
Of the 221 hard disks, 72 had been securely deleted, prohibiting the reconstruction of data on those volumes. This is about 33 % of the functioning hard disks. The rest of the 149 hard disks either had not been deleted at all or had received a simple formatting before being released for auction.

This means that 67 % of the hard disks contained personal or company data that could be reconstructed. In total, 17 million files with a total size of 2.4 Terabytes were recovered from those drives. These files included a large number of Word documents and Excel spreadsheets as well as 60 complete E-mail mailboxes of previous hard disk owners. Additionally, a number of private photos and videos were found, some of which contained pornographic material.

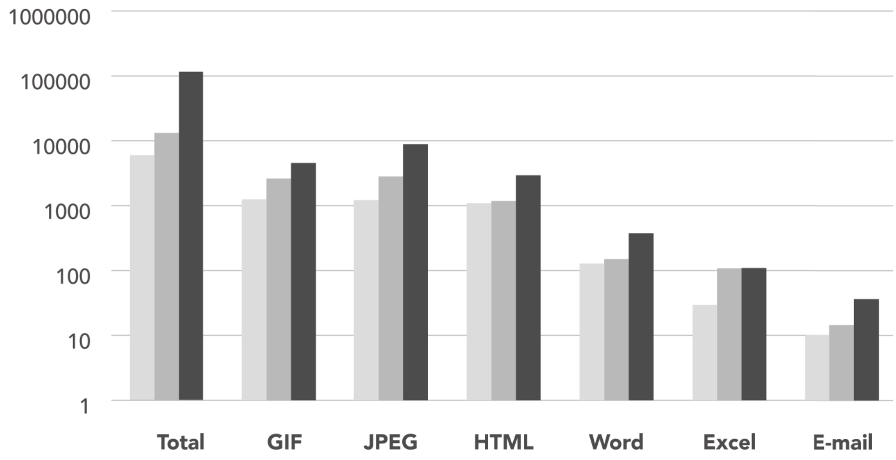
Of the 115 memory cards, USB sticks and digital cameras, 32 were securely deleted, about 27.8 % of those these volumes. On the remaining 83 storage media, or 72.2 %, data could be recovered.

Figure 1: Found Files per Hard Disk

In total, over 17 million files could be restored (2005: 3,3 million, 2004: 590,000). As in previous studies, a large part of these files were images or websites (GIF, JPEG, HTML).

The graph at right shows the average number of found files per storage volume. This average was calculated by dividing the totals for all volumes by the number of functional hard disks.

The Y-axis of the graph is scaled logarithmically.



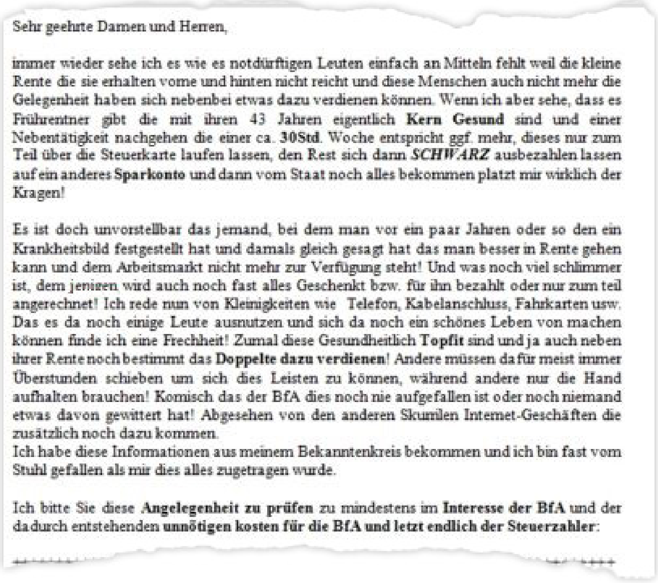
	Total	GIF	JPEG	HTML	Word	Excel	E-mail
Results 2004 □	7867	1988	1889	1047	204	53	17
Results 2005 ▨	29511	3166	3179	1577	354	130	21
Results 2007 ■	114108	6409	9778	4604	581	135	66

Selected Reconstructed Data

Out of the staggering number of reconstructed personal and company data, a selected few cases are presented below. It can be assumed that in all of the below cases, data were either extremely personal or strictly confidential. It is also safe to assume that the original owner of these data would not have liked to see them released to the public.

Tattle Tale, Tattle Tale …

The first case is a hard drive that contained diverse personal documents. Included in these documents was a letter addressed to the German Association of Retirees. In this letter the sender accused an early retiree of working illegally. As one would expect, the accused's complete address and birthday were provided in the letter to aid in the authorities search. It is easy to assume that neither the sender, nor the accused would have wished to be made public.



Sehr geehrte Damen und Herren,

immer wieder sehe ich es wie es notdürftigen Leuten einfach an Mitteln fehlt weil die kleine Rente die sie erhalten vorne und hinten nicht reicht und diese Menschen auch nicht mehr die Gelegenheit haben sich nebenbei etwas dazu verdienen können. Wenn ich aber sehe, dass es Frührentner gibt die mit ihren 43 Jahren eigentlich **Kern Gesund** sind und einer Nebentätigkeit nachgehen die einer ca. **30Std**. Woche entspricht ggf. mehr, dieses nur zum Teil über die Steuerkarte laufen lassen, den Rest sich dann ***SCHWARZ*** ausbezahlen lassen auf ein anderes **Sparkonto** und dann vom Staat noch alles bekommen platzt mir wirklich der Kragen!

Es ist doch unvorstellbar das jemand, bei dem man vor ein paar Jahren oder so den ein Krankheitsbild festgestellt hat und damals gleich gesagt hat das man besser in Rente gehen kann und dem Arbeitsmarkt nicht mehr zur Verfügung steht! Und was noch viel schlimmer ist, dem jenigen wird auch noch fast alles Geschenkt bzw. für ihn bezahlt oder nur zum teil angerechnet! Ich rede nun von Kleinigkeiten wie Telefon, Kabelanschluss, Fahrkarten usw. Das es da noch einige Leute ausnutzen und sich da noch ein schönes Leben von machen können finde ich eine Frechheit! Zumal diese Gesundheitlich **Topfit** sind und ja auch neben ihrer Rente noch bestimmt das **Doppelte dazu verdienen**! Andere müssen da für meist immer Überstunden schieben um sich dies Leisten zu können, während andere nur die Hand aufhalten brauchen! Komisch das der BfA dies noch nie aufgefallen ist oder noch niemand etwas davon gewittert hat! Abgesehen von den anderen Skurilen Internet-Geschäften die zusätzlich noch dazu kommen.
Ich habe diese Informationen aus meinem Bekanntenkreis bekommen und ich bin fast vom Stuhl gefallen als mir dies alles zugetragen wurde.

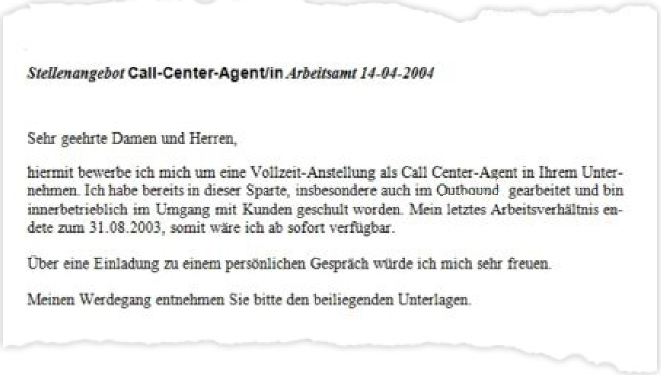
Ich bitte Sie diese **Angelegenheit zu prüfen** zu mindestens im **Interesse der BfA** und der dadurch entstehenden **unnötigen kosten für die BfA und letzt endlich der Steuerzahler**:

Figure 2: Letter to the German Association of Retirees with an accusation of illegal employment (Storage Medium: Hard Disk)

This „Tattle Tale's" hard disk also included a copy of a job application, providing yet another example of data he would surely not like to see released.

Please submit your applications!

Applying for a job usually is associated with the submission of a number of application documents. These days, most job applications are created on a PC, allowing applicants to make a professional impression on potential employers and to reuse and expand on an application for other job prospects. However, these advantages can go awry when an job application's data are saved on a hard drive that is passed on to others without taking the proper precautions.



Stellenangebot **Call-Center-Agent/in** *Arbeitsamt 14-04-2004*

Sehr geehrte Damen und Herren,

hiermit bewerbe ich mich um eine Vollzeit-Anstellung als Call Center-Agent in Ihrem Unternehmen. Ich habe bereits in dieser Sparte, insbesondere auch im Outbound gearbeitet und bin innerbetrieblich im Umgang mit Kunden geschult worden. Mein letztes Arbeitsverhältnis endete zum 31.08.2003, somit wäre ich ab sofort verfügbar.

Über eine Einladung zu einem persönlichen Gespräch würde ich mich sehr freuen.

Meinen Werdegang entnehmen Sie bitte den beiliegenden Unterlagen.

Figure 3: Excerpt from a job application (Storage Medium: Hard Disk)

Data of this kind could be readily recovered from the analyzed media, out of which three cases are described here. The first case is a CV for a 27-year-old German woman, revealing that in 1996 she completed her secondary school degree. Her father is noted here as „unknown".

Another interesting case came from the 32-year-old Telecommunications and Media Design consultant, who likes to spend her free time with her creative design pursuits, water colors and theater activities. It is also states that she is single and has no children.

And then there is the 24-year-old mechanic from eastern Germany. In his application he states that he has not yet completed his military service and has been unemployed for the last two years.

All of the private and personal information mentioned above could be extracted from the hard disks without much effort. It is assumed that the release of this information happened unbeknownst to the persons mentioned. Most likely, these people would have never simply disposed of their job applications in a bin easily reachable by a neighbor's nosey intentions. In the case of a hard disk, such questionable intentions can be even more fruitful.

Private Practices

The analysis of another hard disk produced shocking results. Aside from the personal data of the hard disk's previous owner, the entire E-mail mailbox was reconstructed revealing a multitude of private E-mail correspondences. These included order confirmation from a shop specializing in rubber fetish attire. In addition, contacts to other fetish enthusiasts were also easily found. Here is a short excerpt from an E-mail containing apparent feedback regarding a vacation rental and its tolerance for guests looking to partake in S&M-like activities:

Photos were also found on the hard disk. One photo appears to show a woman posing in her rubber outfit. In another photo, the normally-clad user is posing with his traditional clubhouse comrades. It is easy to image how unfortunate it might be if his colleagues at the clubhouse found out about his vacation activities...

Hallo ihr zwei

Wir sind Rubberpaar H. & H.

Wenn ihr mal wieder die Zeit habt, 3-4 Wochen am Stück fahren zu können, werden auch wir wieder dort hin fahren. Unsere Zeit dort haben wir sehr genossen und wo hat man schon die Möglichkeit seinen Sklaven ganz in Gummi und Kettenfesseln zu halten. Bei uns in der Mietwohnung ging es nicht, das klirren der Ketten wäre zu laut. Ausserdem ist ein schwimmen in Gummi oder bei ihm sogar in einem aufblasbaren Anzug, in unseren Hallenbädern auch nicht möglich.

Gruß H.

Ps.: Wenn ihr noch Fragen habt, Mailt uns einfach noch mal an

Figure 5: E-mail Excerpt (Storage Medium: Hard Disk

The listing of private, personal and company data could go on forever. Perhaps more useful, however, is the recognition of the fact that negligence regarding the data on storage media, such as those listed above, increases the risk of data misuse and theft. Firewall and Anti-virus programs are of little use in such cases. Data are served up on on a silver platter, inviting even the least curious to misuse them

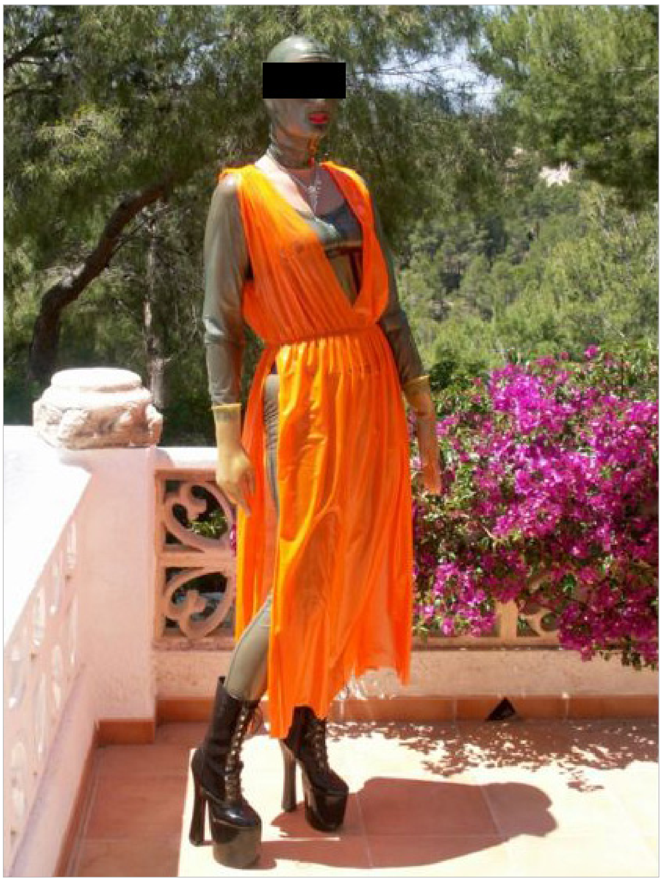

[redacted]

Figure 4: Fetish Vacation Photo (Storage Medium: Hard Disk)

Focus on the USA

For the first time for this study, hard disks originating from the United States were included in the analysis. In January 2003, two researchers at the Massachusetts Institute of Technology published a similar study, in which hard disks were purchased via online auctions on eBay and analyzed for recoverable data. The results of this study show that most of the hard disks still contained data, from private data to bank machine information on customer activities.[1] Have things significantly changed in the years since this study's release. The goal was to find out exactly how critical this issue was in the world's largest IT market. Surprisingly, the results turned out to be similar to those gathered in other countries. Of the 80 hard disks purchased from the USA, 68 drives were intact. The 12 defective hard disks were not included in the study, representing 17.6 % of those original hard disks. On 31 of the intact hard drives, data could be reconstructed. This is „only" about 45 % of those functioning drives, still a high quota considering that the testing pool consisted of only 68 storage volumes.

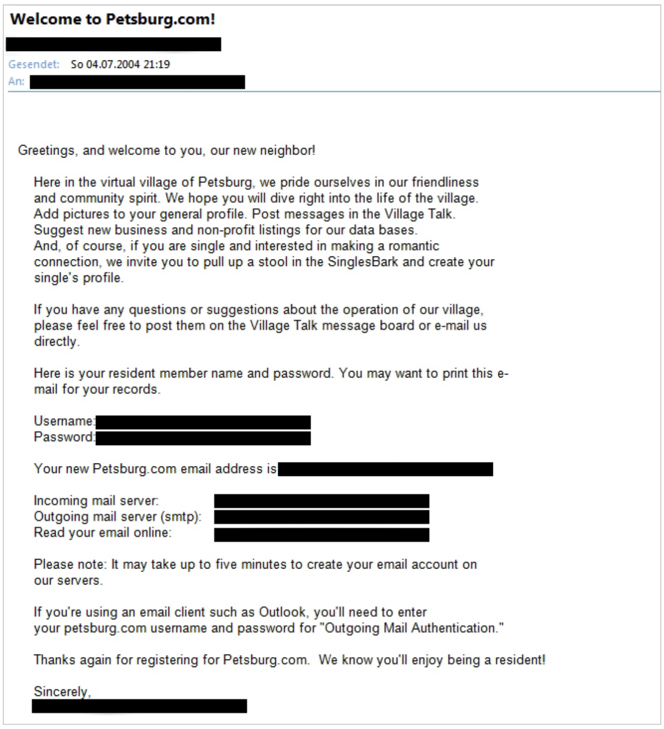
As before, the U.S. hard drives produced some staggering results. Next to the very personal information that was recovered, a large number of military-related data were found.

E-mails

In addition to personal E-mails, the scanned storage media produced company E-mail data as well. In particular the discovery of E-mail account information can allow unauthorized access to not only read E-mails in the account but also to send from it as well. Such abuse lends itself nicely to the production of Spam and, in the worst case, more criminal activities (e.g. „Phishing"). What is worse, the burden of proof in such cases lies with the E-mail account owner, who is generally unaware of the illegal activity until it is too late and the authorities are on the case.

Application Materials from a Laboratory

An E-mail archive was found containing a series of applications addressed for a laboratory specializing in renewable energy in Colorado. All documents are present and include an evaluation in the form of an Excel Spreadsheet sorted by name or evaluation points. Such a group of documents would surely be of interest to any of the applicants involved in the process.



Welcome to Petsburg.com!

[redacted]

Gesendet: So 04.07.2004 21:19
An: [redacted]

Greetings, and welcome to you, our new neighbor!

Here in the virtual village of Petsburg, we pride ourselves in our friendliness and community spirit. We hope you will dive right into the life of the village.
Add pictures to your general profile. Post messages in the Village Talk.
Suggest new business and non-profit listings for our data bases.
And, of course, if you are single and interested in making a romantic connection, we invite you to pull up a stool in the SinglesBark and create your single's profile.

If you have any questions or suggestions about the operation of our village, please feel free to post them on the Village Talk message board or e-mail us directly.

Here is your resident member name and password. You may want to print this e-mail for your records.

Username: [redacted]
Password: [redacted]

Your new Petsburg.com email address is [redacted]

Incoming mail server: [redacted]
Outgoing mail server (smtp): [redacted]
Read your email online: [redacted]

Please note: It may take up to five minutes to create your email account on our servers.

If you're using an email client such as Outlook, you'll need to enter your petsburg.com username and password for "Outgoing Mail Authentication."

Thanks again for registering for Petsburg.com. We know you'll enjoy being a resident!

Sincerely,
[redacted]

Figure 6: Access Information for an E-mail mailbox
(Storage Medium: Hard Disk)

Pictures from Iraq

Many U.S. military personal utilize E-mail and the Internet to stay in contact with loved ones back home. It would make sense then that photos also get sent over the Internet. On a number of hard disks, many such photos could be reconstructed. This is especially surprising considering the relatively small number of hard disks originating from the USA in the testing pool. On the other hand, considering the large number of US soldiers in Iraq and the number of Americans at home associated with them, it is definitely a statistically significant group.

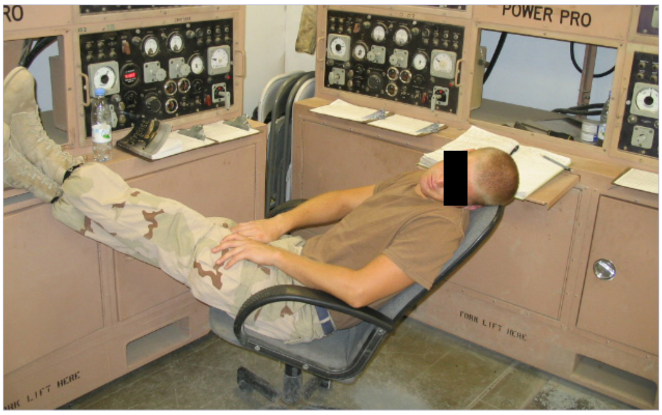


Figure 7: On Break in Iraq (Storage Medium: Hard Disk)

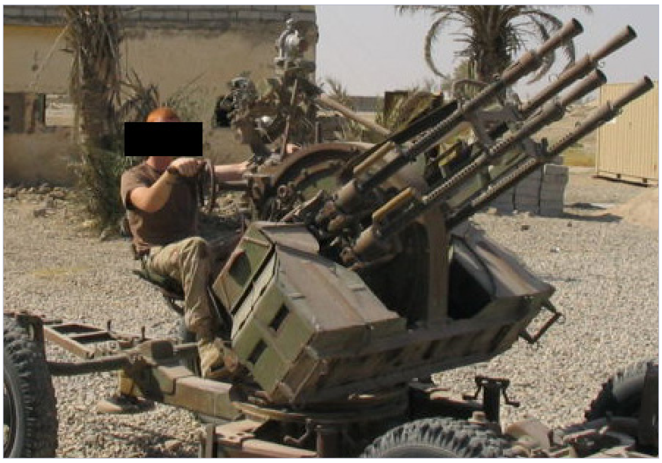


Figure 8: US soldier posing (Storage Medium: Hard Disk)

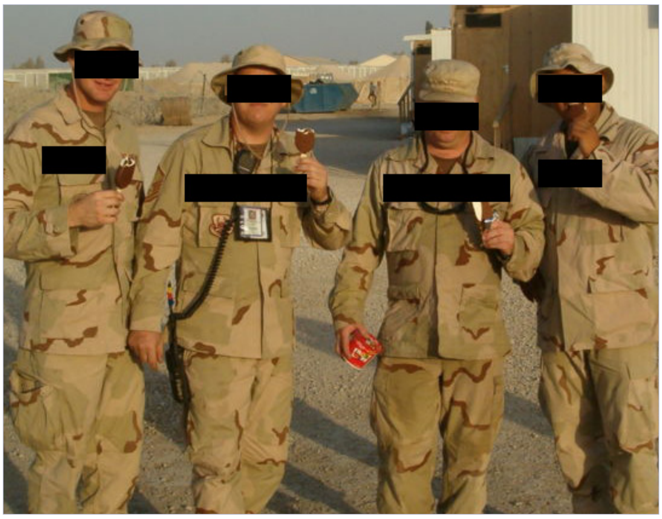


Figure 9: Free time in Iraq (Storage Medium: Hard Disk)

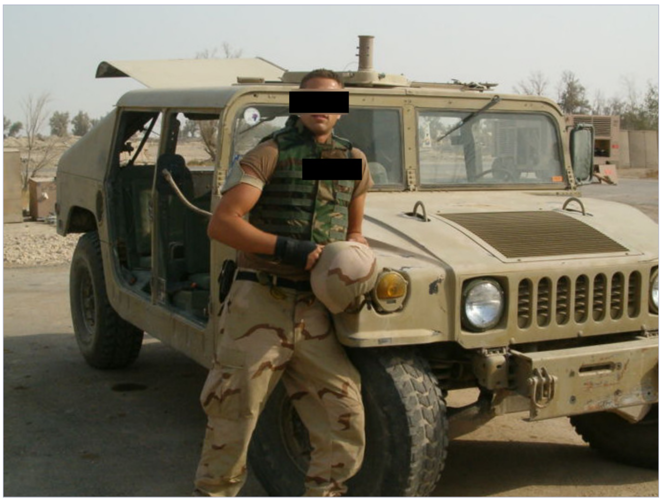
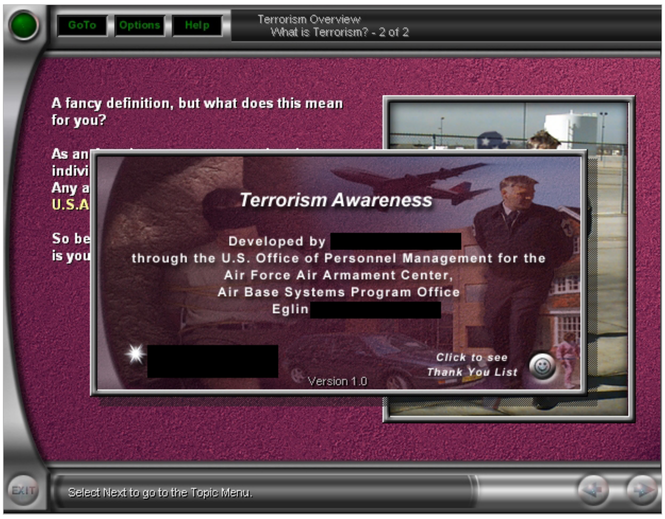


Figure 10: US soldier and Jeep (Storage Medium: Hard Disk)

US Air Force Anti-Terror Videos and Web Access Data
Videos were also found that were specially developed for the US Air Force, depicting their Anti-Terror training. There is no doubt that this information was not meant for public viewing.

In addition, access data were found for accessing a protected website of the US Air Force most likely containing sensitive information. This analysis did not verify the validity of this access information, as that would be a criminal offense. It is, however, troubling to learn that such information could be so easily attained. For some this find might be an „ace in the hole". Despite only purchasing 80 hard disks from the USA, the thought that they could produce so much in terms of personal, company-related and military secrets is staggering.



Terrorism Overview
What is Terrorism? - 2 of 2

A fancy definition, but what does this mean for you?

As an
indivi
Any a
U.S.A

So be
is you

Terrorism Awareness

Developed by [redacted]
through the U.S. Office of Personnel Management for the
Air Force Air Armament Center,
Air Base Systems Program Office
Eglin [redacted]

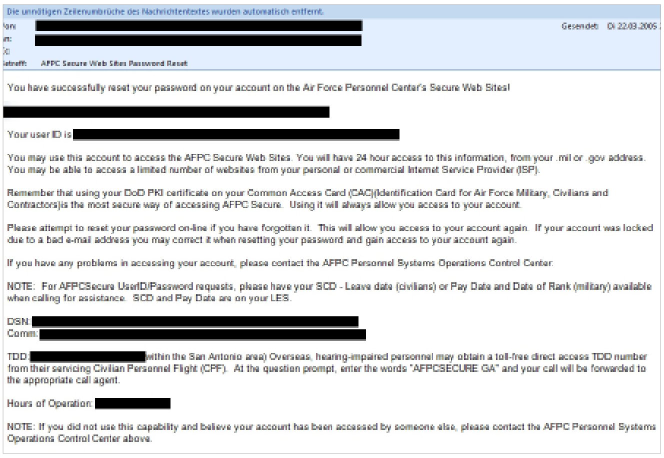
[redacted]

Version 1.0

Click to see
Thank You List

Select Next to go to the Topic Menu.

Figure 11: Training Video for the Anti-Terror Measures
(Storage Medium: Hard Disk)



Die unnötigen Zeilenumbrüche des Nachrichtentextes wurden automatisch entfernt.

on: [redacted]
n: [redacted]
c:
etreff: AFPC Secure Web Sites Password Reset

Gesendet: Di 22.03.2005

You have successfully reset your password on your account on the Air Force Personnel Center's Secure Web Sites!

[redacted]

Your user ID is [redacted]

You may use this account to access the AFPC Secure Web Sites. You will have 24 hour access to this information, from your .mil or .gov address. You may be able to access a limited number of websites from your personal or commercial Internet Service Provider (ISP).

Remember that using your DoD PKI certificate on your Common Access Card (CAC)(Identification Card for Air Force Military, Civilians and Contractors)is the most secure way of accessing AFPC Secure. Using it will always allow you access to your account.

Please attempt to reset your password on-line if you have forgotten it. This will allow you access to your account again. If your account was locked due to a bad e-mail address you may correct it when resetting your password and gain access to your account again.

If you have any problems in accessing your account, please contact the AFPC Personnel Systems Operations Control Center.

NOTE: For AFPCSecure UserID/Password requests, please have your SCD - Leave date (civilians) or Pay Date and Date of Rank (military) available when calling for assistance. SCD and Pay Date are on your LES.

DSN: [redacted]
Comm: [redacted]

TDD: [redacted] within the San Antonio area) Overseas, hearing-impaired personnel may obtain a toll-free direct access TDD number from their servicing Civilian Personnel Flight (CPF). At the question prompt, enter the words "AFPCSECURE GA" and your call will be forwarded to the appropriate call agent.

Hours of Operation: [redacted]

NOTE: If you did not use this capability and believe your account has been accessed by someone else, please contact the AFPC Personnel Systems Operations Control Center above.

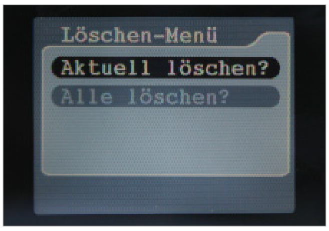
Figure 12: Access Information for a US Military Website
(Storage Medium: Hard Disk)

Digital Photography and USB Sticks

Memory Cards for Digital Cameras

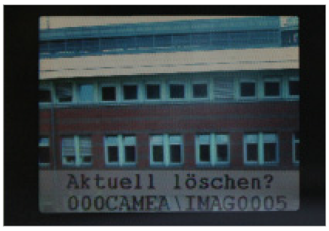
Digital cameras have now replaced traditional cameras. These days, more and more people are taking photos digitally, which means that the rate at which people save those photos for safe keeping has also grown. It has already been shown just how many of the photos could be easily found on used hard disks. For this reason, the scope of this study was expanded, to ascertain how many photos could be recovered from the memory cards used in the cameras themselves.

Today's digital cameras mostly use FAT/FAT32 file systems to save data. This type of file system was developed by Microsoft and is compatible with the Windows operating system. Memory cards operate as nothing more than very small hard drives that can be accessed on a computer by USB cable or card reader. The fact that a Windows file system is utilized allows for direct access to this storage volume without the need for additional software applications. Nevertheless, many digital camera manufacturers still offer software tools for making the editing and importing of photos more comfortable for the user. A disadvantage of this system, however, is that such volumes delete data along the same principles as their larger counterparts.



Löschen-Menü
Aktuell löschen?
Alle löschen?

Figure 13: Deletion Dialog for a Digital Camera



Aktuell löschen?
000CAMEA\IMAG0005

Figure 14: When deleting a file on a digital camera in Windows, there is no mention of the fact that the data are not permanently deleted. Even here it is possible to reconstruct the data using specialized data recovery software. (Storage Medium: Digital Camera)

As described above, the same principles apply with regards to file deletion on memory cards. This means that it is also possible to reconstruct data using the same software as was used with the hard disks. Because the contents of such memory cards tends to be more homogeneous than data on most hard disks (a digital camera usually save photos in the same file format), the scan procedures could be significantly optimized. On all of the memory cards tested, around 3,100 photos were found from a total volume of about 1.8 GB. Among the photos found, were personal images of families and sometimes their automobiles. A few pictures were quite intimate, including some that no doubt took advantage of the the camera's auto-shutter function. In general, it is clear to assume that these pictures were not meant for anyone else's eyes.

[redacted] [redacted]

Figure 15: Digital Vacation Photos (Storage Medium: Memory Card)

[redacted]

Figure 16: Digital Photos from a Breeder of Guinea Pigs and Rabbits (Storage Medium: Memory Card)

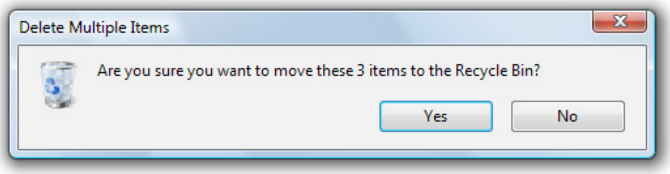
USB Sticks

USB Sticks operate very similar to memory cards. As the capacity of such volumes increase, the more USB Sticks are used as backup media. Exactly as before, the normal deletion of files or the formatting of USB Sticks are no permanent solutions for getting rid of data. Upon the analysis of 12 USB Sticks, a multitude of data was found, including tax deduction forms for a therapist's office and management school examination forms complete with solutions.

Why does this happen?

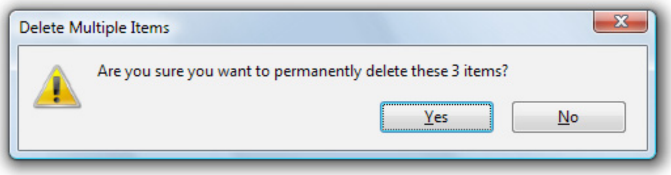
Lack of knowledge is the main problem
After examining the results of the study, one is compelled to ask why it is that users do not properly delete their storage media, so that the contained data cannot be recovered.

Most users, however, are not even aware of the problem because the believe they standard deletion of data is permanent. The Windows Recycle Bin supports this assumption, by providing an intermediate step for disposing of files in the Windows Explorer. This allows the user to to simply restore the data if it becomes clear that a specific is needed. However, when one empties the Recycle Bin, Windows gives the impression that those contained files will be gone forever, even posting a quick warning before the data are deleted.


Delete Multiple Items

Are you sure you want to move these 3 items to the Recycle Bin?

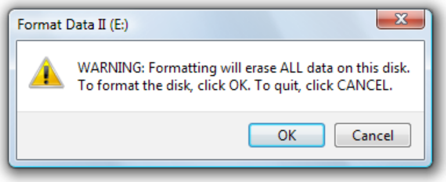
Figure 17: The warning message that appears when moving files into the Recycle Bin in Windows Vista. The files here can easily be „restored".


Delete Multiple Items

Are you sure you want to permanently delete these 3 items?

Figure 18: The deletion warning in Windows suggest to the user that the data will be permanently deleted.

The same questions could also be directed to companies and organizations. As in previous years' studies, this year's test results once again showed that a large amount of confidential data could be recovered that should have never seen the light of day. One can only hope that the use of secure deletion software is a standard procedure in many companies. However, most IT specialists simply underestimate or are unaware of this risk.


Format Data II (E:)

WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.

Figure 19: Even when formatting a volume in Windows the user is informed that the data will be permanently deleted. After completing the formatting, these data are invisible in Windows. However, through the use of specialized software, these data can be easily reconstructed.

A further explanation for the unintentional transmission of personal data became clear upon completion of the study: Defective hard disks, that can no longer be used by the user due to the refusal by Windows to recognize the hardware or file system are generally decommissioned and replaced. In the past, such hard disk drives would have quickly been thrown away. These days, those very same hard disks can find buyers on eBay. These disks, however, can be unlocked with little technical known-how, releasing data that were assumed to be forever lost.

A similar situation arises when formatting a hard disk. The warning notification by Windows leaves the user with the impression that all of the data contained on the formatted disk are permanently deleted. Nothing could be further from the truth. Windows only rewrites the boot sector of the partition, creating a new „Main Index" for the volume. All other data are still present on the disk and can be easily recovered.

Dangers at the Repair Shop
The issue of data security is not isolated to the sale and giving away of older hard disk drives. When a computer needs to be sent for repairs, usually the entire computer is sent, including the hard disk. In such cases, data contained on those hard disks can easily end up in the wrong hands. For this reason, it is very important to only send computers to verified repair specialists. It is important to make sure in form of a signed agreement that the data on a computer are neither read nor copied, unless it is absolutely necessary for the repair of the system.

Just to be sure, it is advised to remove the hard disk before the computer is turned in for repair. This is only possible, however, when the removal of a component does not void the system's warranty or when a repair is possible without the hard disk.

Ignorance
Finally, the roll that ignorance plays is not to be underestimated: Although most online auction salespeople are aware of the fact, that new users can possible read data on used volumes, they do not see it as a critical issue. During the course of the study, three hard disks were acquired that were completely functional and immediately operational when they arrived. At that moment, one has to ask whether the same sellers would want to have all of their own files simply given away in such a manner. In the end, this sort of nonchalance can lead to devastating damages.

Solutions

Formatting is not enough!

Before one can reach for specialized solutions, it is first important to know where the danger of recovering data lies. The results of this study have shown that the deletion or formatting of a hard disk or or storage media in Windows or on a digital camera are definitely not enough to permanently dispose of data. Only the true eradication of data through the physical destruction of the storage volume or the secure overwriting of the data can prevent this form of data theft. In the following sections, both procedures are presented.

Deceiving Security through Data Encryption

One of the most elegant means to protect data is encryption. This means that all of the data on a storage volume are made to be inaccessible to all users who do not possess the necessary username and password

Since the release of Windows 2000, Microsoft has offered the Encrypted File System option (EFS). In Windows XP and Vista, however, this option is only available starting with the Professional and Business Editions. In Windows Vista Ultimate, the more extensive encryption functionality „Bitlocker" has been integrated that starts when the operating system is started and provides comprehensive encryption protection.[2][3]

All of the aforementioned possibilities are not available to users of the Home Edition, because they do not come integrated in the operating system. Such users are forced to purchase additional encryption software. the installation and configuration of such software can be so complicated, that most prefer to forgo with encryption altogether. Moreover, the fact that a single forgotten password would mean no more access to an entire volume, may be unacceptable to some users - a scenario that for some may be more devastating than having the files fall into the wrong hands.

The advantage of encryption is that encrypted data are always protected, whether they are in the hands of a thieves or not. In addition, the user does not have to worry about decrypting and encrypting data, as the operating system takes care of this for the user automatically.

The disadvantage of encryption is visible when disposing of storage volume. The assumption that an encrypted hard disk does not need to be securely deleted is simply wrong.

An encrypted hard disk, just as a unencrypted hard disk, requires secure deletion. The reason for this is the fact that a single password is simply not enough to prevent potential data theft. When faced with such security, an attacker can attempt to acquire the access information through more targeted means. If the attacker knows a bit about encryption mechanisms, it is possible to search for specific data on a hard drive. Many encryption products save their encryption information in specific sectors of a disk, so attackers know right were to go. With the right sort of knowledge, guessing the username and password is also not impossible, as most users usually select passwords that are short and involve common household objects or pets. To be absolutely sure, even users of data encryption technology would be well advised to securely dispose of their data using one of the two methods explained below.

Physical Destruction of Hard Disks

The physical destruction of the hard disk is one of the most secure methods. This ranges from the demagnetization of the disk with industrial electromagnets to the drilling of holes and the smashing of the disk, there are various ways of doing this. All of these methods have one thing in common – the hard disk is then unusable and belongs in the waste bin. However, the costs are relatively high and the processes cannot be carried out in the garden shed without serious safety risks.

In many companies, the physical destruction of the hard disks is out of the question, as they are leased together with the rest of the PC. The whole system must be given back in one piece at the end of the lease.

Software-based Secure Deletion of Data

The cheapest, least complex and most effective method of secure data deletion is that of specialist software. A range of programs can be found on the market that all facilitate the secure deletion of data. Special processes are used that are sanctioned and suggested by such authorities as the US Department of Defense and the German Office for IT security (BSI).[4][5]

One of the most famous algorithms is the extended NISPOM (US DoD 5220.22-M ECE), which defines a sevenfold overwriting process. This uses a combination of random values, predefined values and their complements. The method developed by Peter Gutmann is now regarded as the most secure method of secure deletion. This involves overwriting the data up to 35 times. Restoration of the data by any software method is thereby made impossible.[6]

For this purpose, O&O Software GmbH offers O&O SafeErase for facilitating the secure deletion of all of data in any configuration. It is also able to delete an entire computers including its system files securely with only a few clicks of the mouse. This ensures a system can be cleaned of all its data before it passed onto others. O&O SafeErase offers five different methods for secure deletion, including those mentioned above.

Conclusion

Summary and Comparison with Results of Previous Years' Studie

The subjects of data security and protection were touched on in both the 2004 and 2005 editions of this study. The conclusion then was that most users rely on the standard deletion function in Windows to dispose of their data. The results of this study show that unfortunately, not much has changed with the majority of Windows users making their deleted data available to the public without even knowing it. [7] [8]

For the first time in this study, storage media from the USA were analyzed. The results of this year's tests show that the issue of secure data deletion in the USA is more known than in Germany, where most of the test hard drives originated.

Due to the relatively small number of purchased hard disks originating in the USA, a reliable conclusion is not possible. However, it is assumed that the recently passed federal law in the United States requiring companies and federal institutions to securely delete their data before disposing of hardware has led to more awareness than in Germany.

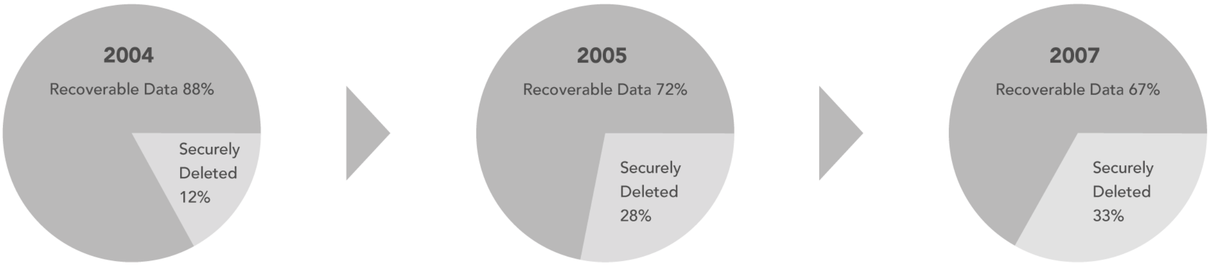
In addition, the results of the testing of memory cards from digital cameras and USB Sticks were also staggering. Three quarters of the media tested were contained recoverable data. One notable trend compared to the previous studies is the rapid increase of digital photos. This correlates most likely to the rapid increase in digital camera sales over the last few years.

Judging from the trends confirmed in this and previous studies, it is safe to say that the issue of secure data deletion is more pressing than ever. A large majority of storage media are being passed on to third parties without properly deleting private and confidential files. It is unclear whether thieves target this sort of data specifically. Most important, however, is that PC users are aware of this danger. What is needed is a similar level of attention given to this issue as is given to the topic of online security. At the moment, only little attention is paid to the reconstruction of data from old storage media - a grave mistake that needs to be addressed.

Dangers of Data Misuse

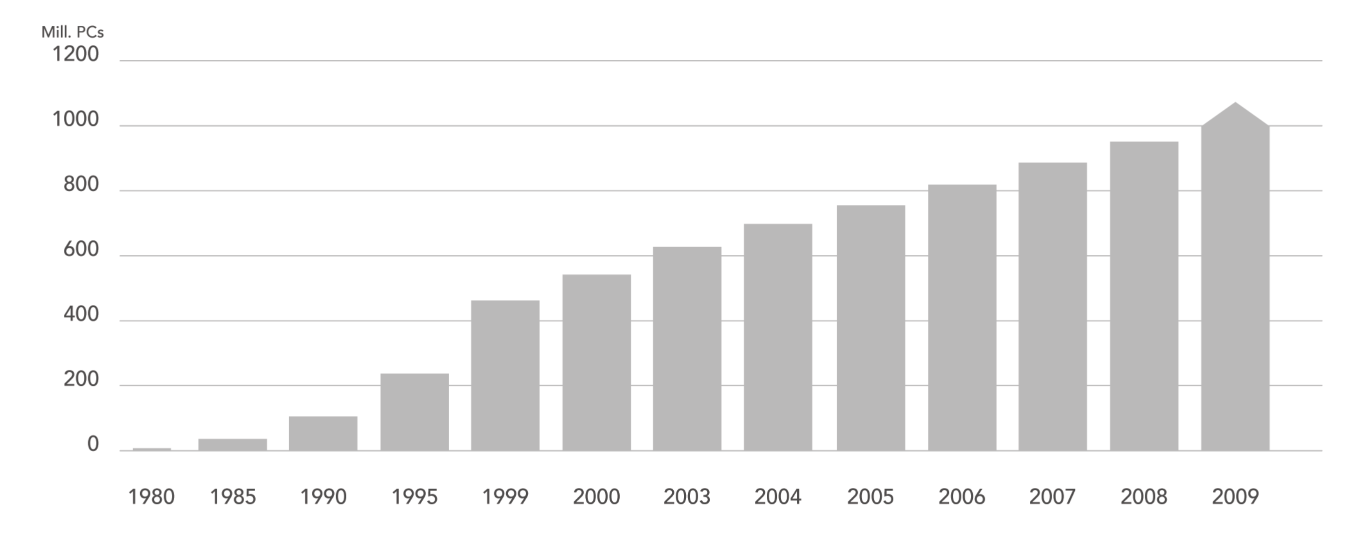
Whenever someone gains access to private data, the danger of identity theft rises dramatically. These data can be used to shop online, sell online or write E-mails in another's name. This can have horrible consequences for the victim. What is worst is the fact that, in such cases, the burden of proof lies with the victims to prove that purchases and E-mail did not come from them. Such an undertaking can be a huge strain on time and resources, not to mention the emotional stress involved.

Figure 20: Data Recovery Rate on Functional Hard Drives



Results produced using data recovery software from O&O Software GmbH

Figure 21: Number of Installed PC Systems Worldwide[9][10]

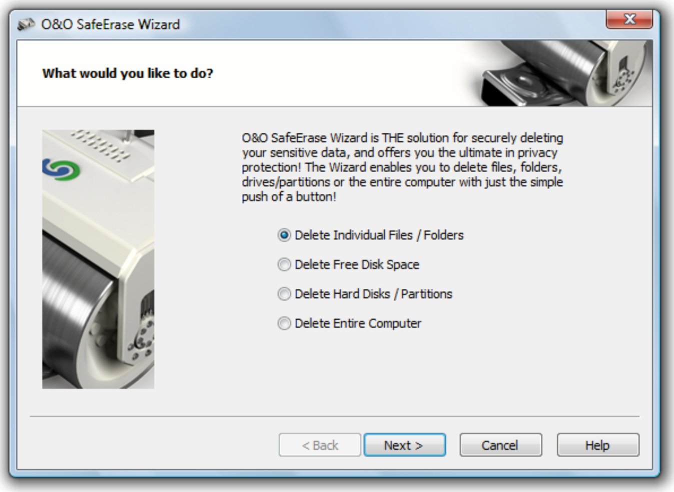


When the contents of data storage volumes in companies or government organizations are released to the public the responsibility lies with a company's or administration's management. Poor judgment on this issue could lead to damages sought by the victims and shareholders. Proceedings in such cases, not to mention the costs and lost of image involved, could threaten the financial and general integrity of a company or organization.

The loss of private data to a home user may be aggravating. However, the devastation caused with the loss of business data could be immeasurable. The publishing of internal data can have civil and even criminal consequences. Person-specific data concerning customers and contractors were readily found in this year's study. If this information would have reached the public it would have meant complete ruins for the parties involved because their reputations would have been irreparably damaged.

Trust is good, control is better!
For the normal PC user the physical destruction of storage media is not a viable option for more than one reason. To make a hard disk unusable through permanent physical damage is a resource-intensive process. Moreover, this does not even cover the costs of actually disposing of the leftover materials, as it is unlawful in most countries to combine electronic waste with the normal household trash. Finally, the earning potential that can be realized through the selling of an old hard disk would be lost by disposing of the hardware in this manner.

The deletion by means of a special software such as O&O Safe-Erase is cost-effective, simple and 100% secure. If users are interested in checking to make sure that the data are really deleted, they need only try running a data recovery program such as O&O Disk Recovery . No data can be recovered. Whatever avenue one decides to take, it is imperative to remember one thing: The standard deletion in Windows or a digital camera is never enough.



What would you like to do?

O&O SafeErase Wizard is THE solution for securely deleting your sensitive data, and offers you the ultimate in privacy protection! The Wizard enables you to delete files, folders, drives/partitions or the entire computer with just the simple push of a button!

● Delete Individual Files / Folders
○ Delete Free Disk Space
○ Delete Hard Disks / Partitions
○ Delete Entire Computer

Figure 22: Secure Deletion Dialog in O&O SafeErase 3

Saving and Deleting Data on Hard Drives

How are data deleted?
Before one can delete data, one has to know where these data are stored. Often it isn't just the file itself that has to be deleted.

When a file is copied, moved or compressed, the original version of the file is often retained. Particular care is advised by, for example, so-called version systems. These deliberately keep old versions or a file in case the user wants to compare or reverse changes. This is particularly the case with the Windows 2003 Server operating system with its „shadow copy" system. This is supposed to prevent the user from changing or deleting a file by accident. Changes to the file are therefore kept in special storage areas on the hard disk, so that old versions can be restored. In this way, it is also necessary to delete the (shadow) file in order to completely delete the data.

Windows also creates copies of data: temporary files include intermediate versions of the actual file. Swap files include storage areas that do not fit in the main memory but are to be moved in later. Temporary files are generally deleted when the relevant program is closed down, but in this case too deletion is just the release of storage space on the disk – these data can also be restored.

Hidden Data Volumes
Data also hide themselves in some other places which the normal user cannot normally access. One problem is the so-called cluster tips. Each hard disk is divided up into clusters when it is formatted. These are the smallest units on a hard disk that the operating system can use. Given the large size (tens of GB) of today's hard disks, clusters of 64 KB are becoming quite usual. For the operating system, this means that even if a file is only 12KB, it will still occupy a space of 64 KB. The rest of the cluster is then unused.

This is normally not a problem, but storage areas are often released for use and then overwritten with new data. Let's imagine that a file has a size of 62 KB and occupies one cluster. This file is then deleted, the data remain but the directory entry disappears. Now a new file is written to this cluster. Let's imagine this is 10 KB. In this case, only the first 10 KB of the file are overwritten and the other 52 KB remains. This example can of course be transferred to any file, as larger files are separated into clusters so that the last cluster is usually not fully occupied. These data fragments are known as cluster tips. The problem with this is that one cannot access these fragments, as the cluster in question is marked as belonging to another file. Only with the help of specialist software can these fragments be erased. This process is know as Disk Wiping.

Data „between the Lines"
The saving of data to a hard disk involves the magnetization of very small iron particles which have a value or either 0 or 1. These particles are transferred to the surface of the disk and are divided into rows so that the hard disk head can read and write the data. However, data are not just written to the main row on the hard disk, but also just beside these rows. These outside rows therefore also contain data. This is normally now a problem, as he hard disk filters this „whispering" out. However, potential attackers can use this data traces in order to restore data. Earlier, simple processes such as the readjustment of the hard disk head were used fort his purpose. Today these data traces are more difficult to reach thanks to greater storage intensity. For this purposes, a great deal of effort and technical know-how is required. It is safe to assume that only very well-equipped data rescue firms and covert agencies are able to use these data traces.

The Deletion of Data
Deleting is more complicated than it sounds. Moving a file to the Recycle Bin and emptying it does not really remove it from the hard disk. The directory entry is removed, but the data themselves remain on the hard disk and can therefore be restored. Even formatting partitions and low-level formatting at the BIOS level does not represent as data can still be restored, even if the effort required is then greater.

Overwriting once or twice can be counterbalanced with the use of an error filter, and old data can thereby be brought to the surface. This is thanks to the physical effects which result from the analog signals of 0 and 1. These never really represent 0 or 1, but are distorted to 0.05 or 1.05. The hard ware counterbalances this defect with tolerance levels meaning that 1 can be saved as 0.95 or 1.05. By using these variations, amicroanalysis of the relevant data signal can provide information about previous data values. If a 0 is replaces another 0, this gives a different signal strength than if a 0 replaces a 1. This process is not exactly easy or cheap, but it shows that simply overwriting the data does not delete them. For this reason, the most common erasure methods are always overwritten with a data value and its complement in order to make this 'difference method' impossible.

Imprint

Acknowledgment
The author would like to thank his colleagues Frank Witter, André Weiß and Matthias Günther for their support over the course of this research, facilitating not only the week-long storage volume purchases, but the data reconstruction and statistical collection as well.

About the Author
The IT specialist Olaf Kehrer is he managing director of the Berlin-based O&O Software GmbH, which has as one of its specialist areas secure deletion of data. Amongst other tasks, he is responsible for the development of new technologies and products for data security.

This includes the products O&O BlueCon, O&O UnErase, O&O DiskRecovery, O&O FormatRecovery, and O&O SafeErase, which apart from the data deletion functions described in the study, allow for the restoration and repair of Windows systems and data.

About the O&O Software GmbH
O&O Software GmbH has been developing Tools for Windows since 1997. These tools are sold in more than 140 countries in a variety of different languages. Customers include home users,SMEs , public institutions and global corporations. The product portfolio includes applications for performance optimization, data restoration, disk imaging and the secure deletion of data. Time and time again, O&O Software recieves outstanding ratings in consumer testing as a leading provider of exceptional software technology.

More information is available on our website or from us directly:

O&O Software GmbH
Am Borsigturm 48
13507 Berlin
Germany

Tel +49 (0)30 4303 43-00
Fax +49 (0)30 4303 43-99

Web www.oo-software.com
E-mail info@oo-software.com

List of Figures

Useful Literature on the Subject

1. Simson L. Garfinkel and Abhi Shelat, „Remembrance of Data Passed: A Study of Disk Sanitization Practices“, IEEE Security & Privacy, vol. 1, no. 1, 2003; pp. 17-28.
2. Microsoft, „Encrypting File System for Windows Vista“, Microsoft Inc.; 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx
3. Microsoft, „BitLocker Drive Encryption“, Microsoft Inc.; 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx
4. Department of Defense, Department of Energy, Nuclear Regulatory Commission, Central Intelligence Agency, „National Industrial Security Program Operating Manual“; 1995, 1997, 2001; http://www.dss.mil/isec/nispom.htm
5. Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch“, BSI; 2006; http://www.bsi.bund.de/gshb/deutsch/
6. Peter Gutmann, „Secure Deletion of Data from Magnetic and Solid-State Memory“, Usenix Assoc.; 1996; http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
7. Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten“; April 2004; http://www.oo-software.com/de/study/
8. Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten 2005“; May 2005; http://www.oo-software.com/de/study/
9. Egil Juliussen, Ph. D., „Computers-In-Use Forecast“, eTForecasts; June 2000; http://www.etforecasts.com/products/ES_cinuse.htm
10. Michael Kanellos, „A billion PC users on the way“, CNET News.com; August 2004; http://news.com.com/A+billion+PC+users+on+the+way/2100-1003_3-5290988.html