

## **Bachelor-Thesis**

### **Presentation and evaluation of common methods of deleting user data in common computer file systems.**

*“Analysis and comparison of selected methods of deleting user data with regard to legal requirements, technical methods and practical implementation options for the secure deletion of data in common file systems.”*

June 2022

**by Florian Weijers**

No. 283045

submitted in the context of the bachelor course of studies in IT-Forensics for  
obtaining the academic degree

**Bachelor of Engineering (BA. Eng.)**

Submitted on July 01, 2022

Primary reviewer: Prof. Dr.-Ing. XXXXXXXXXXXXXXXX

Secondary reviewer: Prof. Dr.-Ing. XXXXXXXXXXXXXXXX

## Terms of reference

In the paper to be worked on here, selected deletion processes in typical workflows of common electronic data processing systems such as PCs and laptops are to be analysed and compared. Specifically, this involves the deletion of general data and special information in file systems, on common data carriers, in data structures (tables, arrays, lists, etc.) and in distributed cloud storage.

The analytical considerations and definitions of terms are carried out from the viewpoint of a private user, a company and a public authority under the respective subjective specifications.

Individual legal requirements and significant internationally recognized standards relating to the secure deletion of data will also be included in the considerations and evaluations. Legal, operational and personal requirements will thus be linked to the technical deletion processes. In doing so, the described conventional deletion processes will be compared with the individually applicable specifications.

The presentation of the different physical deletion processes on commercially available data carriers is only exemplary and generally understandable.

In this respect, current malware and sabotage malware are to be used to illustrate the real application of erasure processes as a concrete danger.

Furthermore, technical data deletion processes in general with regard to hardware and software and their practical implementation possibilities for common users will be demonstrated. Selected software solutions for secure erasure and individual (firmware) tools from well-known manufacturers of data media will be presented as examples.

The final evaluation of the presented erasure methods will be done from the point of view of actual applicability, individual security needs, legal aspects and technical conditions.

Finally, the described erasure methods will be presented in a table with regard to selected criteria such as performance, applicability, security, costs, etc. under the overriding objective of suitability for private users, companies or public authorities.

## Content

1. Problem description	1
2. Definitions and explanations	2
2.1. What is user data?	2
2.2. What is Digital Information?	4
2.3. General remarks	4
2.3.1. Anonymisation according to GDPR	6
2.3.2. Logical and physical deletion	7
2.3.3. From the operating system's point of view	10
2.3.4. Wipe and restore	11
2.3.5. BSI recommendations	13
2.3.6. ISO Standards	14
2.3.7. NIST Guide 800-88 Rev. 1	16
2.4. What is “not recoverable”?	17
2.5. Scenarios of deleting of Data	18
2.5.1. The Recycle Bin solution	18
2.5.2. Deleting in Files	21
2.5.3. Deleting in databases	23
2.5.4. Deleting in compressed containers	27
2.5.5. Deleting in encrypted containers	27
2.5.6. Deleting in virtual machines	30
2.5.7. Deleting of complete hard drives	32
2.5.8. Deleting by resetting to factory state	35
2.5.9. Deleting by cyberattacks (“cyberwar”)	36
2.5.10. Deleting Data in Cloud Storage	39
2.5.11. Deleting by Formatting a device	41
2.6. Software solutions	47

2.6.1. Unix: “wipe”	50
2.6.2. Unix: “shred”	51
2.6.3. Unix: “secure-delete	52
2.6.4. Firmware: “secure-erase”	53
2.6.5. Windows Software: “Eraser”	59
2.6.6. Unix “hdparm”	68
3. Comparison of deletion procedures	69
3.1. For private users	73
3.2. For companies	79
3.3. For public authorities	85
4. Table overview	91
5. Summary	92
6. Classification of the research	93
7. Personal assessment	94
List of references	96
Web Sources	97
List of Figures	100
List of Tables	102
Abbreviations	103
Honourable Assurance	105



## 1. Problem description

At the present time, almost all digital processing operations generate direct or indirect data from users of these IT processes.

Digital personal fingerprints are often created automatically by large corporations or collected and linked by specialized companies. Companies and entrepreneurs store their monetary business data in a wide variety of forms.

Last but not least, the legislator in terms of the GDPR, but also the users or responsible parties of digital systems here demand a deletion of their personal and/or sensitive personal (company) data. In the future, incriminated data (e.g., child pornography files) in cloud storage systems may also have to be irretrievably deleted automatically.

Moreover, can a "right to be forgotten" according to Art 17 GDPR [web 21] or the protection of children by deleting their data be guaranteed with current deletion methods?

In order to be able to consider the interrelationships of the deletion methods, it must first be presented in advance in this elaboration in which forms these most diverse data are usually stored. There are certainly very differentiated applications, such as the storage of personal data in databases, the storage of information in various text or binary-based file formats, or the storage of data in image, video or audio files.

For example, it may be possible to delete and overwrite an image file to prevent recovery of the image content. However, this cannot be done ex equo with individual personal data in a data structure of a database. The extensive deletion of the database or the data carrier would render the system in question unusable, or would strongly influence the performant demands on a modern database system.

Thus, the deletion methods for accumulated data are to be presented in general.

How can data be securely deleted on the physical level? How does this happen in the everyday use of an electronic data processing?

Is the deletion of data ultimately secure, i.e. "irretrievable" according to the current state of the art? What does "secure" mean in the context of deleting data?

What does the legislator provide for this in data protection law?

Can the requirements of deletion obligations be implemented in a compliant manner?

What standards and guidelines exist for this type of data security?

These questions will be presented in the course of this paper with regard to their suitability for private users, companies and public authorities.

To this end, selected technical deletion procedures will be analyzed and compared in connection with the present form and structure of the data and with the security of the data deletion, in order to finally determine whether there are secure deletion procedures for different data, how these would have to be applied and to what extent legal requirements exist for this.

## 2. Definitions and explanations

### 2.1. What is user data?

For further understanding, it must be clarified which data - or rather information - is to be deleted at all. If a private user only wants to free up space on his hard drive at home and deletes blurry test videos from his digital camera, or e-mails that have long since been processed together with their attachments, then in view of this motivation a secure deletion with a high system impairment is obviously not absolutely necessary.

If, however, mandatory legal requirements regarding the necessary deletion of personal data are in the foreground, then secure deletion of this data, even with a higher system impairment, appears to be absolutely necessary, since disregarding these requirements can result in severe sanctions.

The same applies to the deletion of secret company data or sensitive research documents. Under certain circumstances, this data can be the foundation of a company's existence or the basis for economic success.

From this point of view, user data is described in the following in this way:

"User data is digital information with reference to the user on a storage medium that can at least be read again."

In general, that means (in contrast to the "payload" in communications technology) data in file form on hard disks, but also data in main memory or in databases, cloud storage or distributed file systems.

It should be noted that the data area to be deleted can also be only a part of another data area, which may not be deleted under any circumstances.

Conceivable here would be e.g. the data of criminals from a database. In this case, concrete personal data, such as name, address, date of birth, should be deleted from the database according to legal deadlines, but for statistical reasons not the crime itself or the information that an offender has been identified at all.

It becomes apparent that user data for different applications cannot be evaluated in the same way.

Thus, the effort required for the possible recovery of the data must also be considered in a differentiated manner. To restore a half-page text document of a homework assignment that has been deleted by mistake, it is unlikely that major resources will be expended and finally the assignment in question will simply be worked through again.

In this respect, the technical research results of an innovative energy company regarding the geometry of a fusion reactor should certainly be securely deleted, if necessary, so that the data cannot be viewed by a 14-year-old computer science student after purchasing a used server hard disk simply by restoring a deleted file allocation table.

The effort required to restore a deleted file allocation table is, moreover, highly dependent on the connection speed and the computing performance of the computer system, and can usually take between a few hours and a few days (depending on the size of the hard disk).

## 2.2. What is Digital Information?

Digital information is data stored on data carriers of computer systems.

This primarily includes data of the user of the computer system, such as personal or person-related data.

Furthermore, digital information also includes data that is not consciously stored by the user but is eminent for the functionality of the computer system. These are data of the operating system, of applications, log, analysis or monitoring data. This data also contains information about the computer system and allows conclusions to be drawn about its use.

Much of this digital information cannot be read, manipulated or even deleted using conventional methods.

One example would be the S.M.A.R.T. values of a hard disk [web 18]. This data, which is of forensic interest, cannot be manipulated in the controller on the hard disk by user commands.

The S.M.A.R.T. values thus provide unbiased information about the use of a computer system.

This and similar data will not be explicitly considered in the course of this work.

A final deletion of this protected data can only be done by physical destruction of the data carrier (disk or any media device).

## 2.3. General remarks

Let us first discuss the concept of deletion in information processing systems.

"What is deleted is no longer there." my daughter (age 8) said recently when I asked what deletion is. "When is something no longer there?" "When you can't see it anymore." Then I held the crayon behind my back - and asked if I had now deleted it. "No." was the answer. This exactly describes vividly the problematic nature of the term "delete": Is something really no longer there if I can no longer see it? And, if I can no longer see it, but another person can, is it deleted? Is something only deleted if I can't recover it?

For in-depth consideration, let's take a closer look at several intensities of the terms "delete" and "erase" in the field of computer science<sup>1</sup>:

Colloquial Deletion	A data object has been removed, willingly or unwillingly, from its point of origin by means of a "delete" dialogue, and is initially undetectable or gone by the user.
Deletion from the file system	A file's associated meta information is removed from the file system's file allocation table and the allocated storage area is marked as free. However, the file contents remain in the permanent memory until they are overwritten by other data.
Secure delete	Data or a file is deleted in such a way that it is not possible for the average user to recover this information, even with above-average effort.
Deletion by wiping	Information (data, files or partitions) is completely overwritten with other data (mostly random data or random bits) on the fixed storage (HDD, SSD, USB stick, or similar). Wiped data cannot be recovered by conventional forensic means, even with great effort.
Erasure by sanitization	Entire volumes are overwritten (mostly with 0 bits) in such a way that no information remains in the user data area. After this process, no information is available as to whether there was any data at all on the medium in question.
Clearing	Erasing the addressable memory area by logical techniques on the device by standard commands. The data can not be recovered by simple recovery techniques.
Purging	Uses physical or logical techniques to erase data, that make data-recovery not possible under laboratory conditions.
Destroying	Destroying means the physical destruction of the target media, that makes it unusable for further use. The data can not be restored even with state-of-the-art laboratory techniques.
Cryptographic Erase	Cryptographic Erase describes an erasure process that looks at the result of the erasure and is based on completely encrypted media, such as hard disks. In summary, only the decryption key is securely erased, so that the data on the disk cannot be recovered using current methods.

Table 1: Synonyms of deleting in the context of data science by Florian Weijers

---

<sup>1</sup> In reference to NIST SP 800-88 Rev. 1 and ISO/IEC 27040:2015 standard papers [web 11], [9], [8].

We can see that there are different terms (and even many more) in use on the subject of "secure deletion of data". These have adapted to the areas of application and the needs of the users.

The terms "clear", "purge" and "destroy" have been defined by the NIST (see point 2.3.7) and the ISO/IEC papers. However, the terms "secure erase" or "delete" are sometimes unclear in common parlance and are evaluated very differently even by the manufacturers of hard disks.

We will address these ambiguities in the next following points, as the wording in laws and regulations may not allow the technical process to be derived directly.

### 2.3.1. Anonymisation according to GDPR

The GDPR<sup>2</sup> describes different data protection procedures. With regard to the rights of the data subject according to Art. 12 GDPR, from whom the data is collected, the deletion of this personal data plays an important role. One principle is the right to be forgotten according to Art. 17 GDPR, whereby the GDPR only refers to the deletion of personal data.

The consensus is that deletion is assumed so that the data cannot be restored or cannot be restored easily.

One might expect that the data is to be evaluated according to its sensitivity, and that data that is particularly worthy of protection must be deleted more securely than possibly less sensitive data records.

There is no binding definition of the term "deletion" in the GDPR. Art. 4 mentions deletion and destroying as alternative forms of processing. However, deleting and destroying are not necessarily identical and there are technically several levels of data deletion depending on the degree of difficulty of recovery.

---

<sup>2</sup> General Data Protection Regulation - DSGVO in German.

Courts sometimes judge the deletion of data according to the GDPR very differently. In a decision<sup>3</sup> dated December 5th, 2019, the Austrian data protection authority states: "The removal of the personal reference from personal data can in principle be a possible means of deletion in accordance with Art. 17 GDPR. However, it must be ensured that neither the person responsible nor a third party can restore a personal reference without disproportionate effort."

The situation is somewhat more difficult when it comes to anonymising data. Anonymised data sets may be processed according to the GDPR and do not fall under the relevant data protection restrictions.

The problem of deleting data is thereby shifted to the area that only individual data fields of a data record are securely deleted. This indeed poses serious technical hurdles, as many data processing systems have been optimised for processing and storing data, but not for securely deleting individual data fields.

In summary, it can be said that personal data is deleted in the legal sense when it is no longer possible to process and use the data of the person concerned.

The specific technical implementation is not discussed.

### 2.3.2. Logical and physical deletion

Logical deletion of data describes a deletion process on data carriers that removes the entry of the data in the file system without explicitly removing the data. The deleted storage area is marked as "free" in the sense of the file system used.

However, since the useful data is still on the data carrier, this data can be recovered using file carving as a simple method for restoring data.

In the course of operating a computer system, however, the memory marked as free is eventually needed again and overwritten. Thus, the memory area is not

---

<sup>3</sup> Austrian supreme data protection authority DSB-D123.270/0009-DSB/2018 from 05.12.2018 [web 2].

recoverable by usual data recovery techniques. The sole logical deletion of data is not considered sufficiently secure from the point of view of data protection and data security.

Simplified, the logical deletion of data can be represented as follows:

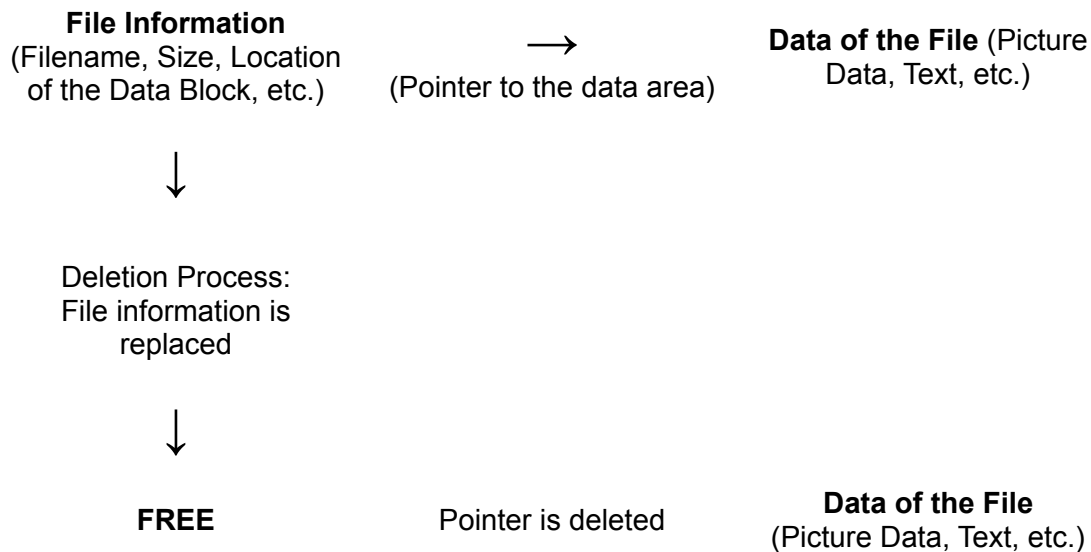


Figure 1: Logical deletion of data - simplified (by F. Weijers)

This is only a schematic view of an erasure procedure on a typical file system such as NTFS, FAT32 or exFAT. Not all the file information data needs to be overwritten in the deletion process. Often, only a free flag in the form of a single bit is set before the data set, which marks the area in the file table as free.

This deletion method has a very large speed advantage due to the few write accesses to the hard disk.

Incidentally, the logical deletion of data can also be optimised in terms of data security by encrypting the user data in the form of file encryption. File carving can only restore the encrypted file at best. The key is then required to access the data.



In addition to the logical deletion of data, there is also the physical deletion of data. This deletion procedure describes the physical state of the data area where the data to be deleted is or was located. Basically, data should be physically deleted by single [2] or multiple overwriting. On magnetic hard disks, physical erasure was a commonly used secure erasure method. However, on other data carriers, such as SSDs [web 25], other write mechanisms and addressing strategies are used with regard to the data carrier organisation, so that new data is not specifically written to the storage area that has recently become free. The firmware of SSDs tries to manage the memory areas optimised for the lifetime, and can also exclude individual memory cells from the write processes. Data can thus be read out again, and the secure deletion of data by overwriting is not applicable per se.

Simplified, the physical deletion of data can be represented as follows:

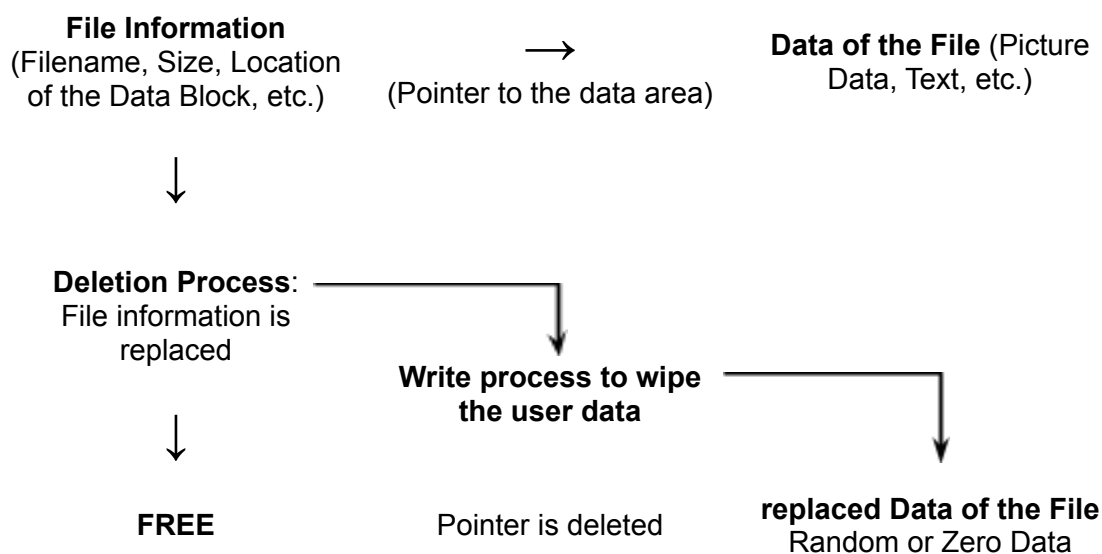


Figure 2: Physical deletion of data - simplified (by F. Weijers)

As can now be seen, the deletion process is extended by another writing process. So that the user data is overwritten and cannot be restored by conventional means.

However, the high system impairment caused by the write processes proves to be critical. These data rates can critically slow down the entire computer system, and thus these deletion processes are rarely used in practice.

Furthermore, during security-relevant deletion processes, the data in the file table is also overwritten with random data or standard data. In this way, no information about the previous data allocation should remain.

On SSDs, the life span of the memory cell can be almost halved by regularly overwriting data.

With the deletion method shown above, we must note that the storage space on which the file was located is precisely overwritten. So the occupied sectors are overwritten with random data or zero bits. Shadow copies or mirror data are not taken into account! In the NTFS [web 12] file system or other modern file systems, this can lead to the data being hidden in other areas of the hard drive and recoverable by file carving or other data recovery processes.

### 2.3.3. From the operating system's point of view

The deletion of data from the point of view of the operating system like Windows, Linux, Unix, macOS, BSD, etc. can basically be described as follows:

1. The data necessary for the functioning of the system must not be deleted.
2. The user receives write access to his data area and may read, write and delete data there. As part of user-friendliness and the fear of accidentally deleting data, the Recycle Bin solution has prevailed in all common operating systems.

During the operation of an operating system, data is generated that must be stored. If this data is no longer required, the data areas are released again by

the operating system in order to avoid a memory shortage. This applies in particular to updates of the entire operating system.

Basically, write access to the hard disk is optimized or minimized by the operating system and the fast RAM memory is primarily used.

However, if the fast RAM memory is full, data is also swapped out to the hard disk. Under the criterion of the efficiency of the operation of the system, the data is usually not deliberately overwritten directly.

This creates a continuous flow of data from the operating system and user data during the operation of a computer system. The organization of the data flow is the responsibility of the operating system. However, the user can initiate different tasks or prioritize them by assigning privileges. It may be the case that in the event of a user command, the data on the hard disk should be erased as quickly as possible, and not only when the operating system has completed all other tasks, such as updates, logging, etc. For security reasons, the user may not want to save his data on the hard disk at all, but only keep it in the volatile RAM memory in order to then send it separately, possibly encrypted (like in the Tails<sup>4</sup> operating system).

Different applications are required for these scenarios, which support the user and meet individual needs.

In summary, it can be stated that an operating system is not primarily designed to securely delete user data, but to ensure smooth, user-friendly and optimally performing operations.

#### 2.3.4. Wipe and restore

The concept of data erasure<sup>5</sup> is therefore to be interpreted in different technical ways.

---

<sup>4</sup> Further more on [www.tails.boum.org](http://www.tails.boum.org).

<sup>5</sup> Discussed on <https://it-forensik.fiw.hs-wismar.de/index.php/Datenvernichtung>.

Two different terms that better describe the objectives of a data processing operation will now be explained.

It is about secure erasure in the form of deleting and restoring data by the user of a computer system.

Wiping is the deletion of an area of data by overwriting it one or more times using different methods, such as random numbers or zero bits.

<u>Data</u>	<u>Wiping-Method</u>	<u>Result</u>
PASSWORD	Overwriting with zero bits	00000000
PASSWORD	Overwriting with Random Data	1tB0OkIr

Table 2: General methods of wiping data (by F. Weijers)

Wiping is therefore a method of deleting an area of data without being recoverable by the user or by normal technical means. The result of the wiping process must not allow any indication of the previously existing data, and it describes a physical deletion process according to 2.3.2.

These erasure algorithms are still recommended today in the hard disk manufacturers' instructions for securely erasing the contents of HDDs. The statement that overwriting data once is sufficient to make recovery of the data impossible has survived to this day.

Recovering a data record also describes an operation that requires a previous non-secure deletion process. Thus, data can be easily recovered by the user from the Recycle Bin. However, user data from hard disk areas that have not yet been overwritten can also be recovered without special data recovery techniques and without laboratory equipment. We will come to the related problems in the NTFS file system during wiping processes later.

The goal of a secure and efficient erasure mechanism is now an application that affects the performance of the operating system as little as possible, and there is the equally important requirement that the erasure process must be

sufficiently secure to make data recovery as difficult or even impossible as possible in the individual use case.

### 2.3.5. BSI recommendations

In this context, the German Federal Office for Information Security (BSI []) publicly gives the following advice for the secure deletion of data on their homepage<sup>6</sup>:

1. Using the "enhanced security erase" command from the ATA standard<sup>7</sup> command set for SSDs and SSHDs
2. 7x overwriting of data on older magnetic hard drives

Recommended: The combination of the two methods from 1. and 2.

This statement from the homepage of the leading German authority for information security now shows the dilemma that has arisen.

Deletion procedures are recommended that ensure the best protection of data and their irretrievable deletion.

But how can a user access the enhanced security erase command? What does this command do on disks? What happens if the ATA commands cannot be sent to the hard drive, for example because the hard drive is connected to the

---

<sup>6</sup> Available at

[https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen\\_node.html#:~:text=Smartphone%20auf%20We rkeinstellungen%20zur%C3%BCksetzen,und%20Apps%20vom%20Ger%C3%A4t%20gel%C3%B6scht.](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html#:~:text=Smartphone%20auf%20We rkeinstellungen%20zur%C3%BCksetzen,und%20Apps%20vom%20Ger%C3%A4t%20gel%C3%B6scht.) (Version from 20.06.2022)

<sup>7</sup> From [https://ata.wiki.kernel.org/index.php/ATA\\_Secure\\_Erase](https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase) accessed on 03.05.2022

computer via USB or even network attached? How should individual files, folders or partitions be deleted?

We will ask ourselves these questions in the further course of this work and, among other things, it can be shown that the hard disk manufacturers often do not use the term "enhanced security erase" at all or combine very different (insecure) deletion processes with this command.

Last but not least, it should then be evaluated whether a deletion process can be used in practice at all, because a deletion process with 7 overwrites can take around 65 hours<sup>8</sup> on a USB 2.0 device with 1 TB storage capacity. On SSDs, this multiple overwrite erase method would dramatically shorten the expected lifetime of the drive (by about 86 percent)<sup>9</sup>.

Inset: CON.6 - Delete and Destroy [3]

In the CON.6 concept from February 2021, the BSI describes minimum requirements for procedures for deleting and destroying data carriers.

A distinction is made between encrypted and unencrypted data carriers. Overwriting the data carrier with random values (PRNG stream) is now described as a sufficiently secure deletion method.

In the case of encrypted data carriers, the crypto key must be securely deleted. In point 3.3 of the concept, requirements for increased protection requirements are formulated. Deletion methods are no longer described, but reference is made to the destruction of data carriers in accordance with ISO/IEC 21964-1.

## 2.3.6. ISO Standards

In 2015, ISO created the international standard ISO/IEC 27040:2015 [8]. This paper deals with data security and the protection of data and the processes that are intended to ensure the highest possible level of data protection. ISO/IEC

---

<sup>8</sup> USB 2.0: 240 Mbit/s write speed (USB 3.0 at 2000 Mbit/s would last about 8 hours over all).

<sup>9</sup> 7-times overwriting decreases the lifespan to 1/7 equals 0,143 equals 14,3%

27040:2015 goes a little deeper into data security than ISO/IEC 27002:2013 from 2013 and its new edition 27002:2022 from 2022.

ISO 27040 describes fundamentally different data security processes. These statements and formulated remarks are certainly interesting, but not particularly relevant for this specific elaboration in deleting specific user data.

However, the section on storage security services<sup>10</sup> should be dealt with in a summarized manner. It is suggested that storage media should be sanitized when it should or can no longer be used. A certificate of sanitization is recommended for this purpose, which contains the information on the treatment process.

The Annex A<sup>11</sup> (media sanitization) is almost identical, where the methods of "Clear", "Purge" and "Destroy/Destruct" are defined. We described these terms at point 2.3. before.

This Annex A comprehensively describes the options for deleting a wide variety of storage devices with the methods of "Clear", "Purge" and "Destruct".

All relevant data areas should at least be overwritten and all related data areas, such as backups or other systems, should be processed.

It is also recommended to monitor and check the deletion processes.

Finally, Annex A.3<sup>12</sup> describes the cryptographic erase method, which also mentions that the security of a cryptographic erase depends on the security of the decryption key. If this key has been read during the lifetime of the data carrier, the data can also be restored by an attacker after a cryptographic erase. We will come to the process of a secure erase in point 2.6.

Basically, the ISO standard 27040 provides basic specifications for the preparation of data carriers and their cleanup. In addition, the deletion and sanitization procedures are also presented in terms of their security and recommended according to the security level.

---

<sup>10</sup> ISO/IEC 2015 p. 37 ff.

<sup>11</sup> ISO/IEC 2015 Annex A p. 60 ff.

<sup>12</sup> ISO/IEC 2015 p. 72 ff.

### 2.3.7. NIST Guide 800-88 Rev. 1

The NIST is the National Institute of Standards and Technology in the United States of America. It is based in the U.S. Department of Commerce or in Gaithersburg, Maryland. The federal agency emerged from the National Bureau of Standards (NBS), which was founded in 1901. The tasks of the NIST include, among other things, the standardization of different technical processes such as the provision of precise timing (atomic clock) or the Guidelines for Media Sanitization, which are now to be described here.

Many international guidelines have adopted the processes for sanitizing storage devices from the NIST guidelines. These guidelines therefore represent almost an international standard and must therefore be addressed here.

This is now specifically about the publication "NIST Special Publication 800-88 Rev. 1" which was published in December 2014 and emerged from the tasks of the Federal Information Security Management Act of 2002.

The elaboration is about the description of processes to irrecoverably delete data from media storage or to make the recovery of the data disproportionately difficult.

The guidelines are aimed at system operators and responsible authorities.

NIST defines the terms "Clear", "Purge" and "Destroy" to describe actions to delete data<sup>13</sup> and on what data carriers to use it.

These definitions can be found in this elaboration under point 2.3., as well as a description of the term "cryptographic erase".

In principle, NIST recommends the use of encrypted data carriers with preset encryption. An emergency wipe of all data on the disk can be accomplished in under a second by effectively erasing the decryption key<sup>14</sup>.

It is also recommended to physically destroy<sup>15</sup> data carriers if they are no longer to be used because they are damaged or similar.

---

<sup>13</sup> NIST SP 800-88 Rev. 1 p. 24 f.

<sup>14</sup> NIST SP 800-88 Rev. 1 p. 10 f.

<sup>15</sup> NIST SP 800-88 Rev. 1 p. 18.



An important aspect is also the control and documentation of the result of the deletion. Samples must be examined regularly<sup>16</sup> to determine whether data has just been irretrievably deleted.

Finally, it can be summarized that the NIST gives a comprehensive guide to the deletion of data carriers. However, the instructions refer to the destruction or cleanup of complete physical data carriers. There are no instructions for deleting data in individual partitions, files, or in network attached cloud storage.

## 2.4. What is “not recoverable”?

How can states of data carriers be defined where data cannot be recovered? The three deletion processes "clear", "purge" and "destroy" from NIST SP 800-88r1 [9] are presented here as examples:

### “clear”

Defines an erase operation that applies logical techniques via typical read and write accesses to erase data at all user-addressable storage areas without being recoverable by simple data recovery methods.

Clearing is therefore the weakest form of deleting data under the view of recoverability.

### “purge”

Is an erasure operation that uses physical or logical techniques that make data recovery impossible under modern laboratory conditions.

Purging is thus a recognized secure form of deleting data from the point of view of recoverability.

### “destroy”

Means an erasure process like shredding, granulating, melting or incinerating, that makes the recovery of target data impossible under modern laboratory conditions, and renders the medium unusable for further use.

---

<sup>16</sup> NIST SP 800-88 Rev1. p. 20 ff

Destroying is after all recognized as the safest form of deleting data and all primary and secondary information from the point of view of recoverability.

It should be noted that the data carriers must be checked ("validate") in a standardized manner after the above-mentioned processes.

In order to meet the NIST SP 800-88r1 erasure standards defined above, hard disk manufacturers have implemented standard commands in their firmware for different types of hard disks to secure erase data. These command sets are discussed later in excerpts.

Returning to the legal evaluation of the state of recovery, it must be said that there is and probably will be no definitive legal opinion on this [10]. In today's legal opinion, the non-recoverability of data is the condition that data cannot be recovered by an average user by ordinary means. However, this could change very quickly with the development of forensic data recovery freeware. The very existence of such software or hardware for data recovery leads to the assumption that data obviously has to be deleted deliberately, checked and reliably.

Let us now assume in the following that data cannot be recovered if the funds and technical possibilities exceed the current scientific possibilities in technical laboratories or if the decryption of the data by guessing the key would take a disproportionately long time (>10 years with pre-quantum computer systems).

## 2.5. Scenarios of deleting of Data

### 2.5.1. The Recycle Bin solution

The most common user-initiated deletion method is moving data to the Recycle Bin. This does not physically delete data, but actually changes its file pointer in

the file allocation table to the Recycle Bin. The background to this method is the frequent accidental deletion of data by the user. Using the Recycle Bin, the files can be recovered without any effort.

Thus, moving to the Recycle Bin is technically not a deletion method, but only a change of the data pointer to the file location. The storage area remains occupied and no new free space is created on the disk.

The Recycle Bin solution is used in the current operating system versions of Microsoft Windows (\$RECYCLE.BIN - Directory) and Apple iOS as the default method for deleting files<sup>17</sup>.

Also in the Linux distributions with Unity/GNOME, MATE, KDE, LXDE and Xfce desktop solutions, the Recycle Bin is included as a delete method in the graphical file managers by default.

A Recycle Bin or trash can also be used in the Linux command line (trash-cli). The files are explicitly not deleted, but moved to the Recycle Bin. This is used for easier recovery of accidentally deleted files.

Files removed from the Recycle Bin can also be recovered using file recovery programs (such as tsk\_recover from sleuthkit). Filecarving methods are used and different operating systems such as Windows, Linux, iOS or BSD are supported.

In summary, it can thus be stated that the user can understand "deletion" as moving files to the Recycle Bin. There, the files can also be recovered by less experienced users, which means that the method cannot be qualified as a secure deletion method.

Actual deletions of the Recycle Bin (MS Windows, Apple iOS, BSD or Unix/Linux) can now be triggered by the user. Automation according to time is also possible.

Deleting from the Recycle Bin removes the file entry from the file allocation table and marks the storage area as "free".

The data can be recovered afterwards only by special applications like piriform recuva, autopsy or others.

---

<sup>17</sup> Deleting files on a Mac: <https://support.apple.com/de-de/guide/mac-help/mchlp1093/mac>.

By the recovery applications, the data is searched and recovered by the method of file carving, where the application algorithms are searching for typical beginning sections of known file types and then looking for the end by known sequences at the end of the file into the raw data stream of the hard disk or storage device.

That is also possible in encrypted file systems if the encryption has been removed. This recovery method becomes problematic after defragmentation has been performed on HDD's when data areas are locally merged for faster acquisition. If the data area is overwritten and filled with other information, also a file carving cannot recover any data, but only read the data currently present there.

The data in the file slack, which is at the end of a file, remains unaffected. File fragments from previous files can be located there.

Microsoft Windows and Apple iOS use optimized defragmentation logics that intelligently group memory areas and rewrite them if necessary.

On SSDs, however, defragmentation is not used because these read and write processes can reduce the life of the memory cells not insignificantly. The firmware of SSDs has its own algorithms for memory optimization in this context. Cells can also be left out for the time being. The data in these cells is thus not overwritten at first either.

As explained in the previous points, moving data to the Recycle Bin is not to be regarded as a deletion process in the technical sense.

The data can be restored by the user in the solutions mentioned.

In the current time, the use of the Recycle Bin of the different operating systems has become so common that data is rarely actually deleted. This behaviour was supported by the enormous availability of cheap data storage space. In normal use, the user hardly has to worry that the memory for text documents, spreadsheets or common applications is running out. In most cases, most computer systems also have easy upgrade options for hard disk space.

## 2.5.2. Deleting in Files

Deletion processes therefore take place in different environments. Deleting user input in files can be viewed very easily. For the sake of simplicity, a word in a text file should now be securely deleted. This may be because of a data correction, or because a name or fact has changed. However, the old data should not be recoverable. Is that possible?

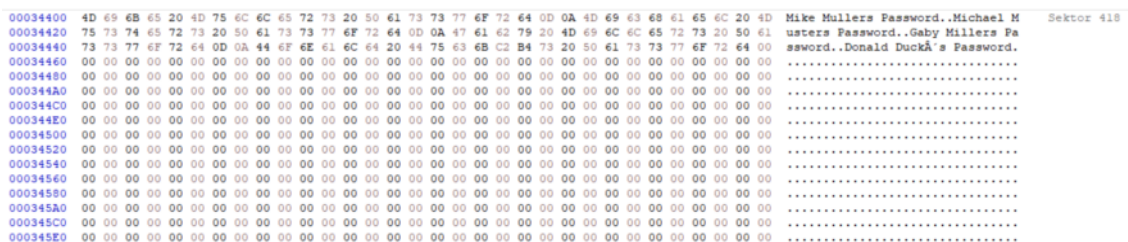


Figure 3: Screenshot of the concerned data area (HxD HexViewer<sup>18</sup>)

The Screenshot shows the original File with some critical Data in a FAT file system at sector 418.

Then we opened the file with an editor, deleted some data and save the file again:

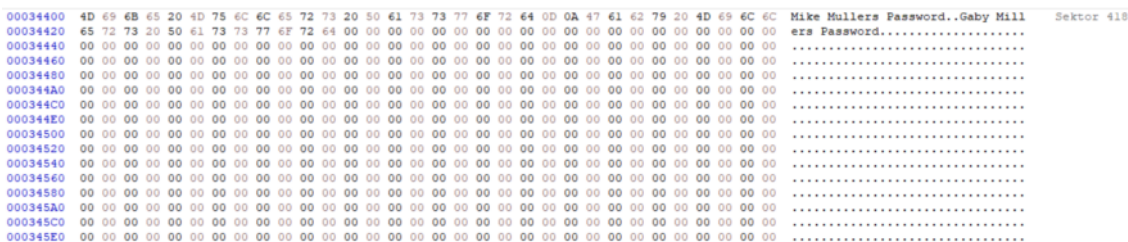


Figure 4: Screenshot of the concerned data area after the manipulation

Now can be seen, that the Data is gone and cannot be recovered, if there was no backup or mirror of the old file.

Next experiment is the same procedure in a standard NTFS file system, how it is used in Windows Computers:

<sup>18</sup>Free download at <https://mh-nexus.de/de/hxd/>

There can be seen the original file at sector 31.478 with some data:

[illegible]

Figure 5: Screenshot of the concerned data area in a NTFS file system

Then two entries in the file were deleted at sector 31.478 with the simple use of a text-editor and the normal file saving:

[illegible]

Figure 6: Screenshot of the concerned data area in a NTFS file system after manipulation

But a mirror copy of the deleted file content at sector 27.728 was created:

Offset	Hex	ASCII	Comment
00DA090	52 43 52 44 28 00 09 00 4F 61 00 00 00 00 00 01 00 00 00 01 00 01 00 E8 0F 00 00 00 00 00 00 00	RCRD[.....Cc.....e.....	Sektor 27.728
00DA0A0	4F 6F 10 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Cc.....Cc.....	
00DA0A0	4A 6D 10 00 00 00 00 00 55 6D 10 00 00 00 00 00 DB 6D 10 00 00 00 00 00 00 00 00 00 00 00 00 00	Jm.....Um.....Um.....	
00DA0B0	00 00 00 00 00 00 00 00 00 D8 03 00 00 92 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....S.....	
00DA0B0	00 00 10 00 00 00 00 00 00 00 10 00	.....	
00DA0C0	4A 6D 10 00 00 00 00 00 15 6E 10 00	Jm.....n.....	
00DA0C0	00 00 00 00 00 00 00 00 00 00 01 00 00 00 18 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00	.....	
00DA0E0	00 00 00 00 00 00 00 00 00 00 38 01 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00	(.....F.....F.....	
00DA100	64 0D 0A 67 61 62 79 20 4D 69 6C 6C 65 72 30 02 60 61 73 73 77 6F 72 64 0D 0A 44 6F 61 6C 6C	d.....Baby Millers Password:Donald	
00DA120	80 44 75 63 6B C2 B4 73 20 50 61 73 73 73 77 6F 72 6A 00 00 00 00 00 00 00 27 6E 10 00 00 00 00 00	Duck's Password:.....'.....	
00DA140	15 6E 10 00 00 00 00 00 00 15 6E 10 00 00 00 00 00 A8 00 00 00 00 00 00 00 01 00 00 00 18 00 00 00	.....	
00DA160	00 00 00 00 00 00 00 00 00 07 0F 00 00 28 00 40 68 00 00 00 00 00 00 18 01 01 38 20 00 06 00 02 00	.....r.....(.....h.....e.....	
00DA180	09 00 00 00 00 00 00 00 00 SE 0F 00 00 00 00 00 00 C7 46 49 FE 80 79 D8 01 C7 46 49 FE 80 79 D8 01	.....C74649FE8079D801.....C74649FE8079D801	
00DA1A0	00 00 00 00 00 00 00 00 00 00 20 00	.....	
00DA1C0	00 00	.....	
00DA1E0	6E 37 3D BE 80 79 D8 01 20 00	n74649FE8079D801.....	

Figure 7: Screenshot of the mirrored data area in a NTFS file system

This circumstance shows dramatically that deleting is not the same as deleting. A normal user cannot tell whether the file content has been deleted or not. It seems to work in a file system of an external data medium (if it is FAT) but on the system hard disk, i.e. in the normal user memory area of documents, images, etc., remnants of the former file content remain without the user knowing about it.

It is therefore not recommended to use an NTFS file system for critical data, because the user cannot completely control the deletion processes in files.

By the way, there are similar methods of data security implemented in other file systems besides NTFS. This is addressed in chapter 2.5.11. "Deleting by formatting a device".

Finally, changing the data content naturally depends on which software is used to edit the file and whether there are backups, etc.

### 2.5.3. Deleting in databases

In conventional database systems<sup>19</sup>, which are widely used today, operations are constantly performed on the data.

This includes inserting data, manipulating data records and also deleting individual data from the database in order to keep the data records up to date or to comply with data protection rules.

We would now like to take a look at an example of a MySQL database with a illustrative data set.

Personal data is stored or inserted, and a person with all data is deleted from the database.

Then only the name of one person is removed to pseudonymise the data set.

In the end, a complete column is pseudonymised from the database because the data was not allowed to be collected for legal reasons.

```
-- create a table
CREATE TABLE persons (
  Id INTEGER PRIMARY KEY,
  name TEXT NOT NULL,
  colour TEXT NOT NULL);

-- insert some Data
INSERT INTO persons VALUES (0001, 'Clark', 'white');
INSERT INTO persons VALUES (0002, 'Dave', 'black');
INSERT INTO persons VALUES (0003, 'Ava', 'brown');
INSERT INTO persons VALUES (0004, 'Zork', 'green');
```

---

<sup>19</sup> More on <https://it-forensik.fiw.hs-wismar.de/index.php/Datenbankmanagementsystem>.

```
-- fetch all
SELECT * FROM persons;

-- delete one entry
DELETE FROM persons WHERE name ='Clark';
SELECT * FROM persons;

-- overwrite one entry
UPDATE persons
SET name = REPLACE(name, 'Dave', 'x' );
SELECT * FROM persons;

-- overwrite colour entries
UPDATE persons
SET colour = REPLACE(colour, colour, 'irrelevant' );
SELECT * FROM persons;
```

Output:

<u>Id</u>	<u>name</u>	<u>colour</u>
1	Clark	white
2	Dave	black
3	Ava	brown
4	Zork	green

<u>Id</u>	<u>name</u>	<u>colour</u>
2	Dave	black
3	Ava	brown
4	Zork	green

<u>Id</u>	<u>name</u>	<u>colour</u>
2	x	black
3	Ava	brown
4	Zork	green

<u>Id</u>	<u>name</u>	<u>colour</u>
-----------	-------------	---------------



2	x	irrelevant
3	Ava	irrelevant
4	Zork	irrelevant

Figure 8: MySQL-Example “Deleting Data in Database MySQL” (by F. Weijers)

As can be seen here, the data in the database is obviously erased and cannot be recovered through conventional means.

If there is no backup of the database, the data is irretrievably lost.

Normally, however, backups of database systems are created regularly to prevent irretrievable data loss. Data to be deleted is usually not removed from the existing backups of the databases. This is simply not possible with the means and processes of the database management software. Precisely because the backups are usually stored separately from the actually running system in a protected, mostly write-protected environment.

So it is not the ongoing operation of the database that is problematic, but rather the versions of the database system that have already been saved, which may contain data to be deleted and consequently would have to be deleted.

Secondly, deleting in a comma-separated database should be shown using the Linux command line. This example also shows deletions in typical text files.

Following, we use the command line tool `sed`<sup>20</sup>:

```
forensix@ForensiX:~$ cat example.txt
001, Clark, white
002, Dave, black
003, Ava, brown
004, Zork, green

- Replacing the name "Dave" with an "X".

forensix@ForensiX:~$ sed -i 's/Dave/X/g' example.txt

forensix@ForensiX:~$ cat example.txt
001, Clark, white
```

---

<sup>20</sup> Tool description on <https://wiki.ubuntuusers.de/sed/>

```
002, X, black
003, Ava, brown
004, Zork, green

- Deleting the entry "Clark".

forensix@ForensiX:~$ sed -i '/Clark/d' example.txt

forensix@ForensiX:~$ cat example.txt
002, X, black
003, Ava, brown
004, Zork, green
```

Figure 9: Linux Terminal with sed (by F. Weijers)

It could now be shown how individual data can be removed from files or a database. However, this is based on readable and unencrypted file formats. In compressed or encrypted backups or similar, these procedures can only be carried out after preliminary work.

With these deletion methods, however, it cannot be guaranteed that the data area used specifically has been overwritten with the new data. Especially on SSDs, individual areas of the data memory can be skipped or excluded by the SSD's firmware during new write processes. The previously existing data is not immediately overwritten and remains in the file slack<sup>21</sup>.

In the case of the legal deletion of data after certain periods, this can actually become a problem. Legally, these circumstances are unclear. For example, data from criminals or witnesses must be deleted from the police database after a certain period of time. However, in very few cases is this data irretrievably deleted and could be restored with moderate effort depending on the database type and the underlying file system.

---

<sup>21</sup> More about Slack Space at: [https://it-forensik.fiw.hs-wismar.de/index.php/Slack\\_Space](https://it-forensik.fiw.hs-wismar.de/index.php/Slack_Space).

#### 2.5.4. Deleting in compressed containers

Deleting data in compressed file containers concerns the targeted deletion of data, e.g. in backups. In some cases, automated backup software is available for this purpose, which compares the original directories with the compressed backup directories and removes files that are no longer present. However, this requires unpacking the archive before each data access, which can greatly increase the system impairment due to the more or less intensive compression process. Finally, files that have been removed from a compressed container cannot be restored with common recovery programs. This requires exact knowledge of the compression algorithm used and the other data in the container.

If a secure password with additional encryption of the compressed container has been used, recovery of the deleted data is not possible according to current knowledge.

The TOP 3 data recovery programs (according to [7datarecovery.com](https://7datarecovery.com)<sup>22</sup>: "Pririform Recuva Professional", "508 Disk Drill Pro" and "Pro Soft Data Rescue 5") cannot recover deleted data from or in compressed containers, but only the containers themselves, if they have been deleted.

Deleting data in a container thus increases the security level of the data stored in it, as it cannot be easily recovered by automated means.

Nevertheless, the clear disadvantage is the process of compression, which can severely affect the system load for a long time in the case of large amounts of data. For a user, this delayed data access is often not tolerable in terms of time.

#### 2.5.5. Deleting in encrypted containers

A very specific scenario is the data deletion in encrypted containers like .zip, .xvdh or other storage containers with a secure encryption and password.

---

<sup>22</sup> Taken from <https://7datarecovery.com/de/best-recovery-apps/> at 02.06.2022.

In data security, the usage of encrypted file containers is very recommended. All data in the container can be encrypted by safe and modern encryption algorithms and can be sent on a normal storage device like a hard disk physically. Even sending the container through the Internet is possible without having fear, it can be decrypted easily with a password. Password security strategies are here very important.

There are several applications and container technologies used today.

Here is a selection of container solutions put together by the University of Edinburgh<sup>23</sup>:

- zip (and variations) for Windows
- zip for macOS
- encrypted disk Image for Apple Macs
- Vera crypt containers for Windows, Macs and Linux

Some methods are missing from the list, of which the container format .vhd and .vhdx must be mentioned, which is available as a standard in Windows 10 and Windows 11 systems. The virtual hard disk format allows the creation of encrypted dynamic BitLocker<sup>24</sup> containers that can also be used for security-critical data storage.



Figure 10: Screenshot of an encrypted BitLocker Container in Windows 10/11

When choosing a current encryption algorithm, such as AES 128/256 (MS BitLocker, Apple APFS), Triple-DES, Blowfish, Twofish, an extremely high level of data security can be achieved.

---

<sup>23</sup> From

<https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypted-containers#:~:text=What%20is%20an%20encrypted%20container,it%20to%20an%20email%20message>  
accessed on 13.06.2022.

<sup>24</sup> More about Bitlocker: <https://it-forensik.fiw.hs-wismar.de/index.php/Bitlocker>.

Decryption is only possible if the key is known. Key security is therefore a crucial factor.

If we want to specifically delete data in such a container, the key must of course be known and the container must first be decrypted. After the decryption process, which only causes a small system load and loss of speed, the data in the container can be accessed normally.

But the files in the container cannot be deleted by moving it to the host Recycle Bin because they are not listed in the host file table. Further, the deleted files cannot be restored from external applications using File Carving, because the bit stream is stored in encrypted form on the hard drive and the size of the encrypted data container usually adapts dynamically to the content.

The deletion process in the NTFS file system with BitLocker encryption (decrypted) is illustrated here:

The screenshot shows a hex editor view of a file at sector 329.130. The file is named 'FILE0...f...' and contains the password 'geheimnis password secret'. The password is highlighted in blue in the ASCII view. The hex view shows the raw data of the file.

Figure 11: Screenshot (HxD HexViewer) with Password-File at sector 329.130

After standard-deletion process:

The screenshot shows the same hex editor view after a standard deletion process. The filename 'FILE0...f...' has disappeared, and the file content is now all zeros. The password 'geheimnis password secret' is still visible in the ASCII view, but it is now part of a file that has been deleted.

Figure 12: Screenshot, Password-File at sector 329.130 (only filename disappeared)

After overwriting free space with Eraser application with random data:

The screenshot shows a hex editor view of a file at sector 329.130. The data is in German and includes a password 'geheimnis password secret' and a username 'geheim'. The file name 'FILE0...0' is visible at the top right.

Figure 13: Screenshot, Password-File at sector 329.130 (nothing changed)

Unfortunately, the NTFS file system is again an exception here, like shown above. The data is not completely removed in the usual deletion process, only the file name is removed. Even the Eraser application did not overwrite the file in the encrypted container. An explanation for this condition could not be found to date. The company has not yet responded. Forums discussing that fact, and it could be, that Eraser is not able to access the data area due to user rights.

Nevertheless, this also shows that deleting data in an encrypted container can be difficult. Apparently, file systems and encryption or deletion methods do not harmonize very well. In a dynamic file container, secure deletion by overwriting can even lead to a memory overflow and a system crash, as the dynamic container file keeps growing while the deletion program writes random values or zeros into it.

For the gullible user of encrypted containers, this can also mean that data is almost never deleted. And if the container is regularly backed up completely in the form of a long term backup, the data remains in it and can be easily restored with file carvers after decryption.

## 2.5.6. Deleting in virtual machines

Virtual machines are computer systems that are encapsulated and run on a host system. There are very different variants of this system environments<sup>25</sup>.

<sup>25</sup> More about virtual Systems on [https://de.wikipedia.org/wiki/Virtuelle\\_Maschine](https://de.wikipedia.org/wiki/Virtuelle_Maschine).

In principle, however, the deletion procedures can also be transferred to these virtual computer systems.

One advantage of the virtual systems is the continuous storage space optimization of the virtual system with respect to the host system. The host makes the memory available to the virtual machine, which can request the memory dynamically during live operation. In most cases, this saves the virtual machine data from the host system's point of view in one large file.

Many virtual systems also work with file or file system encryption.

As a result, the data of the virtual system cannot be accessed from outside without the cryptographic key.

However, as soon as you are in the virtual system, you can, for example, access the Recycle Bin or, if necessary, the fileslack with forensic analysis tools. It should be noted that the fileslack of a virtual machine is no longer accessible in most cases when it is shut down. This is where the previously mentioned memory optimization by the host system comes into play. The fileslack of the virtual system is usually overwritten promptly.

However, in many application areas, snapshots or backups of the virtual machines are regularly created in order to jump back to an earlier point in time if the virtual machine is compromised.

Of course, all data at the time of the snapshot is available in the relevant backup and can be viewed during operation.

So we are back in the data protection problem of backups. Is the data deleted if it is still in a backup? This question will not be dealt with here. It turns out, however, that smooth technical operation is not possible without backups. It is certainly advisable to separate user data and the actual operating system and applications in order to remove user data from the backups or store them separately and securely in another way.

## 2.5.7. Deleting of complete hard drives

When people talk about erasing data, they often mean erasing entire hard drives in computer systems. Basically, as the name suggests, these storage media are designed to store data over a certain period of time. This storage process can take seconds or years. The evolution of memory thus went in the directions of longevity, data security and speed. Longevity means the ability to store data over a certain period of time and the ability to be overwritten as often as possible. Data security describes that data must not be accidentally lost due to defects. And the speed is designed to ensure quick access to the data you need.

It can now be deduced from this that in the evolution of hard disks and other storage systems, secure deletion initially played no role. As a selling point, the ability to securely erase didn't play a role either.

So how do we proceed if we want to erase entire hard drives?

The following procedures are common:

- Formatting the hard drive
- Format and change the file system
- Physical destruction of the hard disk

Example result of formatting with FAT12:

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F Dekodierter Text
00000000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 01 04 00 02 00 02 00 08 F8 06 00 01 00 01 00 80 00 00 00 <.MSDOS5.0.....@.....E... Sektor 0
00000020 00 00 00 00 80 00 29 BF 12 92 94 4E 4F 20 4E 41 4D 45 20 20 20 46 41 54 31 32 20 20 20 33 C9 ....E.).g.'NO NAME FAT12 3E
00000040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C 38 4E 24 7D 24 B8 C1 99 E8 3C 01 72 1C 83 EB 3A ZN=0(20..ZAU%.(8N0)S:AM<C.r.fe:
00000060 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 f.).{f:.iSWuu.eE."V.eA.se3E$F."+
00000080 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 f..F..V..F..N<v."hFuWp..,ae^".
000000A0 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 AH=0.Fu.Npag...ee.r948-t."z.N;)0;
000000C0 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0 FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E at2Nt.fC ;UrmeU 0)'(0-"St.Ht.".
000000E0 BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8 ..I.ei y)ee u)eai.I.i<U.R".e...e
00000100 3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6 ;.re{SV9%.(<uCF0=)CF0)@UnNohNoE
00000120 06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8 66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8 .)Ee... .fEr(Fef.F.fCfAe.e..eE
00000140 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB 4A 52 50 04 53 6A 01 6A 10 91 B8 46 18 96 92 33 J3F.2a=a.Fu.Vp&JRP.Sj.j."fF.-3
00000160 D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42 0-0"<08tEv.S0$8A$.I..E*...u."B
00000180 8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 B8 00 00 60 66 6A 00 EB <0SVI.aar.Bu.B.^".Iu.eAa..fj.e
000001A0 B0 42 4F 4F 54 4D 47 52 20 20 20 20 0D 0A 44 61 74 65 6E 74 72 84 67 65 72 20 65 6E 74 66 65 72 *BOOTMR ..Datentz.ger entfer
000001C0 6E 65 6E FF 0D 0A 4D 65 64 69 65 6E 66 65 68 6C 65 72 FF 0D 0A 4E 65 75 73 74 61 72 74 3A 20 54 neny..Medienfehlery..Neustart: T
000001E0 61 73 74 65 20 64 72 81 63 6B 65 6E 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 AC C4 D3 55 AA aste dr.cken.....-AOU*
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... Sektor 1
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000002A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000002C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000002E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000003A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000003C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000003E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Figure 14: View of the first sectors of a formatted hard disk with FAT12 file system



```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F Dekodierter Text
002FFBC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFBE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFC00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFC20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFC40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFC60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFC80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFCA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFCC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFCE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFD00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFD20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFD40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFD60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFD80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFDA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFDC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFDE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFEE0 EB 52 90 4E 54 46 53 20 20 20 00 02 08 00 00 00 00 00 00 00 00 00 00 01 00 01 00 80 00 00 .....
002FFEF0 00 00 00 00 80 00 80 00 FF 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
002FFFA0 F6 00 00 00 01 00 00 89 32 4C 00 35 4C 00 82 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 .....
002FFFB0 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB .....
002FFFC0 55 AA 75 06 F7 C1 01 00 75 03 E9 D0 00 1E 83 EC 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 .....
002FFFD0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 .....
002FFFE0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D .....
002FFFE0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 .....
002FFFE0 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E .....
002FFFE0 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E .....
002FFFE0 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF .....
002FFFE0 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 A1 FA 01 E8 03 00 F4 EB FD B8 F0 AC 3C 00 74 09 .....
002FFFE0 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 44 61 74 65 6E 74 72 84 67 65 72 2D 4C 65 73 65 66 65 68 6C .....
002FFFE0 65 72 00 0D 0A 42 4F 4F 54 4D 47 52 20 6B 6F 6D 70 72 69 6D 69 65 72 74 00 0D 0A 4E 65 75 73 74 .....
002FFFE0 61 72 74 20 6D 69 74 20 53 74 72 67 2B 41 6C 74 2B 45 6E 74 66 0D 0A 00 65 73 74 61 72 74 0D 0A .....
002FFFE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8A 01 A3 01 B9 01 00 00 55 AA .....

```

Figure 15: View of the last sectors of a formatted hard disk with NTFS file system

Formatting a hard drive regenerates the file system and recreates the file allocation table. If formatted correctly, the data area is completely overwritten with zero bits. Start sectors and end sectors are also created. In some file systems, such as NTFS, there are also sectors in which information about the file system or data is mirrored.

It can be said that with such formatting, there is no longer any useful data on the data carrier, and it can not be restored using standard applications<sup>26</sup>.

Thus, one could state that formatting and changing to another file system is sufficient to securely delete data.

Of course, there is one exception that is often used due to speed advantages: the quick format. With quick formatting, only the table of contents of the hard disk or the area to be formatted is set up fresh. The user data is only marked as free and released for overwriting. This data can be recovered using data recovery programs.

Special applications for securely erasing hard drives take a similar approach to formatting a hard drive. When securely erasing hard drives, the goal is to irretrievably erase all data on the device. This is often realized with multiple overwriting or cryptographic erasing. We will see that this process of multiple

<sup>26</sup> Referring to <https://www.heise.de/tipps-tricks/Was-heisst-eigentlich-formatieren-6113765.html>.

overwriting works well on old magnetic hard drives and is just time-consuming. On modern storage devices such as SSDs, however, the sectors are not evenly written or overwritten due to optimization methods in the firmware, so that data cannot be overwritten with this method in a targeted manner.

Logically, hard disks that were booted from cannot be completely overwritten during operation.

We therefore need special applications or special operating systems in order to be able to securely erase these hard drives.

Some hard drive manufacturers have their own secure erase applications [web 17] for their specific hard drive models with direct access to the firmware.

Other hard drive manufacturers recommend simple operating systems with an erase function for securely erasing the hard drives.

Actually, the manufacturers should install a simple method for the deletion in the firmware of their hard drives, but this has not been implemented consistently. The ATA "secure\_erase" command triggers different erasure algorithms on different models, or may not run at all, depending on the connection type or system configuration [11].

In summary, it can be stated that there are various solutions for deleting entire hard drives. It all depends on what scenario you're in. Deletion procedures can be set up from an insecure quick formatting in the private sector or even to multiple overwriting of sensitive data.

Physical destruction of the hard drive is also conceivable. This is already recommended by international standards in critical systems or for damaged devices that should not or cannot be reused.

Even in the private sphere, a hard drive that is no longer working properly should be damaged to such an extent that it can no longer be read with software.

In the case of mechanical hard drives, mechanical damage (e.g. drilling through) of the magnetic discs and the read/write head is sufficient in most cases. In the case of modern solid drives such as SSDs, individual undamaged

very small memory cells could be read out. However, in contrast to the magnetic hard disks, these are thermally more susceptible and lose their consistency at a few 100 degrees Celsius.

### 2.5.8. Deleting by resetting to factory state

Many technical devices can be reset to the factory settings [web 8]. This applies to mobile phones, laptops, PCs and other computer systems.

Nowadays, the manufacturers of these devices have implemented quite secure methods of erasing all user data on the devices in question.

It is therefore not possible to recover the data on properly reset cell phones or laptops using forensic methods or even under laboratory conditions.

However, this deletion by resetting mainly only affects the system memory and the user memory directly on it. Memory extensions or additional storage, such as second hard drives or memory cards, are not securely deleted and can be recovered by file carving applications.

Most of the time, resetting the system involves the following automatic steps when the reset was triggered:

1. Verifying the Data on the recovery partition (not visible)
2. Deleting the user partition or user directory
3. Restarting the system in reset boot mode
4. Formatting the accessible user and system partitions (clearing all data)
5. Copy the basic system data to the system partition
6. Shutting down the system
7. *(First start of the new system: new user setup)*

These or similar processes run by default when resetting a device. These processes are in most cases standard procedures and are performed on the devices after fabrication.

Modern devices often have standard encryption of the main memory. The key is then securely deleted when it is reset. This means that the data cannot be accessed under any circumstances.

According to current research, no data recovery program advertises the recovery of data from a reset device directly. Data can only be restored from (online) backups such as Google or Apple Cloud, etc.

### 2.5.9. Deleting by cyberattacks (“cyberwar”)

In February 2022, a cyberattack was carried out on Ukraine, which contained a program of sabotage or data deletion.

ESET called the malicious software "CaddyWiper" and published screenshots of the source code and reverse engineering on Twitter.

The malware was about the core goals of digital warfare, namely the destruction of infrastructure.

The program was appropriately named "wiper" software, as its main purpose was to erase data to render the system unusable.

Along with other similar weapon-type erasers such as "IsaacWiper", "HermeticWiper", "DoubleZero", "AcidRain", "Industroyer2" and "WhisperGate & WhisperKill", these programs aim at rendering the targeted computer systems unusable<sup>27</sup>.

---

<sup>27</sup> From <https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/>

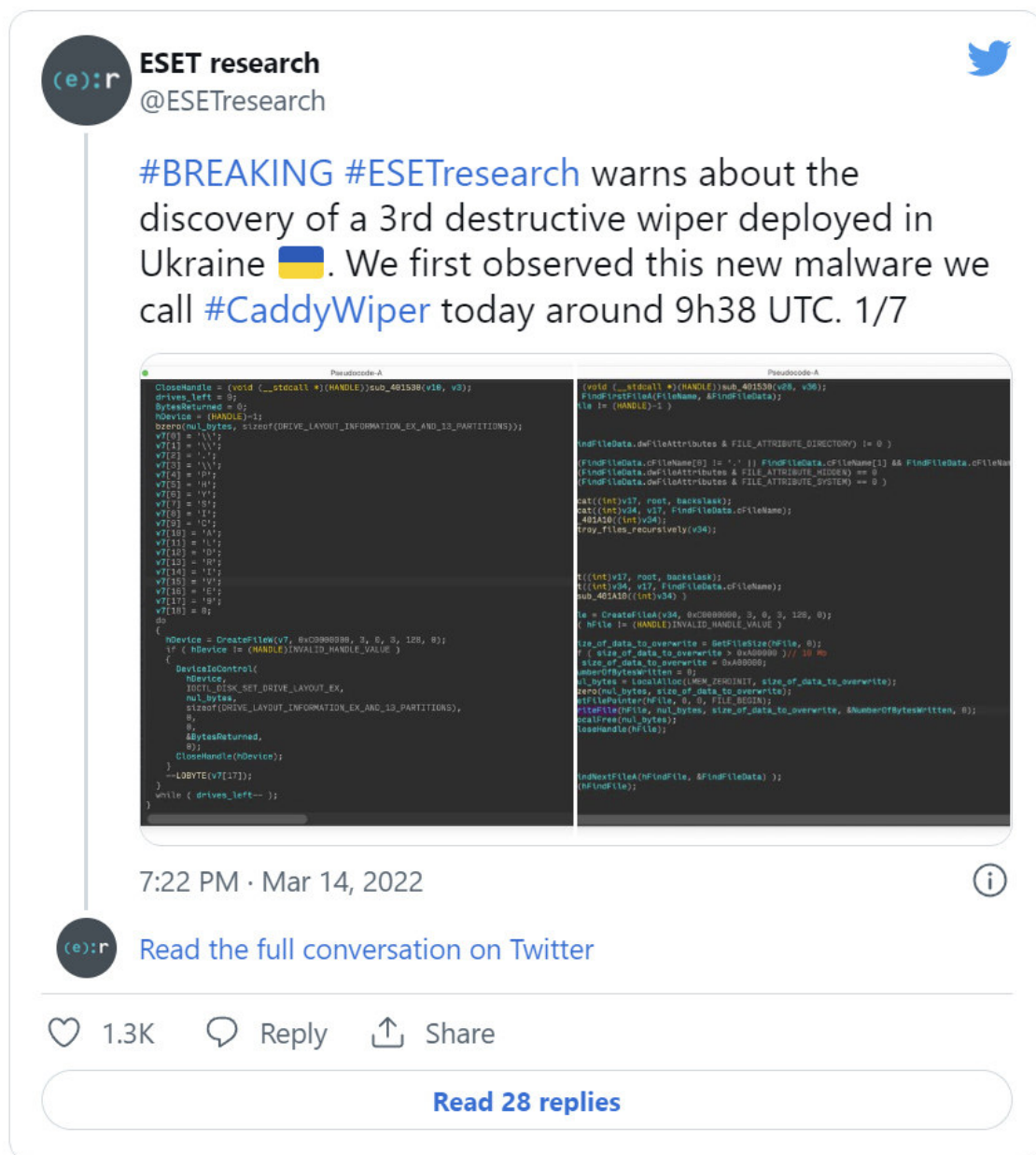


Figure 16: Screenshot of the Twitter-Post from ESET at March 14th

This malware is individually tailored to the specific target and uses different deletion methods. The main point of attack is the user data, which is first attacked, deleted, overwritten or encrypted. Then the operating system and finally the entire memory with the malware itself should be deleted via system rights.

The attack on the satellite network KA-Sat with the wiper malware "AcidRain" shows an example of effectiveness, in which the relevant satellite communication in Ukraine was completely paralysed<sup>28</sup>.

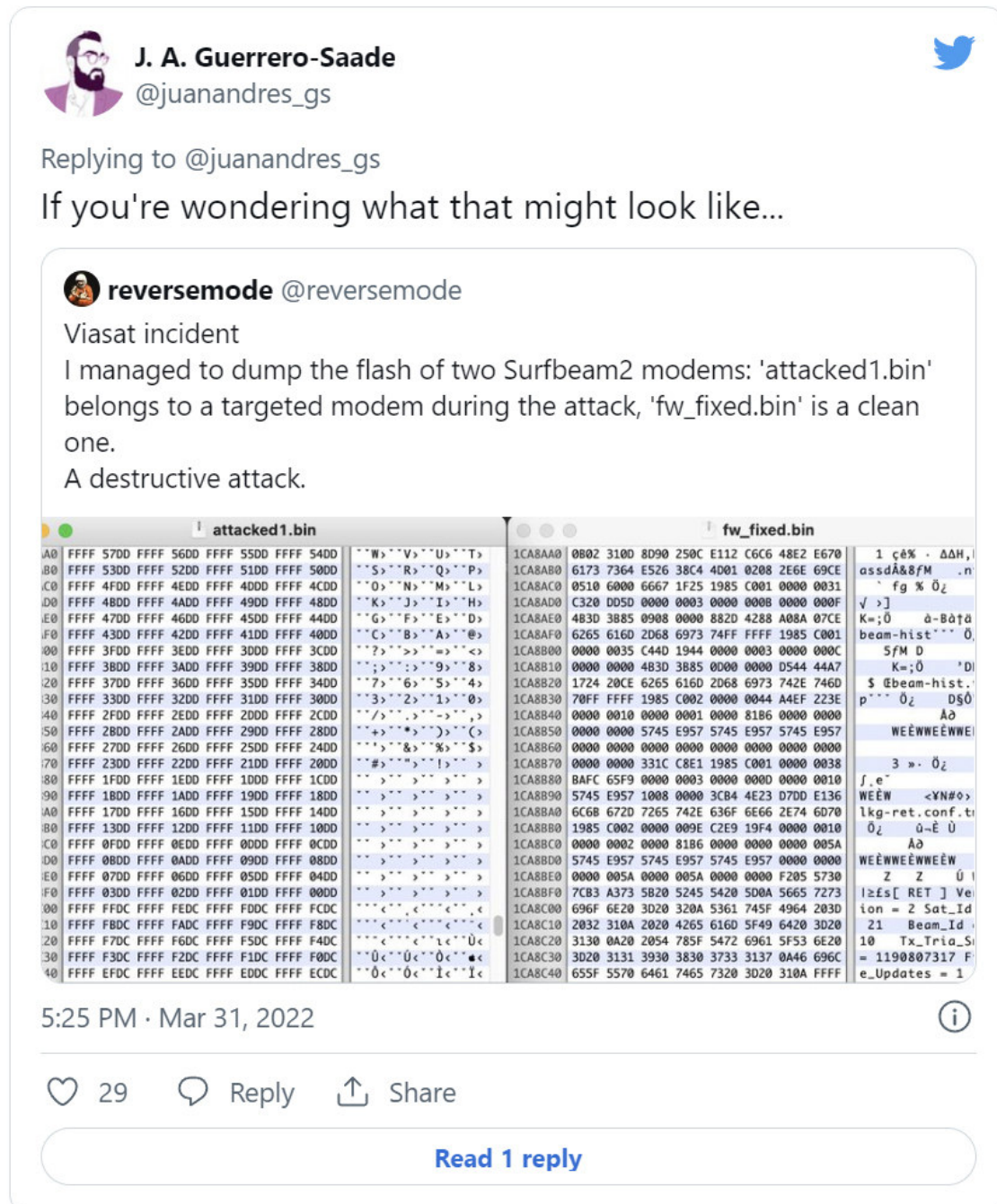


Figure 17: Screenshot of the Twitter Post with attacked file by "AcidRain"

<sup>28</sup> From <https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/>

We can see at the screenshot above, how deletion procedures on byte level is used to destroy the data.

To date, no amounts of damage caused by these attacks have been officially published. However, it can be assumed that the damage caused by the wiper attacks in spring 2022 is in the range of several hundred million dollars and that the damage is not limited to Ukraine.

Due to the current war situation, there is hardly any public information about the exact mode of action of the malware used and its defence techniques.

This topic will not be explored further in this thesis.

The use of deletion algorithms for cyber warfare shows that there are sensitive vulnerabilities in informational systems. Knowledge of deletion methods and their individual function must be taken into account in critical infrastructure in order to be able to better assess attacks.

## 2.5.10. Deleting Data in Cloud Storage

Cloud storage is a remote storage solution via network connections of a cloud storage provider. In the storage centres of the cloud provider, the user data is stored in a storage area of the cloud. Depending on the user's needs, a maximum storage size is defined and the user rents this storage area.

There are also multiple redundant storage solutions and very fail-safe storage architectures (such as Raid systems).

Physically, (at least) one copy of the user's data thus exists with the cloud provider.





Figure 18: Photograph<sup>29</sup> of File server in a storage centre of the Microsoft Azure Cloud.

The user receives different file rights on the server. However, the user does not receive exclusive write access or even access to the firmware of the individual hard drives. Deleting files in a cloud system is therefore only possible logically. How the data is actually stored depends on the structure and architecture of the cloud system.

In a distributed file system (DFS) or a network file system (NFS), the logical data is stored on several network storage devices.

With redundant raid systems, failed hard disks can be replaced during operation without any loss of data.

This suggests differences in the deletion of data on these storage solutions.

In a cloud, no hard disks can be completely deleted, as there is no exclusive right to write and, as a rule, data from other users is also stored there.

Likewise, a targeted overwriting of data is not possible, as the memory is directly released again during deletion and is promptly filled with other useful data within the scope of memory optimization (defragmentation). Small memory

---

<sup>29</sup> Photography available at

<https://news.microsoft.com/de-ch/2021/06/10/neue-services-aus-den-schweizer-datencentern-d er-microsoft-cloud/> from 01.05.2022



areas at the end of the new data remain unwritten, and there may be user data fragments in this file slack.

A common approach to data security is the basic encryption of the user data containers. The user data of each user are encrypted differently with their security factors and cannot even be read by the cloud provider. Since the file slack also contains only encrypted file fragments, a readout would be unsuccessful if the key is unknown.

In this context, cloud providers work with strong encryption methods.

For example, the encryption methods of the Microsoft Azure Cloud with AES 256 bit, BitLocker or dm-crypt are available. These encryption methods are aimed at encrypting data containers and can be classified as extremely secure.

In summary, it can be stated that data security in cloud storage is the responsibility of the cloud provider. Interventions in the deletion process are not possible by the end user - if no Recycle Bin solution is offered.

The currently common encryption methods allow for the secure storage of data in the cloud, and thus also the secure deletion of data in the cloud. Nevertheless, data can be read when the decryption key becomes known or during a decrypted copying process, but this is not the subject of this paper with regard to the deletion problem.

## 2.5.11. Deleting by Formatting a device

Formatting is a popular method of deleting complete storage devices such as hard drives or memory cards. The storage device is prepared to accept data by creating sectors and finally creating the file system with the typical organizational structures.

Modern common formats of file systems are:

	File System	Compatibility (with additional Drivers/Software)	Native Compression and Encryption Options
NTFS	New Technology File System	Windows since 1993, Linux, macOS	optional encryption and compression
FAT 12/16/32	File Allocation Table	DOS since 1977, Windows, Linux	no
exFAT	Extended File Allocation Table	Windows since 2006, (macOS, Linux)	no
APFS	Apple File System	Apple macOS since 2016 (Windows)	optional encryption and compression
HFS+	Hierarchical File System	Apple macOS since 1998 (Windows, Linux)	possible encryption and compression
Btrfs	B-tree File System	Windows since 2007, Linux	possible compression and encryption <sup>30</sup>
ext 2/3/4	Extended File System	Linux since 1992 (Windows, Mac OS)	optional encryption with ext4
ZFS	Zettabyte File System	Unix, Mac OS, (Windows)	possible encryption and compression

Table 3: Overview over some common file systems (by F. Weijers)

The table above shows an extract from the file systems that are used on current computer systems. There are various versions of the individual file systems that can exhibit incompatibilities.

For the aspect of deleting data, the table contains the column encryption and compression, because active encryption and an option for compression have a strong impact on the actual deletion of data within the file system.

If a data medium has been encrypted with a secure key and this key is deleted, the data on the data medium is completely lost, and the device is to be regarded as deleted because the data cannot be viewed again.

<sup>30</sup> From <https://btrfs.wiki.kernel.org/> accessed on 17.05.2022

However, if the encryption is not available or the data medium is unlocked, the file system with all its individual functions can be accessed. File carving on the decrypted data is also possible to recover accidentally deleted files.

Many file systems also have intelligent mechanisms for memory optimization and error correction, up to automatic defragmentation processes. Bad sectors are marked and skipped in future write accesses. Data is aggregated to locally optimize storage areas and to speed up the data access. The prior aim of these optimization techniques is to increase the speed and data security or service life of the data carrier. However, an important factor here is the minimization of write and read access. Many write accesses would wear out the data carrier faster and because secure erase processes require overwriting of the data, these secure erase processes often fall victim to prior optimization techniques.

Some file systems also create duplicate files in order to be able to restore the file contents if necessary. A popular example is the NTFS file system. So-called mirror files are stored here in the free storage area of the NTFS-partition for security benefits. The file content remains (this is shown in point 2.6.5.) and is initially not overwritten until the entire storage space runs out. These basic functionalities make a targeted deletion process quite difficult, because a secure deletion can only be carried out with exact knowledge of the underlying file system.

In the file systems shown, a quick delete process prevails by default. The file name is simply removed from the journal or file mapping table and the file's storage space is marked as free. This deletion process is extremely fast - but also extremely insecure. The question is whether this process can actually be described as deleting, or whether it should only be seen as a preliminary stage of forgetting.

Anyway, changing the file system is a good method to permanently erase the contents of the data storage. The mapping table or the journal is set up again and all sectors are overwritten with zero bits or untouched organization data from the file system.

Windows also allows a quick format option, in which only the mapping table and organizational structures of the NTFS file system are written to disk. The other

sectors remain untouched and the data on them are not initially overwritten, although the sectors are all marked as free.

The next step is to look at a FAT device with a password file on it.

The device is being formatted and analysed, whether data remains on that device:



Figure 19: Screenshot of the concerned data area in a FAT file system

There is the data “mypassword” stored in sector 53.

Now the device is formatted with fast formatting FAT and look on the device:



Figure 20: Screenshot of the concerned data area in a FAT file system after fast formatting

Unfortunately, the “mypassword” data remains in sector 53.

Only the mapping table was set up new, and the whole partition was marked as free.

The next step shows the formatting using FAT:



Figure 21: Screenshot of the concerned data area in a FAT file system after normal format

The Screenshot shows that the data “mypassword” is gone at sector 53 and cannot be found on the partition.

Nerds can try to format partitions in different file systems, and vice versa. So take a look at one example. Let's say, we have a password file in a exFAT file system and then fast format that to NTFS. Can somebody get access to the password-data after deleting in a exFAT file system?

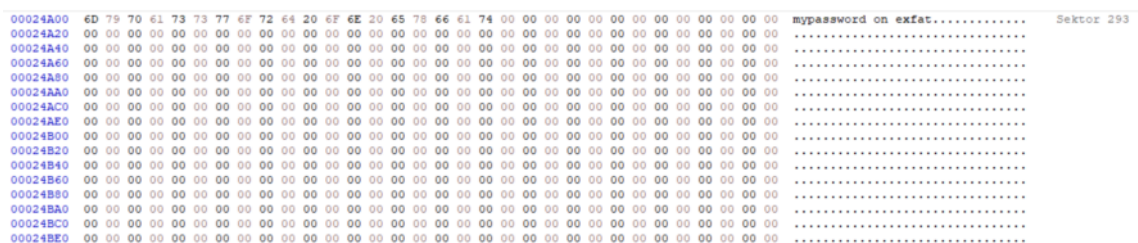


Figure 22: Screenshot of the concerned data area in a exFAT file system

Then formatting to NTFS with fast format:



Figure 23: Screenshot of the concerned data area in the NTFS file system

It can be seen that even fast formatting erased the password file completely. The searching for fragments was negative on the whole device.

Last try with formatting is now a password file on a NTFS file system and then formatting the device to FAT. Let's take a look, whether we can find the data after fast formatting.

Figure 24: Screenshot of the “mypassword” file on the NTFS file system

Then doing a fast format to FAT16:

Figure 25: Screenshot of the concerned data area in the FAT file system after fast format

The data remains here at sector 31.478.

And with normal formatting:

Figure 26: Screenshot of the concerned data area in the FAT file system after normal format

There is no user data left at sector 31.478 (or elsewhere on the drive).

As a result, it can now be definitely said that formatting a disk is not a safe option for erasing data. It all depends on which file system you are in, whether

the file system is encrypted or compressed, and in which file system you carry out the new formatting with which options. There is no gain in time either, because a quick formatting is also the most insecure way.

One option when selecting the file system should currently always be encryption if you want to securely delete data. With this, you can really quickly delete all data in the file system if only the key to it is deleted. There is more to read in this work under the term cryptographic erase.

## 2.6. Software solutions

We would now like to come to the more practically oriented methods and deletion procedures, which can be very interesting for an average user of PC systems.

System administrators and data protection officers must also familiarize themselves with the topics of secure data separation. In the following, however, this is not a programming course for sophisticated deletion methods, but a selection and compilation of common deletion programs. These are usually available free of charge for Windows and Linux via various downloads and can already be used by beginners. However, most tools assume a certain level of familiarity with erasure procedures. The terms wipe, random numbers, sanitization, etc. should be familiar to the user. Furthermore, operating errors can have fatal consequences and render the entire computer system unusable within seconds. And I'm speaking from personal experience as well.

There is a long list of special applications for erasure processes. The following table<sup>31</sup> provides an overview:

<b>Application</b>	<b>Systematics<sup>32</sup></b>	<b>Wiping Functions<sup>33</sup></b>
DBAN (Darik's Boot and Nuke)	Boot (Linux)	hard drives
CBL Data Shredder	Boot, Windows	(non system) hard drives
MHDD	Boot	hard drives
KillDisk	Boot, Windows, Linux, macOS	hard drives (or free space)
format /p:1	Windows, DOS	(non system) hard drives
Macroit Data Wiper	Windows	(non system) hard drives / free space
Eraser	Windows	(non system) hard drives / files / folders / free space
Freeraser	Windows	files / folders
Disk Wipe	Windows	(non system) hard drives
Hardwipe	Windows	(non system) hard drives
Secure Eraser	Windows	(non system) hard drives
PrivaZer	Windows	(non system) hard drives / files / folders
PC Shredder	Windows	folders / drives
AOMEI Partition Assistant	Windows	(non system) hard drives
Remo Drive Wipe	Windows	(non system) hard drives
CCleaner	Windows	files / free space / (non system) hard drives
File Shredder	Windows	files / folders
Hard Drive Eraser	Windows	(non system) hard drives
Super File Shredder	Windows	(non system) hard drives

---

<sup>31</sup> From <https://www.lifewire.com/free-data-destruction-software-programs-2626174>.

<sup>32</sup> Means, whether to start the application (boot means, that it has a bootable media option).

<sup>33</sup> All tools support different secure overwriting procedures, but they can not access the drive, that they were booted on completely.



TewakNow SecureDelete	Windows	files / folders
MiniTool Drive Wipe	Windows	(non system) hard drives
XT File Shredder Lizard	Windows	(non system) hard drives / files / folders
WipeDisk	Windows	(non system) hard drives
Puran Wipe Disk	Windows	(non system) hard drives
BitKiller	Windows	(non system) hard drives
Simple File Shredder	Windows	files
Ashampoo WinOptimizer	Windows	files / folders
AbsoluteShield File Shredder	Windows	files / folders
DeleteOnClick	Windows	files / folders
CopyWipe	Boot, DOS, Windows	hard drives, non system hard drives (Windows, DOS)
SDelete	Windows, DOS	(non system) hard drives
Wise Care 365	Windows	files / folders
ProtectStar Data Shredder	Windows	files / folders
hdparm	Windows, Linux	(non system) hard drives
HDS shredder	Boot, Windows	(non system) hard drives

Table 4: List of Wiping Software (from lifewire.com)

The list above shows that there are fundamentally different strategies for deleting data. These strategies are, on the one hand, methods of erasing of entire hard drives and, on the other hand, erasing of files and folders. This is ensured by applications that either run in the original operating system or that can be booted from an extra medium. The system partitions can only be completely erased if the system was booted externally.

In the following, we will take a look at applications that use different methods and systems for the erasing process.

### 2.6.1. Unix: “wipe”

Wipe is a powerful and user-friendly command line application for securely erasing data on Debian Linux and was developed by Berke Durak, Juao Eriberto Mota Filho and Runa Sandvik around 2009.

Current Version:	wipe 0.24 from 02.11.2016
Features:	Secure deletion of files or data carriers by multiple overwriting with random data.
Options:	<ul style="list-style-type: none"><li>- recursive deletion</li><li>- progress indicator</li><li>- Choice of wipe passes</li><li>- Do not delete file names</li><li>- Overwrite file with 0</li></ul>
Web:	<a href="https://github.com/berke/wipe">https://github.com/berke/wipe</a> <a href="https://wiki.ubuntuusers.de/wipe/">https://wiki.ubuntuusers.de/wipe/</a>

Table 5: Details of the Wipe program for UNIX (from [wiki.ubuntuusers.de/wipe](https://wiki.ubuntuusers.de/wipe/))

Example of deleting a file by overwriting with zeros:

```
sudo wipe -q -Q 1 -R /dev/zero -S r -r $path
```

In practice, wipe in the above configuration proves to be quite performant and suitable for deleting files or individual directories.

The wiped files or directories are not recoverable by file carving.

Alternatives for deleting files are the program “shred” or “secure delete” and the Linux command “dd” for deleting entire data carriers.

## 2.6.2. Unix: “shred”

Shred is a second Linux application for secure deletion by overwriting using the Gutmann method or other overwriting algorithms, and is included in Linux coreutils by default.

It was originally developed by Colin Plumb in 1997 and was written in C.

Current Version:	coreutils v 9.0 from 09/2021
Features:	Unrecoverable deletion of files or data carriers by multiple overwriting with random data.
Options:	<ul style="list-style-type: none"> <li>- progress indicator</li> <li>- Number of overwrites</li> <li>- Overwrite file with Zeros</li> </ul>
Web:	<a href="https://github.com/wertarbyte/coreutils/blob/master/src/shred.c">https://github.com/wertarbyte/coreutils/blob/master/src/shred.c</a> <a href="https://wiki.ubuntuusers.de/shred/">https://wiki.ubuntuusers.de/shred/</a>

Table 6: Details of the coreutils program for Linux (from [wiki.ubuntuusers.de/shred/](https://wiki.ubuntuusers.de/shred/))

Example of deleting a file by overwriting with zeros:

```
sudo shred -v -n 0 -R -z <device>
```

In practice, shred has proven to be very performant in the above configuration and suitable for overwriting files, directories or drives with zero bits or random numbers. Complete blocks are overwritten with zeros, which prevents conclusions about the exact former file size.

Alternatives for deleting files and directories are the program “wipe” or “secure delete” and the Linux command “dd” for deleting entire data carriers.

### 2.6.3. Unix: “secure-delete

Secure-Delete is a Linux toolbox for securely deleting data in files, directories, drives or partitions by (multiple) overwriting. The tools were developed by Marc Heuse (“van Hauser” [www.thc.org](http://www.thc.org)).

It includes the following commands:

Version:	secure-delete v 3.1
srm	secure-remove (Deletes data by overwriting with random numbers)
(smem)	secure clean memory (clears memory)
sswap	secure swap-delete (Deletes the swap partitions in Linux systems)
sfill	secure fill (Fills the free-marked memory with random data)
Features:	Unrecoverable deletion of files, partitions, disks or memory by multiple overwriting with random data.
Options:	<ul style="list-style-type: none"> <li>- progress indicator</li> <li>- Recursive deletion</li> <li>- Set the overwrite operations</li> <li>- choice of method</li> <li>- Overwrite file with 0x00</li> </ul>
Web:	<a href="https://www.systutorials.com/docs/linux/man/1-srm/">https://www.systutorials.com/docs/linux/man/1-srm/</a> <a href="https://linoxide.com/delete-files-permanently-linux/">https://linoxide.com/delete-files-permanently-linux/</a> <a href="http://srm.sourceforge.net/srm.html">http://srm.sourceforge.net/srm.html</a>

Table 7: Details of the secure-erase application for Linux (from [srm.sourceforge.net/](http://srm.sourceforge.net/))

Example of deleting a file by overwriting it with 0x00:

**`sudo srm file -s`**

The application is quite suitable for deleting files and recursive directories. It can use various methods (e.g. Gutmann 35-fold overwriting) to erase data.

Alternatives for deleting files, directories and drives are the program “wipe” or “shred” and the Linux command “dd” for deleting entire data carriers.

The functionality of smem could not be confirmed in current tests. There was no write access to the complete main memory - probably because of protected areas of the current Linux kernel for system security reasons.

#### 2.6.4. Firmware: “secure-erase”

In order to be able to securely erase hard disks, a method in the command set of the hard disks was mainly required by US authorities.

So it came about that all hard drive manufacturers offered a method for securely erasing data. An ATA command “secure erase” was also introduced. Unfortunately, it was not defined how data should be securely erased and which procedures the “secure erase” command should trigger.

On SSDs, all memory cells should be addressed and written with random data or zero bits. It is therefore about irretrievably completely deleting or resetting an SSD.

This means that individual files or areas of the hard disk cannot be specifically addressed with the “secure erase” command.

Secondly, it is up to the manufacturers of SSDs how they initiate or implement this process.

For example, primary hard disks from which the operating system is running cannot initially be erased using the “secure erase” command. The manufacturer recommends booting from another disk and starting the deletion procedure via

DOS or UNIX instructions, which feels like taking a spooky journey back in time to 1994<sup>34</sup>.

Almost all hard disk manufacturers have small utilities for secondary hard disks that are supposed to trigger a "secure erase". First, the command is sent to the hard disk, which then triggers the deletion via its firmware.

Some hard disk manufacturers advertise their erasure processes as "enhanced secure erase", which is intended to suggest an even better erasure. However, the actual erasing routines can vary greatly from manufacturer to manufacturer and can even be quite different from model to model.

There are different tools<sup>35</sup> for applying the "secure erase" processes from Corsair, Crucial, Intel, Samsung, IBM, Western Digital, OCZ (Toshiba), Plextor, Kingston, Patriot, SanDisk, ADATA, and others.

The deletion procedures of the manufacturers IBM, Samsung, Western Digital, SanDisk, Micron, Toshiba and Lenovo were queried as examples in order to clearly describe the terminology of a secure erase or a cryptographic erase.

IBM<sup>36</sup> describes this process as "secure data deletion" and, depending on the type of hard disk, performs a cryptographic erase, a block erase or a random overwrite process (with the Linux tool `hdparm`).

Samsung sporadically shows a deletion method of a secure erase using its own operating program "Samsung Magician 7". Technically, the deletion method is not discussed. After all, it is a DOS program "Samsung SSD Secure Erase v 1.0".

---

<sup>34</sup> Last standalone DOS release MS-DOS 6.22.

<sup>35</sup> From <https://ssdblog.de> accessed on 21.05.2022.

<sup>36</sup> From <https://www.ibm.com/docs/en/flashsystem-7x00/8.3.x?topic=to-secure-data-deletion> on 02.05.2022.

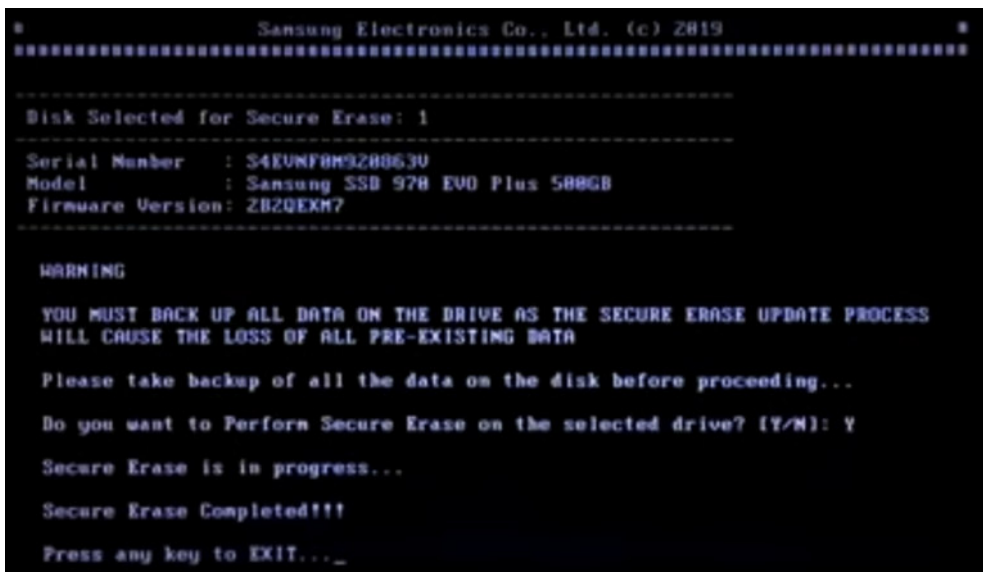


Figure 27: Screenshot of a secure erase process by the Samsung erasing Application from a YouTube Video<sup>37</sup>

Seagate<sup>38</sup> calls its own secure deletion process “Instant Secure Erase” and thus describes a cryptographic erase of its own model hard drives using hardware encryption. In the course of deleting a hardware-encrypted hard drive, only the decryption key that is located in a secure and isolated storage area of the hard drive is securely deleted.

SanDisk describes the secure erase and sanitize deletion processes on the company website<sup>39</sup> as follows:

#### Was ist der Unterschied zwischen Secure Erase und Sanitize?

Secure Erase unterscheidet sich von Sanitize, da es lediglich die Mapping-Tabelle löscht, nicht aber alle beschriebenen Blöcke. Sanitize löscht die Mapping-Tabelle und alle beschriebenen Blöcke. Daher wird Secure Erase schneller abgeschlossen als Sanitize. Nachdem Sie das Laufwerk mit Secure Erase oder Sanitize gelöscht haben, werden alle Benutzerdaten endgültig auf dem gewählten Laufwerk zerstört. Diese Daten können nicht wiederhergestellt werden.

Figure 28: Screenshot from the SanDisk Website for describing the differences between secure erase and sanitize

---

<sup>37</sup> From [https://youtu.be/bjBJ2Vl7j\\_s](https://youtu.be/bjBJ2Vl7j_s) Min 4:51, accessed on 03.04.2022.

<sup>38</sup> From <https://www.seagate.com/gb/en/tech-insights/how-to-ise-your-drive-master-ti/> accessed on 30.03.2022.

<sup>39</sup> From [https://kb-de.sandisk.com/app/answers/detail/a\\_id/16422/~was-ist-der-unterschied-zwischen-secure-erase-und-sanitize%3F](https://kb-de.sandisk.com/app/answers/detail/a_id/16422/~was-ist-der-unterschied-zwischen-secure-erase-und-sanitize%3F) accessed on 30.03.2022.

It should be noted that this statement should be viewed as critical, since the data can currently be recovered even with free data recovery software even if the file allocation table is missing.

Micron describes the erasing processes on the hard drives on the website in detail<sup>40</sup>. An enhanced security erase is carried out on compatible Micron hard drives as a cryptographic erase:

**Note:** If supported by the SSD, the utility will prompt you to select the enhanced secure erase method.

On Micron M500, M510, and M550 SSDs, selecting the enhanced method will execute a cryptographic erase. This operation replaces the SSD's 256-bit encryption key, but will not actually erase any data. This effectively makes all user and operating system data unreadable because the data cannot be decrypted using the new encryption key. This method does not return the SSD to its FOB performance state.

Figure 29: Screenshot from the Technical Note TN-FD-29 "Running Secure Erase on Micron SSDs" Page 4

Micron describes various software-based well-known overwriting routines with 0 bits, random bits, etc. as further secure deletion methods.

It is not apparent that Micron uses its own firmware-based deletion algorithm (e.g. block erase).

The manual for the Western Digital SSD hard drives<sup>41</sup> describes, that secure erase deletes the mapping table on the hard drive and the individual data blocks are not cleaned up:

### Erase Drive—Secure Erase

Secure Erase permanently destroys all user data on the selected SSD.

**Note:** Secure Erase deletes the mapping table on the selected SSD, but it does not erase all blocks that have been written to. This makes Secure Erase a faster "erase" option than the Sanitize function (also see Sanitize).

Figure 30: Screenshot of the "Western Digital SSD Dashboard" User Manual, Page14

---

<sup>40</sup> <https://www.micron.com/about/blog/2017/march/how-to-securely-erase-micron-sata-ssds>  
"How to securely erase Micron SATA SSDs - why data sanitization matters" by Jon Tanguy,  
14.03.2017, accessed on 02.05.2022

<sup>41</sup> From <https://wddashboarddownloads.wdc.com/wdDashboard/um/4779-705161.pdf>,  
accessed on 02.05.2022



Furthermore, Western Digital suggests wiping the hard drives with "Sanitize", which corresponds to an overwriting process with 0 bits.

As a third deletion method, Western Digital mentions an "Erase Drive" of the WD Black PCIe SSD's, which also only deletes the allocation table of the data carriers on this special model.

Toshiba<sup>42</sup> also has a secure erase mechanism in its hard drive models. For this, however, only the tool "Toshiba Storage Utilities" is described by the manufacturer, which is supposed to trigger the secure erase. According to the description of the method in the user manual, it should be a version of the hdparm tool, which is intended to trigger a secure erase, an enhanced secure erase, a block erase or a cryptographic erase. It seems that only Windows 7 is fully supported in the current version:

	Windows 7	Windows 8.1 Windows 10
Normal Secure Erase	Support	Non-support
Enhanced Secure Erase	Support	Non-support
Block Erase	Support	Non-support
Cryptographic Erase	Support	Non-support

Figure 31: Screenshot of the manual of the latest Toshiba Storage Utilities v. 3.11

It should also be noted that the current operating instructions for Toshiba hard drives no longer deal with a secure deletion process.

Finally, the manufacturer Lenovo<sup>43</sup> should also be presented with regard to its deletion strategies. A deletion function "securely erase" is described directly in the BIOS of different PC or laptop systems from the manufacturer.

---

<sup>42</sup> From

[https://personal.kioxia.com/content/dam/kioxia/shared/software/storage-utilities/StorageUtilities311\\_Manual\\_ENG.pdf](https://personal.kioxia.com/content/dam/kioxia/shared/software/storage-utilities/StorageUtilities311_Manual_ENG.pdf) accessed on 02.05.2022

<sup>43</sup> More on

[https://download.lenovo.com/pccbbs/thinkcentre\\_pdf/thinkstation\\_ssd\\_secure\\_erase\\_v1.0.pdf](https://download.lenovo.com/pccbbs/thinkcentre_pdf/thinkstation_ssd_secure_erase_v1.0.pdf)

## Lenovo uses a “Drive Erase Utility” for DOS:

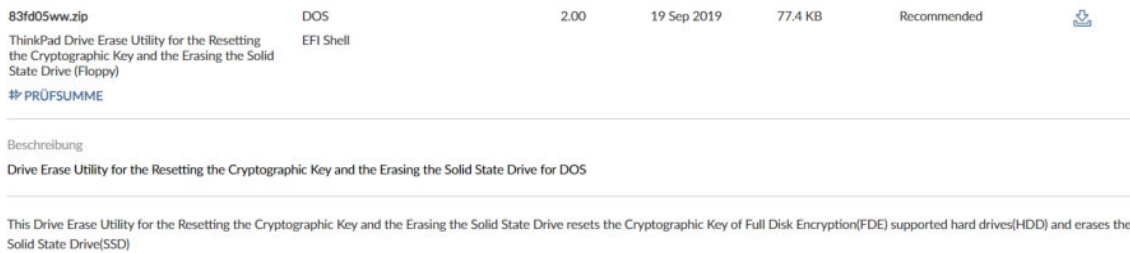


Figure 32: Screenshot of the description of a secure erase at the support webpage of Lenovo.com with reference to Drive Erase Utility for DOS (09/2019)

In summary, it can be said that the terms “secure erase”, “security erase”, “drive erase”, “enhanced secure erase” are not clearly defined across manufacturers. This obviously results from the original requirements of the US authorities for a secure erase.

The security of the deletion process cannot be concluded from this term. Western Digital shows that the completely insecure deletion method of deleting the file allocation table can be designated as a secure erase. In contrast to this, the deletion method of a cryptographic erase can usually be described as quite secure if a secure encryption method, a long key was selected and the key cannot be read (spied on) from the data carrier. In current SSDs with controller-based hardware encryption, the function of a cryptographic erase in the firmware is becoming more and more common. The use of high-performance XTS-AES 128 encryption with a 256-bit key can be observed. However, the encrypted data remains on the hard drive. Only the key is irretrievably deleted. The advantage of this deletion method is a very high speed due to the lack of write access in the data area of the permanent memory.

It can be guessed that the standardization of a secure deletion process has obviously not taken place here.

In addition, the control of the command to the firmware has classic hurdles. The command cannot be sent to the hard disk if it is connected via USB or as a NAS. The hard drive must be connected to the computer via ATA, SATA or eSATA.

Furthermore, not all areas of the hard disk can be reset using "secure erase". Deleting the S.M.A.R.T. values is not possible.

### 2.6.5. Windows Software: "Eraser"

For MS Windows there is some software that is supposed to apply secure deletion processes. As an example of these applications, the software "Eraser" for Windows in version 6.2.0.2993 from 05.10.2021 shall be explained here. The detailed description and download can be found at <https://eraser.heidi.ie>. Alternative programs with a similar mode of operation are "fileshredder" from <https://fileshredder.ord> and "freeraser" from <https://freeraser.com> and others. These programs provide a user interface for different methods of overwriting data and thus deleting it irretrievably.

File wiping process with Eraser on a FAT16 File System:

#### 1. MASTER FILE TABLE (target file: "data.txt")

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00008176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00008192	4D	49	4E	49	5F	44	49	53	4B	20	20	08	00	00	00	00	MINI_DISK ■.... Sektor 16
00008208	00	00	00	00	00	00	0E	4D	B0	54	00	00	00	00	00	00	.....M.T.....
00008224	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B .I.n.f.o.o.r.r.
00008240	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m.a.t.i.o...n...
00008256	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	S.y.s.t.e.o.rm.
00008272	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	.V.o.l.u...m.e.
00008288	53	59	53	54	45	4D	7E	31	20	20	20	16	00	A7	0D	4D	SYSTEM~1 -.*M
00008304	B0	54	B0	54	00	00	0E	4D	B0	54	02	00	00	00	00	00	T.T...M.T.....
00008320	44	41	54	41	20	20	20	20	54	58	54	20	18	61	2E	4D	DATA TXT ja.M
00008336	B0	54	B0	54	00	00	2F	4D	B0	54	04	00	62	00	00	00	T.T../M.T+.b...

Figure 33: Screenshot of the master file table of a FAT16 file system

## 2. DATA CONTENT (file "data.txt" at offset 25600, sector 50)

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00025584	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00025600	FF	FE	2A	00	2A	00	2A	00	53	00	45	00	43	00	55	00	■*.*.*.S.E.C.U. Sektor 50
00025616	52	00	45	00	44	00	41	00	54	00	41	00	2A	00	2A	00	R.E.D.A.T.A.*.*.
00025632	2A	00	50	00	41	00	53	00	53	00	57	00	4F	00	52	00	*.P.A.S.S.W.O.R.
00025648	44	00	2A	00	2A	00	2A	00	4B	00	45	00	59	00	2A	00	D.*.*.*.K.E.Y.*.
00025664	2A	00	2A	00	53	00	45	00	43	00	55	00	52	00	45	00	*.*.S.E.C.U.R.E.
00025680	44	00	41	00	54	00	41	00	2A	00	2A	00	2A	00	0D	00	D.A.T.A.*.*.*.J.
00025696	0A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	■.....

Figure 34: Screenshot of the file content in a FAT16 file system

## 3. MFT after wiping process:

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00008176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00008192	4D	49	4E	49	5F	44	49	53	4B	20	20	08	00	00	00	00	MINI_DISK ■.... Sektor 16
00008208	00	00	00	00	00	00	0E	4D	B0	54	00	00	00	00	00	00	.....MFT.....
00008224	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B .I.n.f.o.®.rr.
00008240	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m.a.t.i.o...n...
00008256	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	OS.y.s.t.e.®.rm.
00008272	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	.V.o.l.u...m.e.
00008288	53	59	53	54	45	4D	7E	31	20	20	20	16	00	A7	0D	4D	SYSTEM~1 -.*M
00008304	B0	54	B0	54	00	00	0E	4D	B0	54	02	00	00	00	00	00	MFT..MFT.....
00008320	E5	41	54	41	20	20	20	20	54	58	54	00	18	00	00	08	DATA TXT.↑...■
00008336	21	00	21	00	00	00	00	08	21	00	00	00	00	00	00	00	!..!....■!.....
00008352	24	52	45	43	59	43	4C	45	42	49	4E	16	00	3C	F4	4D	\$RECYCLEBIN-< M
00008368	B0	54	B0	54	00	00	F5	4D	B0	54	05	00	00	00	00	00	MFT..MFT.....
00008384	E5	36	00	39	00	7B	00	4E	00	4A	00	0F	00	3F	79	00	σ6.9.{.N.J.®.?y.
00008400	7E	00	58	00	00	00	FF	FF	FF	FF	00	00	FF	FF	FF	FF	~.X... ..
00008416	E5	39	7B	4E	4A	59	7E	58	20	20	20	20	00	00	00	08	σ9{NJY~X ...■
00008432	21	00	21	00	00	00	00	08	21	00	00	00	00	00	00	00	!..!....■!.....

Figure 35: Screenshot of the master file table after file wiping with Eraser

## 4. DATA CONTENT after wiping (offset 25600, sector 50)

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00025584	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00025600	D4	3B	18	B4	44	AC	EE	65	5C	4E	A4	35	28	15	A1	77	l; i} D4:ee\Nñ5 (\$iw
00025616	0C	12	4B	32	08	1D	A8	76	A9	A8	29	29	DF	DF	82	1B	*;K2□→zVr-ç)) ■é-
00025632	E4	DD	6E	C3	55	C4	25	14	FA	84	14	AB	83	6E	34	1C	E] n}U-§q·äq\$ân4L
00025648	C5	30	EE	C2	16	AC	A3	11	F2	7A	1C	9E	8E	99	A2	0E	+0eT→üçzL BAÖóJ
00025664	3E	B7	19	3A	DA	C4	9F	E7	C7	3C	1E	87	BB	8E	5D	90	>_l: rfr <▲çqÄ)É
00025680	B1	E5	C0	13	85	8E	B9	DF	4F	82	CE	A3	DB	D7	F9	1A	≡σL!!âÄq■Oéq-ü  ·→
00025696	70	69	55	9F	64	32	9B	AA	F9	B2	7E	68	AE	76	95	A3	piUfd2c-·■~h«vòú
00025712	92	74	65	5B	60	B5	34	E8	25	90	E3	1E	B2	84	B8	29	Æte[ `44q\$EnÄqäq)
00025728	88	AA	66	48	9C	DC	53	92	40	E6	1F	DD	3F	F4	55	D6	è-fH£■SÆ@u} ?{Uf
00025744	7C	CD	99	AA	EB	CB	2B	08	D0	23	F6	3A	FD	68	56	E8	=Ö-δq+□L#÷÷: hVq
00025760	46	06	A6	F4	AC	2E	F5	D6	02	C0	6D	38	66	10	84	FF	F▲·{4. }f·Lm3f→ä
00025776	76	7B	80	C3	5A	F4	6B	E6	B0	5E	5B	70	BA	81	9F	15	v{C-Z{ku~^ [p]uf\$
00025792	51	FC	C6	B2	F4	B9	B0	B4	0F	CD	0C	99	C9	02	87	99	Q"  q q c=+Öf·çÖ
00025808	31	21	77	CF	31	9A	54	F6	3A	59	58	B8	75	99	62	04	l!w=1ÜT÷:YXq uÖb◆
00025824	FB	33	82	2B	67	F3	54	26	A4	D0	09	1F	DD	B1	6A	AC	√3é+g<T&ñloV}≡j4
00025840	6F	C8	E8	10	3D	A4	6A	9F	12	43	D5	33	79	62	06	56	o4q=ñjfiCf3ybaV
00025856	9A	09	29	74	7B	58	CE	CE	01	3F	41	23	A6	EA	A5	DD	Üo) t{Xq q?Aq+Qñ
00025872	8C	D3	81	A2	1C	3E	E5	65	13	5B	A8	A2	54	72	72	7B	iüóL>oe!![çóTrr{
00025888	CB	1E	1C	6B	E5	54	92	7D	CD	3B	94	24	EF	73	EB	D2	qÄLkσTÆ)=;ö\$nsδT
00025904	FB	43	28	98	E6	8B	DA	2B	FD	EF	DF	CF	D2	59	BD	CF	√C(yüi r+·n■LqYJL
00025920	B9	E6	A0	9D	D4	14	17	1A	63	34	B9	10	11	96	B9	63	qúaYLqT-c4q}→q c
00025936	8B	19	C2	5A	F9	B7	F7	C6	40	E3	D9	83	A4	CE	DC	65	iLZ·q= @n-ânq·e
00025952	B9	25	CC	C2	EB	69	66	1C	A2	FA	2E	71	48	02	89	35	q qTδifLó·.qHöë5
00025968	19	45	02	EF	BE	EF	1A	FE	61	E5	56	D6	44	7F	B8	6D	LEon n-■aoVfDqym
00025984	F5	91	56	BB	19	3C	0C	29	73	84	55	5A	CD	F8	A9	86	æVqL<*)säUZ=°râ
00026000	C5	F3	E9	F0	53	71	FD	2C	61	1B	70	9D	62	9A	92	F5	+<θ=Sq²,a-p¥bÜE]
00026016	54	11	73	55	7A	66	5D	2D	15	4A	A3	60	32	D8	D1	5C	T<§Uzf]-§Jú`2+T\
00026032	77	A4	57	15	BE	D1	1A	C0	7D	E9	4D	B6	31	C4	8C	81	wñW\$T-L}ØM l-iü
00026048	AA	AF	39	32	C1	72	64	D4	BB	86	44	29	73	91	E1	4A	→92LrdLqâD)sæßJ
00026064	5C	C4	97	7F	47	5E	CD	C2	05	B5	38	A0	E3	96	6D	8A	\-üoG^=T· 8ânûmè
00026080	B8	BB	3D	C0	C4	04	8F	62	02	DA	52	45	6D	11	46	39	qj=L·Äb·rREM<F9
00026096	81	D9	03	5B	AD	7D	B1	65	F1	90	0A	7A	B2	1D	7D	88	ü·♥[; )≡e±Eßz■-)è

Figure 36: Screenshot of the file content/sector after file wiping with Eraser



## File wiping process with Eraser on a NTFS File System:

### 1. MFT, NTFS-Journal

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00214000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0C	00	.....
00214016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	..... Sektor 418
00214032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214048	00	00	00	00	00	00	00	00	07	03	24	00	55	00	70	00	.....\$.U.p.
00214064	43	00	61	00	73	00	65	00	03	00	00	00	00	00	03	00	C.a.s.e.....
00214080	60	00	50	00	00	00	00	00	05	00	00	00	00	00	05	00	`P.....
00214096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214144	00	00	00	00	00	00	00	00	07	03	24	00	56	00	6F	00	.....\$.V.o.
00214160	6C	00	75	00	6D	00	65	00	05	00	00	00	00	00	05	00	l.u.m.e.....
00214176	58	00	44	00	00	00	00	00	05	00	00	00	00	00	05	00	X.D.....
00214192	02	BE	33	A0	FA	68	D8	01	44	FE	16	CE	FA	68	D8	01	..%3 úhØ.Dp.fúhØ.
00214208	44	FE	16	CE	FA	68	D8	01	44	FE	16	CE	FA	68	D8	01	Dp.fúhØ.Dp.fúhØ.
00214224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214240	06	00	00	10	00	00	00	00	01	03	2E	00	00	00	00	00	.....
00214256	21	00	00	00	00	00	01	00	68	00	52	00	00	00	00	00	!.....h.R.....
00214272	05	00	00	00	00	00	05	00	44	FE	16	CE	FA	68	D8	01	.....Dp.fúhØ.
00214288	00	25	17	CE	FA	68	D8	01	00	25	17	CE	FA	68	D8	01	..%.fúhØ..%.fúhØ.
00214304	00	25	17	CE	FA	68	D8	01	68	00	00	00	00	00	00	00	..%.fúhØ.h.....
00214320	62	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	b.....
00214336	08	00	64	00	61	00	74	00	61	00	2E	00	74	00	78	00	..d.a.t.a...t.x.
00214352	74	00	6F	00	6C	00	75	00	1F	00	00	00	00	00	01	00	t.o.l.u.....
00214368	88	00	74	00	00	00	00	00	05	00	00	00	00	00	05	00	^t.....
00214384	FF	2B	D5	A0	FA	68	D8	01	FF	2B	D5	A0	FA	68	D8	01	ÿ+Õ úhØ.ÿ+Õ úhØ.
00214400	FF	2B	D5	A0	FA	68	D8	01	FF	2B	D5	A0	FA	68	D8	01	ÿ+Õ úhØ.ÿ+Õ úhØ.
00214416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214432	06	00	00	10	00	00	00	00	19	00	53	00	79	00	73	00	.....S.y.s.
00214448	74	00	65	00	6D	00	20	00	56	00	6F	00	6C	00	75	00	t.e.m. .V.o.l.u.
00214464	6D	00	65	00	20	00	49	00	6E	00	66	00	6F	00	72	00	m.e. .I.n.f.o.r.
00214480	6D	00	61	00	74	00	69	00	6F	00	6E	00	00	00	00	00	m.a.t.i.o.n.....
00214496	00	00	00	00	00	00	00	00	10	00	00	00	02	00	00	00	.....
00214512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0C	00	.....

Figure 37: Screenshot of the NTFS Journal with data ("data.txt")

## 2. FILE CONTENT (target file "data.txt", offset 299540, sektor 5.322)

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
02724848	00	00	00	00	00	00	00	00	00	00	00	00	00	00	04	00	.....
02724864	46	49	4C	45	30	00	03	00	F1	67	10	00	00	00	00	00	FILE0...fg..... Sektor 5.322
02724880	01	00	01	00	38	00	01	00	90	01	00	00	00	04	00	00	....8.....
02724896	00	00	00	00	00	00	00	00	03	00	00	00	21	00	00	00	.....!...
02724912	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	.....`...
02724928	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
02724944	44	FE	16	CE	FA	68	D8	01	00	25	17	CE	FA	68	D8	01	Dp.fühø...%.fühø.
02724960	00	25	17	CE	FA	68	D8	01	50	1E	B1	04	FB	68	D8	01	%.fühø.P.±.ühø.
02724976	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02724992	00	00	00	00	06	01	00	00	00	00	00	00	00	00	00	00	.....
02725008	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	.....0...p...
02725024	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00	.....R.....
02725040	05	00	00	00	00	00	05	00	44	FE	16	CE	FA	68	D8	01	.....Dp.fühø.
02725056	44	FE	16	CE	FA	68	D8	01	44	FE	16	CE	FA	68	D8	01	Dp.fühø.Dp.fühø.
02725072	44	FE	16	CE	FA	68	D8	01	00	00	00	00	00	00	00	00	Dp.fühø.....
02725088	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	.....
02725104	08	00	64	00	61	00	74	00	61	00	2E	00	74	00	78	00	..d.a.t.a...t.x.
02725120	74	00	00	00	00	00	00	00	80	00	00	00	80	00	00	00	t.....€...€...
02725136	00	00	18	00	00	00	01	00	62	00	00	00	18	00	00	00	.....b.....
02725152	FF	FE	2A	00	2A	00	2A	00	53	00	45	00	43	00	55	00	ÿp*.*.*.S.E.C.U.
02725168	52	00	45	00	44	00	41	00	54	00	41	00	2A	00	2A	00	R.E.D.A.T.A.*.*.
02725184	2A	00	50	00	41	00	53	00	53	00	57	00	4F	00	52	00	*.P.A.S.S.W.O.R.
02725200	44	00	2A	00	2A	00	2A	00	4B	00	45	00	59	00	2A	00	D.*.*.*.K.E.Y.*.
02725216	2A	00	2A	00	53	00	45	00	43	00	55	00	52	00	45	00	*.*.S.E.C.U.R.E.
02725232	44	00	41	00	54	00	41	00	2A	00	2A	00	2A	00	0D	00	D.A.T.A.*.*.*...
02725248	0A	00	00	00	00	00	00	00	FF	FF	FF	FF	82	79	47	11	.....ÿÿÿÿ,yG.
02725264	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725280	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725296	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725312	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725328	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725344	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	03	00	.....

Figure 38: Screenshot of the file content in NTFS

### 3. MFT/NTFS-Journal after wiping process

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
00214000	60	00	50	00	00	00	00	00	05	00	00	00	00	00	0E	00	`.P.....
00214016	02	BE	33	A0	FA	68	D8	01	02	BE	33	A0	FA	68	D8	01	..%3 úhØ..%3 úhØ. Sektor 418
00214032	02	BE	33	A0	FA	68	D8	01	02	BE	33	A0	FA	68	D8	01	..%3 úhØ..%3 úhØ.
00214048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214064	06	00	00	20	00	00	00	00	07	03	24	00	53	00	65	00	... ..\$.S.e.
00214080	63	00	75	00	72	00	65	00	0A	00	00	00	00	00	0A	00	c.u.r.e.....
00214096	60	00	50	00	00	00	00	00	05	00	00	00	00	00	05	00	`.P.....
00214112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214160	00	00	00	00	00	00	00	00	07	03	24	00	55	00	70	00	.....\$.U.p.
00214176	43	00	61	00	73	00	65	00	03	00	00	00	00	00	03	00	C.a.s.e.....
00214192	60	00	50	00	00	00	00	00	05	00	00	00	00	00	05	00	`.P.....
00214208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214256	00	00	00	00	00	00	00	00	07	03	24	00	56	00	6F	00	.....\$.V.o.
00214272	6C	00	75	00	6D	00	65	00	05	00	00	00	00	00	05	00	l.u.m.e.....
00214288	58	00	44	00	00	00	00	00	05	00	00	00	00	00	05	00	X.D.....
00214304	02	BE	33	A0	FA	68	D8	01	39	BF	70	A2	FC	68	D8	01	..%3 úhØ.9¿p¿úhØ.
00214320	39	BF	70	A2	FC	68	D8	01	E1	FA	57	A3	FC	68	D8	01	9¿p¿úhØ.áúW¿úhØ.
00214336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00214352	06	00	00	10	00	00	00	00	01	03	2E	00	00	00	00	00	.....
00214368	1F	00	00	00	00	00	01	00	88	00	74	00	00	00	00	00	.....^..t.....
00214384	05	00	00	00	00	00	05	00	FF	2B	D5	A0	FA	68	D8	01	.....ÿ+Ö úhØ.
00214400	FF	2B	D5	A0	FA	68	D8	01	FF	2B	D5	A0	FA	68	D8	01	ÿ+Ö úhØ.ÿ+Ö úhØ.
00214416	FF	2B	D5	A0	FA	68	D8	01	00	00	00	00	00	00	00	00	ÿ+Ö úhØ.....
00214432	00	00	00	00	00	00	00	00	06	00	00	10	00	00	00	00	.....
00214448	19	00	53	00	79	00	73	00	74	00	65	00	6D	00	20	00	..S.y.s.t.e.m. .
00214464	56	00	6F	00	6C	00	75	00	6D	00	65	00	20	00	49	00	V.o.l.u.m.e. .I.
00214480	6E	00	66	00	6F	00	72	00	6D	00	61	00	74	00	69	00	n.f.o.r.m.a.t.i.
00214496	6F	00	6E	00	00	00	00	00	00	00	00	00	00	00	00	00	o.n.....
00214512	10	00	00	00	02	00	00	00	FF	2B	D5	A0	FA	68	0E	00	.....ÿ+Ö úh..

Figure 39: Screenshot of the NTFS-Journal after wiping



#### 4. file content after wiping process (sektor 5.322)

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
02724848	00	00	00	00	00	00	00	00	00	00	00	00	00	00	06	00	.....
02724864	46	49	4C	45	30	00	03	00	D4	7F	10	00	00	00	00	00	FILE0...Ö..... Sektor 5.322
02724880	02	00	01	00	38	00	00	00	58	01	00	00	00	04	00	00	....8...X.....
02724896	00	00	00	00	00	00	00	00	0B	00	00	00	21	00	00	00	.....!...
02724912	05	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	.....`...
02724928	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
02724944	10	27	00	00	00	00	00	00	10	27	00	00	00	00	00	00	.'.....'.....
02724960	39	BF	70	A2	FC	68	D8	01	10	27	00	00	00	00	00	00	9¿pëüh0...'.....
02724976	20	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02724992	00	00	00	00	06	01	00	00	00	00	00	00	00	00	00	00	.....
02725008	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	.....0...p...
02725024	00	00	00	00	00	00	0A	00	52	00	00	00	18	00	01	00	.....R.....
02725040	05	00	00	00	00	00	05	00	10	27	00	00	00	00	00	00	.....'.....
02725056	10	27	00	00	00	00	00	00	10	27	00	00	00	00	00	00	.'.....'.....
02725072	10	27	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.'.....'.....
02725088	00	00	00	00	00	00	00	00	20	20	00	00	00	00	00	00	.....
02725104	08	00	39	00	59	00	78	00	54	00	77	00	28	00	52	00	..9.Y.x.T.w.(.R.
02725120	32	00	00	00	00	00	00	00	80	00	00	00	48	00	00	00	2.....€...H...
02725136	01	00	00	00	00	00	03	00	00	00	00	00	00	00	00	00	.....
02725152	FF	FF	FF	FF	FF	FF	FF	40	00	00	00	00	00	00	00	00	yyyyyyyy0.....
02725168	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725184	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725200	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	yyyy,yG.....
02725216	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725232	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725248	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725264	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725280	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725296	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725312	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725328	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725344	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
02725360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	05	00	.....

Figure 40: Screenshot of the file content after wiping (sektor 5.322)

NTFS mirrored the file content to sector 2.678:

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Dekodierter Text
01371120	06	00	05	00	28	00	00	00	28	00	80	00	18	00	F9	E0	.... (... (.€...à
01371136	08	01	00	00	02	00	02	00	08	00	00	00	00	00	00	00	..... Sektor 2.678
01371152	89	02	00	00	00	00	00	00	80	00	00	00	80	00	00	00	.....€...€...
01371168	00	00	18	00	00	00	01	00	62	00	00	00	18	00	00	00	.....b.....
01371184	FF	FE	2A	00	2A	00	2A	00	53	00	45	00	43	00	55	00	ÿp*.*.*.S.E.C.U.
01371200	52	00	45	00	44	00	41	00	54	00	41	00	2A	00	2A	00	R.E.D.A.T.A.*.*.
01371216	2A	00	50	00	41	00	53	00	53	00	57	00	4F	00	52	00	*.P.A.S.S.W.O.R.
01371232	44	00	2A	00	2A	00	2A	00	4B	00	45	00	59	00	2A	00	D.*.*.*.K.E.Y.*.
01371248	2A	00	2A	00	53	00	45	00	43	00	55	00	52	00	45	00	*.*.S.E.C.U.R.E.
01371264	44	00	41	00	54	00	41	00	2A	00	2A	00	2A	00	0D	00	D.A.T.A.*.*.*.
01371280	0A	00	00	00	00	00	00	00	93	75	10	00	00	00	00	00	....."u.....
01371296	78	75	10	00	00	00	00	00	78	75	10	00	00	00	00	00	xu.....xu.....
01371312	28	00	00	00	00	00	00	00	01	00	00	00	18	00	00	00	(.....
01371328	06	00	00	00	00	00	00	00	25	00	00	00	28	00	F0	02	.....%... (.ö.
01371344	28	00	00	00	18	00	01	00	10	01	00	00	02	00	02	00	(.....
01371360	08	00	00	00	00	00	00	00	89	02	00	00	00	00	00	00	.....%.....
01371376	9E	75	10	00	00	00	00	00	93	75	10	00	00	00	00	00	žu....."u.....
01371392	93	75	10	00	00	00	00	00	30	00	00	00	00	00	00	00	"u.....ö.....
01371408	01	00	00	00	18	00	00	00	00	00	00	00	00	00	00	00	.....
01371424	15	00	16	00	28	00	08	00	28	00	08	00	90	00	01	00	.... (... (...
01371440	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
01371456	84	02	00	00	00	00	00	00	F3	02	00	00	01	00	00	00	.....ó.....
01371472	AA	75	10	00	00	00	00	00	9E	75	10	00	00	00	00	00	*u.....žu.....
01371488	9E	75	10	00	00	00	00	00	70	00	00	00	00	00	00	00	žu.....p.....
01371504	01	00	00	00	18	00	00	00	04	00	00	00	00	00	00	00	.....
01371520	05	00	06	00	28	00	48	00	70	00	00	00	18	00	01	00	.... (.H.p.....
01371536	08	01	00	00	02	00	02	00	08	00	00	00	00	00	00	00	.....
01371552	89	02	00	00	00	00	00	00	80	00	00	00	48	00	00	00	%.....€...H...
01371568	01	00	00	00	00	00	03	00	00	00	00	00	00	00	00	00	.....
01371584	00	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
01371600	00	10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
01371616	00	00	00	00	00	00	00	00	21	01	F3	02	00	00	00	00	.....!..ö.....
01371632	BE	75	10	00	00	00	00	00	AA	75	10	00	00	00	F9	E0	%u.....*u.....à

Figure 41: Screenshot of the mirrored file content after wiping (sector 2.678)

We can see here, that the file-mirroring process in NTFS works fine - even, if the file are overwritten with a special wiping program.

This is in line with data security, to prevent accidental deletion and to be able to restore deleted data if necessary. However, it is quite at odds with secure erasure of data.

In general, it must be said that data in the NTFS file system cannot be securely deleted. The only recommended way is to completely erase the hard drive using external utilities with own boot processes.

It should be noted that the wipe operations cannot be performed directly on the entire system hard disk on which Windows is located. However, external memory or secondary hard disks can be completely overwritten. The wipe

procedures can also be applied to individual folders and files, but this does not always work with the NTFS file system. Thus it could be shown in attempts that sectors were deleted contentwise, and/or overwritten, however ghost copies in the NTFS file system were created. The file name was recoverable in every case, which does not show sufficient security as a deletion method. According to current knowledge, the errors in the deletion programs initially only affect the NTFS file system.

Therefore it is highly recommended to use a FAT, FAT12, FAT16, FAT32, exFAT or ext3/ext4 file system if you want to erase data later securely with an application.

A search for temporary copies or thumbnails, etc. does not perform any of the analysed programs. Thus, when deleting and overwriting an image file, one cannot be sure that one or more copies of this file have not been made automatically by the operating system or other applications, as is often the case.

Another big problem of a program like Eraser is the high system load during the wiping process. With larger amounts of data or multiple overwriting of data, the wiping process can take several hours or even days and affects the computer system in such a way that in many cases other applications react only very delayed. An impairment of these parallel running applications is also not excluded and a parallel use of the system for other important tasks is generally not recommended.

However, deletion processes can be automated via schedules in order to regularly erase sensitive data, e.g. on an external storage device.

Nevertheless, individual data from a file or database cannot be deleted.

Basically, the software can operate on any file system that is supported by MS Windows and a write permission exists. If a disk is mounted in read-only mode, the secure erase process cannot logically take effect. After all, a hard disk with an unknown file system can only be completely overwritten. Then all data is irretrievably lost there as well. On SSD's this erase method is not completely

safe, because the device firmware can skip individual memory cells in the write access because of optimization issues.

Nor is it possible to apply the deletion process to online cloud storage. Often, cloud operators even protect themselves against intensive write access to their data media because of the reduced lifespan at high utilization. However, integrated network storage can also be partially deleted with applications after the appropriate rights have been assigned. A total deletion or multiple complete overwriting of a network storage is not possible, though.

### 2.6.6. Unix “hdparm”

Hdparm<sup>44</sup> is a UNIX command line tool by Mark Lord. Originally it was developed for IDE (hdparm) and later for SCSI (sdparm) hard drives.

The tool is used to manipulate and control the hard disk features. The ATA/ATAPI command set is used for this. If other interfaces such as USB or network connections are used, the adapter must support "ATA command pass through", which is rarely the case.

We would now like to look at hdparm (latest Version 9.58) in connection with the "secure erase" function on common hard drives.

The command for erasing drive sdb with the password “p” would look like:

```
sudo hdparm --user-master u --security-erase p /dev/sdb
```

And if secure enhanced erase is supported:

```
sudo hdparm --user-master u --security-erase-enhanced p /dev/sdb
```

It is recommended to read the hdparm manual carefully! It's easy to erase the wrong drive if you're not careful and don't type the commands correctly.

---

<sup>44</sup> Further more on <https://wiki.archlinux.org/title/hdparm>

There are a number of instructions on how to use it on the internet<sup>45</sup>.

The "security erase" command should not be confused with the "secure delete" of the firmware in hard disks.

This secure deletion process can be triggered with `hdparm`. However, in most cases a secure cryptographic erase is performed.

To do this, `hdparm` uses the hardware encryption of the hard disk. In this case, the data on the hard drive is securely encrypted with a password. The password is then discarded, and it is not possible to decrypt the data again. With the usual cryptographic methods, it looks to an uninformed observer from the outside as if the hard disk was written with random data.

Which brings us to the question of why you have to initiate this encryption at all if you couldn't just write random characters to the hard drive in another way.

In summary, `hdparm` is a popular tool for addressing hard drives with ATA commands. In fact, it can trigger a secure deletion process, which, however, is more likely to be described as a cryptographic erase of the entire disk.

However, it also depends on how the hard disk is connected to the system and whether certain ATA commands are blocked by drivers or hardware.

### 3. Comparison of deletion procedures

As we have explained in the previous pages, there are a large number of different erasure methods and variations. In any case, the designations and methods are quite different.

How can we now summarize these different processes and present them clearly to the user?

There are roughly three approaches to deleting data, one of which is followed by the deletion process.

---

<sup>45</sup> Like on [https://ata.wiki.kernel.org/index.php/ATA\\_Secure\\_Erase](https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase) or <https://www.skrilnetz.net/the-truth-about-how-to-securely-erase-a-solid-state-drive-ssd/> accessed on 17.05.2022

1. Deletion by moving data to the Recycle Bin.

In this procedure, the focus is on recovering data when it has been accidentally "deleted".

2. The secure deletion of data using special software.

The focus is on the secure destruction of data in different environments, such as operating systems, file systems or legal conditions. The primary goal of this software is to erase the data in such a way that it cannot be recovered.

3. The destruction of the data medium.

This procedure is intended to erase all information on the disk. So possibly even blocked data areas, time information or type information. The aim of this procedure is therefore the complete destruction of information.

These three methods are evaluated further for private users, commercial users (companies) and public authorities.

The results of the research for the three user groups are presented in compressed form below.

The evaluation is based on a general assessment in a 5-Step comparison:

very low	low	mid	high	very high
<i>The value is negibly small.</i>	<i>The value is measurable, but can be described as insignificant under normal conditions.</i>	<i>The value is there and is usually described as tolerable.</i>	<i>The value is so high that it causes impairments.</i>	<i>The value is so high that it cannot be tolerated.</i>

Table 8: 5-step model for evaluation and comparison from very low to very high

For a better overview, the values are also described with a simple description as follows:

<b>++</b>	<b>+</b>	<b>0</b>	<b>-</b>	<b>--</b>
very positive	positive	neutral	negative	very negative

Table 9: Model for evaluation and comparison from very positive to very negative

The selected criteria for the assessments are:

<b>Performance:</b>	<p>The performance describes the time required for the deletion process in relation to other similar system tasks. The higher the deletion speed, the higher the performance rating.</p> <p>A very low performance rating is caused by a slow deletion process, which is usually unacceptable in terms of time.</p> <p>If a deletion process takes hardly any time or only insignificant time, the rating is to be classified as high or very high. A medium performance is an acceptable time value of the deletion process for the standard user.</p>
<b>Complexity:</b>	<p>The complexity represents the mental requirement for the user. Less time-consuming user input is to be rated as low complexity. The installation of an additional program is represented as medium complexity, and the complicated application of a program with additional functions as very high complexity.</p>
<b>System impairment:</b>	<p>The evaluation of the performance concerns mainly the impairment of the hardware of the system. In general, write access to memory hardware is to be rated negatively in this context. A very high system impairment means that other hardware processes are also negatively</p>

	<p>affected, which limits the usability of the system. A medium system impairment does not exceed the average level and is not critical to the operation of the system.</p> <p>Very low system impairment means that the processes do not cause any noticeable load during operation.</p>
<b>Security:</b>	<p>The security of the deletion process assesses the potential recoverability of the deleted data.</p> <p>Very high security means that the data cannot be recovered even with the most modern means of laboratory technology in the sense of the state of the art.</p> <p>Medium security means that the data is securely deleted in the legal sense of the GDPR and can only be restored with considerable effort by specialists.</p> <p>Very low security means the data can be easily recovered even by ordinary users.</p>
<b>Cost:</b>	<p>In the context of costs, the monetary expenses for the described deletion process are evaluated. If there are no further costs beyond the costs of the normal operation of the system, the costs are described as very low.</p> <p>Medium costs are costs that are incurred for a computer program in the average price segment.</p> <p>Very high costs result from the destruction of the data carrier or the extreme impairment of other computer system components as well.</p>

Table 10: Criteria description for evaluation and comparison



### 3.1. For private users

Private users of a computer system have a special position within the framework of the GDPR. In European data protection law, data may be processed for family purposes or in the context of one's own personal sphere. These two exceptions from the GDPR are regulated in Article 2 Para. 2 GDPR. However, this only includes the legal aspects of data processing.

For private users, however, different areas of application for deleting data are also interesting.

If the owner of a storage device wants to sell it again after some time, he may be interested in deleting all of his sensitive or private data from the device without the buyer is easy able to restore it.

So what are the options that a private user has to securely erase their data on their own device?

In consensus with the points, explanations and explanations already listed, the following options are now available:

#### A) Recycle Bin Solution

The easiest way to get rid of data to clean up the computer system is the procedure of emptying the Recycle Bin. The old data will be overwritten by the operating system over time and the system speed will not be affected. The lifespan of the hard drive doesn't suffer either, since long-lasting write accesses are not made.

Performance:	high	+
Complexity:	low	+
System impairment:	very low	++
Security:	low	-
Cost:	very low	++
<b>Average:</b>	<b>positive</b>	<b>+</b>

Table 11: Evaluation of the Recycle Bin solution for private users

#### Explanation:

Without exception, the manufacturers of the popular operating systems have opted for the implementation of Recycle Bin solutions in the user desktops. It is more about an intermediate stage in deleting data. The user obviously wants to retain the ability to restore the data first. This is initially at the expense of the security of the deletion process, since the data remains available. The speed and the system impairment are almost optimal here. Any user can use this method even with little expertise and also recover accidentally deleted data from Recycle Bin. Furthermore, the system impairment is very low and there are no additional costs, since the functionality is available as standard in the operating systems.

#### Optimization opportunities:

Schedules can be created to remove data from the Recycle Bin. The storage space of older files in the Recycle Bin is then marked as free after a certain period of time and the data is gradually overwritten. This can happen at times of very low system usage, so that the user is completely unaware of the procedures.

#### Limitations:

By using the Recycle Bin, the user accepts certain security restrictions, but this should not pose a particular problem in the private sphere. In addition to the lack of high security, it must also be pointed out that entire data carriers such as hard drives, SD cards or USB sticks cannot be deleted in this way. Likewise, in most cases, very large amounts of data cannot be kept in the Recycle Bin.

## B) Special Software

One possibility for private individuals to destroy data is the use of special software like applications for different operating systems or applications with completely independent boot systems. In the course of the development, some programs were presented that differ in the applicability and security of the deletion procedures. The performance and the impairment of the system also differ from program to program. Of course, it depends on the properties of the computer system in question. Is it a Linux/Unix OS, a Windows or a macOS operating system?

Performance:	mid (low)	o (-)
Complexity:	mid	o
System impairment:	high (very high)	- (- -)
Security:	mid (high)	o (+)
Cost:	mid	o
<b>Average:</b>	<b>neutral</b>	<b>o (-)</b>

Table 12: Evaluation of special software for private users

### Explanation:

In the private sphere, the use of special software for deleting files is not very widespread. This can already be seen from the view above. There are several points that make the use of deletion software in the private sector impractical. On the one hand, any additional software installed increases the system impairment in terms of the required storage space and computing capacity. The user must also be able to use and understand this software. This is almost impossible for the normal user to do when distinguishing between the many deletion methods. Finally, the cost to each user plays a role in the decision-making process. Is it worth buying a new application for the sake of security, for the price of which you can possibly already get a new hard disk?

In the previous chapters, the Eraser application was presented as a representative of secure deletion software for MS Windows.

This application has a number of configuration options and a relatively high security standard due to the multiple overwriting of the selected data. Files, partitions, entire hard drives or just the free storage space can be overwritten with different algorithms. However, this is associated with an enormous and long-lasting system load, so that the computer system is very impaired by the mostly hours-long work of the deletion program.

A big minus of the here selected Windows program "Easer" is that in the NTFS file system deleting of single files is inadequate and not acceptable. Although the sectors of the file are overwritten, but the contents of the file are moved to a front area of the file system using the NTFS methods. The file name is also retained in the MFT mirror. Thus, the overwritten file can be restored very easily in a timely manner from the mirror copy.

This system load is also found in the applications for Unix/Linux and is the result of the very intensive write processes on the drive.

The lifetime of the affected storage devices is reduced as the write operations progress. If the BSI recommends overwriting 7 times, the lifespan of an SSD would be reduced to 1/7 in purely mathematical terms. In other words, you would consume about 85% of the write operations on an SSD just with secure erases, which is totally unacceptable.

#### Optimization opportunities:

The use of special deletion software is not very common in the private sphere. However, freelance journalists, computer nerds and whistleblowers have continued to push the development and improvement of secure computer systems for individuals, and the main aim was to protect one's own data against unauthorized access as good as possible.

This is how e.g. computer hacks with standard programs (see point 2.6.1. or 2.6.2.) came about, e.g. to be able to securely delete data. Individual

cross-operating system programs or even boot systems have also been developed in recent years to be able to securely delete data.

However, the applications mainly relate to very experienced or security-sensitive user groups.

There are no legal restrictions for private users.

At the moment, however, the overwhelming interest of users is going in a different direction than the secure destruction of their own data. Endless masses of images, videos and other content are produced and stored. Some people's greatest treasure are now millions of cell phone photos.

Without the need for security on the part of typical private users, there will be no implementation of secure deletion software for the general market.

The use of special deletion software is not very common in the private sphere. However, freelance journalists, computer nerds and whistleblowers have continued to push the development and improvement of secure computer systems for individuals, and the main aim was to protect one's own data against unauthorized access as best as possible.

This is how e.g. computer hacks with standard programs (see point 2.6.1. or 2.6.2.) came about, e.g. to be able to securely delete data. Individual cross-operating system programs or even boot systems have also been developed in recent years to be able to securely delete data [web 8].

However, the applications mainly relate to very experienced or security-sensitive user groups.

There are no legal restrictions for private users.

At the moment, however, the overwhelming interest of users is going in a different direction than the secure destruction of their own data. Endless masses of images, videos and other content are produced and stored. Some people's greatest treasure are now millions of cell phone photos.

Without the need for security on the part of typical private users, there will be no implementation of secure deletion software for the general market.

After all, the final deletion apparently deters the users, just as the existing deletion programs often delete insufficiently securely or make the computer system unusable for a short time.

#### Limitations:

The current applications actually have hardly any limitations in functionality. Deleting partitions, hard drives, USB sticks, individual files or free storage space is entirely possible. However, it depends very much on the technical knowledge of the user. The tools are mostly described in English and contain program operators and special terms from algorithms. This deters some users from using these deletion programs. The data cannot be restored after using the programs, this includes in particular accidentally deleted and overwritten data.

#### C) Physical Destruction

Destroying the storage device is the most effective and easiest solution to erasure.

It is assumed that the material is comminuted into small pieces of less than 1 cm. These parts are not recoverable, and all information is destructed.

Performance:	very high (high)	++ (+)
Complexity:	low	-
System impairment:	very low	++
Security:	very high	++
Cost:	low (mid)	+ (o)
Average:	positive	+ (++)

Table 13: Evaluation of the physical destruction of storage devices for private users

#### Explanation:

Destroying a storage medium in a shredder only takes a few seconds and can therefore be rated as extremely fast.

The complexity of the deletion process can be described as low. No special knowledge of programming or computer hardware is required. If the hard drives can be easily removed from the device, the process can be described as very simple.

The system impairment is very low in this case. With current hardware, no particular impairment is to be expected when removing hard disks or other memory devices as part of a hot swap.

With regard to the security of the deletion process, this can be described as extremely secure. The data cannot be restored with the most modern means in the laboratory.

The costs depend on the cost of the storage device. In view of the fact that storage media are becoming cheaper and cheaper, the cost of a new storage medium is sometimes lower than paying for software licences for a secure deletion process.

In summary, it can be said that destroying a data medium is the safest, easiest and fastest method in terms of data security in the deletion process. The sustainability of the process and the cost optimization are not particularly valued. Additional costs can arise from purchasing a shredder or hiring a company to granulate the storage medium.

### 3.2. For companies

Data is money. Most companies would sign this statement today without questioning it. In fact, enormous monetary value is built up with customer data, e.g. in social networks. So why should companies delete data at all? - Because they have to do it for legal reasons. The data protection officers of the companies have to check the internal processes and meet the requirements of

the people whose data is stored. In Europe, these regulations are governed by the principle of "no data processing without a legal basis" in the GDPR. There is also the right to be forgotten, i.e. the deletion of personal data after a certain period of time.

The first aspect is therefore the secure deletion of personal data due to legal regulations.

The second scenario in companies is the deletion of sensitive valuable data on data carriers that are to be reused, sold or discarded. Nobody actually wants to give away company secrets on old hard drives to the competitor because the data wasn't erased cleanly. So what can you do? In the following points, possibilities for secure deletion methods for companies are presented in order to meet legal requirements and set up their own security processes:

#### A) Recycle Bin Solution

We have already discussed the Recycle Bin solution in detail already. It is the easiest way to get rid of data to clean up the computer system, but it is not to be seen as a safe solution within the framework of deletion methods for security-related processes. If data is intended for deletion, the Recycle Bin should not be used.

However, unimportant data can be moved to the Recycle Bin to free up disk space.

Performance:	high	+
Complexity:	low	+
System impairment:	very low	++
Security:	low	-
Cost:	very low	++
<b>Average:</b>	<b>positive</b>	<b>+</b>

Table 14: Evaluation of the Recycle Bin solution for companies



Explanation:

The Recycle Bin solution was already discussed in point 3.1. and described in detail. Please be free to get further information there.

With regard to legal requirements and your own security requirements, the Recycle Bin solution cannot be recommended as a deletion method for companies in a legal context.

B) Special Software

An interesting solution is individual software applications for the secure deletion of data in companies. However, these must be adapted to the needs of the company and adapted to running applications, operating systems and the underlying hardware by experts. In these cases, enterprise solutions are available, which are expensive but can certainly meet the legal requirements and your own security requirements.

Performance:	mid	o
Complexity:	low	+
System impairment:	mid	o
Security:	high	+
Cost:	mid	o
<b>Average:</b>	<b>neutral</b>	<b>o (+)</b>

Table 15: Evaluation of Special Software for companies

Explanation:

In the corporate environment, there are very individual demands on computer processes. Contractors program individual software according to specific customer requirements or provide features of existing software. The

applications can be adapted to existing hardware, software and prioritized processes. The performance of these enterprise software versions can definitely be rated as high and, in the best case, are certified according to ISO 27001 and ISO 9001:2015 or ISO 14001 and conform to BSI basic protection. The end user hardly has to deal with the operation of the software and the rest of the computer system is less stressed by individual adjustments. By implementing secure deletion procedures, the deletion processes are very secure and can be checked regularly using standard procedures. Of course, running costs arise due to software and hardware loads. Depending on the size of the company, however, these costs must be estimated. In the event of gross non-compliance with deletion deadlines, there is a risk of severe fines, which have already been imposed in the past.

#### Optimization opportunities:

The special applications can also be controlled via schedules. In some cases, however, programming knowledge is required for this, e.g. to create cronjobs or scheduled tasks.

In order to minimize the write processes without losing data security, only very specific overwrite processes should be carried out.

A very important point for companies is the development and establishment of a deletion concept with constant evaluation.

These deletion concepts are also part of the legal requirements of the GDPR and must be explained in the event of an incident.

#### Limitations:

The current applications have hardly any limitations in functionality and can be adapted to the needs of companies. Deleting partitions, hard drives, USB sticks, individual files or free storage space is entirely possible. The individual tools are

built into the operational infrastructure and cannot normally be influenced by the individual user.

Thus, automatic deletion algorithms are implemented and adapted to the work processes.

A multi-level system is also possible, so that user data is first deleted on one level, but their backups are only deleted some time later. However, this always depends on the individual specifications.

The installation of secure deletion methods in the form of individual software is associated with higher costs. Furthermore, there are regular costs for necessary adjustments to the software. In addition, the hardware is burdened by regular overwriting of the data areas and the failures of data storage devices increase. As a result, the deletion methods shown also have an impact on backup strategies in complex company environments.

### C) Physical Destruction

Destroying the storage device or media is the most effective and easiest solution to erasure. Shredding is recommended by the German Federal Office for Security in Information Technology for media that should not be reused or has some technical defect.

It is assumed that the material is comminuted into small pieces of less than 1 cm. These parts are not recoverable.

Performance:	very high (high)	++ (+)
Complexity:	very low	++
System impairment:	very low	++
Security:	very high	++
Cost:	low	+
Average:	very positive	++

Table 16: Evaluation of the physical destruction of storage devices for companies

### Explanation:

Destroying a storage medium in a shredder only takes a few seconds and can therefore be rated as extremely fast.

There are various service providers who take care of the safe disposal of data carriers<sup>46</sup>.

The complexity of the deletion process can be described as low. No special knowledge of programming or computer hardware is required. If the hard drives can be easily removed from the device, the process can be described as very simple. Basically, the exchange of storage media goes hand in hand with the expected data security of the company.

The system impairment is very low in this case. With current hardware, no particular impairment is to be expected when removing hard disks or other memory devices as part of a hot swap.

With regard to the security of the deletion process, this can be described as extremely secure. The data cannot be restored with the most modern means in the laboratory.

The costs depend on the cost of the storage device. In view of the fact that storage media are becoming cheaper and cheaper, the cost of a new storage medium is sometimes lower than paying for software licences for a secure deletion process.

In summary, it can be said that destroying a data medium is the safest, easiest and fastest method in terms of data security in the deletion process. The sustainability of the process and the cost optimization are not particularly valued. Additional costs can arise from purchasing a shredder, provisioning and training of personnel, or hiring a company to granulate the storage medium. But for the ongoing operation of deletions in a data processing system based on the GDPR, shredding the devices can't be the only worked out strategy. Additional software-based deletion strategies of individual data structures must be set up here.

---

<sup>46</sup> More on <https://www.shredit.com/en-us/secure-shredding-services/hard-drive-destruction> accessed on 17.05.2022

### 3.3. For public authorities

Now we come to what is probably the most complicated assessment of erasure procedures, namely in the official environment.

For this we have to look at the legal requirements, which are as follows: No data processing without a legal basis. From this statement one can deduce that data may only be stored for as long as there is a legal basis. After this individual period, data must be deleted by authorities.

The authorities or legal supervisory authorities or parliaments must decide with what degree of certainty this must be done. The scope of the deletion of data is also mostly unclear. Often only a personal reference has to be removed, and thus parts of data records have to be deleted. In the context of the above statements, the partial deletion of data appears to be extremely difficult and hardly practical.

We will now also look at the typical erasure procedures and make an assessment of the methods used in the authorities' environment.

#### A) Recycle Bin Solution

We have already discussed the Recycle Bin solution in detail already. It is the easiest way to get rid of data to clean up the computer system, but it is not to be seen as a safe solution within the framework of deletion methods for security-related processes. If data is intended for deletion in a government setting, the Recycle Bin should not be used.

However, unimportant data can be moved to the Recycle Bin to free up disk space.

Performance:	high	+
Complexity:	low	+
System impairment:	very low	++
Security:	very low	- -
Cost:	very low	++
<b>Average:</b>	<b>positive</b>	<b>+</b>

Table 17: Evaluation of the Recycle Bin solution

#### Explanation:

The Recycle Bin solution has already been discussed in point 3.1. and described in detail. You are welcome to get more information there.

With regard to legal requirements and your own security needs, the recycle bin solution cannot be recommended as a deletion method in an official environment due to high data protection regulations. Employees' private data should always be processed strictly separately from sensitive government data. This also requires specially trained employees for processing procedures who know and master the different deletion methods.

#### Optimization opportunities:

The Recycle Bin should be replaced by a data shredder in which data is securely deleted by overwriting. Backup copies of data must comply with legal requirements and, if necessary, be regularly filtered and processed.

#### Limitations:

Insecure erasure methods are present in the foundation of many government software solutions or the used operating systems. There is little or no adaptation to the legal requirements. For the user, individual deletions can hardly be initiated, or their own applications can be installed.

## B) Special Software

In the government environment, secure deletion procedures must be installed by the manufacturer of the software in question.

Users or administrators only have limited options for intervening in the system. Incorrect deletion routines can make government data unusable and cause enormous damage. Nevertheless, the deletion methods must meet the required security requirements and must not impair the running system.

This places the highest demands on the software used in the government environment.

Performance:	mid	o
Complexity:	mid	o
System impairment:	mid	o
Security:	high	+
Cost:	high	-
Average:	<b>neutral</b>	<b>o</b>

Table 18: Evaluation of special Software for public authorities

### Explanation:

Deletion procedures can be efficiently built into individual authority software or operating systems. A particular impairment of performance can be reduced by special solutions.

The technical complexity of the deletion process is initially classified as extremely high, although the complexity for the end user should be very low.

Just like the performance, the system impairment of the individual system should also be taken into account. Deletion procedures in the government environment are mostly centralized in databases or out-sourced to data centers. Software-based and hardware-based optimizations are also necessary here.

In terms of security, the highest demands are placed on the implemented procedures. In addition, the programs must be regularly checked and adjusted. Ultimately, this is also reflected in the costs of the software. Buy and forget cannot be used. There are therefore ongoing costs due to adjustments to new legal requirements, new hardware and other new applications.

Optimization opportunities:

Logically, the deletion methods used by authorities have to be constantly adapted and optimized. Multiple or even uncontrolled overwriting of data storage can cause a complete system crash. This results in extremely security-relevant and system-critical processes. External software solutions cannot simply be added to existing databases and storage solutions. An in-house solution - i.e. by official specialists - can represent a solution here.

Limitations:

Complex use cases require complex solutions. This is also the case with the erasure procedures. However, the authorities must have special methods to protect the data of the residents. Thus, society also decides on the use of its data in the government environment. For this purpose, legal requirements must be discussed and specified in concrete terms. However, this is currently not the case, so that unclear formulations in laws also allow unsafe deletion processes in authorities.

It is therefore also currently unclear which deletion procedures are currently being used by authorities.

### C) Physical Destruction

Destroying the storage device is the most effective, safe and easiest solution to erasure.



It is assumed that the material is comminuted into small pieces of less than 1 cm. These parts are not recoverable.

Performance:	very high (high)	++
Complexity:	low	+
System impairment:	very low	++
Security:	very high	++
Cost:	low	+
Average:	very positive	++

Table 20: Evaluation of the physical destruction of storage devices for public authorities

#### Explanation:

Destroying a storage medium in a shredder only takes a few seconds and can therefore be rated as extremely fast.

The complexity of the deletion process can be described as low. No special knowledge of programming or computer hardware is required. If the hard drives can be easily removed from the device, the process can be described as very simple.

The system impairment is very low in this case. With current hardware, no particular impairment is to be expected when removing hard disks or other memory devices as part of a hot swap.

With regard to the security of the deletion process, this can be described as extremely secure. The data cannot be restored with the most modern means in the laboratory.

The costs depend on the cost of the storage device. In view of the fact that storage media are becoming cheaper and cheaper, the cost of a new storage medium is sometimes lower than paying for software licences for a secure deletion process.

In summary, it can be said that the destruction of a data carrier is the safest, easiest and fastest method in the deletion process in terms of data security and complies with the legal requirements of the GDPR. The sustainability of the process and the cost optimization are not particularly valued. Current service providers offer certified destruction methods and seamlessly logged processes. For high-security areas, there are also technical devices for the reliable destruction of data carriers on site.

## 4. Table overview

Based on the comparisons from point 3, an overview of the erasure process was created below, which enables a comprehensive overview of the methods and possibilities for different applications.

The criteria were classified in the same way as in point 3.

	Recycle bin <sup>47</sup>	additional Software <sup>48</sup>	Special Wiping Boot Systems <sup>49</sup>	Physically Destruction <sup>50</sup>
Security Level	low	high	very high	very high
Suitability for private users	high	mid	high <sup>51</sup>	o
Suitability for companies	low	mid	mid	high
Suitability for public authorities	very low	high	low	high
Complexity	very low	mid	high	very low
Performance	very high	low	very low	very high
System Impairment	very low	mid	very high <sup>52</sup>	very low <sup>53</sup>
Cost	very low	low	low	mid <sup>54</sup>
Recommended for security reason	no	might <sup>55</sup>	yes	yes
Complies with legal requirements (GDPR)	no	might <sup>56</sup>	yes	yes
Rating Over All <sup>57</sup>	<b>o</b>	<b>o</b>	<b>o</b>	<b>++</b>

Table 20: Table overview of common deletion procedures and rating by Florian Weijers

<sup>47</sup> Recycle bin is available at different operating systems by overwhelming user request.

<sup>48</sup> Typical problems of additional software are different filesystems (e.g. NTFS) or network storages.

<sup>49</sup> Does not work, if you have no physical access to the system and if you can not boot it externally.

<sup>50</sup> Need of physical access to the drive.

<sup>51</sup> Only if you want to erase complete drives.

<sup>52</sup> System can not be used during the wiping process (can last hours to days).

<sup>53</sup> Drives must be exchanged manually during working system.

<sup>54</sup> Only the cost of the hard drives is considered.

<sup>55</sup> Depends on the forensically verified result of the deletion process.

<sup>56</sup> Depends on the forensically verified result of the deletion process.

<sup>57</sup> The criteria of the security of the deletion process and the legal conformity were rated higher.

## 5. Summary

In the explanations of this work, different deletion methods in the everyday life of a private, commercial or government user were presented. The diversity of the deletion processes in the most varied of applications was shown. Without special knowledge of the entire computer system, it is not possible to say right away whether data has been irretrievably deleted. It all depends on how much effort you want to put into the recovery process. Basically, somebody could even use a brute force attack to break a cryptographic erase. However, normal users may not have the resources for this. Deleted data can also be restored in a database or a simple text file if it has not already been overwritten by the user or the working system.

Overwriting is a fundamentally good idea - if the result is checked. Applications such as Piriforms Eraser, that is on download rank 4/186 at chip.de in 2022, overwrite files during operation under Windows - however, there are file copies in the NTFS file system used, which make it easy to restore them, although this is exactly what users want to prevent.

For authorities, which often have increased requirements for data security and legal requirements, deletion procedures must be specified and controlled. It cannot be the order of the day that data is not visible on the surface and is considered deleted, but is easily recoverable from a backup or by file carving.

Another aspect of the work is the behaviour of the hard drive manufacturers, which shows that the safe removal of data is not a popular topic. A secure erase was implemented with the specifications of the US authorities, which apparently does not deserve the name. It has not been specified how data is erased or what recovery methods these erasure methods must successfully withstand. This fact is of course due to user behaviour. All users want to store their data as securely as possible for as long as possible, preferably with very fast access to this data. These demands prevented the development of standardized extinguishing methods.

Third, in today's world, data means money. In fact, companies only delete what they have to and only in the way they have to. Controls for this erasure methods

are currently unknown, and reliance is placed on statements by the data centers that the data is no longer available. Technically, however, this is not the case in most cases - and it can also be very lucrative for companies to store large amounts of data if the legal requirements somehow allow it.

## 6. Classification of the research

In the present study of secure deletion methods in the private, commercial and government environment, different problems could be identified.

On the one hand, there are different deletion methods that have become established, but which cannot be described as secure. The strategies of the manufacturers of storage media have not developed any secure deletion methods themselves, but have obviously used existing methods and used them in a wide variety of ways after being issued by authorities or built them into their own software.

Unfortunately, the most reliable and cost-effective method for securely deleting data on a data carrier turned out to be its physical destruction. Software solutions work differently in different environments in terms of their reliability. Private users need special knowledge in order to be able to use the software effectively. For companies and authorities, the current software is usually unsuitable for their special applications, so that individual solutions are regularly required.

A solution can lie in the approach of complete encryption of data carriers. These can be completely deleted if only the key is securely deleted. However, secure deletion methods are also required for securely deleting the key, even if it is only a matter of destroying a cryptographic USB stick.

In principle, the owners and users of data have a right, but also an obligation, to the deletion of data. This requires clear legal definitions and methods that can be used by all affected user groups.

## 7. Personal assessment

"Deleting data is old and out." I had to listen to this sentence several times during discussions on the chosen topic. In order to refute this, my motivation increased during the research and the desire for a comprehensive presentation of the topic.

At the latest, when the Ukraine war broke out in spring 2022 with cyberattacks in the area of deletion and sabotage malware, I fully understood the explosive nature of deletion procedures and their understanding.

So my original approach to deleting my private data or sensitive data of my children gave way to a more general question of data security awareness. It was nearly frightening for me to find out that manufacturers of hard drives or computer systems are not particularly interested in the secure erasure of data. The Recycle Bin solution seemed to me to be one of the most popular developments regarding deletion methods in graphical operating systems in the last few decades. Even today, no operating system can be sold to many customers without a Recycle Bin.

In contrast to this is our mania for collecting data in the context of the Internet society. Everyone stores everything, everywhere. Big data companies make billions of dollars worldwide from this data. Nobody knows where this data actually goes, how it is processed or how long the data is stored.

Statutory regulations, such as the GDPR, are intended to set rules and limits for these circumstances. Unfortunately, the formulations there are simply too vague. It doesn't do me any good if my sensitive data is considered currently deleted, but can easily be restored in two years with a clever freeware.

There is - unfortunately - a development of strategic extinguishing software in the current warfare. This technological leap has already taken place there. If companies and public authorities had thought about secure deletion methods earlier, there might already have developed strategies to prevent this situation now, or to better analyse, classify and understand it. Nowadays, data security means primarily that data can be stored securely without malware or dysfunction being able to overwrite and securely delete this data irretrievable.

As a summary of the work, methods of secure deleting data for the three target groups (private, commercial and administration) are shown. However, this is only a temporal snapshot and represents the current status, which can change quickly technologically. If file systems are developed or modified so that data can be deleted with the highest level of security without the computer system noticeably losing its performance, that would be a huge step in the direction I envisage.

## List of references

- [1] Backer-Heuvel, Glindera, Isele, Koeppe, Letter, Mönter, Schlütter, Schütze, "Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen", Bundesverband Gesundheits-IT e. V., Arbeitsgruppe Datenschutz & IT-Sicherheit, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V., Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“, Gesellschaft für Datenschutz und Datensicherheit e. V., Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen vom 20.06.2020.
- [2] Bögeholz, Harald "Sicheres Löschen: Einmal überschreiben genügt", HEISE security 16.01.2009.
- [3] BSI Leitfaden "IT-Forensik", 03/2011  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden\\_IT-Forensik.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2).
- [4] BSI, CON 6: CON.6: Löschen und Vernichten, 02/2021,  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompandium\\_Einzel\\_PDFs\\_2021/03\\_CON\\_Konzepte\\_und\\_Vorgehensweisen/CON\\_6\\_Loeschen\\_und\\_Vernichten\\_Edition\\_2021.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompandium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf?__blob=publicationFile&v=2).
- [5] Die Landesbeauftragte für den Datenschutz Niedersachsen, "Datenschutz bei Behörden und sonstigen öffentlichen Stellen in Niedersachsen" vom 07.09.2018.
- [6] Durmus, Selzer, Podesch, "Das Löschen nach der DSGVO", Datenschutz und Datensicherheit - GOOD PRACTICE, aus 12/2019.
- [7] HP. Technical White Paper, "Additional HP secure erase options on hp desktop workstations" 4AA7-8067ENW aus 07/2020.
- [8] ISO/IEC 27040:2015 "Information technology - Security techniques - Storage security".
- [9] Kissel, Regenscheid, Scholl, Stine, "Guidelines for Media Sanitization", NIST Special Publication 800-88 Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce, from <http://dx.doi.org/10.6028/NIST.SP.800-88r1> am 30.03.2022.
- [10] Schweiger, Thomas,, ENTSCHEIDUNGEN ZUM DATENSCHUTZRECHT "Löschen ist Löschen, oder doch nicht. Reicht Anonymisierung?" v. 03.02.2019 from <https://www.dataprotect.at/2019/02/03/l%C3%B6schen-ist-l%C3%B6schen-oder->



doch-nicht-reicht-anonymisierung/#:~:text=Eine%20L%C3%B6schung%20liegt%20dann%20vor,Fall%20%E2%80%93%20nicht%20mehr%20m%C3%B6glich%20ist. am 22.03.2022.

- [11] Tanguy, Jon, "Data Sanitation: Securely Erasing Micron® SATA SSDs" Rev. B 2/17, CCMMD-676576390-3423, from [https://media-www.micron.com/-/media/client/global/documents/products/technical-marketing-brief/brief\\_ssd\\_secure\\_erase.pdf?la=en&rev=2c2fbe97103d42b68d57af2e88ef50ea](https://media-www.micron.com/-/media/client/global/documents/products/technical-marketing-brief/brief_ssd_secure_erase.pdf?la=en&rev=2c2fbe97103d42b68d57af2e88ef50ea) am 28.03.2022.
- [12] Wright, Kleimann, Sundham "Overwriting Hard Drive Data: The Great Wiping Controversy" <https://security.web.cern.ch/rules/images/The%20Great%20Wiping%20Controversy.pdf> am 20.03.2022.

## Web Sources

- [web 1] BitRaser "How Do I Securely Erase A Hard Drive Using NIST 800-88 Standard?" vom 29.06.2020 <https://www.bitraser.com/kb/how-do-i-securely-erase-a-hard-drive-using-nist.php> accessed on 30.03.2022.
- [web 2] Entscheid der Österreichischen Datenschutzbehörde ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018 [https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT\\_20181205\\_DSB\\_D123\\_270\\_0009\\_DSB\\_2018\\_00/DSBT\\_20181205\\_DSB\\_D123\\_270\\_0009\\_DSB\\_2018\\_00.html](https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html) from 05.12.2018, accessed on 06.06.2022.
- [web 3] Feddern, Boi, "Google-Studie zur Ausfallursache von Festplatten", Heise, 2007, <https://www.heise.de/newsticker/meldung/Google-Studie-zur-Ausfallursache-von-Festplatten-147178.html> am 30.04.2022.
- [web 4] Fischer, Werner auf Thomas-Krenn-Wiki, [https://www.thomas-krenn.com/de/wiki/SSD\\_Secure\\_Erase](https://www.thomas-krenn.com/de/wiki/SSD_Secure_Erase) accessed on 29.03.2022.

- [web 5] Hatfield, Jim, "SMART Attribute Annex", 30.09.2005, <http://www.t13.org/Documents/UploadedDocuments/docs2005/e05148r0-ACS-SMARTAttributesAnnex.pdf> accessed on 30.04.2022.
- [web 6] IBM  
<https://www.ibm.com/docs/en/linux-on-systems?topic=tools-secure-data-deletion-devices> accessed on 21.03.2022.
- [web 7] kernel.org "ATA Secure Erase", [https://ata.wiki.kernel.org/index.php/ATA\\_Secure\\_Erase](https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase) accessed on 30.03.2022.
- [web 8] Labs, Lutz und Abels, Miriam, HEISE c't "Sicher Löschen: Daten von Festplatten, SSDs und Handys entfernen" vom 29.11.2017 from <https://www.heise.de/ct/artikel/Sicher-Loeschen-Daten-von-Festplatten-SSDs-und-Handys-entfernen-3891831.html> accessed on 28.03.2022.
- [web 9] Lenovo, "Data on Toshiba Solid State Drives may be recoverable after running the BIOS Secure Erase Function or the ThinkPad Drive Erase Utility" on <https://support.lenovo.com/uy/de/solutions/ps500072-data-on-toshiba-solid-state-drives-may-be-recoverable-after-running-the-bios-secure-erase-function-or-the-thinkpad-drive-erase-utility> on 23.03.2022.
- [web 10] Lord, Mark, Projektseite hdparm <https://sourceforge.net/projects/hdparm/> accessed on 27.03.2022.
- [web 11] NIST - SANITIZE Command [https://csrc.nist.gov/glossary/term/sanitize\\_command](https://csrc.nist.gov/glossary/term/sanitize_command) accessed on 30.03.2022.
- [web 12] NTFS references from [ntfs.com](https://ntfs.com) (LSoft Technologies Inc.) accessed on 04.05.2022.
- [web 13] NTFS Technical Reference from <https://docs.microsoft.com> accessed on 04.05.2022 (Version 10/08/2009)
- [web 14] Oracle Corporation 2010: "Löschen von Objekten in den Papierkorb" <https://docs.oracle.com/cd/E19620-01/805-5785/6j5f7pj3q/index.html> accessed on 28.03.2022.
- [web 15] Reference hdparm from <https://wiki.debianforum.de/Hdparm> am 27.03.2022.
- [web 16] Rieder, Tobias, SSD Secure Erase mit Herstellertools <https://www.ssdblog.de/2014/10/13/ssd-secure-erase-mit-herstellertools/> from 13.10.2014 accessed on 04.05.2022.
- [web 17] Samsung, "Samsung Magician 7" from [https://semiconductor.samsung.com/resources/software-resources/Samsung\\_](https://semiconductor.samsung.com/resources/software-resources/Samsung_)

Magician\_7\_0\_1\_Installation\_Guide\_v1.1.pdf am 23.03.2022.

- [web 18] Seagate “So löschen Sie Ihre Festplatte sicher” from <https://www.seagate.com/gb/en/tech-insights/how-to-ise-your-drive-master-ti/> am 23.03.2022.
- [web 19] Self-Monitoring, Analysis and Reporting Technology [https://de.wikipedia.org/wiki/Self-Monitoring,\\_Analysis\\_and\\_Reporting\\_Technology](https://de.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology) accessed on 30.04.2022.
- [web 20] Statista, “Marktanteile der Hersteller am weltweiten Absatz von Festplattenlaufwerken (HDD) im 3. Quartal 2020” from <https://de.statista.com/statistik/daten/studie/1070150/umfrage/weltweite-marktanteile-bei-festplattenlaufwerken/> am 23.03.2022.
- [web 21] Toshiba, “Why is Toshiba SSD Secure Erase important?” from <https://www.diskpart.com/ssd-management/toshiba-ssd-secure-erase-3889.html> am 23.03.2022.
- [web 22] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX\\_32016R0679\\_DE\\_TXT.pdf](https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf) am 16.03.2022.
- [web 23] Western Digital “Western Digital SSD Dashboard” from <https://wddashboarddownloads.wdc.com/wdDashboard/um/4779-705161.pdf> am 23.03.2022.
- [web 24] WIKIPEDIA “Löschen (Datei)” from [https://de.wikipedia.org/wiki/L%C3%B6schen\\_\(Datei\)](https://de.wikipedia.org/wiki/L%C3%B6schen_(Datei)) am 02.03.2022.
- [web 25] Wolski u. Schmelzle, PC-WELT, “Daten auf der SSD komplett und sicher löschen” vom 19.02.2022, <https://www.pcwelt.de/ratgeber/Datensicherheit-6581465.html#:~:text=Der%20Befehl%20ATA%20Secure%20Erase,macht%2C%20wie%20am%20ersten%20Tag.> accessed on 21.03.2022.

## List of Figures

- Figure 1. : Logical deletion of data - simplified (by F. Weijers)
- Figure 2. : Physical deletion of data - simplified (by F. Weijers)
- Figure 3. : Screenshot of the concerned data area (HxD HexViewer)
- Figure 4. : Screenshot of the concerned data area after the manipulation
- Figure 5. : Screenshot of the concerned data area in a NTFS file system
- Figure 6. : Screenshot of the concerned data area in a NTFS file system after manipulation
- Figure 7. : Screenshot of the mirrored data area in a NTFS file system
- Figure 8. : MySQL-Example “Deleting Data in Database MySQL” (by F. Weijers)
- Figure 9. : Linux Terminal with sed (by F. Weijers)
- Figure 10. : Screenshot of an encrypted Bitlocker Container in Windows 10
- Figure 11. : Screenshot (HxD HexViewer) with Password-File at Sektor 329.130
- Figure 12. : Screenshot, Password-File at Sektor 329.130 (only filename disappeared)
- Figure 13. : Screenshot, Password-File at Sektor 329.130 (nothing changed)
- Figure 14. : View of the first sectors of a formatted hard disk with FAT12 file system
- Figure 15. : View of the last sectors of a formatted hard disk with NTFS file system
- Figure 16. : Screenshot of the Twitter-Post from ESET at March 14th
- Figure 17. : Screenshot of the Twitter Post with attacked file by “AcidRain”
- Figure 18. : Photograph of File server in a storage centre of the Microsoft Azure Cloud.
- Figure 19. : Screenshot of the concerned data area in a FAT file system
- Figure 20. : Screenshot of the concerned data area in a FAT file system after fast formatting
- Figure 21. : Screenshot of the concerned data area in a FAT file system after normal format
- Figure 22. : Screenshot of the concerned data area in a exFAT file system
- Figure 23. : Screenshot of the concerned data area in the NTFS file system
- Figure 24. : Screenshot of the “mypassword” file on the NTFS file system
- Figure 25. : Screenshot concerned data area in the FAT file system after fast format
- Figure 26. : Screenshot concerned data area in the FAT file system after normal format

- Figure 27. : Screenshot of a secure erase process by the Samsung erasing Application from a YouTube Video
- Figure 28. : Screenshot from the SanDisk Website for describing the differences between secure erase and sanitize
- Figure 29. : Screenshot from the Technical Note TN-FD-29 “Running Secure Erase on Micron SDDs” Page 4
- Figure 30. : Screenshot “Western Digital SSD Dashboard” User Manual, Page14
- Figure 31. : Screenshot from manual of the latest Toshiba Storage Utilities v. 3.11
- Figure 32. : Screenshot of the description of a secure erase at the support webpage of Lenovo.com with reference to Drive Erase Utility for DOS (09/2019)
- Figure 33. : Screenshot of the master file table of a FAT16 file system
- Figure 34. : Screenshot of the file content in a FAT16 file system
- Figure 35. : Screenshot of the master file table after file wiping with Eraser
- Figure 36. : Screenshot of the file content/sector after file wiping with Eraser
- Figure 37. : Screenshot of the NTFS Journal with data (“data.txt”)
- Figure 38. : Screenshot of the file content in NTFS
- Figure 39. : Screenshot of the NTFS-Journal after wiping
- Figure 40. : Screenshot of the file content after wiping (sector 5.322)
- Figure 41. : Screenshot of the mirrored file content after wiping (sector 2.678)

## List of Tables

Table 1. :	Synonyms of deleting in the context of data science (by F. Weijers)
Table 2. :	General methods of wiping data (by F. Weijers)
Table 3. :	Overview over some common file systems (by F. Weijers)
Table 4. :	List of Wiping Software (from lifewire.com)
Table 5. :	Details of the Wipe program for UNIX (from <a href="http://wiki.ubuntuusers.de/wipe">wiki.ubuntuusers.de/wipe</a> )
Table 6. :	Details of the coreutils program for Linux (from <a href="http://wiki.ubuntuusers.de/shred">wiki.ubuntuusers.de/shred</a> )
Table 7. :	Details of the secure-erase application for Linux (from <a href="http://srm.sourceforge.net/">srm.sourceforge.net/</a> )
Table 8. :	5-step model for evaluation and comparison
Table 9. :	Another model for evaluation and comparison with plus and minus
Table 10. :	Criteria description for evaluation and comparison
Table 11. :	Evaluation of the Recycle Bin solution
Table 12. :	Evaluation of special Software
Table 13. :	Evaluation of the physical destruction of storage devices
Table 14. :	Evaluation of the Recycle Bin solution
Table 15. :	Evaluation of special Software
Table 16. :	Evaluation of the physical destruction of storage devices
Table 17. :	Evaluation of the Recycle Bin solution
Table 18. :	Evaluation of special Software
Table 19. :	Evaluation of the physical destruction of storage devices
Table 20. :	Table overview of common deletion procedures and rating by Florian Weijers

## Abbreviations

Art.	Article
ATA	Advanced Technology Attachment
DOS	Disk Operating System
DSGVO	See GDPR
DSF	Distributed file system
ESET	ESET, spol. s. r. o.
etc.	And so on
exFAT	Eextended File Allocation Table
FAT	File Allocation Table
GB	Gigabyte
GDPR	General Data Protection Regulation
HDD	Hard disk
IBM	International Business Machines Corporation
IDE	Integrated Drive Electronics
IEC	International Electrotechnical Commission
ISE	Instant Secure Erase (Seagate)
ISO	International Standards Organization
IT	Information Technology
KA-Sat	Eutelsat KA-SAT A9 satellite network
KB	Kilobyte
MB	Megabyte
MLC	Multi Level Cell (2 bit with 4 charge states)
NFS	Network file system

NIST	National Institute of Standards and Technology - U.S. Department of Commerce
NTFS	New Technology File System
NVMe	Non-Volatile Memory Express
OS	Operating system
Para.	Paragraph
PC	personal computer
PLC	Penta Level Cell (5 bit with 32 charge states)
PRNG	Pseudo random number generator
QLC	Quad Level Cell (4 bit with 16 charge states)
RAM	Random Access Memory
Rev	Revision
SATA	Serial Advanced Technology Attachment
SD	Solid Disk
SLC	Single Level Cell (1 bit with 2 charge states)
S.M.A.R.T.	Self-Monitoring, Analysis and Reporting Technology
SSD	Solid State Disk
SSHD	Solid State Hybrid Disk
TB	Terabyte
TLC	Triple Level Cell (3 bit with 8 charge states)
USB	Universal Serial Bus



## Honourable Assurance

I declare on my honour that I wrote this bachelor thesis independently and that I have used verbatim quotations from the literature and the use of the ideas of other authors at the appropriate places within the work.

The work has not been submitted to any other examination authority in the same or a similar form.

Wismar, 01.07.2022

[Florian Weijers](#)

# Verteidigung Bachelor-Thesis

**“Darstellung und Bewertung gängiger Methoden zum  
Löschen von Benutzerdaten in gängigen  
Computerdateisystemen.” - F. Weijers**

**25.07.2022**

09:00 Uhr bis 09:20 Uhr

# Übersicht der Präsentation

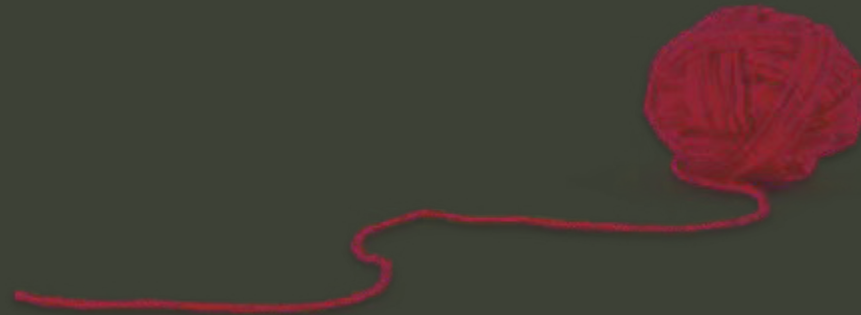
- Klärung der Tatbestände der Aufgabenstellung
- Analyse der Lösungsverfahren
- Arten von Löschmethoden
- Untersuchung der Papierkorblösung
- Untersuchung von Softwarelösungen
- Erläuterungen zur Datenträgerzerstörung
- Crypto Erase und SATA\_SECURE\_ERASE
- Entwicklung von Bewertungskriterien
- Bewertung der Lösungsverfahren

(20 Minuten)



# Arbeitstitel

“Analyse und Vergleich **ausgewählter Verfahren** zur Löschung von **Nutzerdaten** im Hinblick auf **gesetzliche Anforderungen, technische Verfahren** und **praktische Umsetzungsmöglichkeiten** zur **sicheren Löschung** von Daten in gängigen Dateisystemen.”



# Klärung der Tatbestände und Termini

Was meinen wir, wenn wir von “löschen” sprechen?

In welchem Zusammenhang sollen oder müssen Daten gelöscht werden?

Was und warum wollen wir überhaupt löschen? (Informationen? Daten allgemein?)

Was ist in diesem Zusammenhang der Inhalt der wichtigsten Richtlinien?

Was ist aktuell der Stand der Technik, bzw. was wird aktuell technisch angewandt?

Was bedeutet “nicht wiederherstellbar” im Bezug auf das Löschen von Daten?



# Analyse der Lösungsverfahren

- Löschen durch Verschieben in den Papierkorb
- Löschen von Daten in Dateien (e.g. Textdateien)
- Löschen in Datenbanken
- Löschen in komprimierten Datencontainern (.zip, .vhdx, etc.)
- Löschen in verschlüsselten Datencontainern (.vhdx)
- Löschen innerhalb von virtuellen Maschinen
- Löschen von kompletten Festplatten
- Löschen durch Zurücksetzen in den Werkszustand
- Löschen im Rahmen von Cyberattacken/Cyberwar
- Löschen in entfernten Cloudspeichern
- Löschen durch Formatieren
- Löschen durch physikalische Zerstörung des Datenspeichers



# Arten von Löschmethoden

→ Gruppierung in drei Bereiche:

1. Löschen durch Verschieben in den Papierkorb (unsichere Methode, am meisten verbreitet und genutzt)
2. Löschen mittels Spezialanwendungen (als softwarebasierte Methode, unklare Arbeitsweise, zweifelhafte Sicherheit)
3. Löschen durch physikalische Vernichtung (als Referenz für sichere Datenzerstörung, nicht für jeden Löschprozess durchführbar)

Hintergrund sollen die Sicherheitsaspekte der Löschverfahren sein.

Ist die Methode sicher? - Was nutzen die Anwender? - Gibt es Probleme dabei?

---

## **Zentrale Frage:**

Erreichen wir mit der Löschmethode das, was wir mit “Löschen” meinen? → Erstellung einer Löschstrategie.

# Untersuchung der Papierkorblösung

- in allen Betriebssystemen vorhanden
- in Mobilgeräten vorhanden
- unterstützt den Nutzer beim Aufbewahren von Daten
- Vorstufe zum Löschen

→ rechtlich kein Löschvorgang, da die Daten ohne besondere Kenntnisse wiederhergestellt werden können

→ “populärste” Löschmethode wegen Nutzerbedürfnissen





# Untersuchung von Softwarelösungen

- Tools für Windows
- Tools für Linux, iOS, Android, etc.

→ Software arbeitet mit hardwarenahen Schreibroutinen und überschreibt Daten.  
→ Überschriebene Daten können nicht unter Standard Laborbedingungen wiederhergestellt werden.  
→ Es gibt keine Lösung für Daten in Backups, im Cloudspeicher, etc.

+ Die Software arbeitet nicht immer fehlerlos!

Beispiel: Im NTFS Dateisystem werden Mirror-Daten im Wipevorgang nicht berücksichtigt.

→ Somit ist Spezialsoftware nur in Einzelfällen (z.B. bei kompletten Festplatten) anwendbar.

# Erläuterung zur Datenträgerzerstörung

Wichtiges Kriterium: Man braucht physischen Zugriff auf den Datenträger.

Für sensible Daten ist die physikalische Zerstörung im Behördenumfeld weltweit empfohlen (NIST, BSI) und langjährig bewährt.

Praxisnahe Anwendungen:

- Granulierung
- Verbrennen
- Einschmelzen
- Auflösen
- evtl. auch Durchlöchern oder Deformieren

Datenträger kann nach erfolgreicher Zerstörung nicht wiederverwendet werden (auch das Recycling ist aufwändig)

# Crypto Erase und ATA\_SECURE\_ERASE

Im Gedanken gut: ATA\_SECURE\_ERASE

- sollte in der Firmware aller Festplatten seit 2002 vorhanden sein (Vorgaben durch FISMA)
- kann aber nicht immer ausgelöst werden (Blockade durch OS oder BIOS)
- jeder Hersteller von Festplatten hat irgendwie etwas anderes implementiert

*(Warum sollten Festplattenhersteller Tools entwickeln, welche ihre Verkaufszahlen reduzieren würden?)*

## Alternative:

Komplettverschlüsselung der Daten (z.B. Bitlocker) ist im Löschvorgang überaus sicher, wenn der Schlüssel sicher gelöscht wird.

## Negativ:

- Keine intuitive Bedienung
- Zwischenschritte nötig
- Datenkopien, Indexe oder Caches werden ggf. nicht sicher gelöscht
- Muss an den Usecase ggf. umständlich angepasst werden (Cloudspeicherung? Dateisysteme? Einzelne Dateien?)



# Entwicklung von Bewertungskriterien

Wie kann man Lösungsverfahren miteinander vergleichen?

Wie würden Nutzer das Löschen von Daten vergleichen?

Anhand von

- Komplexität ("Ist das Verfahren für mich überhaupt anwendbar?")
- Performance ("Muss ich lange auf das Ergebnis warten?")
- Systembelastung ("Kann ich mein Computersystem dabei weiter benutzen?")
- Sicherheit ("Ist das Lösungsverfahren für meine Ansprüche sicher genug?")
- Kosten ("Sind die Kosten des Verfahrens tragbar?")

5-Kategorien:

++	+	o	-	- -
sehr gut	gut	neutral	negativ	sehr negativ
sehr gering	gering	mittel	hoch	sehr hoch
<i>Der Wert ist vernachlässigbar gering.</i>	<i>Der Wert ist messbar und kann jedoch grundsätzlich als unbedeutend beschrieben werden.</i>	<i>Der Wert ist unter normalen Bedingungen tolerierbar.</i>	<i>Der Wert ist so hoch, dass es zu Beeinträchtigungen kommt.</i>	<i>Der Wert ist so hoch, dass er regelmäßig nicht zu tolerieren ist.</i>



# Bewertung der Lösungsverfahren

	Papierkorbmethode	Spezialsoftware	Spezielle Bootsysteme	physikalische Zerstörung
Sicherheit	gering	hoch	sehr hoch	sehr hoch
Eignung für private Anwender	hoch	mittel	hoch	gering
Eignung für Unternehmen	gering	mittel	mittel	hoch
Eignung für Behörden	sehr gering	hoch	gering	hoch
Komplexität	sehr gering	mittel	hoch	sehr gering
Leistung u. Geschwindigkeit	sehr hoch	gering	sehr gering	sehr hoch
Systembeeinträchtigung	sehr gering	mittel	sehr hoch	sehr gering
Kosten	sehr gering	gering	gering	mittel
Empfehlung i.S. rechtlicher Vorgaben	nein	möglich	ja	ja
Entspricht der DSGVO	nein	möglich	ja	ja
Gesamtbewertung	o (neutral)	o (neutral)	o (neutral)	++ (sehr gut)

# Verteidigung Bachelor-Thesis

## Vielen Dank für die Aufmerksamkeit!

Gerne beantworte ich Fragen zur konkreten Thematik und stehe für fachliche Diskussionen  
selbstverständlich zur Verfügung.

F. Weijers

(PC- u. Einsatzforensik der KPI Kempten)

