Practical Application of Cryptographic Checksums

With an Introduction to Signing and Encryption

Peter Jockisch, Freiburg i. Br.
peterjockisch.de

May 18, 2024

Computer files can be manipulated in many ways unnoticed. Cryptographic checksums, hash values, serve to protect your data: By forming an electronic fingerprint of a file, an always constant numerical value is created. If this value deviates at a later point in time, there is damage or manipulation. With a single mouse click, the integrity of a file can be checked at any time.

Contents

1 Terms and Fields of Application

1.1 Introduction

Cryptographic checksums form the basis for cryptographic signing and encryption, for website- and e-mail certificates, for the qualified electronic signature, and for the technical understanding of revision-proof e-mail archiving, to which all merchants are legally obliged.

This introduction presents two free graphical programs for checksum generation, CyoHash and Jacksum, for file manager operation.

Console-based programs are also described; they are available for all operating systems and are pre-installed under MS Windows as well as under most Unix/BSD and GNU/Linux sys-

tems. This means that no programs need to be installed, the existing operating system resources are completely sufficient to create checksums.

1.2 Functional Principle

1.2.1 Electronic Fingerprints

Humans are complex creatures. In order to identify them quickly and easily, fingerprints are often created. Computer files can be identified according to the same principle: by generating an "electronic fingerprint", the so-called cryptographic checksum, an always constant number. By means of standardized procedures, a fast integrity and authenticity check of files of any kind can be carried out. Human fingerprints are created with stamp pads, electronic fingerprints with a checksum program.

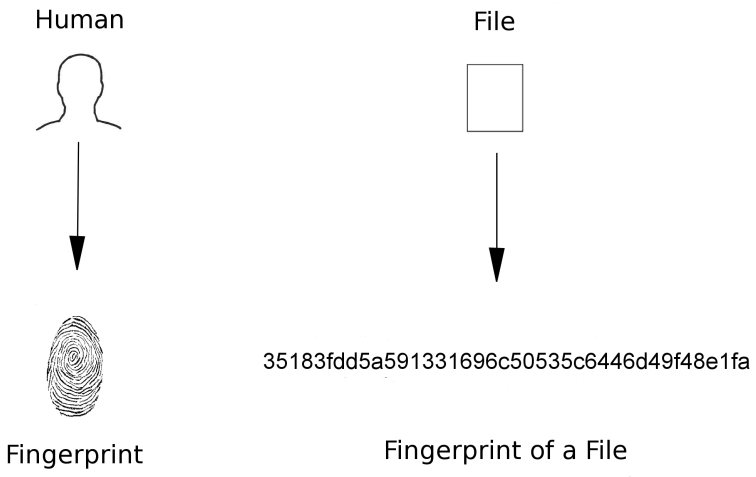

Figure 1: Proof of authenticity for human and computer files

1.2.2 Quality Criteria

We consider *cryptographic* checksums. They are based on hash functions that provide hash values as a result for any file. This value is also called a hash code or hash.

A file, as well as identical copies of it, always has the same hash value checksum. However, if even a single bit or character changes due to damage or manipulation, a completely different hash code should result.

A hash function checksum procedure should therefore always provide different values for different computer files. The calculated checksum is always the same length, depending on the method used. Therefore, of course, only a limited number of numbers can be depicted: There are practically an infinite number of computer files, so that it is impossible to assign a different value to each of these files with a number of fixed length.

From a security perspective, there are various attack scenarios, including the falsification of documents. An attacker wants to create a forged version of a given original file, for example a business order, with a manipulated, increased order quantity that has the same hash value checksum. Once he has made the changes to the document, he then tries to obtain a file version whose cryptographic checksum is identical to that of the original file by trial and error, perhaps by inserting invisible control characters. Supporting computer programs are of course used in such an attack.

If an attacker actually manages to create a second file containing the desired manipulations and with the same cryptographic checksum as the original file in a reasonable amount of time, the hash function method in question is "broken". Once such a weakness becomes known, it should no longer be used. Weaknesses are recognized a long time in advance through continuous research work.

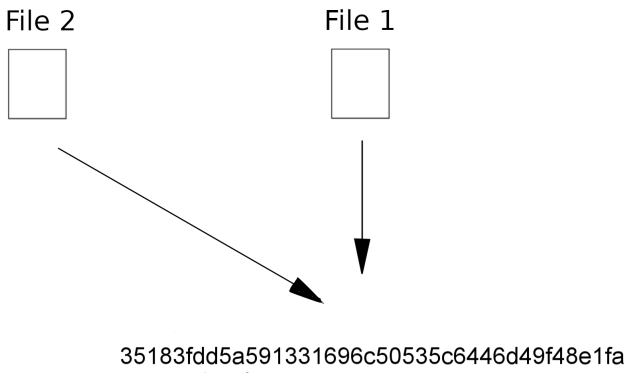

Figure 2: Checksum collision

If there were a computer with infinite computing power, it would theoretically be possible to break every procedure by simply trying out all the possibilities (brute force attack). In practice, such an approach is considered impractical in the majority of cases, as the necessary calculations can almost never be carried out in a reasonable amount of time.

Most hash functions only had a limited lifespan and were eventually replaced by successor procedures for security reasons.

More powerful computer generations contribute to shortening the service life. In addition to computational power-based attacks, however, there are also other types of attacks, and it can never be ruled out that practicable attacks are already possible today with the aid of mathematical creativity.

A huge army of mathematicians works and researches in the background, especially for intelligence services. Not all scientific findings are published.

1.2.3 Prevailing Standards in the West and Russia

Until 2016, the Western IT infrastructure was predominantly based on the SHA-1 algorithm (Secure Hash Algorithm 1). This has been considered definitively broken since 2017, and the computing time required to corrupt it has fallen drastically. Experts now recommend the SHA-2 variants SHA256, SHA384 or SHA512. The recommended successor algorithm to SHA-2, SHA-3[1], has been officially established since 2012.

In Russia and many other CIS states, GOST R 34.11-94 respectively GOST 34.311-95 was the previous hash standard in public authorities and in various economic sectors.[2] As with SHA-1, structural weaknesses were also found with it.

1.3 Are there Technologies that are blocked for the Public?

1.3.1 Outdated Computer Systems

All computational power-related statements in this introduction refer to computer systems and research work that are publicly available or released to the general public. The use of the latest, most advanced computer technology is presumably still reserved for the intelligence services in order to ensure that they always have an advantage in computing power for effectively undermining established encryption technology.

The encryption procedures released to the public may not be easy to break for lower administrative levels. However, at the very top of the hierarchy, i.e. at intelligence service level, there should be unrestricted access to the latest computer technology. In addition, all data transferred via the global network is presumably archived for automatic analysis. From this perspective, the strength of files sent over the Internet that have been encrypted using publicly standardized technology is put into perspective.

It has long been considered that certain cryptographic algorithms that have been elevated to official standards could have inherent mathematical weaknesses that are only known to experts in the intelligence services. The possible influence of the intelligence services on the design of security products (software and possibly hardware backdoor problems, open questions about standards, etc.) is the subject of numerous articles on computer security, for example in "Did NSA Put a Secret Backdoor in New Encryption Standard?". Several renowned companies have already directly or indirectly confirmed that they are working with intelligence services on their product development. One of the official reasons given for this is the intention to to optimize the technical security of company products. The extent of the pressure exerted for "cooperation" can only be guessed at.

Corrupted electronics, known or unknown "advanced" hardware architectures with factory-installed "remote maintenance functions", "possibly even with a radio system built into the processor", represent the other side of the problem.

[1] "NIST Releases SHA-3 Cryptographic Hash Standard", August 05, 2015.

[2] February 02, 2014, extract of the information about the procedures supported by RHash, "Hash Functions": "GOST is a hash function defined in Russian national standard GOST R 34.11-94. It has two widely used versions with testparameters and CryptoPro ones. It's relatively slow, but it is used for digital signature in Russian State banks and enterprises. Hash is a hexadecimal string of length 64."

1.4 Application Examples: Business World, Internet, Archiving

The legally recognized personal proof of authenticity is almost always linked to the use of proprietary software and hardware. Section 1.5.5 contains further sources of information on the comprehensive requirements of the so-called qualified electronic signature, the WP articles "Electronic signature" and "Digital signature" refer to the legal and mathematical/technical aspects (definition of terms).

The creation of cryptographic checksums not only provides information on the authenticity and integrity of files. It also enables confirmations of receipt and a written confirmation of the last processing status of a file, as the following examples demonstrate.

1.4.1 Maintaining File Integrity

You create a business balance sheet and then go on vacation. For quality control purposes, you make a note of the cryptographic checksum of the completed balance sheet file before you leave. After your vacation, you create the checksum again to verify whether the file is intact or whether it has been damaged or manipulated.[3]

Unauthorized access, e. g. to an accounting file, can be detected in this way. In such cases, notify the system administrators and insist on restoring the original file version, which is of course only successful if the file again has the checksum noted.

The file date and version management systems are no substitute for cryptographic checksums, as both can be manipulated directly or indirectly. Specialized programs can change both the creation and modification date of files, even directory-wide.

The consistency check via checksums works faster, more effectively and more securely and is possible at any time thanks to pre-installed operating system programs that can normally be executed under standard user accounts (description in section 2.3).

1.4.2 Indication of the Processing Status of a File

When leaving a company, you would like to have the last processing status of a computer file confirmed in writing, example text: "Confirmation: This is to confirm that the file [file name] last maintained by [first name last name] had the SHA-256 checksum [specific checksum] in its last processing status on [date]. [Company stamp, date, name and signature of supervisor]".

Insist on a legally binding signature (no initials).[4] In this way, company secrecy is maintained and you can still protect yourself to a certain extent. Should there ever be any queries, you will have a written record of your last processing status.

Two or three different cryptographic checksum procedures may be recommended. This could be more secure in the long term, as one of the methods may last longer in the future.

[3] Example taken from "Fingerprinting Your Files", Simson Garfinkel, MIT Technology Review, August 4, 2004.
[4] Further information: Googlee search query "initials vs signature", "Have you seen this? Initial and signature are two different things", "Signature & Initials: What is the Difference".

1.4.3 Armament Against White-Collar Crime, Protection against Bullying

As part of general quality control and whenever corruption, lies, intrigue, bullying, sabotage and white-collar crime are likely, the use of cryptographic checksums is recommended for your own protection, including before presentation dates (file verification). Signing software is often ruled out as it is naturally linked to encryption functions and is therefore not tolerated on every workstation. Company secrets could be encrypted and leaked to the outside world or malware could get in undetected. However, a free checksum program – not to be confused with freeware[5] – can be installed responsibly on company computers if the system administrator deems it appropriate.

1.4.4 File Reference in Contracts and Confirmations of Receipt

For written contracts and confirmations of receipt, electronic fingerprints make it easier to refer to computer files. Files of any kind can be uniquely identified via their hash value, e.g. text documents, video films, call recordings and interviews (generally sound files), programs, CAD files. Services rendered that are finally available in the form of a data carrier, e.g. a CD-ROM or DVD to be delivered, can also be confirmed in writing in this way.

Electronic fingerprints can also be created from archive files.[6] Acknowledgements of receipt are a broad area of application.

In the context of image licensing, reference can be made to photos via checksums.

1.4.5 Telephone transmitted indication of the authenticity of documents sent

The recipient of a file or a data carrier sent by letter post can be informed of the hash function checksum by telephone for verification purposes. Forging a voice has become much easier since the introduction of the "Adobe Voco" software,[7] but it is still time-consuming. However, personalized signing would be more convenient and more secure.

1.4.6 Hash Value Publication as Substitute Proof of Authenticity

Some countries only allow limited encryption and signing (personalized electronic proof of authenticity). To a certain extent, cryptographic checksums can serve as a substitute:

1. First create the message or document separately as a computer file

[5] The term "freeware" is not clearly defined. It may or may not refer to "free software" (source code/"program text" is available, may be modified and distributed). Tendentially, it predominantly refers to software that is distributed free of charge but whose program code remains unpublished ("categories of free and nonfree software").

[6] "Packing programs" are used to create archive files or file archives, known as "archives" for short. In particular, they offer the option of combining several individual files and nested file folders, i.e. those containing subfolders, into a single file. This means, for example, that entire websites and extensive personal compilations of documents can be conveniently attached to an e-mail as a single file or saved to a data carrier. WP article "Data Compression", recommendation "7zip", free data compression software.

[7] Regarding the authenticity of spoken language, everyone is advised to read the sections "Technical details" and "Concerns" in the WP article Adobe Voco.

(text or PDF file, image, video, etc.). Attach the file to an e-mail and send the message.

2. Publish the hash codes of the documents sent on a website in a diary-like manner. Several reputable free (ad-financed) web hosting services are available for this purpose. Internet pages can also be created without (X)HTML knowledge, e.g. with free HTML editors.

Alternatively, free blog systems that do not require any technical design knowledge are recommended, including Blogger.com and WordPress.com, Comment functions can be kept deactivated.[8]

When making your selection, make sure that your website is SSL/TLS-secured and that your user password is also always encrypted for transmission over the Internet.

Finally, create schematic entries, for example in the form checksum method – file checksum. No more information is required. For extensive daily entries, you could optionally add a file name abbreviation. The email attachment "Request.pdf" would then become "R...t.pdf" or simply "R...t".

1.4.7 Publishing Documents with Hash Values

For the publication of documents on the internet or intranet (company networks, etc.), it is advisable to specify hash values, possibly on a subpage, in the download section. The use of a legally recognized SSL/TLS certificate[9] for the encrypted transmission of web pages with the published checksums increases security. By comparing the hash values, users can be relatively certain that documents downloaded from reputable sources are free from malicious code (viruses etc.), manipulation and transfer damage. However, certificates issued by external authorities may be associated with residual risks.[10]

1.4.8 Archiving Files

When archiving files on CD-ROMs and DVDs, it is advisable to make a note of the data carrier hash code. To check this, compare the actual value with the originally noted hash value at regular intervals. In this way, early damage can be detected. Regular copying to new archiving-specialized data carriers at relatively short intervals is unfortunately still unavoidable at present.

1.4.9 Increased Security for Password Storage

There are numerous other possible applications in computer science and electrical engineering, for example a variant of the security-enhanced storage of user account data: Passwords can also be stored exclusively in the form of their associated hash values. If the user enters his plain text password again, the hash value is generated again and compared with the stored one. In the event of a data breach or data

[8] In the overview article "Free Typesetting Software for the Professional Document Preparation", section 13, "Introduction to the Creation of Websites", describes basic aspects

[9] Certificates are IDs for the Internet (networks in general), mostly e-mail or website certificates, they enable encrypted data transmission (https://), which makes it relatively impossible for people and organizations *under* the law to read them (WP article: Digital certificate)

[10] "New Research Suggests That Governments May Fake SSL Certificates ", Seth Schoen, EFF, March 24, 2010

theft, no plain text passwords are lost for the time being.

Good modern hash functions work like one-way functions. They assign an individual hash value to a file. However, the reverse way, the calculation of the original file from the hash value, is not possible in a practicable time - according to the current publicly known state of knowledge, which is based on the publicly available methods and technologies.

1.4.10 Legally recognized, Audit-Proof E-Mail Archiving

In some industries, emails that lead to business transactions/orders are legally regarded as commercial letters.[11] Simple saving or printing is no longer sufficient for their archiving; instead, they must be archived in an audit-proof manner in a technical way that excludes any subsequent, undetectable and unnoticed manipulation of the e-mail data.

The technical implementation is presumably carried out with the help of cryptographic checksums in most programs. Electronic fingerprints are created from all incoming and outgoing emails and stored in encrypted form. If, for example, an auditor wants to gain insight into a specific e-mail, the stored e-mail file is loaded into the corresponding e-mail archiving program, e.g. from a CD-ROM. When it is read in, the cryptographic checksum of the email file is generated again and compared with the originally archived checksum to ensure that it matches.

Only very specific software and/or hardware solutions from specific manufacturers are legally recognized within the scope of the legal requirements. There are numerous high-quality introductory articles on this subject available in the Internet, written by specialized lawyers and IT experts.

1.5 Cryptographic Signature, Website and E-Mail Certificates

1.5.1 Cryptographic Signature and E-Mail Certificates

In the past, people or offices provided their documents with additional proof of authenticity by applying complex patterns, seals, to the documents using sealing lacquer or sealing wax and sealing stamps. Today, cryptographic keys or certificates have taken over the function of the seal stamp: For a document, e.g. an e-mail file, with the help of a certificate (an ID card) an accompanying, personal proof of authenticity is calculated, the so-called cryptographic signature. Upon receipt of the message, the recipient's e-mail program automatically determines (with the help of this signature, among other things) whether the document was actually created by the specified sender (certificate holder/ID card holder).

E-mail and website certificates thus have an identification function with which correspondence partners and websites can prove their identity.

Classic ID cards are issued by state authorities. Email and website certificates are issued by so-called certification authorities. And this is where the two decisive differences lie: classic ID cards are all equivalent to each other and officially recognized, there is only one issuer who also acts as a certification institu-

[11] In German referred to as "Handelsbrief".

tion: the state. E-mail and website certificates, on the other hand, exist in different quality classes with different levels of validity. Only certificates of the highest quality class (class 3 e-mail certificates or EV website certificates), issued by officially recognized certification authorities (CAs), are legally recognized.

The OpenPGP encryption standard works both with and without certification instances, i.e. you can use self-created key certificates for signing and encryption:

1.5.2 Signing and Encrypting Eiles and E-Mails with OpenPGP

The OpenPGP encryption standard enables signed e-mail communication both with and without certification authorities (CAs). For signed (and encrypted) communication, you create a (secret) key (certificate) and send the associated public certificate part to your communication partners by e-mail, publish it on the Internet or hand it over on site on a data carrier. Your private, secret key can also be archived on paper.[12]

When signing documents or e-mails, you then enter your passphrase, whereupon an (accompanying) signature is created for your e-mail or file; the passphrase can optionally be saved temporarily. The e-mail client of your correspondence partner then verifies fully automatically in the background (with the help of your public certificate part) whether the attached signature was created with your secret key (certificate).

If you want to send an encrypted document, you need the public OpenPGP certificate part of the file or e-mail recipient, also in order to check his/her attached e-mail signatures for authenticity.

Installation: An encryption program and the command line would suffice, but most users prefer graphical interfaces. So you need two or three programs:

1. Encryption software

GnuPG, Gnu Privacy Guard (WP article) is a free, cross-platform, 100 % royalty-free encryption program for Unix/ BSD, GNU/Linux, MS-Windows and MacOS. The MS-Windows version is called Gpg4win (no donation required for download). The GPG4win suite already contains the graphical interface, the crypto manager Kleopatra and the program extension GpgEX for the Microsoft file manager Windows Explorer, for right-click file encryption and signing.

2. Graphical Interface

Furthermore, you need one of the numerous free graphical interfaces (frontends), for example the already mentioned Kleopatra for MS-Windows and Unix/BSD or GNU/Linux, to create keys (certificates) via a graphical menu and to sign or encrypt files.

3. E-Mail Program or Extension

For fully automatic operation with e-mail clients, use the standard built-in function or use one of the numerous free (extension) interfaces, such as GpgOL for MS Outlook, which is already included in the GPG4win suite.

[12] Read more about this: “Paperkey – an OpenPGP key archiver”, “Backup your PGP key with pencil and paper”, “Paperkey” and “How to backup gpg keys on paper”.

1.5.3 Key Generation, E-Mail use, Signing and Encrypting Files

Now create your secret key; you can generate as many test keys as you like to try it out.

Generate Iey

Think of a passphrase and then create your key with Kleopatra: "File" → "New Certificate" → "Create a personal OpenPGP key pair". Then make a backup copy on a USB stick and/or CD-ROM/DVD. Use the Kleopatra export function for this (select the key beforehand with a mouse click): "File" → "Export Secret Keys". To export the secret key, you will be asked to enter your secret passphrase. You can open the key in a file viewer or in a text editor, at the beginning or end of the file you will see "-----BEGIN PGP PRIVATE KEY BLOCK-----" resp. "-----END PGP PRIVATE KEY BLOCK-----". Cached key copies could be read.

Exporting the Public Key

Export your public key part via "File" → "Export". Check immediately that this is the public key part, save it on the desktop, for example, and then drag the file into a text editor or a browser, for example Mozilla Firefox. At the end resp. at the beginning is "-----BEGIN PGP PUBLIC KEY BLOCK-----" respectively "-----END PGP PUBLIC KEY BLOCK-----".

E-Mail Use

Some e-mail programs support signing and encryption with OpenPGP by default, others require an extension to be installed beforehand. Look for the corresponding instructions.

After activation, you can sign your emails by default. To be able to check the signatures of incoming emails (or to encrypt for third parties), you must have loaded the public key part of your respective correspondence partner into your program once. Some programs have their own OpenPGP implementation. When using GnuPG, select "File" → "Import Certificates" in the Kleopatra menu to import the public key part.

Each key has a fingerprint, which can also be transmitted verbally over the phone. To display it, select the key under Kleopatra, right-click to open the menu and select "Details". Keys can also be authenticated by third parties. Read: "The Kleopatra Handbook".

Familiarize yourself with the functions, start by writing a signed test e-mail addressed to yourself. Read further instructions, including the WP article "GNU Privacy Guard".

Signing and Encrypting Files

You can create signatures for your files or encrypt them with your own key (or with third-party public keys). Try it out with any document, for example with a text file. Under MS-Windows: Go to the document and press the right mouse button, the drop-down menu opens, select the GpgEX options (symbol with open lock) and select the "Sign" function, whereupon the signature is created after entering your passphrase. Then go to this created accompanying signature file and select the corresponding GpgEX option again, whereby you can carry out an automated check. Try out the numerous functions of the GpgEX options menu.

Encryption with password: You can also encrypt a file with a password so that only those who know the password can open the file.

Files can also simply be dragged into the open Kleopatra window, whereupon an action menu appears, or you can select a desired action in the Kleopatra file menu, which opens the file manager.

If you want to encrypt a file for a specific recipient, you must select his public key. Create a test folder and try out all the functions.

1.5.4 Website Certificate industry under Fire

Internet pages can be accessed in encrypted form (hhttps) so that third parties subject to the law cannot read the content of the web pages accessed or any correspondence (password transfer, data transfer, etc.). Institutions above the law (intelligence services at the highest level) can presumably read everything, if necessary by means of pure computing power, with computer technology blocked for the public. Leaving aside the possibility of direct or indirect backdoors in computer systems and possible inherent mathematical weaknesses in the algorithms, at present everything ultimately boils down to a prime factorization, which in turn is a pure computational problem. A translated excerpt of a German article (2016/2017): "[...] To emphasize once again: Quantum computers mean the end of all currently established public key methods for digital signatures and key exchange, among other things. Thus, a considerable part of the foundation of current crypto systems breaks away completely. An adequate replacement is not yet in sight. [...]".[13] Also read the WP article "Post-quantum cryptography" to get an overview of critical factors and aspects.

The encrypted transmission of Internet pages takes place with the help of (web site) certificates. The international website certificate issuer industry as a whole has been subject to severe criticism for years. On the one hand, because individual CAs (Certification Authorities) repeatedly issue certificates to unauthorized parties due to inadequate verification procedures when applications are submitted. On the other hand, due to hacker intrusions that have occurred, through which third parties were able to issue formally recognized certificates for various popular websites and companies without being noticed. The criticism can be summarized to the effect that the current technical basis of the certificate system is too vulnerable to such errors and attacks and that it cannot be used to take countermeasures effectively and quickly enough. Search terms such as SSL-Desaster, or SSL debacle lead to discussions and further articles in the world wide web. Extensive sources of information: CA/Browser Forum, "The EFF SSL Observatory".

1.5.5 The Qualified Electronic Signature

Cryptographic checksums are part of the personal proof of authenticity of documents (tied to identity), the so-called qualified electronic signature (legally recognized), as well as generally of numerous cryptographic procedures, e.g. the encryption of (message) documents. Knowledge of the relevant contact points

[13] Jürgen Schmidt, "Kryptographie in der IT - Empfehlungen zu Verschlüsselung und Verfahren", sub-article "Elliptische Kurven Verschlüsselung", heise Security.

and sources of information is of advantage.

1.5.6 Central Information Sources on Applied Cryptography

Cryptography at International Business Level

Bert-Jaap Koops' "Cryptography Law Survey" provides information on the basic legal situation regarding cryptography in the individual countries and administrative constructs of the world. Each entry is accompanied by a comprehensive collection of further sources (as of 2014): cryptolaw.org

On the History of Cryptography

Wikipedia provides detailed information on the publicly known history of cryptography, including: "History of cryptography".

1.6 Further Application Possibilities

Checksums have also been used in electrical engineering for many decades, among others to ensure error-free data transmission.

1.7 Possibilities of Misuse

1.7.1 Fully automatic Identification of Consumed Content

Cryptographic checksums can also be used for questionable purposes. The media player of a software manufacturer is said to have sent unsolicited hash codes of the files played in the past.[14]

Theoretically, a fully automated comparison with database tables could be used to determine whether the content used has been licensed and which political films and sound files a user prefers to watch. Individual computers could be identified by a combination of features, and checksums could of course also be sent at operating system level. The same would also be possible for proprietary PDF programs.

Alternatively, free PDF viewers and free media players are available, such as the highly recommended VLC media player. However, comprehensive, maximum security always requires a free operating system basis.

In computer forensics and countless other fields of information technology, the creation or retrieval of cryptographic checksums is ubiquitous. This is a very constructive application, also in terms of preserving evidence in computer crimes, e. g. after network intrusions.

In dictatorships or in occupied, foreign-ruled countries, there is a risk that hard disk searches will be carried out locally or remotely. Software and hardware manufacturers can use backdoors to routinely create cryptographic checksums of all existing hard disk files and then compare them fully automatically with the checksums of "indexed" and censored content, such as political educational films. In this way, it is possible to quickly and effectively check whether citizens tend to cultivate their own opinions and whether they consume political content that contradicts officially proclaimed dogmas. Free thinkers can be easily identified in this way.

If all checksums of files newly created and changed by the user were sent automatically at regular intervals, it would also be possible to determine retrospec-

[14] "Serious privacy problems in Windows Media Player for Windows XP", February 20, 2002

tively in which network or on which computer a document was first created. The amount of data is tiny and, if it is also encrypted, practically indecipherable. Changing the file name does not change the checksum. Other features, such as hardware and software configurations (including unlicensed programs), can also be analyzed and "reported" fully automatically.

In a lecture given at the University of Bielefeld on June 23, 2010, lawyer Udo Vetter mentions software used by the police for hard disk searches, which is said to also have already triggered a false alarm.[15]

It cannot be ruled out that computers of regime critics are deliberately paralyzed remotely. For example, the remote installation of a single process that operates permanently from computer startup and consumes the entire computing power is sufficient, a process that can possibly still be recognized via ps -e but can no longer be terminated (see also pstree). The installation of functional program errors is another way of partially or completely paralyzing the computers of dissidents.

Sabotage measures could also be automated if statistical evaluations in the background show that a high level of political educational films are consumed and that there is a "danger" of distributing or publishing critically scrutinizing information.

1.7.2 Software Activation and Computer Identification via Electronic Fingerprints

In an article on privacy, the Free Software Foundation (FSF) lists computer characteristics that can be used to uniquely identify and recognize a computer. Such characteristics are most probably summarized in a hash and archived in a database. With some proprietary products, software activation (product activation) is linked to the hardware configuration determined. Attempts to install the purchased software on a second computer at the same time often fail.

1.8 Signing and Encrypting Eiles

1.8.1 Real-World Protection with publicly approved Encryption Methods

It cannot be ruled out that officially recommended cryptographic algorithms that have been elevated to standards have inherent mathematical weaknesses in order to make decryption easier for intelligence services. Presumably, truly advanced computer technology is withheld from the public or kept generally off-limits in order to guarantee intelligence services a computational advantage. From this point of view, and in view of the influence that most probably exists on the design of company products (software and hardware backdoor problems), the effectiveness of existing encryption practice is questionable, even if open, free IT infrastructure is used throughout.

Consistently applied signing and encryption, however, ward off at least some of the potential business attackers and

[15] "Netzwoche Bielefeld - Udo Vetter - Das überwachte Netz", entry point in the 18th minute, direct link.

prevent direct access to data in the event of theft or loss of data carriers.

Reducing complexity at program and operating system level is another key factor. In addition, old and very old computers on which outdated proprietary operating systems and programs are still installed can be modernized and security-optimized with continuously updated, specialized, lightweight free operating system distributions.[16]

2 Free Checksum Programs

CyoHash and Jacksum stand out from the large number of free graphical checksum programs. Jacksum, published under an OSI-certified free software license, the GPL, listed in the FSF directory and based on Java, runs on many operating system platforms (software features). It is therefore also suitable for heterogeneous infrastructures of company networks. Numerous internationally common checksum procedures are considered, the file manager integration ensures convenient operation.

Jacksum file manager versions are available for GNOME, KDE, ROX and Thunar (Unix/BSD, GNU/Linux) as well as for the Windows Explorer of MS-Windows and the Finder of Apple Macintosh. The program author Johann Löfflmann maintains a website with detailed information, Jacksum.net. Suggestions for program enhancements can be submitted and the exchange of information between users is also encouraged.

CyoHash, an extension for the MS Windows file manager Explorer, offers only a fraction of the algorithms, but also supports the modern SHA2 algorithms and functions without Java.

Some common ones among the many cross-platform text mode programs for BSD/Unix and GNU/Linux are for example sha224sum, sha256sum, sha384sum, sha512sum, shasum, sha3sum. sha1sum is no longer recommended, the WP article ""sha1sum"" lists alternatives.

A comparative overview of numerous free and proprietary checksum programs can be found in the WP article "Comparison of file verification software" (as of 2020, archived version). Basic terms and key references to free software are discussed in the article "Introduction to Free Software and Operating Systems".

2.1 Cyohash

Cyohash is a free file manager extension for MS Windows Explorer, downloadable from the official project site or from a reputable software directory.

2.1.1 Checksum Creation

Point with the mouse arrow to the corresponding file and click on the right mouse button. In the menu that appears, click on "Cyohash" and select a checksum algorithm, e. g. SHA-256.

A window appears showing the file name together with the directory path and the checksum method and the cryptographic checksum, or a table appears in which this data is listed. A separate entry appears for each checksum created.

You can now compare the calculated checksum with a target value. To do this,

[16] "Introduction to Free Software and Operating Systems", article section "Modern Operating Systems for old Computers".

double-click on the respective table entry to open the corresponding window.

An application example: Program files offered on the world wide web are almost always published together with their checksums. After downloading such an executable file, preferably from the official program project page, copy the corresponding cryptographic checksum published there, then paste it into the input line ("Validate:") that appears at the bottom of the program window and press "OK". If the values match, the input line turns green, otherwise it turns red.

2.1.2 Creating Checksums for multiple Files

Either point to a table entry or to an empty table row and click the right mouse button to display further functions.

You can create checksums for several files at the same time. Select the function "Hash File(s)...". A window opens in which you can select the desired checksum method. Then press "Browse..." and a Windows directory window opens. Select the files in the corresponding directory, hold down the CTRL key and press the mouse button to highlight the individual files. Finally click on "Open". The Windows directory window then disappears, the CyoHash window appears in the foreground, in which you confirm your file selection with "OK". All checksums are then displayed in the table window.

2.2 Jacksum

2.2.1 Installation of Java and Jacksum

Installation of Java

Java is usually already included in Unix and Unix-like operating system distributions, in the \free variant OpenJDK. As an MS Windows user, you call up a search engine site, for example Google, and type in "Java" or "JRE", which is short for "Java Runtime Environment". This step is not necessary if a Java Runtime Environment already exists.

Example of a Java installation under MS Windows:

1. Call up a search engine, for example google.com, and enter "Java"
2. The entries of the official Java manufacturer Oracle (Java.com) for various operating system platforms appear first. Go to one of these websites and follow the instructions there or alternatively:
3. Type in the search term "Java Runtime Environment" to get to the official download page

If the Java manufacturer offers a preselection for the (co-)installation of a Yahoo toolbar, uncheck the box by clicking on it so that the checkbox remains empty. Google search for this topic: Java installation Yahoo toolbar. Such toolbars can be removed at any time. Google article search: uninstall toolbars deinstallieren

Installation and Use of Jacksum under MS-Windows

Detailed instructions can be found in the installation section of the official program website and in the readme.txt file included with the Jacksum download.

Select the "Download" section on the official website, jacksum.net. There,

in the section “File browser integration (optional)”, download the “[...]-windows-explorer-integration-[...]” file (file name varies with the software version number, a ZIP file. Open this directly by double-clicking or right-clicking and open the decompressed folder, read the file readme.txt or start the installation by double-clicking on the executable file “Jacksum Windows Explorer Integration.exe”. A window will appear asking you to extract all files

Now change to the fully extracted folder, where you will see the exe installation file, symbolized by a green circle.

Double-click to start the program installation. From then on you can right-click → “Send to” → [Procedure, e.g.: “Jacksum - 3) All algorithms”] to form cryptographic checksums. The checksum(s) appear in a separate text window

There are numerous possible applications for Jacksum. The command line version unfolds the full potential of this excellent software, including interaction with other programs. The provision of an open application programming interface (API) promotes broad acceptance.

2.2.2 Application under KDE Dolphin

Open the file manager. To select the file, click the right mouse button → “Actions” → “Jacksum” → [select desired function].

2.2.3 GNOME Nautilus

Open the file manager. To select the file, right-click → “Scripts” → “Jacksum” → [select desired function].

2.3 Console-based Checksum Generation

Cryptographic checksums can be created in text mode (console application) under any operating system; practically all manufacturers of proprietary (proprietary software) and free operating systems offer corresponding programs as standard.

Since the introduction of Microsoft's Windows PowerShell, MS Windows users can, in addition to the classic MS DOS commands (cmd.exe), by default also use basic file operation commands from the BSD/Unix world (comparison). Moreover, the GNU Core Utilities make it possible to use other standard Unix programs under MS Windows (List of Unix commands).

2.3.1 On-Board Algorithms under MS-Windows, Unix/BSD and GNU/Linux Systems

SHA algorithms are pre-installed by default on numerous Unix and Unix-like operating systems as well as on MS Windows systems.

Forming cryptographic checksums under MS-Windows: The PowerShell supports numerous basic commands of the Unix shell; for an overview, skim the correspondingcomparison section in the WP article on the PowerShell.

In addition, current SHA algorithms are also supported via the “Get-FileHash” command. Official information can be found in the Microsoft article of the same name; the default setting is SHA-256.

1. *Starting the program:* Go to the search field in the Windows taskbar and enter: PowerShell. The com-

mand line environment opens. To adjust the font size, right-click on the upper window frame and select the “Properties” menu item. In the “Font” tab, under “Size”, you now set the font size, then press “OK”.

2. *Changing to the corresponding directory*: Now change to the file directory containing the file for which the checksum is to be formed. In the example prompt used (figure 3), `"PS C:\Users\nutzer-01>`”, “Users” stands for the Windows Users folder, “nutzer-01” in this example is the name of the user account of the logged-in user. Enter “ls” (list) to display a folder overview: “`PS C:\Users\nutzer-01> ls`” This is followed by a directory listing, which also contains the central folders “Desktop”, “Documents” and “Downloads”; you can move the contents up and down using the mouse wheel or slider. In this example, we will now switch to the desktop folder, whose files are also displayed on the desktop screen by default; we will use the cd (change directory) command to do this: `"PS C:\Users\nutzer-01> cd Desktop"`. You are now in the desktop folder: “PS C:\Users\\ \user-01\Desktop>”; by entering ls again, you can display its contents.

3. Determining the checksum of a file. In this example, the image file foto-01.jpeg, for which a checksum is to be created, is located on the desktop. Like the Unix shell, the PowerShell also has an autocomplete function (WP article Command line completion).

It is sufficient to write “`get-f`” in lower case in the command line, “`PS C:\Users\nutzer-01\Desktop> get-f`” and then press the Tab key for auto-completion, whereupon the command appears in full length and in correct upper and lower case: “`PS C:\Users\nutzer-01\Desktop> Get-FileHash`”. Then add the file name, the autocomplete function can also be used for this: “`PS C:\Users\nutzer-01\Desktop> Get-FileHash foto-01.jpeg`” and obtain the SHA-256 checksum (figure 3).

```
PS C:\Users\nutzer-01\Desktop> Get-FileHash foto-01.jpeg

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          382F8051EC6E42F019771BB36118E064DB49B9AA2963C0F37E6FF61C4BB93C5C       C:\Users\nutzer-01\De...


PS C:\Users\nutzer-01\Desktop>
```

Figure 3: Checksum creation with the PowerShell

Under Unix-like systems: Open a command-line environment (shell), type “sha”, and then press the tab key for the command-line completion to see all existing SHA procedures:

```
> sha
> sha1sum sha224sum sha256sum
```

```
 sha384sum sha512sum shasum
> sha
```

Change to the corresponding directory, select a procedure, add the name of the desired file and press Enter. In the following example, the SHA256 checksum of the file test.html is generated:

```
> sha256sum test.html
> e3b0c44298fc1c149afbf4c8
996fb92427ae41e4649b934ca4
95991b7852b855 test.html
```

The SHA256 checksum value and the name of the associated file are displayed. Implementation and command names may vary. Practically all Unix or Unix-like systems and distributions have corresponding pre-installations. There are dozens of free programs for creating cryptographic checksums, both graphical and text-based, e.g. at sourceforge.net (WP article).

2.3.2 Text Mode Programs for professional Computer Use

The use of thecommand line environment enables highly effective work on the computer. Some applications are written exclusively for the text mode that is mostly emulated today, while others offer a text-based program interface in addition to the graphical one. Text-based programs enable the most effective use of computers in some areas.

In addition to graphical desktop environments and application programs, GNU/Linux distributions also contain text mode software as standard. Programs with character-oriented user interfaces, also known as "text-based user interfaces", are extremely powerful and are among the preferred tools of many users, administrators, IT professionals and scientists. Websites and recommended articles on text mode programs:

WP article: “Console application” • “Text-based (computing)” • “Shell (computing)” • “Command-line interface” • Excellent introduction: Floss manual “Introduction to the Command Line” • WP article: “GNU Screen” • “Computer terminal”• “freie Textmode-Software” • “Webseiten zum Thema Textmode”

.

3 Imprint

Peter Jockisch
Habsburgerstraße 11
79104 Freiburg
Germany

Web: www.peterjockisch.de
E-mail: info@peterjockisch.de
OpenPGP: https://peterjockisch.de/schluessel/key-pub.asc

Document permanent link:
English A4: peterjockisch.de/Checksums_A4.pdf
English A4 two columns: peterjockisch.de/Checksums_A4_2.pdf

English US-Letter: peterjockisch.de/Checksums_US-Letter.pdf
English US-Letter 2 c.: peterjockisch.de/Checksums_US-Letter_2.pdf
German A4: peterjockisch.de/Pruefsummen_A4.pdf
German A4 two columns: peterjockisch.de/Pruefsummen_A4_2.pdf
German US-Letter: peterjockisch.de/Pruefsummen_US-Letter.pdf
German US-Letter 2 c.: peterjockisch.de/Pruefsummen_US-Letter_2.pdf

The PDF file contains all references of the original HTML version, hyperlinks are framed in color, visible in the browser or with a separate PDF viewer; when hovering with the mouse pointer, the address is displayed, by clicking on it the web page opens in the browser. There are no color frames when printing.[17]

Deepl.com (free version) was used extensively to translate the German-language original into English. Introductory article on typesetting, contains comprehensive overviews and a section on translation aspects: "*Free Software for Professional Document Creation: Writing Scientific Literature, Word Processing, Book Creation, Graphical Desktop Publishing, Web PDF Documents, E-Book Typesetting, and the Creation of Websites*",

[17] When reading on a PC, you can switch between application windows using the key combination ALT + TAB, see the Wikipedia article "Alt-Tab".