ANTI-FORENSICS TECHNIQUES RESEARCH

Practical Implementation & Indonesian Legal Analysis

Author: Reihan Daniswara Pramudito

Date: December 2024

KEY FINDINGS

- **Artifact Wiping & Evidence Hiding**:
  - **File Overwriting (Eraser)**: Irrecoverably wiped files with a random overwrite
  - **Hidden Volumes (VeraCrypt)**: Created an encrypted mountable volume
- **Trail Obfuscation & Tool Attacks**:
  - IP Spoofing (Scapy): Sent spoofed packets that bypassed basic firewall/IDS rules
  - Executable Packing (UPX): Packed binaries to evade signature-based scanners
- **Legal Violations**:
  - **ITE Law (Electronic Information and Transaction)**: Prohibits altering or concealing electronic information
  - **KUHP (Criminal Code)**: Punishes hiding or destroying evidence

TOOLS USED

- **Eraser**: 3-pass overwrite on test files
- **VeraCrypt**: Hidden volume creation and detectability checks
- **Scapy (Python)**: Packet-spoofing scripts against test network
- **UPX**: Repacked executables to test scanner evasion

Disclaimer:

This report is for educational purposes only, based on simulated anti-forensic scenarios with test data. Tools, methods, and conclusions do not reflect an actual investigation.

Table Of Contents

1.0 Overview of Anti-Forensics

Digital forensic is a process of gathering and examining digital evidence in a way which maintains the integrity of the evidence. Anti-Forensic techniques on the other hand are ways to make gathering and examining digital evidence difficult or even impossible by altering the quantity and quality of evidence.

When a cybercrime occurs, investigators will analyse digital footprints left behind to determine what happened and who did it. The goal of anti-forensic for threat actors is to remove their digital footprints to avoid detection of their crime and to make sure that their crimes are not linked to them. This could be done by disrupting and increasing the time needed to collect and analyse evidence. In addition, threat actors could try to sabotage the investigation by purposely altering or deleting data to affect the integrity of evidence and cast doubt in the forensic report to make it harder to bring it to court and prosecute them.

The action of anti-forensic could negatively impact the investigation process by giving investigators numerous amounts of obstacle during collection, preservation, and analysis of evidence. Threat actors could delete or manipulate files, log, or metadata which might remove or make key evidence harder to find and harder to trace the action to the threat actor. Data could also be encrypted in such a way that the data becomes harder to interpret. The storage media for data might also be exploited to make evidence within it unrecoverable. Obfuscation could also be used to hide the true meaning of data to make the origin of malicious actions difficult to trace and difficult to identify the threat actors. All this could cast doubt on the integrity of the evidence and might make it inadmissible in court. This could increase the time needed to collect evidence as well as increase the resources needed for the investigation since specialised tools might need to be used to bypass anti-forensic techniques used or to verify the authenticity of evidence.

2.0 Relevant Anti-Forensics Techniques

Common techniques used for anti-forensics could be classify into four main categories, which are artifact wiping, hiding evidence, trail obfuscation, and attack against forensic tools.

2.1 Artifact Wiping

This category involves the complete removal or destruction of data and evidence. The goal of this technique is to make it very difficult for investigators to recover evidence. The simplest way for threat actors to do this is just by erasing file using standard file deletion methods, like moving a file to trash and then deleting it permanently or using a tool like CCleaner. However, using this method the file is not actually deleted from the storage media but is just labelled as “free” and could be overwritten. This means that investigators could still easily recover those files. To avoid this, threat actors might considers using tools, like BCWipe or Eraser, to repeatedly overwrite a file with random data to make recovery of data difficult. Another method is full disk formatting, which is to do a complete wipe of all data stored in a storage media, using tools like DBAN, or commands on the command prompt. The difficulty of recovering from a complete wipe would depend on how thorough the wipe was. To guarantee that the data would be unrecoverable is by physically destroying the storage media making the data inaccessible. This could be done by shredding the storage media into small pieces to make it practically impossible to reconstruct, or by degaussing the storage media, which is by applying a strong magnetic field to make the data irrecoverable.

However, by removing data and evidence intentionally might also be evidence itself, since it would raise suspicion. Investigators could detect that data were erased or tampered with, which means that there is an attempt to hide something, and this could be a clue and lead to a further investigation. An analogy of this is like when someone committed a crime on snow and leaves footprints behind. Then they try to cover the footprints by stomping on the snow. When an investigator finds the crime scene, the absence of footprints suggest that someone is intentionally trying to hide their trail. The absence of footprints is still evidence just like if the footprints are there. Similarly, intentionally removing data and evidence could itself be evidence.

2.2 Hiding Evidence

This category consists of several subcategories and involves hiding or concealing data and evidence to make it difficult to be found and access. The goal is to make it difficult for investigators and other people from accessing data and potentially find evidence but still giving the person hiding the data the ability to access it.

The simplest way is to hide data and files is by creating a hidden file. In Linux and Mac this could be done by simply adding a "**.**" to the front of the file name and the file would not appear on the directory even though it's there. The file is still there and accessible if the name of the file is known, it is just not visible. However, investigators could easily find the hidden file by running a command like "**ls -a**" which is to list all files including hidden files. This means that investigators could still easily access those files.

To avoid this, a method called steganography could be used, which is to hide data inside another file, which could be in the form of video, audio, images, or text for both the data and the file. There is also steganographic file system, invented by Anderson, Needham, and Shamir, where data or files would be hidden using a series of techniques, including hidden inside and combined with cover files using bitwise XOR making it indistinguishable to not raise suspicions, and writing the file in multiple semi-random locations on the disk to make it difficult for others to detect the presence of hidden files. These and other techniques deployed makes hidden data and files undetectable and inaccessible without the right password. For image and audio steganography, a tool called Steghide could be used which also provide encryption and password protection. For text steganography, there are a lot of tools even online like Steganography Online by stylesuxx and many other tools. For steganographic file systems, there are StegFS and Magikfs. However, the investigator could use steganalysis tools to find hidden data, but it would depend on the complexity of the steganography technique used.

Another method is encryption which is changing data to make it unreadable and could only be made readable by using a key. In hiding evidence there are two main types of encryptions which are disk encryption and data encryption. Disk encryption is encrypting the entire storage media making the data in it hard to access, using tools like VeraCrypt and BitLocker. However, disk encryption might slow down the machine depending on the encryption method used. Data encryption is encrypting only individual data within file, folders, or other locations where data might be stored, using a tool like VeraCrypt.

There are also other methods of data hiding like network-based hiding, which uses VPN and proxy servers, memory hiding, which uses shared memory space, hard disk manipulation, which is hiding data in hidden partitions or bad sector, and several other methods.

However, digital forensics investigators are usually trained on how to discover hidden data using specialised methods and tools. In the case of disk encryption for example, investigators usually have knowledge about it and would try and time their seizure to when the machine would be on and running, when the machine is running, and the disk is in used the disk is unencrypted.

2.3 Trail Obfuscation

This category involves efforts to intentionally deceive and make confuse the investigators. The goal is to hide the threat actor's trails and make it difficult for investigators to trace their actions.

The simplest way to is by removing or modifying log files, remove manually using Windows Event Viewer or using tools like Timestomp to modify the log. However, there might still be data remaining in the system, like hidden backup of log files, that could be recovered by investigators which makes the effort ineffective.

To make it harder to detect, threat actor might use spoofing, a technique which modifies information to mislead, usually IP or Mac addresses. IP spoofing is modifying the source IP address of a packet so that it appears to be coming from a different machine in a different location, using packet manipulation tools like Scapy. MAC Address Spoofing modifies the MAC (Media Access Control) address of a device to hide the device's true identity in the network, using tools like macchanger.

Another method is backbone hopping which is to "hop" through a series of networks to hide the original internet traffic to hide the true identity and location of the user. To do this a tool called TOR (The Onion Router) could be used which relays the network request through TOR's network of relay systems and then making the last relay node the origin of the request, hiding the entire path travelled by the request, before reaching the destination, which makes it nearly impossible to trace the original source of the traffic.

Beside TOR, IP chaining could be used which combines multiple proxy servers, using tools like Squid and Privoxy, or VPN services, using tools like NordVPN and ExpressVPN, to make it harder to track the original user. However, backbone hopping slows down the connection speed due to it taking longer to reach the destination.

Another method is using peer-to-peer networks, a decentralise system where a machine can act both as server and client. In trail obfuscation, this could be used to distribute task or data across multiple machines, making it harder to trace actions to a single user. Data or evidence in files could be distributed in a decentralised manner, using tools such as BitTorrent, which obscure the origin of data and the identity of the user, making it difficult to trace the files and their owners. Trails of financial transactions could also be obfuscated by using anonymous cryptocurrencies (privacy coins), like Monero (XMR) and Zcash (ZEC), on a crypto exchange that uses peer-to-peer networks and offers anonymity, like bisq or Uniswap. Anonymous cryptocurrencies are digital coins that uses techniques to protect the identity of users and make transactions harder to trace, unlike normal cryptocurrencies where transactions are transparent and traceable on the blockchain. However, there are a lot of legal and regulatory risks when using peer-to-peer networks since they are usually involved in illegal activities.

However, any small mistake made by threat actors could be enough to lead to their eventual arrest. For example, threat actors might forget to hide their identity on a single occasion or leave behind traces when they did the obfuscation technique that, when analysed over time, create a pattern of behaviour that investigators can detect.

2.4 Attack Against Forensic Tools

This category focuses on attacking or sabotaging software and tools used by investigator. The goal is to make it difficult for investigator to use tools to collect and analyse evidence of a crime. This simplest way is to use disruption tools like the “42.zip” zip file or the “USB Kill” software or USB. The “42.zip” is a zip bomb, which is a compressed zip that contains a very large file size, in the case of 42.zip, the zip file is only 42 kilobytes but when the zip di opened and decompress it expands to become 4.5 petabytes. This would crash the system, might cause memory and CPU overload, and might cause data loss or corruption. The USB version of “USB Kill”, when plug in, could send a high amount of voltage to a computer, destroying its electrical component. The software version of “USB Kill” is a kill switch, it shuts down the computer immediately when a change happened to the USB port, for example when investigator plugs in a USB to use their forensic tools on the live machine or when the plug a “mouse jiggler” to prevent the machine from going to sleep. This is useful since it would prevent the investigator from acquiring what is currently running on the system and eliminate volatile data that might contain useful information for the investigation. In addition, threat actors might use other anti-forensic techniques like encrypting the disk, which means when the laptop is off investigator cannot access the encrypted data, unlike when the system is on, and data is in use there is no encryption to protect it. However, investigators are aware of the existence of zip bombs and USB Kill and have methodical approach to mitigate these methods.

Another method is program packers, which uses tools like UPX to compress or encrypt executable files, could be used to hide malware from forensic tools. However, forensic tools might include packet detectors which increased risk of detection and then investigator could do dynamic malware analysis, instead of static analysis, on the file which might reveal the malware.

Another method is anti-reverse engineering which involves ways to make it difficult to reverse engineer a code or software to find its behaviour. This could be done by making the code harder to read and understand using obfuscator tools like ProGuard or Dotfuscator, or by inserting dead code, lines of codes that do not do anything and is just there to confuse those analysing the program, into the code of the malware. However, using excessive amount of anti-reverse engineering methods increases the chance of introducing errors or bugs into the code. Another method is attacking the integrity and credibility of the forensic investigator to confuse and delay investigation

in hopes of making result of their investigation invalid or other parties losing trust in the investigator. This could be done by launching a smear campaign against the investigating parties, framing them, or other activities to attack the integrity and reputation of the party doing the investigation, but there is a risk that this brings more attention to the investigation and the case.

However, attacking the forensic process could backfire for threat actors because these actions bring more attention to the case which might cause more resources to be allocated and more advance method to be use in the investigation. An analogy of this is like when criminals sabotage police equipment to slow the investigation down but it might raise suspicion and lead to investigator to use more advance tools and examine evidence more carefully and closely, which might lead to the arrest of the criminal.

2.5 Evaluation of All Techniques and Chosen Methods

From each of the four main techniques (Artifact Wiping, Hiding Evidence, Trail Obfuscation, and Attack Against Forensic Tools), one method would be chosen to be used in the demonstration for the later section.

2.5.1 Evaluation on Artifact Wiping

The method chosen is file overwriting, which is deleting files by overwriting it with random data several times to make the original files irrecoverable. The tool chosen is Eraser, a free and widely accessible file overwriting tool which could do multiple files. This method is easy to use but still effective at deleting files while making it hard to recover. Using the standard deletion method is simple and easy to use but it only marks the files deleted as available space which means that it is still in the storage media and could be recovered easily. Full disk formatting could be a simple way to permanently delete files but file writing, using tools like Eraser, allows the deletion of specific files and not all the files in the storage media. Physical destruction of the storage media would lead to permanent deletion of files that could not be recovered but it removes all files and destroys the physical storage media.

2.5.2 Evaluation on Hiding Evidence

The method chosen is encryption, which is protecting data from unauthorise access by using encryption algorithms to make the data inaccessible unless the key to decrypt it is known. The tool chosen is VeraCrypt, a free and widely used encryption tool with variety of encryption algorithms available and the feature to create a hidden volume inside another encrypted volume to further hide data. Using hidden files is simple and an easy way to hide files but it could be discovered quickly by investigators using simple commands/tools, and could easily be accessed once found, unlike encryption which makes it difficult to access without the right password or decryption key even when investigator have physical access to the storage media and knows about the existence of the encrypted file. Steganography could be used to hide data or files inside other data or files but when hiding a large amount of data, it might become obvious that data is hidden inside another data from its size and then could be recovered by investigators. Encryption on the other hand would offer a more secure form of protection from unauthorised access.

2.5.3 Evaluation on Trail Obfuscation

The method chosen is spoofing, specifically IP spoofing, which is modifying or manipulating network packet, in IP spoofing it modifies the source IP address, to make it seems to be coming from a different machine or network to hide the identity and location of the user, making it difficult to track them. The tool chosen is Scapy, a versatile and free python-based network tool to create and manipulate network packets. Removing log files would help obfuscate evidence but they might still be recoverable from hidden backups or other means. Methods involving the use of TOR or VPN would help mask the location of the user and the original IP address. However, this would slow down the network speed and it might still leave traffic patterns. Spoofing, on the other hand, gives a higher flexibility in manipulating each and every packet.

2.5.4 Evaluation on Attack Against Forensic Tools

The method chosen is program packers which obfuscate and compress executable files to hide its true nature, which makes it harder to statically analyse and harder to identify malicious activity using malware signatures. The tool chosen is UPX (Ultimate Packer for eXecutables), a widely used program packing tool for compressing and obfuscating executable files to make it difficult to do malware analysis using automated forensic tools that rely on signature-based detection. Attacks using disruption tools like zip bombing and “USB Kill” would attack on the integrity and availability of evidence but investigators are most likely already be aware of this form of attack and could identify and isolate it to not interfere with the investigation. Using anti-reversing methods like adding dead code or using obfuscator would make it harder to analyse the malware but it might lead to random errors or bugs, increases the size of the file which reduces its efficiency, and make the code stands out for investigators to analyse. Program packers, on the other hand, add a layer of complexity to the program while also reducing its size and not changing the program’s behaviour.

3.0 Legal and Ethical Considerations

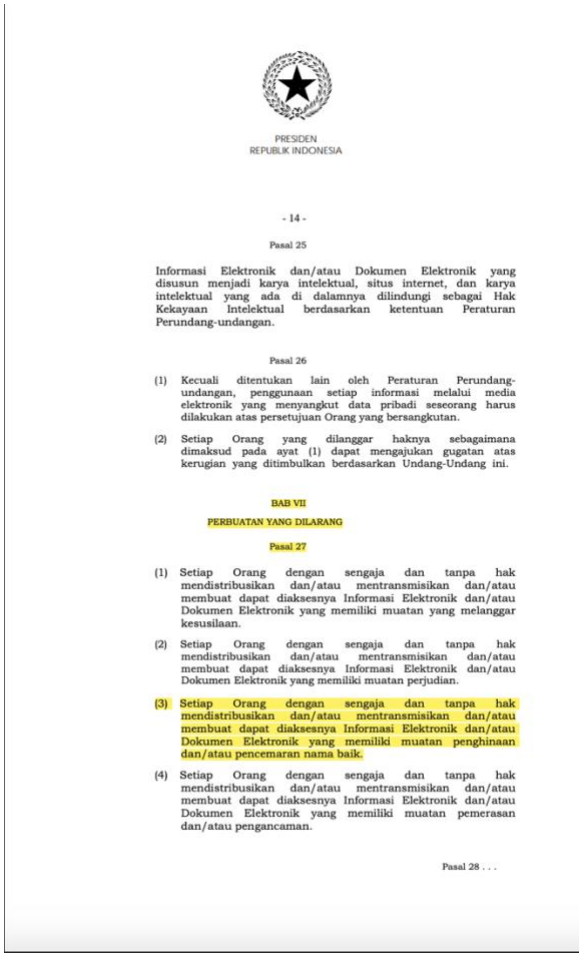
Anti-forensics techniques could be used maliciously by making it more difficult for investigators to gather evidence, but it could also be used for legitimate intent like for protecting sensitive personal data or protecting the privacy of the user. This creates a line between unlawful malicious used for obstruction of justice and legitimate protection of the privacy of individuals, which makes it complex to consider in both legal and ethical perspective. Individuals have the right to protect their privacy and personal data, but the same techniques could be used to hide criminal activity and interfere with investigations. This makes individuals needing to consider the legal and ethical aspect of using anti-forensics techniques. The intent behind the use, the context at which it is implemented, and the potential consequences of its use must be considered when evaluating the use of anti-forensics techniques.

3.1 Legal Considerations When Doing Anti-Forensics Techniques

The use of anti-forensics techniques might raise some legal questions and could be an issue for the individuals using it. Currently there are no laws anywhere explicitly stating that anti-forensics techniques and tools could not be used but there are laws regarding the malicious outcomes of using these tools like destroying or hiding evidence. The laws of Indonesia that would affect the use of anti-forensics techniques would be analyse to see how Indonesia prevent the malicious use of anti-forensics to obstruct justice.

3.1.1 Indonesian Laws on Anti-Forensics

Indonesia's "*Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*" (*UU No.11 thn 2008 tentang ITE*), which roughly translates to "Law No. 11/2008 on Information and Electronic Transactions", aims to regulate the use of information technology and electronic transactions. Focusing on chapter 8 which is about prohibited actions.



PRESIDEN
REPUBLIK INDONESIA

- 14 -

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 26

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

BAB VII

PERBUATAN YANG DILARANG

Pasal 27

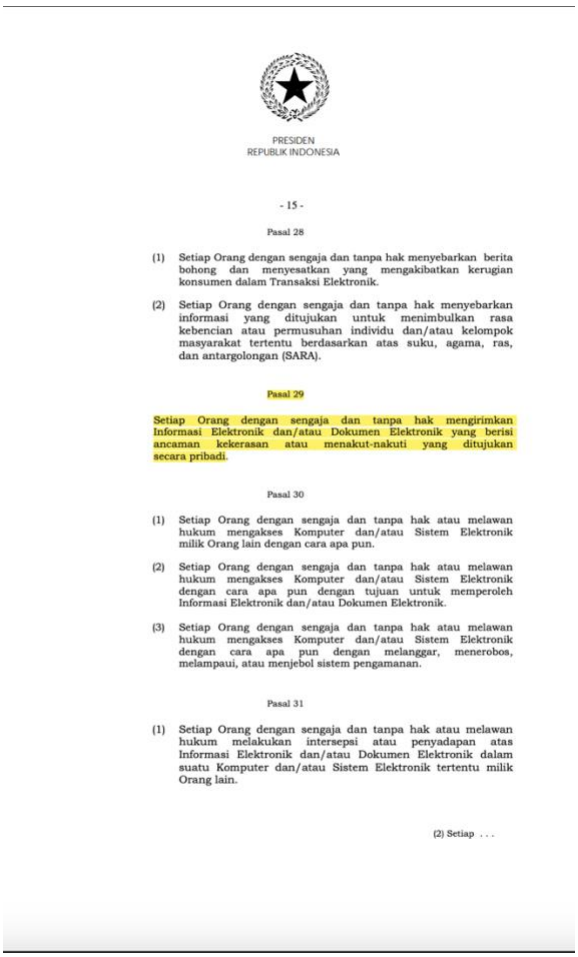
(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28 . . .



PRESIDEN
REPUBLIK INDONESIA

- 15 -

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

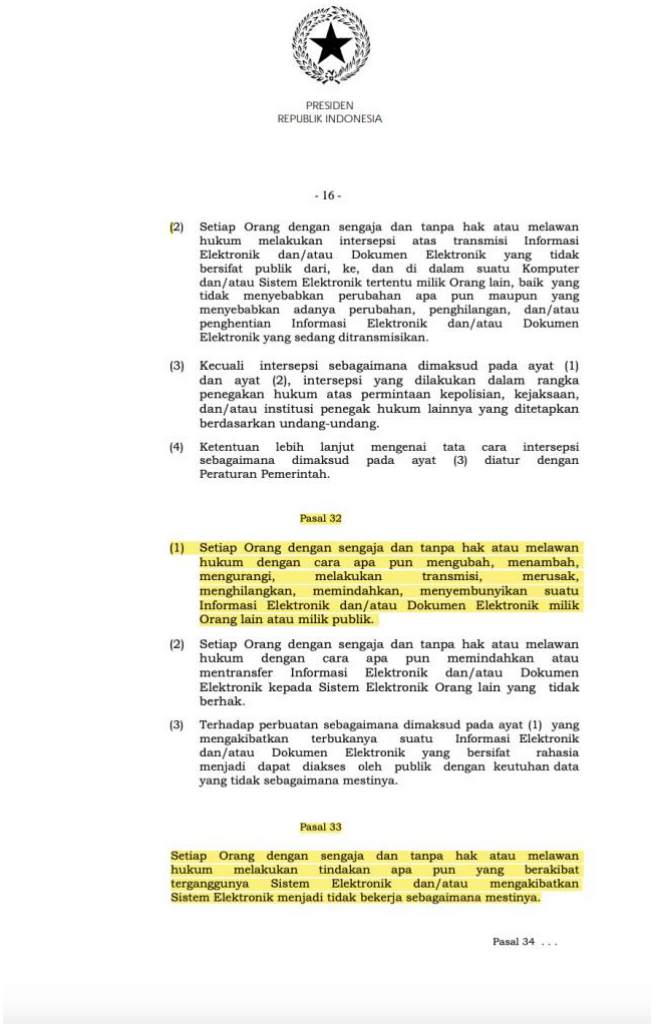
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(2) Setiap . . .

Article 27 verse 3, prohibits the distribution, transmission, and/or making accessible electronic information and/or documents which contains insult or defamation, and article 29 which prohibits intentionally sending electronic information and/or documents that contains threats of violence or intimidation against individuals. This prohibits a part of the technique “Attack on Forensic Tools”, specifically attacking the integrity of the integrity and credibility of investigator, for example through smear campaigns.



PRESIDEN
REPUBLIK INDONESIA

- 16 -

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

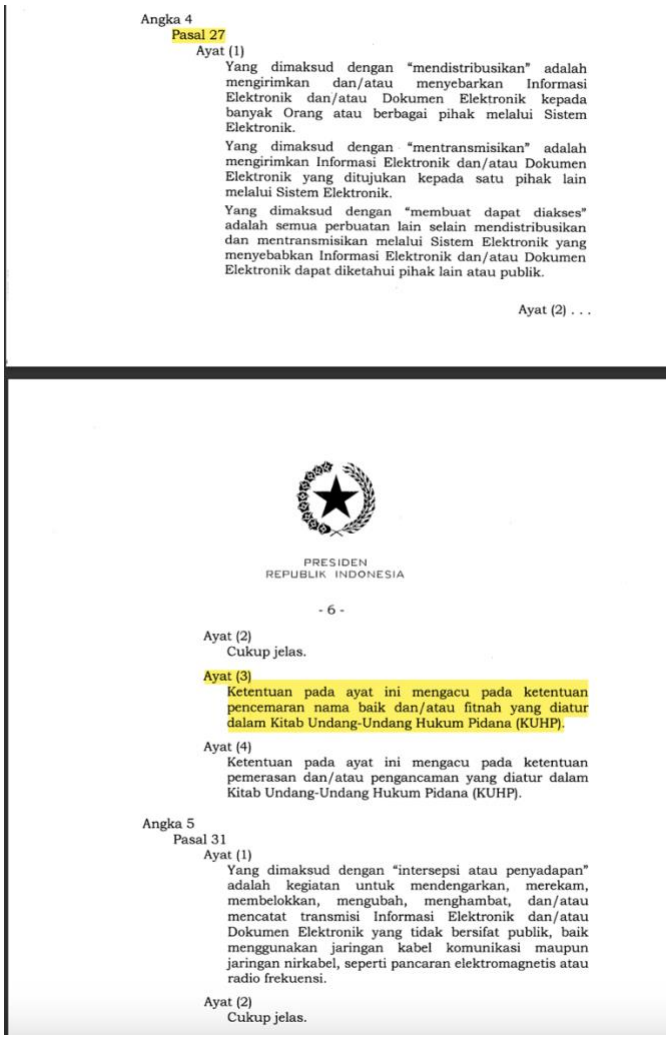
Pasal 34 . . .

Article 32 verse 1 prohibits intentionally altering, adding, reducing, transmitting, damaging, deleting, transferring, concealing electronic information and/or documents own by other people, in this case computers or machines that is now own by investigators. This prohibits the use of almost all the anti-forensics techniques and their methods for malicious use. All methods under artifact wiping are illegal under this since basic file deletion, secure deletion through file overwriting, formatting, and physical destruction of storage media would all either damage or delete electronic information, which could be evidence, from machines that are now own by investigators. Every method under hiding evidence would also be made illegal since creating hidden file, steganography, encryption, and other methods to hide evidence would conceal electronic information. All trail obfuscation methods are also illegal since manipulating log file would be altering electronic information, spoofing would be concealing and altering information,

backbone hopping would be concealing the information of the identity, and using peer-to-peer network would be transmitting and transferring electronic information. For attack against forensic tools might fall under this depending on what it is used for. Program packers and anti-reverse engineering could fall under this if they are used to conceal malicious software which does what is prohibited by the article above.

Article 33 prohibits intentionally causing disruption to electronic systems and/or causing them to not function as intended. In artifact wiping only physical destruction of storage media falls under this since it makes the storage media could not function as intended. In attack on forensic tools, disruption tools like zip bombs and USB Kill are prohibited. A zip bomb might cause a system to crash and becomes unresponsive and the USB version of USB Kill sends a high voltage to the system which usually cause hardware failure or disruption to the system. Both causes disruption and cause the system to not function as intended

In the amendments of the 2008 ITE Law, "*Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik" (UU ITE)*, which roughly translates to "Law No. 19 of 2016, which amends Law No. 11 of 2008 on Information and Electronic Transactions" aims to ensure the right and freedom of other while using technology.



Angka 4

Pasal 27

Ayat (1)

Yang dimaksud dengan "mendistribusikan" adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik.

Yang dimaksud dengan "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.

Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.

Ayat (2) . . .

PRESIDEN
REPUBLIK INDONESIA

- 6 -

Ayat (2)

Cukup jelas.

Ayat (3)

Ketentuan pada ayat ini mengacu pada ketentuan pencemaran nama baik dan/atau fitnah yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Ayat (4)

Ketentuan pada ayat ini mengacu pada ketentuan pemerasan dan/atau pengancaman yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Angka 5

Pasal 31

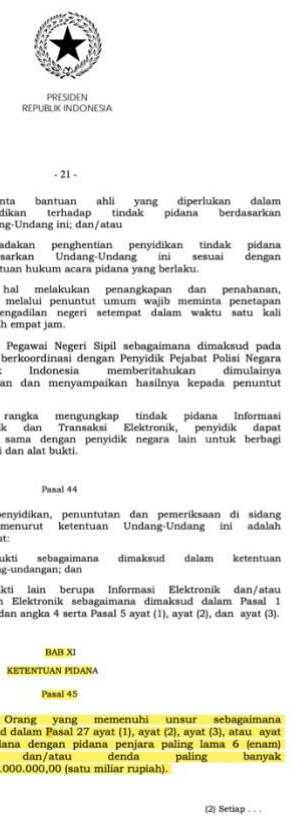
Ayat (1)

Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Ayat (2)

Cukup jelas.

A clarification is made on article 27 verse 3, which was discussed previously, stating that what is meant as defamation and/or slander is as what is stated in Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana*).



PRESIDEN
REPUBLIK INDONESIA

- 21 -

h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau

i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.

(6) Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

(7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.

(8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

Pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

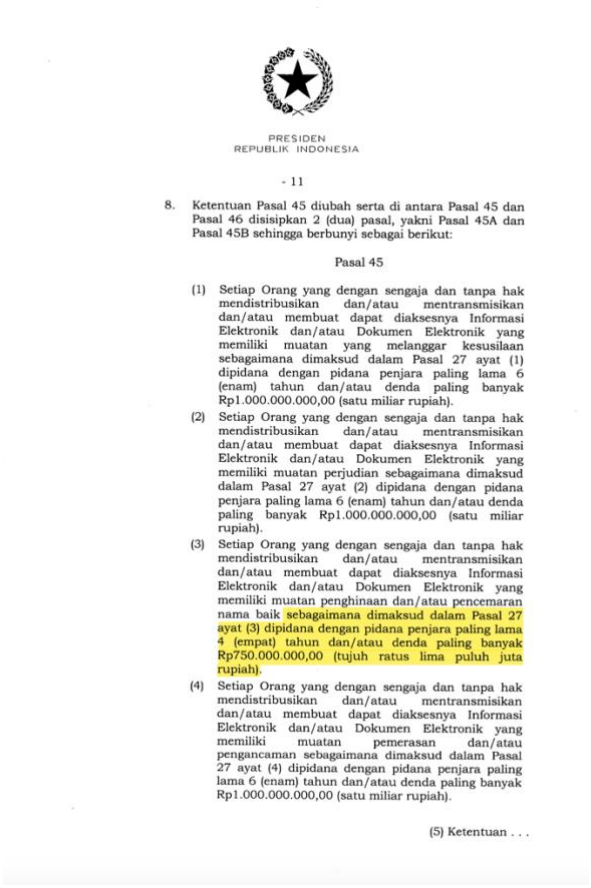
BAB XI

KETENTUAN PIDANA

Pasal 45

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap . . .



PRESIDEN
REPUBLIK INDONESIA

- 11

8. Ketentuan Pasal 45 diubah serta di antara Pasal 45 dan Pasal 46 disisipkan 2 (dua) pasal, yakni Pasal 45A dan Pasal 45B sehingga berbunyi sebagai berikut:

Pasal 45

(1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

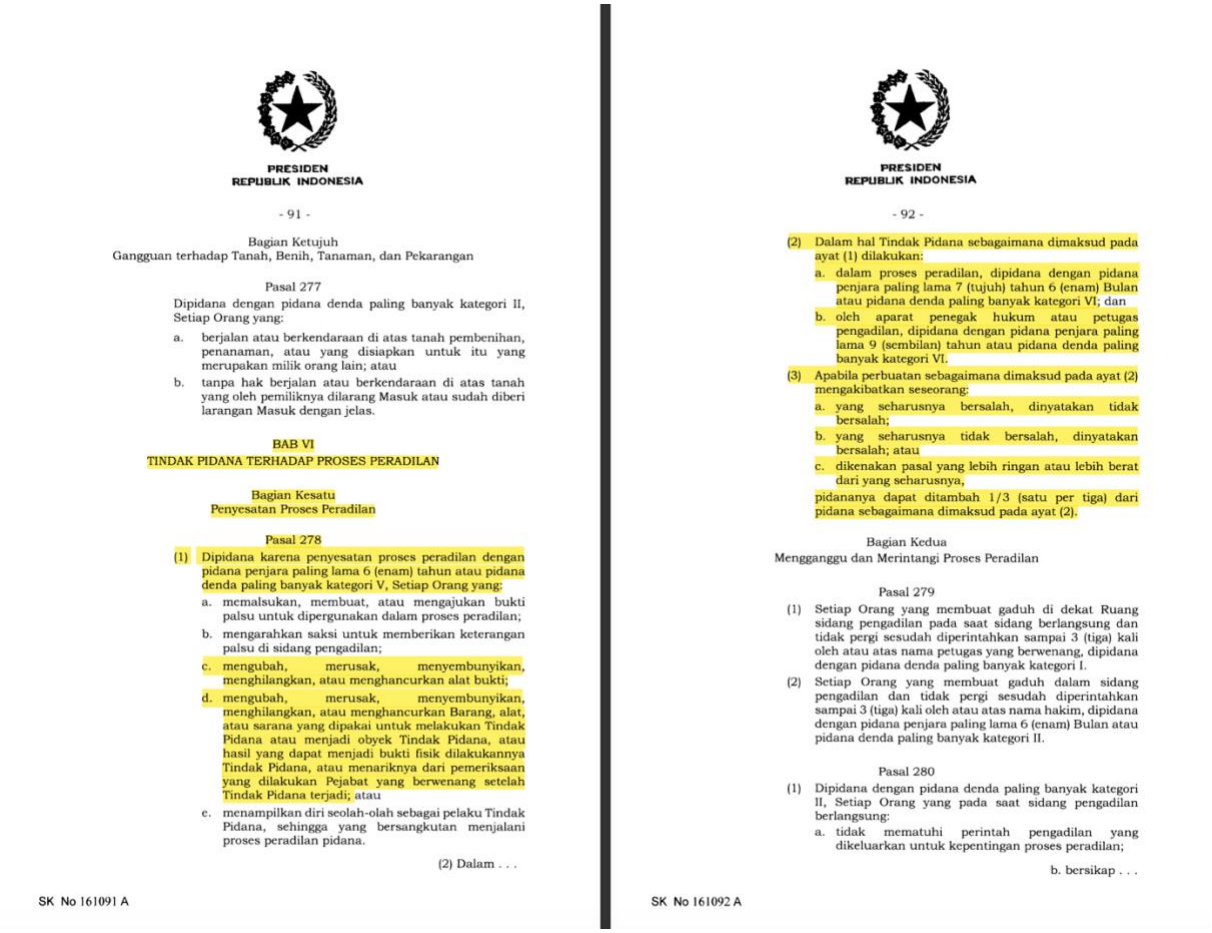
(4) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(5) Ketentuan . . .

2008 ITE Law *2016 Amendment of the 2008 ITE Law*

A change was made to chapter 11, regarding the punishment, article 45. Previously, breaking any verse of article 27 would have the same punishment of up to 6 years in prison and/or a fine of up to Rp1,000,000,000 (one billion rupiah), but now article 27 verse 3, which was discussed previously, have a lighter maximum punishment of up to 4 years in prison and/or a fine of up to Rp750,000,000 (seven hundred and fifty million rupiah).

Indonesia's criminal code, *"Undang-undang (UU) Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana" (KUHP)*, aims to create a legal framework for criminal justice in Indonesia.



PRESIDEN
REPUBLIK INDONESIA

- 91 -

Bagian Ketujuh
Gangguan terhadap Tanah, Benih, Tanaman, dan Pekarangan

Pasal 277

Dipidana dengan pidana denda paling banyak kategori II, Setiap Orang yang:

a. berjalan atau berkendaraan di atas tanah pembenihan, penanaman, atau yang disiapkan untuk itu yang merupakan milik orang lain; atau
b. tanpa hak berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dilarang Masuk atau sudah diberi larangan Masuk dengan jelas.

BAB VI
TINDAK PIDANA TERHADAP PROSES PERADILAN

Bagian Kesatu
Penyesatan Proses Peradilan

Pasal 278

(1) Dipidana karena penyesatan proses peradilan dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V, Setiap Orang yang:
a. memalsukan, membuat, atau mengajukan bukti palsu untuk dipergunakan dalam proses peradilan;
b. mengarahkan saksi untuk memberikan keterangan palsu di sidang pengadilan;
c. mengubah, merusak, menyembunyikan, menghilangkan, atau menghancurkan alat bukti;
d. mengubah, merusak, menyembunyikan, menghilangkan, atau menghancurkan Barang, alat, atau sarana yang dipakai untuk melakukan Tindak Pidana atau menjadi obyek Tindak Pidana, atau hasil yang dapat menjadi bukti fisik dilakukannya Tindak Pidana, atau menariknya dari pemeriksaan yang dilakukan Pejabat yang berwenang setelah Tindak Pidana terjadi; atau
e. menampilkan diri seolah-olah sebagai pelaku Tindak Pidana, sehingga yang bersangkutan menjalani proses peradilan pidana.

(2) Dalam . . .

SK No 161091 A

PRESIDEN
REPUBLIK INDONESIA

- 92 -

(2) Dalam hal Tindak Pidana sebagaimana dimaksud pada ayat (1) dilakukan:
a. dalam proses peradilan, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun 6 (enam) Bulan atau pidana denda paling banyak kategori VI; dan
b. oleh aparat penegak hukum atau petugas pengadilan, dipidana dengan pidana penjara paling lama 9 (sembilan) tahun atau pidana denda paling banyak kategori VI.

(3) Apabila perbuatan sebagaimana dimaksud pada ayat (2) mengakibatkan seseorang:
a. yang seharusnya bersalah, dinyatakan tidak bersalah;
b. yang seharusnya tidak bersalah, dinyatakan bersalah; atau
c. dikenakan pasal yang lebih ringan atau lebih berat dari yang seharusnya,
pidananya dapat ditambah 1/3 (satu per tiga) dari pidana sebagaimana dimaksud pada ayat (2).

Bagian Kedua
Mengganggu dan Merintangi Proses Peradilan

Pasal 279

(1) Setiap Orang yang membuat gaduh di dekat Ruang sidang pengadilan pada saat sidang berlangsung dan tidak pergi sesudah diperintahkan sampai 3 (tiga) kali oleh atau atas nama petugas yang berwenang, dipidana dengan pidana denda paling banyak kategori I.
(2) Setiap Orang yang membuat gaduh dalam sidang pengadilan dan tidak pergi sesudah diperintahkan sampai 3 (tiga) kali oleh atau atas nama hakim, dipidana dengan pidana penjara paling lama 6 (enam) Bulan atau pidana denda paling banyak kategori II.

Pasal 280

(1) Dipidana dengan pidana denda paling banyak kategori II, Setiap Orang yang pada saat sidang pengadilan berlangsung:
a. tidak mematuhi perintah pengadilan yang dikeluarkan untuk kepentingan proses peradilan;

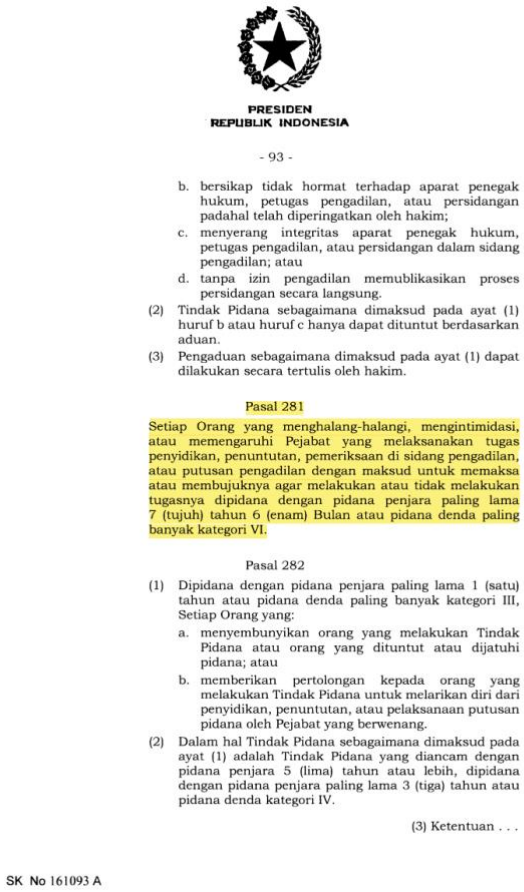
b. bersikap . . .

SK No 161092 A

Chapter 6 of the Indonesia's criminal code (KUHP) talks about criminal acts during the judicial process. Part 1 of this chapter talks about misleading the judiciary process which consists of article 278, and anyone breaking this article would be punished with maximum sentence of 6 years or a fine up to category V, which is Rp500,000,000 (five hundred million rupiah) based on article 79 verse 1 section e. Verse 1 section c of article 278 states that this punishment includes those who alter, damage, hides, remove or destroy evidence. This includes the whole of artifact wiping since the goal is to destroy or remove data or files from a machine which might be evidence of a crime. Any methods under hiding evidence would be punishable by this as well since steganography is hiding information, which might be evidence of a crime, in other files using tools, encryption makes files, which might be evidence, inaccessible to investigators which essentially hides

evidence, and using hidden files also could be used to hide evidence. Some trail obfuscation techniques like manipulating log files and spoofing would fall under this. Manipulation of log files would alter evidence since it would appear different to what it was originally and spoofing alters data like packets, IP addresses, and MAC addresses to hide the identity of the threat actor which might be evidence. Section d of the same article and verse states that the punishment would also punish those who alter, damage, hides, remove, or destroy items, tools, or medium used for a criminal act or is an object of a criminal act, or physical evidence that's a result of a criminal act, or taking it from an investigation that is in progress. Hard disk manipulation using hidden partition or bad sectors, which is under hiding evidence, would fall under this section since it would be altering and hiding items, medium, or tools that is used during a criminal act. Using disruption tools, under attack on forensic tools, like zip bombs and USB Kill would fall under this section as well since the goal is to damage or destroy items or tools used in a criminal act like a laptop for example.

Verse 2 of the same article, article 278, states that if the offence occur during the judicial process the punishment is more severe with maximum sentence of 7 years and 6 months in prison, not 6 years, or a fine of category VI which is Rp2,000,000,000 (two billion rupiah) based on article 79 verse 1 section f, not category V which is Rp500,000,000 (five hundred million rupiah). If the offender is a law enforcement official or court staff the punishment would be a maximum sentence of 9 years or a fine of category VI which is Rp2,000,000,000 (two billion rupiah) based on article 79 verse 1 section f. Verse 3 states that if the action result in the miscarriage of justice, such as declaring the guilty person innocent or vice versa or resulting in a lighter or heavier sentence, the penalty given could be increased by one-third.



PRESIDEN
REPUBLIK INDONESIA

- 93 -

b. bersikap tidak hormat terhadap aparat penegak hukum, petugas pengadilan, atau persidangan padahal telah diperingatkan oleh hakim;
c. menyerang integritas aparat penegak hukum, petugas pengadilan, atau persidangan dalam sidang pengadilan; atau
d. tanpa izin pengadilan memublikasikan proses persidangan secara langsung.

(2) Tindak Pidana sebagaimana dimaksud pada ayat (1) huruf b atau huruf c hanya dapat dituntut berdasarkan aduan.

(3) Pengaduan sebagaimana dimaksud pada ayat (1) dapat dilakukan secara tertulis oleh hakim.

Pasal 281

Setiap Orang yang menghalang-halangi, mengintimidasi, atau memengaruhi Pejabat yang melaksanakan tugas penyidikan, penuntutan, pemeriksaan di sidang pengadilan, atau putusan pengadilan dengan maksud untuk memaksa atau membujuknya agar melakukan atau tidak melakukan tugasnya dipidana dengan pidana penjara paling lama 7 (tujuh) tahun 6 (enam) Bulan atau pidana denda paling banyak kategori VI.

Pasal 282

(1) Dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak kategori III, Setiap Orang yang:
a. menyembunyikan orang yang melakukan Tindak Pidana atau orang yang dituntut atau dijatuhi pidana; atau
b. memberikan pertolongan kepada orang yang melakukan Tindak Pidana untuk melarikan diri dari penyidikan, penuntutan, atau pelaksanaan putusan pidana oleh Pejabat yang berwenang.

(2) Dalam hal Tindak Pidana sebagaimana dimaksud pada ayat (1) adalah Tindak Pidana yang diancam dengan pidana penjara 5 (lima) tahun atau lebih, dipidana dengan pidana penjara paling lama 3 (tiga) tahun atau pidana denda kategori IV.

(3) Ketentuan . . .

SK No 161093 A

Part 2 of chapter 6 talks about disturbing and obstructing the investigation process. Article 281 of this chapter and part talks about anyone hindering, intimidating, or influencing officials that is performing investigations, prosecutions, or examination with the intent to force or persuade the official to do or not to do his/her duties would be punishable of up to 7 years and six months in prison or a fine of category VI which is Rp2,000,000,000 (two billion rupiah) based on article 79 verse 1 section f. This almost encompass anti-forensic techniques in general since the goal for threat actors of using these techniques are to create obstacles to slow down the investigation process or make it impossible.

From laws analysed, there are no law prohibiting the use of anti-forensics techniques and tools if they are used for legitimate purposes like to protect the individual's privacy or to secure personal data. However, malicious used of these tools like to destroy evidence of a crime or create obstacles in the investigation process are prohibited by law.

3.2 Ethical Considerations When Doing Anti-Forensics Techniques

There are some ethical considerations with the use of anti-forensics techniques since it stands in a line between protecting privacy and keeping the integrity of the justice system. Anti-forensics techniques could be used positively for the protection sensitive and personal data, and ensuring one's privacy, or it could be used negatively for the tampering and destroying evidence of a crime, and to create obstacles to slow down or stop the investigation process.

3.2.1 Positive Aspects

Nowadays almost every company tracks user's activities and wants access to user's personal data, and it is freely sold and available for anyone to get or buy. Malicious actors would also try to gain access to personal data to sell it or other malicious intent. Anti-forensics could be used for privacy protection to help secure personal data from malicious actors, companies, or governments which might misuse those data.

Using anti-forensic tools could also be to assert the ownership over the user's own data and have full control over who has access to those data. This is because recently there has been a rise in security breaches, data leaks, and the misuse of personal data by malicious actors. Users using anti-forensics techniques could prevent these unauthorised access and have full control over their own personal data.

Anti-forensics techniques could also be used as security measures to protect sensitive data. For example, if a device is stolen, the user's data still could not be accessed by the thief if it is encrypted or hidden. Another example is when an individual is selling their storage device like hard disk, using artifact wiping methods like overwriting or disk formatting would prevent the buyer from recovering the individual's data after buying the storage device.

3.2.2 Negative Aspects

Anti-forensics techniques could be used for the obstruction of justice since they could be used to destroy or alter evidence. This could lead to the slowing down of the investigation process or leading to the perpetrator getting away with their crime and might lead to wrongful conviction.

Another concern of anti-forensics techniques is that it could be used dishonestly to misdirect investigators or to remove any link to a threat actor that committed the crime. Altering evidence could lead investigators in the wrong direction and reduce the transparency of evidence which prevents the truth from coming out.

Users of anti-forensic techniques might not have malicious intent when using it, but their actions might have unintended consequences. Non-malicious users might accidentally remove, hide, or modify evidence that might help an investigation process they didn't know about.

4.0 Impact of Anti-Forensics Techniques

Each anti-forensics technique has been evaluated and the chosen method and tool from each technique would be analysed.

4.1 Impact of Eraser (File Overwriting) - Artifact Wiping

An advantage of using file overwriting is that it is a secure way to delete files since it overwrites the file with random data. This makes the deleted files almost impossible to recover even using forensic tools. This means that any data in the file, including sensitive data or important evidence of a crime, could be securely destroyed which reduces the risk of a third party accessing those files and data. Another advantage of using Another advantage is that it could help prevent another individual from accessing the data if the device is sold or stolen. It ensures that unused or unwanted data are unrecoverable. This reduces the chance of identity theft or theft of personal data, or convictions of a crime.

A disadvantage of file overwriting is that traces of data could still be left in unallocated space on the disk or in a backup of the storage. This means that the data, or at least a portion of the data, might still be recoverable using advanced forensic tools. This might lead to investigators being able to gather clues and give them proof of intentional deletion of evidence. Another disadvantage is that, due to human error, the wrong file might be deleted which might contain important data. This might lead to the data being gone forever since it is difficult to recover, especially for the normal user.

4.2 Impact of VeraCrypt (Encryption) - Hiding Evidence

An advantage of VeraCrypt for encrypting files is that it contains a large amount of widely use and current encryption algorithms. This means that files and data encrypted is unreadable to anyone which does not have the decryption key. This means that another user would not be able to access the encrypted data while still giving the user access to it. Another advantage is that the encrypted volume created by VeraCrypt could be easily moved from a device or system to another. This means that data could be transported securely even if it's only on an external storage like a USB. This allows the transfer of data more secure and reduces the risk of data loss during the transporting process.

A disadvantage of encrypting file or disk in general is that if the decryption key or password is loss or forgotten, the encrypted files and data could no longer be accessed. This would lead to the permanent loss of data stored within the encrypted volume or part. This means that important data might be lost forever which might cause issue for the user. Another disadvantage is that encrypting and decrypting process requires the system resources. This means that there could be a decrease in the system performance, depending on the specification of the system. This means that in system with lower specification it might take longer to access the encrypted files and data, reducing the productivity of the user.

4.3 Impact of Scapy (IP Spoofing) - Trail Obfuscation

An advantage of IP spoofing using tools like Scapy is that it could modify the IP address of a packet. This would hide the identity and location of the packet sender by making the traffic to appear to be from a different destination. This leads to an increase in anonymity when using the internet and help users protect their identity and location by avoiding surveillance. Another advantage is that modifying the true source of the packet could help avoid intrusion detection or prevention system. This makes it harder for investigators to track the actual source of the attack and what are part of the attack. This gives threat actors more time to execute their crime which means that there is a higher chance of success for the threat actors.

A disadvantage of IP spoofing is that some modern firewalls, and intrusion detection and prevention system might be able to detect fake or spoofed packets. This means that system could easily identify and block these packets. This would lead to attacks becoming less effective and reduces the chance of success to hide the threat actor identity when committing a crime. Another disadvantage of Scapy is that it is complex and requires a high level of knowledge on using it and on networking. This might make new user struggles and fail to use it effectively which limits its usefulness for non-experts.

4.4 Impact of UPX (Program Packers) - Attack Against Forensic Tools

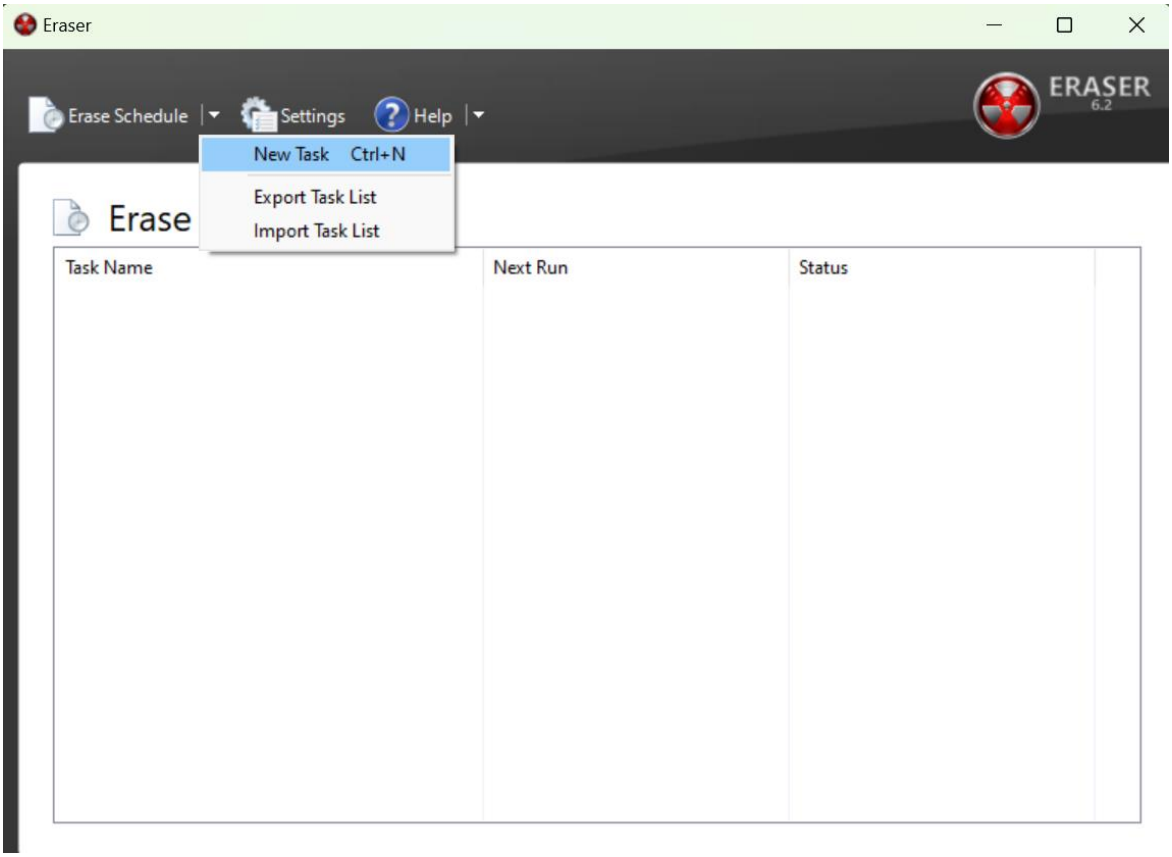
An advantage of using a program packer like UPX is that it could compress executable files to make it undetectable through static analysis. This is because the compressed file is smaller and might appear not malicious to some antivirus and other software. This means that threat actors could avoid detection of their malware when investigators are investigating using simple antivirus and forensic tools. Another advantage is that it could hide the purpose of a malicious program. This means that security system might not be able to detect it since it is compressed. This gives threat actors a higher chance of successfully executing malicious software or code without the security system being able to detect it.

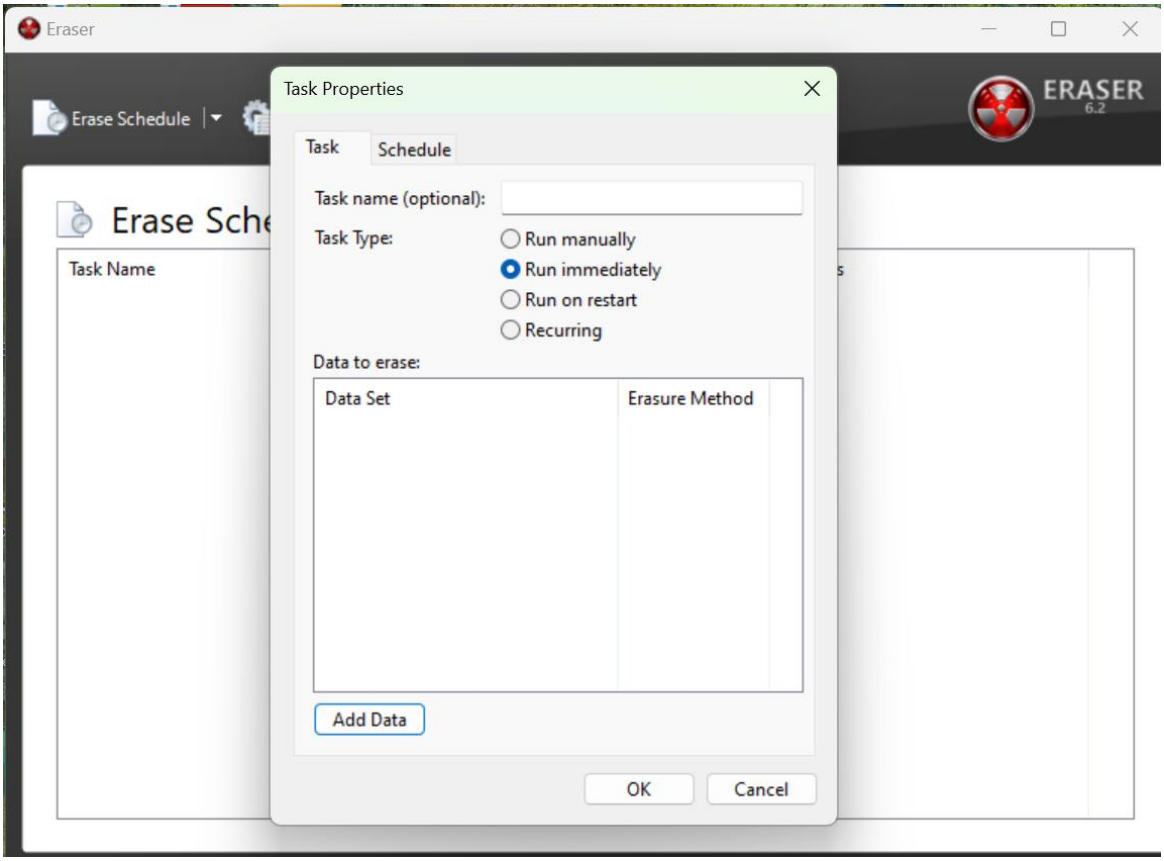
A disadvantage of program packers is that threat actors usually dynamically analyse suspicious executable files. This might uncover the true contents of the malicious executable files and what it does. This means that program packers alone might not be effective to avoid detection. Another disadvantage is that there is a chance that the program being packed could cause it to be unstable. This means that the program might not run the way it was intended, and errors might appear. This means that the program might fail to execute as intended which might lead to the failure of an attack.

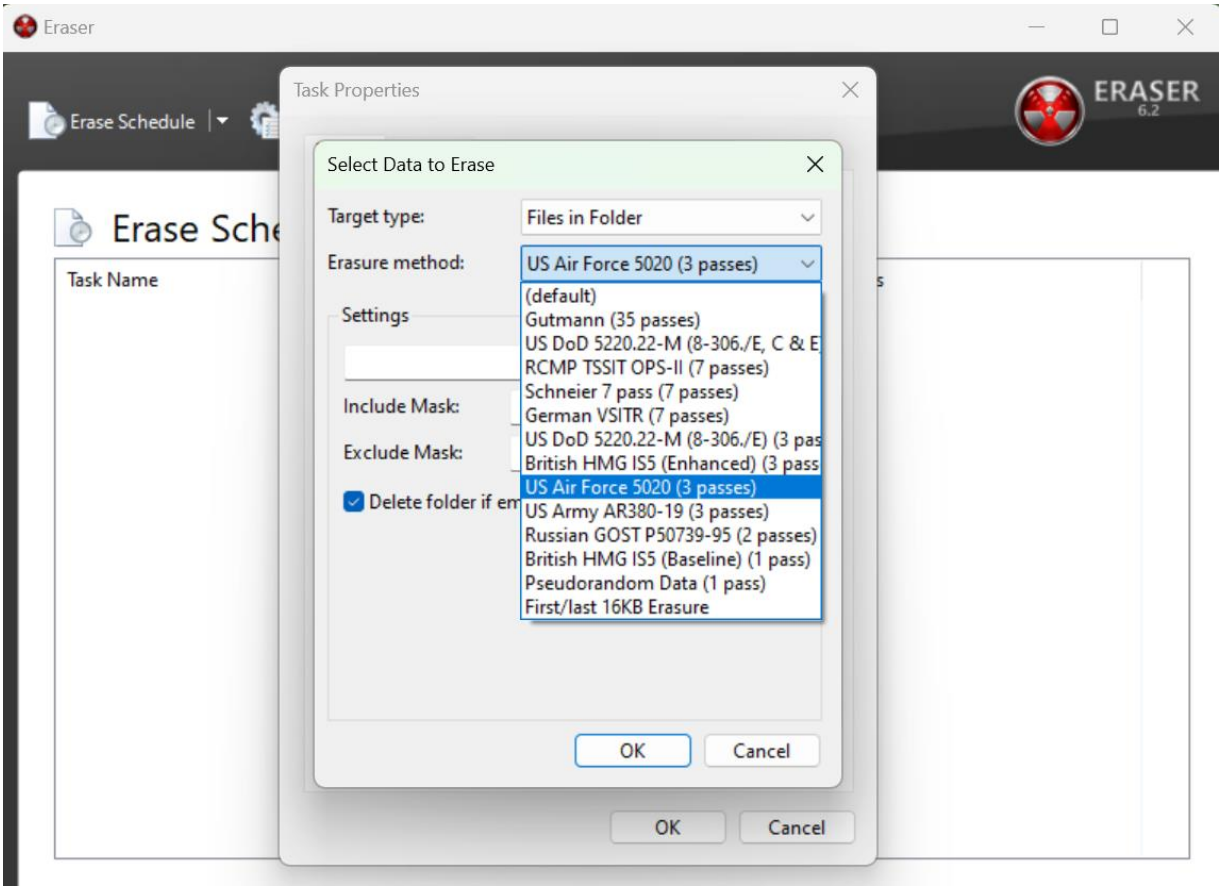
5.0 Tool Demonstration

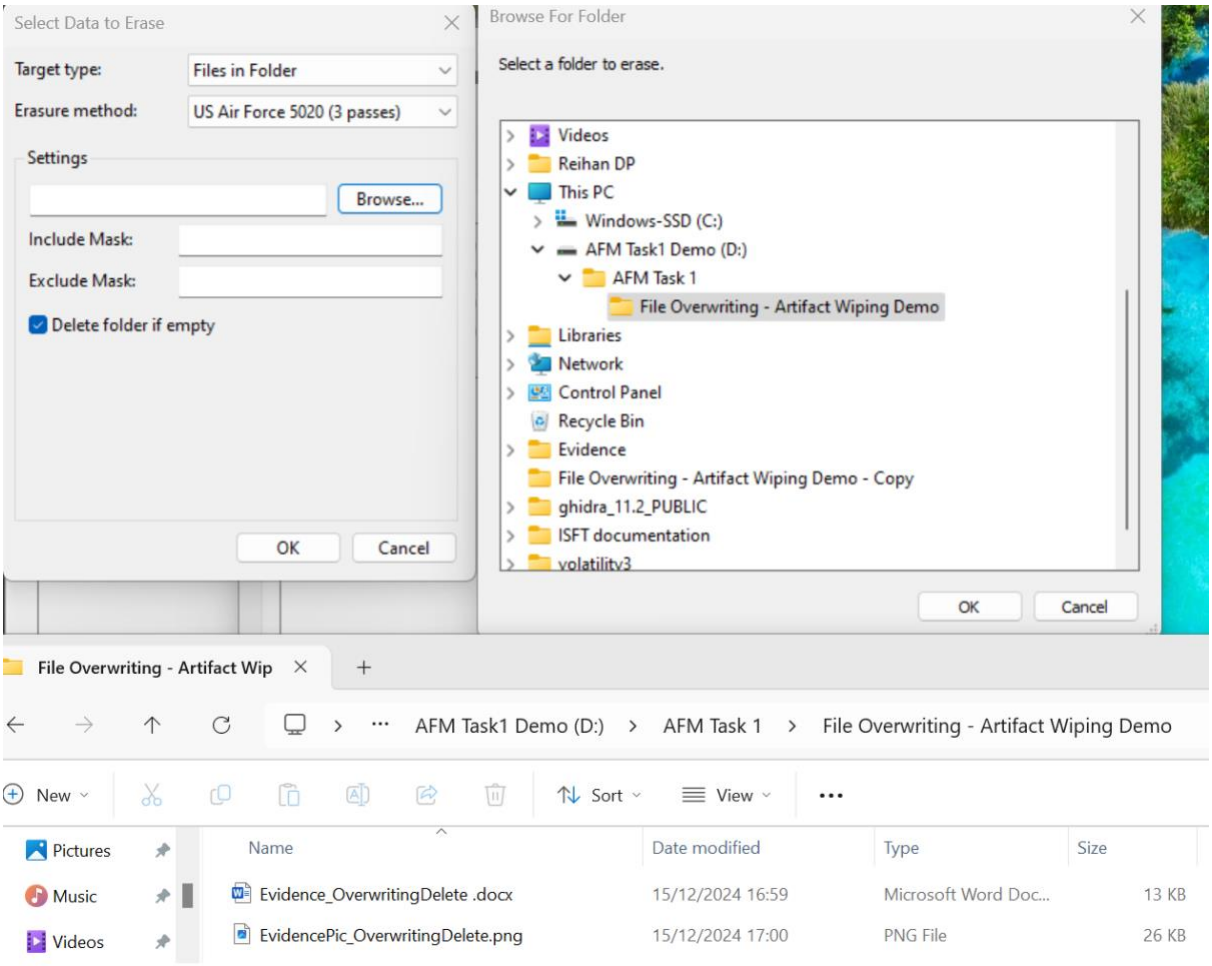
Chosen methods and tools from each anti-forensic technique would be demonstrated, showing its use and functionality.

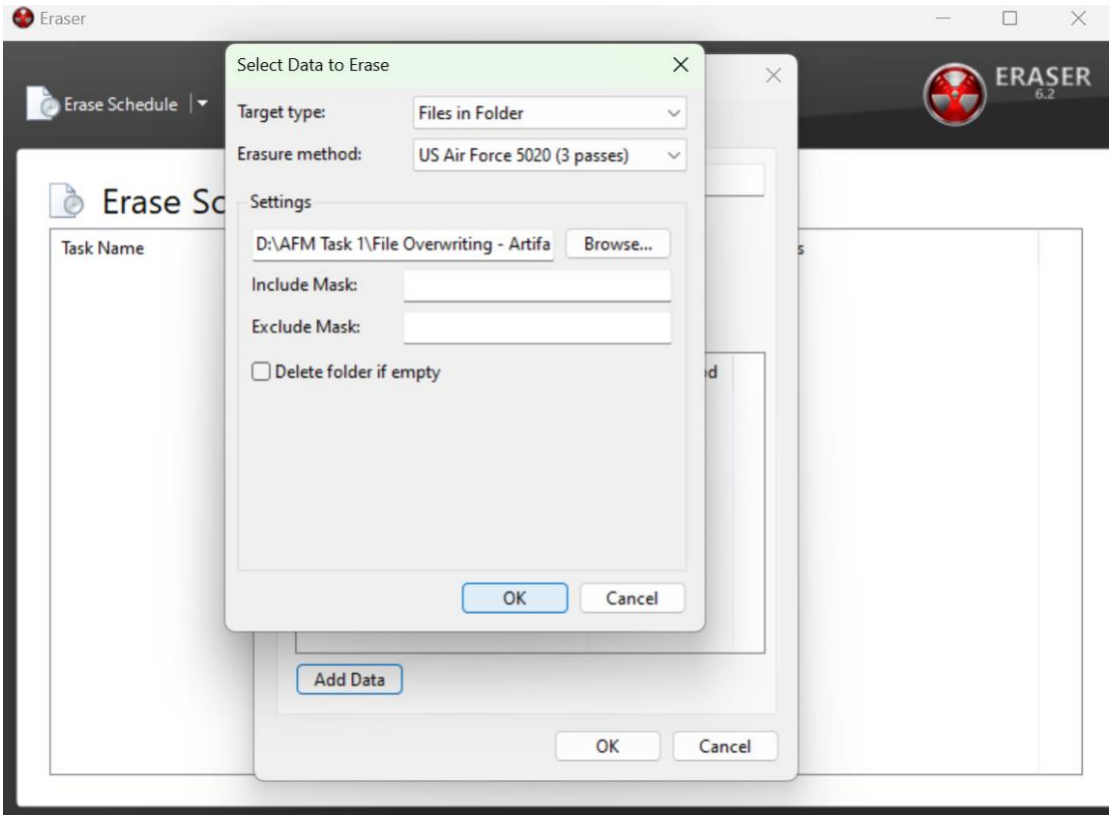
5.1 Eraser (File Overwriting) - Artifact Wiping

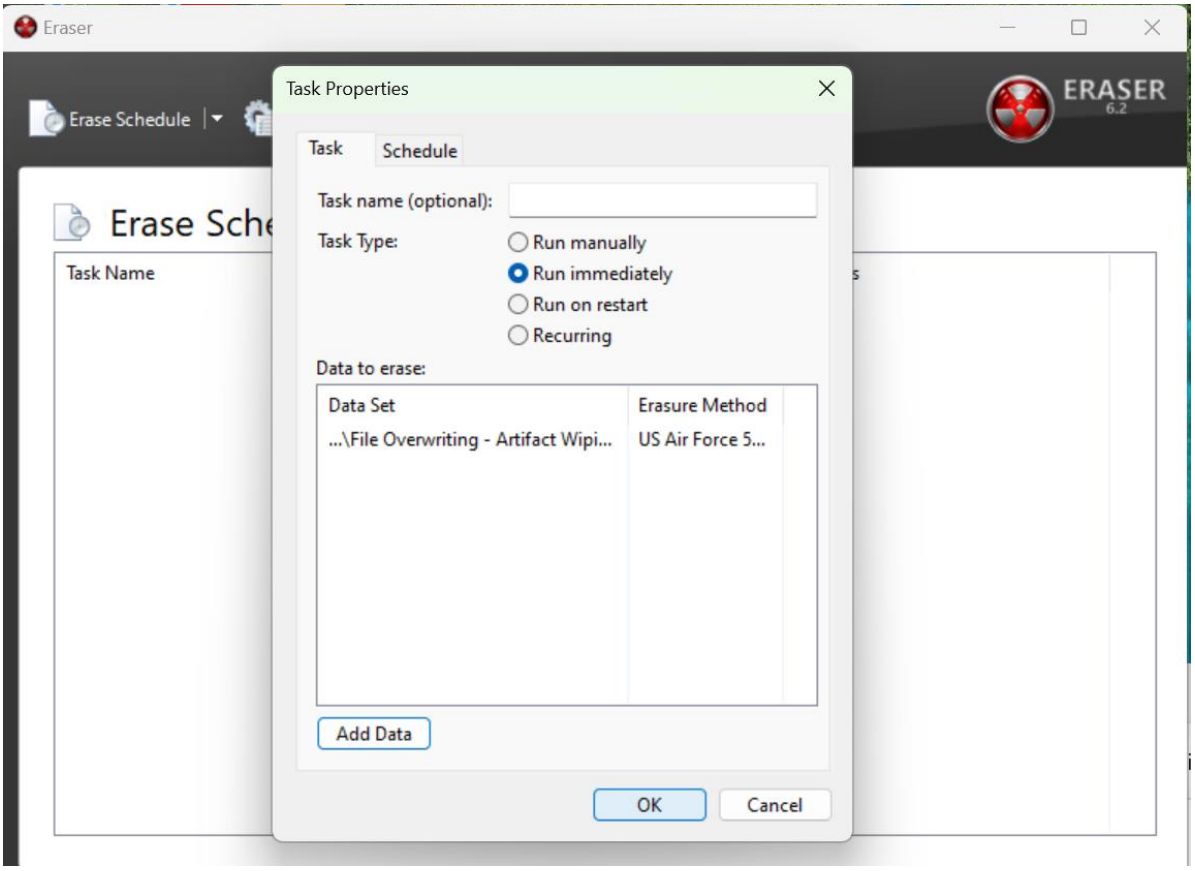


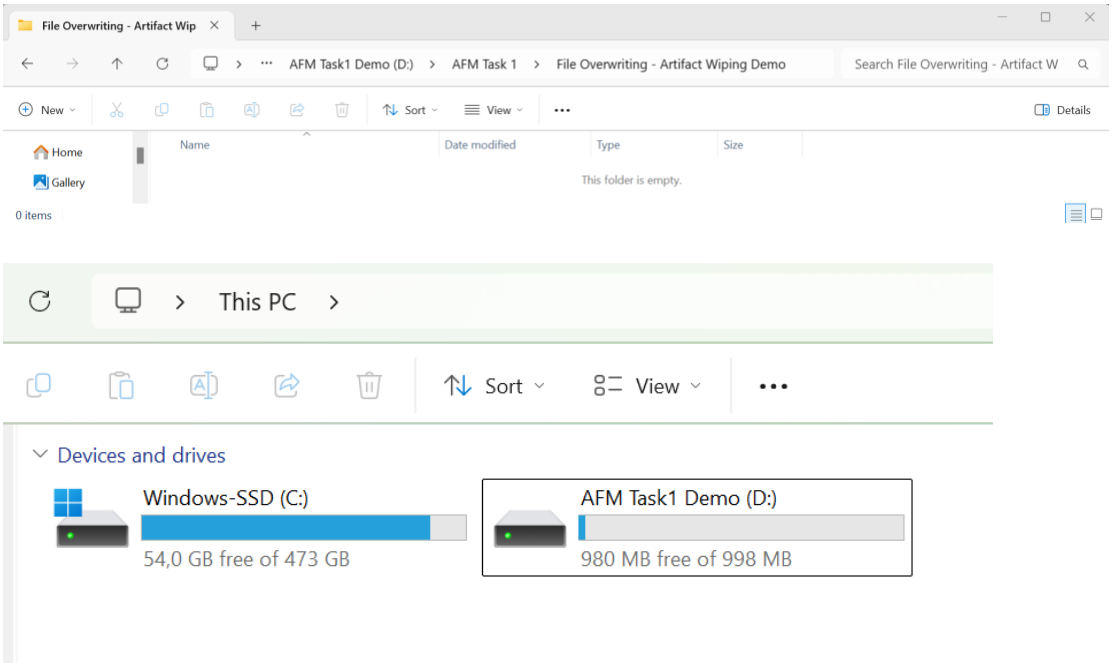

Eraser
Erase Schedule
ERASER
6.2
Erase Sche
Task Name
Task Properties
Task
Schedule
Task name (optional):
Task Type:
Run manually
Run immediately
Run on restart
Recurring
Data to erase:
Data Set
Erasure Method
Add Data
OK
Cancel

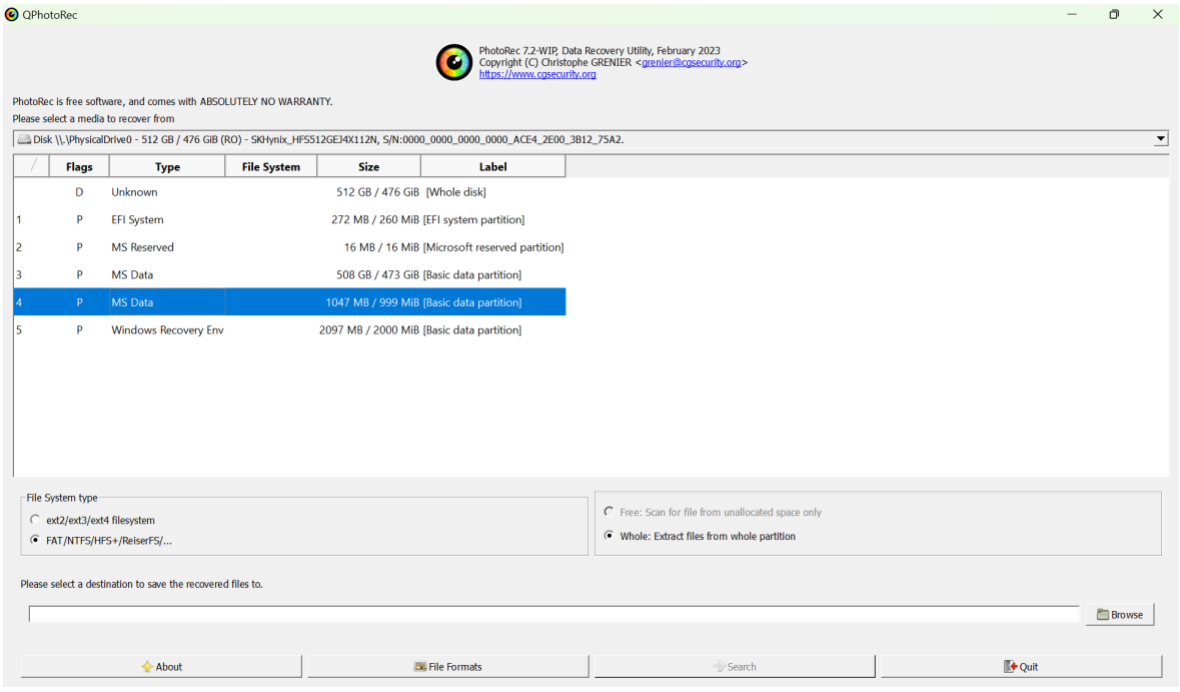

Eraser
Erase Schedule
ERASER
6.2
Erase Sche
Task Name
Task Properties
Select Data to Erase
Target type:
Files in Folder
Erasure method:
US Air Force 5020 (3 passes)
(default)
Gutmann (35 passes)
US DoD 5220.22-M (8-306./E, C & E
RCMP TSSIT OPS-II (7 passes)
Schneier 7 pass (7 passes)
German VSITR (7 passes)
US DoD 5220.22-M (8-306./E) (3 pas
British HMG IS5 (Enhanced) (3 pass
US Air Force 5020 (3 passes)
US Army AR380-19 (3 passes)
Russian GOST P50739-95 (2 passes)
British HMG IS5 (Baseline) (1 pass)
Pseudorandom Data (1 pass)
First/last 16KB Erasure
Settings
Include Mask:
Exclude Mask:
Delete folder if em
OK
Cancel
OK
Cancel

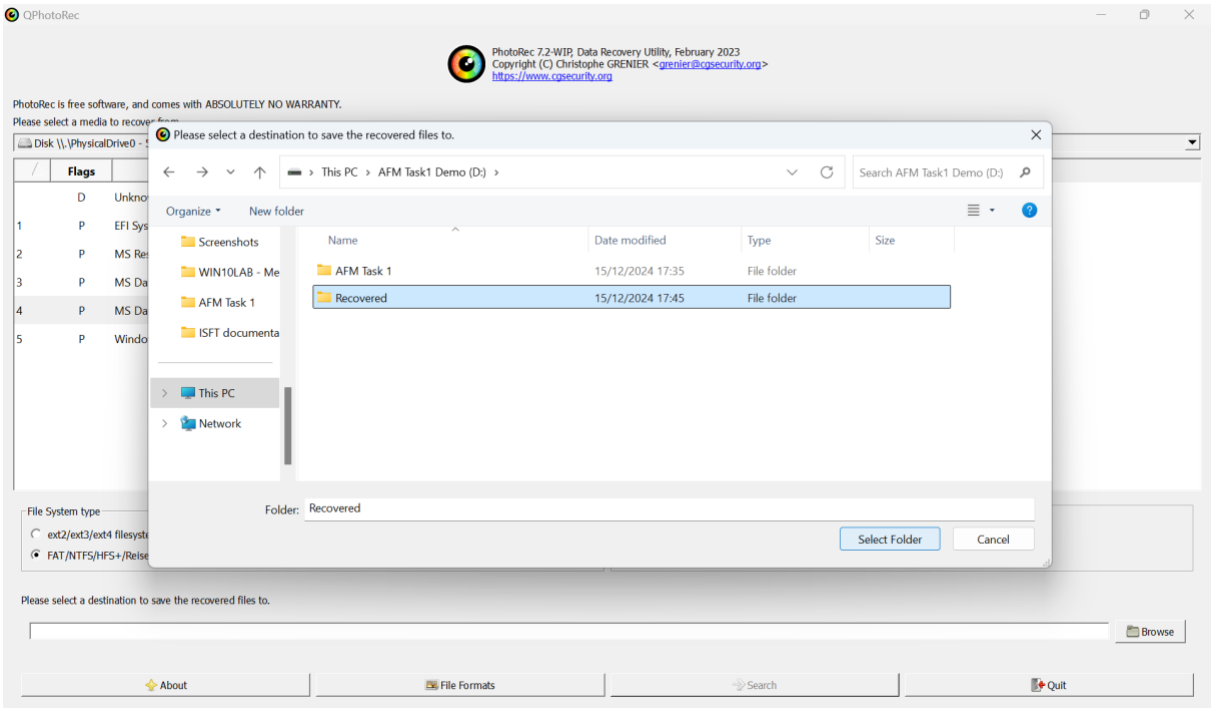

Select Data to Erase
Target type:
Files in Folder
Erasure method:
US Air Force 5020 (3 passes)
Settings
Browse...
Include Mask:
Exclude Mask:
Delete folder if empty
OK
Cancel
Browse For Folder
Select a folder to erase.
Videos
Reihan DP
This PC
Windows-SSD (C:)
AFM Task1 Demo (D:)
AFM Task 1
File Overwriting - Artifact Wiping Demo
Libraries
Network
Control Panel
Recycle Bin
Evidence
File Overwriting - Artifact Wiping Demo - Copy
ghidra_11.2_PUBLIC
ISFT documentation
volatility3
OK
Cancel
File Overwriting - Artifact Wip
AFM Task1 Demo (D:)
AFM Task 1
File Overwriting - Artifact Wiping Demo
New
Sort
View
Pictures
Music
Videos
Name
Date modified
Type
Size
Evidence_OverwritingDelete .docx
15/12/2024 16:59
Microsoft Word Doc...
13 KB
EvidencePic_OverwritingDelete.png
15/12/2024 17:00
PNG File
26 KB

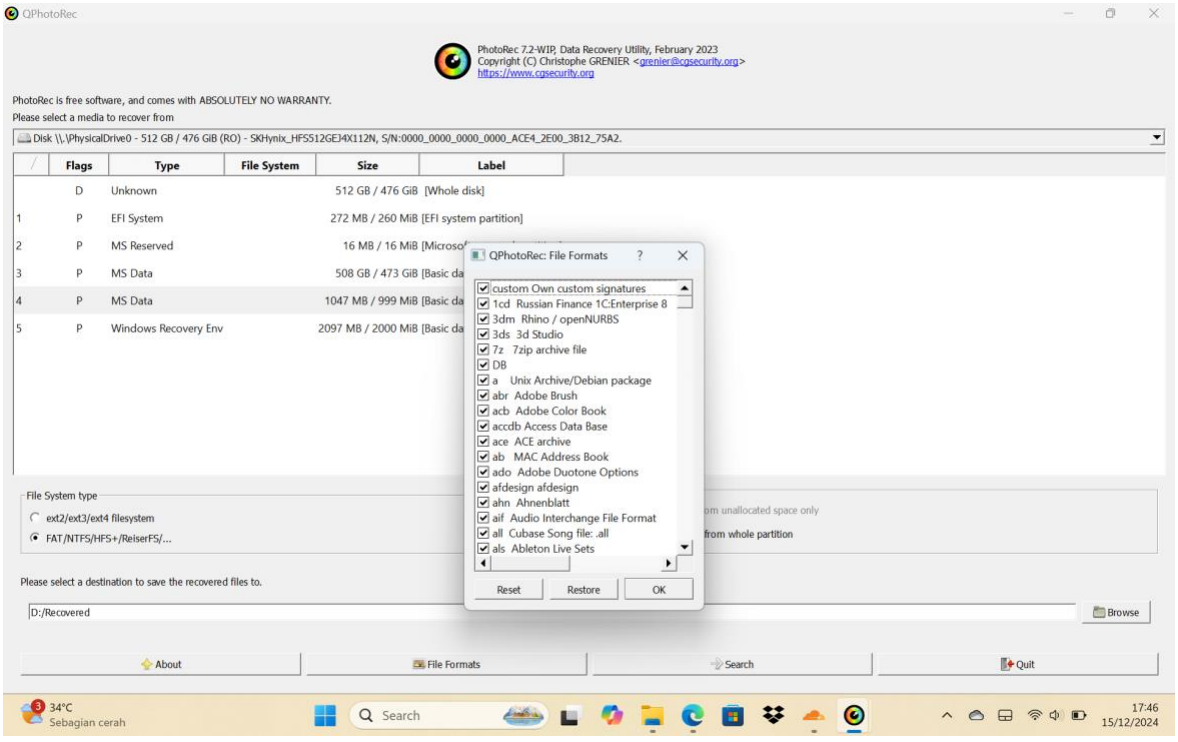

Eraser
Erase Schedule
ERASER
6.2
Erase Sc
Task Name
Select Data to Erase
Target type:
Files in Folder
Erasure method:
US Air Force 5020 (3 passes)
Settings
D:\AFM Task 1\File Overwriting - Artifa
Browse...
Include Mask:
Exclude Mask:
Delete folder if empty
OK
Cancel
Add Data
OK
Cancel

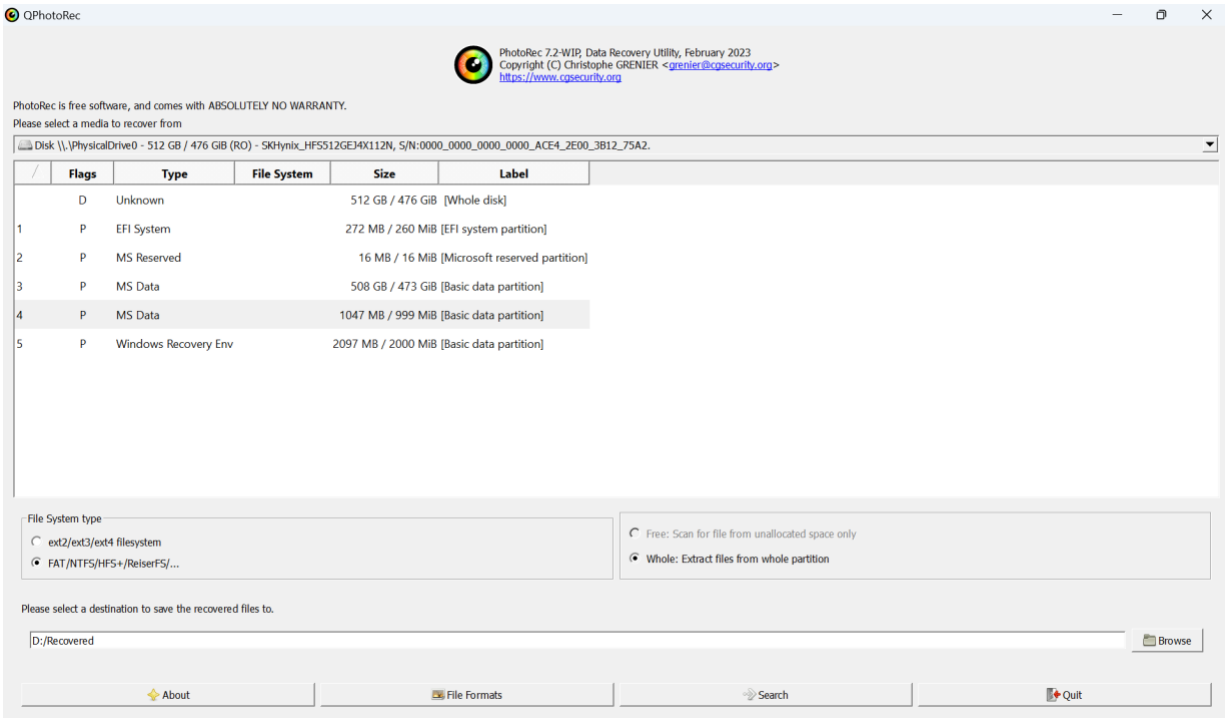

Eraser
Erase Schedule
ERASER
6.2
Erase Sche
Task Name
Task Properties
Task
Schedule
Task name (optional):
Task Type:
Run manually
Run immediately
Run on restart
Recurring
Data to erase:
Data Set
Erasure Method
...\File Overwriting - Artifact Wipi...
US Air Force 5...
Add Data
OK
Cancel

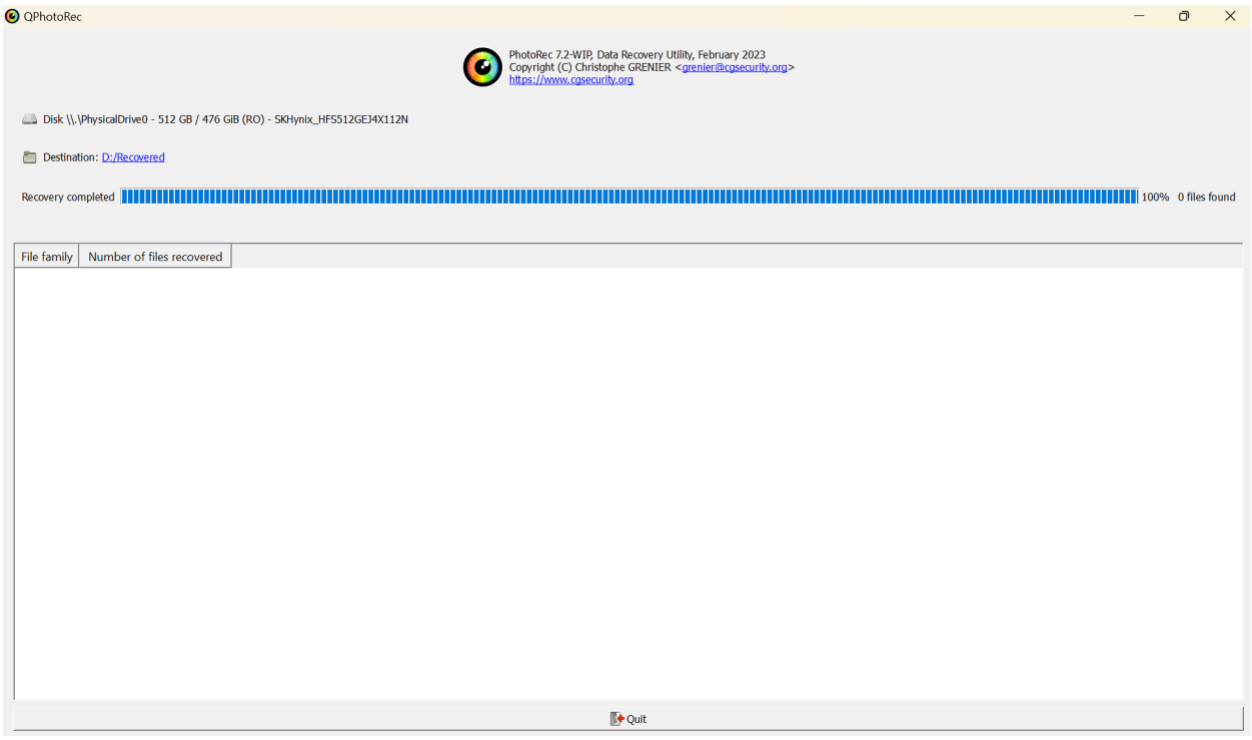

File Overwriting - Artifact Wip
AFM Task1 Demo (D:)
AFM Task 1
File Overwriting - Artifact Wiping Demo
Search File Overwriting - Artifact W
New
Sort
View
Details
Home
Gallery
Name
Date modified
Type
Size
This folder is empty.
0 items
This PC
Sort
View
Devices and drives
Windows-SSD (C:)
54,0 GB free of 473 GB
AFM Task1 Demo (D:)
980 MB free of 998 MB


QPhotoRec
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a media to recover from
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB (RO) - SKHynix_HFS512GEJ4X112N, S/N:0000_0000_0000_0000_ACE4_2E00_3B12_75A2.
Flags
Type
File System
Size
Label
D Unknown 512 GB / 476 GiB [Whole disk]
1 P EFI System 272 MB / 260 MiB [EFI system partition]
2 P MS Reserved 16 MB / 16 MiB [Microsoft reserved partition]
3 P MS Data 508 GB / 473 GiB [Basic data partition]
4 P MS Data 1047 MB / 999 MiB [Basic data partition]
5 P Windows Recovery Env 2097 MB / 2000 MiB [Basic data partition]
File System type
ext2/ext3/ext4 filesystem
FAT/NTFS/HFS+/ReiserFS/...
Free: Scan for file from unallocated space only
Whole: Extract files from whole partition
Please select a destination to save the recovered files to.
Browse
About
File Formats
Search
Quit

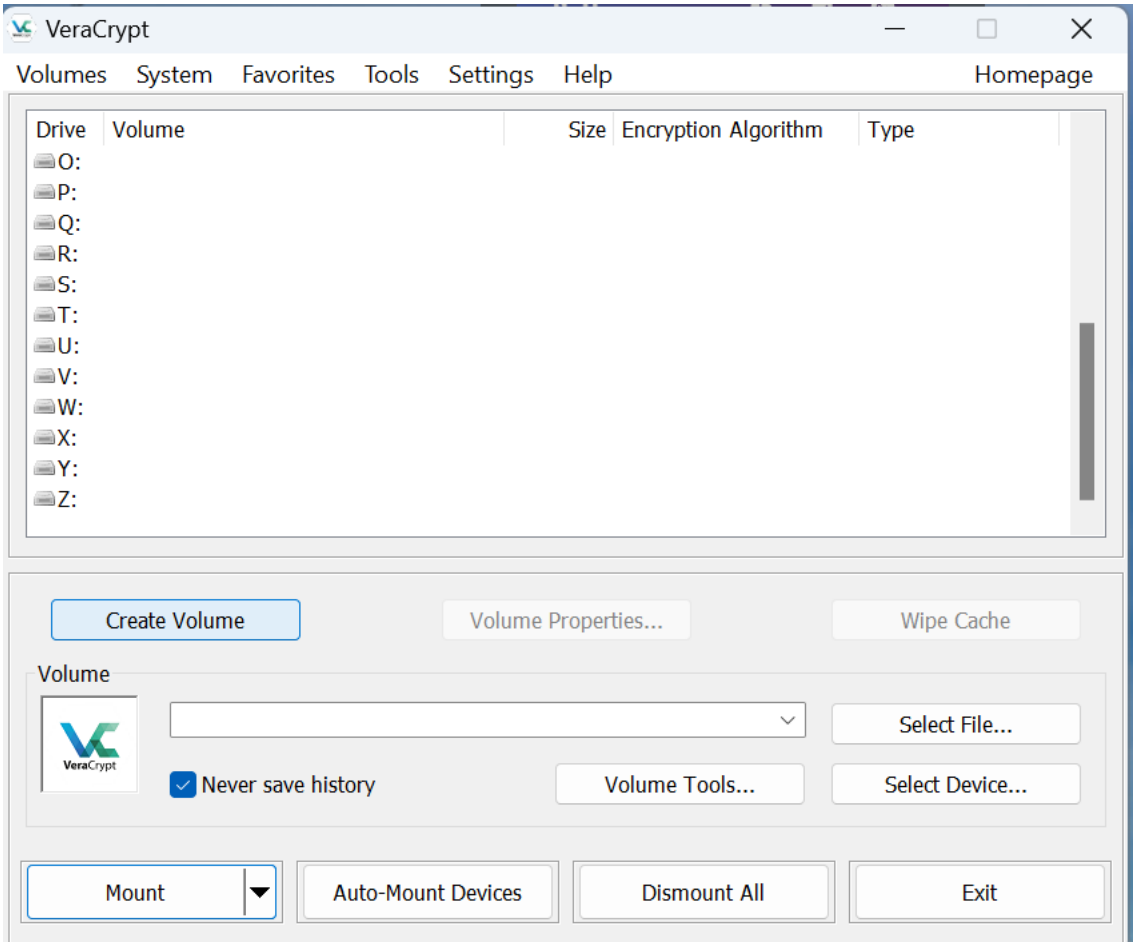

QPhotoRec
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a destination to save the recovered files to.
This PC › AFM Task1 Demo (D:) ›
Search AFM Task1 Demo (D:)
Organize
New folder
Screenshots
WIN10LAB - Me
AFM Task 1
ISFT documenta
This PC
Network
Name
Date modified
Type
Size
AFM Task 1
15/12/2024 17:35
File folder
Recovered
15/12/2024 17:45
File folder
Folder: Recovered
Select Folder
Cancel
File System type
Please select a destination to save the recovered files to.
Browse
About
File Formats
Search
Quit

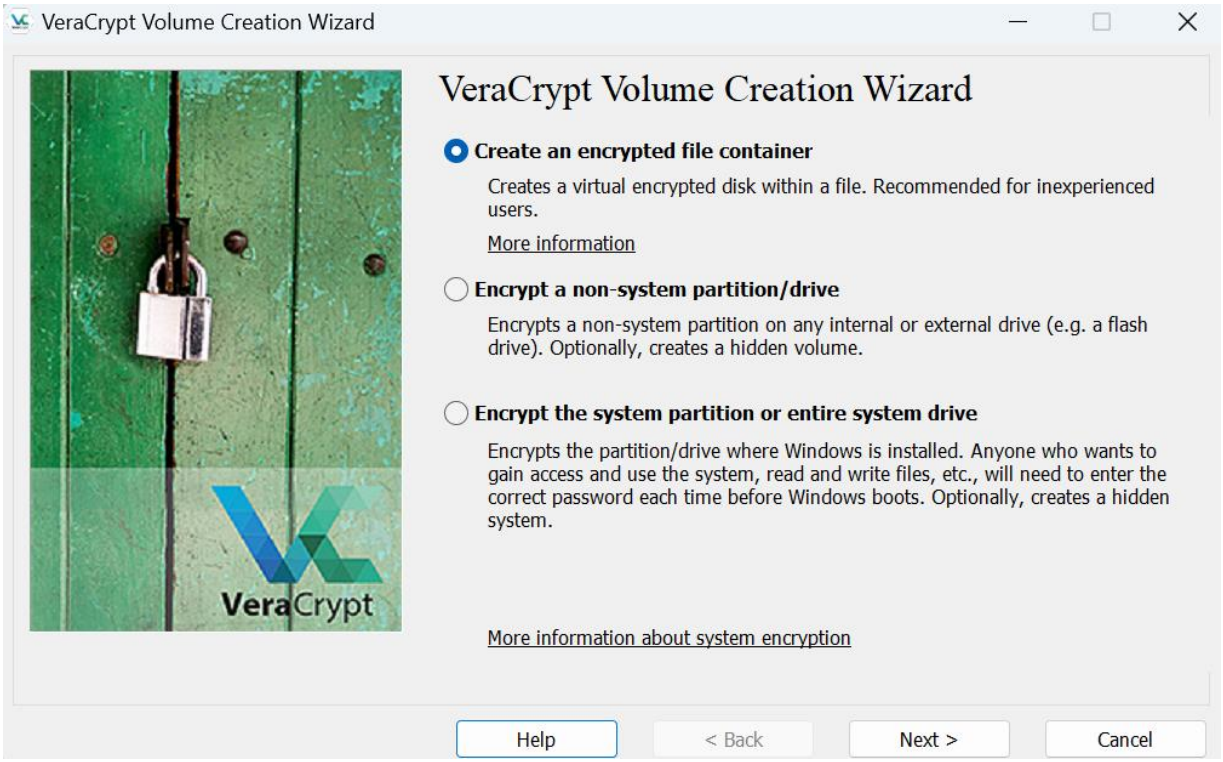

QPhotoRec
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a media to recover from
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB (RO) - SKHynix_HFS512GEJ4X112N, S/N:0000_0000_0000_0000_ACE4_2E00_3B12_75A2.
Flags
Type
File System
Size
Label
D Unknown 512 GB / 476 GiB [Whole disk]
1 P EFI System 272 MB / 260 MiB [EFI system partition]
2 P MS Reserved 16 MB / 16 MiB
3 P MS Data 508 GB / 473 GiB
4 P MS Data 1047 MB / 999 MiB
5 P Windows Recovery Env 2097 MB / 2000 MiB
QPhotoRec: File Formats
custom Own custom signatures
1cd Russian Finance 1C:Enterprise 8
3dm Rhino / openNURBS
3ds 3d Studio
7z 7zip archive file
DB
a Unix Archive/Debian package
abr Adobe Brush
acb Adobe Color Book
accdb Access Data Base
ace ACE archive
ab MAC Address Book
ado Adobe Duotone Options
afdesign afdesign
ahn Ahnenblatt
aif Audio Interchange File Format
all Cubase Song file: .all
als Ableton Live Sets
Reset
Restore
OK
File System type
ext2/ext3/ext4 filesystem
FAT/NTFS/HFS+/ReiserFS/...
Please select a destination to save the recovered files to.
D:/Recovered
Browse
About
File Formats
Search
Quit
34°C
Sebagian cerah
Search
17:46
15/12/2024

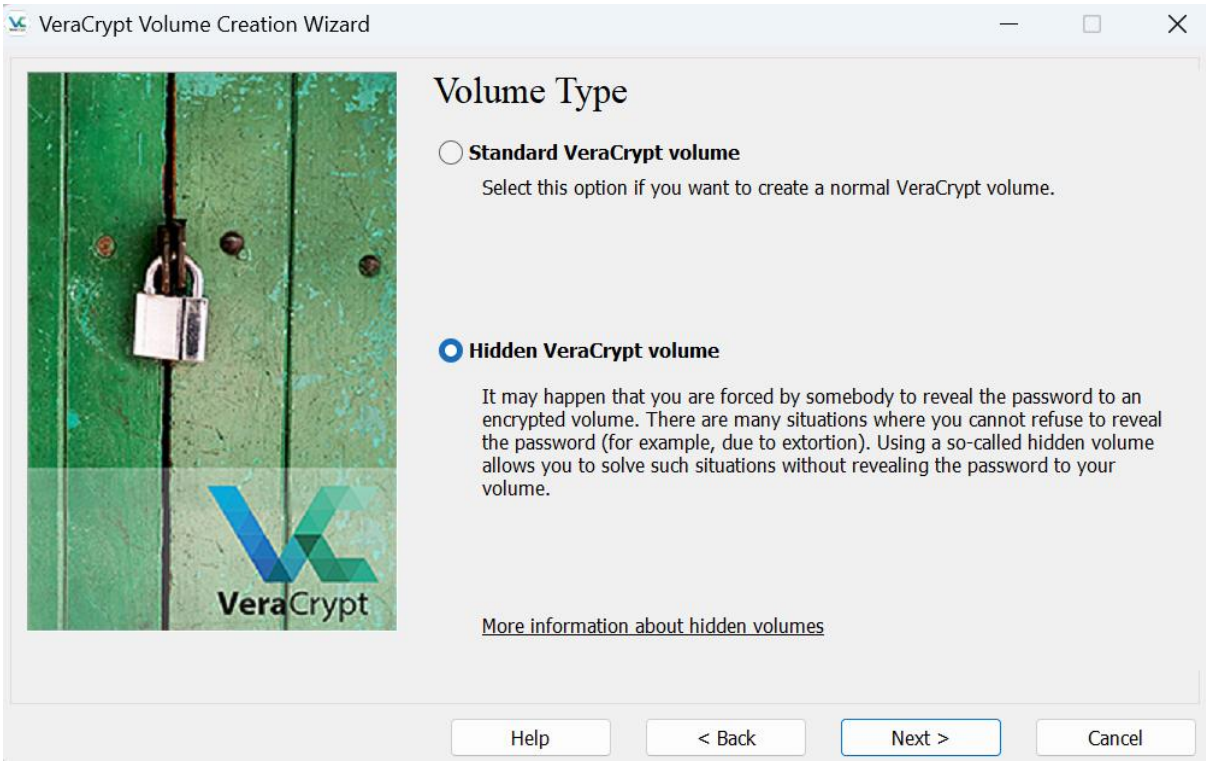

QPhotoRec
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a media to recover from
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB (RO) - SKHynix_HFS512GEJ4X112N, S/N:0000_0000_0000_0000_ACE4_2E00_3B12_75A2.
Flags Type File System Size Label
D Unknown 512 GB / 476 GiB [Whole disk]
1 P EFI System 272 MB / 260 MiB [EFI system partition]
2 P MS Reserved 16 MB / 16 MiB [Microsoft reserved partition]
3 P MS Data 508 GB / 473 GiB [Basic data partition]
4 P MS Data 1047 MB / 999 MiB [Basic data partition]
5 P Windows Recovery Env 2097 MB / 2000 MiB [Basic data partition]
File System type
ext2/ext3/ext4 filesystem
FAT/NTFS/HFS+/ReiserFS/...
Free: Scan for file from unallocated space only
Whole: Extract files from whole partition
Please select a destination to save the recovered files to.
D:/Recovered
Browse
About
File Formats
Search
Quit

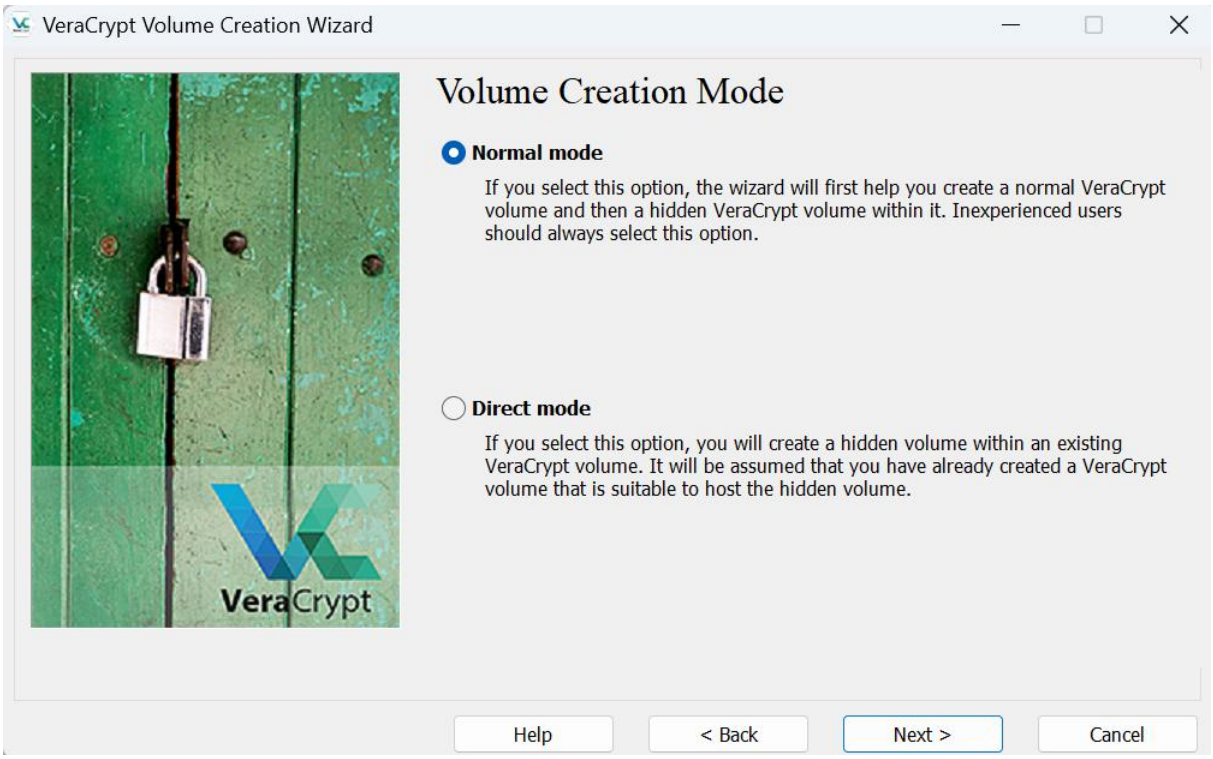

QPhotoRec
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB (RO) - SKHynix_HFS512GEJ4X112N
Destination: D:/Recovered
Recovery completed
100% 0 files found
File family
Number of files recovered
Quit

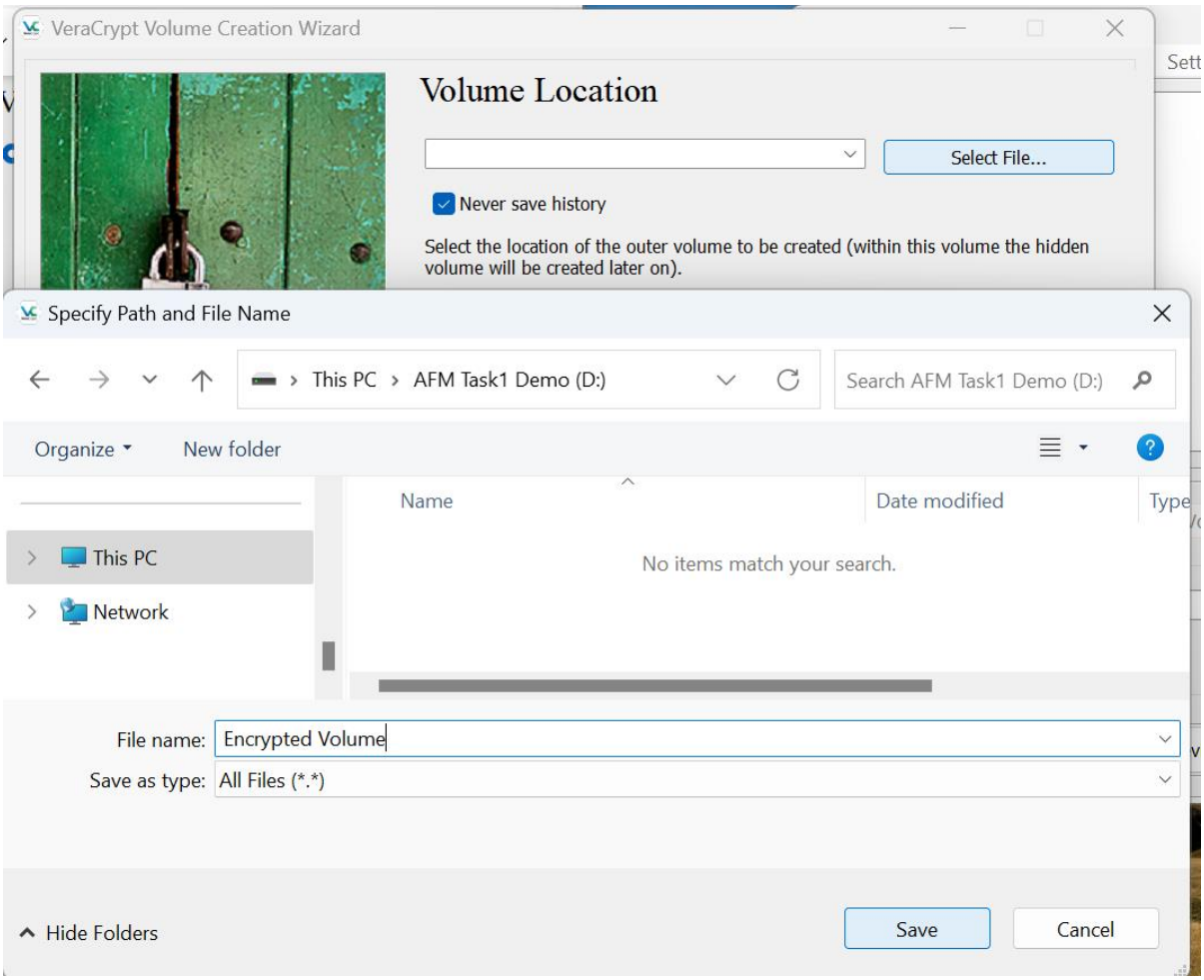
5.2 VeraCrypt (Encryption) - Hiding Evidence

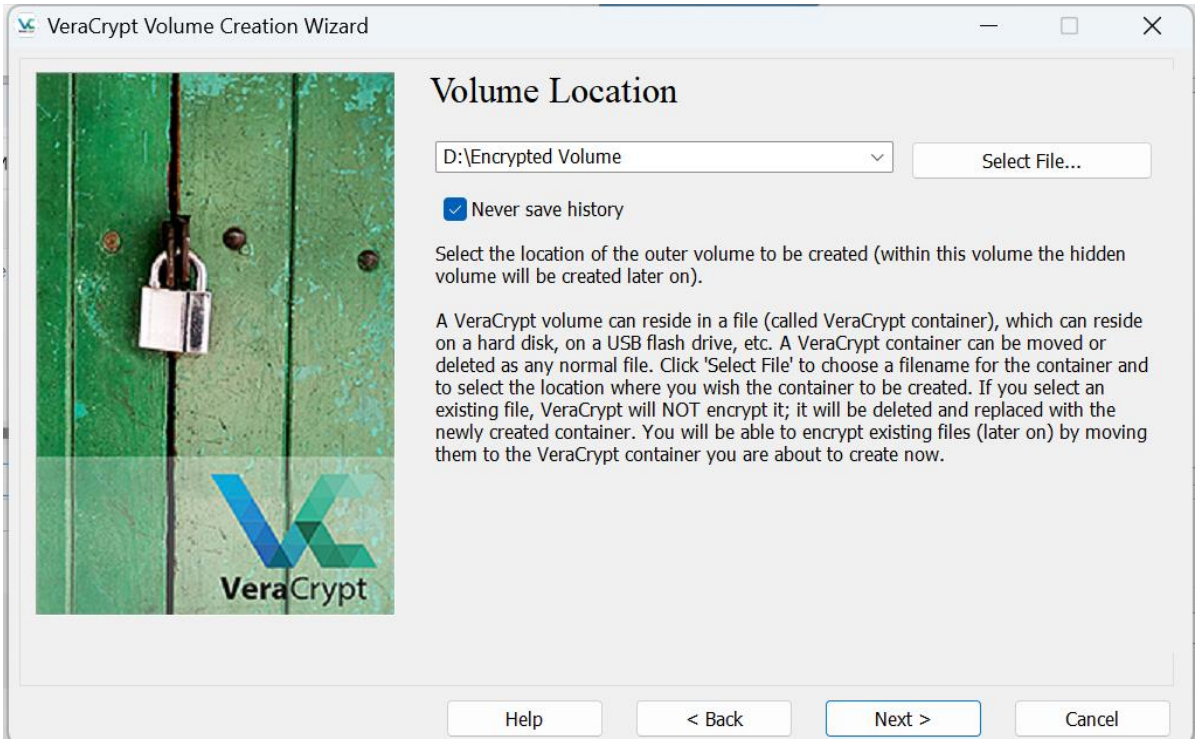


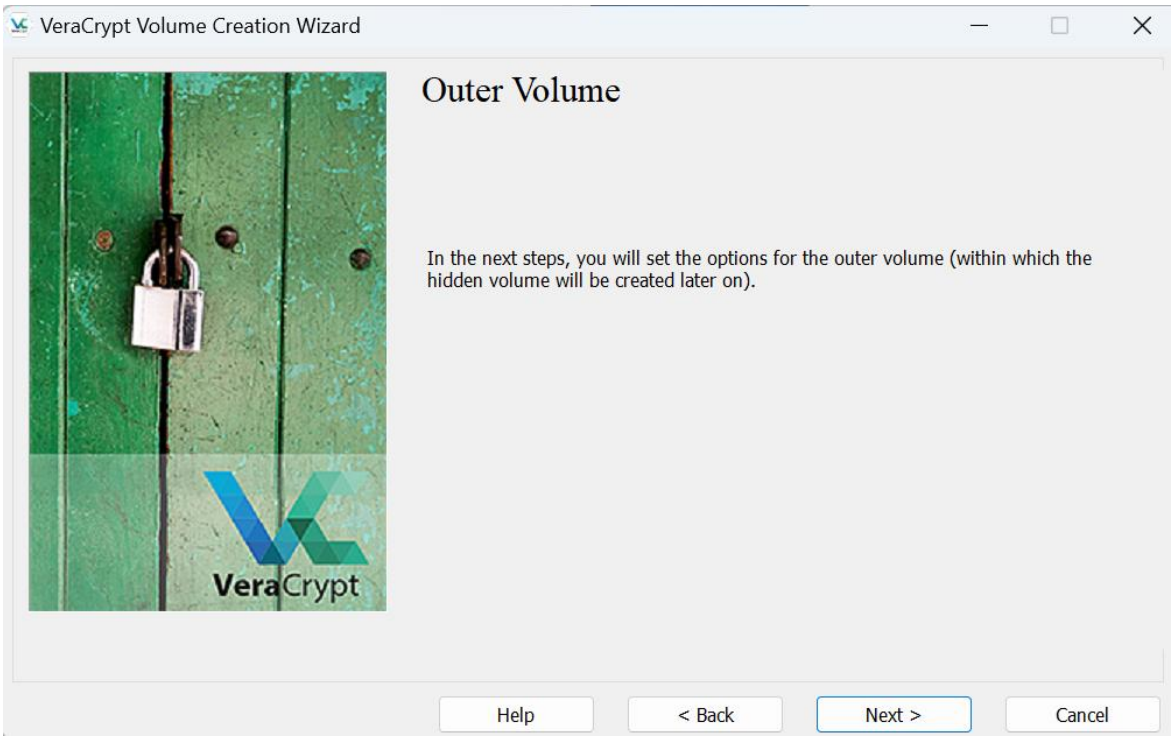

VeraCrypt Volume Creation Wizard
VeraCrypt Volume Creation Wizard
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
VeraCrypt
Help
< Back
Next >
Cancel


VeraCrypt Volume Creation Wizard
Volume Type
Standard VeraCrypt volume
Select this option if you want to create a normal VeraCrypt volume.
Hidden VeraCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
VeraCrypt
Help
< Back
Next >
Cancel

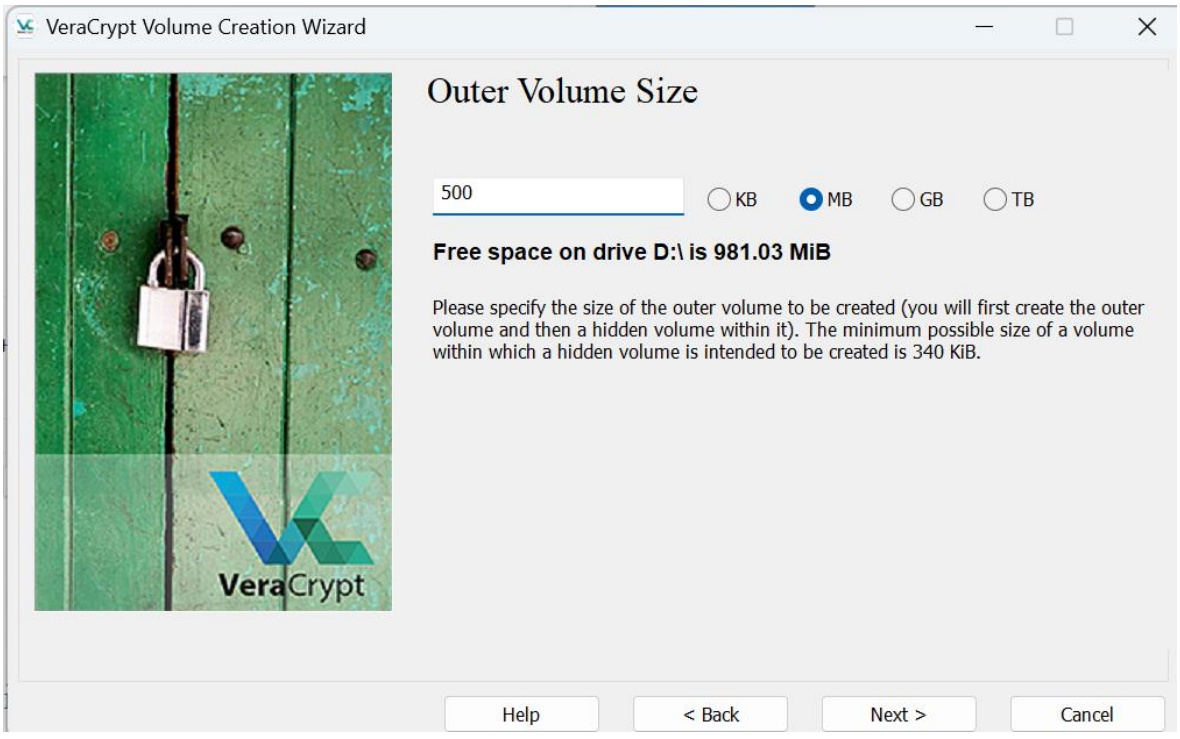

VeraCrypt Volume Creation Wizard
Volume Creation Mode
Normal mode
If you select this option, the wizard will first help you create a normal VeraCrypt volume and then a hidden VeraCrypt volume within it. Inexperienced users should always select this option.
Direct mode
If you select this option, you will create a hidden volume within an existing VeraCrypt volume. It will be assumed that you have already created a VeraCrypt volume that is suitable to host the hidden volume.
VeraCrypt
Help
< Back
Next >
Cancel

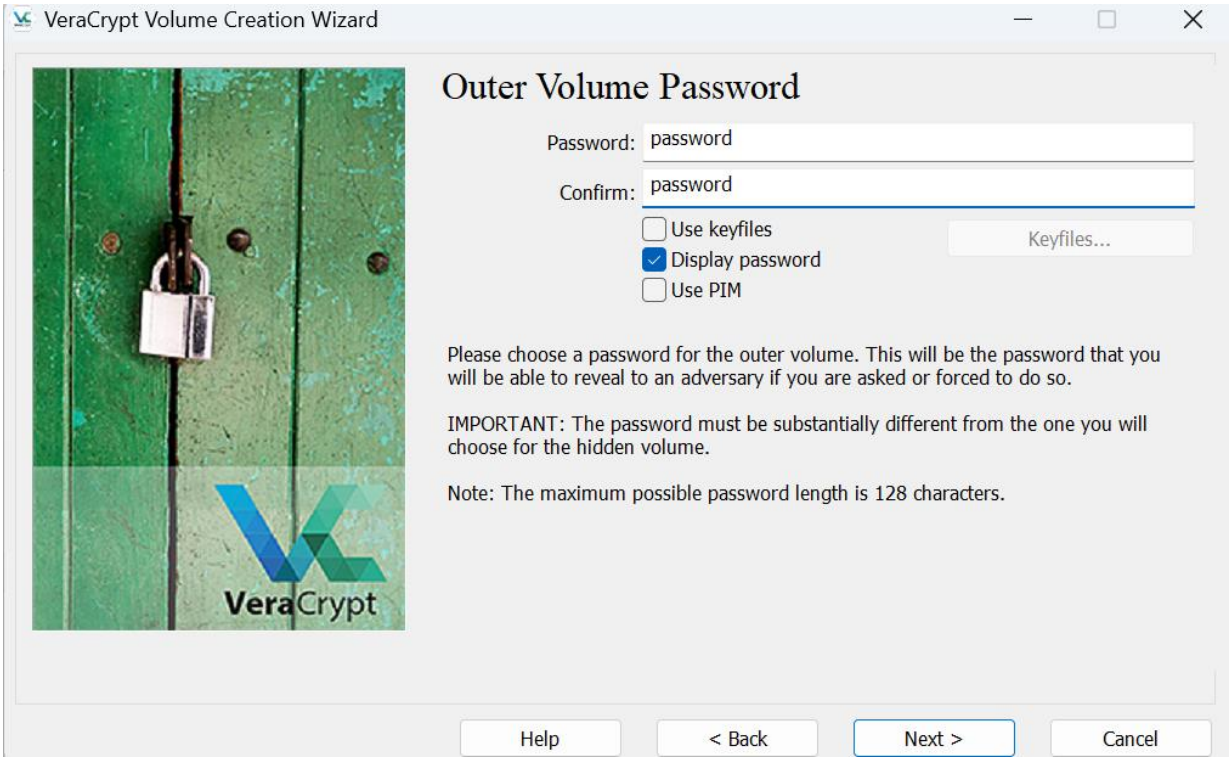

VeraCrypt Volume Creation Wizard
Volume Location
Select File...
Never save history
Select the location of the outer volume to be created (within this volume the hidden volume will be created later on).
Specify Path and File Name
This PC › AFM Task1 Demo (D:)
Search AFM Task1 Demo (D:)
Organize
New folder
Name
Date modified
Type
This PC
Network
No items match your search.
File name: Encrypted Volume
Save as type: All Files (*.*)
Hide Folders
Save
Cancel

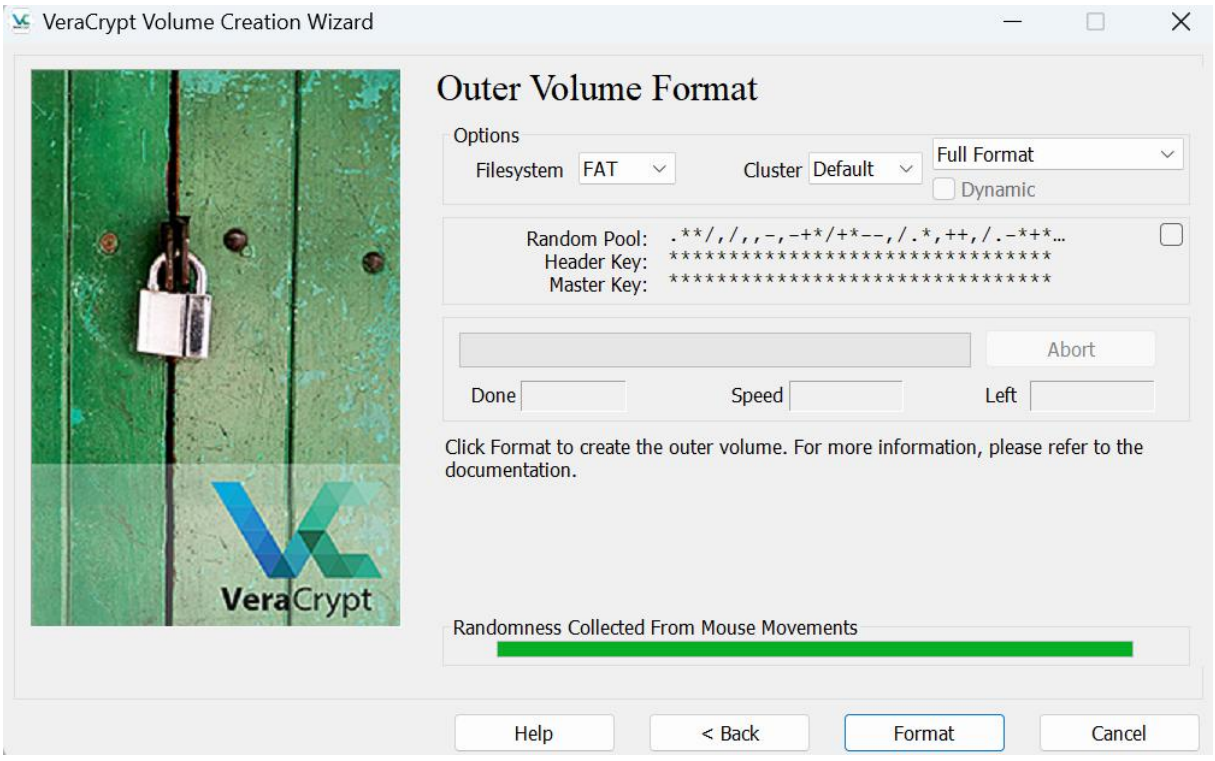

VeraCrypt Volume Creation Wizard
Volume Location
D:\Encrypted Volume
Select File...
Never save history
Select the location of the outer volume to be created (within this volume the hidden volume will be created later on).
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container can be moved or deleted as any normal file. Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created. If you select an existing file, VeraCrypt will NOT encrypt it; it will be deleted and replaced with the newly created container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container you are about to create now.
VeraCrypt
Help
< Back
Next >
Cancel

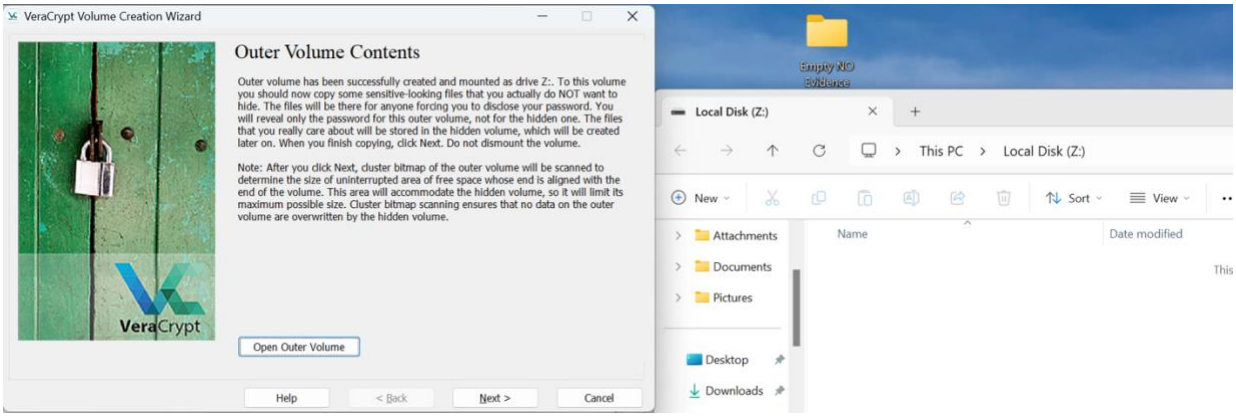

VeraCrypt Volume Creation Wizard
Outer Volume
In the next steps, you will set the options for the outer volume (within which the hidden volume will be created later on).
VeraCrypt
Help
< Back
Next >
Cancel

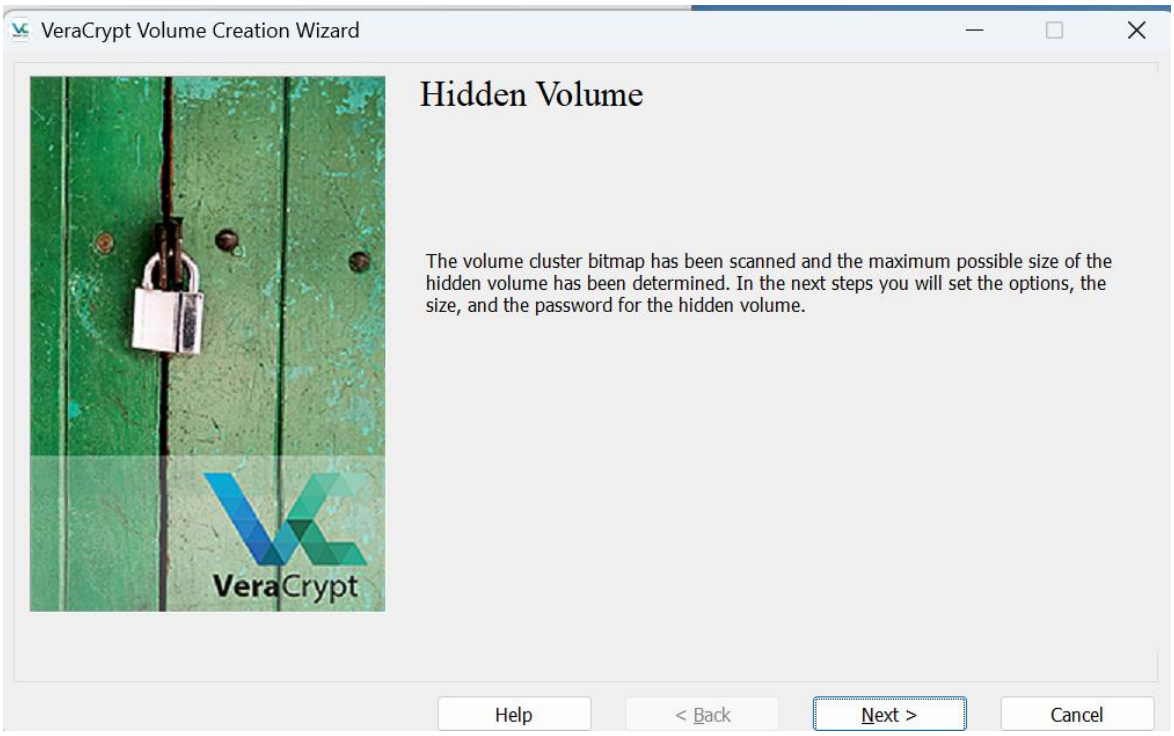

VeraCrypt Volume Creation Wizard
Outer Volume Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
SHA-256
Information on hash algorithms
Help
< Back
Next >
Cancel
VeraCrypt

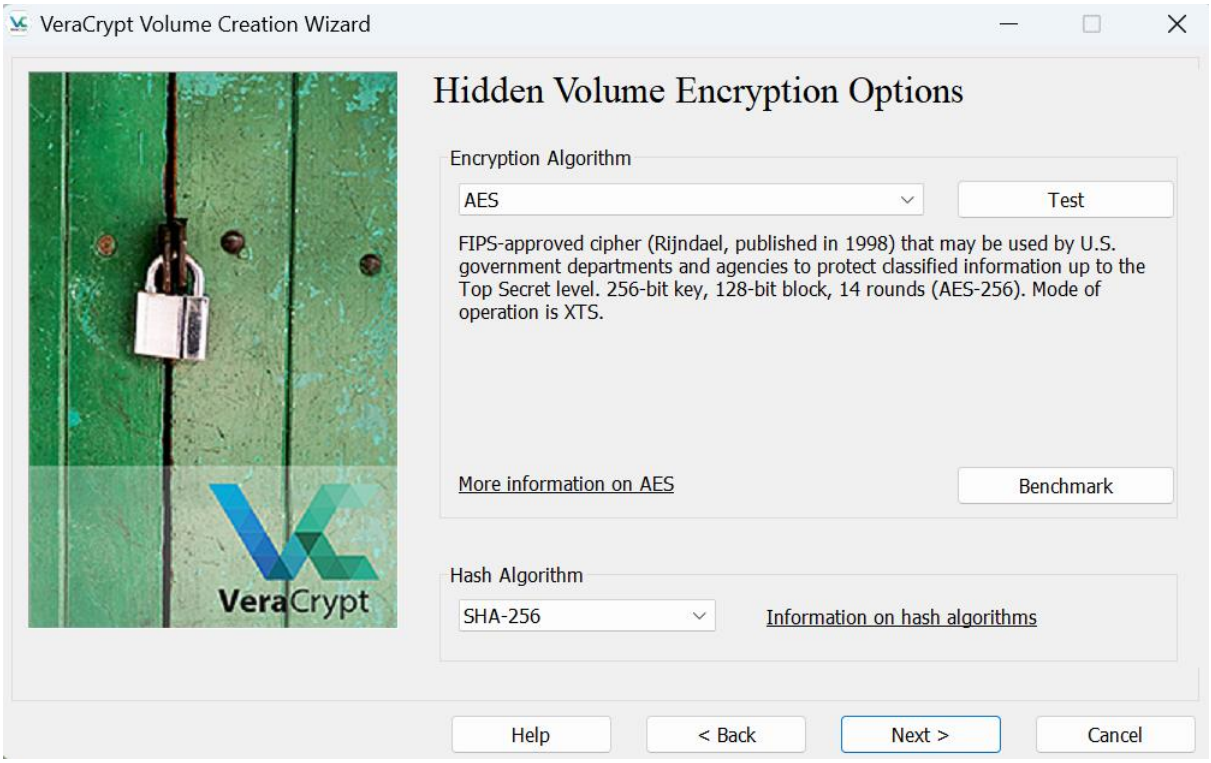

VeraCrypt Volume Creation Wizard
Outer Volume Size
500
KB
MB
GB
TB
Free space on drive D:\ is 981.03 MiB
Please specify the size of the outer volume to be created (you will first create the outer volume and then a hidden volume within it). The minimum possible size of a volume within which a hidden volume is intended to be created is 340 KiB.
Help
< Back
Next >
Cancel
VeraCrypt

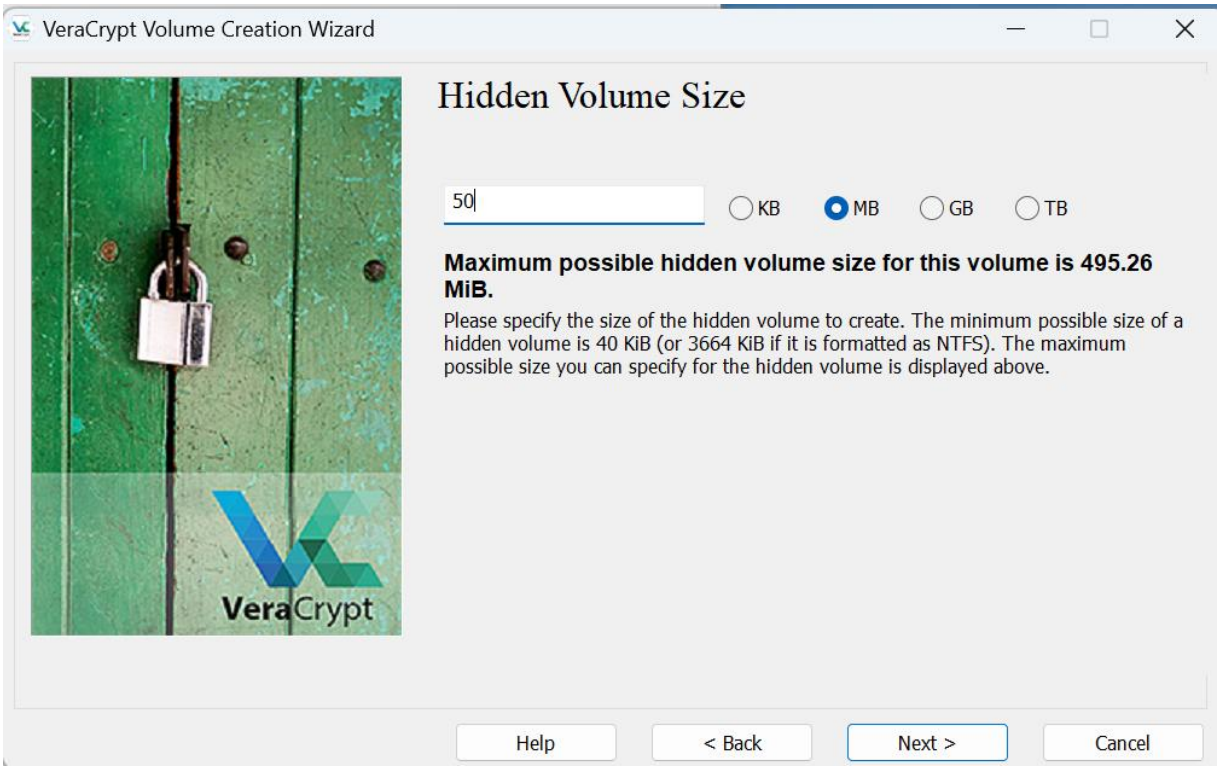

VeraCrypt Volume Creation Wizard
Outer Volume Password
Password: password
Confirm: password
Use keyfiles
Keyfiles...
Display password
Use PIM
Please choose a password for the outer volume. This will be the password that you will be able to reveal to an adversary if you are asked or forced to do so.
IMPORTANT: The password must be substantially different from the one you will choose for the hidden volume.
Note: The maximum possible password length is 128 characters.
VeraCrypt
Help
< Back
Next >
Cancel

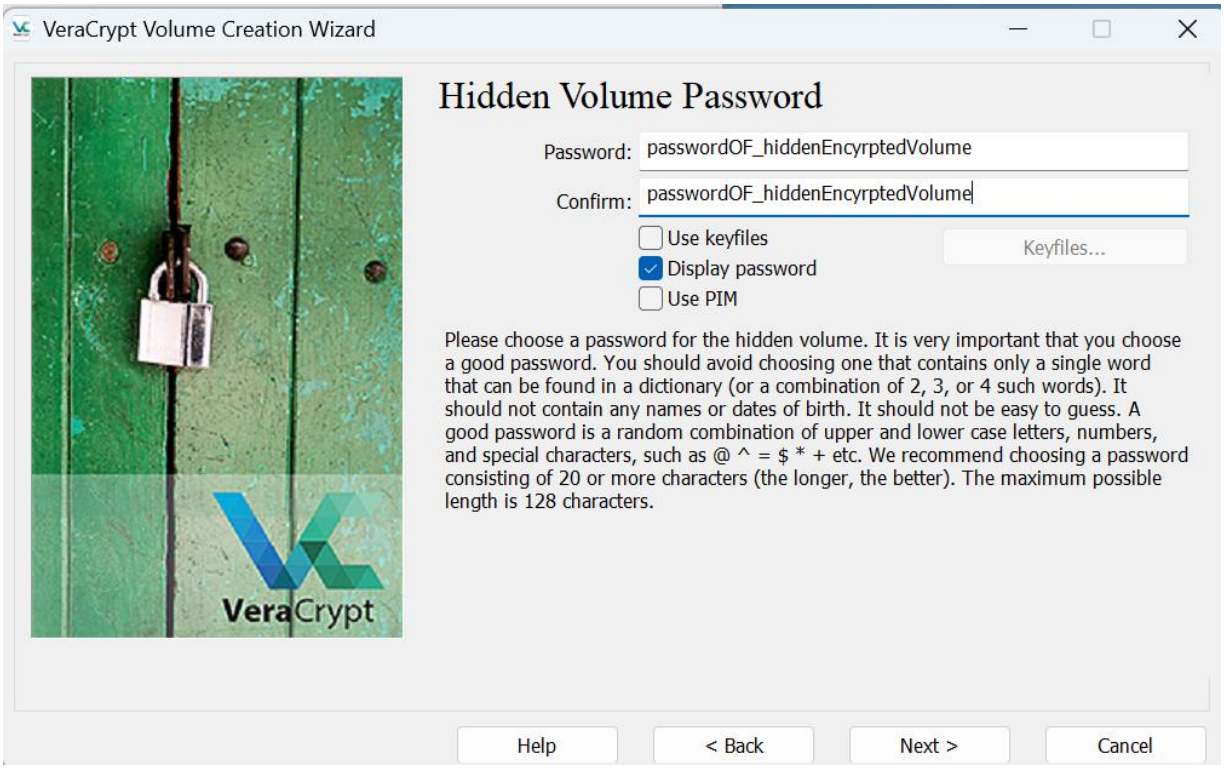

VeraCrypt Volume Creation Wizard
Outer Volume Format
Options
Filesystem FAT
Cluster Default
Full Format
Dynamic
Random Pool: .**/,/,,-,-+*/+*--,/.*,++,/.-*+*...
Header Key: ********************************
Master Key: ********************************
Abort
Done
Speed
Left
Click Format to create the outer volume. For more information, please refer to the documentation.
Randomness Collected From Mouse Movements
VeraCrypt
Help
< Back
Format
Cancel

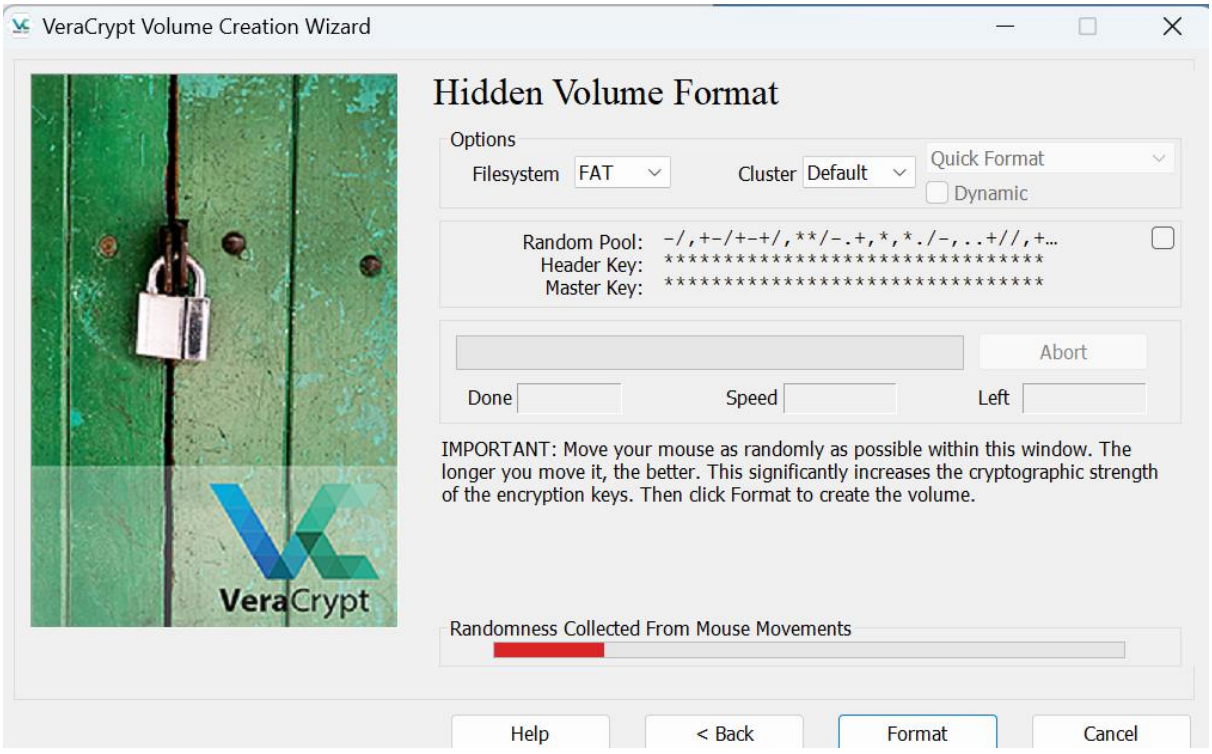

VeraCrypt Volume Creation Wizard
Outer Volume Contents
Outer volume has been successfully created and mounted as drive Z:. To this volume you should now copy some sensitive-looking files that you actually do NOT want to hide. The files will be there for anyone forcing you to disclose your password. You will reveal only the password for this outer volume, not for the hidden one. The files that you really care about will be stored in the hidden volume, which will be created later on. When you finish copying, click Next. Do not dismount the volume.
Note: After you click Next, cluster bitmap of the outer volume will be scanned to determine the size of uninterrupted area of free space whose end is aligned with the end of the volume. This area will accommodate the hidden volume, so it will limit its maximum possible size. Cluster bitmap scanning ensures that no data on the outer volume are overwritten by the hidden volume.
VeraCrypt
Open Outer Volume
Help
< Back
Next >
Cancel
Empty NO Evidence
Local Disk (Z:)
This PC
Local Disk (Z:)
New
Sort
View
Attachments
Documents
Pictures
Desktop
Downloads
Name
Date modified

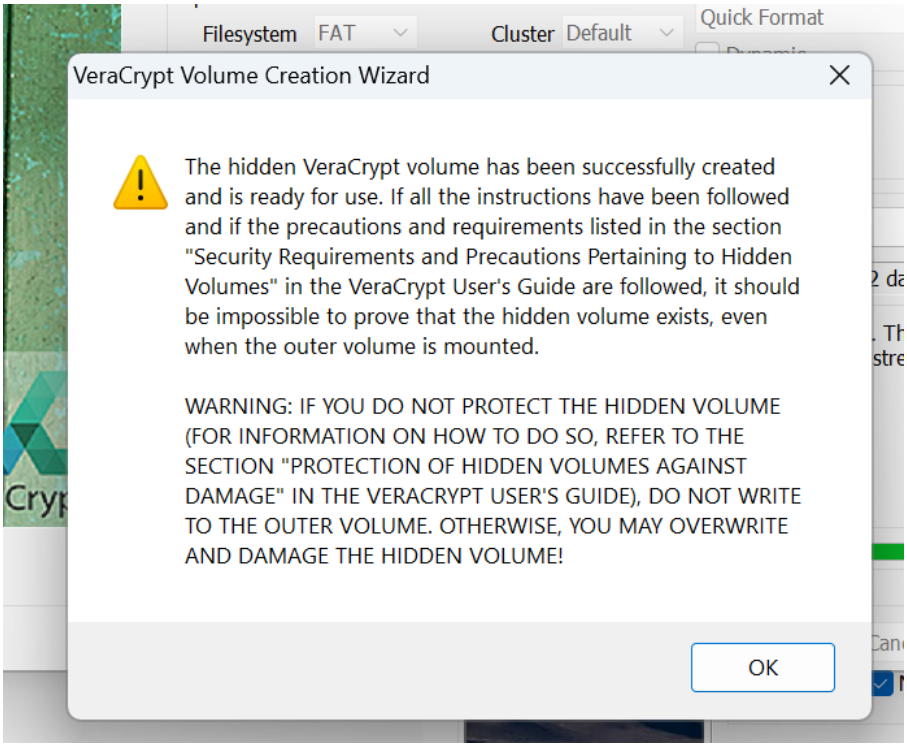

VeraCrypt Volume Creation Wizard
Hidden Volume
The volume cluster bitmap has been scanned and the maximum possible size of the hidden volume has been determined. In the next steps you will set the options, the size, and the password for the hidden volume.
VeraCrypt
Help
< Back
Next >
Cancel

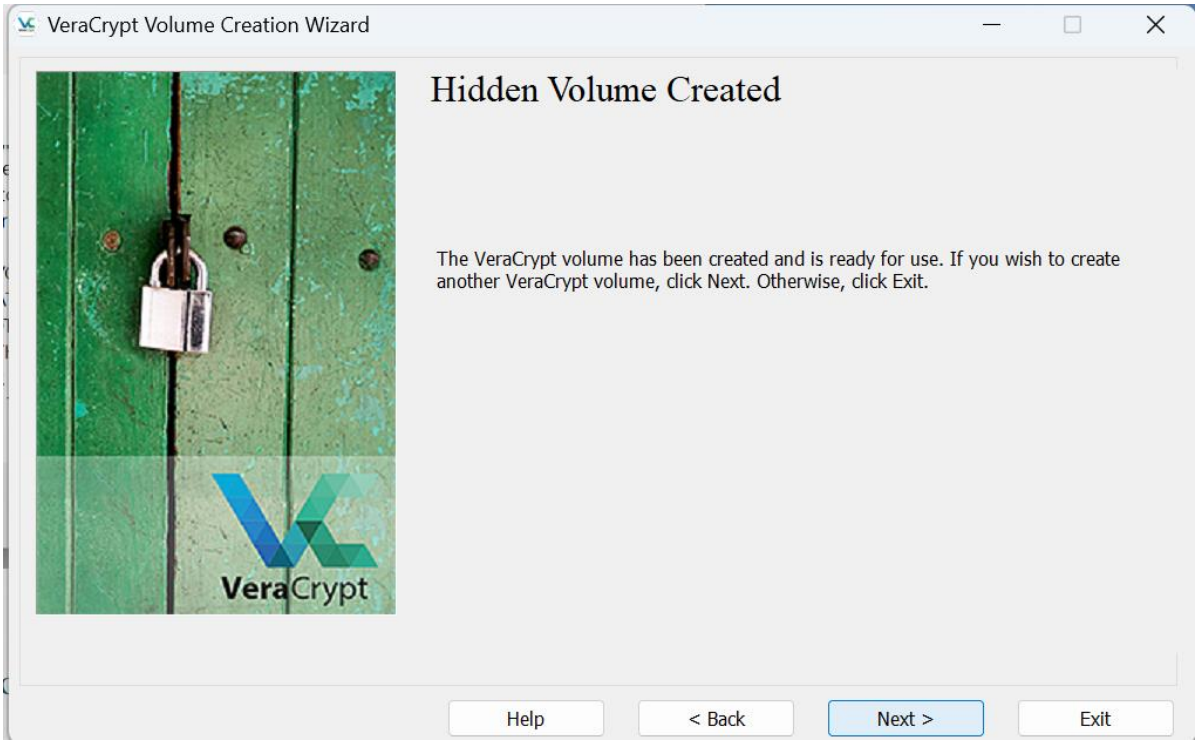

VeraCrypt Volume Creation Wizard
Hidden Volume Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
SHA-256
Information on hash algorithms
VeraCrypt
Help
< Back
Next >
Cancel

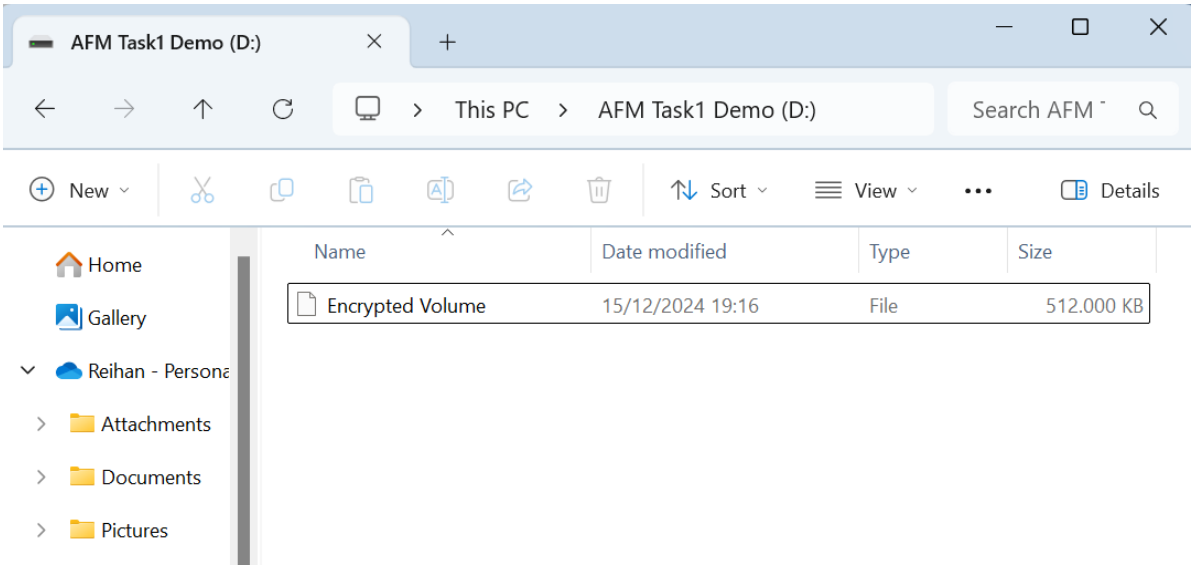

VeraCrypt Volume Creation Wizard
Hidden Volume Size
50
KB
MB
GB
TB
Maximum possible hidden volume size for this volume is 495.26 MiB.
Please specify the size of the hidden volume to create. The minimum possible size of a hidden volume is 40 KiB (or 3664 KiB if it is formatted as NTFS). The maximum possible size you can specify for the hidden volume is displayed above.
VeraCrypt
Help
< Back
Next >
Cancel

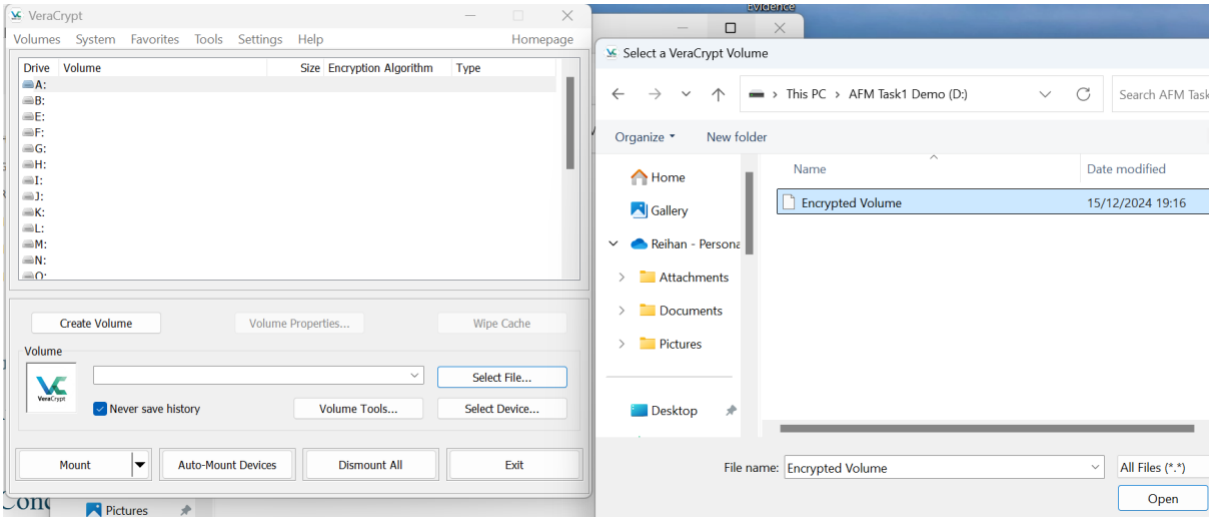

VeraCrypt Volume Creation Wizard
Hidden Volume Password
Password:
passwordOF_hiddenEncyrptedVolume
Confirm:
passwordOF_hiddenEncyrptedVolume
Use keyfiles
Keyfiles...
Display password
Use PIM
Please choose a password for the hidden volume. It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.
VeraCrypt
Help
< Back
Next >
Cancel

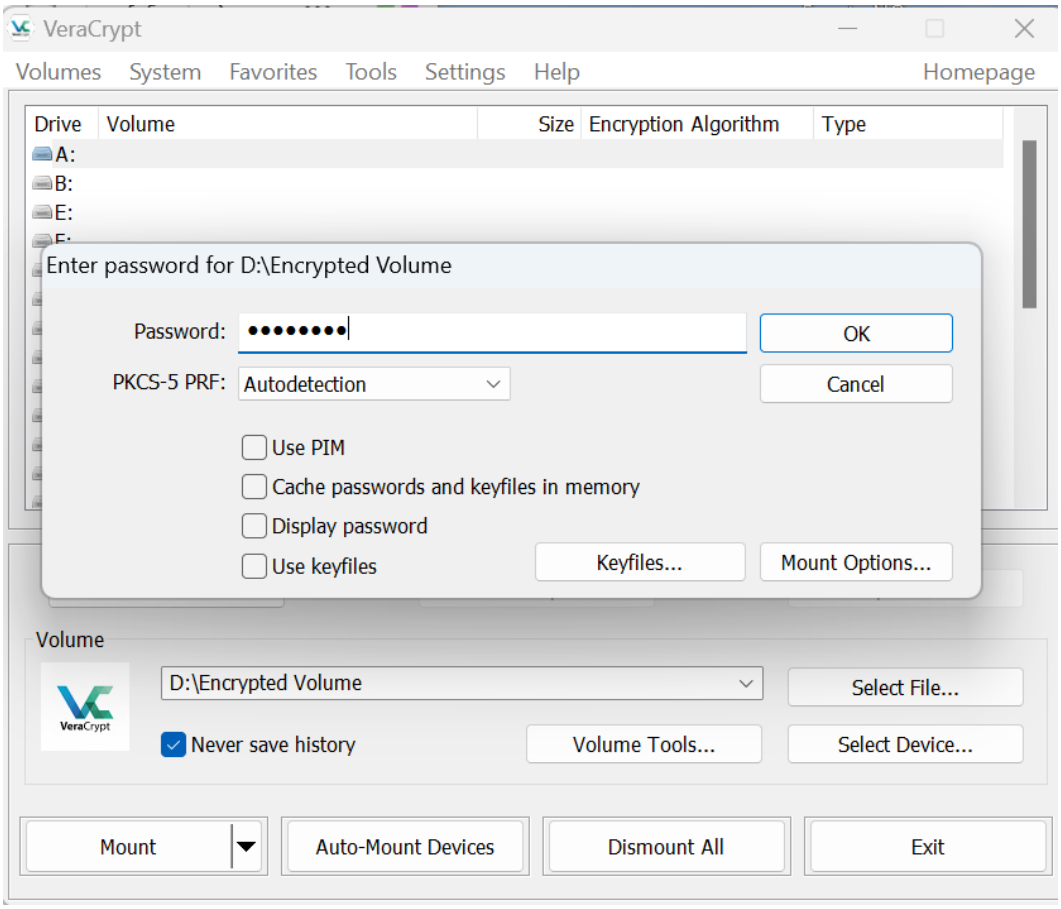

VeraCrypt Volume Creation Wizard
Hidden Volume Format
Options
Filesystem
FAT
Cluster
Default
Quick Format
Dynamic
Random Pool:
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Randomness Collected From Mouse Movements
VeraCrypt
Help
< Back
Format
Cancel

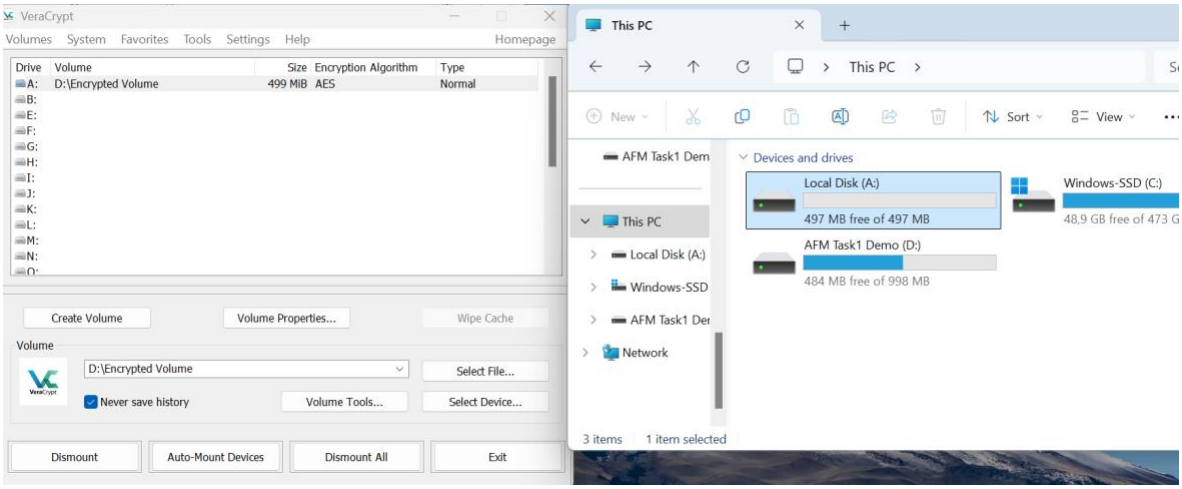

Filesystem FAT
Cluster Default
Quick Format
VeraCrypt Volume Creation Wizard
The hidden VeraCrypt volume has been successfully created and is ready for use. If all the instructions have been followed and if the precautions and requirements listed in the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the VeraCrypt User's Guide are followed, it should be impossible to prove that the hidden volume exists, even when the outer volume is mounted.
WARNING: IF YOU DO NOT PROTECT THE HIDDEN VOLUME (FOR INFORMATION ON HOW TO DO SO, REFER TO THE SECTION "PROTECTION OF HIDDEN VOLUMES AGAINST DAMAGE" IN THE VERACRYPT USER'S GUIDE), DO NOT WRITE TO THE OUTER VOLUME. OTHERWISE, YOU MAY OVERWRITE AND DAMAGE THE HIDDEN VOLUME!
OK

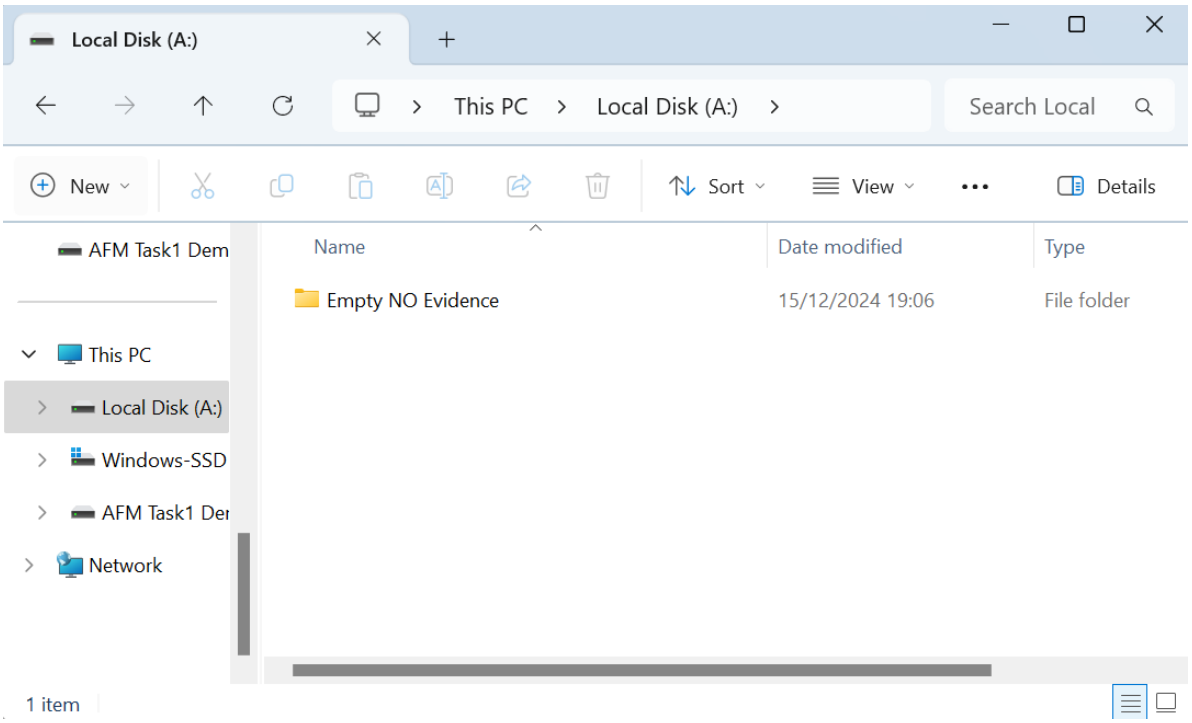

VeraCrypt Volume Creation Wizard
Hidden Volume Created
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.
VeraCrypt
Help
< Back
Next >
Exit

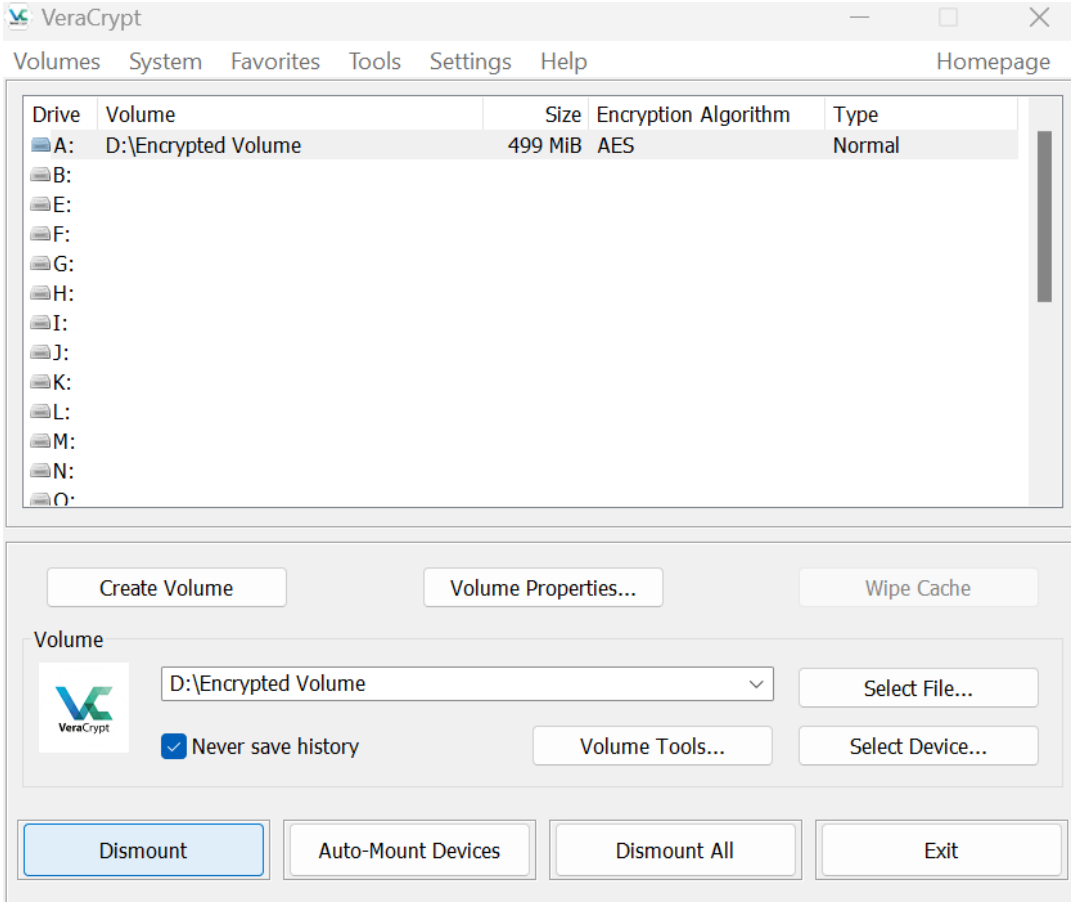

AFM Task1 Demo (D:)
This PC
AFM Task1 Demo (D:)
Search AFM
New
Sort
View
Details
Home
Gallery
Reihan - Persona
Attachments
Documents
Pictures
Name
Date modified
Type
Size
Encrypted Volume
15/12/2024 19:16
File
512.000 KB

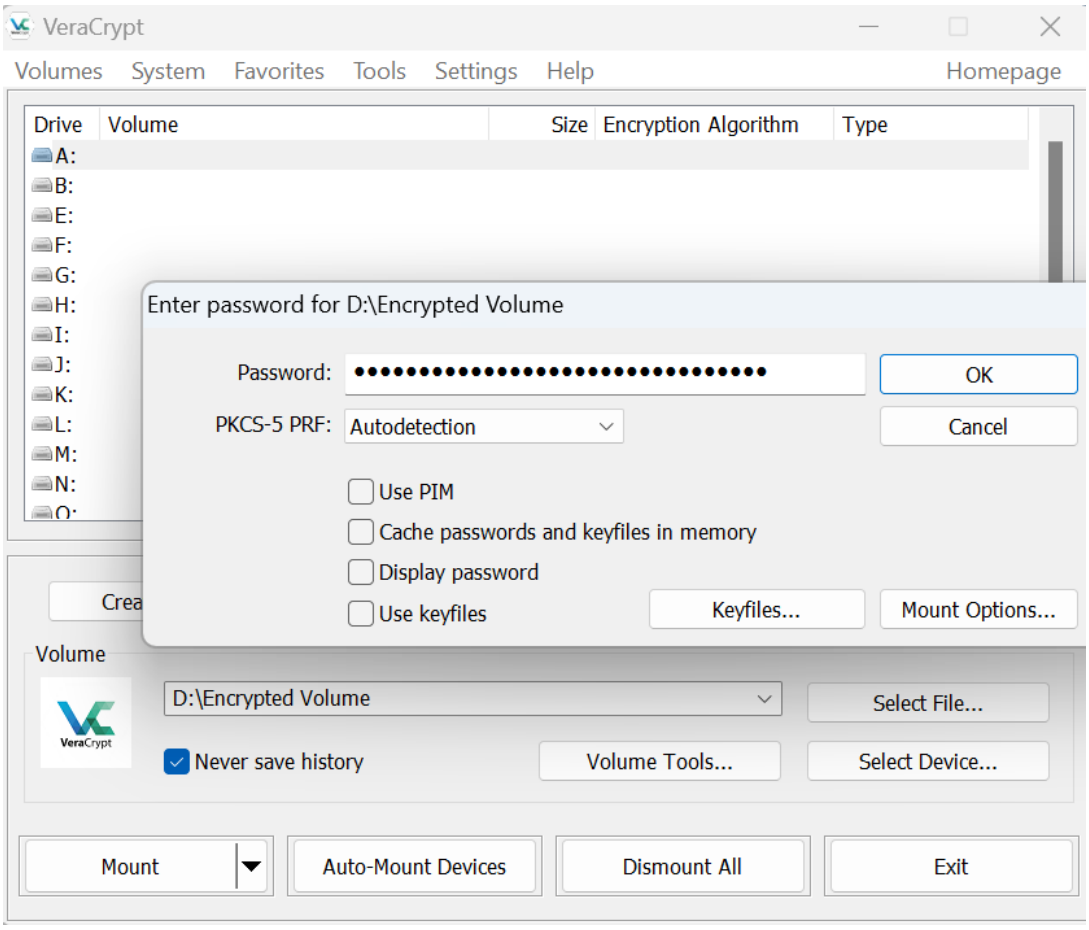

VeraCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
Select a VeraCrypt Volume
This PC
AFM Task1 Demo (D:)
Search AFM Task
Organize
New folder
Home
Gallery
Reihan - Persona
Attachments
Documents
Pictures
Desktop
Name
Date modified
Encrypted Volume
15/12/2024 19:16
File name:
Encrypted Volume
All Files (*.*)
Open

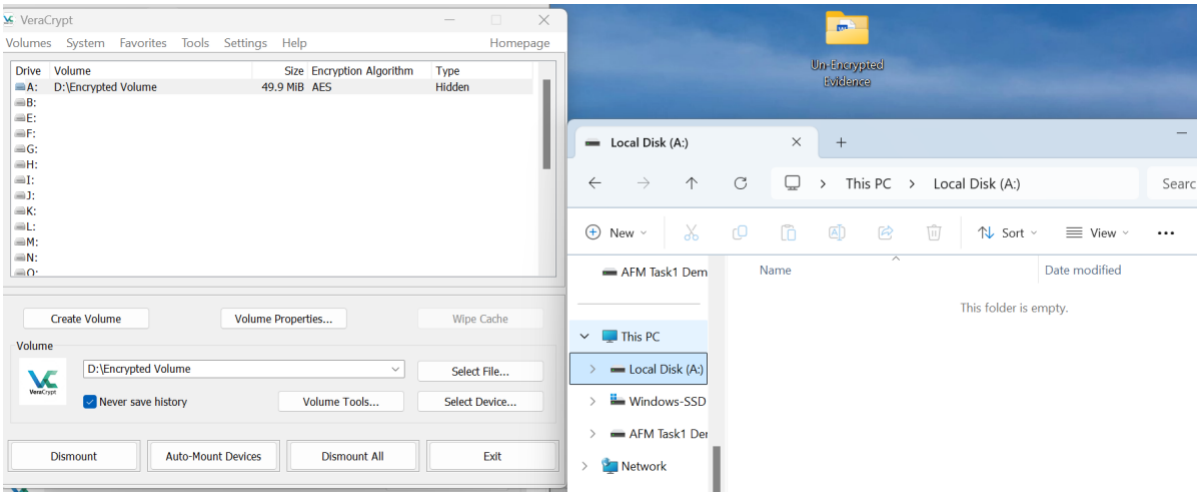

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
E:
Enter password for D:\Encrypted Volume
Password:
OK
PKCS-5 PRF: Autodetection
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

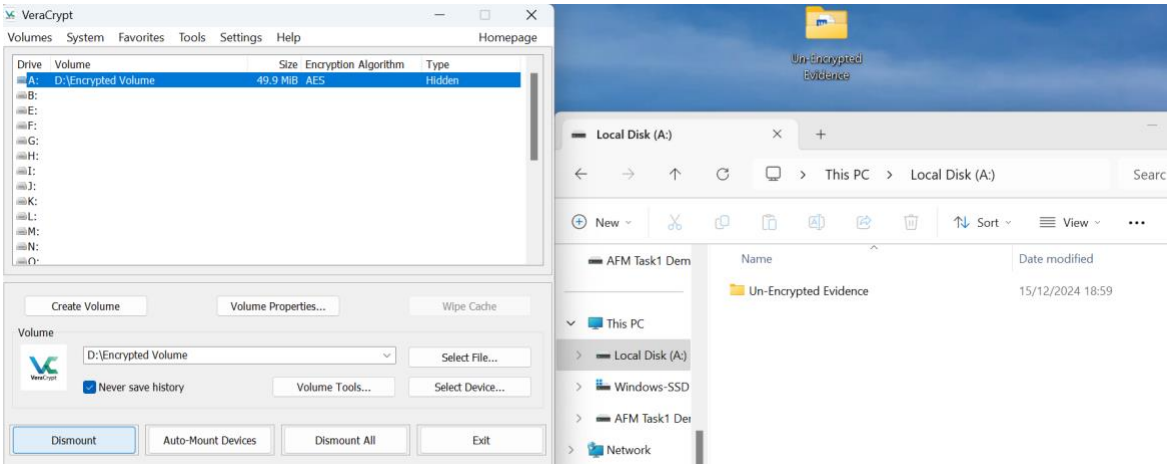

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 499 MiB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
This PC
Devices and drives
Local Disk (A:)
497 MB free of 497 MB
Windows-SSD (C:)
48,9 GB free of 473 G
AFM Task1 Demo (D:)
484 MB free of 998 MB
Network
3 items
1 item selected

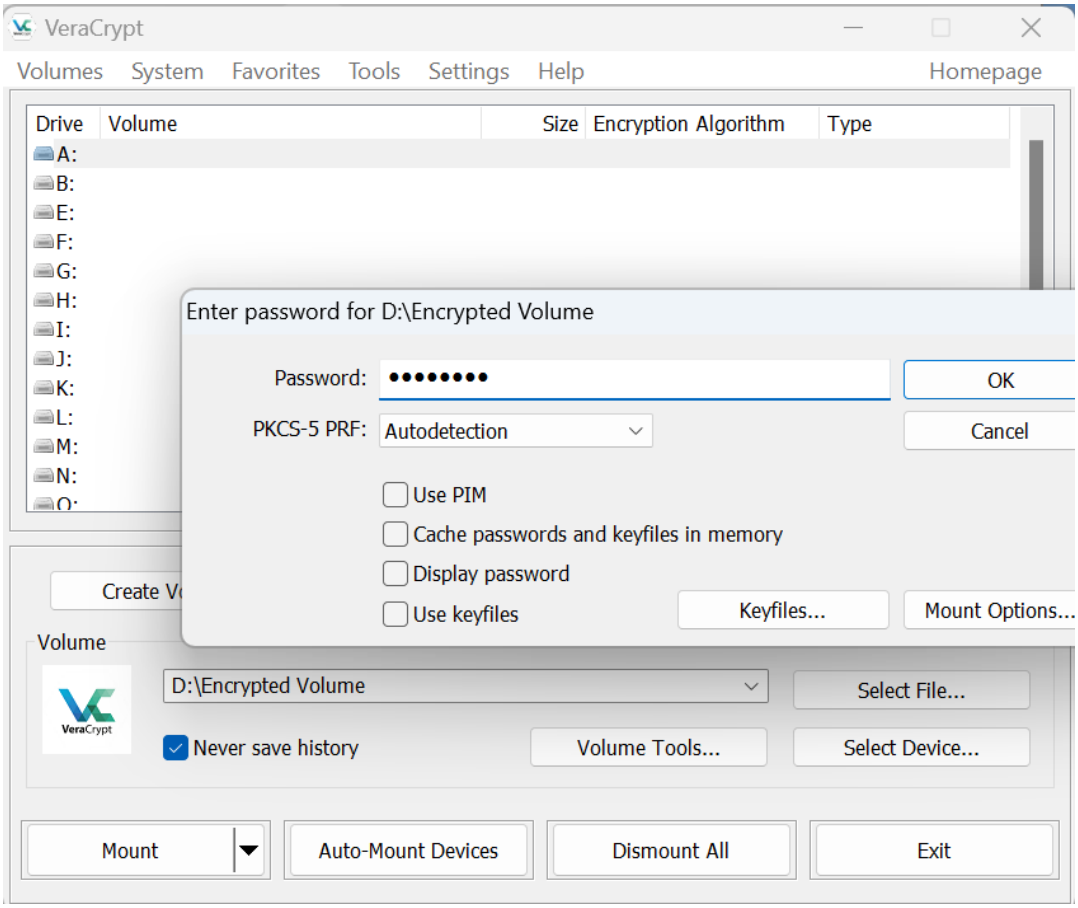

Local Disk (A:)
This PC
Local Disk (A:)
Search Local
New
Sort
View
Details
AFM Task1 Dem
Name
Date modified
Type
Empty NO Evidence
15/12/2024 19:06
File folder
This PC
Local Disk (A:)
Windows-SSD
AFM Task1 Der
Network
1 item

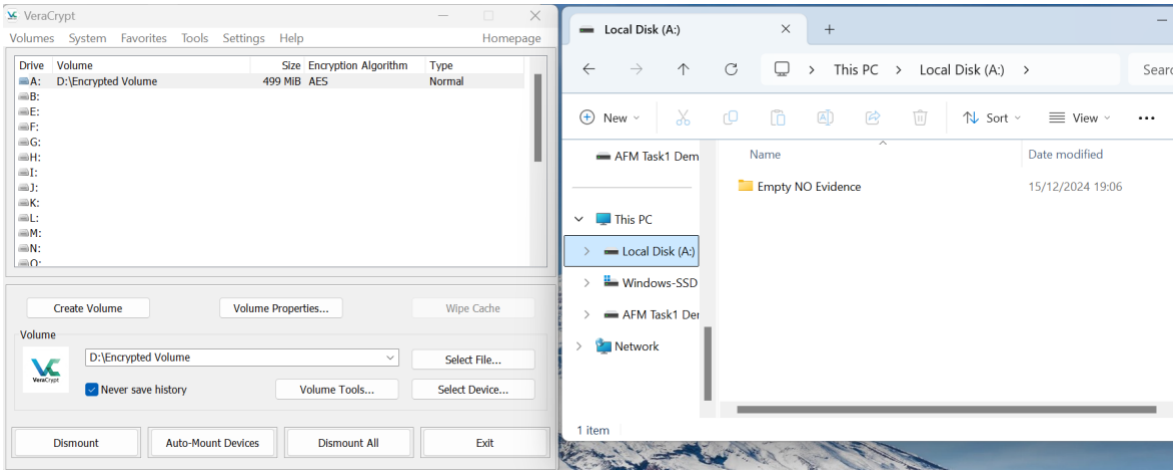

VeraCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
A:
D:\Encrypted Volume
499 MiB
AES
Normal
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

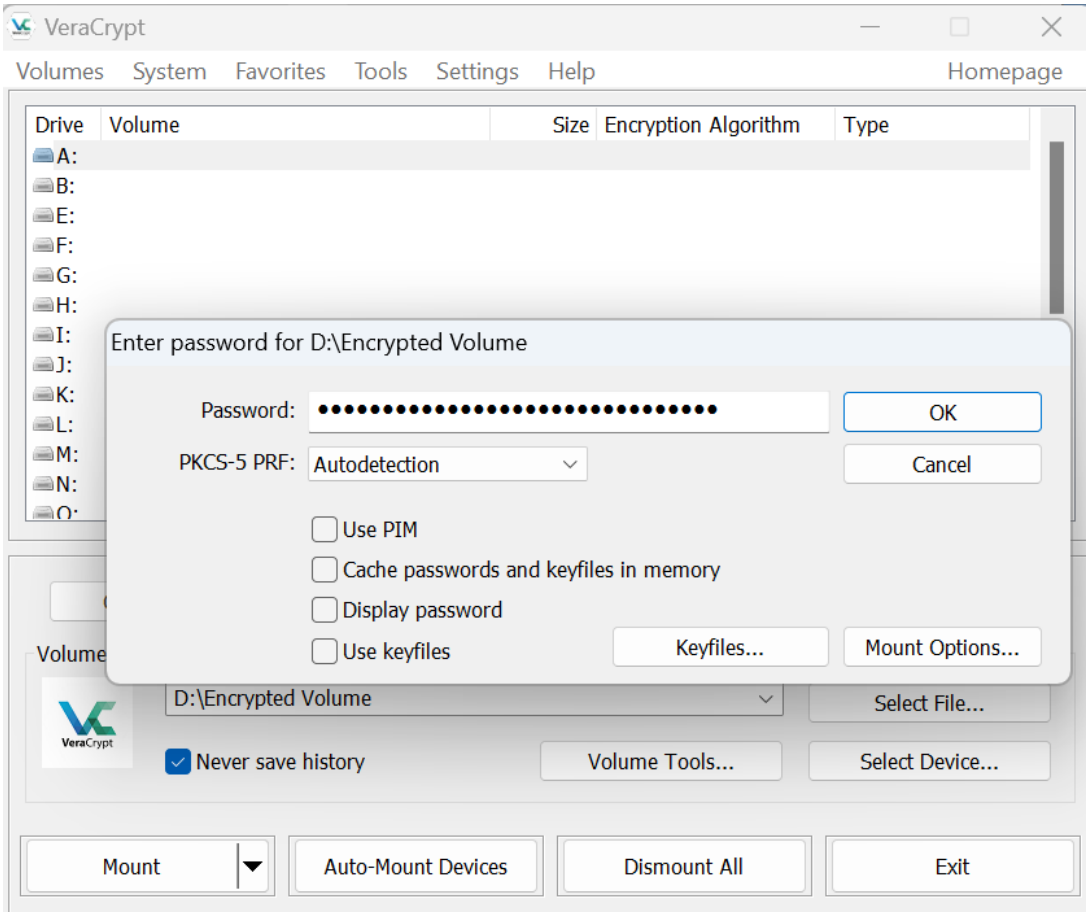

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Enter password for D:\Encrypted Volume
Password:
OK
PKCS-5 PRF: Autodetection
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

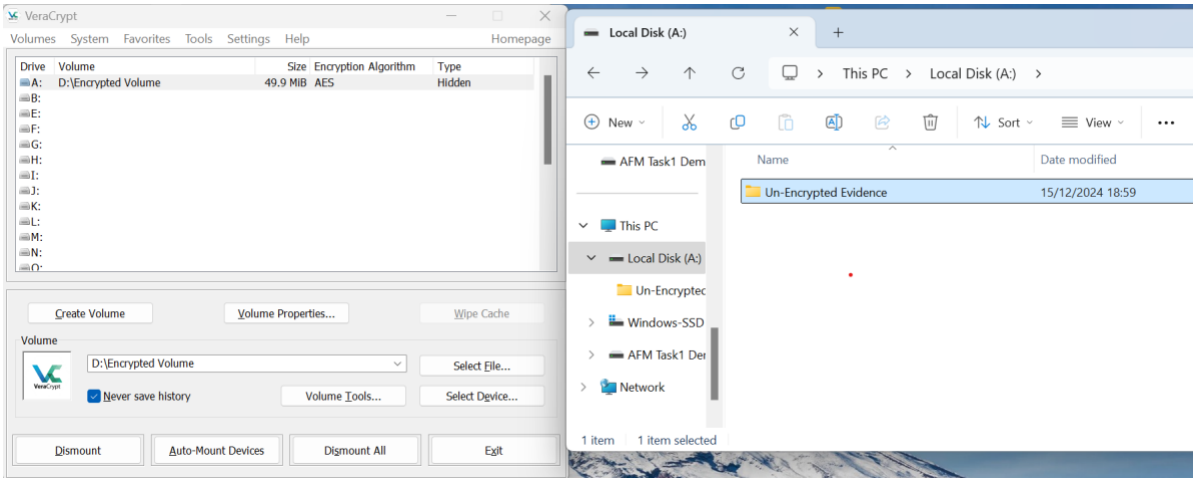

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 49.9 MiB AES Hidden
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Un-Encrypted Evidence
Local Disk (A:)
This PC
Local Disk (A:)
New
Sort
View
Name
Date modified
This folder is empty.
This PC
Local Disk (A:)
Windows-SSD
Network

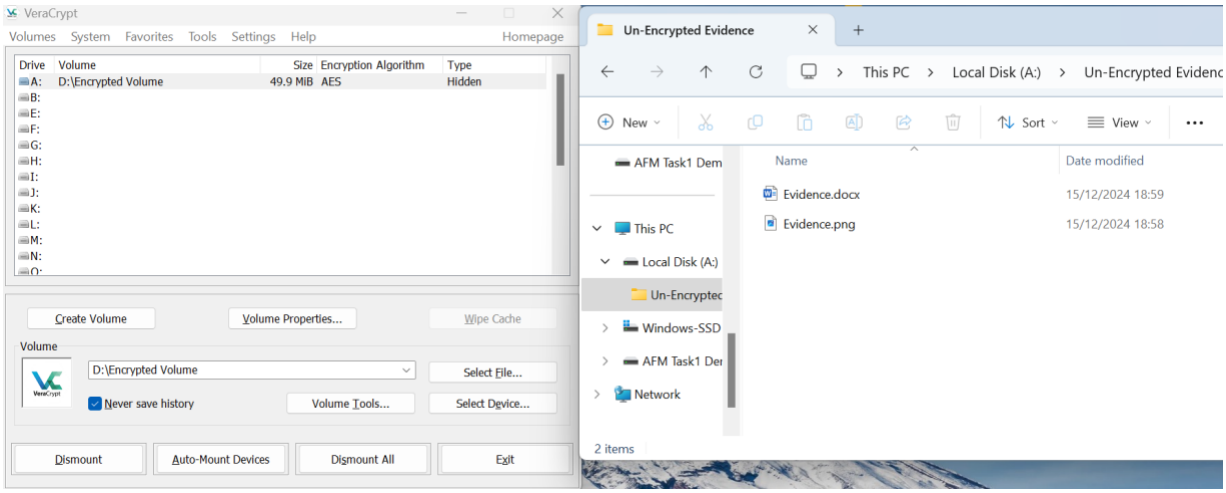

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 49.9 MiB AES Hidden
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Un-Encrypted Evidence
Local Disk (A:)
This PC
Local Disk (A:)
New
Sort
View
Name
Date modified
Un-Encrypted Evidence
15/12/2024 18:59
Windows-SSD
Network


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
Enter password for D:\Encrypted Volume
Password:
OK
PKCS-5 PRF: Autodetection
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

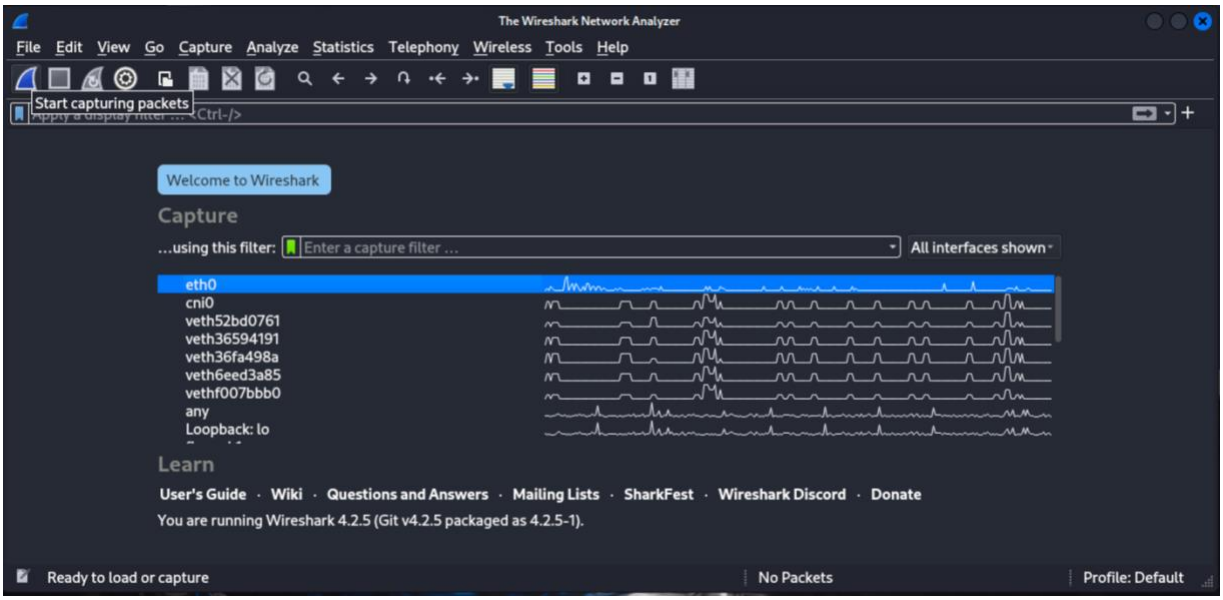

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 499 MiB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Local Disk (A:)
This PC › Local Disk (A:)
New
Sort
View
AFM Task1 Dem
Name
Date modified
Empty NO Evidence
15/12/2024 19:06
This PC
Local Disk (A:)
Windows-SSD
AFM Task1 Der
Network
1 item

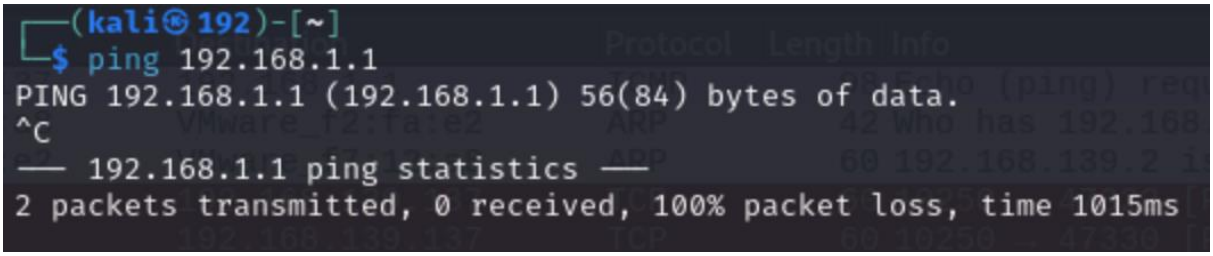

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Enter password for D:\Encrypted Volume
Password:
OK
PKCS-5 PRF: Autodetection
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 49.9 MiB AES Hidden
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Local Disk (A:)
This PC › Local Disk (A:) ›
New
Sort
View
AFM Task1 Dem
Name
Date modified
Un-Encrypted Evidence
15/12/2024 18:59
This PC
Local Disk (A:)
Un-Encryptec
Windows-SSD
AFM Task1 Der
Network
1 item
1 item selected


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: D:\Encrypted Volume 49.9 MiB AES Hidden
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\Encrypted Volume
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Un-Encrypted Evidence
This PC › Local Disk (A:) › Un-Encrypted Evidenc
New
Sort
View
AFM Task1 Dem
Name
Date modified
Evidence.docx
15/12/2024 18:59
Evidence.png
15/12/2024 18:58
This PC
Local Disk (A:)
Un-Encryptec
Windows-SSD
AFM Task1 Der
Network
2 items

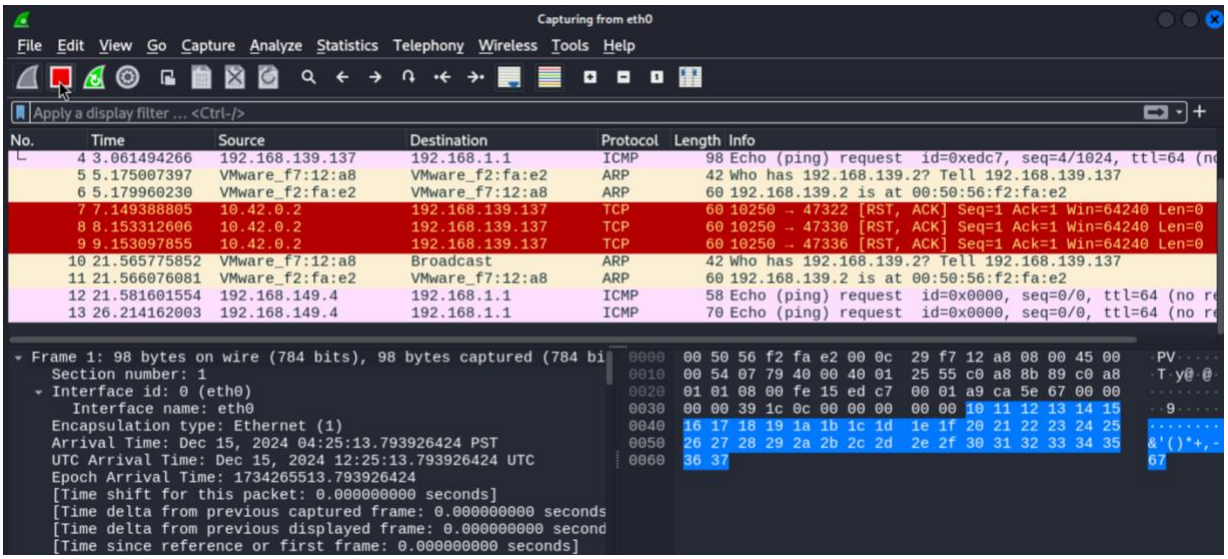
5.3 Scapy (IP Spoofing) - Trail Obfuscation

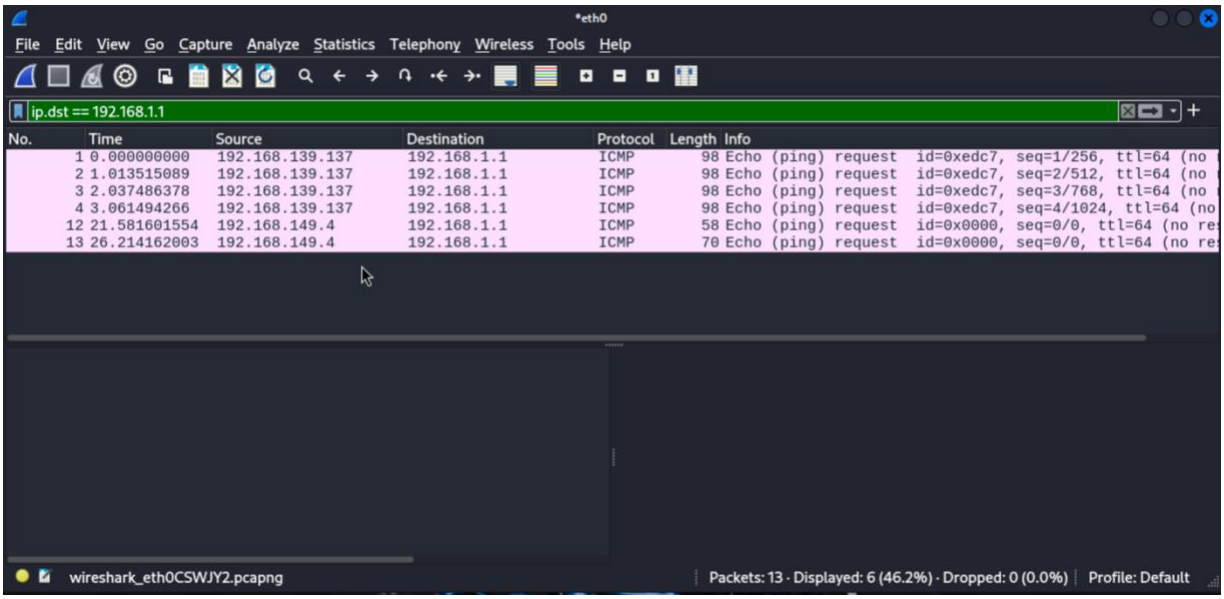


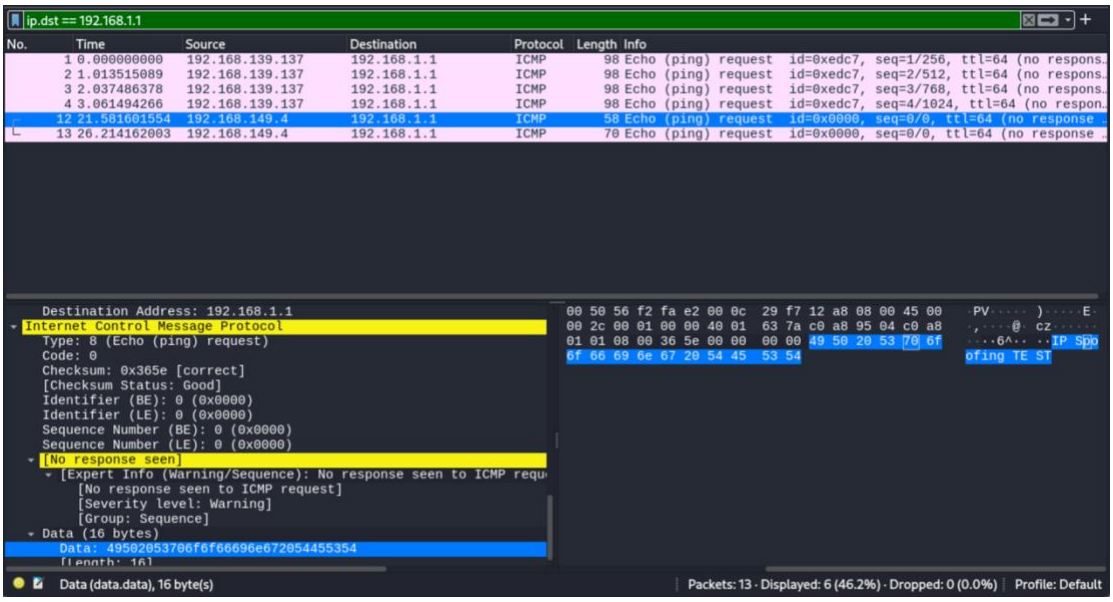


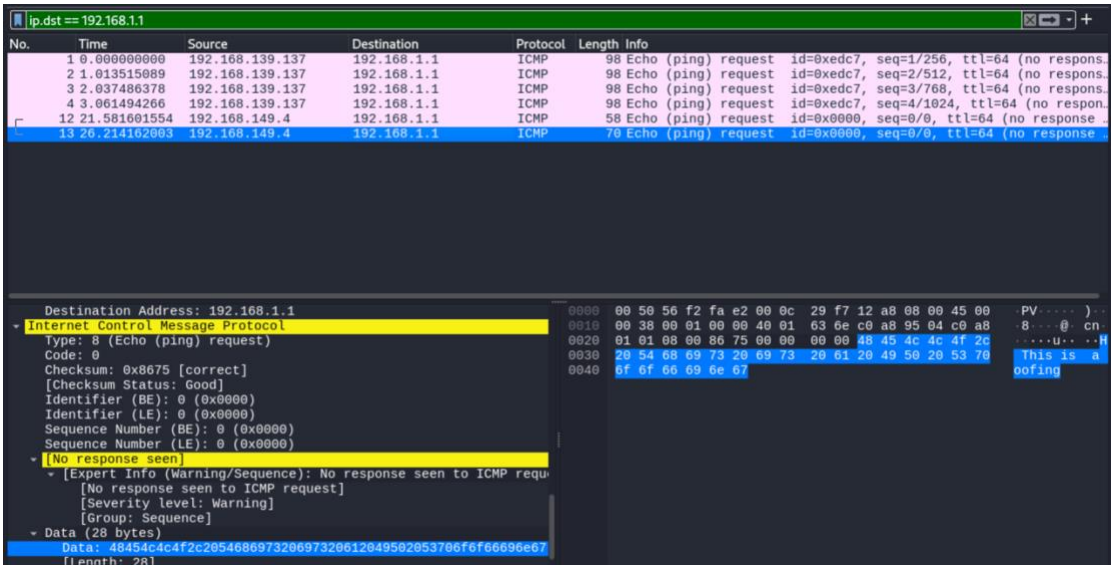
```
┌──(kali㉿192)-[~]
└─$ sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.5.0+git20240324.2b58b51
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft me if you can.
       scccccp///pSP///p          p//Y   |                 -- IPv6 layer
      sY//////////y  caa           S//P   |
       cayCyayP//Ya                pY/Ya
        sY/PsY////YCc             aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                       using IPython 8.20.0
>>>
```

```
>>> send(IP(src="192.168.149.4",dst="192.168.1.1")/ICMP()/"IP Spoofing TEST")
.
Sent 1 packets.
>>> send(IP(src="192.168.149.4",dst="192.168.1.1")/ICMP()/"HELLO, This is a IP Spoofing")
.
Sent 1 packets.
>>> exit
```

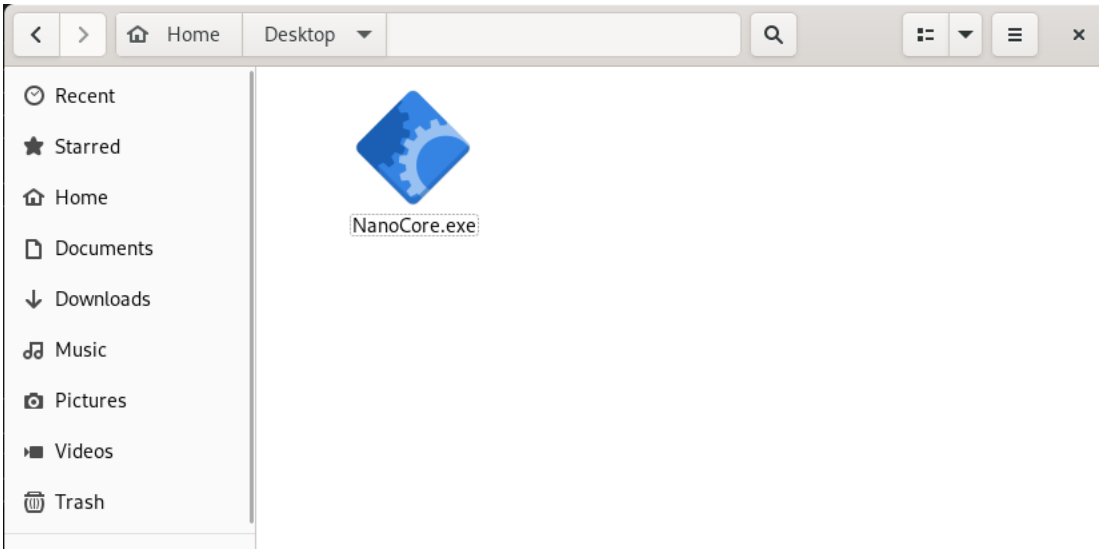



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 192.168.1.1
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=1/256, ttl=64 (no
2 1.013515089 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=2/512, ttl=64 (no
3 2.037486378 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=3/768, ttl=64 (no
4 3.061494266 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=4/1024, ttl=64 (no
12 21.581601554 192.168.149.4 192.168.1.1 ICMP 58 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no re
13 26.214162003 192.168.149.4 192.168.1.1 ICMP 70 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no re
wireshark_eth0CSWJY2.pcapng
Packets: 13 · Displayed: 6 (46.2%) · Dropped: 0 (0.0%)
Profile: Default


ip.dst == 192.168.1.1
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=1/256, ttl=64 (no respons
2 1.013515089 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=2/512, ttl=64 (no respons
3 2.037486378 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=3/768, ttl=64 (no respons
4 3.061494266 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=4/1024, ttl=64 (no respon
12 21.581601554 192.168.149.4 192.168.1.1 ICMP 58 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response
13 26.214162003 192.168.149.4 192.168.1.1 ICMP 70 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response
Destination Address: 192.168.1.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x365e [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP requ
[No response seen to ICMP request]
[Severity level: Warning]
[Group: Sequence]
Data (16 bytes)
Data: 49502053706f6f66696e672054455354
00 50 56 f2 fa e2 00 0c 29 f7 12 a8 08 00 45 00
00 2c 00 01 00 00 40 01 63 7a c0 a8 95 04 c0 a8
01 01 08 00 36 5e 00 00 00 00 49 50 20 53 70 6f
6f 66 69 6e 67 20 54 45 53 54
Data (data.data), 16 byte(s)
Packets: 13 · Displayed: 6 (46.2%) · Dropped: 0 (0.0%)
Profile: Default


ip.dst == 192.168.1.1
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=1/256, ttl=64 (no respons
2 1.013515089 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=2/512, ttl=64 (no respons
3 2.037486378 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=3/768, ttl=64 (no respons
4 3.061494266 192.168.139.137 192.168.1.1 ICMP 98 Echo (ping) request id=0xedc7, seq=4/1024, ttl=64 (no respon
12 21.581601554 192.168.149.4 192.168.1.1 ICMP 58 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response
13 26.214162003 192.168.149.4 192.168.1.1 ICMP 70 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response
Destination Address: 192.168.1.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x8675 [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP requ
[No response seen to ICMP request]
[Severity level: Warning]
[Group: Sequence]
Data (28 bytes)
Data: 48454c4c4f2c20546869732069732061204950205370f6f66696e67
[Length: 28]
0000 00 50 56 f2 fa e2 00 0c 29 f7 12 a8 08 00 45 00
0010 00 38 00 01 00 00 40 01 63 6e c0 a8 95 04 c0 a8
0020 01 01 08 00 86 75 00 00 00 00 48 45 4c 4c 4f 2c
0030 20 54 68 69 73 20 69 73 20 61 20 49 50 20 53 70
0040 6f 6f 66 69 6e 67

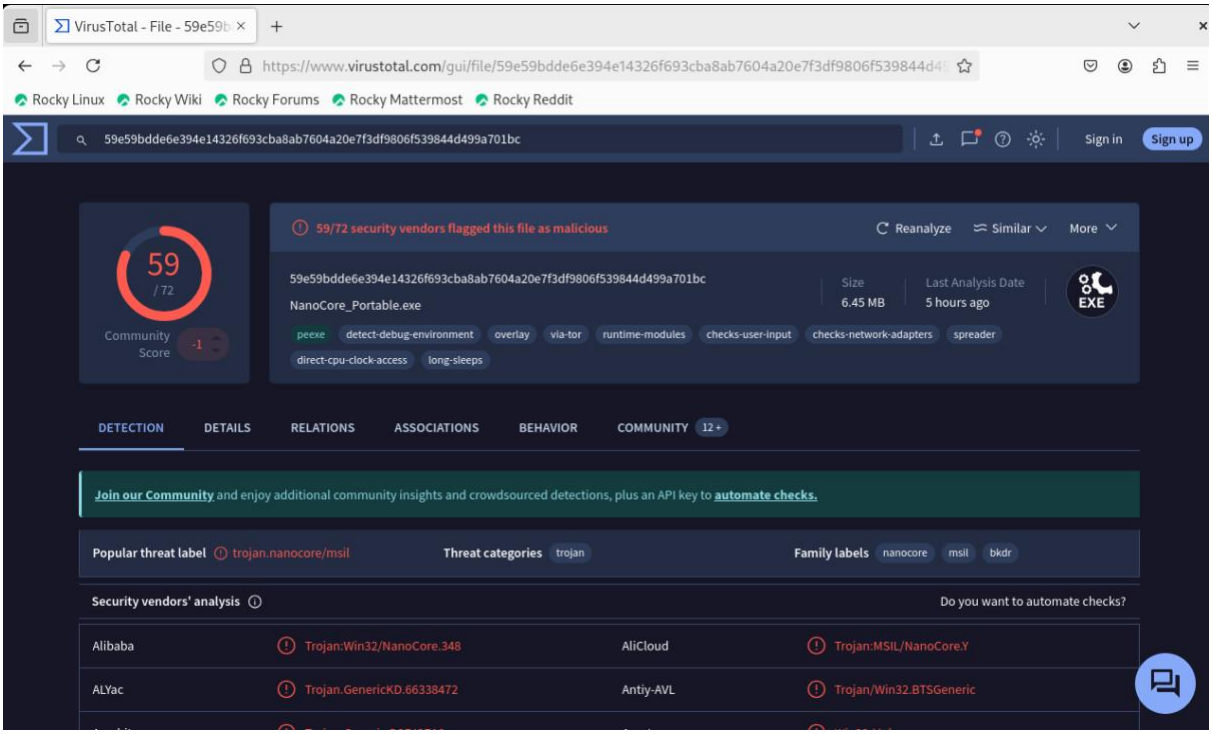
5.4 UPX (Program Packers) - Attack Against Forensic Tools

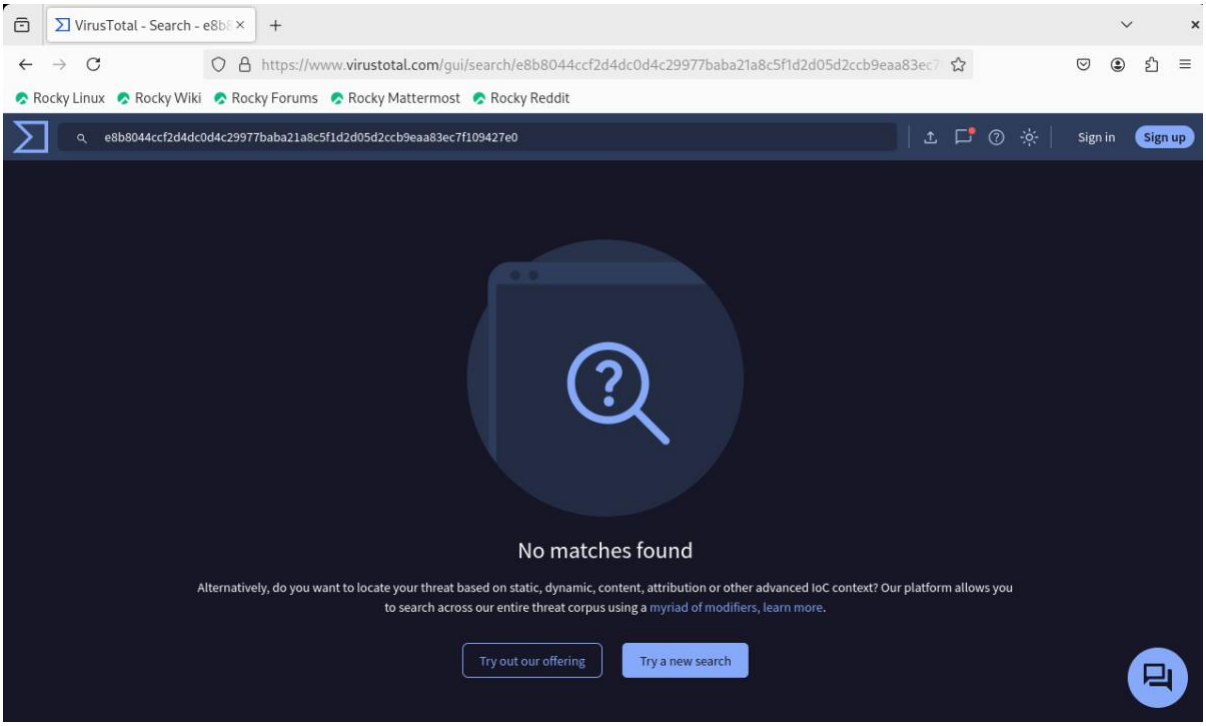



```
[ReihanSNA@server Desktop]$ sha256sum NanoCore.exe
59e59bdde6e394e14326f693cba8ab7604a20e7f3df9806f539844d499a701bc  NanoCore.exe
```

```
[ReihanSNA@server Desktop]$ upx -9 NanoCore.exe -o NanoCore_witUPX.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.4       Markus Oberhumer, Laszlo Molnar & John Reiser    May 9th 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   6759129 ->   6661337   98.55%    win32/pe     NanoCore_witUPX.exe

Packed 1 file.
```

```
[ReihanSNA@server Desktop]$ sha256sum NanoCore*.*
59e59bdde6e394e14326f693cba8ab7604a20e7f3df9806f539844d499a701bc  NanoCore.exe
e8b8044ccf2d4dc0d4c29977baba21a8c5f1d2d05d2ccb9eaa83ec7f109427e0  NanoCore_witUPX.exe
```


VirusTotal - File - 59e59b
https://www.virustotal.com/gui/file/59e59bdde6e394e14326f693cba8ab7604a20e7f3df9806f539844d4
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
59e59bdde6e394e14326f693cba8ab7604a20e7f3df9806f539844d499a701bc
Sign in
Sign up
59
/ 72
Community Score
-1
59/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
59e59bdde6e394e14326f693cba8ab7604a20e7f3df9806f539844d499a701bc
NanoCore_Portable.exe
Size
6.45 MB
Last Analysis Date
5 hours ago
EXE
peexe
detect-debug-environment
overlay
via-tor
runtime-modules
checks-user-input
checks-network-adapters
spreader
direct-cpu-clock-access
long-sleeps
DETECTION
DETAILS
RELATIONS
ASSOCIATIONS
BEHAVIOR
COMMUNITY 12+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.nanocore/msil
Threat categories trojan
Family labels nanocore msil bkdr
Security vendors' analysis
Do you want to automate checks?
Alibaba
Trojan:Win32/NanoCore.348
AliCloud
Trojan:MSIL/NanoCore.Y
ALYac
Trojan.GenericKD.66338472
Antiy-AVL
Trojan/Win32.BTSGeneric


VirusTotal - Search - e8b8
https://www.virustotal.com/gui/search/e8b8044ccf2d4dc0d4c29977baba21a8c5f1d2d05d2ccb9eaa83ec7
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
e8b8044ccf2d4dc0d4c29977baba21a8c5f1d2d05d2ccb9eaa83ec7f109427e0
Sign in
Sign up
No matches found
Alternatively, do you want to locate your threat based on static, dynamic, content, attribution or other advanced IoC context? Our platform allows you to search across our entire threat corpus using a myriad of modifiers, learn more.
Try out our offering
Try a new search

6.0 References

ArcherHall. (2024, July 9). *Understanding Anti-Forensics Methods - ArcherHall*. https://archerhall.com/primers/anti-forensics/

Badman, A., & Forrest, A. (2024, August 20). What is digital forensics? *IBM*. https://www.ibm.com/topics/digital-forensics#:~:text=Digital%20forensics%20is%20the%20process%20of%20collecting%20and,can%20also%20help%20with%20criminal%20and%20civil%20investigations.

Bischoff, P., & Bischoff, P. (2023, October 2). *Best Disk Encryption Software – the 5 top tools to secure your data*. Comparitech. https://www.comparitech.com/blog/information-security/disk-encryption-software/

CCleaner. (n.d.). *CCleaner Official website*. https://www.ccleaner.com/

CGSecurity. (2023, May 21). *Digital picture and file recovery*. CGSecurity. https://www.cgsecurity.org/wiki/PhotoRec

Cluley, G. (2015, May 7). *USBKill - how to turn a USB stick into a kill switch that can force a computer to destroy what you were doing*. Bitdefender. https://www.bitdefender.com/en-us/blog/hotforsecurity/usbkill-how-to-turn-a-usb-stick-into-a-kill-switch-that-can-force-a-computer-to-destroy-what-you-were-doing

Corrons, L. (2024, July 23). *What is a zip bomb and how does it work?* Norton. https://us.norton.com/blog/malware/zip-bomb

Cryptopedia Staff. (2023, October 3). *UNISWAP (UNI): a Decentralized Crypto exchange*. Gemini. https://www.gemini.com/cryptopedia/uniswap-decentralized-exchange-crypto-defi#section-uniswap-101

Daisy, & Galasso, E. (2024, November 27). *Does formatting a drive erase everything? yes or no?* EaseUS. https://www.easeus.com/resource/does-formatting-drive-erase-everything.html#:~:text=The%20answer%20is%20no.%20Formatting%20does%20not%20erase,hard%20drive%20without%20losing%20data%20in%20Windows%2010.

Ebuehi, A. (2024, October 7). *Top 5 Anonymous Cryptocurrencies | Best privacy Cryptos in 2024*. AZCryptoExchanges.com. https://www.azcryptoexchanges.com/guides/best-anonymous-cryptos/#:~:text=Below%2C%20we%20list%20the%20top%20five%20privacy%20coins

%2C,key%20features%2C%20market%20cap%2C%20and%20other%20relevant%20information.

Ec-Council. (2023, November 2). *Five Anti-Forensic techniques used to cover digital footprints*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/anti-forensic-techniques-used-to-cover-digital-footprints/

Ec-Council. (2024, August 20). *What is Digital Forensics*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/

Enaholo, O. (2024, August 29). *Best Anonymous Crypto exchanges*. CoinJournal. https://coinjournal.net/compare/best-anonymous-cryptocurrency-exchanges/#:~:text=Our%20Top%208%20Best%20Anonymous%20Crypto%20Exchanges%20Without,%E2%80%93%20Best%20Decentralized%20P2P%20Marketplace%20. . .%20More%20items

Eraser. (n.d.). *Secure Erase Files from Hard Drives*. https://eraser.heidi.ie/

GeeksforGeeks. (2023, January 27). *Anti forensics*. GeeksforGeeks. https://www.geeksforgeeks.org/anti-forensics/

GeeksforGeeks. (2024, August 7). *What is Reverse Engineering Technique in Cybersecurity?* GeeksforGeeks. https://www.geeksforgeeks.org/what-is-reverse-engineering-technique-in-cybersecurity/

George, R. (2024, October 30). *21 Hard drive data destruction methods: shredding, degaussing. . .* IT Asset Management Group. https://www.itamg.com/data-storage/hard-drive/destruction-methods/

Hephaest0s. (n.d.). *GitHub - hephaest0s/usbkill: « usbkill » is an anti-forensic kill-switch that waits for a change on your USB ports and then immediately shuts down your computer.* GitHub. https://github.com/hephaest0s/usbkill

Horton, V. (2024, May 30). *Anti-Forensics: What it is, Examples and How to Defend Against it*. IT Governance Blog En. https://www.itgovernance.eu/blog/en/anti-forensics-what-it-is-examples-and-how-to-defend-against-it

Jetico. (n.d.). *Wipe Files with BCWipe*. https://www.jetico.com/data-wiping/wipe-files-bcwipe

Kaspersky. (2021, October 26). *Full disk encryption (FDE)*. https://encyclopedia.kaspersky.com/glossary/full-disk-encryption-fde/

Kejriwal, S. (2023, October 23). *Is Monero Anonymous? How Untraceable is XMR?* Coin Bureau. https://coinbureau.com/analysis/is-monero-anonymous/#monero-vs.-other-networks

Khaliq, W. (2024, December 12). *7 Top No KYC crypto exchanges in 2025*. Coin Bureau. https://coinbureau.com/analysis/no-kyc-crypto-exchange/

MONERO. (n.d.). *Merchants & exchanges*. getmonero.org, the Monero Project. https://www.getmonero.org/community/merchants/

Odintsova, S., & Maiorova, M. (2024, December 13). *Best Crypto P2P exchange for safe and simple trades 2024*. BeInCrypto. https://beincrypto.com/top-picks/best-p2p-crypto-platforms/

Panhalkar, T. (2020, July 20). *Anti-Forensics techniques: trail obfuscation, artifact wiping, encryption, encrypted network protocols and program packers*. Infosavvy Security and IT Management Training. https://info-savvy.com/anti-forensics-techniques-trail-obfuscation-artifact-wiping-encryption-encrypted-network-protocols-and-program-packers/

ProxyScrape. (2024, June 2). *How Does TOR Hide Your IP Address? A Comprehensive Guide for 2024*. https://proxyscrape.com/blog/does-tor-hide-your-ip

Sheldon, R., Loshin, P., & Cobb, M. (2024, February 7). *encryption*. Search Security. https://www.techtarget.com/searchsecurity/definition/encryption

Simplilearn. (2024, August 13). *What is Steganography? Types, Techniques, Examples & Applications*. Simplilearn.com. https://www.simplilearn.com/what-is-steganography-article

The UPX Team. (n.d.). *UPX: the Ultimate Packer for eXecutables*. https://upx.github.io/

USBKill. (n.d.). *USB Kill devices for pentesting & law-enforcement*. https://usbkill.com/

Vaidya, S. (n.d.). *OpenStego*. https://www.openstego.com/concepts

Vasile, I. (2024, October 25). *17 Best No KYC Crypto Exchanges: Top choices in 2024*. BeInCrypto. https://beincrypto.com/learn/no-kyc-crypto-exchanges/

Vermaak, W. (2021, August 21). *What are Peer-to-Peer (P2P) networks?* CoinMarketCap Academy. https://coinmarketcap.com/academy/article/what-is-peer-to-peer-p2p

Walton, J. (2023, October 19). *Tested: Windows 11 Pro's On-By-Default encryption slows SSDs up to 45%.* Tom's Hardware. https://www.tomshardware.com/news/windows-software-bitlocker-slows-performance