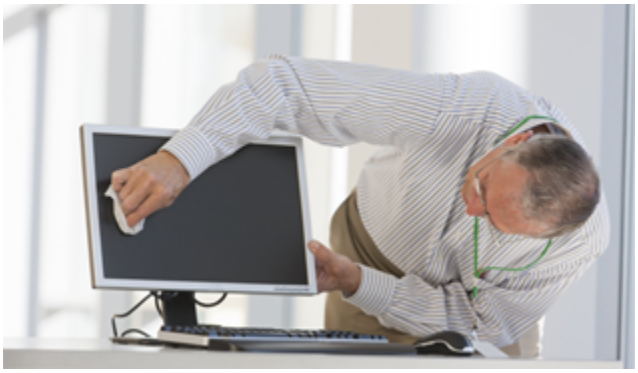
Anti-Forensic Techniques (/en/blog/anti-forensic-techniques)

Posted on 12/02/2014, by Asier Martínez (INCIBE)



Depending on the anti-forensic technique used, we can identify the following classification: 1. Destruction of evidence. - 2. Evidence hiding. - 3. Elimination of the sources of evidence. - 4. Evidence tampering.

1. DESTRUCTION OF EVIDENCE

This method aims to eliminate evidence and make its recovery impossible.

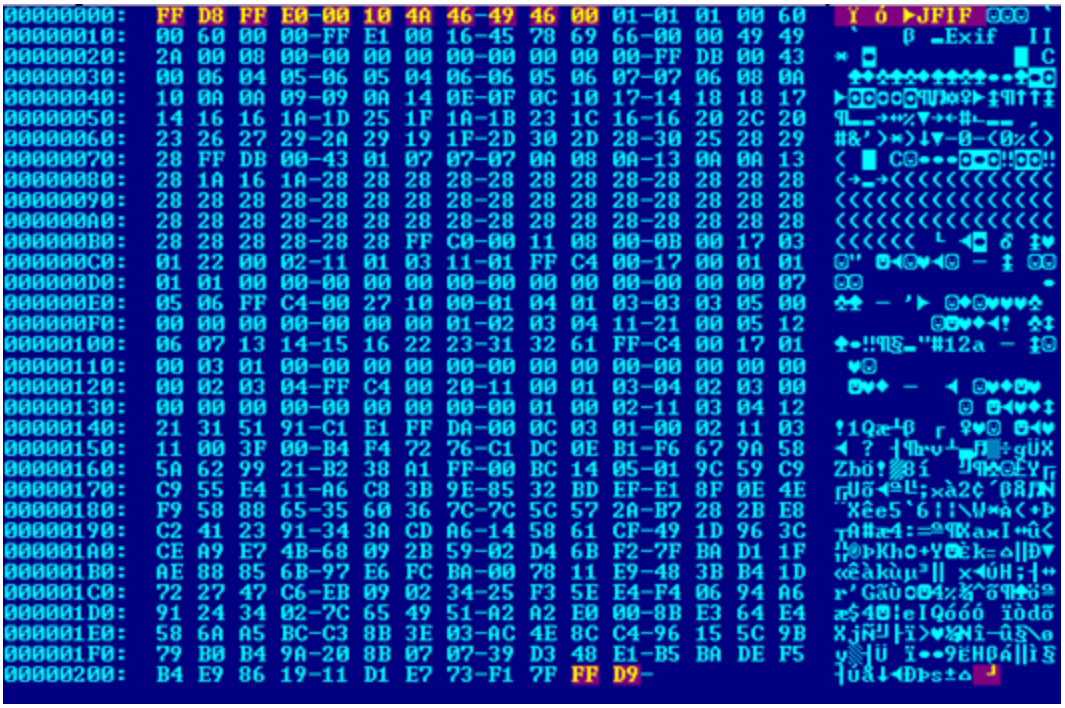
Two strategies can be carried out in order to do this:

- Physical destruction: for example, by using magnetic fields or other less subtle and unconventional methods .
- Logical destruction: by overwriting data or eliminating it.

In order to recover overwritten, damaged or eliminated data, different techniques such as **file carving** or **slack space** are used.

File carving: it is a process that consists in identifying and recovering files by analysing their format characteristics.

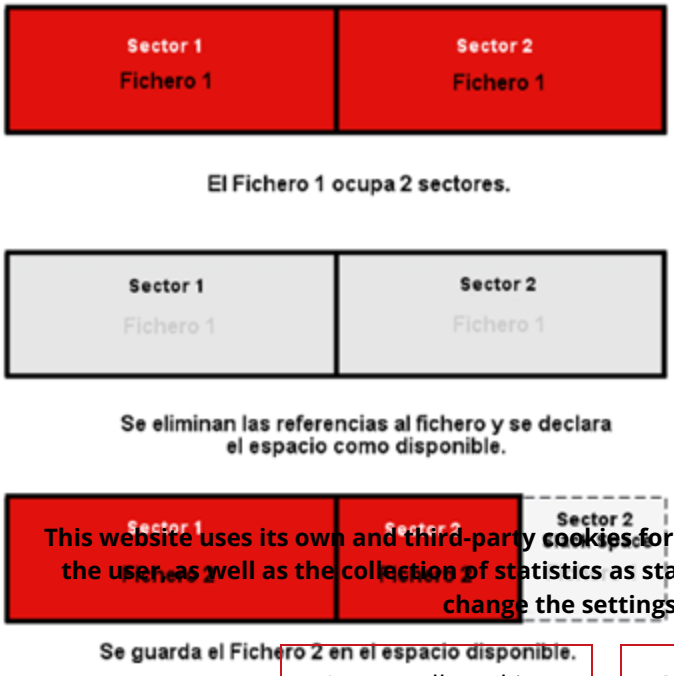
Generally, all kinds of files have common characteristics. For example, if we take a look at their structure, all JPG/JFIF files start in FF D8 FF E0 00 10 4A 46 49 46 00 and end in FF D9, as you can observe in the following image.



Knowing this, blocks that correspond to JPGs can be located within data streams, based on the beginning and ending of their structure.

Slack space: when Windows eliminates a file, in the case of a hard disk drive, it does not really eliminate it. Instead, Windows erases the references to the file. It is like eliminating the index in a book but not the information inside. Besides, it also states that the space occupied by the file is available, so when you save a new file it uses this space.

If the new file occupies a smaller amount of space than the size of the data cluster where it is going to be stored (the smallest allocation unit that is made up of various sectors), the excess space is known as slack space . Slack space holds information corresponding to files that have been previously eliminated, as can be observed in the following image.



Likewise, there are a number of tools that allow the deliberate concealment of information in an unassigned

space, but this information can be recovered via forensic techniques and specialized software.

It must be noted that these types of techniques, both file carving and slack space, are carried out through a slow and costly process in terms of resources, and its efficiency is not ideal.

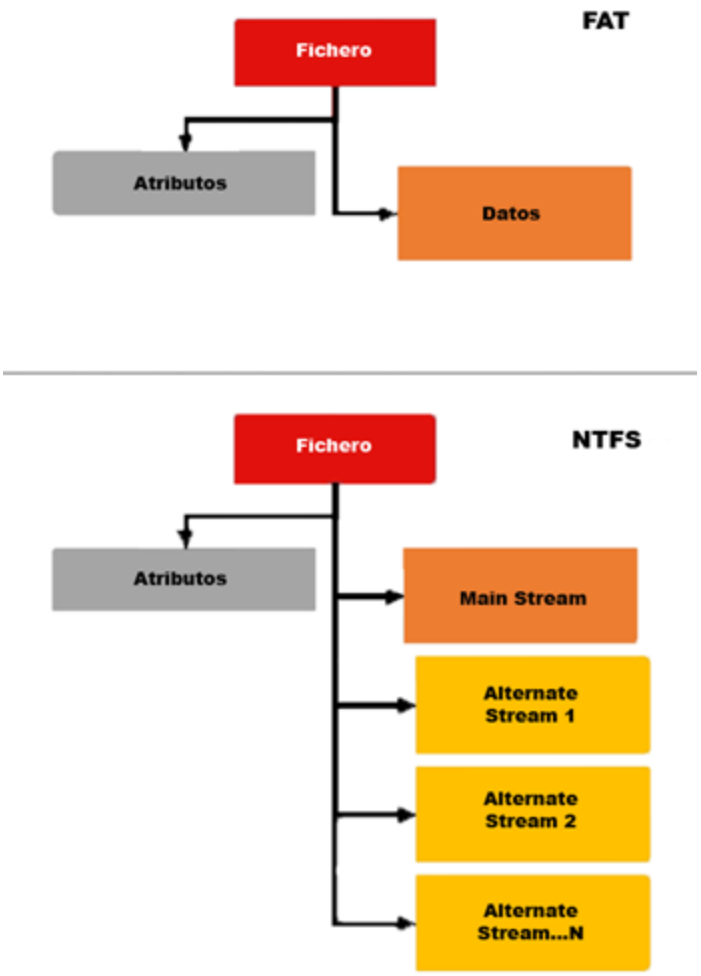
2. EVIDENCE HIDING

This method does not aim to manipulate or destroy evidence but make it as inaccessible as possible. To do so, various techniques can be used such as covert channels or steganography, which enables the concealment and masking of certain information inside another. To detect these kinds of practices, steganalysis tools must be used that search hidden information via complex statistic mechanisms or through searching anomalies in relation to standard formats.

In the following example, corresponding to steganography, both images look exactly the same. However, the second one contains concealed text which says: “Secret message concealed with steghide”.

Imagen Original	
Imagen con texto oculto	

A specific case of covert channels can be found in NTFS filesystem that present a feature known as Alternate Data Streams, through which a file can be concealed inside another, as can be observed in the following image.



This characteristic can be used to hide images in text files without varying their original size or even for camouflaging compressed files inside images. Since Windows Vista, it is possible to view alternate data streams through the /R parameter in the DIR command, but on previous versions specific tools such as ADSCheck or Streams are needed.

It must be noted that the practice of covert channels or steganography can be combined with cryptographic methods with the objective of frustrating the investigation even more.

The use of cryptography as an information protection method has been very important throughout history; from the times of the Caesar cipher, passing on to the Enigma machine , until now, different methods have been used to add a layer of security to the data. The use of cipher tools notably obstructs an investigator's work, who must resort to cryptanalysis methods such as meet in the middle, side-channel attacks or brute-force attacks to be able to view the ciphered content.

Another technique to conceal evidence is rootkits, used mainly by cybercriminals. That is why, when gathering evidence in a forensic analysis, it is mandatory to use a kit for gathering and analysing evidence with utilities that are completely independent from the system's, with the objective of trying to confirm the veracity of the data. Some tools such as Procl or RootkitRevealer enable you to create a list of files using the system's API first and then create another list with its own implemented methods. Once both lists are finished, they are compared and you can see the existence of concealed files.

Another way of detecting rootkits is starting up the system that is thought to be affected with a rootkit from another system (CD-ROM or USB). In this way, the rootkit stays inactive and its detection will be relatively

easy.

3. ELIMINATION OF THE SOURCES OF EVIDENCE

This technique could be considered as the most basic as it simply consists in not leaving traces to conceal a trail and thus avoid being detected. For instance, a simple way to prevent writing to disk may be deactivating the system's logs.

4. EVIDENCE TAMPERING

This method consists in creating false evidence, in order to frustrate the investigator's work. Some of the most typical examples of evidence falsification are:

- Launching attacks from compromised systems, such as Botnets.
- The use of compromised networks.
- The use of compromised user accounts.
- The modification of metadata via utilities such as ExifTool .
- Spoofing messages sent through instant messaging software, such as WhatsApp, or identity theft via SIM card cloning .

Go back

Last Posts

DrDoS cyberattacks based on the ARD protocol (/en/blog/drdos-cyberattacks-based-ard-protocol)

Posted on 07/21/2022, by INCIBE

This post presents some lines of action that should be followed to deal with a DrDoS cyberattack based on the ARD protocol, describing in detail the prevention, identification and response phases to...

White channel and black channel (/en/blog/white-channel-and-black-channel)

Posted on 07/07/2022, by INCIBE

Although the use of black channel is associated with physical safety, it is also part of logical safety. Here we can see how the black channel intervenes in communications, its contribution,...

Machine learning in ICS (/en/blog/machine-learning-ics)

Posted on 06/23/2022, by INCIBE

In recent years, the concept of machine learning has gained more prominence, mainly driven by advances in parallel computing capacity. More and more developments, applications and programs are using...

Threat analysis study: Grandoreiro (/en/blog/threat-analysis-study-grandoreiro)

Posted on 06/02/2022, by INCIBE

Grandoreiro, also known as Delephant, is a banking trojan from South America, which has spread its operations to other regions, especially Europe, including Spain and Portugal. According to ESET...

TCP Middlebox Reflection: new DDoS attack vector (/en/blog/tcp-middlebox-reflection-new-ddos-attack-vector)

Posted on 05/26/2022, by INCIBE

Weaknesses in TCP protocol implementation in middleboxes could provide a means to carry out distributed reflection denial-of-service (DrDoS) attacks against any target.

(https://www.incibe.es/sites/default/files/certificado_sgsi_26102021.pdf) (https://www.incibe.es/sites/default/files/certificado_sgc_08112021.pdf)

More information

Follow us:

(https://twitter.com/incibe_cert) (https://www.youtube.com/user/intecocert)

(https://www.linkedin.com/showcase/incibe-cert)

NIPO: 094-20-022-9