9- Anti- Forensics

A- 9.1 Introduction

Anti-forensics is the practice of attempting to thwart يعيقcomputer forensic analysis,this may include:

- **Encryption.**
- **Over-writing of data to make it unrecoverable.**
- **Modification of files' metadata.**
- **file obfuscation (disguising files تمويه).**

Anti-investigation techniques aim to make the job performed by automated tools very difficult and/or unreliable.

Usually, it is possible to distinguish anti-forensic techniques in specific categories, **the purpose of each technique is to attack one or more steps that will be performed by analysts during their activity (for instance Identification; Acquisition; Analyzing; reporting…….).**

In reality, it is very rare to see anti-forensics tools used correctly and frequently enough to totally obscure either their presence or the presence of the evidence that they were used to hide.

B- 9.2 Anti-forensic categories

These are the general anti-forensic categories, they can be summurized into:

1. **Data Hiding**
2. **Obfuscation التشويش and Encryption**
3. **Data Forgery**
4. **Data Deletion**

5. **Physical Destruction**
6. **Analysis Prevention**
7. **Online Anonymity**

http://resources.infosecinstitute.com/anti-forensics-part-1/

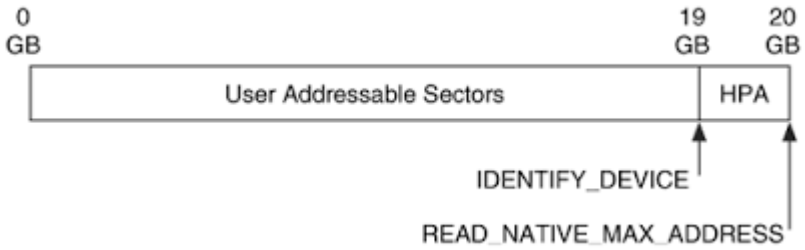
9.2.1 Data Hiding, Obfuscation and Encryption

The great advantage of hiding data is to maintain the availability of these when there is need. Regardless of the operating system, **using the physical disk for data hiding is a widely used technique**, but those related to the OS or the file system in use are quite common. **At this stage, we are going to explain the attack on the first phase of an investigation: "Identification"**.

If evidence cannot be found, in fact, it will be neither analyzed nor reported.

A- *HPA Area* مهمه

The most common technique to hide data at the hardware level is to use the *Host Protected Area* (HPA) of disk. This is generally an area not accessible by the OS and is usually used only for recovery operations. This area is also invisible to certain forensic tools and is **therefore ideal for hiding data that attacker do not want to be found easily.** The following image shows a representation of HPA within a physical media.



B- DCO Area (Device Configuration Overlay).

The use of the **DCO** is another good way to hide potentially incriminating data. **This technique is stealthier than the use of HPA and is also less known.** The following image shows a representation of DCO within a physical media.

The more effective way to detect DCO areas remains the use of ATA command *DEVICE CONFIGURATION IDENTIFY*, which is able to show the real size of a disk. Comparing the output of this command with that resulting from the command **"READ_NATIVE_MAX_ADDRESS"** makes it easy to find any hidden areas. It's also important to note that "*The ATA Forensic Tool*" is also able to find hidden areas of this kind.

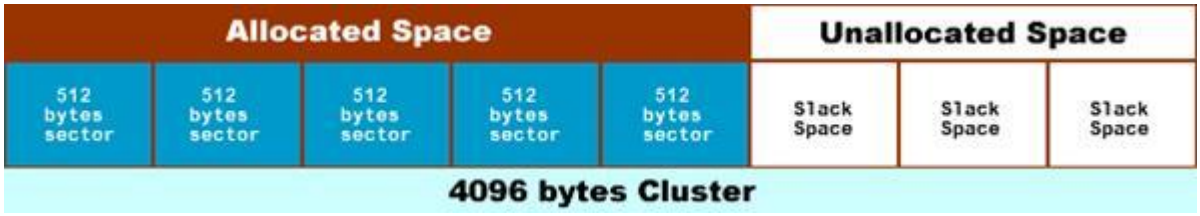
There are three ATA commands involved in creating and using a hidden protected area. The commands are:

- ***IDENTIFY DEVICE***
- ***SET MAX ADDRESS***
- ***READ NATIVE MAX ADDRESS***

C- Use of Slack Space

The "Slack Space" is the unused space between the end of a stored file, and the end of a given data unit, also known as cluster or block. When a file is written into the disk, and it doesn't occupy the entire cluster, the remaining space is called slack space.

The image below shows a graphical representation of how the slack space can appear within a cluster:



The use of this technique is quite widespread, and is more commonly known as "*file slack.*" However, there are many other places to hide data through the "*slack space*" technique, such as the so-called **"*Partition Slack*".**

C- D- Bad Sector مهمة

Another common technique is to mark some fully usable sectors as **"*bad*"** in such a way that these **will no longer be accessible by the OS**. By manipulating file system metadata that identifies "*bad blocks*" **like *$BadClus* in NTFS, it's possible to obtain blocks that will contain hidden data.**

E-Steganography

Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination.

Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone

scanning your data will fail to know it contains encrypted data. The stenographic algorithms aim to keep the "plausible الضاهري" form of data that they are intended to protect, so that no suspicion will be raised regarding actual secret content. The steganographic technique currently most widespread is the Least Significant Bit or LSB. In Digital Image it is based on the fact that a high resolution image is not going to change its overall appearance if we change some minor bits inside it.

For example, consider the 8-bit binary number 11111111 (1 byte): the right-most 1-bit is considered the least significant because it's one that, if changed, has the least effect on the value of this number. therefore, the idea is to break down the binary format of the message and put it on the LSBs of each pixel of the image. Steganography, obviously, may be used with many types of file formats, such as audio, video, binary and text.

Steganography, alone, cannot guarantee the confidentiality of the hidden data, although it remains difficult to go back to an original hidden message without knowing the generation algorithm. **However, if these techniques are associated with cryptographic algorithms, the security level of the hidden message increases significantly, adding also the variable of "plausible deniability" about the information hidden**. It's possible, finally, to mention one of the most widely used software in time to apply steganography: S-Tool. This is software that is already dated, but still effective. However, a lot of software designed for this purpose are available online.

9.2.2 Data Forgery

Data forgery is also a practice aimed to avoiding the identification of incriminating material المواد الجرميه. In addition to changing file extensions, there are other methods that can significantly falsify the true nature of information.

Information hidedin this technique will not be identified & analyzed. The three majour techniques used can be summurized as:

A-Transmogrification تحويل المظهر الخارجى

The easiest way to implement this technique is to modify the header of a file so that it can no longer be associated with any type of file already known.

Obviously, by changing these values, and restoring them only in case of necessity, it is possible to avoid detection of a hypothetical compromising document. This approach is adopted by "Transmogrify," an anti-forensic tool developed by the MAFIA (Metasploit Anti-Forensic Investigation Arsenal). **The technique basically aims to deceive the signature-based scan engine of these tools.**

Many forensic tools for recovering files within the analyzed systems available in forensics marked built to assist investigators avoiding this techniqe.

B-Timestamp Alterations / MACB Scrambling تخليط

The purpose of these activities is to prevent a reliable reconstruction of the operations performed by a user or during the breach of a system.

Usually, these events are reconstructed in a "timeline" primarily through the use of MACB timestamp parameters of the file system, where MACB stands for "Modified, Accessed, Changed, and Birth."

The following is a fast representation of the meaning of MACB broken down by type of file system: غير مطلوب

File System	M	A	C	B
FAT	Written	Accessed	Changed	–
NTFS	Modified	Accessed	MFT Modified	Created
Ext 2/3	Modified	Accessed	Changed	–
Ext 4	Modified	Accessed	Changed	Created
UFS	Modified	Accessed	Changed	–

C-Log Files مهمة

Every computer professional knows of their existence and the ease with which they can be altered. Specifically, in contrast to a forensic analysis, **the log files can be altered in order to insert dummy, misleading or malformed data. Simply, they can also be destroyed**. However, the latter case is not recommended, because a forensic analyst expects to find some data if he goes to look for them in a specific place, and, if he doesn't find them, will immediately think that some manipulation is in place, which of course could also be demonstrated. The best way to deal with log files is to allow the analyst to find what he is looking for, but of course making sure that he will see what we want him to see.

It's good to know that the first thing that a forensic analyst will do if he suspects a log alteration, will be to try to find as many alternative sources as possible, both inside and outside of the analyzed system (backup system). So it is good to pay attention to any log files replicated or redundant.

9.2.3 Data Deletion

The first mission of a forensic examiner is to find as much information as possible (files) relating to a current investigation. **For this purpose, he will do anything to try to recover as many files as possible from among those deleted or fragmented** تجزأ . **However, there are some practices to prevent or hinder this process in a very efficient way**.

A- Wiping

If you want to irreversibly delete your data, you should consider the adoption of this technique. **When we delete a file in our system, the space it formally occupied is in fact marked only as free. The content of this space, however, remains available, and a forensics analyst could still recover it. The technique known as "disk wiping" overwrites this "space" with random data or with the same data for each sector of disk, in such a way that the original data is no longer recoverable.**

" Data wiping" can be performed at software level, with dedicated programs that are able to perform overwriting of entire disks or based on specific areas in relation to individual files.