Chapter 14

Understanding Anti-Forensics Techniques for Combating Digital Security Breaches and Criminal Activity

Ricardo Marques
Pontifícia Universidade Católica de Campinas, Brazil

Alexandre Mota
Pontifícia Universidade Católica de Campinas, Brazil

Lia Mota
Pontifícia Universidade Católica de Campinas, Brazil

ABSTRACT

This chapter deals with the understanding of techniques that are used to create damage to the expert in an investigative process. The name used for these techniques is called anti-forensics, whose mission is to conceal, remove, alter evidence, or make inaccessible a cybercrime. These techniques aim to make the work of the slower expert or difficult to reach a conclusion; however, this chapter will explore some techniques used as measures to subvert digital evidence through anti-forensic measures.

INTRODUCTION

The computer forensics research appears in order to ensure that the evidence of crimes involving computers and network, preserved for presentation in court, constituting convincing aspect in the materiality of an offense. The difficulty in maintaining the integrity of digital evidence emerges as challenge, because they depend on a number of appropriate technical knowledge and use of specific tools for analysis and verification of all traces possibly left by the criminal in devices and networks.

Even as challenges ahead to enable the understanding of new research fronts in digital forensics field, it is also relate, the fields for the study of anti-forensic techniques, consisting of hiding evidence

DOI: 10.4018/978-1-5225-0193-0.ch014

and artifacts; purpose to further restrict access to devices with use of encryption, highlighting progress through techniques of steganography, which become reality as a matter of anti-forensic disciplines. Obviously, to speak of anti-forensic measures this article also address the principles of computer forensics.

Whereas the principles of Forensic Sciences also apply for Computer and Network Engineering, which features some basic processes, such as preservation, preparation, collection, examination, analysis and presentation of all traces and evidence at crime scenes, anti-forensic techniques can appear in any of these steps:

The techniques most used in anti-forensic concept are:

1. Working in networks, VPN's, the botnet or transparent proxy. The tools involved and discussed in this context are public VPN's and open proxy systems.
2. Acting on hard drives, data encryption. The involved and tools discussed in this context are Microsoft Bitlocker and Truecrypt.
3. Acting on hard drives, data wipe techniques in hard drives. Some tools will exhibited in this topic.
4. Acting on hard drives using the physical destruction of hard drives.
5. Acting images, steganography. Some tools will exhibited in this topic.

For techniques that work in networks, fraudsters use is the use of VPN's (Virtual Private Network), use of botnet networks or transparent proxy, so that they are not identified by IP address, because these network resources, create a mechanism to mask network connection outlet for criminal actions.

For data encryption techniques, the expert is faced with an environment where the files to be analyzed have encryption often is not possible to describe or interpret the information. This encryption can see through individual files, batch files, called containers and encrypted entire disks.

For cases involving wipe data on hard drives, the expert has involved a scenario where the hard drive in the investigation undergone several wipe techniques, eliminating the expert's work possibilities will be demonstrate some forms and mechanisms. Cases involving the unallocated disk space, it is an underdeveloped technique, which involves using tools to blind data through disk space slack where the fraudster uses is a dedicated hard disk space by operating systems, which for example in Microsoft systems are defined but not used.

- For cases involving hard drives using the physical destruction of hard drives, where this considered the safest in the fraudster's vision, where recovery becomes virtually impossible in the aspect of recovery of information stored there used in this aspect, drills holes in hard drives, among others.
- For cases involving steganography, the fraudster can hide any file type or codes in pictures, so that it is very hard to see if any kind of information or inserted file. Despite steganography, techniques used to create digital signatures on documents the objectives studied here focused on the use of steganography in order to hide evidence or data.
- For cases involving operating systems, the fraudster can use techniques and tools such as rootkits able to hide or camouflage the traces and remnants so that there are no conditions to investigate the source or origin of a particular fraud or attack, usually makes use of access administrative on the computer for installation.