Chapter 3
Anti-Forensics: The Art of Deceiving and Evading Cybersecurity Analysts

Robert John Mapa Soler
https://orcid.org/0009-0006-2466-5412
Illinois Institute of Technology, USA

ABSTRACT

Today's world has seen rapid advancements in technology. With that comes even more rapid advancements in cybersecurity. And to combat that, criminals and adversaries have also developed even more advanced techniques to combat cybersecurity. Many of these techniques fall under the field of anti-forensics. Digital forensics is the branch of cybersecurity that deals with investigating incidents in cyberspace. So, to hide themselves even more, cybercriminals have come up with very created anti-forensic techniques to evade these investigators and make it harder to prove that they actually committed a crime. This paper highlights published and proven anti-forensic techniques across different devices. It covers the technical details of these techniques, as well as the forensic techniques that they evade. Although many of the techniques in this paper can be used for malicious purposes, forensic investigators should nevertheless know these so that they can continue to perform their jobs effectively despite the rapid growth of techniques that are used against them.

DOI: 10.4018/979-8-3373-0857-9.ch003

I. INTRODUCTION

A. Background and Significance

This is the digital age. Everything makes use of technology. All technology makes use of information. In short, everything we do today relies on information technology. And that includes cybercrime and cyberwarfare.

The field of cybersecurity is like a game of cat and mouse. It's a never-ending cycle of opposing sides getting better than each other. Attackers find a clever way to get past the defenses of systems, then the defenders find a clever solution to prevent that, then the attackers yet again find a more advanced way to hack into those systems, and then the defenders find an even more advanced solution to that problem, and so on and so forth. The same thing happens with forensics and anti-forensics. Investigators have found ways to extract data that should not be extractable by normal means, then people made tools to cleverly hide that information even further so that investigators can't find them, then investigators made their own tools to counter that, and then other people made even more advanced tools that are harder to counter, and so on and so forth. With that being said, it's clear that the field of cybersecurity is only getting more and more advanced.

This paper will focus on two branches of cybersecurity: forensics and anti-forensics. In this context, forensics is the science of retrieving and recovering data from a machine for further purposes. In law and crime, this information can be used as evidence admissible in court (Slonopas, 2024). In cyberwarfare, this information can be used to gain intelligence on the adversary (ADF Solutions, 2023) and even reverse-engineer their own technology.

On the other hand, anti-forensics is the science of evading forensics. Criminals use this to make themselves harder to track and harder to be proven guilty in court. In warfare, militaries use this on their technology to make it harder for their opponents to gain information about them and the technology they use (ADF Solutions, 2023). All this is done in the name of hiding information that would give their opposition an edge against them.

However, anti-forensics has only recently been acknowledged as a legitimate field of study, and because of this, there is a general lack of knowledge on anti-forensics techniques. Therefore, the aim of this paper is to fill that gap and provide knowledge to everyone in the technology sector, especially the people in the field of cybersecurity.

Though it would seem that this paper mostly helps criminals or people trying to hide suspicious information, it is also actually true the other way around. As stated in the previous paragraph, the information in this paper can be used to enlighten cybersecurity professionals as well, so that they may be aware of the possible anti-