

Chapter 2

What Is Cybercrime?

Abstract Computer forensic experts are commonly faced with the misconception that they work primarily on cybercrimes. The reality is quite opposite, namely that digital forensics is of importance in pretty much every possible type of crime ranging from computer intrusions to theft. This chapter provides a discussion on what cybercrime is, from the author's perspective. But more importantly, this chapter gives the reader a presentation on how and in what cases digital evidence can be of use during criminal investigations. The aim of the chapter is to make the reader understand that in the modern world, we leave digital traces almost all the time. We may not always be aware of this fact, but knowing and understanding how digital traces are left behind is of great importance for a computer forensic expert. For instance, even if a criminal is conducting a crime without so much as looking at her phone or computer, chances are that she is using a chat client to talk to some friend about what she did. This action can leave incriminating evidence that can be valuable in court.

Keywords Cybercrime · Digital evidence · Computer aided crime

Before dwelling deeper into forensics it seems reasonable to have a discussion on what signifies cybercrime. Or, maybe more importantly, how and when digital evidence comes in play during criminal investigations. I choose to include this discussion due to the fact that during my work as a forensic examiner, I was often faced with the misconception that my daily work was with cybercrime in the sense of computer hacking and that sort of things. In reality, digital evidence is present in crimes of almost every kind.

To begin this discussion, it is interesting to look at what Rogers wrote back in 2000. He uses the traditional approach of Means, Motive, and Opportunity to discuss cyber criminals. In this discussion Motive is the reason for why someone is committing a crime. Take defrauding for example, the common motive for defrauding someone is to earn money. Means would be the tools used to commit the crime and opportunity could be described as the possibility to commit the crime. One could argue that a crime begins in motive and that the means and opportunity

are mere results of the easiest way to achieve what is wanted as motive. This way of thinking opens up the discussion on cybercrime to not only cover “hard” computer crimes such as hacking, but also to involve any crime that is aided by computers.

This view is further discussed by Rogers (2001), who described different types of computer criminals. On the topic of online fraudsters, he argued that online fraudsters are simply fraudsters that commit their crimes online. The same can be said about criminals that sell drugs online and that are involved in child exploitation crimes, and a wide range of other criminals. They are committing traditional crimes and have traditional motives, but they see the opportunity to commit the crimes from the comfort of their own house, using the Internet. Also, as of today, the means to commit the crimes becomes owning a computer and most people have a computer already.

In a study conducted by Kävrestad (2014), online frauds were examined to model and define the online fraud process. This study made it clear that there is no real difference between online and offline fraudsters, the difference lies in the way that the crime is committed. However, it should not go unnoticed that crimes committed online provide a criminal investigation with opportunities that are hard to come by in the case of crimes committed offline. This is due to the fact that actions carried out on a computer leaves traces and this fact gives a forensic examiner the chance to recreate and uncover what has happened. This data is often very valuable evidence.

As an end to this brief cybercrime discussion, we should not forget how digital evidence can play a big role even in crimes that are totally offline. Thing is, in modern society it is very hard to do anything without leaving digital traces. Even if you are doing something totally offline, in the heat of the moment or whatnot, there is a great chance that there can be digital evidence to support what happened. This can involve communication logs that can show what the criminal did after the crime was committed. Maybe he looked up punishments for the crime he committed, or even talked to some friend about what he did? I have even seen an example where a cell phone was used to tie a suspect to a crime scene, when the cell phone was not even used, it was just present!

2.1 Questions and Tasks

The task for this chapter is to get hold of two verdicts, then read them and consider how digital evidence what used in the cases. Try to get one verdict about a traditional cybercrime such as hacking or copyright infringement and one about something unrelated to the digital world, such as theft. In Sweden you can call a local court and have them send you verdicts over e-mail and you are often able to find verdicts online, just make sure you do not break any local laws!

References

- Kävrestad, J. (2014). Defining, categorizing and defending against online fraud.
- Rogers, L. (2000). Cybersleuthing: Means, Motive, and Opportunity. Available online: <http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitysum00.cfm> [fetched 2017-05-01].
- Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study* Doctoral dissertation, University of Manitoba.

Guide to Digital Forensics

A Concise and Practical Introduction

Kävrestad, J.

2017, XII, 147 p. 79 illus., Softcover

ISBN: 978-3-319-67449-0