Chapter 16
Novel First Responder Digital Forensics Tool as a Support to Law Enforcement

Mitko Bogdanoski
Military Academy "General Mihailo Apostolski", Macedonia

Marjan Stoilkovski
Ministry of Interior, Macedonia

Aleksandar Risteski
Ss. Cyril and Methodius University, Macedonia

ABSTRACT

There are many freeware and commercial tools which can be used to provide forensics information based on dead and live forensics acquisition. The main problem with these tools is that in many cases the investigator cannot explain the script functionality and generated results and information during the trial. Because of this reason there is an increased need for developing and using script which can be easy explained and adapted to any analysis which should be made by the examiners. The chapter presents a novel developed First Responder script which can be used to perform a live and dead forensics analysis in support of Law Enforcement during the investigation process.

INTRODUCTION

Nowadays, the security of information systems is crucial. There is almost no organization that does not take appropriate security measures on its own level in order to protect systems from external and internal attacks. To ensure an adequate level of security, the organizations have started establishing special CERT (*Community Emergency Response Team*) teams whose key objective is to increase information security in the organization. In case if there are no such teams established, this role is undertaken by system administrators, who must *attend specialized training* to perform those unique duties connected with cyber security.

In order to increase the information security and users' awareness, all the users of the information systems in the organization should be trained

DOI: 10.4018/978-1-4666-8793-6.ch016

about the secure usage of the systems, ethics in information system, and the way of reporting for any registered computer incident. The need for this training is because each of them can, intentionally or unintentionally, harm the security of the information systems, and consequently harm the security of the organization.

However, no matter how much the companies invest in information security and no matter how much the staff is trained, there will always be malicious users, which driven by different motives will try to exploit vulnerabilities in hardware and software solutions in the company, as well as employees' negligence. Very often, the attackers in their intentions are supported by internal attacks made by employees in companies (insiders).

The goal of the companies is to stop attackers in the perimeter network, i.e. not to allow them to enter the internal network of the company/organization. The reason for this is that when the attacker enters in the internal network and systems the only thing left is to resist malicious users using computer forensics. However, very often the responsible for information security in the companies cannot catch the attackers at the perimeter network, so after registering intrusion into the system they must react immediately and analyze the intentions of the attackers. In order the analysis to be at the highest level the responsible for information security must be trained to make a detailed analysis of the attack and, if it is possible, to discover as much information about the attacker. Sure that, even the attacker is discovered, the intrusion must be reported and companies need to ask for assistance from the competent authorities to tackle cyber threats (law enforcement), and to initiate appropriate action against the attackers.

In this whole process of discovering the intentions of the attack, as well as detection of offenders, the computer forensics takes a main role. In the process of information gathering basic analysis will be performed using traditional forensics, but if there is the slightest chance, live forensics should be performed on the running computer systems. Using the live response the investigator can capture all the volatile data that will be lost as soon as the machine is powered down, such as the current configuration of the machine and the data in its RAM memory. It should be noted that, whether traditional or live forensics is performed, during the entire process of systems' analysis the investigators should avoid possible corruption of the original data.

The purpose of this chapter is to provide basic concepts for live forensics and to explain its advantage when instead of automated software tools for computer forensics the investigators are using specially created scripts that are easy to adapt as necessary, i.e. accordingly to the needs of the forensic examiners. For this purpose, the rest of the chapter is organized as follows. Section 2 gives a brief overview of live computer forensics investigation process. Moreover, Section 3 explains how other disciplines are impacted by computer forensics. Section 4 shows the classification of the digital forensics as well as different models and frameworks for digital investigation process. Section 5 outlines the process of analysis of the RAM. In Section 6 the functionality and capabilities of the developed First Responder script are explained. Finally, the Section 7 concludes our work.

COMPUTER FORENSICS INVESTIGATION PROCESS

Digital forensics, as a branch of forensic, is a process of discovering and interpreting of the electronic data that would later be used in court. In fact, according to (Politt, 2004), the digital forensics is not just a process, but a group of processes used in the investigation. The purpose of these processes is to provide evidence in its most original form while performing investigation by collecting, identifying and validating the digital information in order to reconstruct some events