Chapter 13
Memory Based Anti-Forensic Tools and Techniques

Hamid Jahankhani
University of East London, UK

Elidon Beqiri
University of East London, UK

ABSTRACT

Computer forensics is the discipline that deals with the acquisition, investigation, preservation and presentation of digital evidence in the court of law. Whereas anti-forensics is the terminology used to describe malicious activities deployed to delete, alter or hide digital evidence with the main objective of manipulating, destroying and preventing the creation of evidence .Various anti-forensic methodologies and tools can be used to interfere with digital evidence and computer forensic tools. However, memory-based anti-forensic techniques are of particular interest because of their effectiveness, advanced manipulation of digital evidence and attack on computer forensic tools. These techniques are mainly performed in volatile memory using advanced data alteration and hiding techniques. For these reasons memory-based anti-forensic techniques are considered to be unbeatable. This chapter aims to present some of the current anti-forensic approaches and in particular reports on memory-based anti-forensic tools and techniques.

INTRODUCTION

The advent of Information Technology and personal computers has transformed significantly our way of living. Most of our day to day activities rely heavily upon the use of electronic devices and digital communications. More people are relying on these technologies to learn, work and entertain. In 2003, USA Census Bureau estimated that sixty-two percent of the households had access to a personal computer while fifty-five percent had access to the internet (Census, 2003). Without doubts digital communications can be considered as one of the greatest inventions of the last century because of its impact and benefits on the society.

On the other hand, digital communications have provided new opportunities for criminals

DOI: 10.4018/978-1-61692-000-5.ch013

and shaped the ways they commit crime (Shinder, 2002). Criminals are exploiting now digital communications to commit a wide range of crimes such as identity theft, online piracy, financial fraud, terrorism and pornography distribution. Furthermore the incidences of some of types of crimes increased significantly with the introduction of digital communications and personal computers. For example, internet communications have escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution and the ease of its accessibility (Wortley, 2004).

According to Bruce Schneier, electronic crime is flourishing because of three main reasons: a). automation, b) action at distance, c) technique propagation (Schneier, 2000).

a) Automation: Software packages are used to perform repetitive tasks and cross reference more and more data.
b) Action at distance: We live in a global digital communication era. Criminals perform electronic crimes in distance and with a high rate of anonymity.
c) Technique Propagation: successful electronic crime techniques and malicious software is propagated easily through the internet.

Law enforcement agencies have started dealing with crimes involving electronic devices and communications since the 1970's when these technologies were introduced. These were coined as electronic crimes since electronic devices and digital communications were used to commit them; while electronic evidence was defined as information or data of investigative value that is stored or transmitted by electronic devices (Ashcroft, 2001).

Law enforcement investigators initially considered electronic evidence as any other type of evidence; however they realised soon that this was not the case and that the conventional approach was not suitable to collect, preserve and analyze electronic evidence. This is because "conventional evidence lives in an analog world, whereas computer-derived evidence comes from a digital world and the transition between these worlds is not always as smooth as one would hope" (Johansson, 2002).

Computer forensics was then established as a discipline to support law enforcement agencies in their fight against electronic crime. Computer forensics deals with the acquisition, investigation, preservation and presentation of digital evidence in the court of law with the final objective of finding evidence that would lead to prosecution. Computer forensics is also known as cyber forensics since it deals with crimes committed in the cyber world (electronic world). The main areas of searching for evidence are: hard drives, removable devices, volatile memory, deleted or hidden files, password protected files, pornographic material etc.

The most important input of a computer forensic investigation is the digital evidence. Digital evidence can be envisaged as the counterpart of fingerprints or DNA in the digital world. Criminals will attempt to cover the traces of their malicious work by using anti-forensic methods to manipulate and tamper the evidence or interfere directly with the process (Harris, 2006).

Anti-forensics is the terminology used to define the activities of hackers or other cyber criminals aiming to undermine or mislead a computer forensic investigation. There are no well-established definitions regarding this discipline since it is quite new and it is yet to be explored. Peron and Legary define it as *"..four categories of evidence destruction, evidence source elimination, evidence hiding and evidence counterfeiting…."(*Harris, 2006), while, Grugq, (Ruxcon, 2004) defines anti-forensics as "*[The attempt] to limit the quantity and quality of forensic evidence.* "

Although Anti-Forensics is a field under development, however, there are already categories of available tools. Grugq seems to be one of the most dedicated anti-forensic researchers so far. With more than five years of anti-forensic studies,

Related Content

An Iterative CrowWhale-Based Optimization Model for Energy-Aware Multicast Routing in IoT
Dipali K. Shende, Yogesh S. Angaland S.C. Patil. (2022). *International Journal of Information Security and Privacy (pp. 1-24).*
www.irma-international.org/article/an-iterative-crowwhale-based-optimization-model-for-energy-aware-multicast-routing-in-iot/300317

Security Issues of Blockchain-Based Information System to Manage Supply Chain in a Global Crisis
Kamalendu Pal (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 1240-1263).*
www.irma-international.org/chapter/security-issues-of-blockchain-based-information-system-to-manage-supply-chain-in-a-global-crisis/310506

Data Hiding Method Based on Inter-Block Difference in Eight Queens Solutions and LSB Substitution
Vinay Kumar, Abhishek Bansaland Sunil Kumar Muttoo (2014). *International Journal of Information Security and Privacy (pp. 55-68).*
www.irma-international.org/article/data-hiding-method-based-on-inter-block-difference-in-eight-queens-solutions-and-lsb-substitution/130655

Pilot Portfolio Model: Portuguese Navy
Ricardo Simplício, Jorge Gomesand Mário Romão (2020). *International Journal of Risk and Contingency Management (pp. 45-56).*
www.irma-international.org/article/pilot-portfolio-model/252181

Pilot Portfolio Model: Portuguese Navy
Ricardo Simplício, Jorge Gomesand Mário Romão (2020). *International Journal of Risk and Contingency Management (pp. 45-56).*
www.irma-international.org/article/pilot-portfolio-model/252181