Chapter 3
Digital Forensics of Cybercrimes and the Use of Cyber Forensics Tools to Obtain Digital Evidence

ABSTRACT

This chapter evaluates the most relevant methodologies and best practices for conducting digital investigations, preserving digital forensic evidence and following chain of custody (CoC) of cybercrimes. Cybercriminals are assuming new strategies to launch their sophisticated cyberattacks within the ever-changing digital ecosystems. The authors recommend that digital investigations must continually shift to tackle cybercrimes and prosecute cybercriminals to increase international collaboration networks, to share prevention knowledge, and to analyze lessons learned. They also establish a cyber forensics model for miscellaneous ecosystems called cyber forensics model in digital ecosystems (CFMDE). This chapter also reviews the most important categories of tools to conduct digital investigations. Nevertheless, as the cybercrime sophistication keeps improving, it is also necessary to harden technologies, techniques, methodologies, and tools to acquire digital evidence in order to support and make cyber investigation cases stronger.

DOI: 10.4018/978-1-7998-4162-3.ch003

INTRODUCTION

The Information Age has led to humanity an accelerated acceptance of technology in modern societies. This era empowers us to access information freely and the ability to access knowledge almost instantly. We no longer depend on personal computers to achieve this purpose; the vast proliferation of digital devices has allowed us to depend on technology. From laptops to tablets, from landlines to smart phones, from private networks to public wireless networks – all these technologies keep improving in terms of processing power, miniaturization, portability, display resolution, battery lifespan, storage and connectivity (Sabillon et al., 2014).

This technology blast has also created a negative effect, with the creation of computer related crimes or the use of digital devices to commit common crimes. To investigate the cybercriminality in more in-depth analysis, it was required the inception of computer forensics methodologies that over the years have evolved into cyberforensics or digital forensics.

Digital forensics is define as the use of scientific methodologies to preserve, collect, validate, identify, analyze, interpret, document and present evidence from digital devices for civil purposes, to prove and prosecute cybercrimes.

These days, cybercrime continues to escalate due to global connectivity, the advancements of networks, information exchange and the proliferation of mobile technologies. Moreover, digital investigators and prosecutors need to understand how cybercriminals act in order to understand their modus operandi including Techniques, Tactics and Procedures (TTP) of criminal hacking.

Cyberattacks constantly increase its sophistication to avoid detection, monitoring, remediation and eradication. The proliferation of digital devices has attracted endless possibilities to commit cybercrimes or to utilize these devices to perpetrate common crimes. Cybercriminals are frequently launching cyberattacks that are conducive to grow in sophistication, the adoption of anti-forensics techniques and the use of procedures to avoid cybercrime detection and tracing.

McAffee (2014) determined that cybercrime costs $ 400 billion to the global economy on an annual basis, but this can easily reach a maximum of $ 575 billion. Stolen personal information could cost $ 160 billion per annum, G20 nations experience most financial losses due to cybercrime activities especially the USA, China, Japan and Germany. Developing countries are only experiencing small losses yet this tendency will likely change in the future as business use Internet for commercial purposes particularly mobile