International Journal of Information Security and Privacy
Volume 11 • Issue 2 • April-June 2017

Digital Forensic Analysis of Cybercrimes:
Best Practices and Methodologies

Regner Sabillon, Universitat Oberta de Catalunya, Barcelona, Spain
Jordi Serra-Ruiz, Universitat Oberta de Catalunya, Barcelona, Spain
Victor Cavaller, Universitat Oberta de Catalunya, Barcelona, Spain
Jeimy J. Cano, Universidad de los Andes, Bogota, Colombia

ABSTRACT

This paper reviews the existing methodologies and best practices for digital investigations phases like collecting, evaluating and preserving digital forensic evidence and chain of custody of cybercrimes. Cybercriminals are adopting new strategies to launch cyberattacks within modified and ever changing digital ecosystems, this article proposes that digital investigations must continually readapt to tackle cybercrimes and prosecute cybercriminals, working in international collaboration networks, sharing prevention knowledge and lessons learned. The authors also introduce a compact cyber forensics model for diverse technological ecosystems called Cyber Forensics Model in Digital Ecosystems (CFMDE). Transferring the knowledge, international collaboration, best practices and adopting new digital forensic tools, methodologies and techniques will be hereinafter paramount to obtain digital evidence, enforce organizational cybersecurity policies, mitigate security threats, fight anti-forensics practices and indict cybercriminals. The global Digital Forensics community ought to constantly update current practices to deal with cybercriminality and foreseeing how to prepare to new technological environments where change is always constant.

KEYWORDS

Cybercrime, Digital Evidence, Digital Forensic Methodologies, Digital Forensic Procedures, Digital Investigations

1. INTRODUCTION

Nowadays, cybercrime continues to grow at accelerated rates due to global connectivity and the advancements of networks, information exchange and mobile technologies. Furthermore, digital investigators and prosecutors need to understand how cybercriminals behave in order to assimilate their modus operandi including Techniques, Tactics and Procedures (TTP) of criminal hacking.

Cyberattacks continually increase its sophistication to avoid detection, monitoring, remediation and eradication. The proliferation of digital devices has attracted countless possibilities to commit cybercrimes or to utilize these devices to perpetrate common crimes.

Cybercriminals are continually launching cyberattacks that tend to grow in sophistication, the adoption of anti-forensics techniques and the use of procedures to avoid cybercrime detection and tracing.

In 2015, the IC3-FBI received over 8,000 complaints with a combined loss of around $ 275 million, the IC3 dealt with 3,463,620 cybercrime complaints during a period of six years (2010-2015) and they estimate that only 15% of the cyber victims file a complaint. According to their Internet Crime Report (2015), the top 5 cyber victimization by country occurs in the USA, UK, Nigeria,

DOI: 10.4018/IJISP.2017040103

China and India mostly linked to non-delivery of products or payment, 419 schemes, identity theft, online auctions, personal data breach, cyber extortion, employment fraud, credit cards, phishing and cyber harassment. The IC3 follows specific procedures to fight cybercrime including detection, victim complaint, mitigation, liaison with industry/law enforcement, cybercrime analysis, deterrence, investigation, prosecution and prevention.

McAffee (2014) estimated 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 trend will likely change in the future as business use Internet for commercial purposes particularly mobile platforms and network connectivity. Nevertheless, most cybercrime activities go unreported on the organizational level to avoid further impacts like harming business operations, customer relationships and company reputations. The cybercrime effect targeting end users is not different when it comes to the theft of personal information.

For years, digital forensics methodologies and practices have not been evolving at the same rate that cybercriminality exploits Information and Communication Technologies (ICT) vulnerabilities. In our paper, we evaluate existing methods and how is necessary to revisit cybercrime and digital investigations operations to cover a vast number of technological environments. Our proposed Cyber Forensics Model combines the most relevant phases of digital investigations and targets multiple environments in digital ecosystems.

Arief et al. (2015) argue that because cybercrime losses are normally presented using surveys, these surveys do not provide a representative sample of the losses. Furthermore, surveys can be distorted and it does not exist an authoritative source for calculating cybercrime losses as many incidents are never reported to not lose reputation. They highlight that the number of cybercrime losses is arguable but what is undeniable is the rising threat of cybercrime. In order to examine how cybercrime operates, we ought to comprehend the attackers, the defenders and the victim's environments.

This paper studies in Section 2 the new digital ecosystems for cybercriminality; the literature review in Section 3 compares 26 Digital Forensic methodologies organized in three periods (1984-2006; 2007-2010 and 2011-2016). Section 4 highlights the importance of Digital Forensic investigations; Section 5 presents an overview of Digital Forensics tools and in Section 6 we emphasize the importance of digital evidence to prosecute cybercriminals. In Section 7, we propose our Cyber Forensics Model in Digital Ecosystems (CFMDE) and Section 8 includes concluding remarks and future work.

2. DIGITAL ECOSYSTEMS FOR CYBERCRIMINAL

According to Cano (2016), cybercriminals modus operandi has been elevated from traditional cyber operations to cybercrime digital ecosystems where they take advantage of logic infrastructures, digital platforms and highly connected users. He defines a Criminal Digital Ecosystem (CDEco), as the group of relationships between local and global participants that interact to create a flexible network to engage in criminal activities by exploiting vulnerabilities of cyber victims; above all, aiming at specific goals under full anonymity and leaving untraceable digital evidence when possible.

He argues that the intent of the cybercriminal's actions is set on five premises:

1. Maximum effectiveness with minimum effort;
2. Maximum anonymity, with the minimum possible evidence;
3. Maximum legal ambiguity, with minimal technological knowledge available;
4. The use of free digital platforms, assisted by specialized communities;