

Chapter 29

Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies

Regner Sabillon

Universitat Oberta de Catalunya, Spain

Jordi Serra-Ruiz

Universitat Oberta de Catalunya, Spain

Victor Cavaller

Universitat Oberta de Catalunya, Spain

Jeimy J. Cano

Universidad de los Andes, 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.

DOI: 10.4018/978-1-5225-3822-6.ch029

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, 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.

McAfee (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

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/digital-forensic-analysis-of-cybercrimes/189493

Related Content

Blog Snippets Based Drug Effects Extraction System Using Lexical and Grammatical Restrictions

Shiho Kitajima, Rafal Rzepka and Kenji Araki (2014). *International Journal of Multimedia Data Engineering and Management* (pp. 1-17).

www.irma-international.org/article/blog-snippets-based-drug-effects-extraction-system-using-lexical-and-grammatical-restrictions/113304

Managerial Computer Business Games

Luigi Proserpio, Massimo Magni and Bernardino Provera (2011). *Gaming and Simulations: Concepts, Methodologies, Tools and Applications* (pp. 1513-1520).

www.irma-international.org/chapter/managerial-computer-business-games/49463

ClassSim: An Approach to Educator Development Through a Simulation

Brian Ferry, Lisa Kervin and Lisa Carrington (2011). *Gaming and Simulations: Concepts, Methodologies, Tools and Applications* (pp. 956-970).

www.irma-international.org/chapter/classsim-approach-educator-development-through/49429

A Real-Time 3D Visualization Framework for Multimedia Data Management, Simulation, and Prediction: Case Study in Geospatial-Temporal Biomedical Disease Surveillance Networks

Nathaniel Rossol, Irene Cheng, Iqbal Jamal, John Berezowski and Anup Basu (2011). *International Journal of Multimedia Data Engineering and Management* (pp. 1-18).

www.irma-international.org/article/real-time-visualization-framework-multimedia/54459

A Real-Time 3D Visualization Framework for Multimedia Data Management, Simulation, and Prediction: Case Study in Geospatial-Temporal Biomedical Disease Surveillance Networks

Nathaniel Rossol, Irene Cheng, Iqbal Jamal, John Berezowski and Anup Basu (2011). *International Journal of Multimedia Data Engineering and Management* (pp. 1-18).

www.irma-international.org/article/real-time-visualization-framework-multimedia/54459